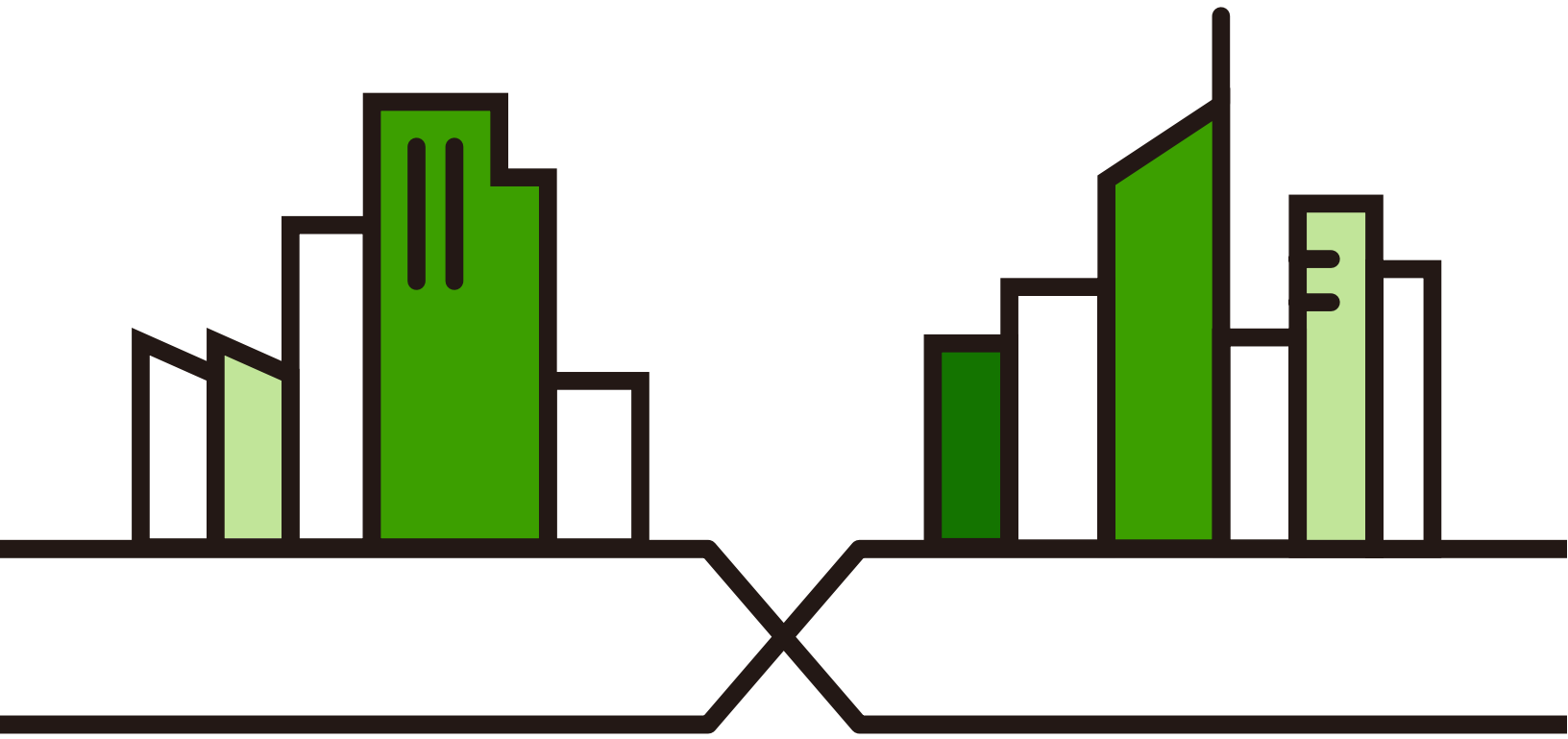
ZYXEL NETWORKS

CLI Reference Guide

ZyWALL ZLD Series

Default Login Details	
LAN Port IP Address	https://192.168.1.1
User Name	admin
Password	See Zyxel Device label or 1234

Version 4.10–5.42 Ed1, 2/2026



Copyright © 2026 Zyxel and/or its affiliates. All rights reserved.

IMPORTANT!
READ CAREFULLY BEFORE USE.
KEEP THIS GUIDE FOR FUTURE REFERENCE.

This is a Reference Guide for a series of products intended for people who want to configure the Zyxel Device via Command Line Interface (CLI).

Note: The version number on the cover page refers to the latest firmware version supported by the Zyxel Device at the time of writing.

How To Use This Guide

1 Read Chapter 1 on page 26 for how to access and use the CLI (Command Line Interface).

2 Read Chapter 2 on page 42 to learn about the CLI user and privilege modes.

Some commands or command options in this guide may not be available in your product. See your product's User's Guide for a list of supported features.
Do not use commands not documented in this guide. Use of undocumented commands or misconfiguration can damage the unit and possibly render it unusable.
Some commands are renamed between firmware versions. In cases where a command has multiple names, the Reference Guide lists each variation.

Related Documentation

- Quick Start Guide

  The Quick Start Guide shows how to connect the Zyxel Device and access the Web Configurator.

- User's Guide

  The ZyWALL USG, ATP, USG FLEX and VPN series User Guides explain how to use the Web Configurator to configure the Zyxel Device. It also shows the product feature matrix for each device. General feature differences are written in the Introduction chapter while a more detailed table is in the Product Feature appendix.

Note: It is recommended you use the Web Configurator to configure the Zyxel Device.

- More Information

  Go to support.zyxel.com to find other information on Zyxel Device.

Contents Overview

Introduction 25

Command Line Interface 26
User and Privilege Modes 42

Reference 44

Object Reference 45
Status 47
Registration 53
AP Management 56
Built-in AP 67
AP Group 69
Wireless LAN Profiles 76
Rogue AP 97
Wireless Health 101
Wireless Frame Capture 106
Dynamic Channel Selection 109
Auto-Healing 110
LEDs 112
Interfaces 114
Trunks 162
Route 166
Routing Protocol 176
Zones 183
DDNS 186
Virtual Servers 189
HTTP Redirect 200
Redirect Service 202
ALG 206
UPnP 209
IP/MAC Binding 212
Layer 2 Isolation 214
Secure Policy 217
Cloud CNM 239
Web Authentication 251
Hotspot 262
IPSec VPN 277
SSL VPN 295
L2TP VPN 299

Bandwidth Management 307
Application Patrol 313
Anti-Virus 316
RTLS 324
Reputation Filter 326
Sandboxing 345
IDP Commands 348
Content Filtering 365
Anti-Spam 399
Collaborative Detection & Response 411
SSL Inspection 418
IP Exception 426
Device HA 428
Device Insight 438
User/Group 443
Application Object 455
Addresses 458
Services 467
Schedules 470
AAA Server 472
Authentication Objects 479
Authentication Server 490
Certificates 492
ISP Accounts 498
SSL Application 501
DHCPv6 Objects 504
Dynamic Guest Accounts 507
System 510
System Remote Management 526
File Manager 539
Logs 565
Reports and Reboot 572
Diagnostics and Remote Assistance 578
Session Timeout 581
Packet Flow Explore 582
Maintenance Tools 586
Miscellaneous 597
Managed AP Commands 604

Table of Contents

Contents Overview 3

Table of Contents 5

Part I: Introduction 25

Chapter 1
Command Line Interface 26

1.1 Overview 26
1.1.1 The Configuration File 27
1.2 Accessing the CLI 28
1.2.1 Console Port 28
1.2.2 Web Configurator Console 29
1.2.3 Telnet 30
1.2.4 SSH (Secure SHell) 30
1.3 How to Find Commands in this Guide 31
1.4 How Commands Are Explained 31
1.4.1 Background Information (Optional) 31
1.4.2 Command Input Values (Optional) 32
1.4.3 Command Summary 32
1.4.4 Command Examples (Optional) 32
1.4.5 Command Syntax 32
1.4.6 Naming Conventions 32
1.4.7 Changing the Password 33
1.4.8 Idle Timeout 33
1.5 CLI Modes 33
1.6 Shortcuts and Help 34
1.6.1 List of Available Commands 34
1.6.2 List of Sub-commands or Required User Input 35
1.6.3 Entering Partial Commands 35
1.6.4 Entering a ? in a Command 36
1.6.5 Command History 36
1.6.6 Navigation 36
1.6.7 Erase Current Command 36
1.6.8 The no Commands 36
1.7 Input Values 36
1.8 Ethernet Interfaces 40
1.9 Saving Configuration Changes 40

1.10 Logging Out 41
1.11 Resetting the Zyxel Device 41

Chapter 2
User and Privilege Modes 42

2.1 User And Privilege Modes 42

Part II: Reference 44

Chapter 3
Object Reference 45

3.1 Object Reference Commands 45
3.1.1 Object Reference Command Example 46

Chapter 4
Status 47

4.1 ATP Dashboard Commands 51
4.2 CPU Temperature Monitor Commands 52
4.3 System Protection Signature Commands 52

Chapter 5
Registration 53

5.1 Registration Overview 53
5.2 myZyxel Overview 53
5.2.1 Subscription Services Available on the Zyxel Device 53
5.3 Registration Commands 54
5.3.1 Command Examples 55
5.4 Update License Commands 55

Chapter 6
AP Management 56

6.1 AP Management Overview 56
6.1.1 AP Modes 56
6.1.2 Airtime Fairness 57
6.2 AP Management Value 57
6.3 General AP Management Commands 57
6.3.1 AP Management Commands Example 62
6.4 Remote AP 64
6.4.1 Remote AP Notes 65
6.4.2 Remote AP Commands 66

Chapter 7
Built-in AP 67

7.1 Built-in AP Commands 67

Chapter 8
AP Group 69

8.1 Wireless Load Balancing Overview 69
8.2 AP Group Commands 69
8.2.1 AP Group Examples 73

Chapter 9
Wireless LAN Profiles 76

9.1 Wireless LAN Profiles Overview 76
9.2 AP Radio & Monitor Profile Commands 76
9.2.1 AP Radio & Monitor Profile Commands Example 85
9.3 SSID Profile Commands 86
9.3.1 SSID Profile Example 89
9.4 Security Profile Commands 89
9.4.1 Security Profile Example 92
9.4.2 SSID and Security Profiles Example 93
9.5 MAC Filter Profile Commands 94
9.5.1 MAC Filter Profile Example 94
9.6 ZyMesh Profile Commands 95

Chapter 10
Rogue AP 97

10.1 Rogue AP Detection Overview 97
10.2 Rogue AP Detection Commands 97
10.2.1 Rogue AP Detection Examples 98
10.3 Rogue AP Containment Overview 99
10.4 Rogue AP Containment Commands 100
10.4.1 Rogue AP Containment Example 100

Chapter 11
Wireless Health 101

11.1 Wireless Health Overview 101
11.2 Wireless Health Commands 101
11.2.1 Wireless Health Radio and Station Settings 103
11.2.2 Wireless Health Radio and Station Actions 104
11.2.3 Wireless Health Command Examples 104

Chapter 12
Wireless Frame Capture 106

12.1 Wireless Frame Capture Overview 106
12.2 Wireless Frame Capture Commands 106
12.2.1 Wireless Frame Capture Examples 107
12.2.2 Remote Packet Capture 107

Chapter 13
Dynamic Channel Selection 109

13.1 DCS Overview 109
13.2 DCS Commands 109

Chapter 14
Auto-Healing 110

14.1 Auto-Healing Overview 110
14.2 Auto-Healing Commands 110
14.2.1 Auto-Healing Examples 111

Chapter 15
LEDs 112

15.1 LED Suppression Mode 112
15.2 LED Suppression Commands 112
15.2.1 LED Suppression Commands Example 112
15.3 LED Locator 112
15.4 LED Locator Commands 113
15.4.1 LED Locator Commands Example 113

Chapter 16
Interfaces 114

16.1 Interface Overview 114
16.1.1 Types of Interfaces 114
16.1.2 Relationships Between Interfaces 116
16.2 Interface General Commands Summary 118
16.2.1 Basic Interface Properties and IP Address Commands 118
16.2.2 IGMP Proxy Commands 125
16.2.3 Proxy ARP Commands 126
16.2.4 DHCP Setting Commands 127
16.2.5 Interface Parameter Command Examples 132
16.2.6 RIP Commands 133
16.2.7 OSPF Commands 134
16.2.8 Connectivity Check (Ping-check) Commands 135
16.3 Ethernet Interface Specific Commands 136
16.3.1 MAC Address Setting Commands 137
16.3.2 Port Grouping Commands 137
16.4 Virtual Interface Specific Commands 139

16.4.1 Virtual Interface Command Examples 139
16.5 PPPoE/PPTP Specific Commands 139
16.5.1 PPPoE/PPTP Interface Command Examples 141
16.6 Cellular Interface Specific Commands 141
16.6.1 Cellular Status 144
16.6.2 Cellular Interface Command Examples 146
16.7 Tunnel Interface Specific Commands 147
16.7.1 Tunnel Interface Command Examples 148
16.8 USB Storage Specific Commands 149
16.8.1 Firmware Upgrade via USB Stick 150
16.8.2 USB Storage Commands Example 152
16.9 VLAN Interface Specific Commands 152
16.9.1 VLAN Interface Command Examples 153
16.10 Bridge Specific Commands 153
16.10.1 Bridge Interface Command Examples 154
16.11 LAG Commands 154
16.11.1 LAG Interface Command Example 157
16.12 VTI Commands 158
16.12.1 Restrictions for IPsec Virtual Tunnel Interface 158
16.12.2 VTI Interface Command Example 161

Chapter 17
Trunks 162

17.1 Trunks Overview 162
17.2 Trunk Scenario Examples 162
17.3 Trunk Commands Input Values 163
17.4 Trunk Commands Summary 163
17.5 Trunk Command Examples 164

Chapter 18
Route 166

18.1 Policy Route 166
18.1.1 Source Network Address Translation (SNAT) 166
18.2 Policy Route Commands 167
18.2.1 Assured Forwarding (AF) PHB for DiffServ 172
18.2.2 Policy Route Command Example 172
18.3 IP Static Route 173
18.4 Static Route Commands 174
18.4.1 Static Route Commands Examples 175

Chapter 19
Routing Protocol 176

19.1 Routing Protocol Overview 176

19.2 Routing Protocol Commands Summary 176
19.2.1 RIP Commands 177
19.2.2 General OSPF Commands 177
19.2.3 OSPF Area Commands 178
19.2.4 Virtual Link Commands 178
19.2.5 Learned Routing Information Commands 179
19.2.6 Show IP Route Command Example 179
19.3 BGP (Border Gateway Protocol) 179
19.3.1 BGP Commands 181

Chapter 20
Zones 183

20.1 Zones Overview 183
20.2 Zone Commands Summary 184
20.2.1 Zone Command Examples 185

Chapter 21
DDNS 186

21.1 DDNS Overview 186
21.2 DDNS Commands Summary 186
21.3 DDNS Commands Example 188

Chapter 22
Virtual Servers 189

22.1 Virtual Server Overview 189
22.1.1 1:1 NAT and Many 1:1 NAT 189
22.2 Virtual Server Commands Summary 189
22.2.1 Virtual Server Command Examples 191
22.2.2 Tutorial - How to Allow Public Access to a Server 192
22.3 Virtual Server Load Balancing 193
22.3.1 Load Balancing Example 1 193
22.3.2 Load Balancing Example 2 194
22.3.3 Virtual Server Load Balancing Process 194
22.3.4 Load Balancing Rules 195
22.3.5 Virtual Server Load Balancing Algorithms 196
22.3.6 Virtual Server Load Balancing Commands 197

Chapter 23
HTTP Redirect 200

23.1 HTTP Redirect Overview 200
23.1.1 Web Proxy Server 200
23.2 HTTP Redirect Commands 200
23.2.1 HTTP Redirect Command Examples 201

Chapter 24
Redirect Service 202

24.1 HTTP Redirect 202
24.2 SMTP Redirect 202
24.3 Redirect Commands 202
24.3.1 Redirect Command Example 205

Chapter 25
ALG 206

25.1 ALG Introduction 206
25.2 ALG Commands 207
25.3 ALG Commands Example 208

Chapter 26
UPnP 209

26.1 UPnP and NAT-PMP Overview 209
26.2 UPnP and NAT-PMP Commands 209
26.3 UPnP & NAT-PMP Commands Example 210

Chapter 27
IP/MAC Binding 212

27.1 IP/MAC Binding Overview 212
27.2 IP/MAC Binding Commands 212
27.3 IP/MAC Binding Commands Example 213

Chapter 28
Layer 2 Isolation 214

28.1 Layer 2 Isolation Overview 214
28.2 Layer 2 Isolation Commands 215
28.2.1 Layer 2 Isolation White List Sub-Commands 215
28.3 Layer 2 Isolation Commands Example 216

Chapter 29
Secure Policy 217

29.1 Secure Policy Overview 217
29.2 Secure Policy Commands 218
29.2.1 Secure Policy Sub-Commands 221
29.2.2 Security Services Multiple Profiles 223
29.2.3 Secure Policy Command Examples 224
29.3 Output Control Commands 228
29.3.1 Output Control Sub-Commands 230
29.4 Session Limit Commands 230
29.5 ADP Commands Overview 232

29.5.1 ADP Command Input Values 233
29.5.2 ADP Activation Commands 233
29.5.3 ADP Global Profile Commands 233
29.5.4 ADP Zone-to-Zone Rule Commands 234
29.5.5 ADP Add/Edit Profile Sub Commands 234
29.5.6 ADP Flood Detection Whitelist Commands 237

Chapter 30
Cloud CNM 239

30.1 Cloud CNM Overview 239
30.2 Cloud CNM SecuManager 239
30.2.1 Introduction to XMPP 240
30.2.2 Cloud CNM SecuManager Commands 241
30.2.3 Cloud CNM SecuManager Command Example 244
30.3 Cloud CNM SecuReporter 244
30.3.1 Cloud CNM SecuReporter Commands 245
30.3.2 Cloud CNM SecuReporter Commands Example 247
30.4 Management Modes 247
30.5 Nebula 248
30.6 Cloud Monitoring Mode 248
30.6.1 Nebula Monitor Mode Command 249

Chapter 31
Web Authentication 251

31.1 Web Authentication Overview 251
31.1.1 User Two-Factor Authentication 251
31.1.2 802.1X Single Sign-On 252
31.1.3 Summary of User Authentication Methods 252
31.2 Web Authentication Commands 253
31.2.1 web-auth login setting Sub-commands 255
31.2.2 web-auth policy Sub-commands 256
31.2.3 Facebook Wi-Fi Commands 258
31.3 SSO Overview 258
31.3.1 SSO Configuration Commands 259
31.3.2 SSO Show Commands 259
31.3.3 Command Setup Sequence Example 260
31.3.4 Two-Factor Web Authentication Command Example 260

Chapter 32
Hotspot 262

32.1 Hotspot Overview 262
32.2 Billing Overview 262
32.3 Billing Commands 262

32.3.1 Billing Profile Sub-commands 264
32.3.2 Billing Command Example 264
32.3.3 Payment Service 266
32.4 Printer Manager Overview 269
32.5 Printer-manager Commands 269
32.5.1 Printer-manager Printer Sub-commands 270
32.5.2 Printer-manager Command Example 270
32.6 Free Time Overview 271
32.7 Free-Time Commands 271
32.8 Free-Time Commands Example 272
32.9 IPnP Overview 272
32.10 IPnP Commands 272
32.11 IPnP Commands Example 273
32.12 Walled Garden Overview 273
32.13 Walled Garden Commands 273
32.13.1 walled-garden rule Sub-commands 274
32.13.2 walled-garden domain-ip rule Sub-commands 275
32.13.3 Walled Garden Command Example 275
32.14 Advertisement Overview 275
32.15 Advertisement Commands 276
32.15.1 Advertisement Command Example 276

Chapter 33
IPSec VPN 277

33.1 IPSec VPN Overview 277
33.2 IPSec VPN Commands Summary 278
33.2.1 IPv4 IKEv1 SA Commands 278
33.2.2 IPv4 IPSec SA Commands (except Manual Keys) 281
33.2.3 IPv4 IPSec SA Commands (for Manual Keys) 285
33.2.4 VPN Concentrator Commands 286
33.2.5 VPN Configuration Provisioning Commands 286
33.2.6 SA Monitor Commands 288
33.2.7 IPv4 IKEv2 SA Commands 289
33.2.8 IPv6 IKEv2 SA Commands 290
33.2.9 IPv6 IPSec SA Commands 292
33.2.10 IPv6 VPN Concentrator Commands 294

Chapter 34
SSL VPN 295

34.1 SSL Access Policy 295
34.1.1 SSL Application Objects 295
34.1.2 SSL Access Policy Limitations 295
34.2 SSL VPN Commands 295

34.2.1 SSL VPN Commands 296
34.2.2 Setting an SSL VPN Rule Tutorial 297

Chapter 35
L2TP VPN 299

35.1 L2TP VPN Overview 299
35.2 IPSec Configuration 299
35.2.1 Using the Default L2TP VPN Connection 299
35.3 LAN Policy Route 300
35.4 WAN Policy Route 300
35.5 L2TP VPN Commands 301
35.5.1 L2TP VPN Commands 301
35.5.2 L2TP Account Commands 303
35.6 L2TP VPN Examples 303
35.6.1 Configuring the Default L2TP VPN Gateway Example 304
35.6.2 Configuring the Default L2TP VPN Connection Example 304
35.6.3 Configuring the L2TP VPN Settings Example 305
35.6.4 Configuring the LAN Policy Route for L2TP Example 305
35.6.5 Configuring the WAN Policy Route for L2TP Example 306

Chapter 36
Bandwidth Management 307

36.1 Bandwidth Management Overview 307
36.1.1 BWM Type 307
36.2 Bandwidth Management Commands 307
36.2.1 Bandwidth Sub-Commands 308
36.3 Bandwidth Management Commands Examples 311

Chapter 37
Application Patrol 313

37.1 Application Patrol Overview 313
37.2 Application Patrol Commands Summary 313
37.2.1 Application Patrol Commands 313

Chapter 38
Anti-Virus 316

38.1 Anti-Virus Overview 316
38.2 Anti-Virus Commands 316
38.2.1 General Anti-Virus Commands 316
38.2.2 Anti-Virus Profile 318
38.2.3 White and Black Lists 319
38.2.4 Signature Search Anti-Virus Command 321
38.3 Update Anti-Virus Signatures 322

38.3.1 Update Signature Examples 322
38.4 Anti-Virus Statistics 323
38.4.1 Anti-Virus Statistics Example 323

Chapter 39
RTLS 324

39.1 RTLS Overview 324
39.1.1 RTLS Configuration Commands 325
39.1.2 RTLS Configuration Examples 325

Chapter 40
Reputation Filter 326

40.1 Overview 326
40.1.1 Signature Database Priority 327
40.2 IP Reputation Commands 327
40.2.1 Update IP Reputation Signatures 329
40.2.2 IP Reputation Statistics 329
40.2.3 IP Reputation External Black List 329
40.3 URL Threat Filter Commands 331
40.3.1 URL Threat Filter Command Examples 333
40.3.2 URL Threat Filter Profile Commands 334
40.3.3 URL Threat Filter External Black List 335
40.3.4 Update URL Threat Filter Signatures 337
40.3.5 Update Signature Examples 338
40.3.6 URL Threat Filter Statistics 338
40.3.7 URL Threat Filter Statistics Example 339
40.4 DNS Threat Filter Commands 341
40.5 Blocking Secure DNS Query Packets Command Examples 344

Chapter 41
Sandboxing 345

41.1 Sandboxing Overview 345
41.2 Sandbox Commands 345
41.2.1 Sandbox Command Examples 347

Chapter 42
IDP Commands 348

42.1 Overview 348
42.2 General IDP Commands 349
42.2.1 IDP Activation 349
42.3 IDP Profile Commands 350
42.3.1 Global Profile Commands 350
42.3.2 Editing/Creating IDP Signature Profiles 351

42.3.3 Editing Rate Based Signatures Profiles 352
42.3.4 Signature Search 353
42.4 IDP Custom Signatures 355
42.4.1 Custom Signature Examples 356
42.5 Update IDP Signatures 359
42.5.1 Update Signature Examples 360
42.6 IDP Statistics 360
42.6.1 IDP Statistics Example 362
42.7 IDP White List 362
42.8 IDP Packet Capture 363
42.8.1 IDP Packet Capture Example 364

Chapter 43
Content Filtering 365

43.1 Content Filtering Overview 365
43.1.1 Web Content Filter 365
43.1.2 DNS Content Filter 365
43.2 External Web Filtering Service 366
43.3 Content Filter Command Input Values 367
43.4 Web Content Filter 369
43.4.1 General Web Content Filter Commands 369
43.4.2 Web Content Filter Profile Commands 371
43.4.3 Web Content Filtering Statistics 376
43.4.4 Web Content Filtering Statistics Example 376
43.5 DNS Content Filter 376
43.5.1 DNS Content Filter Commands 377
43.5.2 DNS Content Filter Profile Commands 378
43.5.3 DNS Content Filtering Statistics 379
43.6 Web Content Filtering Example 379
43.7 Content Filter Category Definitions 382
43.8 Web Content Filter Example 395
43.9 DNS Content Filter Example 396

Chapter 44
Anti-Spam 399

44.1 Anti-Spam Overview 399
44.2 Anti-Spam Commands 399
44.2.1 Anti-Spam Profile Rules 399
44.2.2 White and Black Lists 404
44.2.3 DNSBL Anti-Spam Commands 406
44.3 Anti-Spam Statistics 409
44.3.1 Anti-Spam Statistics Example 410

Chapter 45
Collaborative Detection & Response 411

45.1 Overview 411
45.1.1 CDR Example Scenario 411
45.2 Before You Begin 412
45.3 CDR Commands 413
45.3.1 CDR General Commands 413
45.3.2 CDR Show Commands 416
45.3.3 Update CDR Signatures 416

Chapter 46
SSL Inspection 418

46.1 SSL Inspection Overview 418
46.2 SSL Inspection Commands Summary 418
46.2.1 SSL Inspection General Settings 419
46.2.2 SSL Inspection Exclusion Command Input Values 420
46.2.3 SSL Inspection Exclusion Commands 420
46.2.4 SSL Inspection Profile Settings 422
46.2.5 SSL Inspection Certificate Cache 423
46.2.6 SSL Inspection Certificate Update 423
46.2.7 SSL Inspection Statistics 424
46.2.8 SSL Inspection Command Examples 424

Chapter 47
IP Exception 426

47.1 IP Exception Overview 426
47.2 IP Exception Commands 426

Chapter 48
Device HA 428

48.1 Device HA Overview 428
48.1.1 Before You Begin 428
48.1.2 Device HA and Device HA Pro 429
48.2 General Device HA Commands 430
48.3 Active-Passive Mode Device HA 430
48.4 Active-Passive Mode Device HA Commands 431
48.4.1 Active-Passive Mode Device HA Commands 431
48.4.2 Active-Passive Mode Device HA Command Example 433
48.5 Device HA Pro 433
48.5.1 Deploying Device HA Pro 433
48.5.2 Device HA Pro Commands 434
48.5.3 Device HA2 Command Example 436

Chapter 49
Device Insight 438

49.1 Device Insight Overview 438
49.1.1 Device Insight Commands 439
49.1.2 Device Insight Command Examples 440

Chapter 50
User/Group 443

50.1 User Account Overview 443
50.1.1 User Types 443
50.2 User/Group Commands Summary 444
50.2.1 User Commands 444
50.2.2 User Group Commands 446
50.2.3 User Setting Commands 446
50.2.4 MAC Auth Commands 449
50.2.5 Additional User Commands 451

Chapter 51
Application Object 455

51.1 Application Object Commands Summary 455
51.1.1 Application Object Commands 455
51.1.2 Application Object Group Commands 456

Chapter 52
Addresses 458

52.1 Address Overview 458
52.2 Address Commands Summary 458
52.2.1 Address Object Commands 459
52.2.2 Address Group Commands 463
52.2.3 FQDN Object 464
52.2.4 Geo IP 465
52.2.5 FQDN / Geo IP Commands 465
52.2.6 Geo IP Command Examples 466

Chapter 53
Services 467

53.1 Services Overview 467
53.2 Services Commands Summary 467
53.2.1 Service Object Commands 467
53.2.2 Service Group Commands 469

Chapter 54
Schedules 470

54.1 Schedule Overview 470
54.2 Schedule Commands Summary 470
54.2.1 Schedule Command Examples 471

Chapter 55
AAA Server.... 472

55.1 AAA Server Overview 472
55.2 Authentication Server Command Summary 472
55.2.1 ad-server Commands 472
55.2.2 ldap-server Commands 473
55.2.3 radius-server Commands 474
55.2.4 radius-server Command Example 474
55.2.5 aaa group server ad Commands 474
55.2.6 aaa group server ldap Commands 475
55.2.7 aaa group server radius Commands 477
55.2.8 aaa group server Command Example 478

Chapter 56
Authentication Objects 479

56.1 Authentication Objects Overview 479
56.2 aaa authentication Commands 479
56.2.1 aaa authentication Command Example 480
56.3 test aaa Command 480
56.3.1 Test a User Account Command Example 481
56.4 VPN/Admin Two-Factor Authentication 481
56.4.1 Two-Factor Authentication Methods 482
56.4.2 Two-Factor Authentication with SMS/Email 482
56.4.3 SMS/Email Configuration 483
56.4.4 Two-Factor Authentication with Google Authenticator 483
56.5 Two-Factor Authentication Commands 484
56.5.1 Two-Factor Authentication VPN Access 484
56.5.2 VPN Access Two-Factor Command Example 486
56.5.3 Admin Access 487
56.5.4 Admin Access Two-Factor Command Examples 488

Chapter 57
Authentication Server....490

57.1 Authentication Server Overview 490
57.2 Authentication Server Commands 490
57.2.1 Authentication Server Command Examples 491

Chapter 58
Certificates.... 492

58.1 Certificates Overview 492
58.2 Certificate Commands 492
58.3 Certificates Commands Input Values 492
58.4 Certificates Commands Summary 494
58.5 Certificates Commands Examples 497

Chapter 59
ISP Accounts 498

59.1 ISP Accounts Overview 498
59.1.1 PPPoE and PPTP Account Commands 498
59.1.2 Cellular Account Commands 499

Chapter 60
SSL Application 501

60.1 SSL Application Overview 501
60.1.1 SSL Application Object Commands 501
60.1.2 SSL Application Command Examples 503

Chapter 61
DHCPv6 Objects 504

61.1 DHCPv6 Object Commands Summary 504
61.1.1 DHCPv6 Object Commands 504
61.1.2 DHCPv6 Object Command Examples 505

Chapter 62
Dynamic Guest Accounts 507

62.1 Dynamic Guest Accounts Overview 507
62.2 Dynamic-guest Commands 507
62.2.1 dynamic-guest Sub-commands 508
62.2.2 Dynamic-guest Command Example 509

Chapter 63
System 510

63.1 System Overview 510
63.2 Customizing the WWW Login Page 510
63.3 Host Name Commands 512
63.4 Time and Date 512
63.4.1 Date/Time Commands 513
63.5 Console Port Speed 514
63.6 DNS Overview 514
63.6.1 Domain Zone Forwarder 514
63.6.2 DNS Commands 515
63.6.3 DNS Command Examples 517

63.7 Authentication Server Overview 517
63.7.1 Authentication Server Commands 518
63.7.2 Authentication Server Command Examples 519
63.8 Notification 519
63.8.1 Mail Server Commands 519
63.8.2 SMS Service Commands 520
63.8.3 Response Message Commands 522
63.9 Language Commands 523
63.10 IPv6 Commands 523
63.11 ZON Overview 523
63.11.1 LLDP 524
63.11.2 ZON Commands 524
63.11.3 ZON Examples 524
63.12 Fast Forwarding 525
63.12.1 Fast Forwarding Technical Overview 525
63.12.2 Fast Forwarding Commands 525

Chapter 64
System Remote Management 526

64.1 Remote Management Overview 526
64.1.1 Remote Management Limitations 526
64.1.2 System Timeout 526
64.2 Common System Command Input Values 527
64.3 HTTP/HTTPS Commands 527
64.3.1 HTTP/HTTPS Command Examples 529
64.4 SSH 530
64.4.1 SSH Implementation on the Zyxel Device 530
64.4.2 Requirements for Using SSH 530
64.4.3 Diffie-Hellman (DH) Key Exchange 530
64.4.4 SSH Commands 531
64.4.5 SSH Command Examples 532
64.5 Telnet 532
64.6 Telnet Commands 532
64.6.1 Telnet Commands Examples 533
64.7 Configuring FTP 533
64.7.1 FTP Commands 534
64.7.2 FTP Commands Examples 534
64.8 SNMP 535
64.8.1 Supported MIBs 535
64.8.2 SNMP Traps 535
64.8.3 SNMP Commands 536
64.8.4 SNMP Commands Examples 537
64.9 ICMP Filter 538

Chapter 65
File Manager 539

65.1 File Directories 539
65.2 Configuration Files and Shell Scripts Overview 539
65.2.1 Comments in Configuration Files or Shell Scripts 540
65.2.2 Errors in Configuration Files or Shell Scripts 541
65.2.3 Zyxel Device Configuration File Details 542
65.2.4 Configuration File Flow at Restart 542
65.2.5 Sensitive Data Protection 543
65.3 File Manager Commands Input Values 544
65.4 File Manager Commands Summary 545
65.5 File Manager Dual Firmware Commands 546
65.6 File Manager Command Examples 547
65.7 FTP File Transfer 548
65.7.1 Command Line FTP File Upload 548
65.7.2 Command Line FTP Configuration File Upload Example 548
65.7.3 Command Line FTP File Download 549
65.7.4 Command Line FTP Configuration File Download Example 549
65.8 Cloud Helper Commands 550
65.8.1 Cloud Helper Command Examples 553
65.9 Zyxel Device File Usage at Startup 554
65.10 Notification of a Damaged Recovery Image or Firmware 555
65.11 Restoring the Recovery Image 556
65.12 Restoring the Firmware 558
65.13 Restoring the Default System Database 560
65.13.1 Using the atkz -u Debug Command 562

Chapter 66
Logs 565

66.1 Log Commands Summary 565
66.1.1 Log Entries Commands 566
66.1.2 System Log Commands 566
66.1.3 Debug Log Commands 567
66.1.4 E-mail Profile Commands 569
66.1.5 Console Port Logging Commands 570

Chapter 67
Reports and Reboot 572

67.1 Report Commands Summary 572
67.1.1 Report Commands 572
67.1.2 Report Command Examples 573
67.1.3 Session Commands 573
67.1.4 Packet Size Statistics Commands 574

67.2 Email Daily Report Commands 574
67.2.1 Email Daily Report Example 575
67.3 Reboot 577

Chapter 68
Diagnostics and Remote Assistance 578

68.1 Diagnostics 578
68.2 Diagnosis Commands 578
68.3 Diagnosis Commands Example 579
68.4 Remote Assistance 579
68.5 Remote Assistance Commands 580

Chapter 69
Session Timeout 581

Chapter 70
Packet Flow Explore 582

70.1 Packet Flow Explore 582
70.2 Packet Flow Explore Commands 582
70.3 Packet Flow Explore Commands Example 583

Chapter 71
Maintenance Tools 586

71.1 Maintenance Command Examples 589
71.1.1 Packet Capture Command Example 591
71.2 Scheduled Reboot 593
71.2.1 High Availability Reboot Process 594
71.3 Configuration File Backup 595

Chapter 72
Miscellaneous 597

72.1 SDWan OnCloud 597
72.2 Watchdog Timer 597
72.2.1 Hardware Watchdog Timer 597
72.2.2 Software Watchdog Timer 597
72.2.3 Application Watchdog 598
72.3 Conserve Memory 601
72.3.1 Converse Memory Settings 601
72.3.2 Conserve Memory Commands 601
72.3.3 Conserve Memory Example 602
72.4 GUI Visibility 603
72.5 Google Analytics 603

Chapter 73
Managed AP Commands 604

73.1 Managed Series AP Commands Overview 604
73.2 Accessing the AP CLI 604
73.3 CAPWAP Client Commands 604
73.3.1 CAPWAP Client Commands Example 605
73.4 DNS Server Commands 606
73.4.1 DNS Server Commands Example 607
73.4.2 DNS Server Commands and DHCP 607

List of Commands (Alphabetical) 608

PART I
Introduction

CHAPTER 1
Command Line Interface

1.1 Overview

Zyxel Device refers to these models as outlined below:

The latest firmware for these Zyxel Devices, at the time of writing, is ZLD version 4.60.

- ZyWALL
  - ZyWALL 110
  - ZyWALL 310
  - ZyWALL 1100
- ZyWALL USG (Unified Security Gateway)
  - USG40
  - USG40W
  - USG60
  - USG60W
  - USG110
  - USG210
  - USG310
  - USG1100
  - USG1900
  - USG2200
  - USG2200-VPN

The latest firmware for these Zyxel Devices, at the time of writing, is ZLD version 5.31.

- ZyWALL NS (National Security)
  - NS5000
  - NS7000

The latest firmware for these Zyxel Devices, at the time of writing, is ZLD version 5.37.

- ZyWALL VPN
  - VPN50
  - VPN100
  - VPN300
  - VPN1000

The latest firmware for these Zyxel Devices, at the time of writing, is ZLD version 5.42.

- ZyWALL USG (Unified Security Gateway)
  - USG FLEX 50 (USG20-VPN)

  - USG FLEX 50AX
  - USG20W-VPN

- ZyWALL USG FLEX

  - USG FLEX 100
  - USG FLEX 100AX
  - USG FLEX 100W
  - USG FLEX 200
  - USG FLEX 500
  - USG FLEX 700

- ZyWALL ATP (Advanced Threat Protection)

  - ATP100
  - ATP100W
  - ATP200
  - ATP500
  - ATP700
  - ATP800

If you have problems with your Zyxel Device, customer support may request that you issue some of these commands to assist them in troubleshooting.

> Use of undocumented commands or misconfiguration can damage the Zyxel Device and possibly render it unusable.

1.1.1 The Configuration File

When you configure the Zyxel Device using either the CLI (Command Line Interface) or the web configurator, the settings are saved as a series of commands in a configuration file on the Zyxel Device. You can store more than one configuration file on the Zyxel Device. However, only one configuration file is used at a time.

You can perform the following with a configuration file:

- Back up Zyxel Device configuration once the Zyxel Device is set up to work in your network.
- Restore Zyxel Device configuration.
- Save and edit a configuration file and upload it to multiple Zyxel Devices (of the same model) in your network to have the same settings.

Note: You may also edit a configuration file using a text editor.

1.2 Accessing the CLI

You can access the CLI using a terminal emulation program on a computer connected to the console port, from the web configurator or access the Zyxel Device using Telnet or SSH (Secure SHell).

Note: The Zyxel Device might force you to log out of your session if re-authentication time, lease time, or idle timeout is reached. See Chapter 49 on page 438 for more information about these settings.

1.2.1 Console Port

The default settings for the console port are as follows.

Table 1 Managing the Zyxel Device: Console Port

SETTING	VALUE
Speed	115200 bps
Data Bits	8
Parity	None
Stop Bit	1
Flow Control	Off

When you turn on your Zyxel Device, it performs several internal tests as well as line initialization. You can view the initialization information using the console port.

- Garbled text displays if your terminal emulation program's speed is set lower than the Zyxel Device's.
- No text displays if the speed is set higher than the Zyxel Device's.
- If changing your terminal emulation program's speed does not get anything to display, restart the Zyxel Device.
- If restarting the Zyxel Device does not get anything to display, contact your local customer support.

Figure 1 Console Port Power-on Display

```
U-Boot 2013.07 (Development build, svnversion: u-boot:518M, exec:)-svn517
(Build time: Feb 16 2017 - 10:06:38)

BootModule Version: V1.13 | Feb 16 2017 10:06:38
DRAM: Size = 2048 Mbytes

Press any key to enter debug mode within 3 seconds.
```

After the initialization, the login screen displays.

Figure 2 Login Screen

```
Welcome to ATP100W

Username:
```

Enter the user name and password at the prompts.

Note: The default login username is admin and password is 1234. The username and password are case-sensitive.

1.2.2 Web Configurator Console

Note: Before you can access the CLI through the web configurator, make sure your computer supports the Java Runtime Environment. You will be prompted to download and install the Java plug-in if it is not already installed.

When you access the CLI using the web console, your computer establishes a SSH (Secure SHell) connection to the Zyxel Device. Follow the steps below to access the web console.

1 Log into the web configurator.

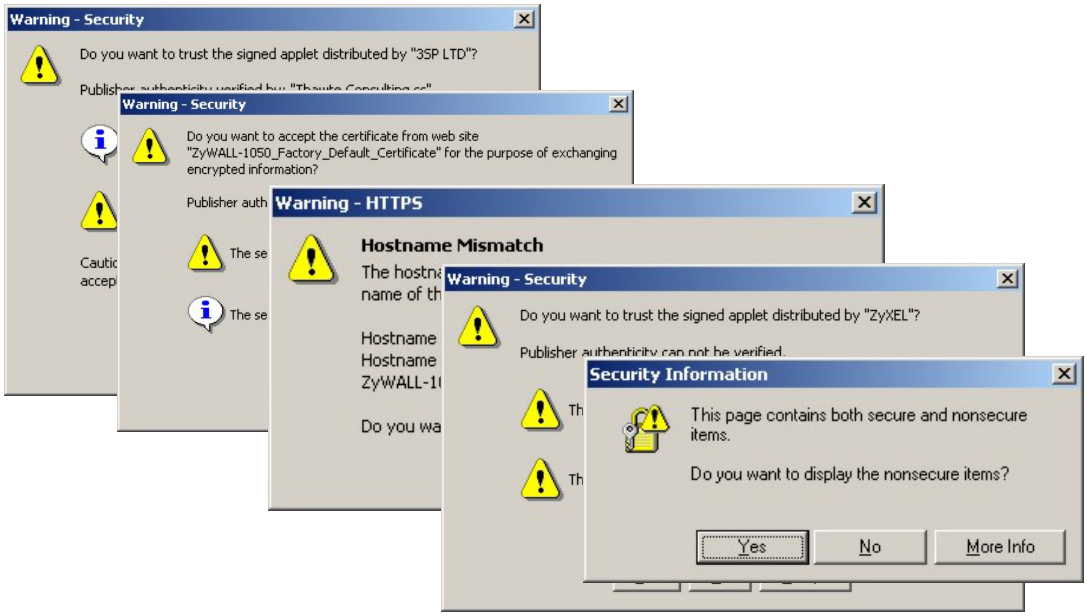
2 Click the Console icon in the top-right corner of the web configurator screen.

3 If the Java plug-in is already installed, skip to step 4.

Otherwise, you will be prompted to install the Java plug-in. If the prompt does not display and the screen remains gray, you have to download the setup program.

4 The web console starts. This might take a few seconds. One or more security screens may display. Click Yes or Always.

Figure 3 Web Console: Security Warnings



Finally, the User Name screen appears.

Figure 4 Web Console: User Name

5 Enter the user name you want to use to log in to the console. The console begins to connect to the Zyxel Device.

Note: The default login username is admin. It is case-sensitive.

Then, the Password screen appears.

Figure 5 Web Console: Password

6 Enter the password for the user name you specified earlier. If you enter the password incorrectly, you get an error message.

Figure 6 Login Error Message

7 To use most commands in this User's Guide, enter `configure terminal`. The prompt should change to `Router(config)#`.

1.2.3 Telnet

Use the following steps to Telnet into your Zyxel Device.

1 Using the Web Configurator, enable and configure Telnet at System > TELNET.

2 Ensure that the Telnet protocol is allowed from your computer's zone to the Zyxel Device. By default, add TELNET to the default service group at Object > Service > Service Group > Default_Allow_WAN_To_ZyWALL.

3 In Windows, click Start (usually in the bottom left corner) and Run. Then type `telnet` and the Zyxel Device's IP address. For example, enter `telnet 192.168.1.1` (the default management IP address).

4 Click OK. A login screen displays. Enter the user name and password at the prompts.

Note: The default login username is admin and password is 1234. The username and password are case-sensitive.

1.2.4 SSH (Secure SHell)

You can use an SSH client program to access the CLI. The following figure shows an example using a text-based SSH client program. Refer to the documentation that comes with your SSH program for information on using it.

Before connecting, do the following:

- Using the Web Configurator, enable SSH at System > SSH.
- Ensure that the SSH protocol is allowed from your computer's zone to the Zyxel Device. By default, add SSH to the service group Default_Allow_WAN_To_ZyWALL at Object > Service > Service Group. This group defines which services are allowed in the default WAN_to_Device security policy.

Note: The default login username is admin and password is 1234. The username and password are case-sensitive.

Figure 7 SSH Login Example

```
C:\>ssh2 admin@192.168.1.1
Host key not found from database.
Key fingerprint:
xolor-takel-fipef-zevit-visom-gydog-vetan-bisol-lysob-cuvun-muxex
You can get a public key's fingerprint by running
% ssh-keygen -F publickey.pub
on the keyfile.
Are you sure you want to continue connecting (yes/no)? yes

Host key saved to C:/Documents and Settings/user/Application Data/SSH/
hostkeys/
ey_22_192.168.1.1.pub
host key for 192.168.1.1, accepted by user Tue Jul 11 2023 09:48:17
admin's password:
Authentication successful.
```

1.3 How to Find Commands in this Guide

You can simply look for the feature chapter to find commands. In addition, you can use the List of Commands (Alphabetical) at the end of the guide. This section lists the commands in alphabetical order that they appear in this guide.

If you are looking at the CLI Reference Guide electronically, you might have additional options (for example, bookmarks or Find...) as well.

1.4 How Commands Are Explained

Each chapter explains the commands for one keyword. The chapters are divided into the following sections.

1.4.1 Background Information (Optional)

Note: See the User's Guide for background information about most features.

This section provides background information about features that you cannot configure in the web configurator. In addition, this section identifies related commands in other chapters.

1.4.2 Command Input Values (Optional)

This section lists common input values for the commands for the feature in one or more tables

1.4.3 Command Summary

This section lists the commands for the feature in one or more tables.

1.4.4 Command Examples (Optional)

This section contains any examples for the commands in this feature.

1.4.5 Command Syntax

The following conventions are used in this User's Guide.

- A command or keyword in `courier new` must be entered literally as shown. Do not abbreviate.
- Values that you need to provide are in *`italics`*.
- Required fields that have multiple choices are enclosed in curly brackets `{}`.
- A range of numbers is enclosed in angle brackets <>.
- Optional fields are enclosed in square brackets `[]`.
- The | symbol means OR.

For example, look at the following command to create a TCP/UDP service object.

`service-object` *`object-name`* `{tcp | udp} {eq <1..65535> | range <1..65535> <1..65535>}`

1. Enter `service-object` exactly as it appears.
2. Enter the name of the object where you see *`object-name.`*
3. Enter `tcp` or `udp`, depending on the service object you want to create.
4. Finally, do one of the following.
   - Enter `eq` exactly as it appears, followed by a number between 1 and 65535.
   - Enter `range` exactly as it appears, followed by two numbers between 1 and 65535.

1.4.6 Naming Conventions

The ATP and USG devices may have different names for the same service, but the commands for both devices are the same. The command names will be used to refer to these services throughout this reference guide. A list of naming differences are in the next table.

Table 2 Naming differences between USG and ATP devices

COMMAND NAME	USG SERIES NAME	USG FLEX SERIES NAME	ATP SERIES NAME
anti-virus	Anti-Virus	Anti-Malware	Anti-Malware

Table 2 Naming differences between USG and ATP devices (continued)

COMMAND NAME	USG SERIES NAME	USG FLEX SERIES NAME	ATP SERIES NAME
anti-spam	Anti-Spam	Email Security	Email Security
threat-website	N/A	URL Threat Filter	URL Threat Filter

1.4.7 Changing the Password

It is highly recommended that you change the password for accessing the Zyxel Device. See Section 50.2 on page 444 for the appropriate commands.

1.4.8 Idle Timeout

See Section 50.2.1 on page 444 for commands on changing the default logout time when no activity is recorded.

1.5 CLI Modes

You run CLI commands in one of several modes.

After you log into the Zyxel Device, you will see this prompt `Router>` in User mode.

Type `enable` and you will see this prompt `Router#` in Privilege mode.

Type `configure terminal` and you will see this prompt `Router(config)#` in Configuration mode.

This is a summary of the modes.

Table 3 CLI Modes

	USER	PRIVILEGE	CONFIGURATION	SUB-COMMAND
What Guest users can do	Unable to access	Unable to access	Unable to access	Unable to access
What User users can do	• Look at (but not run) available commands	Unable to access	Unable to access	Unable to access
What Limited-Admin users can do	• Look at system information (like Status screen) • Run basic diagnostics	• Look at system information (like Status screen) • Run basic diagnostics	Unable to access	Unable to access
What Admin users can do	• Look at system information (like Status screen) • Run basic diagnostics	• Look at system information (like Status screen) • Run basic diagnostics	• Configure simple features (such as an address object) • Create or remove complex parts (such as an interface)	• Configure complex parts (such as an interface) in the Zyxel Device
How you enter it	Log in to the Zyxel Device	Type enable in User mode	Type configure terminal in User or Privilege mode	Type the command used to create the specific part in Configuration mode

Table 3 CLI Modes (continued)

	USER	PRIVILEGE	CONFIGURATION	SUB-COMMAND

What the prompt looks like	`Router>`	`Router#`	`Router(config)#`	(varies by part)
				`Router(zone)#`
				`Router(config-if-ge)#`
				`...`

How you exit it	Type exit	Type disable	Type exit	Type exit

See Chapter 49 on page 438 for more information about the user types. User users can only log in, look at (but not run) the available commands in User mode, and log out. Limited-Admin users can look at the configuration in the web configurator and CLI, and they can run basic diagnostics in the CLI. Admin users can configure the Zyxel Device in the web configurator or CLI.

At the time of writing, there is not much difference between User and Privilege mode for admin users. This is reserved for future use.

1.6 Shortcuts and Help

1.6.1 List of Available Commands

A list of valid commands can be found by typing ? or [TAB] at the command prompt. To view a list of available commands within a command group, enter `<command> ?` or `<command>` [TAB].

Figure 8 Help: Available Commands Example 1

```
Router> ?
<cr>
apply
atse
clear
configure
------------------[Snip]--------------------
shutdown
telnet
test
traceroute
write
Router>
```

Figure 9 Help: Available Command Example 2

```
Router> show ?
<wlan ap interface>
aaa
access-page
account
ad-server
address-object
------------------[Snip]--------------------
wlan
workspace
zone
Router> show
```

1.6.2 List of Sub-commands or Required User Input

To view detailed help information for a command, enter <command> <sub command> ?.

Figure 10 Help: Sub-command Information Example

```
Router(config)# ip telnet server ?
;
<cr>
port
rule
|
Router(config)# ip telnet server
```

Figure 11 Help: Required User Input Example

```
Router(config)# ip telnet server port ?
<1..65535>
Router(config)# ip telnet server port
```

1.6.3 Entering Partial Commands

The CLI does not accept partial or incomplete commands. You may enter a unique part of a command and press [TAB] to have the Zyxel Device automatically display the full command.

For example, if you enter **config** and press [TAB] , the full command of **configure** automatically displays.

If you enter a partial command that is not unique and press [TAB], the Zyxel Device displays a list of commands that start with the partial command.

Figure 12 Non-Unique Partial Command Example

```
Router# c [TAB]
clear      configure  copy
Router# co [TAB]
configure  copy
```

1.6.4 Entering a ? in a Command

Typing a ? (question mark) usually displays help information. However, some commands allow you to input a ?, for example as part of a string. Press [CTRL+V] on your keyboard to enter a ? without the Zyxel Device treating it as a help query.

1.6.5 Command History

The Zyxel Device keeps a list of commands you have entered for the current CLI session. You can use any commands in the history again by pressing the up (↑) or down (↓) arrow key to scroll through the previously used commands and press [ENTER].

1.6.6 Navigation

Press [CTRL]+A to move the cursor to the beginning of the line. Press [CTRL]+E to move the cursor to the end of the line.

1.6.7 Erase Current Command

Press [CTRL]+U to erase whatever you have currently typed at the prompt (before pressing [ENTER]).

1.6.8 The no Commands

When entering the no commands described in this document, you may not need to type the whole command. For example, with the "`[no] mss <536..1452>`" command, you use "`mss 536`" to specify the MSS value. But to disable the MSS setting, you only need to type "`no mss`" instead of "no mss 536".

1.7 Input Values

You can use the ? or [TAB] to get more information about the next input value that is required for a command. In some cases, the next input value is a string whose length and allowable characters may not be displayed in the screen. For example, in the following example, the next input value is a string called `<description>`.

```
Router# configure terminal
Router(config)# interface ge1
Router(config-if-ge)# description
<description>
```

When you use the example above, note that Zyxel Device USG 200 and below models use a name such as wan1, wan2, opt, lan1, ext-wlan, or dmz.

The following table provides more information about input values like <description>.

Table 4 Input-Value Formats for Strings in CLI Commands

TAG	# VALUES	LEGAL VALUES
*	1	*
all	--	ALL
authentication key	Used in IPSec SA	
	32-40 16-20	“0x” or “0X” + 32-40 hexadecimal values alphanumeric or ;|`~!@#$%^&*()_+\\{}':,./<>=-
	Used in MD5 authentication keys for RIP/OSPF and text authentication key for RIP	
	0-16	alphanumeric or _-
	Used in text authentication keys for OSPF	
	0-8	alphanumeric or _-
certificate name	1-31	alphanumeric or ;`~!@#$%^&()_+[\]{}',.=-
community string	0-63	alphanumeric or .- first character: alphanumeric or -
connection_id	1+	alphanumeric or -_:
contact	1-61	alphanumeric, spaces, or '()+,/:=?;!*#@$_%-.
country code	0 or 2	alphanumeric
custom signature file name	0-30	alphanumeric or _-. first character: letter
description	Used in keyword criteria for log entries	
	1-64	alphanumeric, spaces, or '()+,/:=?;!*#@$_%-.
	Used in other commands	
	1-61	alphanumeric, spaces, or '()+,/:=?;!*#@$_%-
distinguished name	1-511	alphanumeric, spaces, or .@=,_-
domain name	Used in content filtering	
	0+	lower-case letters, numbers, or .-
	Used in ip dns server	
	0-247	alphanumeric or .- first character: alphanumeric or -
	Used in domainname, ip dhcp , and ip domain	
	0-254	alphanumeric or ._- first character: alphanumeric or -
email	1-63	alphanumeric or .@_-
e-mail	1-64	alphanumeric or .@_-
encryption key	16-64 8-32	“0x” or “0X” + 16-64 hexadecimal values alphanumeric or ;|`~!@#$%^&*()_+\\{}':,./<>=-
file name	0-31	alphanumeric or _-
filter extension	1-256	alphanumeric, spaces, or '()+,/:=?;!*#@$_%.-

Table 4 Input-Value Formats for Strings in CLI Commands (continued)

TAG	# VALUES	LEGAL VALUES
fqdn	Used in ip dns server	
	0-252	alphanumeric or .- first character: alphanumeric or -
	Used in ip ddns, time server, device HA, VPN, certificates, and interface ping check	
	0-254	alphanumeric or .- first character: alphanumeric or -
full file name	0-256	alphanumeric or _/.-
hostname	Used in hostname command	
	0-63	alphanumeric or .-_ first character: alphanumeric or -
	Used in other commands	
	0-252	alphanumeric or .- first character: alphanumeric or -
import configuration file	1-26+".conf"	alphanumeric or ;`~!@#$%^&()_+[]{}',.=- add ".conf" at the end
import shell script	1-26+".zysh"	alphanumeric or ;`~!@#$%^&()_+[]{}',.=- add ".zysh" at the end
initial string	1-64	alphanumeric, spaces, or '()+,/:=!*#@$_%-.&
isp account password	0-63	alphanumeric or `~!@#$%^&*()_\-+={}|\;:'<,>./
isp account username	0-30	alphanumeric or -_@$./
ipv6_addr		An IPv6 address. The 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address 2001:0db8:1a2b:0015:0000:0000:1a2f:0000. IPv6 addresses can be abbreviated in two ways: Leading zeros in a block can be omitted. So 2001:0db8:1a2b:0015:0000:0000:1a2f:0000 can be written as 2001:db8:1a2b:15:0:0:1a2f:0. Any number of consecutive blocks of zeros can be replaced by a double colon. A double colon can only appear once in an IPv6 address. So 2001:0db8:0000:0000:1a2f:0000:0000:0015 can be written as 2001:0db8::1a2f:0000:0000:0015, 2001:0db8:0000:0000:1a2f::0015, 2001:db8::1a2f:0:0:15 or 2001:db8:0:0:1a2f::15.
key length	--	512, 768, 1024, 1536, 2048, 4096
license key	25	"S-" + 6 upper-case letters or numbers + "-" + 16 upper-case letters or numbers
mac address	--	aa:bb:cc:dd:ee:ff (hexadecimal)
mail server fqdn		lower-case letters, numbers, or -.
name	1-31	alphanumeric or _-
notification message	1-81	alphanumeric, spaces, or '()+,/:=?;!*#@$_%-
password: less than 15 chars	1-15	alphanumeric or `~!@#$%^&*()_\-+={}|\;:'<,>./

Table 4 Input-Value Formats for Strings in CLI Commands (continued)

TAG	# VALUES	LEGAL VALUES
password: less than 8 chars	1-8	alphanumeric or ;/?:@&=+$\.-_!~*'()%,#$
password	Used in user and ip ddns	
	1-63	alphanumeric or `~!@#$%^&*()_-+={}|\;:'<,>./
	Used in e-mail log profile SMTP authentication	
	1-63	alphanumeric or `~!@#$%^&*()_-+={}|\;:'<>./
	Used in device HA synchronization	
	1-63	alphanumeric or ~#%^*_-={}:,.
	Used in registration	
	6-20	alphanumeric or .@_-
phone number	1-20	numbers or ,+
preshared key	16-64	“0x” or “0X” + 16-64 hexadecimal values alphanumeric or ;|`~!@#$%^&*()_+\{}':,./<>=-
profile name	0-30	alphanumeric or _- first character: letters or _-
proto name	1-16	lower-case letters, numbers, or -
protocol name	0-30	alphanumeric or _- first character: letters or _-
quoted string less than 127 chars	1-255	alphanumeric, spaces, or ;/?:@&=+$\.- _!~*'()%,
quoted string less than 63 chars	1-63	alphanumeric, spaces, or ;/?:@&=+$\.-_!~*'()%
quoted string	0+	alphanumeric, spaces, or punctuation marks enclosed in double quotation marks (“) must put a backslash (\) before double quotation marks that are part of input value itself
service name	0-63	alphanumeric or -_@$./
spi	2-8	hexadecimal
string less than 15 chars	1-15	alphanumeric or -_
string: less than 63 chars	1-63	alphanumeric or `~!@#$%^&*()_-+={}|\;:'<,>./
string	1+	alphanumeric or -_@
subject	1-61	alphanumeric, spaces, or '()+,./:=?;!*#@$_%-
system type	0-2	hexadecimal
timezone [-+]*hh*	--	-12 through +12 (with or without “+”)
url	1-511	alphanumeric or '()+,/:.=?;!*#@$_%-

Table 4 Input-Value Formats for Strings in CLI Commands (continued)

TAG	# VALUES	LEGAL VALUES
url	Used in content filtering redirect	
	“http://”+ “https://”+	alphanumeric or ;/?:@&=+$\.-_!~*'()%, starts with “http://” or “https://” may contain one pound sign (#)
	Used in other content filtering commands	
	“http://”+	alphanumeric or ;/?:@&=+$\.-_!~*'()%, starts with “http://” may contain one pound sign (#)
user name	Used in VPN extended authentication	
	1-31	alphanumeric or _-
	Used in other commands	
	0-30	alphanumeric or _- first character: letters or _-
username	6-20	alphanumeric or .@_- registration
user name	1+	alphanumeric or -_. logging commands
user@domainname	1-80	alphanumeric or .@_-
vrrp group name: less than 15 chars	1-15	alphanumeric or _-
week-day sequence, i.e. 1=first,2=second	1	1-4
xauth method	1-31	alphanumeric or _-
xauth password	1-31	alphanumeric or ;|`~!@#$%^&*()_+\{}':,./<>=-
mac address	0-12 (even number)	hexadecimal for example: aa aabbcc aabbccddeeff

1.8 Ethernet Interfaces

How you specify an Ethernet interface depends on the Zyxel Device model.

- For some Zyxel Device models, use ge*x*, *x* = 1~N, where N equals the highest numbered Ethernet interface for your Zyxel Device model.
- For other Zyxel Device models use a name such as wan1, wan2, opt, lan1, or dmz.

1.9 Saving Configuration Changes

Use the `write` command to save the current configuration to the Zyxel Device.

Note: Always save the changes before you log out after each management session. All unsaved changes will be lost after the system restarts.

1.10 Logging Out

Enter the `exit` or `end` command in configure mode to go to privilege mode.

Enter the `exit` command in user mode or privilege mode to log out of the CLI.

1.11 Resetting the Zyxel Device

If you cannot access the Zyxel Device by any method, try restarting it by turning the power off and then on again. If you still cannot access the Zyxel Device by any method or you forget the administrator password(s), you can reset the Zyxel Device to its factory-default settings. Any configuration files or shell scripts that you saved on the Zyxel Device should still be available afterwards.

Use the following command to reset the Zyxel Device to its factory-default settings. This overwrites the settings in the startup-config.conf file with the settings in the system-default.conf file.

Note: This procedure removes the current configuration. Note that there is a space after apply in the command.

Figure 13 Resetting the Zyxel Device

```
Router> apply /conf/system-default.conf
```

CHAPTER 2
User and Privilege Modes

2.1 User And Privilege Modes

This is the mode you are in when you first log into the CLI. (Do not confuse 'user mode' with types of user accounts the Zyxel Device uses. See Chapter 49 on page 438 for more information about the user types. 'User' type accounts can only run 'exit' in this mode. However, they may need to log into the device in order to be authenticated for 'user-aware' policies, for example a firewall rule that a particular user is exempt from or a VPN tunnel that only certain people may use.)

Type 'enable' to go to 'privilege mode'. No password is required. All commands can be run from here except those marked with an asterisk. Many of these commands are for trouble-shooting purposes, for example debug commands. Customer support may ask you to run some of these commands and send the results if you need assistance troubleshooting your device.

For admin logins, all commands are visible in 'user mode' but not all can be run there. The following table displays which commands can be run in 'user mode'. All commands can be run in 'privilege mode'.

Type *ezmode activate* if you have a simple network environment with one ISP for Internet access for example. You'll enter Easy Mode every time you log in to the Zyxel Device using the Web Configurator. Objects created in Easy Mode begin with EZ_

Type *ezmode deactivate* if you have a complex network environment with two ISPs for Internet access for example. You'll enter Expert Mode every time you log in to the Zyxel Device using the Web Configurator. Some EZ_ objects cannot be edited in Expert Mode.

The **psm** commands are for Zyxel's internal manufacturing process.

Table 5 User (U) and Privilege (P) Mode Commands

COMMAND	MODE	DESCRIPTION
apply	P	Applies a configuration file.
atse	U/P	Displays the seed code
clear	U/P	Clears system or debug logs or DHCP binding.
configure	U/P	Use 'configure terminal' to enter configuration mode.
copy	P	Copies configuration files.
debug (*)	U/P	For support personnel only! The device needs to have the debug flag enabled.
delete	P	Deletes configuration files.
details	P	Performs diagnostic commands.
diag	P	Provided for support personnel to collect internal system information. It is not recommended that you use these.
diag-info	P	Has the Zyxel Device create a new diagnostic file.
dir	P	Lists files in a directory.

Table 5 User (U) and Privilege (P) Mode Commands (continued)

COMMAND	MODE	DESCRIPTION
`disable`	U/P	Goes from privilege mode to user mode
`enable`	U/P	Goes from user mode to privilege mode
`exit`	U/P	Goes to a previous mode or logs out.
`interface`	U/P	Dials or disconnects an interface.
`no packet-trace`	U/P	Turns off packet tracing.
`nslookup`	U/P	Resolves an IP address to a host name and vice-versa.
`packet-trace`	U/P	Performs a packet trace.
`ping`	U/P	Pings an IP address or host name.
`ping6`	U/P	Pings an IPv6 address or a host name.
`psm`	U/P	Goes to psm (product support module) mode for setting product parameters. Only use psm commands if your customer support Engineer asks you to during troubleshooting. Note: These commands are for Zyxel's internal manufacturing process.
`reboot`	P	Restarts the device.
`release`	P	Releases DHCP information from an interface.
`rename`	P	Renames a configuration file.
`renew`	P	Renews DHCP information for an interface.
`run`	P	Runs a script.
`setenv`	U/P	Turns stop-on-error on (terminates booting if an error is found in a configuration file) or off (ignores configuration file errors and continues booting).
`show`	U/P	Displays command statistics. See the associated command chapter in this guide.
`shutdown`	P	Writes all d data to disk and stops the system processes. It does not turn off the power.
`telnet`	U/P	Establishes a connection to the TCP port number 23 of the specified host name or IP address.
`test aaa`	U/P	Tests whether the specified user name can be successfully authenticated by an external authentication server.
`traceroute`	P	Traces the route to the specified host name or IP address.
`traceroute6`	P	Traces the route to the specified host name or IPv6 address.
`write`	P	Saves the current configuration to the Zyxel Device. All unsaved changes are lost after the Zyxel Device restarts.

Subsequent chapters in this guide describe the configuration commands. User/privilege mode commands that are also configuration commands (for example, 'show') are described in more detail in the related configuration command chapter.

Part II
Reference

CHAPTER 3
Object Reference

3.1 Object Reference Commands

The object reference commands are used to see which configuration settings reference a specific object. You can use this table when you want to delete an object because you have to remove references to the object first.

Table 6 `show reference` Commands

COMMAND	DESCRIPTION
`show reference object username [username]`	Displays which configuration settings reference the specified user object.
`show reference object address [object_name]`	Displays which configuration settings reference the specified address object.
`show reference object address6 [object_name]`	Displays which configuration settings reference the specified IPv6 address object.
`show reference object service [object_name]`	Displays which configuration settings reference the specified service object.
`show reference object schedule [object_name]`	Displays which configuration settings reference the specified schedule object.
`show reference object interface [interface_name | virtual_interface_name]`	Displays which configuration settings reference the specified interface or virtual interface object.
`show reference object aaa authentication [default | auth_method]`	Displays which configuration settings reference the specified AAA authentication object.
`show reference object ca category {local|remote} [cert_name]`	Displays which configuration settings reference the specified authentication method object.
`show reference object account pppoe [object_name]`	Displays which configuration settings reference the specified PPPoE account object.
`show reference object account pptp [object_name]`	Displays which configuration settings reference the specified PPTP account object.
`show reference object app-patrol [profile-name]`	Displays which configuration settings reference the specified application patrol profile.
`show reference object sslvpn application [object_name]`	Displays which configuration settings reference the specified SSL VPN application object.
`show reference object crypto map [crypto_name]`	Displays which configuration settings reference the specified VPN connection object.
`show reference object isakmp policy [isakmp_name]`	Displays which configuration settings reference the specified VPN gateway object.
`show reference object sslvpn policy [object_name]`	Displays which configuration settings reference the specified SSL VPN object.

Table 6 show reference Commands (continued)

COMMAND	DESCRIPTION
show reference object zone [*object_name*]	Displays which configuration settings reference the specified zone object.
show reference object dhcp6-lease-object [*object_name*]	Displays which configuration settings reference the specified DHCPv6 lease object.
show reference object dhcp6-request-object [*object_name*]	Displays which configuration settings reference the specified DHCPv6 request object.
show reference object-group username [*username*]	Displays which configuration settings reference the specified user group object.
show reference object-group address [*object_name*]	Displays which configuration settings reference the specified address group object.
show reference object-group address6 [*object_name*]	Displays which configuration settings reference the specified IPv6 address group object.
show reference object-group service [*object_name*]	Displays which configuration settings reference the specified service group object.
show reference object-group interface [*object_name*]	Displays which configuration settings reference the specified trunk object.
show reference object-group aaa ad [*group_name*]	Displays which configuration settings reference the specified AAA AD group object.
show reference object-group aaa ldap [*group_name*]	Displays which configuration settings reference the specified AAA LDAP group object.
show reference object-group aaa radius [*group_name*]	Displays which configuration settings reference the specified AAA RADIUS group object.

3.1.1 Object Reference Command Example

This example shows how to check which configuration is using an address object named LAN1_SUBNET. For the command output, firewall rule 3 named LAN1-to-USG-2000 is using the address object.

```
Router(config)# show reference object address LAN1_SUBNET

LAN1_SUBNET References:
Category
Rule Priority        Rule Name
Description
================================================================================
Security Policy Control
3                    N/A
LAN1-to-USG-2000
Router(config)#
```

CHAPTER 4
Status

This chapter explains some commands you can use to display information about the Zyxel Device's current operational state.

Table 7 Status Show Commands

COMMAND	DESCRIPTION
`show boot status`	Displays details about the Zyxel Device's startup state.
`show comport status`	Displays whether the console is on or off.
`show cpu status`	Displays the CPU utilization.
`show cpu all`	Displays the CPU utilization of each CPU.
`show disk`	Displays the disk utilization.
`show extension-slot`	Displays the status of the extension card slot and USB ports and the names of devices connected to them.
`show led status`	Displays the status of each LED on the Zyxel Device.
`show mac`	Displays the Zyxel Device's MAC address.
`show mem status`	Displays what percentage of the Zyxel Device's memory is currently being used.
`show ram-size`	Displays the size of the Zyxel Device's on-board RAM.
`show serial-number`	Displays the serial number of this Zyxel Device.
`show socket listen`	Displays the Zyxel Device's listening ports
`show socket open`	Displays the ports that are open on the Zyxel Device.
`show system uptime`	Displays how long the Zyxel Device has been running since it last restarted or was turned on.
`show version`	Displays the Zyxel Device's model, firmware and build information.
`show ap-info total {sta | usage} {24G | 5G | 6G| all}` *`timer`*	Displays how many wireless stations are connected to all managed APs or the amount of data (in bytes) sent/received by the connected stations. *`timer`*: a period of time (from 1 to 24 hours) over which the station number is recorded or the traffic flow occurred.
`show ap-info top` *`number`* `{sta | usage}` *`timer`*	Displays how many wireless stations are connected to the top managed AP(s) or the amount of data (in bytes) sent/received by the connected stations. *`number`*: 1 to 64, the top "N" number of managed APs. *`timer`*: a period of time (from 1 to 24 hours) over which the station number is recorded or the traffic flow occurred.
`show ap-info {`*`mac_address`* `| all} {sta | usage} {24G | 5G | 6G| all}` *`timer`*	Displays how many wireless stations are connected to a specific or all managed APs or the amount of data (in bytes) sent/received by the connected stations. *`mac_address`*: the managed AP's MAC address. *`timer`*: a period of time (from 1 to 24 hours) over which the station number is recorded or the traffic flow occurred.

Table 7 Status Show Commands

COMMAND	DESCRIPTION
`show sta-info {mac_address | all} usage timer`	Displays data usage of a specific or all connected wireless stations. *mac_address*: the wireless station's MAC address. *timer*: a period of time (from 1 to 24 hours) over which the traffic flow occurred.
`show sta-info total usage timer`	Displays data usage of all connected wireless station(s). *timer*: a period of time (from 1 to 24 hours) over which the traffic flow occurred.
`show sta-info top number usage timer`	Displays data usage of the top connected wireless station(s). *number*: 1 to 64, the top "N" number of connected wireless stations. *timer*: a period of time (from 1 to 24 hours) over which the traffic flow occurred.

Here are examples of the commands that display the CPU and disk utilization.

Use `show cpu all` to check all the Zyxel Device CPU utilization. Use `show cpu status` to check the Zyxel Device average CPU utilization. You can use these commands to check your cpu status if you feel the Zyxel Device's performance is becoming slower

Use `show disk` to check the percentage of Zyxel Device onboard flash memory that is currently being used. You can use this command to check your disk status if you're having trouble saving files on the Zyxel Device, such as the firmware or the packet capture files.

```
Router(config)# show cpu status
Router> show cpu status
CPU utilization: 11 %
CPU utilization for 1 min: 2 %
CPU utilization for 5 min: 2 %
Router> show cpu all
CPU core 0 utilization: 3 %
CPU core 0 utilization for 1 min: 4 %
CPU core 0 utilization for 5 min: 2 %
CPU core 1 utilization: 0 %
CPU core 1 utilization for 1 min: 2 %
CPU core 1 utilization for 5 min: 4 %
Router> show disk
No. Disk                Size(MB)        Usage
================================================================================
====
1   image               116             93%
2   onboard flash       1007            12%
```

Here are examples of the commands that display the MAC address, memory usage, RAM size, and serial number. You need the MAC address and serial number if you want to pass the Zyxel Device management to Nebula.

```
Router(config)# show mac
MAC address: 28:61:32:89:37:61-28:61:32:89:37:67
Router(config)# show mem status
memory usage: 39%
Router(config)# show ram-size
ram size: 510MB
Router(config)# show serial-number
serial number: XXXXXXXXXXXX
```

Here is an example of the command that displays the listening ports.

```
Router(config)# show socket listen
No.   Proto Local_Address         Foreign_Address       State
================================================================================
1     tcp   0.0.0.0:2601          0.0.0.0:0             LISTEN
2     tcp   0.0.0.0:2602          0.0.0.0:0             LISTEN
3     tcp   127.0.0.1:10443       0.0.0.0:0             LISTEN
4     tcp   0.0.0.0:2604          0.0.0.0:0             LISTEN
5     tcp   0.0.0.0:80            0.0.0.0:0             LISTEN
6     tcp   127.0.0.1:8085        0.0.0.0:0             LISTEN
7     tcp   1.1.1.1:53            0.0.0.0:0             LISTEN
8     tcp   172.16.37.205:53      0.0.0.0:0             LISTEN
9     tcp   10.0.0.8:53           0.0.0.0:0             LISTEN
10    tcp   172.16.37.240:53      0.0.0.0:0             LISTEN
11    tcp   192.168.1.1:53        0.0.0.0:0             LISTEN
12    tcp   127.0.0.1:53          0.0.0.0:0             LISTEN
13    tcp   0.0.0.0:21            0.0.0.0:0             LISTEN
14    tcp   0.0.0.0:22            0.0.0.0:0             LISTEN
15    tcp   127.0.0.1:953         0.0.0.0:0             LISTEN
16    tcp   0.0.0.0:443           0.0.0.0:0             LISTEN
17    tcp   127.0.0.1:1723        0.0.0.0:0             LISTEN
```

Here is an example of the command that displays the open ports.

```
Router(config)# show socket open
No.   Proto Local_Address         Foreign_Address       State
==========================================================================
1     tcp   172.23.37.240:22      172.23.37.10:1179     ESTABLISHED
2     udp   127.0.0.1:64002       0.0.0.0:0
3     udp   0.0.0.0:520           0.0.0.0:0
4     udp   0.0.0.0:138           0.0.0.0:0
5     udp   0.0.0.0:138           0.0.0.0:0
6     udp   0.0.0.0:138           0.0.0.0:0
7     udp   0.0.0.0:138           0.0.0.0:0
8     udp   0.0.0.0:138           0.0.0.0:0
9     udp   0.0.0.0:138           0.0.0.0:0
10    udp   0.0.0.0:138           0.0.0.0:0
11    udp   0.0.0.0:32779         0.0.0.0:0
12    udp   192.168.1.1:4500      0.0.0.0:0
13    udp   1.1.1.1:4500          0.0.0.0:0
14    udp   10.0.0.8:4500         0.0.0.0:0
15    udp   172.23.37.205:4500    0.0.0.0:0
16    udp   172.23.37.240:4500    0.0.0.0:0
17    udp   127.0.0.1:4500        0.0.0.0:0
18    udp   127.0.0.1:63000       0.0.0.0:0
19    udp   127.0.0.1:63001       0.0.0.0:0
20    udp   127.0.0.1:63002       0.0.0.0:0
21    udp   0.0.0.0:161           0.0.0.0:0
22    udp   127.0.0.1:63009       0.0.0.0:0
23    udp   192.168.1.1:1701      0.0.0.0:0
24    udp   1.1.1.1:1701          0.0.0.0:0
25    udp   10.0.0.8:1701         0.0.0.0:0
26    udp   172.23.37.205:1701    0.0.0.0:0
27    udp   172.23.37.240:1701    0.0.0.0:0
28    udp   127.0.0.1:1701        0.0.0.0:0
29    udp   127.0.0.1:63024       0.0.0.0:0
30    udp   127.0.0.1:30000       0.0.0.0:0
31    udp   1.1.1.1:53            0.0.0.0:0
32    udp   172.23.37.205:53      0.0.0.0:0
33    udp   10.0.0.8:53           0.0.0.0:0
34    udp   172.23.37.240:53      0.0.0.0:0
35    udp   192.168.1.1:53        0.0.0.0:0
36    udp   127.0.0.1:53          0.0.0.0:0
37    udp   0.0.0.0:67            0.0.0.0:0
38    udp   127.0.0.1:63046       0.0.0.0:0
39    udp   127.0.0.1:65097       0.0.0.0:0
40    udp   0.0.0.0:65098         0.0.0.0:0
41    udp   192.168.1.1:500       0.0.0.0:0
42    udp   1.1.1.1:500           0.0.0.0:0
43    udp   10.0.0.8:500          0.0.0.0:0
44    udp   172.23.37.205:500     0.0.0.0:0
45    udp   172.23.37.240:500     0.0.0.0:0
46    udp   127.0.0.1:500         0.0.0.0:0
```

Here are examples of the commands that display the system uptime and model, firmware, and build information.

```
Router> show system uptime
system uptime: 04:18:00
Router> show version
Zyxel Communications Corp.
model           : ZyWALL USG 110
firmware version: 2.20(AQQ.0)b3
BM version      : 1.08
build date      : 2014-01-21 01:18:06
```

This example shows the current LED states on the Zyxel Device. The SYS LED lights on and green. The HDD LEDs is off.

```
Router> show led status
sys: green
usbled: off
Router>
```

4.1 ATP Dashboard Commands

Use these commands to view status and statistics information about security services on the ZyWALL ATP models.

Table 8 Dashboard Commands

COMMAND	DESCRIPTION
`show anti-botnet dashboard statistics summary`	Displays the number of the connection attempts detected or blocked, and the number of malware threats.
`show ip-reputation dashboard statistics summary`	Displays the number of IPv4 addresses that have been scanned, the number of hit counts on the scanned IPv4 addresses, and the number of IPv4 address for each threat level.
`show anti-spam dashboard statistics summary`	Displays the number of emails that the Zyxel Device's email security feature has checked, the number of spam emails and the number of suspicious websites known for phishing.
`show anti-virus statistics summary`	Displays the number of viruses detected.
`show content-filter dashboard statistics summary`	Displays the number of web pages that the Zyxel Device's content filtering feature has checked.
`show idp dashboard statistics summary`	Displays the number of sessions and packets that the Zyxel Device's IDP feature has checked.
`show sandbox dashboard statistics summary`	Displays the number of files that have been scanned or destroyed and the scan result.
`show security-service status`	Displays whether the security service, such as content filtering or sandboxing is enabled on the Zyxel Device.
`threat-website dashboard statistics flush`	Clears the URL Threat Filter statistics on the dashboard.
`content-filter dashboard statistics flush`	Clears the content-filter statistics on the dashboard.

4.2 CPU Temperature Monitor Commands

Use these commands to have the Zyxel Device periodically write CPU temperatures to the system logs.

Table 9 Dashboard Commands

COMMAND	DESCRIPTION
`show cpu-temperature-monitor status`	Displays whether CPU temperature monitoring is enabled, and how often the temperature is written to the system logs.
`[no] cpu-temperature-monitor activate`	Enables or disables CPU monitoring.
`cpu-temperature-monitor period` *`minutes`*	Sets how often in minutes that the Zyxel Device writes CPU temperature to the system logs. The valid range is 5-120.
`cpu-temperature-monitor unit {celsius| fahrenheit}`	Sets the temperature unit that the Zyxel Device uses when it writes CPU temperature to the system logs.

4.3 System Protection Signature Commands

Use these commands to view the system protection signature information and update the signatures if necessary.

Table 10 System Protection Signature Commands

COMMAND	DESCRIPTION
`show system protection signatures version`	Displays system protection signatures of the Zyxel Device. These signatures do not require a license. The Zyxel Device will synch with the Cloud Helper Server every day to update these signatures automatically. You can also update manually using the command below. Please note that in the web configurator, the system protection signature version displays in Dashboard > About. System protection signatures protect your Zyxel Device and local networks from web attacks, such as command injection, cross-site scripting and path traversal. Command injection: This is an attack in which an attacker uses the Zyxel Device vulnerabilities to execute commands to control your Zyxel Device. Cross-site scripting: This is an attack in which an attacker implants malicious scripts in a website. When you visit this website, the malicious scripts are sent and executed on your web browser. Path traversal: This is an attack that allows an attacker to access files you store in the web root folder.
`show system protection signature update status`	Displays if the system protection signatures are updated to the latest version.
`system protection signature update signature`	Use this command to update the system protection signatures to the latest version. Make sure the Zyxel Device can access the Cloud Helper Server when you want to update the signatures.

CHAPTER 5
Registration

5.1 Registration Overview

This chapter introduces myZyxel and shows you how to register the Zyxel Device for IDP/AppPatrol, anti-virus, content filtering, and SSL VPN services using commands.

5.2 myZyxel Overview

myZyxel is Zyxel's online services center where you can register your Zyxel Device and manage subscription services available for the Zyxel Device.

Note: You need to create an account before you can register your device and activate the services at myZyxel.

First, go to *http://www.myZyxel* with the Zyxel Device's serial number and LAN MAC address to register the Zyxel Device. Refer to the web site's on-line help for details. You can also go to the portal and see license status using the Licensing > Registration screens.

Note: To activate a service on a Zyxel Device, you need to access myZyxel via that Zyxel Device.

5.2.1 Subscription Services Available on the Zyxel Device

Refer to Section 1.4.6 on page 32 for differences between ATP and USG license names.

The Zyxel Device can use anti-virus, anti-spam, IDP/AppPatrol (Intrusion Detection and Prevention and application patrol), SSL VPN, and content filtering subscription services.

ZyWALL models need a license for UTM (Unified Threat Management) functionality. See the Introduction chapter in the Zyxel Device User's Guide or the product datasheet for details.

You can purchase an EiCard and enter the license key from it, at *http://www.myZyxel.com* to have the ZyWALL use UTM services or have the Zyxel Device use more SSL VPN tunnels. See the respective chapters in the User's Guide for more information about UTM features.

- The Zyxel Device's anti-virus packet scanner uses signature files on the Zyxel Device to detect virus. Your Zyxel Device scans files transmitted through enabled interfaces into the network. Subscribe to signature updates for Zyxel's anti-virus engine. After the service is activated, the Zyxel Device can download the up-to-date signatures from the update server.

  After the trial expires, you need to purchase an EiCard and enter the PIN number (license key) at *http://www.myZyxel.com*.

- The IDP and application patrol features use IDP/AppPatrol signatures on the Zyxel Device. IDP detects malicious or suspicious packets and responds immediately. Application patrol conveniently manages the use of various applications on the network. After the service is activated, the Zyxel Device can download the up-to-date signature files from the update server.
- SSL VPN tunnels provide secure network access to remote users. You can purchase and enter a license key to have the Zyxel Device use more SSL VPN tunnels.
- Content filter allows or blocks access to web sites. Subscribe to category-based content filtering to block access to categories of web sites based on content. Your Zyxel Device accesses an external database that has millions of web sites categorized based on content. You can have the Zyxel Device block, block and/or log access to web sites based on these categories.
- You will get automatic e-mail notification of new signature releases from mySecurityZone after you activate the IDP/AppPatrol service. You can also check for new signatures at *http://mysecurity.zyxel.com*.

See the respective chapters for more information about these features.

Note: To update the signature file or use a subscription service, you have to register the Zyxel Device and activate the corresponding service at myZyxel (through the Zyxel Device).

5.3 Registration Commands

The following table describes the commands available for registration. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 11 Command Summary: Registration

COMMAND	DESCRIPTION
`service-register checkexpire`	Gets information of all service subscriptions from myZyxel and updates the status table.
`service-register _setremind {after-10-days | after-180-days | after-30-days | every-time | never}`	Sets how often you want to display the network risk warning screen in the Web Configurator. The screen shows the security services which are not registered or disabled on the Zyxel Device.
`show device-register status`	Displays whether the device is registered and account information.
`show service-register status {all | application-security | as | av | cdr | concurrent-device-upgrade | content-filter | firmware-upgrade | geo-ip | idp | malware-blocker | ctdb | managed-ap-service | pkg | reputation-filter | sandbox | secu-reporter | secure-wifi | sslvpn | sslvpn-status | web-security | zymesh| network-premium}`	Displays the status of your service registrations. Use all to show all registrations as a list. Note: Options for this command might vary depending on the Zyxel Device model and firmware version.
`show service-register status content-filter {commtouch}`	Displays Commtouch content filter service license information.
`show service-register status sslvpn-status`	Displays the status of SSL VPN tunnels. The first number is the actual number of VPN tunnels up and the second number is the maximum number of SSL VPN tunnels allowed.
`show service-register content-filter-engine`	Displays which external web filtering service the Zyxel Device is set to use for content filtering.

5.3.1 Command Examples

The following command displays the account information and whether the device is registered.

```
Router# configure terminal
Router(config)# show device-register status
username               : example
password               : 123456
device register status : yes
expiration self check  : no
```

The following command displays the service registration status and type and how many days remain before the service expires.

```
Router# configure terminal
Router(config)# show service-register status all
Service              Status       Type     Count    Expiration
==============================================================================
IDP Signature        Licensed     Standard N/A      176
Anti-Virus           Not Licensed None     N/A      0
SSLVPN               Not Licensed None     5        N/A
Content-Filter       Not Licensed None     N/A      0
```

5.4 Update License Commands

The following table describes the commands you need to use to update the signatures through a proxy server on the Intranet. The Intranet proxy server downloads signatures from the Zyxel Cloud signature server. The Zyxel Device then downloads signatures from the Intranet proxy server. Contact your local support at http://www.zyxel.com for any questions on setting up the proxy server.

You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 12 Command Summary: Update License

COMMAND	DESCRIPTION
`[no] security-service update-server activate`	Enables the Intranet proxy server used to update signatures. The no command disables this feature.
`security-service update-server server-url <url>`	Sets the Intranet proxy server used to update signatures.
`show security-service update-server`	Displays the status and URL of the Intranet proxy server used to update signatures.

CHAPTER 6
AP Management

6.1 AP Management Overview

The Zyxel Device allows you to remotely manage all of the Access Points (APs) on your network. You can manage a number of APs without having to configure them individually as the Zyxel Device automatically handles basic configuration for you.

The commands in this chapter allow you to add, delete, and edit the APs managed by the Zyxel Device by means of the CAPWAP protocol. An AP must be moved from the wait list to the management list before you can manage it. If you do not want to use this registration mechanism, you can disable it and then any newly connected AP is registered automatically.

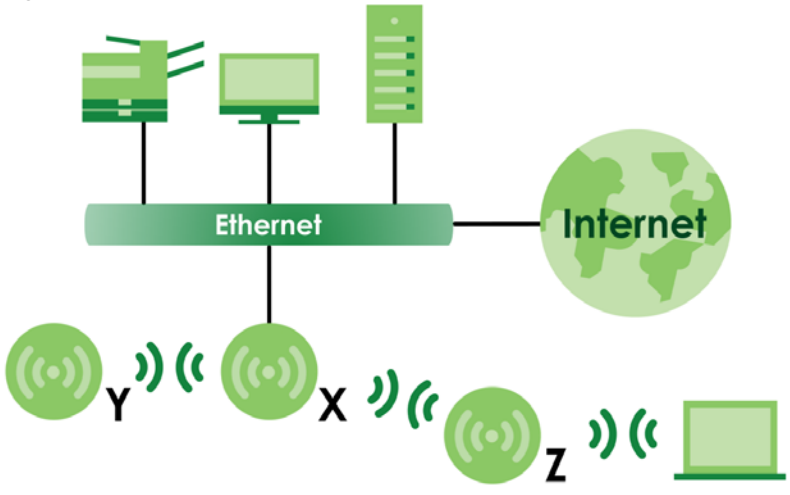
6.1.1 AP Modes

This section describes some of the different roles that the AP can take up within a network.

- Access Point: This is used to allow wireless clients to connect to the Internet.
- Monitor AP: A monitor AP acts as a wireless monitor, which can detect rogue APs and help you in building a list of friendly ones.
- Root AP: A root AP connects to the gateway or switch through a wired Ethernet connection and has wireless repeaters connected to it to extend its range.
- Repeater: A repeater connects to a root AP using a WiFi connection and extends the network's WiFi range.

In the figure below, the repeater (Z) is connected to the root AP (X) using a WiFi connection. X is connected to a wired network. The monitor repeater (Y) is also connected to X using a WiFi connection. Y is monitoring the WiFi network.

Figure 14 AP Network Roles Application



6.1.2 Airtime Fairness

Airtime is the time it takes for a client to receive packets from the AP it is associated with. The amount of time each client needs may vary depending on various reasons, such as the distance between the client and the AP, the client's operating system, or the IEEE standard the client is using.

Airtime fairness is a feature that makes sure all connected clients of an AP get the same amount of time to receive packets. Without airtime fairness, a client that needs more airtime will take up more time and bandwidth of an AP to receive packets. This will slow down your WiFi network overall.

6.2 AP Management Value

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 13 Input Values for AP Management Commands

LABEL	DESCRIPTION
ap_mac	The Ethernet MAC address of the managed AP. Enter 6 hexidecimal pairs separated by colons. You can use 0-9, a-z and A-Z.
ap_model	The model name of the managed AP, such as NWA5160N, NWA5560-N, NWA5550-N, NWA5121-NI or NWA5123-NI.
slot_name	The slot name for the AP's on-board wireless LAN card. Use either *slot1* or *slot2*. (The NWA5560-N supports up to 2 radio slots.)
profile_name	The wireless LAN radio profile name. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
ap_description	The AP description. This is strictly used for reference purposes and has no effect on any other settings. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
sta_mac	The MAC address of the wireless client. Enter 6 hexidecimal pairs separated by colons. You can use 0-9, a-z and A-Z.

6.3 General AP Management Commands

The following table describes the commands available for general AP management. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 14 Command Summary: AP Management

COMMAND	DESCRIPTION
`[no] capwap activate`	Enables or disables the AP controller service.
`capwap ap <mac address> [no] airtime-fairness activate`	Enables airtime fairness on the specified AP. The no command disables airtime fairness on the AP.
`capwap ap ap_mac`	Enters the sub-command mode for the specified AP.
`slot_name ap-profile profile_name`	Sets the radio (*slot_name*) to AP mode and assigns a created profile to the radio. See Section 6.1.1 on page 56 for more information on different modes.

Table 14 Command Summary: AP Management (continued)

COMMAND	DESCRIPTION
`no slot_name ap-profile`	Removes the AP mode profile assignment for the specified radio (*slot_name*). See Section 6.1.1 on page 56 for more information on different modes.
`slot_name monitor-profile profile_name`	Sets the specified radio (*slot_name*) to monitor mode and assigns a created profile to the radio. See Section 6.1.1 on page 56 for more information on different modes. See also Section 9.2 on page 76 for more information on rogue APs and friendly APs.
`no slot_name monitor-profile`	Removes the monitor mode profile assignment for the specified radio (*slot_name*).
`slot_name {root-ap | repeater-ap } zymesh-profile_name`	Sets the specified radio (*slot_name*) to root AP or repeater mode and assigns a created ZyMesh profile to the radio. See Section 6.1.1 on page 56 for more information on different modes. See also Section 9.6 on page 95 for more information about ZyMesh.
`slot_name wireless-bridge {enable | disable}`	Enables or disables wireless bridging on the specified radio (*slot_name*). The radio should be in repeater mode. VLAN and bridge interfaces are created automatically according to the VLAN settings. See Section 6.1.2 on page 57 for more information on wireless bridge. When wireless bridging is enabled, the managed repeater AP can still transmit data through its Ethernet port(s) after the ZyMesh/WDS link is up. Be careful to avoid bridge loops. See Section 6.1.1 on page 56 for more information on different modes. The managed APs in the same ZyMesh/WDS must use the same static VLAN ID.
`antenna config slot_name chain3 {ceiling | wall}`	Adjusts coverage depending on each radio's antenna orientation.
`[no] antenna sw-control enable`	Enables the adjustment of coverage depending on the orientation of the antenna for the AP radios using the web configurator or the command line interface (CLI), The `no` command disables adjustment through the web configurator or the command line interface (CLI).
`ap-group-profile ap-group-profile_name`	Sets the AP group to which the AP belongs.
`description ap_description`	Sets the description for the specified AP.
`[no] force vlan`	Sets whether or not the Zyxel Device changes the AP's management VLAN to match the one you configure using the `vlan` sub-command. The management VLAN on the Zyxel Device and AP must match for the Zyxel Device to manage the AP. This takes priority over the AP's CAPWAP client commands described in Chapter 73 on page 604.
`lan-provision lan_port {activate | inactivate} pvid <1..4094>`	Sets the Zyxel Device to enable or disable the specified LAN port on the AP and configures a PVID (Port VLAN ID) for this port. *lan_port*: the name of the AP's LAN port (lan1 for example).

Table 14 Command Summary: AP Management (continued)

COMMAND	DESCRIPTION
lan-provision *vlan_interface* {activate | inactivate} vid <1..4094> join *lan_port* {tag | untag} [*lan_port* {tag | untag}] [*lan_port* {tag | untag}]	Sets the Zyxel Device to create a new VLAN or configure an existing VLAN. You can disable or enable the VLAN, set the VLAN ID, assign up to three ports to this VLAN as members and set whether the port is to tag outgoing traffic with the VLAN ID. *vlan_interface*: the name of the VLAN (vlan1 for example).
[no] override-full-power activate	Forces the AP to draw full power from the power sourcing equipment. This improves performance in cases when a PoE injector that does not support PoE negotiation is used. Use the no command to disable this feature.
[no] load-balancing <group1 | group2> *group_name*	Assigns a load balancing group to the AP. Use the no command to remove the group1 or group2 assignment of the AP.
[no] override *slot_name* {output-power | radio-setting | ssid-setting}	Sets the Zyxel Device to overwrite the AP's output power, radio or SSID profile settings for the specified radio. Use the no command to not overwrite the specified settings.
[no] override lan-provision	Sets the Zyxel Device to overwrite the AP's LAN port settings. Use the no command to not overwrite the specified settings.
[no] override vlan-setting	Sets the Zyxel Device to overwrite the AP's LAN port settings. Use the no command to not overwrite the specified settings.
vlan <1..4094> {tag | untag}	Sets the VLAN ID for the specified AP as well as whether packets sent to and from that ID are tagged or untagged.
exit	Exits the sub-command mode for the specified AP.
capwap ap ac-ip *{primary_ac_ip} {secondary_ac_ip}*	Specifies the primary and secondary IP address or domain name of the AP controller (the Zyxel Device) to which the AP connects.
capwap ap ac-ip auto	Sets the AP to use DHCP to get the address of the AP controller (the Zyxel Device).
capwap ap add *ap_mac* [*ap_model*]	Adds the specified AP to the Zyxel Device for management. If manual add is disabled, this command can still be used; if you add an AP before it connects to the network, then this command simply preconfigures the management list with that AP's information.
capwap ap factory default *ap_mac*	Resets the specified AP to its factory default settings.
capwap ap fallback disable	Sets the managed AP(s) to not change back to associate with the primary AP controller when the primary AP controller is available.
capwap ap fallback enable	Sets the managed AP(s) to change back to associate with the primary AP controller as soon as the primary AP controller is available.
capwap ap fallback interval <30..86400>	Sets how often (in seconds) the managed AP(s) check whether the primary AP controller is available.
capwap ap idle timeout {25–100}	Sets the default period after which idle wireless clients are kicked from an AP, in minutes. This setting takes affect if setting Disassociate station when overloaded is enabled.

Table 14 Command Summary: AP Management (continued)

COMMAND	DESCRIPTION
`capwap ap kick {all | ap_mac}`	Removes the specified AP (*ap_mac*) or all connected APs (*all*) from the management list. Doing this removes the AP(s) from the management list. If the Zyxel Device is set to automatically add new APs to the AP management list, then any kicked APs are added back to the management list as soon as they reconnect.
`capwap ap led-off ap_mac`	Sets the LEDs of the specified AP to turn off after it's ready.
`capwap ap led-on ap_mac`	Sets the LEDs of the specified AP to stay lit after the Zyxel Device is ready.
`capwap ap reboot ap_mac`	Forces the specified AP (*ap_mac*) to restart. Doing this severs the connections of all associated stations.
`capwap manual-add {enable | disable}`	Allows the Zyxel Device to either automatically add new APs to the network (*disable*) or wait until you manually confirm them (*enable*).
`capwap station kick sta_mac`	Forcibly disconnects the specified station from the network.
`show capwap ap {all | ap_mac}`	Displays information of all managed APs (*all*) or information of an AP on the Specified MAC address (*ap_mac*).
`show capwap ap {all | ap_mac} config status`	Displays whether or not any AP's configuration or the specified AP's configuration is in conflict with the Zyxel Device's settings for the AP, and displays the settings in conflict if there are any.
`country-code country_code`	Sets the country where the Zyxel Device is located/installed. This is the default country code the Zyxel Device uses in a new radio profile or monitor profile if you do not change it. The available channels vary depending on the country you selected. *country_code*: 2-letter country-codes, such as TW, DE, or FR.
`lan-provision ap ap_mac`	Enters the sub-command mode for the specified AP
`lan_port {activate | inactivate} pvid <1..4094>`	Enables or disables the specified LAN port on the AP and configures a PVID (Port VLAN ID) for this port. *lan_port*: the name of the AP's LAN port (lan1 for example).
`vlan_interface {activate | inactivate} vid <1..4094> join lan_port {tag | untag} [lan_port {tag | untag}] [lan_port {tag | untag}]`	Creates a new VLAN or configures an existing VLAN. You can disable or enable the VLAN, set the VLAN ID, assign up to three ports to this VLAN as members and set whether the port is to tag outgoing traffic with the VLAN ID. *vlan_interface*: the name of the VLAN (vlan1 for example).
`[no] vlan_interface`	Removes the specified VLAN.
`ap internal-auth shared-secret key`	Enter the shared secret key used by APs to authenticate with an Access Point Controller (APC) authentication server. The key is encrypted before being saved to the Zyxel Device. You can use the following characters: 0-9a-zA-Z`~!@#$%^&*()_\-+={}|\\;:'<,>\?.\
`ap internal-auth no shared-secret`	Resets the shared secret key to default.
`show capwap ap {all | ap_mac}`	Displays the management list (*all*) or whether the specified AP is on the management list (*ap_mac*).
`show capwap ap ap_mac slot_name detail`	Displays details for the specified radio (*slot_name*) on the specified AP (*ap_mac*).

Table 14 Command Summary: AP Management (continued)

COMMAND	DESCRIPTION
`show capwap ap {all | ap_mac} config status`	Displays whether or not any AP's configuration or the specified AP's configuration is in conflict with the Zyxel Device's settings for the AP and displays the settings in conflict if there are any.
`show capwap ap ac-ip`	Displays the address of the Zyxel Device or `auto` if the AP finds the Zyxel Device through broadcast packets.
`show capwap ap all statistics`	Displays radio statistics for all APs on the management list.
`show capwap ap fallback`	Displays whether the managed AP(s) will change back to associate with the primary AP controller when the primary AP controller is available.
`show capwap ap fallback interval`	Displays the interval for how often the managed AP(s) check whether the primary AP controller is available.
`show capwap ap idle timeout`	Displays the default period after which idle wireless clients are kicked from an AP, in minutes,
`show capwap ap wait-list`	Displays a list of connected but as-of-yet unmanaged APs. This is known as the 'wait list'.
`show capwap manual-add`	Displays the current manual add option.
`show capwap station all`	Displays information for all stations connected to the APs on the management list.
`show country-code list`	Displays a reference list of two-letter country codes.
`show default country-code`	Displays the default country code configured on the Zyxel Device.
`show lan-provision ap ap_mac interface {lan_port | vlan_interface | all| ethernet | uplink | vlan}`	Displays the port and/or VLAN settings for the specified AP. You can also set to display settings for a specified port, a sepcified VLAN, all physical Ethernet ports, the uplink port or all VLANs on the AP.

6.3.1 AP Management Commands Example

The following example shows you how to add an AP to the management list, and then edit it.

```
Router# show capwap ap wait-list
index: 1
  IP: 192.168.1.35, MAC: 00:11:11:11:11:FE
  Model: NWA5160N, Description: AP-00:11:11:11:11:FE
index: 2
  IP: 192.168.1.36, MAC: 00:19:CB:00:BB:03
  Model: NWA5160N, Description: AP-00:19:CB:00:BB:03
Router# configure terminal
Router(config)# capwap ap add 00:19:CB:00:BB:03
Router(config)# capwap ap 00:19:CB:00:BB:03
Router(AP 00:19:CB:00:BB:03)# slot1 ap-profile approf01
Router(AP 00:19:CB:00:BB:03)# exit
Router(config)# show capwap ap all
index: 1
  Status: RUN
  IP: 192.168.1.37, MAC: 40:4A:03:05:82:1E
  Description: AP-404A0305821E
  Model: NWA5160N
  R1 mode: AP, R1Prof: default
  R2 mode: AP, R2Prof: n/a
  Station: 0, RadioNum: 2
  Mgnt. VLAN ID: 1, Tag: no
  WTP VLAN ID: 1, WTP Tag: no
  Force VLAN: disable
  Firmware Version: 2.25(AAS.0)b2
  Recent On-line Time: 08:43:04 2013/05/24
  Last Off-line Time: N/A

Router(config)# show capwap ap 40:4A:03:05:82:1E slot1 detail
index: 1
  SSID: Zyxel, BSSID: 40:4A:03:05:82:1F
  SecMode: NONE, Forward Mode: Local Bridge, Vlan: 1

Router(config)# show capwap ap all statistics
index: 1
  Status: RUN, Loading: -
  AP MAC: 40:4A:03:05:82:1E
  Radio: 1, OP Mode: AP
  Profile: default, MAC: 40:4A:03:05:82:1F
  Description: AP-404A0305821E
  Model: NWA5160N
  Band: 2.4GHz, Channel: 6
  Station: 0
  RxPkt: 4463, TxPkt: 38848
  RxFCS: 1083323, TxRetry: 198478
```

The following example displays the management list and radio statistics for the specified AP.

```
Router(config)# show capwap ap all
index: 1
  Status: RUN
  IP: 192.168.1.37, MAC: 60:31:97:82:F5:AF
  Description: AP-60319782F5AF
  Model: WAC5302D-S
  CPU Usage: 12 %
  R1 mode: AP, R1Prof: default
  R2 mode: AP, R2Prof: default2
  AP Group Profile: default
  Override Slot1 Radio Profile: disable
  Override Slot1 SSID Profile: disable
  slot1-SSID Profile 1: default
  slot1-SSID Profile 2:
  slot1-SSID Profile 3:
  slot1-SSID Profile 4:
  slot1-SSID Profile 5:
  slot1-SSID Profile 6:
  slot1-SSID Profile 7:
  slot1-SSID Profile 8:
  Override Slot1 Output Power: disable
  Slot1 Output Power: 30dBm
  Override Slot2 Radio Profile: disable
  Override Slot2 SSID Profile: disable
  slot2-SSID Profile 1: default
  slot2-SSID Profile 2:
  slot2-SSID Profile 3:
  slot2-SSID Profile 4:
  slot2-SSID Profile 5:
  slot2-SSID Profile 6:
  slot2-SSID Profile 7:
  slot2-SSID Profile 8:
  Override Slot2 Output Power: disable
  Slot2 Output Power: 30dBm
  Station: 2, RadioNum: 2
  Override VLAN Setting: disable
  Mgnt. VLAN ID: 1, Tag: no
  WTP VLAN ID: 1, WTP Tag: no
  Force VLAN: disable
  Support Lan-provision: yes
  Override LAN Provision: disable
  Firmware Version: 5.00(ABFH.1)b1
  Primary AC IP: broadcast
  Secondary AC IP: N/A
  Recent On-line Time: 03:15:30 2016/11/11
  Last Off-line Time: 03:10:48 2016/11/11
  Loop State: N/A
  LED Status: N/A
  Suppress Mode Status: Enable
  Locator LED Status: N/A
  Locator LED Time: 0
  Locator LED Time Lease: 0
  Power Mode: Full
  Antenna Switch SW-Control: N/A
  Antenna Switch Radio 1: N/A
  Antenna Switch Radio 2: N/A
```

```
  Compatible: No
  Capability: 32
  Port Number: 4
Router(config)# show capwap ap 60:31:97:82:F5:AF slot1 detail
index: 1
  SSID: ZyXEL
  BSSID: 60:31:97:82:F5:B0
  SecMode: NONE, Forward Mode: Local Bridge, Vlan: 1
Router(config)# show capwap ap all statistics
index: 1
  Status: RUN, Loading: -
  AP MAC: 60:31:97:82:F5:AF
  Radio: 1, OP Mode: AP
  Profile: default, MAC: F0:FD:F0:FD:F0:FD
  Description: AP-60319782F5AF
  Model: WAC5302D-S
  Band: 2.4GHz, Channel: 6
  Station: 0
  Rx: 101395, Tx: 866288
  RxFCS: 42803, TxRetry: 897
  TxPower: 15 dBm
  Antenna Type: N/A

index: 2
  Status: RUN, Loading: -
  AP MAC: 60:31:97:82:F5:AF
  Radio: 2, OP Mode: AP
  Profile: default2, MAC: F0:FD:F0:FD:F0:FD
  Description: AP-60319782F5AF
  Model: WAC5302D-S
  Band: 5GHz, Channel: 36/40
  Station: 2
  Rx: 864251, Tx: 1076862
  RxFCS: 169608, TxRetry: 2816
  TxPower: 16 dBm
  Antenna Type: N/A

Router(config)#
```

6.4 Remote AP

Remote AP enables the ZyXEL device to connect to an Access Point (AP) through a secure VPN tunnel. This allows you to set up VPN-enabled WiFi APs in remote locations, such as in a branch office or at home. Clients connected to these APs can securely access your network through the VPN tunnel.

Figure 15 Remote AP: Secure Tunnel SSID

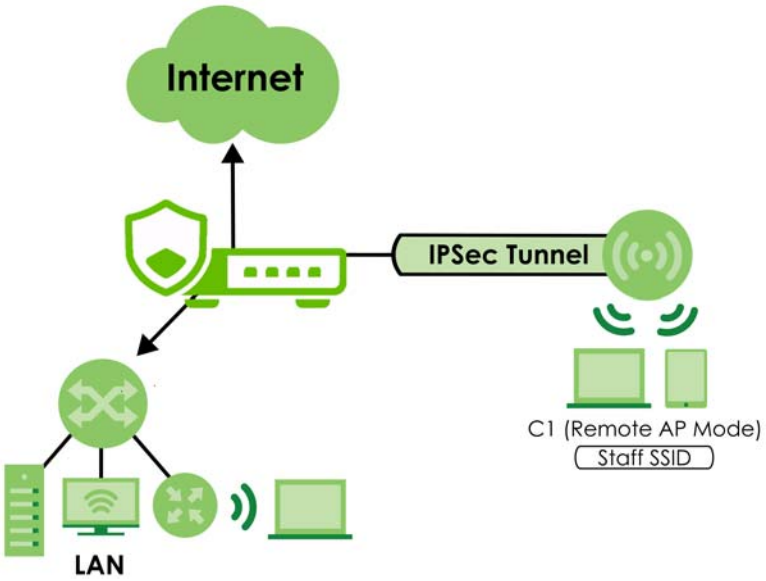
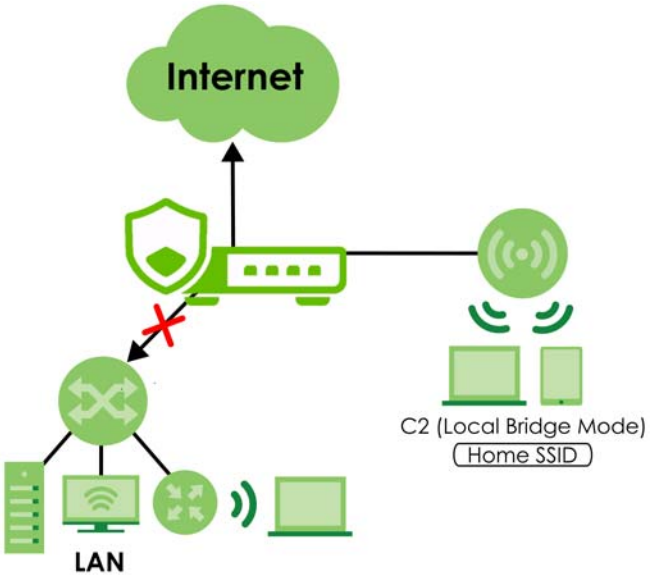


Figure 16 Remote AP: Local Bridge SSID



6.4.1 Remote AP Notes

- When you enable Remote AP, the Zyxel Device automatically creates a secure Network Virtualization Using Generic Routing Encapsulation (NVGRE) over IPSec tunnel between itself and the AP using the default VPN profile _remote_ap_vpn_profile. This profile cannot be edited.
- The first time Remote AP is enabled on an AP, the Zyxel Device adds the CAPWAP-CONTROL service to the service group Default_Allow_WAN_To_ZyWALL. If Remote AP is disabled on all APs, this rule is removed.
- Enabling Remote AP automatically enables Ethernet and wireless storm control on the AP.
- Remote AP is only supported on certain AP models. To check whether an AP supports Remote AP, run the command `show capwap ap` *`ap_mac`*, and then ensure that “Remote AP Capability” equals “Yes”.
- Remote AP only supports IP version 4 (IPv4).

6.4.2 Remote AP Commands

The following table describes the commands available for managing Remote AP (RAP). You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 15 Command Summary: Remote AP Management

COMMAND	DESCRIPTION
`capwap ap ap_mac`	Enters the sub-command mode for the specified AP.
`role remote`	Enables the Remote AP feature on the AP.
`no role`	Disables the Remote AP feature on the AP.
`rap slot_name ap-profile profile_name`	Sets the radio (*slot_name*) to AP mode and assigns a created profile to the radio.
`no rap slot_name ap-profile`	Removes the AP mode profile assignment for the specified radio (*slot_name*).
`rap slot_name output-power wlan_power`	Sets the output power (between 0 to 30 dBm) for the AP radio.
`rap slot_name ssid-profile <1..6> ssid_profile_name [tunlif interface] vid vlan_id`	Sets an SSID profile and VLAN ID that is associated with this AP. You can associate up to six SSID profiles with a Remote AP radio. • SSID profiles 1 to 4 are Secure Tunnel SSIDs. Network traffic from clients connected to these SSIDs is sent through the RAP tunnel to the ZyXEL device. The ZyXEL device then sends the traffic out through the interface defined in the SSID profile. This outgoing interface can be overridden by specifiying an interface with the command `tunlif`. • SSID profiles 5 and 6 are Local Bridge SSIDs. Network traffic from clients connected to these SSIDs is sent directly to the network through the AP's local gateway. • Traffic is tagged with the VLAN ID defined by *vlan_id*.
`no rap slot_name ssid-profile <1..6>`	Removes the SSID profile from the AP.
`show sa monitor [ap-description desc] rap`	Displays the current IPSec SA for each Remote AP.
`vpn-policy-pool start start_ip end end_ip`	Sets the start and end IPv4 addresses for the shared Remote AP IP address pool. The interface of the RAP IPSec tunnel on the AP is assigned an IP address from this pool.
`show vpn-policy-pool`	Displays the start and end IPv4 address for the Remote AP VPN pool.

CHAPTER 7
Built-in AP

If your Zyxel Device has a built-in AP, then use this function to allow WiFi clients to access your Zyxel Device wirelessly to connect to the network.

Note: The Zyxel Device cannot mange external APs when the built-in AP is enabled.

Table 16 Input Values for Built-in AP Commands

LABEL	DESCRIPTION
slot_name	The slot name for the Zyxel Device's on-board wireless LAN card. Use either *slot1* or *slot2*.

7.1 Built-in AP Commands

Table 17 Command Summary: Built-in AP

COMMAND	DESCRIPTION
capwap ap local-ap	Enter sub-command mode for the built-in AP.
[no] *slot_name* ap-profile *radio_profile_name*	Sets the specified built-in radio to work as an AP and specifies the radio profile the radio is to use. Use the no command to remove the specified profile.
[no] *slot_name* monitor-profile *monitor_profile_name*	Sets the specified built-in radio to work in monitor mode and specifies the monitor profile the radio is to use. Use the no command to remove the specified profile.
[no] *slot_name* output-power *wlan_power*	Sets the output power (between 0 to 30 dBm) for the built-in AP radio. Use the no command to remove the output power setting.
[no] *slot_name* ssid-profile <1..8> *ssid_profile_name*	Sets the SSID profile that is associated with this profile. You can associate up to eight SSID profiles with an AP radio. Use the no command to remove the specified profile.
[no] *slot_name* zymesh-profile *zymesh_profile_name*	Sets the ZyMesh profile the built-in AP radio (in root AP or repeater mode) uses to connect to a root AP or repeater. Use the no command to remove the specified profile.
ap-group-profile *ap-group-profile_name*	Sets the AP group to which the built-in AP belongs.
[no] ap-mode detection activate	Sets the built-in AP to detect Rogue APs in then network. Use the no parameter to disable rogue AP detection. For details about this feature, see Chapter 10 on page 97.

COMMAND	DESCRIPTION
location *location*	Sets the name of the place where the AP is located, for admin reference. Use the no command to remove the specified setting.
[no] override *slot_name* {output-power | radio-setting | ssid-setting}	Sets the Zyxel Device to overwrite the built-in AP's output power, radio or SSID profile settings for the specified radio. Use the no command to not overwrite the specified settings.
sysname *system_name*	Sets a name to identify the AP on a network. This is usually the AP's fully qualified domain name. Use the no command to remove the specified setting.
exit	Exits sub-command mode.

Chapter 8
AP Group

If your Zyxel Device has a built-in AP, then use this function to allow WiFi clients to access your Zyxel

Device wirelessly to connect to the network.This chapter shows you how to configure AP groups, which define the radio, port, VLAN and load balancing settings and apply the settings to all APs in the group. An AP can belong to one AP group at a time.

8.1 Wireless Load Balancing Overview

Wireless load balancing is the process whereby you limit the number of connections allowed on an wireless access point (AP) or you limit the amount of wireless traffic transmitted and received on it. Because there is a hard upper limit on the AP's wireless bandwidth, this can be a crucial function in areas crowded with wireless users. Rather than let every user connect and subsequently dilute the available bandwidth to the point where each connecting device receives a meager trickle, the load balanced AP instead limits the incoming connections as a means to maintain bandwidth integrity.

8.2 AP Group Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 18 Input Values for General AP Management Commands

LABEL	DESCRIPTION
ap_group_profile_name	The wireless LAN radio profile name. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
slot_name	The slot name for the AP's on-board wireless LAN card. Use either *slot1* or *slot2*. (The NWA5560-N supports up to 2 radio slots.)

The following table describes the commands available for AP groups. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 19 Command Summary: AP Group

COMMAND	DESCRIPTION
`ap-group first-priority` *ap_group_profile_name*	Sets an AP group file that is used as the default group file. Any AP that is not configured to associate with a specific AP group belongs to the default group automatically.
`ap-group flush wtp-setting` *ap_group_profile_name*	Sets the Zyxel Device to overwrite the settings of all managed APs in the specified group with the group profile settings.
`ap-group-member` *ap_group_wlan_name*`[no] member local-ap`	Specifies the SSID of the built-in AP that you want to apply the specified AP group profile and add to the group. Use the no command to remove the built-in AP from this group.

Table 19 Command Summary: AP Group (continued)

COMMAND	DESCRIPTION
ap-group-member *ap_group_profile_name* [no] member *mac_address*	Specifies the MAC address of the AP that you want to apply the specified AP group profile and add to the group. Use the no command to remove the specified AP from this group.
[no] ap-group-profile *ap_group_profile_name*	Enters configuration mode for the specified AP group profile. Use the no command to remove the specified profile.
[no] *slot_name* ap-profile *radio_profile_name*	Sets the specified radio to work as an AP and specifies the radio profile the radio is to use. Use the no command to remove the specified profile.
[no] *slot_name* monitor-profile *monitor_profile_name*liInterval	Sets the specified radio to work in monitor mode and specifies the monitor profile the radio is to use. Use the no command to remove the specified profile.
[no] *slot_name* output-power *wlan_power*	Sets the output power (between 0 to 30 dBm) for the radio on the AP that belongs to this group. Use the no command to remove the output power setting.
[no] *slot_name* ssid-profile <1..8> *ssid_profile_name*	Sets the SSID profile that is associated with this profile. You can associate up to eight SSID profiles with an AP radio. Use the no command to remove the specified profile.
[no] *slot_name* repeater-ap *radio_profile_name*	Sets the specified AP radio to work as a repeater and specifies the radio profile the radio is to use. Use the no command to remove the specified profile.
[no] *slot_name* root-ap *radio_profile_name*	Sets the specified radio to work as a root AP and specifies the radio profile the radio is to use. A root AP supports the wireless connections with other APs (in repeater mode) to form a ZyMesh to extend its wireless network. Use the no command to remove the specified profile.
[no] *slot_name* zymesh-profile *zymesh_profile_name*	Sets the ZyMesh profile the radio (in root AP or repeater mode) uses to connect to a root AP or repeater. Use the no command to remove the specified profile.
description *description*	Sets a description for this group. You can use up to 31 characters, spaces and underscores allowed. Use the no command to remove the specified description.
exit	Exits configuration mode for this profile.
[no] force vlan	Sets the Zyxel Device to change the AP's management VLAN to match the configuration in this profile. Use the no command to not change the AP's management VLAN setting.
[no] lan-provision model {nwa5301-nj | wac6502d-e | wac6502d-s | wac6503d-s | wac6553d-e} *ap_lan_port* activate pvid <1..4094>	Sets the model of the managed AP and enable the model-specific LAN port and configure the port VLAN ID. Use the no command to remove the specified port and VLAN settings. *ap_lan_port*: the Ethenet LAN port on the managed AP, such as lan1 or lan2.

Table 19 Command Summary: AP Group (continued)

COMMAND	DESCRIPTION
`[no] lan-provision model {nwa5301-nj | wac6502d-e | wac6502d-s | wac6503d-s | wac6553d-e} ap_lan_port inactivate pvid <1..4094>`	Sets the model of the managed AP and disable the model-specific LAN port and configure the port VLAN ID. Use the no command to remove the specified port and VLAN settings. *ap_lan_port*: the Ethenet LAN port on the managed AP, such as lan1 or lan2.
`[no] lan-provision model {nwa5301-nj | wac6502d-e | wac6502d-s | wac6503d-s | wac6553d-e} vlan_interface activate vid <1..4094> join ap_lan_port {tag | untag} [ap_lan_port {tag | untag}] [ap_lan_port {tag | untag}]`	Sets the model of the managed AP, enable a VLAN and configure the VLAN ID. It also sets the Ethernet port(s) on the managed AP to be a member of the VLAN, and sets the port(s) to send packets with or without a VLAN tag. Use the no command to remove the specified port and VLAN settings. *vlan_interface*: the name of the VLAN, such as vlan0. *ap_lan_port*: the Ethenet LAN port on the managed AP, such as lan1 or lan2.
`[no] lan-provision model {nwa5301-nj | wac6502d-e | wac6502d-s | wac6503d-s | wac6553d-e} vlan_interface inactivate vid <1..4094> join ap_lan_port {tag | untag} [ap_lan_port {tag | untag}] [ap_lan_port {tag | untag}]`	Sets the model of the managed AP, disable a VLAN and configure the VLAN ID. It also sets the Ethernet port(s) on the managed AP to be a member of the VLAN, and sets the port(s) to send packets with or without a VLAN tag. Use the no command to remove the specified port and VLAN settings. *vlan_interface*: the name of the VLAN, such as vlan0. *ap_lan_port*: the Ethenet LAN port on the managed AP, such as lan1 or lan2.
`[no] load-balancing [slot1 | slot2] activate`	Enables load balancing. Use the no parameter to disable it. Optionally specify a radio slot.
`load-balancing [slot1 | slot2] alpha <1..255>`	Sets the load balancing alpha value. When the AP is balanced, then this setting delays a client's association with it by this number of seconds. Note: This parameter has been optimized for the Zyxel Device and should not be changed unless you have been specifically directed to do so by Zyxel support.
`load-balancing [slot1 | slot2] beta <1..255>`	Sets the load balancing beta value. When the AP is overloaded, then this setting delays a client's association with it by this number of seconds. Note: This parameter has been optimized for the Zyxel Device and should not be changed unless you have been specifically directed to do so by Zyxel support.
`load-balancing [slot1 | slot2] kickInterval <1..255>`	Enables the kickout feature for load balancing and also sets the kickout interval in seconds. While load balancing is enabled, the AP periodically disconnects stations at intervals equal to this setting. This occurs until the load balancing threshold is no longer exceeded.
`[no] load-balancing [slot1 | slot2] kickout`	Enables an overloaded AP to disconnect ("kick") idle clients or clients with noticeably weak connections.

Table 19 Command Summary: AP Group (continued)

COMMAND	DESCRIPTION
load-balancing [slot1 | slot2] liInterval <1..255>	Sets the interval in seconds that each AP communicates with the other APs in its range for calculating the load balancing algorithm. Note: This parameter has been optimized for the Zyxel Device and should not be changed unless you have been specifically directed to do so by Zyxel support.
load-balancing [slot1 | slot2] max sta <1..127>	If load balancing by the number of stations/wireless clients, this sets the maximum number of devices allowed to connect to a load-balanced AP.
load-balancing mode [slot1 | slot2] {station | traffic | smart-classroom}	Enables load balancing based on either number of stations (also known as wireless clients) or wireless traffic on an AP. station or traffic: once the threshold is crossed (either the maximum station numbers or with network traffic), the AP delays association request and authentication request packets from any new station that attempts to make a connection. smart-classroom: the AP ignores association request and authentication request packets from any new station when the maximum number of stations is reached.
load-balancing [slot1 | slot2] sigma <51..100>	Sets the load balancing sigma value. This value is algorithm parameter used to calculate whether an AP is considered overloaded, balanced, or underloaded. It only applies to 'by traffic mode'. Note: This parameter has been optimized for the Zyxel Device and should not be changed unless you have been specifically directed to do so by Zyxel support.
load-balancing [slot1 | slot2] timeout <1..255>	Sets the length of time that an AP retains load balancing information it receives from other APs within its range.
load-balancing [slot1 | slot2] traffic level {high | low | medium}	If load balancing by traffic threshold, this sets the traffic threshold level.
vlan <1..4094> {tag | untag}	Sets the management VLAN ID for the AP(s) in this group as well as whether packets sent to and from that VLAN ID are tagged or untagged.
show ap-group first-priority	Displays the name of the default AP group profile.
show ap-group-profile {all | *ap_group_profile_name*}	Displays the settings of the AP group profile(s). *all*: Displays all profiles. *ap_group_profile_name*: Displays the specified profile.
show ap-group-profile *ap_group_profile_name* load-balancing config	Displays the load balancing configuration of the specified AP group profile.
show ap-group-profile *ap_group_profile_name* lan-provision interface {all | vlan | ethernet | *ap_lan_port* | *vlan_interface*} model {nwa5301-nj | wac6502d-e | wac6502d-s | wac6503d-s | wac6553d-e}	Displays the LAN port and/or VLAN settings on the managed AP which is in the specified AP group and of the specified model. *vlan_interface*: the name of the VLAN, such as vlan0. *ap_lan_port*: the Ethenet LAN port on the managed AP, such as lan1 or lan2.

Table 19 Command Summary: AP Group (continued)

COMMAND	DESCRIPTION
`show ap-group-profile ap_group_profile_name lan-provision model`	Shows the model name of the managed AP which belongs to the specified AP group.
`show ap-group-profile rule_count`	Displays how many AP group profiles have been configured on the Zyxel Device.
`ap-group-profile rename` *`ap_group_profile_name1 ap_group_profile_name2`*	Gives an existing AP group profile (*`ap_group_profile_name1`*) a new name (*`ap_group_profile_name2`*).

8.2.1 AP Group Examples

The following example shows you how to create an AP group profile (named “TEST”) and configure the AP’s first radio to work in repeater mode using the “default” radio profile and the “ZyMesh_TEST” ZyMesh profile. It also adds the AP with the MAC address 00:a0:c5:01:23:45 to this AP group.

```
Router(config)# ap-group-profile TEST
Router(config-ap-group TEST)# slot1 repeater-ap default
Router(config-ap-group TEST)# exit
Router(config)# ap-group-member TEST member 00:a0:c5:01:23:45
Router(config)#
```

The following example shows you how to create an AP group profile (named GP1) and configure AP load balancing in "by station" mode. The maximum number of stations is set to 1.

```
Router(config)# ap-group-profile GP1
Router(config-ap-group GP1)# load-balancing mode station
Router(config-ap-group GP1)# load-balancing max sta 1
Router(config-ap-group GP1)# exit
Router(config)# show ap-group-profile GP1 load-balancing config
AP Group Profile:GP1
load balancing config:
Activate: yes
Kickout: no
Mode: station
Max-sta: 1
Traffic-level: high
Alpha: 5
Beta: 10
Sigma: 60
Timeout: 20
LIInterval: 10
KickoutInterval: 20
Router(config)#
```

The following example shows you how to create an AP group profile (named GP2) and configure AP load balancing in "by traffic" mode. The traffic level is set to low, and "disassociate station" is enabled.

```
Router(config)# ap-group-profile GP2
Router(config-ap-group GP2)# load-balancing mode traffic
Router(config-ap-group GP2)# load-balancing traffic level low
Router(config-ap-group GP2)# load-balancing kickout
Router(config-ap-group GP2)# exit
Router(config)# show ap-group-profile GP2 load-balancing config
AP Group Profile:GP2
load balancing config:
Activate: yes
Kickout: yes
Mode: traffic
Max-sta: 1
Traffic-level: low
Alpha: 5
Beta: 10
Sigma: 60
Timeout: 20
LIInterval: 10
KickoutInterval: 20
Router(config)#
```

The following example shows the settings and status of the VLAN(s) configured for the managed APs (NWA5301-NJ) in the default AP group.

```
Router(config)# show ap-group-profile default lan-provision interface vlan
model nwa5301-nj
No. Name            Active VID   Member
==============================================================================
1   vlan0           yes    1     lan1,lan2,lan3
Router(config)# show ap-group-profile default lan-provision interface vlan0
model nwa5301-nj
active: yes
interface name: vlan0
VID: 1
member: lan1&lan2&lan3
lan1_tag: untag
lan2_tag: untag
lan3_tag: untag
Router(config)#
```

The following example shows the status of Ethernet ports for the managed APs (NWA5301-NJ) in the default AP group. It also shows whether the lan1 port is enabled and what the port's VLAN ID is.

```
Router(config)# show ap-group-profile default lan-provision interface
ethernet model nwa5301-nj
No. Name            Active PVID
================================================================================
1   uplink          yes    n/a
2   lan1            yes    1
3   lan2            yes    1
4   lan3            yes    1
Router(config)# show ap-group-profile default lan-provision interface lan1
model nwa5301-nj
Name            Active PVID
================================================================================
lan1            yes    1
Router(config)#
```

CHAPTER 9
Wireless LAN Profiles

This chapter shows you how to configure wireless LAN profiles on your Zyxel Device.

9.1 Wireless LAN Profiles Overview

The managed Access Points designed to work explicitly with your Zyxel Device do not have on-board configuration files, you must create “profiles” to manage them. Profiles are preset configurations that are uploaded to the APs and which manage them. They include: Radio and Monitor profiles, SSID profiles, Security profiles, and MAC Filter profiles. Altogether, these profiles give you absolute control over your wireless network.

9.2 AP Radio & Monitor Profile Commands

The radio profile commands allow you to set up configurations for the radios onboard your various APs. The monitor profile commands allow you to set up monitor mode configurations that allow your APs to scan for other APs in the vicinity.

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 20 Input Values for General Radio and Monitor Profile Commands

LABEL	DESCRIPTION
radio_profile_name	The radio profile name. You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
monitor_profile_name	The monitor profile name. You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
interval	Enters the dynamic channel selection interval time. The range is 10 ~ 1440 minutes.
wlan_role	Sets the wireless LAN radio operating mode. At the time of writing, you can use ap for Access Point.
wireless_channel_2g	Sets the 2 GHz channel used by this radio profile. The channel range is `1 ~ 14`. Note: Your choice of channel may be restricted by regional regulations.
`wireless_channel_5g`	Sets the 5 GHz channel used by this radio profile. The channel range is `36 ~ 165`. Note: Your choice of channel may be restricted by regional regulations.
wlan_htcw	Sets the HT channel width. Select either `20`, `20/40` or `20/40/80`.
wlan_htgi	Sets the HT guard interval. Select either `long` or `short`.
chain_mask	Sets the network traffic chain mask. The range is `1 ~ 7`.

Table 20 Input Values for General Radio and Monitor Profile Commands (continued)

LABEL	DESCRIPTION
wlan_power	Sets the radio output power.
scan_method	Sets the radio's scan method while in Monitor mode. Select `manual` or `auto`.
wlan_interface_index	Sets the radio interface index number. The range is `1 ~ 8`.
ssid_profile	Sets the associated SSID profile name. This name must be an existing SSID profile. You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

The following table describes the commands available for radio and monitor profile management. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 21 Command Summary: Radio Profile

COMMAND	DESCRIPTION
`show wlan-radio-profile {all | radio_profile_name}`	Displays the radio profile(s). *all*: Displays all profiles. *radio_profile_name*: Displays the specified profile.
`dcs dfs-aware {enable|disable}`	Enables this to force the Zyxel Device to only use the non-DFS channels. Disables this to allow the Zyxel Device to use the DFS channels for more channel options. Dynamic Frequency Selection (DFS) is a channel WiFi allocation scheme that allows APs to use channels in the 5 Ghz band normally reserved for radar. Before using a DFS channel, an AP must ensure there is no radar present by performing a Channel Availability Check (CAC). This check takes 1-10 minutes, depending on the country in which the AP is located.
`wlan-radio-profile rename radio_profile_name1 radio_profile_name2`	Gives an existing radio profile (*radio_profile_name1*) a new name (*radio_profile_name2*).
`[no] wlan-radio-profile radio_profile_name`	Enters configuration mode for the specified radio profile. Use the *no* parameter to remove the specified profile.
`2g-basic-speed speed`	
`2g-channel wireless_channel_2g`	Sets the broadcast band for this profile in the 2.4 GHz frequency range. The default is 6.
`2g-multicast-speed wlan_2g_support_speed`	When you disable `multicast` to `unicast`, use this command to set the data rate `{ 1.0 | 2.0 | … }` in Mbps for 2.4 GHz multicast traffic.
`2g-wlan-rate-control rate_2g`	Sets the minimum data rate that 2.4Ghz WiFi clients can connect at, in Mbps. At the time of write, allowed values are: 1, 2,5. 5, 6, 9, 11, 12, 18, 24, 36, 48, 54. Increasing the minimum data rate can reduce network overhead and improve WiFi network performance in high density environments. However, WiFi clients that do not support the minimum data rate will not be able to connect to the AP.
`5g-basic-speed speed`	
`5g-channel wireless_channel_5g`	Sets the broadcast band for this profile in the 5 GHz frequency range. The default is 36.

Table 21 Command Summary: Radio Profile (continued)

COMMAND	DESCRIPTION
5g-multicast-speed *wlan_5g_basic_speed*	When you disable multicast to unicastt, use this command to set the data rate { 6.0 | 9.0 | … } in Mbps for 5 GHz multicast traffic.
5g-wlan-rate-control rate_5g	Sets the minimum data rate that 5 Ghz WiFi clients can connect at, in Mbps. At the time of write, allowed values are: 6,9, 12, 18, 24, 36, 48, 54. Increasing the minimum data rate can reduce network overhead and improve WiFi network performance in high density environments. However, WiFi clients that do not support the minimum data rate will not be able to connect to the AP.
6g-channel *wireless_channel_6g*	Sets the broadcast band for this profile in the 6 GHz frequency range.
6g-multicast-speed *wlan_6g_basic_speed*	When you disable multicast to unicastt, use this command to set the data rate in Mbps for 6 GHz multicast traffic.
6g-wlan-rate-control *rate_6g*	Sets the minimum data rate that 6 Ghz WiFi clients can connect at, in Mbps. At the time of write, allowed values are: 6,9, 12, 18, 24, 36, 48, 54. Increasing the minimum data rate can reduce network overhead and improve WiFi network performance in high density environments. However, WiFi clients that do not support the minimum data rate will not be able to connect to the AP.
[no] activate	Makes this radio profile active or inactive.
[no] ampdu	Activates MPDU frame aggregation for this profile. Use the *no* parameter to disable it. Message Protocol Data Unit (MPDU) aggregation collects Ethernet frames along with their 802.11n headers and wraps them in a 802.11n MAC header. This method is useful for increasing bandwidth throughput in environments that are prone to high error rates. By default this is enabled.
limit-ampdu < *100..65535*>	Sets the maximum frame size to be aggregated using MPDU. By default this is 50000.
subframe-ampdu *<2..64>*	Sets the maximum number of frames to be aggregated each time. By default this is 32.
[no] amsdu	Activates MPDU frame aggregation for this profile. Use the *no* parameter to disable it. Mac Service Data Unit (MSDU) aggregation collects Ethernet frames without any of their 802.11n headers and wraps the header-less payload in a single 802.11n MAC header. This method is useful for increasing bandwidth throughput. It is also more efficient than A-MPDU except in environments that are prone to high error rates. By default this is enabled.
limit-amsdu *<2290..4096>*	Sets the maximum frame size to be aggregated using MPDU. The default is 4096.

Table 21 Command Summary: Radio Profile (continued)

COMMAND	DESCRIPTION
band {2.4G |5G| 6G} band-mode {bg | bgn | a | ac | an | bgnax | anacax| ax}	Sets the radio band (2.4 GHz, 5 GHz or 6 GHz) and band mode for this profile. Band mode details: For 2.4 GHz, bg lets IEEE 802.11b and IEEE 802.11g clients associate with the AP. For 2.4 GHz, bgn lets IEEE 802.11b, IEEE 802.11g, and IEEE 802.11n clients associate with the AP. For 2.4 GHz, bgnax lets IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, and IEEE802.11ax clients associate with the AP. For 5 GHz, a lets only IEEE 802.11a clients associate with the AP. For 5 GHz, ac lets IEEE 802.11a, IEEE 802.11n, and IEEE 802.11ac clients associate with the AP. For 5 GHz, an lets IEEE 802.11a and IEEE 802.11n clients associate with the AP. For 5 GHz, anacax lets IEEE 802.11a, IEEE 802.11n, IEEE 802.11ac, and IEEE802.11ax clients associate with the AP. For 6 GHz, ax lets IEEE802.11ax clients associate with the AP.
beacon-interval <*40..1000*>	Sets the beacon interval for this profile. When a wirelessly networked device sends a beacon, it includes with it a beacon interval. This specifies the time period before the device sends the beacon again. The interval tells receiving devices on the network how long they can wait in low-power mode before waking up to handle the beacon. This value can be set from 40ms to 1000ms. A high value helps save current consumption of the access point. The default is 100.
[no] block-ack	Makes block-ack active or inactive. Use the *no* parameter to disable it.
bss-color <0~63>	Sets the BSS color of the AP, which distinguishes it from other nearby APs when they transmit over the same channel. Set it to 0 to automatically assign a BSS color.
[no] disable-bss-color	Disables BSS coloring. Use the no command to enable BSS coloring.
ch-width *wlan_htcw*	Sets the channel width for this profile.
country-code *country_code*	Sets the country where the Zyxel Device is located/installed. The available channels vary depending on the country you selected. Be sure to select the correct/same country for both radios on an AP and all connected APs, in order to prevent roaming failure and interference to other systems. *country_code*: 2-letter country-codes, such as TW, DE, or FR.

Table 21 Command Summary: Radio Profile (continued)

COMMAND	DESCRIPTION
`[no] ctsrts <0..2347>`	Sets or removes the RTS/CTS value for this profile. Use RTS/CTS to reduce data collisions on the wireless network if you have wireless clients that are associated with the same AP but out of range of one another. When enabled, a wireless client sends an RTS (Request To Send) and then waits for a CTS (Clear To Send) before it transmits. This stops wireless clients from transmitting packets at the same time (and causing data collisions). A wireless client sends an RTS for all packets larger than the number (of bytes) that you enter here. Set the RTS/CTS equal to or higher than the fragmentation threshold to turn RTS/CTS off. The default is 2347.
`[no] dcs activate`	Starts dynamic channel selection to automatically find a less-used channel in an environment where there are many APs and there may be interference. Use the no parameter to turn it off.
`dcs 2g-selected-channel` *`2.4g_channels`*	Specifies the channels that are available in the 2.4 GHz band when you manually configure the channels an AP can use.
`dcs 5g-selected-channel` *`5g_channels`*	Specifies the channels that are available in the 5 GHz band when you manually configure the channels an AP can use.
`dcs 6g-selected-channel` *`6g_channels`*	Specifies the channels that are available in the 6 GHz band when you manually configure the channels an AP can use.
`dcs dcs-2g-method {auto|manual}`	Sets the AP to automatically search for available channels or manually configure the channels the AP uses in the 2.4 GHz band.
`dcs dcs-5g-method {auto|manual}`	Sets the AP to automatically search for available channels or manually configure the channels the AP uses in the 5 GHz band.
`dcs dcs-6g-method {auto|manual}`	Sets the AP to automatically search for available channels or manually configure the channels the AP uses in the 6 GHz band.
`dcs client-aware {enable|disable}`	When enabled, this ensures that an AP will not change channels as long as a client is connected to it. If disabled, the AP may change channels regardless of whether it has clients connected to it or not.
`dcs channel-deployment {3-channel|4-channel}`	Sets either a 3-channel deployment or a 4-channel deployment. In a 3-channel deployment, the AP running the scan alternates between the following channels: 1, 6, and 11. In a 4-channel deployment, the AP running the scan alternates between the following channels: 1, 4, 7, and 11 (FCC) or 1, 5, 9, and 13 (ETSI). Sets the option that is applicable to your region. (Channel deployment may be regulated differently between countries and locales.)
`dcs dfs-aware {enable|disable}`	Enable this to allow an AP to avoid phase DFS channels below the 5 GHz spectrum. Note: This feature is automatically disabled when Zero-Wait DFS is enabled.

Table 21 Command Summary: Radio Profile (continued)

COMMAND	DESCRIPTION
`dcs mode {interval|schedule}`	Sets the AP to use DCS at the end of the specified time interval or at a specifc time on selected days of the week.
`dcs schedule <hh:mm> {mon|tue|wed|thu|fri|sat|sun}`	Sets what time of day (in 24-hour format) the AP starts to use DCS on the specified day(s) of the week.
`dcs sensitivity-level {high|medium |low}`	Sets how sensitive DCS is to radio channel changes in the vicinity of the AP running the scan.
`dcs time-interval` *`interval`*	Sets the interval that specifies how often DCS should run.
`description` *`description`*	Sets the description of the profile. You may use up to 60 alphanumeric characters, underscores (_), or dashes (-).
`[no] disable-dfs-switch`	Makes the DFS switch active or inactive. By default this is inactive.
`dot11-preamble {long|short}`	
`[no] dot11n-disable-coexistence`	Fixes the channel bandwidth as 40 MHz. The no command has the AP automatically choose 40 MHz if all the clients support it or 20 MHz if some clients only support 20 MHz.
`dtim-period <1..255>`	Sets the DTIM period for this profile. Delivery Traffic Indication Message (DTIM) is the time period after which broadcast and multicast packets are transmitted to mobile clients in the Active Power Management mode. A high DTIM value can cause clients to lose connectivity with the network. This value can be set from 1 to 255. The default is 1.
`[no] force-mu-mimo`	
`[no] frag <256..2346>`	Sets or removes the fragmentation value for this profile. The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. The default is 2346.
`guard-interval` *`wlan_htgi`*	Sets the guard interval for this profile. The default for this is *`short`*.
`[no] htprotect`	Activates HT protection for this profile. Use the *no* parameter to disable it. By default, this is disabled.
`[no] ignore-country-ie`	Prevents the AP from broadcasting a country code, also called a country Information Element (IE), in beacon frames. This makes the AP incompatible with 802.11d networks and devices. The no command allows the AP to broadcast the country code. 802.11d is a WiFi network specification that allows an AP to broadcast a country code to WiFi clients. The country code tells clients where the AP is located. Note: Run this command if WiFi clients are unable to connect to the AP because of an incompatible country code.
`max-sw-retries <0..10>`	

Table 21 Command Summary: Radio Profile (continued)

COMMAND	DESCRIPTION
`[no] multicast-to-unicast`	"Multicast to unicast" broadcasts wireless multicast traffic to all wireless clients as unicast traffic to provide more reliable transmission. The data rate changes dynamically based on the application's bandwidth requirements. Although unicast provides more reliable transmission of the multicast traffic, it also produces duplicate packets. The no command turns multicast to unicast off to send wireless multicast traffic at the rate you specify with the `2g-multicast-speed`, `5g-multicast-speed` or `6g-multicast-speed` command.
`[no] nol-channel-block`	Enables or disables temporary DFS channel blacklisting. If enabled, the AP will block a DFS channel if it detects a radar signal within that range. Note: This feature is automatically disabled when Zero-Wait DFS is enabled.
`output-power` *`wlan_power`*	Sets the output power (between 0 to 30 dBm) for the radio in this profile.
`pn-check-thres <0..100>`	
`[no] reject-legacy-station`	
`role` *`wlan_role`*	Sets the profile's wireless LAN radio operating mode.
`rssi-dbm <-20~-76>`	When using the RSSI threshold, set a minimum client signal strength for connecting to the AP. -20 dBm is the strongest signal you can require and -76 is the weakest.
`rssi-interval (1..86400>`	
`rssi-kickout <-20~-105>`	Sets a minimum kick-off signal strength. When a wireless client's signal strength is lower than the specified threshold, the Zyxel Device disconnects the wireless client from the AP. -20 dBm is the strongest signal you can require and -105 is the weakest.
`rssi-optype <0-3>`	
`rssi-privilegetime`	
`[no] rssi-retry`	Allows a wireless client to try to associate with the AP again after it is disconnected due to weak signal strength. Use the *no* parameter to disallow it.
`rssi-retrycount <1~100>`	Sets the maximum number of times a wireless client can attempt to re-connect to the AP.
`[no] rssi-thres`	Sets whether or not to use the Received Signal Strength Indication (RSSI) threshold to ensure wireless clients receive good throughput. This allows only wireless clients with a strong signal to connect to the AP.
`rssi-verifytime`	
`rx-mask` *`chain_mask`*	Sets the incoming chain mask rate.
`schedule` *`schedule_object`*	Sets the radio profile to be activate according to the schedule defined by the specified schedule object.
`[no] ssid-profile` *`wlan_interface_index ssid_profile`*	Assigns an SSID profile to this radio profile. Requires an existing SSID profile. Use the *no* parameter to disable it.
`subframe-ampdu <2..64>`	

Table 21 Command Summary: Radio Profile (continued)

COMMAND	DESCRIPTION
`[no] suppress-retry-rts`	
`tx-mask` *`chain_mask`*	Sets the outgoing chain mask rate.
`[no] zero-wait-dfs`	Enables or disables zero-wait DFS (Dynamic Frequency Selection) on the AP. Note: Zero-wait DFS is only supported on certain AP models, such as the WAX650S. DFS is a channel WiFi allocation scheme that allows APs to use channels in the 5Ghz band normally reserved for radar. Before using a DFS channel, an AP must ensure that no radar present by performing a Channel Availability Check (CAC). This check takes 1-10 minutes, depending on the country in which the AP is located. Zero-Wait DFS allows an AP to provide network services to WiFi clients using a primary 5Ghz radio, while simultaneously checking DFS channels for the presence of radar using a secondary 5Ghz radio. If no radar is detected on a DFS channel, the AP adds it to a list of cleared channels. The AP can then switch the primary radio to any cleared DFS channel without having to wait 1-10 minutes for a Channel Availability Check. Note: When zero-wait DFS is enabled, 5Ghz DFS Aware (`dcs dfs-aware`) and Blacklist DFS Channels (`nol-channel-block`) are automatically disabled on the AP.
`exit`	Exits configuration mode for this profile.
`storm-control ethernet ap` *`mac_address`*	Enables Ethernet storm control and then enters the Ethernet storm control sub-command mode for the specified radio profile. Ethernet storm control prevents WiFi clients from receiving excessive broadcast or multicast traffic sent from wired clients in the same subnet.
`[no] broadcast`	Enables or disables broadcast storm control, which drops broadcast packets from ingress traffic if the traffic rate exceeds the configured maximum rate.
`broadcast pps <1~10000>`	Sets the maximum allowed rate for broadcast traffic, in packets per second.
`[no] multicast`	Enables or disables multicast storm control, which drops multicast packets from ingress traffic if the traffic rate exceeds the configured maximum rate.
`multicast pps <1~10000>`	Sets the maximum allowed rate for multicast traffic, in packets per second.
`exit`	Exits configuration mode for this profile.
`no storm-control ethernet ap` *`mac_address`*	Disables Ethernet broadcast and multicast storm control, and removes all Ethernet storm control settings for the specified AP.

Table 21 Command Summary: Radio Profile (continued)

COMMAND	DESCRIPTION
`storm-control wireless ap` *mac_address*	Enables wireless storm control and then enters the wireless storm control sub-command mode for the specified AP. Wireless storm control prevents wired clients from receiving excessive broadcast or multicast traffic sent from WiFi clients in the same subnet. Note: To enable wireless storm control, Remote AP must be enabled on the AP and the AP must be running firmware version 6.20 or later.
`[no] broadcast`	Enables or disables broadcast storm control, which drops broadcast packets from ingress traffic if the traffic rate exceeds the configured maximum rate.
`broadcast pps <1~10000>`	Sets the maximum allowed rate for broadcast traffic, in packets per second.
`[no] multicast`	Enables or disables multicast storm control, which drops multicast packets from ingress traffic if the traffic rate exceeds the configured maximum rate.
`multicast pps <1~10000>`	Sets the maximum allowed rate for multicast traffic, in packets per second.
`exit`	Exits configuration mode for this profile.
`no storm-control wireless ap` *mac_address*	Disables wireless broadcast and multicast storm control, and removes all wireless storm control settings for the specified AP.
`show storm-control ethernet ap` *mac_address*	Displays broadcast/multicast storm control settings on the specified AP.
`show wlan-monitor-profile {all |` *monitor_profile_name*`}`	Displays all monitor profiles or just the specified one.
`wlan-monitor-profile rename` *monitor_profile_name1 monitor_profile_name2*	Gives an existing monitor profile (*monitor_profile_name1*) a new name (*monitor_profile_name2*).
`[no] wlan-monitor-profile` *monitor_profile_name*	Enters configuration mode for the specified monitor profile. Use the *no* parameter to remove the specified profile.
`[no] activate`	Makes this profile active or inactive. By default, this is enabled.
`country-code` *country_code*	Sets the country where the Zyxel Device is located/installed. The available channels vary depending on the country you selected. Be sure to select the correct/same country for both radios on an AP and all connected APs, in order to prevent roaming failure and interference to other systems. *country_code*: 2-letter country-codes, such as TW, DE, or FR.
`scan-method` *scan_method*	Sets the channel scanning method for this profile.
`[no] 2g-scan-channel` *wireless_channel_2g*	Sets the broadcast band for this profile in the 2.4 Ghz frequency range. Use the *no* parameter to disable it.
`[no] 5g-scan-channel` *wireless_channel_5g*	Sets the broadcast band for this profile in the 5 GHz frequency range. Use the *no* parameter to disable it.

Table 21 Command Summary: Radio Profile (continued)

COMMAND	DESCRIPTION
`scan-dwell <100..1000>`	Sets the duration in milliseconds that the device using this profile scans each channel.
`exit`	Exits configuration mode for this profile.

9.2.1 AP Radio & Monitor Profile Commands Example

The following example shows you how to set up the radio profile named 'RADIO01', activate it, and configure it to use the following settings:

- 2.4G band with channel 6
- channel width of 20MHz
- a DTIM period of 2
- a beacon interval of 100ms
- AMPDU frame aggregation enabled
- an AMPDU buffer limit of 65535 bytes
- an AMPDU subframe limit of 64 frames
- AMSDU frame aggregation enabled
- an AMSDU buffer limit of 4096
- block acknowledgement enabled
- a short guard interval
- an output power of 100%

It will also assign the SSID profile labeled 'default' in order to create WLAN VAP (wlan-1-1) functionality within the radio profile.

```
Router(config)# wlan-radio-profile RADIO01
Router(config-profile-radio)# activate
Router(config-profile-radio)# band 2.4G band-mode bgn
Router(config-profile-radio)# 2g-channel 6
Router(config-profile-radio)# ch-width 20/40
Router(config-profile-radio)# dtim-period 2
Router(config-profile-radio)# beacon-interval 100
Router(config-profile-radio)# ampdu
Router(config-profile-radio)# limit-ampdu 65535
Router(config-profile-radio)# subframe-ampdu 64
Router(config-profile-radio)# amsdu
Router(config-profile-radio)# limit-amsdu 4096
Router(config-profile-radio)# block-ack
Router(config-profile-radio)# guard-interval short
Router(config-profile-radio)# tx-mask 5
Router(config-profile-radio)# rx-mask 7
Router(config-profile-radio)# output-power 21dBm
Router(config-profile-radio)# ssid-profile 1 default
```

9.3 SSID Profile Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 22 Input Values for General SSID Profile Commands

LABEL	DESCRIPTION
ssid_profile_name	The SSID profile name. You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
ssid	The SSID broadcast name. You may use 1-32 alphanumeric characters, underscores (_), or dashes (-). This value is case-sensitive.
wlan_qos	Sets the type of QoS the SSID should use. *disable*: Turns off QoS for this SSID. *wmm*: Turns on QoS for this SSID. It automatically assigns Access Categories to packets as the device inspects them in transit. *wmm_be*: Assigns the "best effort" Access Category to all traffic moving through the SSID regardless of origin. *wmm_bk*: Assigns the "background" Access Category to all traffic moving through the SSID regardless of origin. *wmm_vi*: Assigns the "video" Access Category to all traffic moving through the SSID regardless of origin. *wmm_vo*: Assigns the "voice" Access Category to all traffic moving through the SSID regardless of origin.
vlan_iface	The VLAN interface name of the controller (in this case, it is Zyxel Device). The maximum VLAN interface number is product-specific; for the Zyxel Device, the number is 512.
securityprofile	Assigns an existing security profile to the SSID profile. You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
macfilterprofile	Assigns an existing MAC filter profile to the SSID profile. You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
description2	Sets the description of the profile. You may use up to 60 alphanumeric characters, underscores (_), or dashes (-). This value is case-sensitive.

The following table describes the commands available for SSID profile management. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 23 Command Summary: SSID Profile

COMMAND	DESCRIPTION
`show wlan-ssid-profile {all | ssid_profile_name}`	Displays the SSID profile(s). *all*: Displays all profiles for the selected operating mode. *ssid_profile_name*: Displays the specified profile for the selected operating mode.
`wlan-ssid-profile rename ssid_profile_name1 ssid_profile_name2`	Gives an existing SSID profile (*ssid_profile_name1*) a new name (*ssid_profile_name2*).
`[no] wlan-ssid-profile ssid_profile_name`	Enters configuration mode for the specified SSID profile. Use the *no* parameter to remove the specified profile.

Table 23 Command Summary: SSID Profile (continued)

COMMAND	DESCRIPTION
`[no] bandselect balance-ratio <1..8>`	Sets a ratio of the wireless clients using the 5 GHz band to the wireless clients using the 2.4 GHz band. Use the *no* parameter to turn off this feature.
`bandselect check-sta-interval <1..60000>`	Sets how often (in seconds) the AP checks and deletes old wireless client data.
`bandselect drop-authentication <1..16>`	Sets how many authentication request from a client to a 2.4GHz Wi-Fi network is ignored during the specified timeout period.
`bandselect drop-probe-request <1..32>`	Sets how many probe request from a client to a 2.4GHz Wi-Fi network is ignored during the specified timeout period.
`bandselect min-sort-interval <1..60000>`	Sets the minimum interval (in seconds) at which the AP sorts the wireless client data when the client queue is full.
`bandselect mode {disable | force | standard}`	To improve network performance and avoid interference in the 2.4 GHz frequency band, you can enable this feature to use the 5 GHz band first. You should set 2.4GHz and 5 GHz radio profiles to use the same SSID and security settings. Note: The managed APs must be dual-band capable. `disable`: to turn off this feature. `force`: to have the wireless clients always connect to an SSID using the 5 GHZ band. Connections to an SSID using the 2.4GHz band are not allowed. It is recommended you select this option when the AP and wireless clients can function in either frequency band. `standard`: to have the AP try to connect the wireless clients to the same SSID using the 5 GHZ band. Connections to an SSID using the 2.4GHz band are still allowed.
`[no] bandselect stop-threshold <10..20>`	Sets the threshold number of the connected wireless clients at which the AP disables the band select feature. Use the *no* parameter to turn off this feature.
`bandselect time-out-force <1..255>`	Sets the timeout period (in seconds) within which the AP accepts probe or authentication requests to a 2.4GHz Wi-Fi network when the band select mode is set to `force`.
`bandselect time-out-period <1..255>`	Sets the timeout period (in seconds) within which the AP drops the specified number of probe or authentication requests to a 2.4GHz Wi-Fi network.
`bandselect time-out-standard <1..255>`	Sets the timeout period (in seconds) within which the AP accepts probe or authentication requests to a 2.4GHz Wi-Fi network when the band select mode is set to `standard`.
`[no] block-intra`	Enables intra-BSSID traffic blocking. Use the no parameter to disable it in this profile. By default this is disabled.
`data-forward localbridge`	Sets the data forwarding mode used by the SSID to localbridge mode. In this mode, all of the wireless station's traffic is routed through the associated AP's gateway and tagged with the VLAN ID set by command `vlan-id`. This is the default data forwarding mode.

Table 23 Command Summary: SSID Profile (continued)

COMMAND	DESCRIPTION
`data-forward tunnel` *`interface`*	Sets the data forwarding mode used by the SSID to tunnel mode. In this mode, all of the wireless station's traffic is routed through the Zyxel Device via the specified interface. Note: The interface must be a VLAN or internal Ethernet interface. The interface cannot be a member of a bridge.
`downlink-rate-limit` *`data_rate`*	Sets the maximum incoming transmission data rate (either in mbps or kbps) on a per-station basis.
`[no] hide`	Prevents the SSID from being publicly broadcast. Use the no parameter to re-enable public broadcast of the SSID in this profile. By default this is disabled.
`[no] macfilter` *`macfilterprofile`*	Assigns the specified MAC filtering profile to this SSID profile. Use the no parameter to remove it. By default, no MAC filter is assigned.
`qos` *`wlan_qos`*	Sets the type of QoS used by this SSID.
`security` *`securityprofile`*	Assigns the specified security profile to this SSID profile.
`ssid`	Sets the SSID. This is the name visible on the network to wireless clients. Enter up to 32 characters, spaces and underscores are allowed. The default SSID is 'ZyXEL'.
`[no] ssid-schedule`	Enables the SSID schedule. Use the no parameter to disable the SSID schedule.
`{mon|tue|wed|thu|fri|sat|sun} {disable | enable} <hh:mm> <hh:mm>`	Sets whether the SSID is enabled or disabled on each day of the week. This also specifies the hour and minute (in 24-hour format) to set the time period of each day during which the SSID is enabled/enabled. `<hh:mm> <hh:mm>`: If you set both start time and end time to 00:00, it indicates a whole day event. Note: The end time must be larger than the start time.
`uplink-rate-limit` *`data_rate`*	Sets the maximum outgoing transmission data rate (either in mbps or kbps) on a per-station basis.
`vlan-id` *`<1..4094>`*	Applies to each SSID profile that uses `localbridge`. If the VLAN ID is equal to the AP's native VLAN ID then traffic originating from the SSID is not tagged. The default VLAN ID is 1.
`exit`	Exits configuration mode for this profile.

9.3.1 SSID Profile Example

The following example creates an SSID profile with the name 'ZyXEL'. It makes the assumption that both the security profile (SECURITY01) and the MAC filter profile (MACFILTER01) already exist.

```
Router(config)# wlan-ssid-profile SSID01
Router(config-ssid-radio)# ssid ZyXEL
Router(config-ssid-radio)# qos wmm
Router(config-ssid-radio)# data-forward localbridge
Router(config-ssid-radio)# security SECURITY01
Router(config-ssid-radio)# macfilter MACFILTER01
Router(config-ssid-radio)# exit
Router(config)#
```

9.4 Security Profile Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 24 Input Values for General Security Profile Commands

LABEL	DESCRIPTION
security_profile_name	The security profile name. You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
wep_key	Sets the WEP key encryption strength. Select either *64bit* or *128bit*.
wpa_key	Sets the WPA/WPA2 pre-shared key in ASCII. You may use 8~63 alphanumeric characters. This value is case-sensitive.
wpa_key_64	Sets the WPA/WPA2 pre-shared key in HEX. You muse use 64 alphanumeric characters.
secret	Sets the shared secret used by your network's RADIUS server.
auth_method	The authentication method used by the security profile.

The following table describes the commands available for security profile management. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 25 Command Summary: Security Profile

COMMAND	DESCRIPTION
`show wlan-security-profile {all | `*security_profile_name*`}`	Displays the security profile(s). *all*: Displays all profiles for the selected operating mode. *security_profile_name*: Displays the specified profile for the selected operating mode.
`wlan-security-profile rename` *security_profile_name1 security_profile_name2*	Gives existing security profile (*security_profile_name1*) a new name, (*security_profile_name2*).
`[no] wlan-security-profile` *security_profile_name*	Enters configuration mode for the specified security profile. Use the `no` parameter to remove the specified profile.

Table 25 Command Summary: Security Profile (continued)

COMMAND	DESCRIPTION
`[no] accounting interim-interval <1..1440>`	Sets the time interval for how often the AP is to send an interim update message with current client statistics to the accounting server. Use the no parameter to clear the interval setting.
`[no] accounting interim-update`	Sets the AP to send accounting update messages to the accounting server at the specified interval. Use the no parameter to disable it.
`description` *description*	Sets the description for the profile. You may use up to 60 alphanumeric characters, underscores (_), or dashes (-). This value is case-sensitive
`[no] dot11r activate`	Turns on IEEE 802.11r fast roaming on the AP. Use the no parameter to turn it off.
`[no] dot11r over-the-ds activate`	Sets the clients to communicate with the target AP through the current AP. The communication between the client and the target AP is carried in frames between the client and the current AP, and is then sent to the target AP through the wired Ethernet connection. Use the no parameter to have the clients communicate directly with the target AP.
`[no] dot1x-eap`	Enables 802.1x secure authentication. Use the no parameter to disable it.
`[no] dot11w`	Data frames in 802.11 WLANs can be encrypted and authenticated with WEP, WPA or WPA2. But 802.11 management frames, such as beacon/probe response, association request, association response, de-authentication and disassociation are always unauthenticated and unencrypted. IEEE 802.11w Protected Management Frames allows APs to use the existing security mechanisms (encryption and authentication methods defined in IEEE 802.11i WPA/WPA2) to protect management frames. This helps prevent wireless DoS attacks. Enables management frame protection (MFP) to add security to 802.11 management frames. Use the no parameter to disable it.
`dot11w-op <1..2>`	Sets whether wireless clients have to support management frame protection in order to access the wireless network. 1: if you do not require the wireless clients to support MFP. Management frames will be encrypted if the clients support MFP. 2: wireless clients must support MFP in order to join the AP's wireless network.
`eap {external | internal` *auth_method*`}`	Sets the 802.1x authentication method.
`group-key <30..30000>`	Sets the interval (in seconds) at which the AP updates the group WPA/WPA2 encryption key. The default is 3000.
`idle <30..30000>`	Sets the idle interval (in seconds) that a client can be idle before authentication is discontinued. The default is 300.
`[no] internal-eap-proxy activate`	Allows the Zyxel Device to act as a proxy server and forward the authentication packets to the connected RADIUS server. Use the no parameter to disable it.

Table 25 Command Summary: Security Profile (continued)

COMMAND	DESCRIPTION
`[no] mac-auth activate`	MAC authentication has the AP use an external server to authenticate wireless clients by their MAC addresses. Users cannot get an IP address if the MAC authentication fails. The no parameter turns it off. RADIUS servers can require the MAC address in the wireless client's account (username/password) or Calling Station ID RADIUS attribute.
`mac-auth auth-method` *`auth_method`*	Sets the authentication method for MAC authentication.
`mac-auth case account {upper | lower}`	Sets the case (upper or lower) the external server requires for using MAC addresses as the account username and password. For example, use `mac-auth case account upper` and `mac-auth delimiter account dash` if you need to use a MAC address formatted like 00-11-AC-01-A0-11 as the username and password.
`mac-auth case calling-station-id {upper | lower}`	Sets the case (upper or lower) the external server requires for letters in MAC addresses in the Calling Station ID RADIUS attribute.
`mac-auth delimiter account {colon | dash | none}`	Specify the separator the external server uses for the two-character pairs within MAC addresses used as the account username and password. For example, use `mac-auth case account upper` and `mac-auth delimiter account dash` if you need to use a MAC address formatted like 00-11-AC-01-A0-11 as the username and password.
`mac-auth delimiter calling-station-id {colon | dash | none}`	Select the separator the external server uses for the pairs in MAC addresses in the Calling Station ID RADIUS attribute.
`mode {none | enhanced-open | wep | wpa2 | wpa2-mix | wpa3}`	Sets the security mode for this profile.
`[no] reauth <30..30000>`	Sets the interval (in seconds) between authentication requests. The default is 0.
`[no] server-acct <1..2> activate`	Enables user accounting through an external server. Use the no parameter to disable.
`server-acct <1..2> ip address` *`ipv4_address`* `port <1..65535> secret` *`secret`*	Sets the IPv4 address, port number and shared secret of the external accounting server.
`no server-acct <1..2>`	Clears the specified user accounting setting.
`[no] server-auth <1..2> activate`	Activates server authentication for the account. The no command deactivates authentication.
`server-auth <1..2> ip address` *`ipv4_address`* `port <1..65535> secret` *`secret`*	Sets the IPv4 address, port number and shared secret of the RADIUS server to be used for authentication.
`no server-auth <1..2>`	Clears the server authentication setting.
`[no] transition-mode`	Enables backward compatibility when used with WPA3 or Enhanced Open security mode. WPA3 falls back to WPA2, while Enhanced Open falls back to open (none).

Table 25 Command Summary: Security Profile (continued)

COMMAND	DESCRIPTION
wep <64 | 128> default-key <1..4>	Sets the WEP encryption strength (*64 or 128*) and the default key value (*1 ~ 4*). If you select WEP-64 enter 10 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (for example, 0x11AA22BB33) for each Key used; or enter 5 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey) for each Key used. If you select WEP-128 enter 26 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (for example, 0x00112233445566778899AABBCC) for each Key used; or enter 13 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey12345678) for each Key used. You can save up to four different keys. Enter the default-key (*1 ~ 4*) to save your WEP to one of those four available slots.
wep-auth-type {open | share}	Sets the authentication key type to either *open* or *share*.
wpa-encrypt {tkip | aes | auto}	Sets the WPA/WPA2 encryption cipher type. auto: This automatically chooses the best available cipher based on the cipher in use by the wireless client that is attempting to make a connection. tkip: This is the Temporal Key Integrity Protocol encryption method added later to the WEP encryption protocol to further secure. Not all wireless clients may support this. aes: This is the Advanced Encryption Standard encryption method, a newer more robust algorithm than TKIP Not all wireless clients may support this.
wpa-psk {*wpa_key* | *wpa_key_64*}	Sets the WPA/WPA2 pre-shared key.
[no] wpa2-preauth	Enables pre-authentication to allow wireless clients to switch APs without having to re-authenticate their network connection. The RADIUS server puts a temporary PMK Security Authorization cache on the wireless clients. It contains their session ID and a pre-authorized list of viable APs. Use the no parameter to disable this.
exit	Exits configuration mode for this profile.

9.4.1 Security Profile Example

The following example creates a security profile with the name 'SECURITY01'.

```
Router(config)# wlan-security-profile SECURITY01
Router(config-security-profile)# mode wpa2
Router(config-security-profile)# wpa-encrypt aes
Router(config-security-profile)# wpa-psk 12345678
Router(config-security-profile)# idle 3600
Router(config-security-profile)# reauth 1800
Router(config-security-profile)# group-key 1800
Router(config-security-profile)# exit
Router(config)#
```

9.4.2 SSID and Security Profiles Example

This is an example of creating different WiFi network groups for different types of users, such as guests or employees at your company. You can configure different SSIDs and security modes for each group.

Follow the steps below to set up a wireless network for your company guest. Use the parameters in the table below.

Table 26 SSID and Security Profiles Settings Example

	GUEST
SSID	Guest
Security Mode	WPA2
Pre-Share Key	guest123

1 Create an SSID profile. Set the profile name as Guest. Enter sub-command mode for this profile.

```
Router# configure terminal
Router(config)# wlan-ssid-profile Guest
Router(config-wlan-ssid Guest)#
```

2 Set the SSID as Guest. Exit the sub-command mode.

```
Router(config-wlan-ssid Guest)# ssid Guest
Router(config-wlan-ssid Guest)# exit
Router(config)#
```

3 Create a security profile. Set the profile name as GuestSecurity. Enter sub-command mode for this profile.

```
Router(config)# wlan-security-profile GuestSecurity
Router(config-wlan-security GuestSecurity)#
```

4 Set the security mode to WPA2. Set the pre-shared key to guest123. Exit the sub-command mode.

```
Router(config-wlan-security GuestSecurity)# mode wpa2
Router(config-wlan-security GuestSecurity)# wpa-psk guest123
Router(config-wlan-security GuestSecurity)# exit
Router(config)#
```

5 Enter the Guest SSID profile sub command mode. Apply the GuestSecurity security profile to this SSID.

```
Router(config)# wlan-ssid-profile Guest
Router(config-wlan-ssid Guest)# security GuestSecurity
```

9.5 MAC Filter Profile Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 27 Input Values for General MAC Filter Profile Commands

LABEL	DESCRIPTION
macfilter_profile_name	The MAC filter profile name. You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
description2	Sets the description of the profile. You may use up to 60 alphanumeric characters, underscores (_), or dashes (-). This value is case-sensitive.

The following table describes the commands available for security profile management. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 28 Command Summary: MAC Filter Profile

COMMAND	DESCRIPTION
`show wlan-macfilter-profile {all | macfilter_profile_name}`	Displays the security profile(s). *all*: Displays all profiles for the selected operating mode. *macfilter_profile_name*: Displays the specified profile for the selected operating mode.
`wlan-macfilter-profile rename macfilter_profile_name1 macfilter_profile_name2`	Gives an existing security profile (*macfilter_profile_name1*) a new name (*macfilter_profile_name2*).
`[no] wlan-macfilter-profile macfilter_profile_name`	Enters configuration mode for the specified MAC filter profile. Use the *no* parameter to remove the specified profile.
`filter-action {allow | deny}`	Permits the wireless client with the MAC addresses in this profile to connect to the network through the associated SSID; select deny to block the wireless clients with the specified MAC addresses. The default is set to *deny*.
`[no] sta_mac description description2`	Sets the description of the wireless client with this MAC address. Enter up to 60 characters. Spaces and underscores allowed.
`exit`	Exits configuration mode for this profile.

9.5.1 MAC Filter Profile Example

The following example creates a MAC filter profile with the name 'MACFILTER01'.

```
Router(config)# wlan-macfilter-profile MACFILTER01
Router(config-macfilter-profile)# filter-action deny
Router(config-macfilter-profile)# 01:02:03:04:05:06  description MAC01
Router(config-macfilter-profile)# 01:02:03:04:05:07  description MAC02
Router(config-macfilter-profile)# 01:02:03:04:05:08  description MAC03
Router(config-macfilter-profile)# exit
Router(config)#
```

9.6 ZyMesh Profile Commands

ZyMesh is a ZyXEL-proprietary feature. In a ZyMesh, multiple managed APs form a WDS (Wireless Distribution System) to expand the wireless network and provide services or forward traffic between the Zyxel Device and wireless clients. ZyMesh also allows the Zyxel Device to use CAPWAP to automatically update the configuration settings on the managed APs (in repeater mode) through wireless connections. The managed APs (in repeater mode) are provisioned hop by hop.The managed APs in a WDS or ZyMesh must use the same SSID, channel number and pre-shared key. A manged AP can be either a root AP or repeater in a ZyMesh.

Note: All managed APs should be connected to the Zyxel Device directly to get the configuration file before being deployed to build a ZyMesh/WDS. Ensure you restart the managed AP after you change its operating mode using the `wlan-radio-profile` *`radio_profile_name`* `role` commands.

- Root AP: a managed AP that can transmit and receive data from the Zyxel Device via a wired Ethernet connection.
- Repeater: a managed AP that transmit and/or receive data from the Zyxel Device via a wireless connection through a root AP.

Note: When managed APs are deployed to form a ZyMesh/WDS for the first time, the root AP must be connected to an AP controller (the Zyxel Device).

The maximum number of hops (the repeaters beteen a wireless client and the root AP) you can have in a ZyMesh varies according to how many wireless clients a managed AP can support.

Note: A ZyMesh/WDS link with more hops has lower throughput.

Note: When the wireless connection between the root AP and the repeater is up, in order to prevent bridge loops, the repeater would not be able to transmit data through its Ethernet port(s). The repeater then could only receive power from a PoE device if you use PoE to provide power to the managed AP via an 8-ping Etherent cable.

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 29 Input Values for General ZyMesh Profile Commands

LABEL	DESCRIPTION
`zymesh_profile_name`	The ZyMesh profile name. You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

The following table describes the commands available for ZyMesh profile management. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 30 Command Summary: ZyMesh Profile

COMMAND	DESCRIPTION
`show zymesh ap info`	Displays the number of currently connected/offline ZyMesh APs.
`show zymesh link info {repeater-ap | root-ap}`	Displays the ZyMesh/WDS traffic statistics between the managed APs. `repeater-a`: the managed AP is acting as a repeater in a ZyMesh. `root-ap`: the managed AP is acting as a root AP in a ZyMesh.

Table 30 Command Summary: ZyMesh Profile (continued)

COMMAND	DESCRIPTION
`show zymesh provision-group`	Displays the current ZyMesh Provision Group MAC address in the Zyxel Device.
`show zymesh-profile {all | zymesh_profile_name}`	Displays the ZyMesh profile settings. *all*: Displays all profiles. *zymesh_profile_name*: Displays the specified profile.
`zymesh-profile rename zymesh_profile_name1 zymesh_profile_name2`	Gives an existing radio profile (*zymesh_profile_name1*) a new name (*zymesh_profile_name2*).
`[no] zymesh-profile zymesh_profile_name`	Enters configuration mode for the specified ZyMesh profile. Use the *no* parameter to remove the specified profile.
`psk psk`	Sets a pre-shared key of between 8 and 63 case-sensitive ASCII characters (including spaces and symbols) or 64 hexadecimal characters.The key is used to encrypt the wireless traffic between the APs.
`ssid ssid`	Sets the SSID with which you want the managed AP to connect to a root AP or repeater to build a ZyMesh link. Note: The ZyMesh SSID is hidden in the outgoing beacon frame so a wireless device cannot obtain the SSID through scanning using a site survey tool.
`exit`	Exits configuration mode for this profile.
`zymesh provision-group ac_mac`	Enters the ZyMesh Provision Group MAC address of the primary AP controller in your network to use this Zyxel Device to replace the primary AP controller.

CHAPTER 10
Rogue AP

This chapter shows you how to set up Rogue Access Point (AP) detection and containment.

10.1 Rogue AP Detection Overview

Rogue APs are wireless access points operating in a network's coverage area that are not under the control of the network's administrators, and can potentially open holes in the network security. Attackers can take advantage of a rogue AP's weaker (or non-existent) security to gain illicit access to the network, or set up their own rogue APs in order to capture information from wireless clients.

Conversely, a friendly AP is one that the Zyxel Device network administrator regards as non-threatening. This does not necessarily mean the friendly AP must belong to the network managed by the Zyxel Device; rather, it is any unmanaged AP within range of the Zyxel Device's own wireless network that is allowed to operate without being contained. This can include APs from neighboring companies, for example, or even APs maintained by your company's employees that operate outside of the established network.

10.2 Rogue AP Detection Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 31 Input Values for Rogue AP Detection Commands

LABEL	DESCRIPTION
ap_mac	Specifies the MAC address (in XX:XX:XX:XX:XX:XX format) of the AP to be added to either the rogue AP or friendly AP list. The no command removes the entry.
description2	Sets the description of the AP. You may use 1-60 alphanumeric characters, underscores (_), or dashes (-). This value is case-sensitive.

The following table describes the commands available for rogue AP detection. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 32 Command Summary: Rogue AP Detection

COMMAND	DESCRIPTION
`rogue-ap detection`	Enters sub-command mode for rogue AP detection.
`[no] activate`	Activates rogue AP detection. Use the no parameter to deactivate rogue AP detection.
`rogue-ap` *ap_mac description2*	Sets the device that owns the specified MAC address as a rogue AP. You can also assign a description to this entry on the rogue AP list.
`no rogue-ap` *ap_mac*	Removes the device that owns the specified MAC address from the rogue AP list.

Table 32 Command Summary: Rogue AP Detection (continued)

COMMAND	DESCRIPTION
`friendly-ap ap_mac description2`	Sets the device that owns the specified MAC address as a friendly AP. You can also assign a description to this entry on the friendly AP list.
`no friendly-ap ap_mac`	Removes the device that owns the specified MAC address from the friendly AP list.
`monitoring flush`	Removes all detected APs from the rogue AP list.
`exit`	Exits configuration mode for rogue AP detection.
`show rogue-ap detection monitoring`	Displays a table of detected APs and information about them, such as their MAC addresses, when they were last seen, and their SSIDs, to name a few.
`show rogue-ap detection list {rogue | friendly| all}`	Displays the specified rogue/friendly/all AP list.
`show rogue-ap detection status`	Displays whether rogue AP detection is on or off.
`show rogue-ap detection info`	Displays a summary of the number of detected devices from the following categories: rogue, friendly, ad-hoc, unclassified, and total.

10.2.1 Rogue AP Detection Examples

This example sets the device associated with MAC address 00:13:49:11:11:11 as a rogue AP, and the device associated with MAC address 00:13:49:11:11:22 as a friendly AP. It then removes MAC address from the rogue AP list with the assumption that it was misidentified.

```
Router(config)# rogue-ap detection
Router(config-detection)# rogue-ap 00:13:49:11:11:11 rogue
Router(config-detection)# friendly-ap 00:13:49:11:11:22 friendly
Router(config-detection)# no rogue-ap 00:13:49:11:11:11
Router(config-detection)# exit
```

This example displays the rogue AP detection list.

```
Router(config)# show rogue-ap detection list rogue
no.   mac               description
contain
================================================================================
1    00:13:49:18:15:5A
0
```

This example shows the friendly AP detection list.

```
Router(config)# show rogue-ap detection list friendly
no.   mac                description
================================================================================
1     11:11:11:11:11:11   third floor
2     00:13:49:11:22:33
3     00:13:49:00:00:05
4     00:13:49:00:00:01
5     00:0D:0B:CB:39:33   dept1
```

This example shows the combined rogue and friendly AP detection list.

```
Router(config)# show rogue-ap detection list all
no.   role         mac                description
================================================================================
1     friendly-ap  11:11:11:11:11:11   third floor
2     friendly-ap  00:13:49:11:22:33
3     friendly-ap  00:13:49:00:00:05
4     friendly-ap  00:13:49:00:00:01
5     friendly-ap  00:0D:0B:CB:39:33   dept1
6     rogue-ap     00:13:49:18:15:5A
```

This example shows both the status of rogue AP detection and the summary of detected APs.

```
Router(config)# show rogue-ap detection status
rogue-ap detection status: on

Router(config)# show rogue-ap detection info
rogue ap: 1
friendly ap: 4
adhoc: 4
unclassified ap: 0
total devices: 0
```

10.3 Rogue AP Containment Overview

These commands enable rogue AP containment. You can use them to isolate a device that is flagged as a rogue AP. They are global in that they apply to all managed APs on the network (all APs utilize the same containment list, but only APs set to monitor mode can actively engage in containment of rogue APs). This means if we add a MAC address of a device to the containment list, then every AP on the network will respect it.

Note: Containing a rogue AP means broadcasting unviable login data at it, preventing legitimate wireless clients from connecting to it. This is a kind of Denial of Service attack.

10.4 Rogue AP Containment Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 33 Input Values for Rogue AP Containment Commands

LABEL	DESCRIPTION
ap_mac	Specifies the MAC address (in XX:XX:XX:XX:XX:XX format) of the AP to be contained. The no command removes the entry.

The following table describes the commands available for rogue AP containment. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 34 Command Summary: Rogue AP Containment

COMMAND	DESCRIPTION
`rogue-ap containment`	Enters sub-command mode for rogue AP containment.
`[no] activate`	Activates rogue AP containment. Use the no parameter to deactivate rogue AP containment.
`[no] contain` *ap_mac*	Isolates the device associated with the specified MAC address. Use the no parameter to remove this device from the containment list.
`exit`	Exits configuration mode for rogue AP containment.
`show rogue-ap containment config`	Displays whether rogue AP containment is enabled or not.
`show rogue-ap containment list`	Displays the rogue AP containment list.

10.4.1 Rogue AP Containment Example

This example contains the device associated with MAC address 00:13:49:11:11:12 then displays the containment list for confirmation.

```
Router(config)# rogue-ap containment
Router(config-containment)# activate
Router(config-containment)# contain 00:13:49:11:11:12
Router(config-containment)# exit
Router(config)# show rogue-ap containment list
no.   mac
=================================================================
1     00:13:49:11:11:12
```

CHAPTER 11
Wireless Health

11.1 Wireless Health Overview

This chapter describes the wireless health commands. Wireless health is a way to measure the APs wireless network performance in Zyxel Device networks. Wireless health is defined by the number of times APs have to resend packets before packets are sent out successfully. The more times an AP has to resend the packets, the poorer the state of wireless health the AP is in.

The Zyxel Device improves the wireless network performance by doing the following:

- Scan for the least busy channel bandwidth and select the channel with lease interference (Dynamic Channel Selection).
- Direct clients to APs with a stronger WiFi signal.

11.2 Wireless Health Commands

The following table describes the commands available for the wireless health.

Table 35 Command Summary: Wireless Health

COMMAND	DESCRIPTION
`show wireless-health-action`	Displays the wireless health settings.
`show ap-info top 10 alert {2.4G | 5G | 6G| all}`	Displays the top 10 APs that are in poor states of wireless health for the most times.
`show sta-info top 10 alert {2.4G | 5G | 6G| all}`	Displays how many times the client is in a poor state of wireless health.

The following table describes the commands available for the wireless health. You must use the `configure terminal` commands to enter the configuration mode before you can use the configuration commands. Commands that do not have IPv6 specified in the description are for IPv4.

Table 36 Command Summary: Wireless Health

COMMAND	DESCRIPTION
`wireless-health-action aggressiveness {high | standard | low}`	Sets a level to decide when the Zyxel Device takes actions to improve the APs wireless network performance. Actions the Zyxel Device can take are changing the channel bandwidth from 80MHz to 20MHz, DCS, or directing clients to APs with a stronger WiFi signal. High, standard and low stand for different traffic rate threshold levels. The Zyxel Device will postpone the actions implemented on APs until your network is less busy if the threshold is exceeded. `High`: Sets the level to high if you want the Zyxel Device to postpone the action set when the AP network traffic is more than heavy. `Standard`: Sets the level to standard if you want the Zyxel Device to postpone the action set when the AP network traffic is more than medium. `Low`: Sets the level to low if you want the Zyxel Device to postpone the action set when the AP network traffic is more than low.
`[no] wlan-radio-profile` *`radio profile name`*	Enters configuration mode for the specified radio profile. Use the `no` command to remove the specified profile.
`[no] wireless-health {activate | radio | sta}`	`activate`: Enables Wireless Health. Use the `no` command to disable this feature. `radio:` Configure wireless health settings for the APs in Zyxel Device networks. See Section 11.2.1 on page 103 for more information on radio settings commands. `sta:` Configure wireless health settings for the wireless clients which are connected to the supported APs in Zyxel Device networks. See Section 11.2.1 on page 103 for more information on station settings commands.

11.2.1 Wireless Health Radio and Station Settings

The following table describes the configuration commands available for the wireless health radio and station. You must be in the configuration mode to configure a specified radio profile before you can use the commands. Commands that do not have IPv6 specified in the description are for IPv4.

Table 37 Command Summary: Wireless Health

COMMAND	DESCRIPTION
`wireless-health radio {action | act-lock-time <1...1440> | recovery-threshold <10...1000>| act-threshold <10...1000>| data-collect-interval <0...120>}`	`action:` Configure the actions taken to improve the AP wireless network performance. See Section 11.2.2 on page 104 for more information on radio actions commands. `act-lock-time`: Configure the length of time in seconds the Zyxel Device cannot implement the action you set to the APs in a poor state of wireless health. For example, if you set the time to 30, the Zyxel Device can only have the AP choose a channel that has the least interference (DCS) or change the AP channel bandwidth from 80MHz to 20MHz (adaptive channel width) once even if the Zyxel Device detects that the AP is in a poor state of wireless health more than once within 30 seconds. `recovery-threshold:` Configure the length of time in seconds the AP changes the channel bandwidth from 20 MHz to 80 MHz. Use this command if you set the action to `downgrade_cw`, which will change the AP channel bandwidth from 80MHz to 20 MHz. See Section 11.2.2 on page 104 for more information. `act-threshold:` Configure how many times the AP has to resend the packets will trigger the action you set. For example, if you set the threshold to 10, the Zyxel Device will have the AP choose a channel that has the least interference (DCS) or change the AP channel bandwidth from 80MHz to 20MHz (adaptive channel width) if the AP has to try 10 times before it can send out packets successfully. `data-collect-interval:` Configure the time period over which the AP wireless health state is recorded.
`wireless-health sta {action | act-lock-time <1...1440>| act-threshold <10...1000>| data-collect-interval <0...120>}`	`action:` Configure the actions taken to improve the wireless network performance of clients that are connected to the Zyxel Device supported APs. See Section 11.2.2 on page 104 for more information on radio actions commands. `act-lock-time`: Configure the length of time in seconds the Zyxel Device cannot implement the action you set to the clients in a poor state of wireless health. For example, if you set the time to 30, the Zyxel Device can only steer the wireless clients connected to an AP with a poor signal to an AP with a strong signal once even if the Zyxel Device detects that the AP is in a poor state of wireless health more than once within 30 seconds. `act-threshold:` Configure how many times the AP the clients is connected to has to resend the packets will trigger the action you set. For example, if you set the threshold to 10, the Zyxel Device will steer the wireless clients to an AP with a strong signal if the AP the clients is connected to has to try 10 times before it can send out packets successfully. `data-collect-interval:` Configure the time period over which the client wireless health state is recorded.

11.2.2 Wireless Health Radio and Station Actions

The following table describes the action commands available for the wireless health radio and station. You must be in the configuration mode to configure a specified radio profile before you can use the commands. Commands that do not have IPv6 specified in the description are for IPv4.

Table 38 Command Summary: Wireless Health

COMMAND	DESCRIPTION
`wireless-health radio action {dcs_now | downgrade_cw | none}`	`dcs_now`: Sets the action to dcs_now to have the AP scan and choose a radio channel that has the least interference. `downgrade_cw`: Sets the action to `downgrade_cw` to have the AP change the channel bandwidth from 80 MHz to 20 MHz to reduce the radio interference with other APs. `none`: Sets the action to `none` to have no action taken when the AP is in a poor state of health.
`wireless-health sta action {kick_sta | none}`	`kick_sta`: Sets the action to `kick_sta` to have the Zyxel Device try to steer the wireless clients connected to an AP with a poor signal to an AP with a strong signal every 30 minutes. `none`: Sets the action to `none` to have no action taken when the client is in a poor state of wireless health.

11.2.3 Wireless Health Command Examples

For how the APs wireless network performance is improved, see Section 11.1 on page 101 for more information.

You can set the wireless health action aggressiveness to different levels to decide when the Zyxel Device scans for a better WiFi channel or channel bandwidth to improve the APs wireless network performance.

A low aggressiveness level will temporarily disconnect and scan for a better WiFi channel or channel bandwidth only when there is low level traffic in the network.

A high aggressiveness level will temporarily disconnect and scan for a better WiFi channel or channel bandwidth when there is medium or low level traffic in the network.

Table 39 Wireless Health Action Aggressiveness Comparison

AGGRESSIVENESS LEVEL	TRAFFIC LEVEL	CHANGE CHANNEL BANDWIDTH/DCS
Low	Little traffic	Yes
	Medium traffic	No
	Heavy traffic	No
High	Little traffic	Yes
	Medium traffic	Yes
	Heavy traffic	No

You're streaming videos and you need to make sure you're connected to the Internet all the time. You only want the Zyxel Device to scan for a better WiFi channel or channel bandwidth when there is low level traffic in the network. The example below shows you how to accomplish this task.

```
Router> configure terminal
Router(config)# wireless-health-action aggressiveness
high       low        standard
Router(config)# wireless-health-action aggressiveness low
Router(config)# exit
Router# show wireless-health-action
radio-24g: none
radio-5g: none
station: none
aggressiveness: low
```

CHAPTER 12
Wireless Frame Capture

This chapter shows you how to configure and use wireless frame capture on the Zyxel Device.

12.1 Wireless Frame Capture Overview

Troubleshooting wireless LAN issues has always been a challenge. Wireless sniffer tools like Ethereal can help capture and decode packets of information, which can then be analyzed for debugging. It works well for local data traffic, but if your devices are spaced increasingly farther away then it often becomes correspondingly difficult to attempt remote debugging. Complicated wireless packet collection is arguably an arduous and perplexing process. The wireless frame capture feature in the Zyxel Device can help.

This chapter describes the wireless frame capture commands, which allows a network administrator to capture wireless traffic information and download it to an Ethereal/Tcpdump compatible format packet file for analysis.

12.2 Wireless Frame Capture Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 40 Input Values for Wireless Frame Capture Commands

LABEL	DESCRIPTION
ip_address	The IP address of the Access Point (AP) that you want to monitor. Enter a standard IPv4 IP address (for example, 192.168.1.2).
mon_dir_size	The total combined size (in kbytes) of all files to be captured. The maximum you can set is 50 megabtyes (52428800 bytes.)
file_name	The file name prefix for each captured file. The default prefix is monitor while the default file name is monitor.dump. You can use 1-31 alphanumeric characters, underscores or dashes but the first character cannot be a number. This string is case sensitive.

The following table describes the commands available for wireless frame capture. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 41 Command Summary: Wireless Frame Capture

COMMAND	DESCRIPTION
`frame-capture configure`	Enters sub-command mode for wireless frame capture.
`src-ip {add|del} {`*`ipv4_address`*` | local}`	Sets or removes the IPv4 address of an AP controlled by the Zyxel Device that you want to capture wireless network traffic going through the AP interfaces. You can use this command multiple times to add additional IPs to the list.
`file-prefix `*`file_name`*	Sets the file name prefix for each captured file. Enter up to 31 alphanumeric characters. Spaces and underscores are not allowed.
`files-size `*`mon_dir_size`*	Sets the total combined size (in kbytes) of all files to be captured.
`exit`	Exits configuration mode for wireless frame capture.
`[no] frame-capture activate`	Starts wireless frame capture. Use the no parameter to turn it off.
`show frame-capture status`	Displays whether frame capture is running or not.
`show frame-capture config`	Displays the frame capture configuration.

12.2.1 Wireless Frame Capture Examples

This example configures the wireless frame capture parameters for an AP located at IP address 192.168.1.2.

```
Router(config)# frame-capture configure
Router(frame-capture)# src-ip add 192.168.1.2
Router(frame-capture)# file-prefix monitor
Router(frame-capture)# files-size 1000
Router(frame-capture)# exit
Router(config)#
```

This example shows frame capture status and configuration.

```
Router(config)# show frame-capture status
capture status: off

Router(config)# show frame-capture config
capture source: 192.168.1.2
file prefix: monitor
file size: 1000
```

12.2.2 Remote Packet Capture

Remote packet capture allows you to capture network traffic going through an AP, and output the captured packets to a packet analyzer (also known as network or protocol analyzer) such as Wireshark. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Note: To start, stop, and configure remote packet capture on an AP, log into the Web Configurator and then go to Maintenance > Diagnostics > Packet Capture > Remote Capture.

Table 42 Command Summary: Remote Capture

COMMAND	DESCRIPTION
`show capwap ap all lite2`	Lists all connected APs, and shows whether they support packet capture and remote packet capture.
show remote-capture status	Shows whether remote capture is currently running on the Zyxel Device.

CHAPTER 13
Dynamic Channel Selection

This chapter shows you how to configure and use dynamic channel selection on the Zyxel Device.

13.1 DCS Overview

Dynamic Channel Selection (DCS) is a feature that allows an AP to automatically select the radio channel upon which it broadcasts by passively listening to the area around it and determining what channels are currently being broadcast on by other devices.

When numerous APs broadcast within a given area, they introduce the possibility of heightened radio interference, especially if some or all of them are broadcasting on the same radio channel. This can make accessing the network potentially rather difficult for the stations connected to them. If the interference becomes too great, then the network administrator must open his AP configuration options and manually change the channel to one that no other AP is using (or at least a channel that has a lower level of interference) in order to give the connected stations a minimum degree of channel interference.

13.2 DCS Commands

See Section 9.2 on page 76 for detailed information about how to configure DCS settings in a radio profile.

The following table describes the commands available for dynamic channel selection. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 43 Command Summary: DCS

COMMAND	DESCRIPTION
`dcs now {ap_mac | profile_name}`	Sets the managed AP to scan for and select an available channel immediately.

CHAPTER 14
Auto-Healing

This chapter shows you how to configure auto-healing settings.

14.1 Auto-Healing Overview

Auto-healing allows you to extend the wireless service coverage area of the managed APs when one of the managed APs fails.

14.2 Auto-Healing Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 44 Input Values for Auto-Healing Commands

LABEL	DESCRIPTION
interval	Enters the auto-healing interval time. The range is 5 ~ 30 minutes.

The following table describes the commands available for auto-healing. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 45 Command Summary: Auto-Healing

COMMAND	DESCRIPTION
`[no] auto-healing activate`	Turns on the auto-healing feature. Use the no parameter to turn it off.
`auto-healing healing-interval` *interval*	Sets the interval that specifies how often the managed APs scan their neighborhoods and report the status of neighbor APs to the AP controller (Zyxel Device). An AP is considered “failed” if the AP controller obtains the same scan result that the AP is missing from the neighbor list of other APs three times.
`auto-healing healing-threshold`	Sets a minimum signal strength. A managed AP is added to the neighbor lists only when the signal strength of the AP is stronger than the specified threshold.
`auto-healing power-threshold <-50~-80>`	Sets a power threshold (in dBm). This value is used to calculate the power level (`power-threshold` + `margin`) to which the neighbor APs of the failed AP increase their output power in order to extend their wireless service coverage areas. When the failed AP is working again, its neighbor APs return their output power to the original level.

Table 45 Command Summary: Auto-Healing (continued)

COMMAND	DESCRIPTION
`auto-healing margin`	Enters a number from 0 to 9. This value is used to calculate the power level (`power-threshold` + `margin`) to which the neighbor APs of the failed AP increase their output power in order to extend their wireless service coverage areas.
`auto-healing update`	Sets all manged APs to immediately scan their neighborhoods three times in a row and update their neighbor lists to the AP controller (Zyxel Device).
`show auto-healing config`	Displays the current auto-healing configuration.

14.2.1 Auto-Healing Examples

This example enables auto-healing and sets the power level (in dBm) to which the neighbor APs of the failed AP increase their output power.

```
Router(config)# auto-healing activate
Router(config)# auto-healing power-threshold -70
Router(config)# show auto-healing config
auto-healing activate: yes
auto-healing interval: 10
auto-healing power threshold: -70 dBm
auto-healing healing threshold: -85 dBm
auto-healing margin: 0
Router(config)#
```

CHAPTER 15
LEDs

15.1 LED Suppression Mode

This chapter describes two features that controls the LEDs of the managed APs connected to your Zyxel Device - Locator and Suppression.

The LED Suppression feature allows you to control how the LEDs of an AP behave after it's ready. The default LED suppression setting of the AP is different depending on your AP model.

Note: When the AP is booting or performing firmware upgrade, the LEDs will light regardless of the setting in LED suppression.

15.2 LED Suppression Commands

Use these commands to set how you want the LEDs to behave after the device is ready. You must use the `configure terminal` command before you can use these commands.

Table 46 LED Suppression Commands

COMMAND	DESCRIPTION
`led_suppress` *`ap_mac_address`* `enable`	Sets the LEDs of the specified AP to turn off after it's ready.
`led_suppress` *`ap_mac_address`* `disable`	Sets the LEDs of the specified AP to stay lit after the Zyxel Device is ready.
`show led_suppress` *`ap_mac_address`* `status`	Displays whether LED suppression mode is enabled or disabled on the specified AP.

15.2.1 LED Suppression Commands Example

The following example activates LED suppression mode on the AP with the MAC address 00:a0:c5:01:23:45 and displays the settings.

```
Router(config)# led_suppress 00:a0:c5:01:23:45 enable
Router(config)# show led_suppress 00:a0:c5:01:23:45 status
Suppress Mode Status : Enable
Router(config)#
```

15.3 LED Locator

The LED locator feature identifies the location of the WAC AP among several devices in the network. You can run this feature and set a timer.

15.4 LED Locator Commands

Use these commands to run the LED locator feature. You must use the `configure terminal` command before you can use these commands.

Table 47 LED Locator Commands

COMMAND	DESCRIPTION
`led_locator` *`ap_mac_address`* `on`	Enables the LED locator function on the specified AP. It will show the actual location of the AP among several devices in the network.
`led_locator` *`ap_mac_address`* `off`	Disables the LED locator function on the specified AP.
`led_locator` *`ap_mac_address`* `blink-timer <1..60>`	Sets a time interval between 1 and 60 minutes to stop the locator LED from blinking on the specified AP. Note: You should run this command before enabling the LED locator function.
`show led_locator` *`ap_mac_address`* `status`	Displays whether LED locator function is enabled on the specified AP and the timer setting.

15.4.1 LED Locator Commands Example

The following example turns on the LED locator feature on the AP with the MAC address 00:a0:c5:01:23:45, sets how long the locator LED stays blinking, and also displays the settings.

```
Router(config)# led_locator 00:a0:c5:01:23:45 blink-timer 5
Router(config)# led_locator 00:a0:c5:01:23:45 on
Router(config)# show led_locator 00:a0:c5:01:23:45 status
Locator LED Status : ON
Locator LED Time : 5
Router(config)#
```

CHAPTER 16
Interfaces

16.1 Interface Overview

In general, an interface has the following characteristics.

- An interface is a logical entity through which (layer-3) packets pass.
- An interface is bound to a physical port or another interface.
- Many interfaces can share the same physical port.
- An interface is bound to at most one zone.
- Many interfaces can belong to the same zone.
- Layer-3 virtualization (IP alias, for example) is a kind of interface.

Some characteristics do not apply to some types of interfaces.

16.1.1 Types of Interfaces

You can create several types of interfaces in each Zyxel Device model. The types supported vary by Zyxel Device model.

- Port groups create a hardware connection between physical ports at the layer-2 (data link, MAC address) level.
- Ethernet interfaces are the foundation for defining other interfaces and network policies. RIP and OSPF are also configured in these interfaces.
- VLAN interfaces receive and send tagged frames. The Zyxel Device automatically adds or removes the tags as needed. Each VLAN can only be associated with one Ethernet interface.
- Bridge interfaces create a software connection between Ethernet or VLAN interfaces at the layer-2 (data link, MAC address) level. Unlike port groups, bridge interfaces can take advantage of some security features in the Zyxel Device. You can also assign an IP address and subnet mask to the bridge.
- PPPoE/PPTP interfaces support Point-to-Point Protocols (PPP). ISP accounts are required for PPPoE/PPTP interfaces.
- Cellular interfaces are for 3G WAN connections via a connected 3G device.
- Virtual interfaces (IP alias) provide additional routing information in the Zyxel Device. There are three types: virtual Ethernet interfaces, virtual VLAN interfaces, and virtual bridge interfaces.
- VPN Tunnel Interface (VTI) encrypts or decrypts IPv4 traffic from or to the interface according to the IP routing table.
- Link Aggregation Group (LAG) interfaces combine multiple physical Ethernet interfaces into a single logical interface, thus increasing uplink bandwidth and availability in the event a link goes down.
- Trunks manage load balancing between interfaces.

Port groups, and trunks have a lot of characteristics that are specific to each type of interface. These characteristics are listed in the following tables and discussed in more detail farther on.

Table 48 Characteristics of Ethernet, VLAN, Bridge, PPPoE/PPTP, and Virtual Interface (for some Zyxel Device models)

CHARACTERISTICS	ETHERNET	VLAN	BRIDGE	PPPOE/PPTP	VIRTUAL
Name*	gex	vlanx	brx	pppx	**
IP Address Assignment					
static IP address	Yes	Yes	Yes	Yes	Yes
DHCP client	Yes	Yes	Yes	Yes	No
routing metric	Yes	Yes	Yes	Yes	Yes
Interface Parameters					
bandwidth restrictions	Yes	Yes	Yes	Yes	Yes
packet size (MTU)	Yes	Yes	Yes	Yes	No
data size (MSS)	Yes	Yes	Yes	Yes	No
traffic prioritization	Yes	Yes	Yes	Yes	No
DHCP					
DHCP server	Yes	Yes	Yes	No	No
DHCP relay	Yes	Yes	Yes	No	No
Ping Check	Yes	Yes	Yes	Yes	No

* - The format of interface names is strict. Each name consists of 2-4 letters (interface type), followed by a number (*x*, limited by the maximum number of each type of interface). For example, Ethernet interface names are ge1, ge2, ge3, ...; VLAN interfaces are vlan0, vlan1, vlan2, ...; and so on.

** - The names of virtual interfaces are derived from the interfaces on which they are created. For example, virtual interfaces created on Ethernet interface ge1 are called ge1:1, ge1:2, and so on. Virtual interfaces created on VLAN interface vlan2 are called vlan2:1, vlan2:2, and so on. You cannot specify the number after the colon(:) in the web configurator; it is a sequential number. You can specify the number after the colon if you use the CLI to set up a virtual Interface Parameters

Table 49 Ethernet, VLAN, Bridge, PPP, and Virtual Interface Characteristics (For other Zyxel Device models)

CHARACTERISTICS	ETHERNET	ETHERNET	ETHERNET	VLAN	BRIDGE	PPP	VIRTUAL
Name*	opt	wan1, wan2	lan1, ext-wlan, dmz	vlan*x*	br*x*	ppp*x*	**
Configurable Zone	Yes	No	No	Yes	Yes	No	No
IP Address Assignment							
Static IP address	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DHCP client	Yes	Yes	No	Yes	Yes	Yes	No
Routing metric	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Interface Parameters							
Bandwidth restrictions	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Packet size (MTU)	Yes	Yes	Yes	Yes	Yes	Yes	No
Data size (MSS)	Yes	Yes	Yes	Yes	Yes	Yes	No
DHCP							
DHCP server	Yes	No	Yes	Yes	Yes	No	No

Table 49 Ethernet, VLAN, Bridge, PPP, and Virtual Interface Characteristics (For other Zyxel Device models) (continued)

CHARACTERISTICS	ETHERNET	ETHERNET	ETHERNET	VLAN	BRIDGE	PPP	VIRTUAL
DHCP relay	Yes	No	Yes	Yes	Yes	No	No
Connectivity Check	Yes	Yes	No	Yes	Yes	Yes	No

* - Each name consists of 2-4 letters (interface type), followed by a number (*x*). For most interfaces, x is limited by the maximum number of the type of interface. For VLAN interfaces, x is defined by the number you enter in the VLAN name field. For example, Ethernet interface names are wan1, wan2, opt, lan1, ext-wlan, dmz; VLAN interfaces are vlan0, vlan1, vlan2, ...; and so on.

** - The names of virtual interfaces are derived from the interfaces on which they are created. For example, virtual interfaces created on Ethernet interface wan1 are called wan1:1, wan1:2, and so on. Virtual interfaces created on VLAN interface vlan2 are called vlan2:1, vlan2:2, and so on. You cannot specify the number after the colon(:) in the web configurator; it is a sequential number. You can specify the number after the colon if you use the CLI to set up a virtual interface.

Table 50 Cellular and WLAN Interface Characteristics

CHARACTERISTICS	CELLULAR	
Name*	cellular*x*	
Configurable Zone	Yes**	
IP Address Assignment		
Static IP address	Yes	
DHCP client	Yes	
Routing metric	Yes	
Interface Parameters		
Bandwidth restrictions	Yes	
Packet size (MTU)	Yes	
Data size (MSS)	Yes	
DHCP		
DHCP server	No	
DHCP relay	No	
Connectivity Check	Yes	

* - Each name consists of letters (interface type), followed by a number (*x*). For most interfaces, x is limited by the maximum number of the type of interface. For WLAN interfaces, the first number identifies the slot and the second number identifies the individual interface.

** - Cellular interfaces can be added to the WAN zone or no zone.

16.1.2 Relationships Between Interfaces

In the Zyxel Device, interfaces are usually created on top of other interfaces. Only Ethernet interfaces are created directly on top of the physical ports (or port groups). The relationships between interfaces are explained in the following table.

Table 51 Relationships Between Different Types of Interfaces

INTERFACE	REQUIRED PORT / INTERFACE
Ethernet interface	physical port port group
VLAN interface	Ethernet interface

Table 51 Relationships Between Different Types of Interfaces (continued)

INTERFACE	REQUIRED PORT / INTERFACE
bridge interface	Ethernet interface* VLAN interface*
PPPoE/PPTP interface (For some Zyxel Device models)	Ethernet interface* VLAN interface* bridge interface
PPPoE/PPTP interface (For other Zyxel Device models)	WAN1, WAN2, OPT*
virtual interface (virtual Ethernet interface) (virtual VLAN interface) (virtual bridge interface)	 Ethernet interface* VLAN interface* bridge interface
trunk	Ethernet interface Cellular interface VLAN interface bridge interface PPPoE/PPTP interface

* - You cannot set up a PPPoE/PPTP interface, virtual Ethernet interface, or virtual VLAN interface if the underlying interface is a member of a bridge. You also cannot add an Ethernet interface or VLAN interface to a bridge if the member interface has a virtual interface or PPPoE/PPTP interface on top of it.

16.2 Interface General Commands Summary

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 52 Input Values for General Interface Commands

LABEL	DESCRIPTION
interface_name	The name of the interface. Ethernet interface: For some Zyxel Device models, use ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your Zyxel Device model. For other Zyxel Device models use a name such as wan1, wan2, opt, lan1, ext-wlan, or dmz. virtual interface on top of Ethernet interface: add a colon (:) and the number of the virtual interface. For example: ge*x*:*y*, *x* = 1 - N, *y* = 1 - 4 VLAN interface: vlan*x*, *x* = 0 - 4094 virtual interface on top of VLAN interface: vlan*x*:*y*, *x* = 0 - 4094, *y* = 1 - 4 bridge interface: br*x*, *x* = 0 - N, where N depends on the number of bridge interfaces your Zyxel Device model supports. virtual interface on top of bridge interface: br*x*:*y*, *x* = the number of the bridge interface, *y* = 1 - 4 PPPoE/PPTP interface: ppp*x*, *x* = 0 - N, where N depends on the number of PPPoE/PPTP interfaces your Zyxel Device model supports.
profile_name	The name of the DHCP . You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
domain_name	Fully-qualified domain name. You may up to 254 alphanumeric characters, dashes (-), or periods (.), but the first character cannot be a period.

The following sections introduce commands that are supported by several types of interfaces. See Section 16.6 on page 141 for the unique commands for each type of interface.

16.2.1 Basic Interface Properties and IP Address Commands

This table lists basic properties and IP address commands.

Table 53 `interface` General Commands: Basic Properties and IP Address Assignment

COMMAND	DESCRIPTION
`show interface {ethernet | vlan | bridge | ppp} status`	Displays the connection status of the specified type of interfaces.
`show interface {`*`interface_name`*` | ethernet | vlan | bridge | ppp | virtual ethernet | virtual vlan | virtual bridge | all}`	Displays information about the specified interface, specified type of interfaces, or all interfaces. See Section 16.6.1 on page 144 for all possible cellular status description.
`show ipv6 interface {`*`interface_name`*` | all}`	Displays information about the specified IPv6 interface or all IPv6 interfaces.
`show ipv6 static address` *`interface`*	Displays the static IPv6 addresses configured on the specified IPv6 interface.
`show ipv6 nd ra status` *`config_interface`*	Displays the specified IPv6 interface's IPv6 router advertisement configuration.

Table 53 `interface` General Commands: Basic Properties and IP Address Assignment (continued)

COMMAND	DESCRIPTION
`show interface send statistics interval`	Displays the interval for how often the Zyxel Device refreshes the sent packet statistics for the interfaces.
`show interface summary all`	Displays basic information about the interfaces.
`show interface summary all status`	Displays the connection status of the interfaces.
`[no] interface` *`interface_name`*	Creates the specified interface if necessary and enters sub-command mode. The `no` command deletes the specified interface.
`[no] description` *`description`*	Specifies the description for the specified interface. The `no` command clears the description. *`description`*: You can use alphanumeric and `()+/:=?!*#@$_%-` characters, and it can be up to 60 characters long.
`[no] downstream <0..1048576>`	This is reserved for future use. Specifies the downstream bandwidth for the specified interface. The `no` command sets the downstream bandwidth to 1048576.
`exit`	Leaves the sub-command mode.
`[no] ip address dhcp`	Makes the specified interface a DHCP client; the DHCP server gives the specified interface its IP address, subnet mask, and gateway. The `no` command makes the IP address static IP address for the specified interface. (See the next command to set this IP address.)
`ip address dhcp option-60 <text>`	This command is available for external interfaces only. DHCP Option 60 is used by the Zyxel Device for identification to the DHCP server using the VCI (Vendor Class Identifier) on the DHCP server. The Zyxel Device adds it in the initial DHCP discovery message that a DHCP client broadcasts in search of an IP address. The DHCP server can assign different IP addresses or options to clients with the specific VCI or reject the request from clients without the specific VCI. Type a string using up to 63 of these characters [a-zA-Z0-9!\"#$%&\'()*+,-./:;<=>?@\[\\\]^_`{ }] to identify this Zyxel Device to the DHCP server. For example, Zyxel-TW.
`[no] ip address` *`ip subnet_mask`*	Assigns the specified IP address and subnet mask to the specified interface. The `no` command clears the IP address and the subnet mask.
`[no] ip gateway` *`ip`*	Adds the specified gateway using the specified interface. The `no` command removes the gateway.
`ip gateway` *`ip`* `metric <0..15>`	Sets the priority (relative to every gateway on every interface) for the specified gateway. The lower the number, the higher the priority.
`[no] metric <0..15>`	Sets the tunnel, PPPoE/PPTP, or cellular interface's priority relative to other interfaces. The lower the number, the higher the priority.
`[no] mss <536..1460>`	Specifies the maximum segment size (MSS) the interface is to use. MSS is the largest amount of data, specified in bytes, that the interface can handle in a single, unfragmented piece. The `no` command has the interface use its default MSS.
`[no] mtu <576..1500>`	Specifies the Maximum Transmission Unit, which is the maximum number of bytes in each packet moving through this interface. The Zyxel Device divides larger packets into smaller fragments. The `no` command resets the MTU to 1500.

Table 53 `interface` General Commands: Basic Properties and IP Address Assignment (continued)

COMMAND	DESCRIPTION
`[no] shutdown`	Deactivates the specified interface. The no command activates it.
`traffic-prioritize {tcp-ack|content-filter|dns|ipsec-vpn|ssl-vpn} bandwidth <0..1048576> priority <1..7> [maximize-bandwidth-usage];`	Applies traffic priority when the interface sends TCP-ACK traffic, traffic for querying the content filter, traffic for resolving domain names, or encrypted traffic for an IPSec or SSL VPN tunnel. It also sets how much bandwidth the traffic can use and can turn on maximize bandwidth usage.
`traffic-prioritize {tcp-ack|content-filter|dns|ipsec-vpn|ssl-vpn} deactivate`	Turns off traffic priority settings for when the interface sends the specified type of traffic.
`[no] upstream <0..1048576>`	Specifies the upstream bandwidth for the specified interface. The no command sets the upstream bandwidth to 1048576.
`interface` *`interface_name`* `ipv6`	Creates the specified IPv6 interface if necessary and enters sub-command mode.
`address` *`ipv6_addr_prefix`*	Sets an IPv6 address with prefix for the interface.
`gateway` *`ipv6_addr`* `metric <0..15>`	Sets the specified IPv6 address's metric.
`enable`	Turns on the IPv6 interface.
`nd ra accept`	Sets the IPv6 interface to accept IPv6 neighbor discovery router advertisement messages.
`nd ra advertise`	Sets the IPv6 interface to send IPv6 neighbor discovery router advertisement messages.
`nd ra managed-config-flag`	Turns on the flag in IPv6 router advertisements that tells hosts to use managed (stateful) protocol for address autoconfiguration in addition to any addresses autoconfigured using stateless address autoconfiguration.
`nd ra other-config-flag`	Turns on the other stateful configuration flag in IPv6 router advertisements that tells hosts to use administered (stateful) protocol to obtain autoconfiguration information other than addresses.
`nd ra mtu <1280..1500> | <0>`	Sets the Maximum Transmission Unit (MTU) size of IPv6 packets sent on the interface.
`nd ra hop-limit <0..255>`	Sets the maximum number of hops for router advertisements and all IPv6 packets originating from the interface.
`nd ra router-preference {low | medium | high }`	Sets the Default Router Preference (DRP) extension metric (low, medium, or high) in the interface's IPv6 neighbor discovery router advertisement messages.
`nd ra prefix-advertisement` *`ipv6_addr_prefix`* `[ auto { on | off} ] [ link{ on | off } ] [ preferred-time { <0..4294967294> | infinity }] [valid-time{ <0..4294967294> | infinity }]`	Sets the IPv6 prefix that the Zyxel Device advertises to its clients, whether or not to advertise it, and how long before the prefix's preference and lifetime expire.
`nd ra min-rtr-interval <3..1350>`	Sets the minimum IPv6 router advertisement transmission interval.
`nd ra max-rtr-interval <4..1800>`	Sets the maximum IPv6 router advertisement transmission interval.
`nd ra reachable-time <0..3600000>`	Sets the amount of time a remote IPv6 node is considered reachable after a reachability confirmation event.

Table 53 `interface` General Commands: Basic Properties and IP Address Assignment (continued)

COMMAND	DESCRIPTION
`nd ra default-lifetime <4..9000>`	Sets the router lifetime value is included in all IPv6 router advertisements sent out the interface. The router lifetime value should be equal to or greater than the router advertisement interval.
`nd ra retrans-timer <0..4294967295>`	Sets the IPv6 router advertisement retransmission interval in milliseconds.
`ipv6 address` *`dhcp6_profile dhcp6_suffix_128`*	Has the Zyxel Device obtain an IPv6 prefix from the ISP or a connected uplink router for an internal network, such as the LAN or DMZ. *`dhcp6_profile`*: Specify the DHCPv6 request object to use. *`dhcp6_suffix_128`*: Specify the ending part of the IPv6 address, a slash (/), and the prefix length. The Zyxel Device appends it to the delegated prefix. For example, you got a delegated prefix of 2003:1234:5678/48. You want to configure an IP address of 2003:1234:5678:1111::1/128 for this interface, then enter ::1111:0:0:0:1/128 for the *`dhcp6_suffix_128`*.
`nd ra prefix-advertisement` *`dhcp6_profile dhcp6_suffix_64`*	Configures the network prefix to use a delegated prefix as the beginning part of the network prefix. *`dhcp6_profile`*: Specify the DHCPv6 request object to use for generating the network prefix for the network. *`dhcp6_suffix_64`*: Specify the ending part of the IPv6 network address plus a slash (/) and the prefix length. The Zyxel Device appends it to the selected delegated prefix. The combined address is the network prefix for the network. For example, you got a delegated prefix of 2003:1234:5678/48. You want to divide it into 2003:1234:5678:1111/64 for this interface and 2003:1234:5678:2222/64 for another interface. You can use ::1111/64 and ::2222/64 for the suffix address respectively. But if you do not want to divide the delegated prefix into subnetworks, enter ::0/48 here, which keeps the same prefix length (/48) as the delegated prefix.
`dhcp6 { server | client | relay upper {` *`config_interface | ipv6_addr`* `} }`	Sets the IPv6 interface to be a DHCPv6 server, client or relay. For relay, specify an interface from which to get the DHCPv6 server's address or the IPv6 address of a DHCPv6 server.
`dhcp6 rapid-commit`	This shortens the DHCPv6 message exchange process from four to two steps to help reduce network traffic. Note: Make sure you also enable this option in the DHCPv6 clients to make rapid commit work.
`dhcp6 address-request`	Get this interface's IPv6 address from the DHCPv6 server.
`dhcp6 refresh-time { <600..4294967294> | infinity }`	Sets the number of seconds a DHCPv6 client should wait before refreshing information retrieved from DHCPv6.
`dhcp6 duid {` *`duid`* `| mac }`	Specify the DHCP Unique IDentifier (DUID) of the interface or have it generated from the interface's default MAC address.
`dhcp6-lease-object` *`dhcp6_profile`*	For a DHCPv6 server interface, specify the profile of DHCPv6 lease settings to offer to DHCPv6 clients.
`dhcp6-request-object` *`dhcp6_profile`*	For a DHCPv6 client interface, specify the profile of DHCPv6 request settings that determine what additional information to get from the DHCPv6 server.

Table 53 `interface` General Commands: Basic Properties and IP Address Assignment (continued)

COMMAND	DESCRIPTION
`interface` *`interface_name`* `no ipv6`	Enters the sub-command mode for deleting the specified IPv6 address or removing it's settings.
`enable`	Turns off the IPv6 interface.
`address` *`ipv6_addr_prefix`*	Removes the IPv6 interface's IPv6 prefix setting.
`gateway`	Removes the IPv6 interface's gateway setting.
`nd ra accept`	Sets the IPv6 interface to discard IPv6 neighbor discovery router advertisement messages.
`nd ra advertise`	Has the IPv6 interface not send IPv6 neighbor discovery router advertisement messages.
`nd ra managed-config-flag`	Turns off the flag in IPv6 router advertisements that tells hosts to use managed (stateful) protocol for address autoconfiguration in addition to any addresses autoconfigured using stateless address autoconfiguration.
`nd ra other-config-flag`	Turns off the other stateful configuration flag in IPv6 router advertisements that tells hosts to use administered (stateful) protocol to obtain autoconfiguration information other than addresses.
`nd ra mtu`	Removes the Maximum Transmission Unit (MTU) size setting for IPv6 packets the interface sends.
`nd ra hop-limit`	Removes the maximum number of hops setting for router advertisements and all IPv6 packets originating from the interface.
`nd ra min-rtr-interval`	Removes the minimum IPv6 router advertisement transmission interval setting.
`nd ra max-rtr-interval`	Removes the maximum IPv6 router advertisement transmission interval setting.
`nd ra reachable-time`	Sets the amount of time a remote IPv6 node is considered reachable after a reachability confirmation event to the default.
`nd ra default-lifetime`	Sets the router lifetime value included in all IPv6 router advertisements the interface sends to the default. The router lifetime value should be equal to or greater than the router advertisement interval.
`nd ra retrans-timer`	Sets the IPv6 router advertisement retransmission interval to the default.
`ipv6 address` *`dhcp6_profile dhcp6_suffix_128`*	Removes the specified setting for having the Zyxel Device obtain an IPv6 prefix from the ISP or a connected uplink router for an internal network.
`nd ra prefix-advertisement DHCP6_PROFILE DHCP6_SUFFIX_64`	Removes the specified setting for using a delegated prefix as the beginning part of the network prefix.
`dhcp6`	Sets the interface's DHCPv6 setting back to the default.
`dhcp6 address-request`	Has the Zyxel Device not get this interface's IPv6 address from the DHCPv6 server.
`dhcp6 rapid-commit`	Has the Zyxel Device use the full four-step DHCPv6 message exchange process. Note: Make sure you also disable this option in the DHCPv6 clients.
`dhcp6-lease-object` *`dhcp6_profile`*	Removes the specified profile of DHCPv6 lease settings to offer to DHCPv6 clients.

Table 53 `interface` General Commands: Basic Properties and IP Address Assignment (continued)

COMMAND	DESCRIPTION
`dhcp6-request-object` *dhcp6_profile*	Removes the specified profile of DHCPv6 request settings that determine what additional information to get from the DHCPv6 server.
`interface reset` {*interface_name*|*virtual_interface_name*|`all`}	Resets the interface statistics TxPkts (transmitted packets) and RxPkts (received packets) counts to 0. You can use the `show interface summary all status` command to see the interface statistics.
`interface send statistics interval` <15..3600>	Sets how often the Zyxel Device sends interface statistics to external servers. For example, syslog server and Vantage Report server.
`show interface-name`	Displays all PPP and Ethernet interface system name and user-defined name mappings.
`interface-name` {*ppp_interface* | *ethernet_interface*} *user_defined_name*	Specifies a name for a PPP or an Ethernet interface. It can use alphanumeric characters, hyphens, and underscores, and it can be up to 11 characters long. *ppp_interface* | *ethernet_interface*: This must be the system name of a PPP or an Ethernet interface. Use the `show interface-name` command to see the system name of interfaces. *user_defined_name*: • This name cannot be one of the follows: "ethernet", "ppp", "vlan", "bridge", "virtual", "wlan", "cellular", "aux", "tunnel", "status", "summary", "all" • This name cannot begin with one of the follows either: "ge", "ppp", "vlan", "wlan-", "br", "cellular", "aux", "tunnel".
`interface-rename` *old_user_defined_name* *new_user_defined_name*	Modifies the user-defined name of a PPP or an Ethernet interface.

16.2.1.1 Basic Interface Properties Command Examples

The following commands make Ethernet interface ge1 a DHCP client.

```
Router# configure terminal
Router(config)# interface ge1
Router(config-if)# ip address dhcp
Router(config-if)# exit
```

This example shows how to modify the name of interface ge4 to “VIP”. First you have to check the interface system name (ge4 in this example) on the Zyxel Device. Then change the name and display the result.

```
Router> show interface-name
No.  System Name     User Defined Name
================================================================================
1    ge1             ge1
2    ge2             ge2
3    ge3             ge3
4    ge4             ge4
5    ge5             ge5
Router> configure terminal
Router(config)# interface-name ge4 VIP
Router(config)# show interface-name
No.  System Name     User Defined Name
================================================================================
1    ge1             ge1
2    ge2             ge2
3    ge3             ge3
4    ge4             VIP
5    ge5             ge5
Router(config)#
```

This example shows how to change the user defined name from VIP to Partner. Note that you have to use the “interface-rename” command if you do not know the system name of the interface. To use the “interface-name” command, you have to find out the corresponding system name first (ge4 in this example). This example also shows how to change the user defined name from Partner to Customer using the “interface-name” command.

```
Router(config)# interface-rename VIP Partner
Router(config)# show interface-name
No.  System Name     User Defined Name
================================================================================
1    ge1             ge1
2    ge2             ge2
3    ge3             ge3
4    ge4             Partner
5    ge5             ge5
Router(config)#
Router(config)# interface-name ge4 Customer
Router(config)# show interface-name
No.  System Name     User Defined Name
================================================================================
1    ge1             ge1
2    ge2             ge2
3    ge3             ge3
4    ge4             Customer
5    ge5             ge5
```

This example shows how to restart an interface. You can check all interface names on the Zyxel Device. Then use either the system name or user-defined name of an interface (ge4 or Customer in this example) to restart it.

```
Router> show interface-name
No.  System Name     User Defined Name
================================================================================
1    ge1             ge1
2    ge2             ge2
3    ge3             ge3
4    ge4             Customer
5    ge5             ge5
Router> configure terminal
Router(config)# interface reset ge4
Router(config)# interface reset Customer
Router(config)#
```

16.2.2 IGMP Proxy Commands

Internet Group Management Protocol (IGMP) proxy is used for multicast routing. IGMP proxy enables the Zyxel Device to issue IGMP host messages on behalf of hosts that the Zyxel Device discovered on its IGMP-enabled interfaces. The Zyxel Device acts as a proxy for its hosts.

Enter configuration terminal mode and select an interface

Table 54 `interface` Commands: IGMP Proxy Commands

COMMAND	DESCRIPTION
`[no]igmp activate`	Enables IGMP proxy on this interface. The no command disables IGMP proxy on this interface.
`igmp direction`	Sets the direction for IGMP proxy on this interface. • downstream - enable on the interface which connects to the multicast hosts. • upstream - enable on the interface which connects to a router running IGMP that is closer to the multicast server
`igmp version <1..3>`	Sets the IGMP version to be used on this Zyxel Device interface.

16.2.2.1 IGMP Command Example

The following commands activate IGMP version 2 upstream on the lan1 interface.

```
Router> enable
Router#
Router# configure terminal
Router(config)# interface lan1
Router(config-if-lan1)# igmp
activate
direction
version
Router(config-if-lan1)# igmp activate
Router(config-if-lan1)# igmp direction
downstream
upstream
Router(config-if-lan1)# igmp direction upstream
Router(config-if-lan1)# igmp version
<1..3>
Router(config-if-lan1)# igmp version 2
Router(config-if-lan1)#

Router(config-if-lan1)# exit
```

16.2.3 Proxy ARP Commands

Enable Proxy ARP (RFC 1027) to allow the Zyxel Device to answer external interface ARP requests on behalf of a device on its internal interface. Interfaces supported are:

- Ethernet
- VLAN
- Bridge

Enter configuration terminal mode and select an interface

Table 55 `interface` Commands: Proxy ARP Commands

COMMAND	DESCRIPTION
`[no] ip proxy-arp activate`	Enables proxy ARP on this interface. The `no` command disables proxy ARP on this interface.
`[no] ip proxy-arp {`*`ipv4`* `|` *`ipv4_range`* `|` *`ipv4_cidr`*`}`	Sets the proxy ARP target IP address, IP address range or IP address subnet on this interface. *`ipv4`*: IPv4 address <W.X.Y.Z> *`ipv4_range:`* Range of IPv4 addresses <W.X.Y.Z>-<W.X.Y.Z> *`ipv4_cidr:`* IPv4 subnet in CIDR format, i.e. 192.168.1.0/32 <W.X.Y.Z>/<1..32> The Zyxel Device answers external ARP requests only if they match one of these inputted target IP addresses. For example, if *`ipv4`* is 192.168.1.5, then the Zyxel Device will answer ARP requests coming from the WAN only if it contains 192.168.1.5 as the target IP address. The `no` command disables the proxy ARP target IP address, IP address range or IP address subnet on this interface.

Table 55 `interface` Commands: Proxy ARP Commands (continued)

COMMAND	DESCRIPTION
`show interface` *`interface_name`* `proxy-arp address`	Displays the proxy ARP target IP address, IP address range or IP address subnet on the named interface.
`show interface` *`interface_name`* `proxy-arp status`	Displays if proxy ARP is enabled on the named interface.

16.2.3.1 Proxy ARP Command Example

The following commands activate proxy ARP on the lan1 interface.

```
Router(config)# interface lan1
Router(config-if-lan1)# ip proxy-arp activate
Router(config-if-lan1)# ip proxy-arp 192.168.1.5
Router(config-if-lan1)# exit
Router(config)# show interface lan1 proxy-arp status
Proxy ARP status: yes
Router(config)# show interface lan1 proxy-arp address
No. IP Address
==============================================================================
1   192.168.1.5
Router(config)#
```

16.2.4 DHCP Setting Commands

This table lists DHCP setting commands. DHCP is based on DHCP pools. Create a DHCP pool if you want to assign a static IP address to a MAC address or if you want to specify the starting IP address and pool size of a range of IP addresses that can be assigned to DHCP clients. There are different commands for each configuration. Afterwards, in either case, you have to bind the DHCP pool to the interface.

Table 56 `interface` Commands: DHCP Settings

COMMAND	DESCRIPTION
`show ip dhcp list interface {all |` *`interface name`*`} keyword` *`keyword`*	Shows the interfaces and their static and DHCP-assigned IP addresses. `all`: Uses this to list all interfaces and their static and DHCP-assigned IP addresses. *`interface name`*: Uses this to show the specified interface and to which devices it has assigned static and DHCP IP addresses. `keyword`: You can use up to 63 alphanumeric and ()+/:=?!*#@$_%- characters. This searches the interfaces and their information, such as IP addresses, MAC addresses and so on.
`show ip dhcp static interface {all |` *`interface name`*`}`	Shows the interfaces and their static IP addresses. `all`: Uses this to list all interfaces and their static IP addresses. *`interface name`*: Uses this to show the specified interface and to which devices it has assigned static IP addresses.
`show ip dhcp dhcp-options`	Shows the DHCP extended option settings.
`show ip dhcp pool [`*`profile_name`*`]`	Shows information about the specified DHCP pool or about all DHCP pools.

Table 56 `interface` Commands: DHCP Settings (continued)

COMMAND	DESCRIPTION
`show ip dhcp pool` *`profile_name`* `dhcp-options`	Shows the specified DHCP pool's DHCP extended option settings.
`ip dhcp pool rename` *`profile_name profile_name`*	Renames the specified DHCP pool from the first *`profile_name`* to the second *`profile_name`*.
`ip dhcp static _import_static_file` *`import file name`* `interface` *`interface name`*	Imports a csv file to the specified interface on the Zyxel Device. The IP/MAC binding settings and description to identify these settings in the file will be applied to the Zyxel Device. Configure your csv file in the order of IP address, MAC address and description. Spaces are allowed. Separate each item with a comma, for example, 1.1.1.1,22:22:33:44:55:02,test. Press enter to configure the next group in a new line. Your currently configured IP/MAC binding settings and entries description will be overwritten once you import the file.
`[no] ip dhcp pool` *`profile_name`*	Creates a DHCP pool if necessary and enters sub-command mode. You can use the DHCP pool to create a static entry or to set up a range of IP addresses to assign dynamically. About the sub-command settings: • If you use the `host` command, the Zyxel Device treats this DHCP pool as a static DHCP entry. • If you do not use the `host` command and use the `network` command, the Zyxel Device treats this DHCP pool as a pool of IP addresses. • If you do not use the `host` command or the `network` command, the DHCP pool is not properly configured and cannot be bound to any interface. The `no` command removes the specified DHCP pool.
`show`	Shows information about the specified DHCP pool.
	Use the following commands to create a static DHCP entry. If you do not use the `host` command, the commands that are not in this section have no effect, but you can still set them.
`[no] host` *`ip`*	Specifies the static IP address the Zyxel Device should assign. Use this command, along with `hardware-address`, to create a static DHCP entry. Note: The IP address must be in the same subnet as the interface to which you plan to bind the DHCP pool. When this command is used, the Zyxel Device treats this DHCP pool like a static entry, regardless of the `network` setting. The `no` command clears this field.
`[no] hardware-address` *`mac_address`*	Reserves the DHCP pool for the specified MAC address. Use this command, along with `host`, to create a static DHCP entry. The `no` command clears this field.
`[no] client-identifier` *`mac_address`*	Specifies the MAC address that appears in the DHCP client list. The `no` command clears this field.
`[no] client-name` *`host_name`*	Specifies the host name that appears in the DHCP client list. The `no` command clears this field. *`host_name`*: You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
	Use the following commands to create a pool of IP addresses. These commands have no effect if you use the `host` command. You can still set them, however.

Table 56 `interface` Commands: DHCP Settings (continued)

COMMAND	DESCRIPTION
`dhcp-option <1..254> option_name {boolean <0..1>| uint8 <0..255> | uint16 <0..65535> | uint32 <0..4294967295> | ip ipv4 [ipv4 [ipv4]] | fqdn fqdn [fqdn [fqdn]] | text text | hex hex | vivc enterprise_id hex_s [enterprise_id hex_s] | vivs enterprise_id hex_s [enterprise_id hex_s]`	Adds or edits a DHCP extended option for the specified DHCP pool. *text*: String of up to 250 characters *hex*: String of up to 250 hexadecimal pairs. *vivc*: Vendor-Identifying Vendor Class option. A DHCP client may use this option to unambiguously identify the vendor that manufactured the hardware on which the client is running, the software in use, or an industry consortium to which the vendor belongs. *enterprise_id*: Number <0..4294967295>. *hex_s*: String of up to 120 hexadecimal pairs. *vivs*: Vendor-Identifying Vendor-Specific option. DHCP clients and servers may use this option to exchange vendor-specific information.
`no dhcp-option <1..254>`	Removes the DHCP extended option for the specified DHCP pool.

`network IP/<1..32>`
`network ip mask`
`no network`
	Specifies the IP address and subnet mask of the specified DHCP pool. The subnet mask can be written in w.x.y.z format or in /<1..32> format.
	Note: The DHCP pool must have the same subnet as the interface to which you plan to bind it.
	The `no` command clears these fields.

`[no] default-router ip`	Specifies the default gateway DHCP clients should use. The no command clears this field.
`[no] description description`	Specifies a description for the DHCP pool for identification. The no command removes the description.
`[no] domain-name domain_name`	Specifies the domain name assigned to DHCP clients. The no command clears this field.
`[no] starting-address ip -size <1..65535>`	Sets the IP start address and maximum pool size of the specified DHCP pool. The final pool size is limited by the subnet mask. Note: You must specify the `network number` first, and the start address must be in the same subnet. The `no` command clears the IP start address and maximum pool size.
`[no] first-dns-server {ip | interface_name {1st-dns | 2nd-dns | 3rd-dns} | ZyWALL}`	Sets the first DNS server to the specified IP address, the specified interface's first, second, or third DNS server, or the Zyxel Device itself. The `no` command resets the setting to its default value.
`[no] second-dns-server {ip | interface_name {1st-dns | 2nd-dns | 3rd-dns} | ZyWALL}`	Sets the second DNS server to the specified IP address, the specified interface's first, second, or third DNS server, or the Zyxel Device itself. The `no` command resets the setting to its default value.
`[no] third-dns-server {ip | interface_name {1st-dns | 2nd-dns | 3rd-dns} | ZyWALL}`	Sets the third DNS server to the specified IP address, the specified interface's first, second, or third DNS server, or the Zyxel Device itself. The `no` command resets the setting to its default value.
`[no] first-wins-server ip`	Specifies the first WINS server IP address to assign to the remote users. The no command removes the setting.

Table 56 `interface` Commands: DHCP Settings (continued)

COMMAND	DESCRIPTION
`[no] second-wins-server ip`	Specifies the second WINS server IP address to assign to the remote users. The no command removes the setting.
`[no] lease {<0..365> [<0..23> [<0..59>]] | infinite}`	Sets the lease time to the specified number of days, hours, and minutes or makes the lease time infinite. The no command resets the first DNS server setting to its default value.
`(no) bootp-server <w.x.y.z>`	Sets the PXE (Preboot eXecution Environment) server public IPv4 address. PXE is available for computers on internal interfaces to allow them to boot up using boot software on a PXE server. The Zyxel Device acts as an intermediary between the PXE server and the computers that need boot software. You must enable DHCP Server on the Zyxel Device so that it can receive information from the PXE server.
`(no) bootfile-name <filename>`	Sets the file name and extension of the boot loader software file (a computer program that loads the operating system for the computer) that is on the PXE server. If the wrong filename is typed, then the client computers cannot boot.
`interface interface_name`	Enters sub-command mode.
`[no] ip dhcp-pool profile_name`	Binds the specified interface to the specified DHCP pool. You have to remove any DHCP relays first. The no command removes the binding.
`[no] ip helper-address ip`	Creates the specified DHCP relay. You have to remove the DHCP pool first, if the DHCP pool is bound to the specified interface. The no command removes the specified DHCP relay.
`release dhcp interface-name`	Releases the TCP/IP configuration of the specified interface. The interface must be a DHCP client. This command is available in privilege mode, not configuration mode.
`renew dhcp interface-name`	Renews the TCP/IP configuration of the specified interface. The interface must be a DHCP client. This command is available in privilege mode, not configuration mode.
`show ip dhcp binding [ip]`	Displays information about DHCP bindings for the specified IP address or for all IP addresses.
`clear ip dhcp binding {ip | *}`	Removes the DHCP bindings for the specified IP address or for all IP addresses.

16.2.4.1 DHCP Setting Command Examples

The following example uses these commands to configure DHCP DHCP_TEST.

```
Router# configure terminal
Router(config)# ip dhcp  DHCP_TEST
Router(config-ip-dhcp-)#  network 192.168.1.0 /24
Router(config-ip-dhcp-)#  domain-name zyxel.com
Router(config-ip-dhcp-)#  first-dns-server 10.1.5.1
Router(config-ip-dhcp-)#  second-dns-server ge1 1st-dns
Router(config-ip-dhcp-)#  third-dns-server 10.1.5.2
Router(config-ip-dhcp-)#  default-router 192.168.1.1
Router(config-ip-dhcp-)#  lease 0 1 30
Router(config-ip-dhcp-)#  starting-address 192.168.1.10 -size 30
Router(config-ip-dhcp-)#  hardware-address 00:0F:20:74:B8:18
Router(config-ip-dhcp-)#  client-identifier 00:0F:20:74:B8:18
Router(config-ip-dhcp-)#  client-name TWtester1
Router(config-ip-dhcp-)# exit
Router(config)#  interface ge1
Router(config-if)# ip dhcp- DHCP_TEST
Router(config-if)# exit
Router(config)# show ip dhcp server status
binding interface : ge1
  binding     : DHCP_TEST
```

16.2.4.2 DHCP Extended Option Setting Command Example

The following example configures the DHCP_TEST with a SIP server (code 120) extended DHCP option with one IP address to provide to the SIP clients.

```
Router# configure terminal
Router(config)# ip dhcp  DHCP_TEST
Router(config-ip-dhcp-)#  dhcp-option 120 sip ip 192.168.1.20
Router(config-ip-dhcp-)# exit
```

16.2.4.3 CSV File Example

The following example shows how to configure a csv file.

```
1.1.1.1,22:22:33:44:55:02,test1
2.2.2.2,2C:54:91:88:C9:E3,test2
3.3.3.3,00:1B:44:11:3A:B7,test3
```

16.2.5 Interface Parameter Command Examples

This table shows an example of each interface type's sub-commands. The sub-commands vary for different interface types.

Table 57 Examples for Different Interface Parameters

ETHERNET	VIRTUAL INTERFACE	PPPOE/PPTP
Router(config)# interface wan1 Router(config-if-wan1)# description downstream exit igmp intra-link ip ipv6 mac mss mtu no ping-check shutdown traffic-prioritize type upstream use-defined-mac	Router(config)# interface wan1:1 Router(config-if-vir)# description downstream exit ip no shutdown upstream	Router(config)# interface wan1_ppp Router(config-if-ppp)# account bind connectivity description downstream exit holdoff ipv6 local-address metric mss mtu no ping-check remote-address shutdown traffic-prioritize upstream
CELLULAR	**VLAN**	**BRIDGE**
Router(config)# interface cellular1 Router(config-if-cellular)# account band budget connectivity description device downstream encrypted-pin exit local-address metric mtu network-selection no pin ping-check remote-address shutdown traffic-prioritize upstream	Router(config)# interface vlan1 Router(config-if-vlan)# description downstream exit igmp intra-link ip ipv6 mac mss mtu no ping-check port priority-code shutdown traffic-prioritize type upstream use-defined-mac vlan-id	Router(config)# interface br0 Router(config-if-brg)# description downstream exit igmp intra-link ip ipv6 join mss mtu no ping-check shutdown traffic-prioritize type upstream

Table 57 Examples for Different Interface Parameters (continued)

TUNNEL	VTI	LAG
downstream exit ip ipv6 metric mtu no ping-check shutdown traffic-prioritize tunnel upstream	downstream exit ip metric no ping-check shutdown traffic-prioritize upstream	arp-interval arp-ip-target description downdelay downstream exit igmp intra-link ip ipv6 lacp-rate link-monitoring miimon mode mss mtu no ping-check primary shutdown slave traffic-prioritize type updelay upstream xmit-hash-policy

16.2.6 RIP Commands

This table lists the commands for RIP settings.

Table 58 `interface` Commands: RIP Settings

COMMAND	DESCRIPTION
`router rip`	Enters sub-command mode.
`[no] network` *interface_name*	Enables RIP for the specified interface. The no command disables RIP for the specified interface.
`[no] passive-interface` *interface_name*	Sets the RIP direction of the specified interface to in-only. The no command makes RIP bi-directional in the specified interface.
`[no] outonly-interface` *interface_name*	Sets the RIP direction of the specified interface to out-only. The no command makes RIP bi-directional in the specified interface.
`interface` *interface_name*	Enters sub-command mode.
`[no] ip rip {send | receive} version <1..2>`	Sets the send or receive version to the specified version number. The no command sets the send or received version to the current global setting for RIP. See Chapter 19 on page 176 for more information about routing protocols.
`[no] ip rip v2-broadcast`	Enables RIP-2 packets using subnet broadcasting. The no command uses multi-casting.
`show rip {global | interface {all |` *interface_name*`}}`	Displays RIP settings.

16.2.7 OSPF Commands

This table lists the commands for OSPF settings.

Table 59 `interface` Commands: OSPF Settings

COMMAND	DESCRIPTION
`router ospf`	Enters sub-command mode.
`[no] network interface_name area ip`	Makes the specified interface part of the specified area. The no command removes the specified interface from the specified area, disabling OSPF in this interface.
`[no] passive-interface interface_name`	Sets the OSPF direction of the specified interface to in-only. The no command makes OSPF bi-directional in the specified interface.
`interface interface_name`	Enters sub-command mode.
`[no] ip ospf priority <0..255>`	Sets the priority of the specified interface to the specified value. The no command sets the priority to 1.
`[no] ip ospf cost <1..65535>`	Sets the cost to route packets through the specified interface. The no command sets the cost to 10.
`no ip ospf authentication`	Disables authentication for OSPF in the specified interface.
`ip ospf authentication`	Enables text authentication for OSPF in the specified interface.
`ip ospf authentication message-digest`	Enables MD5 authentication for OSPF in the specified interface.
`ip ospf authentication same-as-area`	To exchange OSPF routing information with peer border routers, you must use the same authentication method that they use. This command makes OSPF authentication in the specified interface follow the settings in the corresponding area.
`[no] ip ospf authentication-key password`	Sets the simple text password for OSPF text authentication in the specified interface. The no command clears the text password. *password*: 1-8 alphanumeric characters or underscores
`ip ospf message-digest-key <1..255> md5 password`	Sets the ID and password for OSPF MD5 authentication in the specified interface. *password*: 1-16 alphanumeric characters or underscores
`no ip ospf message-digest-key`	Clears the ID and password for OSPF MD5 authentication in the specified interface.
`[no] ip ospf hello-interval <1..65535>`	Sets the number of seconds between “hello” messages to peer routers. These messages let peer routers know the Zyxel Device is available. The no command sets the number of seconds to 10. See `ip ospf dead-interval` for more information.
`[no] ip ospf dead-interval <1..65535>`	Sets the number of seconds the Zyxel Device waits for “hello” messages from peer routers before it assumes the peer router is not available and deletes associated routing information. The no command sets the number of seconds to 40. See `ip ospf hello-interval` for more information.
`[no] ip ospf retransmit-interval <1..65535>`	Sets the number of seconds the Zyxel Device waits for an acknowledgment in response to a link state advertisement before it re-sends the advertisement. Link state advertisements (LSA) are used to share the link state and routing information between routers.

16.2.8 Connectivity Check (Ping-check) Commands

Use these commands to have an interface regularly check the connection to the gateway you specified to make sure it is still available. You specify how often the interface checks the connection, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the Zyxel Device stops routing to the gateway. The Zyxel Device resumes routing to the gateway the first time the gateway passes the connectivity check.

This table lists the `ping-check` commands

Table 60 `interface` Commands: Ping Check

COMMAND	DESCRIPTION
`show ping-check [`*`interface_name`*` | status]`	Displays information about ping check settings for the specified interface or for all interfaces. `status`: displays the current connectivity check status for any interfaces upon which it is activated.
`[no] connectivity-check continuous-log activate`	Use this command to have the Zyxel Device log connectivity check result continuously. The no command disables the setting.
`show connectivity-check continuous-log status`	Displays the continuous log setting about connectivity check.
`interface` *`interface_name`*	Enters sub-command mode.
`[no] ping-check activate`	Enables ping check for the specified interface. The no command disables ping check for the specified interface.
`ping-check {`*`FQDN`*` | `*`IPv4`*` | default-gateway} [period <5..3600>] [timeout <1..10>] [fail-tolerance <1..10>] [method {icmp | tcp}] [port <1..65535>] [probe-condition {any | all}]`	Specifies what the Zyxel Device pings for the ping check; you can specify a fully-qualified domain name, IP address, or the default gateway for the interface. `period`: number of seconds between each ping check. `timeout`: number of seconds the Zyxel Device waits for a response. `fail-tolerance`: number of times the Zyxel Devicetimes out before if stops routing through he specified interface. `method`: how the Zyxel Device checks the connection to the gateway. `icmp` pings the gateway you specify to make sure it is still available, while `tcp` performs a TCP handshake with the gateway you specify to make sure it is still available. `port`: the pot number to use for a TCP connectivity check. `probe-condition`: if you ping two IP addresses or domain names, determines whether the ping fails only if both addresses do not respond (`any`) or if at least one does not respond (`all`).

16.2.8.1 Connectivity Check Command Example

The following commands show you how to set the WAN1 interface to use a TCP handshake on port 8080 to check the connection to IP address 1.1.1.2

```
Router# configure terminal
Router(config)# interface wan1
Router(config-if-wan1)# ping-check 1.1.1.2 method tcp port 8080
Router(config-if-wan1)# exit
Router(config)# show ping-check
Interface: wan1
Check Method: tcp
IP Address: 1.1.1.2
Period: 30
Timeout: 5
Fail Tolerance: 5
Activate: yes
Port: 8080
Router(config)#
```

16.3 Ethernet Interface Specific Commands

This section covers commands that are specific to Ethernet interfaces.

The default IPv4 LAN subnet range starts from 192.168.1.0/24. The following list shows the examples of what the IPv4 LAN subnet range will change to if it conflicts with the WAN IPv4 address.

- 192.168.1.0/24 will change to 192.168.10.0/24.
- 192.168.2.0/24 will change to 192.168.11.0/24.
- 192.168.3.0/24 will change to 192.168.12.0/24.
- 192.168.4.0/24 will change to 192.168.13.0/24.

If you upgrade the Zyxel Device firmware version from 4.29 to 5.31, and your settings in the Zyxel Device firmware version 4.29 meets the conditions listed below, the default LAN subnet will change when the IPv4 address the WAN interface gets from the DHCP server conflicts with any IPv4 address in the default LAN subnet:

- The WAN is using a static IPv4 address.
- The WAN is using a dynamically assigned IPv4 address.
- The WAN is using an IPv4 address assigned by the PPPoE server.

If the Zyxel Device is using firmware version 5.31, when the WAN IPv4 address conflicts with any IPv4 address in the default LAN subnet, the Zyxel Device will only change the default LAN subnet if it is in default settings.

When you configure the WAN or the LAN IPv4 networks, please note that they must not conflict with each other. The Zyxel Device will not automatically change the LAN IPv4 subnet if the WAN IPv4 address conflicts with the LAN IPv4 networks you configure.

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 61 Input Values for Ethernet Interface Commands

LABEL	DESCRIPTION
interface_name	The name of the Ethernet interface. This depends on the Zyxel Device model. For some Zyxel Device models, use ge*x*, *x* = 1~N, where N equals the highest numbered Ethernet interface for your Zyxel Device model. For other Zyxel Device models use a name such as wan1, wan2, opt, lan1, ext-wlan, or dmz.

16.3.1 MAC Address Setting Commands

This table lists the commands you can use to set the MAC address of an interface. On some Zyxel Device models, these commands only apply to a WAN or OPT interface.

Table 62 `interface` Commands: MAC Setting

COMMAND	DESCRIPTION
`interface` *interface_name*	Enters sub-command mode.
`no mac`	Has the interface use its default MAC address.
`mac` *mac*	Specifies the MAC address the interface is to use.
`type {internal | external | general}`	Sets which type of network you will connect this interface. The Zyxel Device automatically adds default route and SNAT settings for traffic it routes from internal interfaces to external interfaces; for example LAN to WAN traffic. `internal`: Set this to connect to a local network. Other corresponding configuration options: DHCP server and DHCP relay. The Zyxel Device automatically adds default SNAT settings for traffic flowing from this interface to an external interface. `external`: Set this to connect to an external network (like the Internet). The Zyxel Device automatically adds this interface to the default WAN trunk. `general`: Set this if you want to manually configure a policy route to add routing and SNAT settings for the interface.
`no use-defined-mac`	Has the interface use its default MAC address.
`use-defined-mac`	Has the interface use a MAC address that you specify.

16.3.2 Port Grouping Commands

This section covers commands that are specific to port grouping.

Note: In CLI, representative interfaces are also called representative ports.

Table 63 Basic Interface Setting Commands

COMMAND	DESCRIPTION
`show port-grouping`	Displays which physical ports are assigned to each representative interface.
`port status Port<1..`*x*`>`	Enters a sub-command mode to configure the specified port's settings.

Table 63 Basic Interface Setting Commands (continued)

COMMAND	DESCRIPTION
`[no] duplex <full | half>`	Sets the port's duplex mode. The no command returns the default setting.
`exit`	Leaves the sub-command mode.
`[no] negotiation auto`	Sets the port to use auto-negotiation to determine the port speed and duplex. The no command turns off auto-negotiation.
`[no] speed <100,10>`	Sets the Ethernet port's connection speed in Mbps. The no command returns the default setting.
`show port setting`	Displays the Ethernet port negotiation, duplex, and speed settings.
`show port type physical`	Displays the cable type that is used on the port.
`show port status`	Displays statistics for the Ethernet ports.
`show port statistic portx interval <5..3600>`	Displays the specified port's statistics and updates them according to the interval you set.

16.3.2.1 Port Grouping Command Examples

The following commands add physical port 7 to representative interface lan2.

```
Router# configure terminal
Router(config)# show port-grouping
No. Representative Name  Port1 Port2 Port3 Port4 Port5 Port6 Port7
================================================================================
1   wan1                 yes   no    no    no    no    no    no
2   wan2                 no    yes   no    no    no    no    no
3   opt                  no    no    yes   no    no    no    no
4   lan1                 no    no    no    yes   yes   yes   no
5   lan2                 no    no    no    no    no    no    no
6   reserved             no    no    no    no    no    no    no
7   dmz                  no    no    no    no    no    no    yes
Router(config)#
Router(config)# port-grouping lan2
Router(config-port-grouping)# port 7
Router(config-port-grouping)# exit
Router(config)# show port-grouping
No. Representative Name  Port1 Port2 Port3 Port4 Port5 Port6 Port7
================================================================================
1   wan1                 yes   no    no    no    no    no    no
2   wan2                 no    yes   no    no    no    no    no
3   opt                  no    no    yes   no    no    no    no
4   lan1                 no    no    no    yes   yes   yes   no
5   lan2                 no    no    no    no    no    no    yes
6   reserved             no    no    no    no    no    no    no
7   dmz                  no    no    no    no    no    no    no
Router(config)#
```

The following commands set port 1 to use auto-negotiation auto and port 2 to use a 10 Mbps connection speed and half duplex.

```
Router(config)# port status Port1
Router(config-port-status)# negotiation auto
Router(config-port-status)# exit
Router(config)# port status Port2
Router(config-port-status)# duplex half
Router(config-port-status)# speed 10
Router(config-port-status)# exit
Router(config)# exit
```

16.4 Virtual Interface Specific Commands

Virtual interfaces use many of the general interface commands discussed at the beginning of Section 16.2 on page 118. There are no additional commands for virtual interfaces.

16.4.1 Virtual Interface Command Examples

The following commands set up a virtual interface on top of Ethernet interface ge1. The virtual interface is named ge1:1 with the following parameters: IP 1.2.3.4, subnet 255.255.255.0, gateway 4.6.7.8, upstream bandwidth 345, downstream bandwidth 123, and description “I am vir interface”.

```
Router# configure terminal
Router(config)# interface ge1:1
Router(config-if-vir)# ip address 1.2.3.4 255.255.255.0
Router(config-if-vir)# ip gateway 4.6.7.8
Router(config-if-vir)# upstream 345
Router(config-if-vir)# downstream 123
Router(config-if-vir)# description I am vir interface
Router(config-if-vir)# exit
```

16.5 PPPoE/PPTP Specific Commands

This section covers commands that are specific to PPPoE/PPTP interfaces. PPPoE/PPTP interfaces also use many of the general interface commands discussed at the beginning of Section 16.2 on page 118.

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 64 Input Values for PPPoE/PPTP Interface Commands

LABEL	DESCRIPTION
interface_name	PPPoE/PPTP interface: ppp*x*, *x* = 0 - N, where N depends on the number of PPPoE/PPTP interfaces your Zyxel Device model supports.
profile_name	The name of the ISP account. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

This table lists the PPPoE/PPTP interface commands.

Table 65 `interface` Commands: PPPoE/PPTP Interfaces

COMMAND	DESCRIPTION
`interface dial` *`interface_name`*	Connects the specified PPPoE/PPTP interface.
`interface disconnect` *`interface_name`*	Disconnects the specified PPPoE/PPTP interface.
`interface` *`interface_name`*	Creates the specified interface if necessary and enters sub-command mode.
`[no] account` *`profile_name`*	Specifies the ISP account for the specified PPPoE/PPTP interface. The no command clears the ISP account field.
`[no] bind` *`interface_name`*	Specifies the base interface for the PPPoE/PPTP interface. The no command removes the base interface.
`[no] connectivity {nail-up | dial-on-demand}`	Specifies whether the specified PPPoE/PPTP interface is always connected (nail-up) or connected only when used (dial-on-demand). The no command sets it to dial-on-demand.
`[no] local-address` *`ip`*	Specifies a static IP address for the specified PPPoE/PPTP interface. The no command makes the PPPoE/PPTP interface a DHCP client; the other computer assigns the IP address.
`[no] remote-address` *`ip`*	Specifies the IP address of the PPPoE/PPTP server. If the PPPoE/PPTP server is not available at this IP address, no connection is made. The no command lets the Zyxel Device get the IP address of the PPPoE/PPTP server automatically when it establishes the connection.
`[no] mss <536..1452>`	Specifies the maximum segment size (MSS) the interface can use. MSS is the largest amount of data, specified in bytes, that the interface can handle in a single, unfragmented piece. The no command has the Zyxel Device use its default MSS setting.
`mtu <576..1492>`	Sets the Maximum Transmission Unit in bytes.
`[no] ipv6 enable`	Turns on the IPv6 interface. The no command turns it off.
`[no] ipv6 nd ra accept`	Sets the IPv6 interface to accept IPv6 neighbor discovery router advertisement messages. The no command sets the IPv6 interface to discard IPv6 neighbor discovery router advertisement messages.
`[no] ipv6 metric <0..15>`	Sets the interface's metric for IPv6 traffic. The no command clears it.
`[no] ipv6 address` *`dhcp6_profile dhcp6_suffix_128`*	Has the Zyxel Device obtain an IPv6 prefix from the ISP or a connected uplink router for an internal network, such as the LAN or DMZ. The no command removes the specified setting for using a delegated prefix as the beginning part of the network prefix. *`dhcp6_profile`*: Specify the DHCPv6 request object to use. *`dhcp6_suffix_128`*: Specify the ending part of the IPv6 address, a slash (/), and the prefix length. The Zyxel Device appends it to the delegated prefix. For example, you got a delegated prefix of 2003:1234:5678/48. You want to configure an IP address of 2003:1234:5678:1111::1/128 for this interface, then enter ::1111:0:0:0:1/128 for the *`dhcp6_suffix_128.`*
`ipv6 dhcp6 [client]`	Sets the IPv6 interface to be a DHCPv6 client.
`[no] ipv6 dhcp6 rapid-commit`	Shortens the DHCPv6 message exchange process from four to two steps to help reduce network traffic. The no command sets the full four-step DHCPv6 message exchange process.
`[no] ipv6 dhcp6 address-request`	Get this interface's IPv6 address from the DHCPv6 server. The no command has the Zyxel Device not get this interface's IPv6 address from the DHCPv6 server.

Table 65 `interface` Commands: PPPoE/PPTP Interfaces (continued)

COMMAND	DESCRIPTION
`ipv6 dhcp6 duid { duid | mac }`	Specify the DHCP Unique IDentifier (DUID) of the interface or have it generated from the interface's default MAC address.
`[no] ipv6 dhcp6-request-object dhcp6_profile`	For a DHCPv6 client interface, specify the profile of DHCPv6 request settings that determine what additional information to get from the DHCPv6 server. The no command removes the DHCPv6 request settings profile.
`show interface ppp system-default`	Displays system default PPP interfaces (non-deletable) that come with the Zyxel Device.
`show interface ppp user-define`	Displays all PPP interfaces that were manually configured on the Zyxel Device.

16.5.1 PPPoE/PPTP Interface Command Examples

The following commands show you how to configure PPPoE/PPTP interface ppp0 with the following characteristics: base interface ge1, ISP account Hinet, local address 1.1.1.1, remote address 2.2.2.2, MTU 1200, upstream bandwidth 345, downstream bandwidth 123, description "I am ppp0", and dialed only when used.

```
Router# configure terminal
Router(config)# interface ppp0
Router(config-if-ppp)# account Hinet
Router(config-if-ppp)# bind ge1
Router(config-if-ppp)# local-address 1.1.1.1
Router(config-if-ppp)# remote-address 2.2.2.2
Router(config-if-ppp)# mtu 1200
Router(config-if-ppp)# upstream 345
Router(config-if-ppp)# downstream 123
Router(config-if-ppp)# connectivity dial-on-demand
Router(config-if-ppp)# description I am ppp0
Router(config-if-ppp)# exit
```

The following commands show you how to connect and disconnect ppp0.

```
Router# interface dial ppp0
Router# interface disconnect ppp0
```

16.6 Cellular Interface Specific Commands

Use a 3G (Third Generation) cellular device with the Zyxel Device for wireless broadband Internet access.

Use these commands to add, edit, dial, disconnect, or delete cellular interfaces. When you add a new cellular interface, make sure you enter the account. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 66 `Interface` Cellular Commands

COMMAND	DESCRIPTION
`[no] interface` *`interface_name`*	Creates the specified interface if necessary and enters sub-command mode. The `no` command deletes the specified interface.
`account` *`profile_name`*	Specifies the ISP account for the specified cellular interface.
`[no] band {auto|wcdma|gsm|lte}`	Sets (or clears) the cellular band that the cellular interface uses. `auto` has the Zyxel Device always use the fastest network that is in range. `gsm` has this interface only use a 2.5G or 2.75G network (respectively). If you only have a GSM network available to you, you may want to use this so the Zyxel Device does not spend time looking for a WCDMA network. `wcdma` has this interface only use a 3G or 3.5G network (respectively). You may want to use this if you want to make sure the interface does not use the GSM network. `lte` has this interface only use a 4G LTE network. This option only appears when a USG dongle for 4G technology is inserted.
`[no] network-selection {auto|home}`	Home network is the network to which you are originally subscribed. `Home` has the 3G device connect only to the home network. If the home network is down, the Zyxel Device's 3G Internet connection is also unavailable. `Auto` is the default setting and allows the 3G device to connect to a network to which you are not subscribed when necessary, for example when the home network is down or another 3G base station's signal is stronger. This is recommended if you need continuous Internet connectivity. If you select this, you may be charged using the rate of a different network.
`[no] budget active`	Sets a monthly limit for the user account of the installed 3G card. You can set a limit on the total traffic and/or call time. The Zyxel Device takes the actions you specified when a limit is exceeded during the month. Use the no command to disable budget control.
`[no] budget time active <1..672>`	Sets the amount of time (in hours) that the 3G connection can be used within one month. If you change the value, the Zyxel Device resets the statistics. Use the no command to disable time budget control.

Table 66 `Interface` Cellular Commands (continued)

COMMAND	DESCRIPTION
`[no] budget data active {download-upload|download|upload} <1..100000>`	Sets how much downstream and/or upstream data (in Mega bytes) can be transmitted via the 3G connection within one month. `download`: set a limit on the downstream traffic (from the ISP to the Zyxel Device). `upload`: set a limit on the upstream traffic (from the Zyxel Device to the ISP). `download-upload`: set a limit on the total traffic in both directions. If you change the value, the Zyxel Device resets the statistics. Use the `no` command to disable data budget control.
`budget reset-day <0..31>`	Sets the date on which the Zyxel Device resets the budget every month. If the date you selected is not available in a month, such as 30th or 31st, the Zyxel Device resets the budget on the last day of the month.
`budget reset-counters`	Resets the time and data budgets immediately. The count starts over with the 3G connection's full configured monthly time and data budgets. This does not affect the normal monthly budget restart.
`budget {log|log-alert}[recursive <1..65535>]`	Sets the Zyxel Device to create a log (log) or an alert log (log-alert) when the time or data limit is exceeded. You can also specify how often (from 1 to 65535 minutes) to generate a log or an alert.
`no budget log`	Sets the Zyxel Device to not create a log when the time or data limit is exceeded.
`budget new-connection {allow|disallow}`	Sets to permit (`allow`) or drop/block (`disallow`) new 3G connections when the time or data limit is exceeded.
`budget current-connection {keep|drop}`	Sets to maintain the existing 3G connection (keep) or disconnect it (drop) when the time or data limit is exceeded. You cannot set budget new-connection to `allow` and budget current-connection to `drop` at the same time. If you set budget new-connection to disallow and budget current-connection to keep, the Zyxel Device allows you to transmit data using the current connection, but you cannot build a new connection if the existing connection is disconnected.
`budget percentage {ptime|pdata} <0..99>`	Sets a percentage (0~99) of time budget (`ptime`) or data (`pdata`) limit. When the specified limit is exceeded, the Zyxel Device takes the action configured using the `budget {log-percentage|log-percentage-alert} command`.
`budget {log-percentage|log-percentage-alert} [recursive <1..65535>]`	Sets to have the Zyxel Device create a log (`log-percentage`) or an alert log (`log-percentage-alert`) when the set percentage of time budget or data limit is exceeded. You can configure the percentage using the `budget percentage` command. You can also set how often (from 1 to 65535 minutes) to send the log or alert.
`no budget log-percentage`	Sets the Zyxel Device to not create a log when the set percentage of time budget or data limit is exceeded. You can configure the percentage using the `budget percentage` command.

Table 66 `Interface` Cellular Commands (continued)

COMMAND	DESCRIPTION
`connectivity {nail-up | dial-on-demand}`	Sets the connection to be always on or only when there is traffic.
`[no] local-address <ip>`	Sets (or clears) the cellular interface's local (own) IP address.
`mtu <576..1492>`	Sets the Maximum Transmission Unit in bytes.
`[no] pin <pin code>`	Sets (or clears) the PIN code for the cellular device's 3G card. Use 1-4 alphanumeric characters, underscores(_), or dashes (-).
`[no] remote-address <ip>`	Sets (or clears) the IP address of the cellular interface's peer (like a gateway or PPPoE server).
`interface cellular budget-auto-save <5..1440>`	Sets how often (in minutes) the Zyxel Device saves time and data usage records for a connection using the 3G card.
`show interface cellular [corresponding-slot|device-status|support-device]`	Shows the status of the specified cellular interface.
`show interface cellular corresponding-slot`	Shows which cellular interface is on which slot and whether which cellular interface has been configured.
`show interface cellular device-status`	Displays the installed SIM card and 3G card status.
`show interface cellular support-device`	Displays all 3G card models the Zyxel Device can support.
`show interface cellular budget-auto-save`	Displays how often (in minutes) the Zyxel Device records time and data usage of your 3G budgets.
`show interface cellular status`	Displays the traffic statistics and connection status for your cellular interfaces. See Section 16.6.1 on page 144 for all possible cellular status descriptions.
`show interface interface_name [budget]`	Displays the budget control settings for the specified cellular interface.
`show interface interface_name device status`	Displays the 3G card and SIM card information for the specified cellular interface.
`show interface interface_name device profile`	Displays the 3G connection profile settings of the specified cellular interface.

16.6.1 Cellular Status

The following table describes the different kinds of cellular connection status on the Zyxel Device.

Table 67 Cellular Status

STATUS	DESCRIPTION
No device	no 3G device is connected to the Zyxel Device.
No service	no 3G network is available in the area; you cannot connect to the Internet.
Limited service	returned by the service provider in cases where the SIM card is expired, the user failed to pay for the service and so on; you cannot connect to the Internet.
Device detected	displays when you connect a 3G device.
Device error	a 3G device is connected but there is an error.
Probe device fail	the Zyxel Device's test of the 3G device failed.
Probe device ok	the Zyxel Device's test of the 3G device failed.
Init device fail	the Zyxel Device was not able to initialize the 3G device.

Table 67 Cellular Status

STATUS	DESCRIPTION
Init device ok	the Zyxel Device initialized the 3G card.
Check lock fail	the Zyxel Device's check of whether or not the 3G device is locked failed.
Device locked	the 3G device is locked.
SIM error	there is a SIM card error on the 3G device.
SIM locked-PUK	the PUK is locked on the 3G device's SIM card.
SIM locked-PIN	the PIN is locked on the 3G device's SIM card.
Unlock PUK fail	Your attempt to unlock a WCDMA 3G device's PUK failed because you entered an incorrect PUK.
Unlock PIN fail	Your attempt to unlock a WCDMA 3G device's PIN failed because you entered an incorrect PIN.
Unlock device fail	Your attempt to unlock a CDMA2000 3G device failed because you entered an incorrect device code.
Device unlocked	You entered the correct device code and unlocked a CDMA2000 3G device.
Get dev-info fail	The Zyxel Device cannot get cellular device information.
Get dev-info ok	The Zyxel Device succeeded in retrieving 3G device information.
Searching network	The 3G device is searching for a network.
Get signal fail	The 3G device cannot get a signal from a network.
Network found	The 3G device found a network.
Apply config	The Zyxel Device is applying your configuration to the 3G device.
Device unready	The 3G interface is disabled.
Active	The 3G interface is enabled.
Incorrect device	The connected 3G device is not compatible with the Zyxel Device.
Correct device	The Zyxel Device detected a compatible 3G device.
Set band fail	Applying your band selection was not successful.
Set band ok	The Zyxel Device successfully applied your band selection.
Set profile fail	Applying your ISP settings was not successful.
Set profile ok	The Zyxel Device successfully applied your ISP settings.
PPP fail	The Zyxel Device failed to create a PPP connection for the cellular interface.
Need auth-password	You need to enter the password for the 3G card in the cellular edit screen.
Device ready	The Zyxel Device successfully applied all of your configuration and you can use the 3G connection.

16.6.2 Cellular Interface Command Examples

This example shows the configuration of a cellular interface named cellular2 for use with a Sierra Wireless AC850 3G card. It uses only a 3G (or 3.5G) connection, PIN code 1234, an MTU of 1200 bytes, a description of "This is cellular2" and sets the connection to be nailed-up.

```
Router(config)# interface cellular2
Router(config-if-cellular)# device AC850
Router(config-if-cellular)# band wcdma
Router(config-if-cellular)# pin 1234
Router(config-if-cellular)# connectivity nail-up
Router(config-if-cellular)# description This is cellular2
Router(config-if-cellular)# mtu 1200
Router(config-if-cellular)# exit
```

This second example shows specifying a new PIN code of 4567.

```
Router(config)# interface cellular2
Router(config-if-cellular)# pin 4567
Router(config-if-cellular)# exit
```

This example shows the 3G and SIM card information for interface cellular2 on the Zyxel Device.

```
Router(config)# show interface cellular2 device status
interface name: cellular2
extension slot: USB 1
service provider: Chunghwa Telecom
cellular system: WCDMA
signal strength: -95 dBm
signal quality: Poor
device type: WCDMA
device manufacturer: Huawei
device model: E220/E270/E800A
device firmware: 076.11.07.106
device IMEI/ESN: 351827019784694
SIM card IMSI: 466923100565274
```

This example shows the 3G connection profile settings for interface cellular2 on the Zyxel Device. You have to dial *99***1# to use profile 1, but authentication is not required. Dial *99***2# to use profile 2 and authentication is required.

```
Router(config)# show interface cellular2 device profile
profile: 1
apn: internet
dial-string: *99***1#
authentication: none
user: n/a
password: n/a
profile: 2
apn: internet
dial-string: *99***2#
authentication: chap
user:
password: ***
---------------------SNIP!-----------------------------------------------
```

16.7 Tunnel Interface Specific Commands

The Zyxel Device uses tunnel interfaces in Generic Routing Encapsulation (GRE), IPv6 in IPv4, and 6to4 tunnels. This section covers commands specific to tunnel interfaces. Tunnel interfaces also use many of the general interface commands discussed at the beginning of Section 16.2 on page 118.

Use these commands to add, edit, activate, deactivate, or delete tunnel interfaces. You must use the `configure terminal` command to enter the configuration mode before you can use these commands. GRE mode tunnels support ping check. See Section 16.2.8 on page 135 for more on ping check.

Table 68 `interface` Tunnel Commands

COMMAND	DESCRIPTION
`[no] interface tunnel_iface`	Creates the specified interface if necessary and enters sub-command mode. The `no` command deletes the specified interface. *tunnel_iface*: Name of tunnel interface. tunnel([0-3]).
`[no] shutdown`	Deactivates the specified interface. The `no` command activates it.
`tunnel source [ipv4|tunnel_bind_interface|_any ]`	Configures the outer source IP address of the tunneled packets. Specify an IPv4 address or use the IP address of an interface. _any: Have automatically select the outer source IP. Not available for ipv6ip mode tunnels.
`tunnel destination ipv4`	Configures the outer destination IP address of the tunneled IPv4 packets.
`ip address ipv4 ipv4`	Sets the inner source IP of packets sent through the tunnel interface.
`tunnel mode ip gre`	Sets this interface to use GRE tunnel mode.
`[no] mtu <576..1480>`	Specifies the Maximum Transmission Unit, which is the maximum number of bytes in each packet moving through this interface. The Zyxel Device divides larger packets into smaller fragments. The `no` command resets the MTU to 1480.

Table 68 `interface` Tunnel Commands (continued)

COMMAND	DESCRIPTION
`[no] downstream <0..1048576>`	Specifies the downstream bandwidth for the specified interface. The `no` command sets the downstream bandwidth to 1048576.
`tunnel mode [ipv6ip [manual | 6to4]]]`	Sets the interface to be an IPv6 over IPv4 tunnel. `manual`: Use for a point-to-point manual tunnel for IPv6 transition. You must also configure a policy route for the tunnel. 6to4: Use for a 6to4/6RD automatic tunnel.
`ipv6 address` *`ipv6_addr_prefix`*	Sets an IPv6 address with prefix for the interface.
`ipv6 6to4 [prefix` *`ipv6_addr_prefix`* `| destination-prefix` *`ipv4_cidr`* `| relay` *`ipv4`*`]`	For a 6to4 tunnel, sets the IPv6 address with prefix, remote gateway prefix, or relay router IPv4 address.
`traffic-prioritize {tcp-ack|content-filter|dns} bandwidth <0..1048576> priority <1..7> [maximize-bandwidth-usage];`	Applies traffic priority when the interface sends TCP-ACK traffic, traffic for querying the content filter, or traffic for resolving domain names. It also sets how much bandwidth the traffic can use and can turn on maximize bandwidth usage.
`traffic-prioritize {tcp-ack|content-filter|dns} priority-code <0..7> deactivate`	Turns off traffic priority settings for when the interface sends the specified type of traffic.
`exit`	Leaves the sub-command mode.
`show interface` *`tunnel_iface`*	Displays the specified tunnel's settings.
`show interface tunnel status`	Displays the status of the tunnel interfaces.

16.7.1 Tunnel Interface Command Examples

This example creates a tunnel interface called tunnel0 that uses wan1 as the source, 168.168.168.168 as the destination, and 10.0.0.100 and 255.255.0.0 as the inner source IP.

```
Router> configure terminal
Router(config)# interface tunnel0
Router(config-if-tunnel)# tunnel source wan1
Router(config-if-tunnel)# tunnel destination 168.168.168.168
Router(config-if-tunnel)# ip address 10.0.0.100 255.255.0.0
Router(config-if-tunnel)# exit

Router(config)# show interface tunnel
tunnel interface: 1
  interface name: tunnel0
  local address: ge2
  local address type: bind
  remote address: 168.168.168.168
  mode: gre
  IP address: 10.0.0.100
  netmask: 255.255.0.0
  status: Inactive
  active: no
```

16.8 USB Storage Specific Commands

The Zyxel Device can use a connected USB device to store system logs, diagnostic information and firmware.

Note: The USB device must allow writing (it cannot be read-only) and use the FAT16, FAT32, EXT2, or EXT3 file system.

For Zyxel Devices that have more than one USB port, these commands only apply to the first USB storage device that is attached to the Zyxel Device.

Use these commands to configure settings that apply to the USB storage device connected to the Zyxel Device.

You must be in configuration mode (`configure terminal`) to use the indented commands shown below.

Table 69 USB Storage General Commands

COMMAND	DESCRIPTION
`show usb-storage`	Displays the status of the connected USB storage device.
`[no] usb-storage activate`	Enables or disables the connected USB storage service.
`usb-storage warn` *`number`* `<`*`percentage`*`|megabyte>`	Sets a number and the unit (`percentage` or `megabyte`) to have the Zyxel Device generate a log at the alert level when the remaining USB storage space is less than the set value.
`usb-storage mount`	Mounts the connected USB storage device.
`usb-storage umount`	Unmounts the connected USB storage device.
`[no] logging usb-storage`	Sets to have the Zyxel Device log or not log any information about the connected USB storage device(s) for the system log.
`show logging status usb-storage`	Displays the logging settings for the connected USB storage device.
`logging usb-storage category` *`category`* `level <all|normal>`	Configures the logging settings for the specified category for the connected USB storage device.
`logging usb-storage category` *`category`* `disable`	Stops logging for the specified category to the connected USB storage device.
`logging usb-storage flushThreshold <1..100>`	Configures the maximum storage space (in percentage) for storing system logs on the connected USB storage device.
`[no] diag-info copy usb-storage`	Sets to have the Zyxel Device save or stop saving the current system diagnostics information to the connected USB storage device. You may need to send this file to customer support for troubleshooting.
`show diag-info copy usb-storage`	Displays whether (enable or disable) the Zyxel Device saves the current system diagnostics information to the connected USB storage device.
`[no] corefile copy usb-storage`	Sets to have the Zyxel Device save or not save a process's core dump to the connected USB storage device if the process terminates abnormally (crashes). You may need to send this file to customer support for troubleshooting.

Table 69 USB Storage General Commands (continued)

COMMAND	DESCRIPTION
`show corefile copy usb-storage`	Displays whether (enable or disable) the Zyxel Device saves core dump files to the connected USB storage device.
`[no] usb-storage log_rotate_activate`	Has the Zyxel Device overwrite the oldest log file when the remaining USB storage space is less than the value you set above. The Zyxel Device will generate a log at the alert level. Note: Make sure to save the log files to your computer.

16.8.1 Firmware Upgrade via USB Stick

In addition to uploading firmware via the web configurator (see the User's Guide) or console port, you can also upload firmware directly from a USB stick connected to the Zyxel Device.

1. Create a folder on the USB stick called '/[ProductName_dir]/firmware'. For example, if your Zyxel Device is USG110, then create a '/usg110_dir/firmware/' folder on the stick.
2. Put one firmware 'bin' file into the firmware folder. Make sure the firmware ID and version number are correct for your model (the firmware ID is in brackets after the firmware version number - for USG100 it is AAPH).

   Note: Do not put more than one firmware 'bin' file into the firmware folder.

   The firmware version in the USB stick must be different to the currently running firmware. If the firmware on the USB stick is older, then the Zyxel Device will 'upgrade' to the older version. It is recommended that the firmware on the USB stick be the latest firmware version.
3. Insert the USB stick into the Zyxel Device. The firmware uploads to the standby system space.
4. The SYS LED blinks when the Zyxel Device automatically reboots making the upgraded firmware in standby become the running firmware.

   Note: If the startup-config.conf configuration file has problems and you are upgrading to 4.25 or later firmware, then the Zyxel Device will revert (failover) to the previously running firmware.

   If the startup-config.conf configuration file has problems and you are upgrading to earlier than 4.25 firmware, then the Zyxel Device uses the new earlier firmware, but generates a log and tries the existing lastgood.conf configuration file. If there isn't a lastgood.conf configuration file or it also has an error, the Zyxel Device applies the system-default.conf configuration file.

You must be in configuration mode (`configure terminal`) to use the indented commands shown below.

Table 70 USB Firmware Upgrade and Space Commands

COMMAND	DESCRIPTION
`show usb-storage update-firmware status`	Displays if updating firmware from USB storage is allowed.
`show usb-storage space`	Displays USB storage space details. `Criterion Number` is 10~99/100~9999 depending on whether you chose `percentage/megabyte` as the `Criterion Unit` for available USB storage. `Status` displays whether the USB device connected to the Zyxel Device is `none` (no USB device connected) / `Ready` / `Unused` (USB device connected but not in use). `Detail` displays whether the USB device connected to the Zyxel Device is `none` (no USB device connected) / `Removing` (USB device is being unmounted) / `Mounting` (USB device is being mounted / `Deactivated` (USB device is disabled) / `OutOfSpace` ((USB device is full). If both `Status` and `Detail` are `none`, then no USB device is connected. If `Status` is `Ready` and `Detail` is `none`, then a USB device is available.
`show usb-storage space ftp`	Displays total and available FTP space on the RAM memory of the Zyxel Device in /tmp (in bytes). RAM is cleared when the Zyxel Device restarts.
`show usb-storage space tmp`	Displays total and available space on the Flash memory of the Zyxel Device in /db/etc/zyxel/ftp/tmp/ (in bytes).
`show usb-storage space usb`	Displays total size of the system link file and available space of the USB device connected to the Zyxel Device in /mnt/usb.
`[no] usb-storage update-firmware enable`	Enables updating firmware from USB storage. The `no` command disables updating firmware from USB storage.
`usb-storage warn <10..99> percentage`	Sets a warning to display when available USB storage falls below the specified percentage.
`usb-storage warn <100..9999> megabyte`	Sets a warning to display when available USB storage falls below the specified number of megabytes.

16.8.2 USB Storage Commands Example

This example shows how to display the status of the connected USB storage device.

```
Router(config)# usb-storage activate
Router(config)# usb-storage mount
Router(config)# usb-storage update-firmware enable
Router(config)# usb-storage warn 50 percentage
Router# show usb-storage
USBStorage Configuration:
Activation: enable
Criterion Number: 50
Criterion Unit: percentage
USB Storage Status:
Device description: UFD 3.0 Silicon-Power32G
Usage: 28.9GB
Filesystem: unknown
Speed: USB 2.0 480Mbps
Status: Unused
Detail: OutOfSpace

Router# show usb-storage space ftp
Total space: 91384832
Remaining space: 42306560
Router# show usb-storage space tmp
Total space: 516079616
Remaining space: 502071296
Router# show usb-storage space usb
Total space: 5
Remaining space: 0
Router#
```

16.9 VLAN Interface Specific Commands

This section covers commands that are specific to VLAN interfaces. VLAN interfaces also use many of the general interface commands discussed at the beginning of Section 16.2 on page 118.

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 71 Input Values for VLAN Interface Commands

LABEL	DESCRIPTION
interface_name	VLAN interface: vlan*x*, *x* = 0 - 4094 Ethernet interface: For some Zyxel Device models, use ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your Zyxel Device model. For other Zyxel Devicemodels use a name such as wan1, wan2, opt, lan1, ext-wlan, or dmz.

This table lists the VLAN interface commands.

Table 72 `interface` Commands: VLAN Interfaces

COMMAND	DESCRIPTION
`interface` *`interface_name`*	Creates the specified interface if necessary and enters sub-command mode.
`[no] port` *`interface_name`*	Specifies the Ethernet interface on which the VLAN interface runs. The `no` command clears the port.
`[no] vlan-id <1..4094>`	Specifies the VLAN ID used to identify the VLAN. The `no` command clears the VLAN ID.
`[no] priority-code <0..7.`	Sets the 802.1p priority for vlan outgoing traffic from 0 to 7 where 0 is the lowest priority (lowest, background traffic) and 7 the highest (network control traffic).
`show port vlan-id`	Displays the Ethernet interface VLAN settings.

16.9.1 VLAN Interface Command Examples

The following commands show you how to set up VLAN vlan100 with the following parameters: VLAN ID 100, interface ge1, IP 1.2.3.4, subnet 255.255.255.0, MTU 598, gateway 2.2.2.2, description "I am vlan100", upstream bandwidth 345, and downstream bandwidth 123.

```
Router# configure terminal
Router(config)# interface vlan100
Router(config-if-vlan)# vlan-id 100
Router(config-if-vlan)# port ge1
Router(config-if-vlan)# ip address 1.2.3.4 255.255.255.0
Router(config-if-vlan)# ip gateway 2.2.2.2
Router(config-if-vlan)# mtu 598
Router(config-if-vlan)# upstream 345
Router(config-if-vlan)# downstream 123
Router(config-if-vlan)# description I am vlan100
Router(config-if-vlan)# exit
```

16.10 Bridge Specific Commands

This section covers commands that are specific to bridge interfaces. Bridge interfaces also use many of the general interface commands discussed at the beginning of Section 16.2 on page 118.

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 73 Input Values for Bridge Interface Commands

LABEL	DESCRIPTION
`interface_name`	The name of the interface. Ethernet interface: For some Zyxel Device models use ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your Zyxel Device model. For other Zyxel Device models use a name such as wan1, wan2, opt, lan1, ext-wlan, or dmz. VLAN interface: vlan*x*, *x* = 0 - 4094 bridge interface: br*x*, *x* = 0 - N, where N depends on the number of bridge interfaces your Zyxel Device model supports.

This table lists the bridge interface commands.

Table 74 `interface` Commands: Bridge Interfaces

COMMAND	DESCRIPTION
`interface` *`interface_name`*	Creates the specified interface if necessary and enters sub-command mode.
`[no] join` *`interface_name`*	Adds the specified Ethernet interface or VLAN interface to the specified bridge. The `no` command removes the specified interface from the specified bridge.
`show bridge available member`	Displays the available interfaces that could be added to a bridge.

16.10.1 Bridge Interface Command Examples

The following commands show you how to set up a bridge interface named br0 with the following parameters: member ge1, IP 1.2.3.4, subnet 255.255.255.0, MTU 598, gateway 2.2.2.2, upstream bandwidth 345, downstream bandwidth 123, and description “I am br0”.

```
Router# configure terminal
Router(config)# interface br0
Router(config-if-brg)# join ge1
Router(config-if-brg)# ip address 1.2.3.4 255.255.255.0
Router(config-if-brg)# ip gateway 2.2.2.2
Router(config-if-brg)# mtu 598
Router(config-if-brg)# upstream 345
Router(config-if-brg)# downstream 123
Router(config-if-brg)# description I am br0
Router(config-if-brg)# exit
```

16.11 LAG Commands

This section covers commands that are specific to Link Aggregation Group (LAG) interfaces. LAG is a way to combine multiple physical Ethernet interfaces into a single logical interface. This increases uplink bandwidth. It also increases availability as even if a member link goes down, LAG can continue to transmit and receive traffic over the remaining links.

To configure LAG, configure a link number and specify the member ports in the link. All ports must have the same speed and be in full-duplex mode. You must configure the LAG on both sides of the link and you must set the interfaces on either side of the link to be the same speed.

Note: At the time of writing, up to 4 ports can be grouped into a LAG and up to 4 LAGs can be configured on a Zyxel Device.

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 75 Input Values for LAG Interface Commands

LABEL	DESCRIPTION
interface_name	LAG interface: lag*x*, *x* = 0 - 4 (at the time of writing). Ethernet interface: For some Zyxel Device models use ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your Zyxel Device model. For other Zyxel Device models use a name such as wan1, wan2, opt, lan1, ext-wlan, or dmz. VLAN interface: vlan*x*, *x* = 0 - 4094

This table lists the LAG-specific interface commands. See Table 53 on page 118 for common `interface` commands.

Table 76 `interface` Commands: LAG Interfaces

COMMAND	DESCRIPTION
`interface` *interface_name*	Creates the specified LAG interface (`lag0` for example) and enters sub-command mode.
`traffic-prioritize {tcp-ack|content-filter|dns} bandwidth <0..1048576>];`	Applies traffic priority when the interface sends TCP-ACK traffic, traffic for querying the content filter, or traffic for resolving domain names. It also sets how much bandwidth the traffic can use.
`traffic-prioritize {tcp-ack|content-filter|dns} priority-code <0..7> deactivate`	Turns off traffic priority settings for when the interface sends the specified type of traffic.
`mode {802_3ad | active-backup | balance-alb | mode 802_3ad}`	Sets the LAG mode. Mode refers to whether the LAG is acting as follows: • **`active-backup`** where only one slave in the LAG interface is active and another slave becomes active only if the active slave fails. • **`802.3ad`** (IEEE 802.3ad Dynamic link aggregation) where Link Aggregation Control Protocol (LACP) negotiates automatic combining of links and balances the traffic load across the LAG link by sending LACP packets to the directly connected device that also implements LACP. The slaves must have the same speed and duplex settings. • **`balance-alb`** (adaptive load balancing) where traffic is distributed according to the current load on each slave by ARP negotiation. Incoming traffic is received by the current slave. If the receiving slave fails, another slave takes over the MAC address of the failed receiving slave.
`[no] slave` *interface_name*	Specifies the member ports in the link. A slave is a physical Ethernet interface that is a member of a LAG. Slaves do not have an IP Address and in some cases share the same MAC address. The `no` command removed the member ports from the link.
`link-monitoring {arp | mii | none}`	Sets link monitoring to be `arp`, `mii` or `none`. • `arp` monitoring sends ARP queries and uses the reply to know if the link is up and that traffic is flowing over the link • `mii` monitoring monitors the state of the local interface; it can't tell if the link can transmit or receive packets. • `none` means no link monitoring is done.

Table 76 `interface` Commands: LAG Interfaces (continued)

COMMAND	DESCRIPTION
`arp {arp-interval <1..1000> | arp-ip-target <W.X.Y.Z>}`	Configure for `arp` Link Monitoring. `arp-interval:` Specifies the frequency of ARP requests sent to confirm a that slave interface is up. `arp-ip-target <W.X.Y.Z>:` Specifies the IP address of the link to send ARP queries.
`miimon <1..1000>`	Configure for `mii` Link Monitoring. Specifies the link check interval in milliseconds that the system polls the Media Independent Interface (MII) to get status.
`xmit-hash-policy {layer2 | layer2_3}`	Configure for `802.3ad` Mode. Specifies the algorithm for slave selection according to the selected TCP/IP layer.
`lacp-rate {fast | slow}`	Configure for `802.3ad` Mode. Specifies the preferred LACPDU packet transmission rate (`fast | slow`) to request from 802.3ad partner.
`updelay <0..1000>`	Configure for `mii` Link Monitoring. Specifies the waiting time in milliseconds to confirm the slave interface status is up.
`downdelay <0..1000>`	Configure for `mii` Link Monitoring. Specifies the waiting time in milliseconds to confirm the slave interface status is down.
`igmp {activate | direction {downstream | upstream} | version <1..3>}`	See Table 54 on page 125 for these command descriptions.
`ping-check`	See Table 60 on page 135 for these command descriptions.
`type {external | general | internal}`	Specifies one of the following option depending on the type of network to which the Zyxel Device is connected or if you want to additionally manually configure some related settings. **`internal`** is for connecting to a local network. Other corresponding configuration options: DHCP server and DHCP relay. The Zyxel Device automatically adds default SNAT settings for traffic flowing from this interface to an external interface. **`external`** is for connecting to an external network (like the Internet). The Zyxel Device automatically adds this interface to the default WAN trunk. For **`general`**, the rest of the screen's options do not automatically adjust and you must manually configure a policy route to add routing and SNAT settings for the interface.
`show lag available slaves`	Displays the available slaves that could be added to a LAG.
`show interface lag`	Displays interface details for all LAG interfaces.
`show interface lagx`	Displays interface details for LAG x.

16.11.1 LAG Interface Command Example

The following commands set up a LAG with slaves ge3, ge5 and ge6.

```
Router# configure terminal
Router(config)# interface lag1
Router(config-if-lag)# mode 802_3ad
Router(config-if-lag)# slave ge3
Router(config-if-lag)# slave ge5
Router(config-if-lag)# slave ge6
Router(config-if-lag)# link-monitoring mii
Router(config-if-lag)# miimon 1000
Router(config-if-lag)# xmit-hash-policy layer2
Router(config-if-lag)# lacp-rate fast
Router(config-if-lag)# updelay 500
Router(config-if-lag)# downdelay 500
Router(config-if-lag)# igmp activate
Router(config-if-lag)# type external
Router(config-if-lag)# exit
Router(config)# show lag available slaves
available slave count: 5
available slave: ge1,ge2,ge4,ge7,ge8
Router(config)# show interface lag1
active: yes
interface name: lag1
modifiable: yes
mode: 802.3ad
primary: none
slaves count: 3
slaves: ge3,ge5,ge6
description:
type: external
link monitoring: mii
miimon: 1000
updelay: 500
downdelay: 500
ARP interval: 20
ARP IP target: 0.0.0.0
LACP rate: fast
xmit hash policy: layer2
IP type: static
IP address: 0.0.0.0
netmask: 0.0.0.0
gateway:
metric: 0
igmp active: yes
igmp direction: upstream
igmp version: IGMPv3
upstream: 1048576
downstream: 1048576
MTU: 1500
MSS: 0
tcp-ack traffic prioritize:
    active                      : yes
    bandwidth                   : 1048576
    priority                    : 1
    maximize-bandwidth-usage    : yes
```

```
Router(config)# show interface lag
No. Name            Address type IP address      Mode            Active Slaves
================================================================================
1   lag0            static       0.0.0.0         active-backup   yes
2   lag1           static       0.0.0.0         802.3ad         yes    ge3, ge5, ge6
```

16.12 VTI Commands

IPsec VPN Tunnel Interface (VTI) encrypts or decrypts IPv4 traffic from or to the interface according to the IP routing table.

VTI allows static routes to send traffic over the VPN. The IPsec tunnel endpoint is associated with an actual (virtual) interface. Therefore many interface capabilities such as Policy Route, Static Route, Trunk, and BWM can be applied to the IPsec tunnel as soon as the tunnel is active

Create a trunk using VPN tunnel interfaces for load balancing.

16.12.1 Restrictions for IPsec Virtual Tunnel Interface

- IPv4 traffic only
- IPSec tunnel mode only. A shared keyword must not be configured when using tunnel mode.
- With a VTI VPN you do not add local or remote LANs to your VPN configuration.
- For a VTI VPN you should only have one local and one remote WAN.
- A dynamic peer is not supported
- The IPsec VTI is limited to IP unicast and multicast traffic only.

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 77 Input Values for VTI Interface Commands

LABEL	DESCRIPTION
interface_name	VTO interface: lag*x*, where x is a number from 0 to the maximum number of VPN connections allowed for your Zyxel Device model. Ethernet interface: For some Zyxel Device models use ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your Zyxel Device model. For other Zyxel Device models use a name such as wan1, wan2, opt, lan1, ext-wlan, or dmz. VLAN interface: vlan*x*, *x* = 0 - 4094

This table lists the LAG-specific interface commands. See Table 53 on page 118 for common `interface` commands.

Table 78 `interface` Commands: VTI Interfaces

COMMAND	DESCRIPTION
`interface` *`interface_name`*	Creates the specified VTI interface (`vti1` for example) and enters sub-command mode. Note: You should have created a VPN tunnel for a Vpn Tunnel Interface scenario first.
`[no] downstream <0..1048576>`	Specifies the downstream bandwidth for the specified interface. The `no` command sets the downstream bandwidth to 1048576.
`[no] ip address` *`ip subnet_mask`*	Assigns the specified IP address and subnet mask to the specified interface. The `no` command clears the IP address and the subnet mask.
`[no] metric <0..15>`	Sets the VTI interface's priority relative to other interfaces. The lower the number, the higher the priority.
`[no] ping-check activate`	Enables ping check for the specified interface. The `no` command disables ping check for the specified interface.
`ping-check {`*`domain_name | ip`*`}`	Specifies what the Zyxel Device pings for the ping check; you can specify a fully-qualified domain name or IP address for the interface.
`ping-check {`*`domain_name | ip`*`} period <5..30>`	Specifies what the Zyxel Device pings for the ping check and sets the number of seconds between each ping check.
`ping-check {`*`domain_name | ip`*`} timeout <1..10>`	Specifies what the Zyxel Device pings for the ping check and sets the number of seconds the Zyxel Device waits for a response.
`ping-check {`*`domain_name | ip`*`} fail-tolerance <1..10>`	Specifies what the Zyxel Device pings for the ping check and sets the number of times the Zyxel Device times out before it stops routing through the specified interface.
`ping-check {`*`domain_name | ip`*`} method {icmp | tcp}`	Sets how the Zyxel Device checks the connection to the gateway. `icmp`: ping the domain name or IP address you specify to make sure it is still available. `tcp`: perform a TCP handshake with the domain name or IP address you specify to make sure it is still available.
`ping-check {`*`domain_name | ip`*`} port <1..65535>`	Specifies the port number to use for a TCP connectivity check.
`[no] shutdown`	Deactivates the specified interface. The `no` command activates it.
`[no] upstream <0..1048576>`	Specifies the upstream bandwidth for the specified interface. The `no` command sets the upstream bandwidth to 1048576
`[no] ip ospf priority` *`priority`*	Sets the priority (between 0 and 255) of this interface when the OSPF autonomous area is looking for a Designated Router (DR) or Backup Designated Router (BDR). The highest-priority interface identifies the DR, and the second-highest-priority interface identifies the BDR. Set the priority to zero if the interface can not be the DR or BDR. The `no` command sets the priority to 1.
`ip ospf cost <1..65535>`	Sets the cost (between 1 and 65,535) to route packets through this interface. The `no` command sets the priority to 10

Table 78 `interface` Commands: VTI Interfaces (continued)

COMMAND	DESCRIPTION
`ip ospf dead-interval <1..65535>`	Sets how long to wait for hello packets before declaring that the neighbor is dead. The no command resets the interval.
`ip ospf hello-interval <1..65535>`	Sets how often to send a hello packet to check if a neighbor is still alive. The no command resets the interval.
`ip ospf retransmit-interval <1..65535>`	Sets the time between Link-State Advertisement (LSA) retransmissions to adjacent routers for a given interface. The no command resets the interval.
`[no] ip ospf {authentication-key` *`key8`* `| encrypted-authentication-key` *`encrypted_str`*`}`	Sets an authentication method. To exchange OSPF routing information with peer border routers, you must use the same authentication method that they use. The no command disables the configured authentication. *`encrypted_str`*: string used for encryption *`key8`*: key used for authentication and can contain1-8 alphanumeric characters, underscores, and dashes.
`[no] ip ospf message-digest-key <1..255> {md5` *`dr_authkey_16`* `| encrypted-md5` *`encrypted_str`*`}`	Sets the ID (between 1 and 255) for MD5 authentication and the password (up to 16 alphanumeric characters and the underscore) for text authentication or MD5 authentication of the Designated Router (DR). The no command disables the configured authentication. *`dr_authkey_16`*: password for authentication and can contain1-16 alphanumeric characters, underscores, and dashes. *`encrypted_str`*: string used for encryption
`[no] ip ospf authentication [message-digest | same-as-area]`	Uses the default authentication method in the area. disables authentication. The no command disables using the default authentication method in the area.
`[no] ip rip {send | receive} version <1..2> [1.2]`	Sets the RIP version(s) used for sending or receiving RIP packets. Choices are 1, 2, and 1 and 2.
`[no] ip v2-broadcast`	Sends RIP-2 packets using subnet broadcasting; otherwise, the Zyxel Device uses multicasting.
`[no] igmp direction {upstream | downstream}`	Sets the RIP direction `downstream:` This interface receives routing information. `upstream:` This interface sends routing information.
`[no] igmp activate`	Allows the Zyxel Device to act as an IGMP proxy for hosts connected on the IGMP downstream interface.
`binding interface` *`interface_name`* `crypto-map` *`map_name`*	Binds the VTI interface to an IPSec SA that uses the VPN Tunnel Interface scenario `vpn-tunnel-interface`)
`vpn-interface-restriction activate`	Turns on interface restrictions for IPSec VPN traffic. When the remote IPSec VPN device initiates a VPN tunnel to one of the Zyxel Device's WAN interface, outgoing VPN traffic can only be sent through the WAN interface on which the incoming VPN traffic was received. If the original WAN interface is down or disabled, the Zyxel Device will discard the outgoing VPN traffic instead of forwarding it through another active WAN interface. Note: The command takes effect after you restart the Zyxel Device.

Table 78 `interface` Commands: VTI Interfaces (continued)

COMMAND	DESCRIPTION
`vpn-interface-restriction deactivate`	Turns off interface restrictions for IPSec VPN traffic. When the WAN interface on which incoming VPN traffic was received has failed or the VPN client is connected to the LAN, the Zyxel Device can forward outgoing VPN traffic via a different interface. Note: The command takes effect after you restart the Zyxel Device.
`show interface vti`	Displays interface details for all VTI interfaces.
`show interface vtix`	Displays interface details for VTI x.
`show vpn-interface-restriction status`	Displays whether interface restrictions for IPSec VPN traffic is enabled or not.

16.12.2 VTI Interface Command Example

The following commands set up a VTI interface with the shown parameters and binds it to an IPSec SA using a VPN Tunnel Interface scenario.

```
Router# configure terminal
Router(config)# interface vti0
Router(config-if-vti)# downstream 10000
Router(config-if-vti)# upstream 10000
Router(config-if-vti)# ip address 1.1.1.1 255.255.255.0
Router(config-if-vti)# metric 5
Router(config-if-vti)# traffic-prioritize content-filter deactivate
Router(config-if-vti)# exit
Router(config)# show interface vti0
interface name: vti0
active: no
vpn rule:
connection: no
IP address: 1.1.1.1
netmask: 255.255.255.0
upstream: 10000
downstream: 10000
metric: 5
Router(config)#
Router(config)# crypto map test
Router(config-crypto test)# scenario vpn-tunnel-interface
Router(config-crypto test)# exit
Router(config)# binding interface vti0 crypto-map test
Router(config)#
```

CHAPTER 17
Trunks

17.1 Trunks Overview

You can group multiple interfaces together into trunks to have multiple connections share the traffic load to increase overall network throughput and enhance network reliability. If one interface's connection goes down, the Zyxel Device sends traffic through another member of the trunk. For example, you can use two interfaces for WAN connections. You can connect one interface to one ISP (or network) and connect the another to a second ISP (or network). The Zyxel Device can balance the load between multiple connections. If one interface's connection goes down, the Zyxel Device can automatically send its traffic through another interface.

You can use policy routing to specify through which interface to send specific traffic types. You can use trunks in combination with policy routing. You can also define multiple trunks for the same physical interfaces. This allows you to send specific traffic types through the interface that works best for that type of traffic, and if that interface's connection goes down, the Zyxel Device can still send its traffic through another interface.

17.2 Trunk Scenario Examples

Suppose one of the Zyxel Device's interfaces is connected to an ISP that is also your Voice over IP (VoIP) service provider. You may want to set that interface as active and set another interface (connected to another ISP) to passive. This way VoIP traffic goes through the interface connected to the VoIP service provider whenever the interface's connection is up.

Another example would be if you use multiple ISPs that provide different levels of service to different places. Suppose ISP A has better connections to Europe while ISP B has better connections to Australia. You could use policy routing and trunks to send traffic for your European branch offices primarily through ISP A and traffic for your Australian branch offices primarily through ISP B.

17.3 Trunk Commands Input Values

The following table explains the values you can input with the `interface-group` commands.

Table 79 interface-group Command Input Values

LABEL	DESCRIPTION
group-name	A descriptive name for the trunk. Zyxel Device uses up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive.
interface-name	The name of an interface, it could be an Ethernet, PPP, VLAN or bridge interface. The possible number of each interface type and the abbreviation to use are as follows. Ethernet interface: For some Zyxel Device models, use ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your Zyxel Device model. Other Zyxel Device models use a name such as wan1, wan2, opt, lan1, or dmz. PPPoE/PPTP interface: ppp*x*, *x* = 0 - N, where N depends on the number of PPPoE/PPTP interfaces your Zyxel Device model supports. VLAN interface: vlan*x*, *x* = 0 - 4094 bridge interface: br*x*, *x* = 0 - N, where N depends on the number of bridge interfaces your Zyxel Device model supports.
num	The interface's position in the trunk's list of members <1..8>.
<CR>	Carriage Return (the "enter" key).

17.4 Trunk Commands Summary

The following table lists the `interface-group` commands. You must use the `configure terminal` command to enter the configuration mode before you can use these commands. See Table 79 on page 163 for details about the values you can input with these commands.

Table 80 interface-group Commands Summary

COMMAND	DESCRIPTION
`show interface-group {system-default|user-define|`*group-name*`}`	Displays pre-configured system default trunks, your own user configuration trunks or a specified trunk's settings.
`[no] interface-group` *group-name*	Creates a trunk name and enters the trunk sub-command mode where you can configure the trunk. The no command removes the trunk.
`algorithm {wrr|llf|spill-over}`	Sets the trunk's load balancing algorithm.
`exit`	Leaves the trunk sub-command mode.
`flush`	Deletes a trunk's interface settings.
`interface {`*num*`|append|insert` *num*`}` *interface-name* `[weight <1..10>|limit <1..2097152>|passive]`	This subcommand adds an interface to a trunk. Sets the interface's number. It also sets the interface's weight and spillover limit or sets it to be passive.

Table 80 interface-group Commands Summary (continued)

COMMAND	DESCRIPTION
loadbalancing-index <inbound|outbound|total>	Use this command only if you use least load first or spill-over as the trunk's load balancing algorithm. Set either inbound, outbound, or total (outbound and inbound) traffic to which the Zyxel Device will apply the specified algorithm. Outbound traffic means the traffic travelling from an internal interface (ex. LAN) to an external interface (ex. WAN). Inbound traffic means the opposite.
mode {normal|trunk}	Sets the mode for a trunk. Do this first in the trunk's sub-command mode.
move <1..8> to <1..8>	Changes the interface order in a trunk.
[no] interface {*num*|*interface-name*}	Removes an interface from the trunk.
system default-interface-group *group-name*	Sets the Zyxel Device to first attempt to use the the specified WAN trunk.
[no] system default-snat	Enables or disables Source NAT (SNAT). When SNAT is enabled, the Zyxel Device uses the IP address of the outgoing interface as the source IP address of the packets it sends out through the WAN interfaces.
show system default-snat	Displays whether the Zyxel Device enable SNAT or not. The Zyxel Device performs SNAT by default for traffic going to or from the WAN interfaces.
show system default-interface-group	Displays the WAN trunk the Zyxel Device first attempts to use.

17.5 Trunk Command Examples

The following example creates a weighted round robin trunk for Ethernet interfaces ge1 and ge2. The Zyxel Device sends twice as much traffic through ge1.

```
Router# configure terminal
Router(config)# interface-group wrr-example
Router(if-group)# mode trunk
Router(if-group)# algorithm wrr
Router(if-group)# interface 1 ge1 weight 2
Router(if-group)# interface 2 ge2 weight 1
Router(if-group)# exit
Router(config)#
```

The following example creates a least load first trunk for Ethernet interface ge3 and VLAN 5, which will only apply to outgoing traffic through the trunk. The Zyxel Device sends new session traffic through the least utilized of these interfaces.

```
Router# configure terminal
Router(config)# interface-group llf-example
Router(if-group)# mode trunk
Router(if-group)# algorithm llf
Router(if-group)# interface 1 ge3
Router(if-group)# interface 2 vlan5
Router(if-group)# loadbalancing-index outbound
Router(if-group)# exit
Router(config)#
```

The following example creates a spill-over trunk for Ethernet interfaces ge1 and ge3, which will apply to both incoming and outgoing traffic through the trunk. The Zyxel Device sends traffic through ge1 until it hits the limit of 1000 kbps. The Zyxel Device sends anything over 1000 kbps through ge3.

```
Router# configure terminal
Router(config)# interface-group spill-example
Router(if-group)# mode trunk
Router(if-group)# algorithm spill-over
Router(if-group)# interface 1 ge1 limit 1000
Router(if-group)# interface 2 ge3 limit 1000
Router(if-group)# loadbalancing-index total
Router(if-group)# exit
Router(config)#
```

CHAPTER 18
Route

18.1 Policy Route

Traditionally, routing is based on the destination address only and the Zyxel Device takes the shortest path to forward a packet. IP Policy Routing (IPPR) provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to incoming packets on a per interface basis, prior to the normal routing.

18.1.1 Source Network Address Translation (SNAT)

SNAT allows the Zyxel Device to rewrite the source IP address of packets in a policy route. This means you can make packets coming from an IP address appear to originate from a different IP address.

18.1.1.1 SNAT with the ZyWALL Interface

In firmware version 5.0 and later, you can apply SNAT to packets sent from the ZyWALL interface. This can be used to separate internally generated Zyxel Device traffic from other traffic.

For example: The Zyxel Device has two IP addresses, 6.6.6.6 and 6.6.6.7, on a WAN interface. There is a firewall in front of the Zyxel Device with the following security rules:

- IP address 6.6.6.6 is client traffic. There are no restrictions.
- IP address 6.6.6.7 is Zyxel Device traffic, Packets can only go to *.myzyxel.com and *.cloud.zyxel.com.

If clients are connected to LAN1 on the Zyxel Device, then you need to create two policy routes with SNAT enabled:

- Client_Route - Incoming interface: LAN1, SNAT: 6.6.6.6.
- Device_Route - Incoming interface: ZyWALL, SNAT: 6.6.6.7.

18.2 Policy Route Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 81 Input Values for General Policy Route Commands

LABEL	DESCRIPTION
address_object	The name of the IP address (group) object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
address6_object	The name of the IPv6 address (group) object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
interface_name	The name of the interface. Ethernet interface: Some Zyxel Device models use ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your Zyxel Device model. Other Zyxel Device models use a name such as wan1, wan2, opt, lan1, ext-wlan, or dmz. virtual interface on top of Ethernet interface: add a colon (:) and the number of the virtual interface. For example: ge*x*:*y*, *x* = 1 - N, *y* = 1 - 4 VLAN interface: vlan*x*, *x* = 0 - 4094 virtual interface on top of VLAN interface: vlan*x*:*y*, *x* = 0 - 4094, *y* = 1 - 12 bridge interface: br*x*, *x* = 0 - N, where N depends on the number of bridge interfaces your Zyxel Device model supports. virtual interface on top of bridge interface: br*x*:*y*, *x* = the number of the bridge interface, *y* = 1 - 4 PPPoE/PPTP interface: ppp*x*, *x* = 0 - N, where N depends on the number of PPPoE/PPTP interfaces your Zyxel Device model supports.
policy_number	The number of a policy route. 1 - *X* where *X* is the highest number of policy routes the Zyxel Device model supports. See the Zyxel Device's User's Guide for details.
schedule_object	The name of the schedule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
service_name	The name of the service (group). You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
user_name	The name of a user (group). You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
destv6	The IPv6 route prefix (subnet address) for the destination.
prefix	The IPv6 prefix length, 0 - 128.
gatewayv6	The IPv6 address of the specified gateway.
ipv6_addr	An IPv6 address.
ipv6_global_address	An IPv6 address excluding the link-local address (fe80::).
ipv6_link_local	An fe80:: IPv6 address.

The following table describes the commands available for policy route. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 82 Command Summary: Policy Route

COMMAND	DESCRIPTION
`[no] bwm activate`	Globally enables bandwidth management. You must globally activate bandwidth management to have individual policy routes or application patrol policies apply bandwidth management. The `no` command globally disables bandwidth management.
`policy {`*`policy_number`* `| append | insert` *`policy_number`*`}`	Enters the policy-route sub-command mode to configure, add or insert a policy.
`[no] auto-destination`	When you set `tunnel` as the next-hop type (using the `next-hop tunnel` command) for this route, you can use this command to have the Zyxel Device use the local network of the peer router that initiated an incoming dynamic IPSec tunnel as the destination address of the policy instead of what you configure by using the `destination` command. The `no` command disables the setting.
`[no] auto-disable`	When you set `interface` or `trunk` as the next-hop type (using the `next-hop interface` or `next-hop trunk` command) for this route, you can use this command to have the Zyxel Device automatically disable this policy route when the next-hop's connection is down. The `no` command disables the setting.
`conn-check {FQDN | addr | activate}`	Turns on the connection check to the gateway identified by its FQDN or IP address.
`[no] deactivate`	Disables the specified policy. The `no` command enables the specified policy.
`[no] description` *`description`*	Sets a descriptive name for the policy. The `no` command removes the name for the policy.
`[no] destination {`*`address_object`*`|any}`	Sets the destination IP address the matched packets must have. The `no` command resets the destination IP address to the default (any). `any` means all IP addresses.
`[no] dscp {any | <0..63>}`	Sets a custom DSCP code point (0~63). This is the DSCP value of incoming packets to which this policy route applies. `any` means all DSCP value or no DSCP marker.
`[no] dscp class {default |` *`dscp_class`*`}`	Sets a DSCP class. Use `default` to apply this policy route to incoming packets that are marked with DSCP value 0. Use one of the pre-defined AF classes (including af11~af13, af21~af23, af31~af33, and af41~af43) to apply this policy route to incoming packets that are marked with the DSCP AF class. The "af" entries stand for Assured Forwarding. The number following the "af" identifies one of four classes and one of three drop preferences. See Assured Forwarding (AF) PHB for DiffServ on page 172 for more details. *`dscp_class`* can set cs0~cs7 too.
`dscp-marking <0..63>`	Sets a DSCP value to have the Zyxel Device apply that DSCP value to the route's outgoing packets.
`dscp-marking class {default |` *`dscp_class`*`}`	Sets how the Zyxel Device handles the DSCP value of the outgoing packets that match this route. Set this to `default` to have the Zyxel Device set the DSCP value of the packets to 0. Set this to an "af" class (including af11~af13, af21~af23, af31~af33, and af41~af43) which stands for Assured Forwarding. The number following the "af" identifies one of four classes and one of three drop preferences. See Assured Forwarding (AF) PHB for DiffServ on page 172 for more details. *`dscp_class`* can set cs0~cs7 too.

Table 82 Command Summary: Policy Route (continued)

COMMAND	DESCRIPTION
`no dscp-marking`	Use this command to have the Zyxel Device not modify the DSCP value of the route's outgoing packets.
`exit`	Leaves the sub-command mode.
`[no] interface interface_name`	Sets the interface on which the incoming packets are received. The no command resets the incoming interface to the default (any). any means all interfaces. ZyWALL is a default interface which the Zyxel Device uses to send internally generated trafffic. For example, the Zyxel Device uses the ZyWALL interface to download device licensing information from MyZyxel, and to send authentication requests to an external RADIUS server.
`[no] next-hop {auto|gateway address object |interface interface_name |trunk trunk_name|tunnel tunnel_name}`	Sets the next-hop to which the matched packets are routed. The no command resets next-hop settings to the default (auto).
`[no] schedule schedule_object`	Sets the schedule. The no command removes the schedule setting to the default (none). none means any time.
`[no] service {service_name|any}`	Sets the IP protocol. The no command resets service settings to the default (any). any means all services.
`[no] snat {outgoing-interface| {address_object}}`	Applies Source Network Address Translation (SNAT) to packets within the policy route. Each packet's source address is rewritten to the IP address of the outgoing interface or address object. The no command removes source NAT settings from the rule. Note: If the address object is a group or range of IP addresses, then the Zyxel Device picks one IP address randomly from the group or range, and then assigns the address perminantly to the policy. Note: In Zyxel Device firmware version 4.60 and earlier, it is not possible to configure this setting if the policy's interface is set to "ZyWALL". In Zyxel Device firmware version 5.0 and later, this limitation is removed. Note: To configure this setting in the Web Configurator when the policy's interface is set to "ZyWALL", you must using the gui-visibility command. For details, see Section 72.4 on page 603.
`[no] source {address_object|any}`	Sets the source IP address that the matched packets must have. The no command resets the source IP address to the default (any). any means all IP addresses.
`[no] srcport {profile_name|any}`	Sets the source port that the matched packets must have. The no command resets the source port to the default (any). any means all ports.
`[no] sslvpn tunnel_name`	Sets the incoming interface to an SSL VPN tunnel. The no command removes the SSL VPN tunnel through which the incoming packets are received.
`[no] tunnel tunnel_name`	Sets the incoming interface to an IPSec VPN tunnel. The no command removes the IPSec VPN tunnel through which the incoming packets are received.
`[no] user user_name`	Sets the user name. The no command resets the user name to the default (any). any means all users.
`policy6 {policy_number | append | insert policy_number}`	Enters the IPv6 policy-route sub-command mode to configure, add or insert a policy.

Table 82 Command Summary: Policy Route (continued)

COMMAND	DESCRIPTION
[no] deactivate	Disables the specified policy. The no command enables the specified policy.
[no] description *description*	Sets a descriptive name for the IPv6 policy. The no command removes the name for the policy.
[no] destination {*address6_object*|any}	Sets the destination IPv6 IP address the matched packets must have. The no command resets the destination IP address to the default (any). any means all IP addresses.
[no] dscp {any | <0..63>}	Sets a custom DSCP code point (0~63). This is the DSCP value of incoming packets to which this policy route applies. any means all DSCP value or no DSCP marker.
[no] dscp class {default | *dscp_class*}	Sets a DSCP class. Use default to apply this policy route to incoming packets that are marked with DSCP value 0. Use one of the pre-defined AF classes (including af11~af13, af21~af23, af31~af33, and af41~af43) to apply this policy route to incoming packets that are marked with the DSCP AF class. The "af" entries stand for Assured Forwarding. The number following the "af" identifies one of four classes and one of three drop preferences. See Assured Forwarding (AF) PHB for DiffServ on page 172 for more details. *dscp_class* can set cs0~cs7 too.
dscp-marking <0..63>	Sets a DSCP value to have the Zyxel Device apply that DSCP value to the route's outgoing packets.
dscp-marking class {default | *dscp_class*}	Sets how the Zyxel Device handles the DSCP value of the outgoing packets that match this route. Set this to default to have the Zyxel Device set the DSCP value of the packets to 0. Set this to an "af" class (including af11~af13, af21~af23, af31~af33, and af41~af43) which stands for Assured Forwarding. The number following the "af" identifies one of four classes and one of three drop preferences. See Assured Forwarding (AF) PHB for DiffServ on page 172 for more details. *dscp_class* can set cs0~cs7 too.
no dscp-marking	Use this command to have the Zyxel Device not modify the DSCP value of the route's outgoing packets.
exit	Leaves the sub-command mode.
[no] interface *interface_name*	Sets the interface on which the matched packets are received. The no command resets the incoming interface to the default (any). any means all interfaces.
[no] next-hop {auto|gateway *address_object* |interface *interface_name* |trunk *trunk_name*|tunnel *tunnel_name*}	Sets the next-hop to which the matched packets are routed. The no command resets next-hop settings to the default (auto).
[no] schedule *schedule_object*	Sets the schedule. The no command removes the schedule setting to the default (none). none means any time.
[no] service {*service_name*|any}	Sets the IP protocol. The no command resets service settings to the default (any). any means all services.
[no] source {*address6_object*|any}	Sets the source IPv6 IP address that the matched packets must have. The no command resets the source IP address to the default (any). any means all IP addresses.
[no] srcport {*profile_name*|any}	Sets the source port that the matched packets must have. The no command resets the source port to the default (any). any means all ports.
[no] tunnel *tunnel_name*	Sets the incoming interface to an IPSec VPN tunnel. The no command removes the IPSec VPN tunnel through which the incoming packets are received.

Table 82 Command Summary: Policy Route (continued)

COMMAND	DESCRIPTION
[no] user *user_name*	Sets the user name. The no command resets the user name to the default (any). any means all users.
[no] policy controll-ipsec-dynamic-rules activate	Enables the Zyxel Device to use policy routes to manually specify the destination addresses of dynamic IPSec rules. You must manually create these policy routes. The Zyxel Device automatically obtains source and destination addresses for dynamic IPSec rules that do not match any of the policy routes. The no command has the Zyxel Device automatically obtain source and destination addresses for all dynamic IPSec rules.
policy default-route	Enters the policy-route sub-command mode to set a route with the name "default-route".
policy delete *policy_number*	Removes a routing policy.
policy flush	Clears the policy routing table.
policy list table	Displays all policy route settings.
policy move *policy_number* to *policy_number*	Moves a routing policy to the number that you specified.
[no] policy override-direct-route activate	Has the Zyxel Device forward packets that match a policy route according to the policy route instead of sending the packets to a directly connected network. Use the no command to disable it.
[no] policy controll-virtual-server-rules activate	Gives policy routes priority over NAT virtual server rules (1-1 SNAT). Use the no command to give NAT virtual server rules priority over policy routes.
[no] policy6 override-direct-route activate	Has the Zyxel Device forward IPv6 packets that match a policy route according to the policy route instead of sending the packets to a directly connected network. Use the no command to disable it.
show bwm activation	Displays whether or not the global setting for bandwidth management on the Zyxel Device is enabled.
show bwm-usage < [policy-route *policy_number*] | [interface *interface_name*]	Displays the specified policy route or interface's bandwidth allotment, current bandwidth usage, and bandwidth usage statistics.
show policy-route [*policy_number*]	Displays all or specified policy route settings.
show policy-route begin <1..200> end <1..200>	Displays the specified range of policy route settings.
show policy-route conn-check	Displays the policy route for the connection check.
show policy-route conn-check [*policy_number*]	Displays the specified policy route for the connection check.
show policy-route conn-check status [*policy_number*]	Displays the connection check status for the specified policy route.
show policy-route controll-ipsec-dynamic-rules	Displays whether the Zyxel Device checks policy routes first before IPSec dynamic rules.
show policy-route override-direct-route	Displays whether or not the Zyxel Device forwards packets that match a policy route according to the policy route instead of sending the packets to a directly connected network.
show policy-route controll-virtual-server-rules	Displays whether or not policy routes have priority over NAT virtual server rules (1-1 SNAT).
show policy-route6 override-direct-route	Displays whether or not the Zyxel Device forwards IPv6 packets that match a policy route according to the policy route instead of sending the packets to a directly connected network.

Table 82 Command Summary: Policy Route (continued)

COMMAND	DESCRIPTION
`show policy-route rule_count`	Displays the number of policy routes that have been configured on the Zyxel Device.
`show policy-route underlayer-rules`	Displays all policy route rule details for advanced debugging.
`show policy-route6 [policy_number]`	Displays all or specified IPv6 policy route settings.
`show policy-route6 begin <1..200> end <1..200>`	Displays the specified range of IPv6 policy route settings.
`show policy-route6 controll-ipsec-dynamic-rules`	Displays whether the Zyxel Device checks IPv6 policy routes first before IPSec dynamic rules.
`show policy-route6 rule_count`	Displays the number of IPv6 policy routes that have been configured on the Zyxel Device.

18.2.1 Assured Forwarding (AF) PHB for DiffServ

Assured Forwarding (AF) behavior is defined in RFC 2597. The AF behavior group defines four AF classes. Inside each class, packets are given a high, medium or low drop precedence. The drop precedence determines the probability that routers in the network will drop packets when congestion occurs. If congestion occurs between classes, the traffic in the higher class (smaller numbered class) is generally given priority. Combining the classes and drop precedence produces the following twelve DSCP encodings from AF11 through AF43. The decimal equivalent is listed in brackets.

Table 83 Assured Forwarding (AF) Behavior Group

	CLASS 1	CLASS 2	CLASS 3	CLASS 4
Low Drop Precedence	AF11 (10)	AF21 (18)	AF31 (26)	AF41 (34)
Medium Drop Precedence	AF12 (12)	AF22 (20)	AF32 (28)	AF42 (36)
High Drop Precedence	AF13 (14)	AF23 (22)	AF33 (30)	AF43 (38)

18.2.2 Policy Route Command Example

The following commands create two address objects (TW_SUBNET and GW_1) and insert a policy that routes the packets (with the source IP address TW_SUBNET and any destination IP address) through the

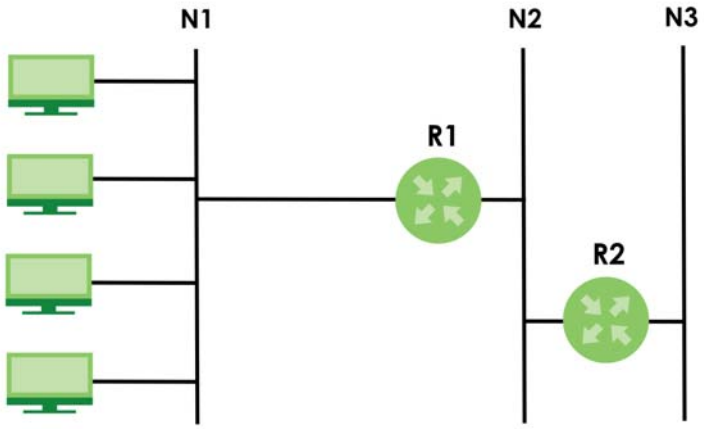
interface ge1 to the next-hop router GW_1. This route uses the IP address of the outgoing interface as the matched packets' source IP address.

```
Router(config)# address-object TW_SUBNET 192.168.2.0 255.255.255.0
Router(config)# address-object GW_1 192.168.2.250
Router(config)# policy insert 1
Router(policy-route)# description example
Router(policy-route)# destination any
Router(policy-route)# interface ge1
Router(policy-route)# next-hop gateway GW_1
Router(policy-route)# snat outgoing-interface
Router(policy-route)# source TW_SUBNET
Router(policy-route)# exit
Router(config)# show policy-route 1
index: 1
  active: yes
  auto-disable: no
  description: example
  user: any
  schedule: none
  interface: ge1
  tunnel: none
  sslvpn: none
  source: TW_SUBNET
  destination: any
  DSCP code: any
  service: any
  srcport: any
  nexthop type: Gateway
  nexthop: GW_1
  nexthop state: Not support
  auto destination: no
  SNAT: outgoing-interface
  DSCP marking: preserve
  connectivity-check: no
Router(config)#
```

18.3 IP Static Route

The Zyxel Device has no knowledge of the networks beyond the network that is directly connected to the Zyxel Device. For instance, the Zyxel Device knows about network N2 in the following figure through gateway R1. However, the Zyxel Device is unable to route a packet to network N3 because it doesn't know that there is a route through the same gateway R1 (via gateway R2). The static routes are for you to tell the Zyxel Device about the networks beyond the network connected to the Zyxel Device directly.

Figure 17 Example of Static Routing Topology



18.4 Static Route Commands

The following table describes the commands available for static route. You must use the `configure terminal` command to enter the configuration mode before you can use these commands. See Section Table 81 on page 167 for information on input values.

Table 84 Command Summary: Static Route

COMMAND	DESCRIPTION
`[no] ip route {w.x.y.z} {w.x.y.z} {interface|w.x.y.z} <0..127>`	Sets a static route. The no command deletes a static route.
`ip route replace {w.x.y.z} {w.x.y.z} {interface|w.x.y.z} <0..127> with {w.x.y.z} {w.x.y.z} {interface|w.x.y.z} <0..127>`	Changes an existing route's settings.
`show ip route-settings`	Displays static route information. Use `show ip route` to see learned route information. See Section 19.2.5 on page 179.
`ip6 route destv6/prefix { ipv6_global_address | ipv6_link_local | interface} [<0..127>]`	Sets an IPv6 static route.
`ip6 route destv6/prefix { ipv6_link_local interface} [<0..127>]`	Sets an IPv6 link local static route.
`no ip6 route destv6/prefix { gatewayv6 | interface} [<0..127>]`	Deletes the specified IPv6 static route.
`ip6 route replace destv6/prefix { gatewayv6 | interface} [<0..127>] with destv6/prefix { gatewayv6 | interface} [<0..127>]`	Changes an existing IPv6 route's settings.
`[no] ip route control-virtual-server-rules activate`	Gives static routes priority over NAT virtual server rules (1-1 SNAT). It also automatically gives policy routes priority over NAT virtual server rules. Use the no command to give NAT virtual server rules priority over static routes.
`show ip route control-virtual-server-rules`	Displays whether or not static routes have priority over NAT virtual server rules (1-1 SNAT).

18.4.1 Static Route Commands Examples

The following command sets a static route with IP address 10.10.10.0 and subnet mask 255.255.255.0 and with the next-hop interface ge1. Then use the show command to display the setting.

```
Router(config)# ip route 10.10.10.0 255.255.255.0 ge1
Router(config)#
Router(config)# show ip route-settings
Route           Netmask         Nexthop         Metric
================================================================================
10.10.10.0      255.255.255.0   ge1             0
```

The following commands set and show three examples of static IPv6 routes for traffic destined for IPv6 addresses with prefix 2002:22:22:34::. The first route sends the traffic out through interface ge2 and uses metric 1. The second sends the traffic to gateway 2001:12::12 and uses metric 2. The third sends the traffic to the fe80::1:2 link local gateway on interface ge2 and uses metric 2.

```
Router(config)# ip6 route 2002:22:22:34::/64 ge2 1
Router(config)# ip6 route 2002:22:22:34::/64 2001:12::12 2
/* link-local gateway bind on interface */
Router(config)# ip6 route 2002:22:22:34::/64 fe80::1:2 ge2 2
Router(config)# show ip6 route-settings
No.  Route                                              Prefix Length
     Nexthop                                            Metric
================================================================================
1    2002:22:22:34::                                    64
     2001:12::12                                        2
     2002:22:22:34::                                    64
     ge2                                                1
2    2002:22:22:34::                                    64
     2001:12::12                                        2
3    2002:22:22:34::                                    64
     Fe80::1:2                                          2
```

The following command deletes a specific static IPv6 route.

```
Router(config)# no ip6 route 2002:22:22:34::/64 2001:12::12
```

The following command deletes all static IPv6 routes with the same prefix.

```
Router(config)# no ip6 route 2002:22:22:34::/64
```

CHAPTER 19
Routing Protocol

19.1 Routing Protocol Overview

Routing protocols give the Zyxel Device routing information about the network from other routers. The Zyxel Device then stores this routing information in the routing table, which it uses when it makes routing decisions. In turn, the Zyxel Device can also provide routing information via routing protocols to other routers.

The Zyxel Device supports two standards, RIP and OSPF, for routing protocols. RIP and OSPF are compared in Table 85 on page 176, and they are discussed further in the next two sections.

Table 85 OSPF vs. RIP

	OSPF	RIP
Network Size	Large	Small (with up to 15 routers)
Metric	Bandwidth, hop count, throughput, round trip time and reliability.	Hop count
Convergence	Fast	Slow

19.2 Routing Protocol Commands Summary

The following table describes the values required for many routing protocol commands. Other values are discussed with the corresponding commands.

Table 86 Input Values for Routing Protocol Commands

LABEL	DESCRIPTION
ip	The 32-bit name of the area or virtual link in IP address format.
authkey	The password for text or MD5 authentication. You may use alphanumeric characters or underscores(_). text password: 1-8 characters long MD5 password: 1-16 characters long

The following sections list the routing protocol commands.

19.2.1 RIP Commands

This table lists the commands for RIP.

Table 87 router Commands: RIP

COMMAND	DESCRIPTION
`router rip`	Enters sub-command mode.
`[no] network interface_name`	Enables RIP on the specified Ethernet interface. The no command disables RIP on the specified interface.
`[no] redistribute {static | ospf}`	Enables redistribution of routing information learned from the specified source. The no command disables redistribution from the specified source.
`redistribute {static | ospf} metric <0..16>`	Sets the metric when redistributing routing information learned from the specified source.
`[no] version <1..2>`	Sets the default RIP version for all interfaces with RIP enabled. If the interface RIP version is blank, the interface uses the default version. This is not available in the GUI. The no command sets the default RIP version to 2.
`[no] passive-interface interface_name`	Sets the direction to “In-Only” for the specified interface. The no command sets the direction to bi-directional.
`[no] authentication mode {md5 | text}`	Sets the authentication mode for RIP. The no command sets the authentication mode to “none”.
`[no] authentication string authkey`	Sets the password for text authentication. The no command clears the password.
`authentication key <1..255> key-string authkey`	Sets the MD5 ID and password for MD5 authentication.
`no authentication key`	Clears the MD5 ID and password.
`[no] outonly-interface interface_name`	Sets the direction to “Out-Only” for the specified interface. The no command sets the direction to “BiDir”.
`encrypted-string ciphertext`	Sets the cipher to encrypt the string.

19.2.2 General OSPF Commands

This table lists the commands for general OSPF configuration.

Table 88 router Commands: General OSPF Configuration

COMMAND	DESCRIPTION
`router ospf`	Enters sub-command mode.
`[no] redistribute {static | rip}`	Enables redistribution of routing information learned from the specified non-OSPF source. The no command disables redistribution from the specified non-OSPF source.
`[no] redistribute {static | rip} metric-type <1..2> metric <0..16777214>`	Sets the metric for routing information learned from the specified non-OSPF source. The no command clears the metric.
`[no] passive-interface interface_name`	Sets the direction to “In-Only” for the specified interface. The no command sets the direction to “BiDir”.
`[no] router-id IP`	Sets the 32-bit ID (in IP address format) of the Zyxel Device. The no command resets it to “default”, or the highest available IP address.

19.2.3 OSPF Area Commands

This table lists the commands for OSPF areas.

Table 89 router Commands: OSPF Areas

COMMAND	DESCRIPTION
`router ospf`	Enters sub-command mode.
`[no] network interface area IP`	Adds the specified interface to the specified area. The no command removes the specified interface from the specified area.
`[no] area IP [{stub | nssa}]`	Creates the specified area and sets it to the indicated type. The no command removes the area.
`[no] area IP authentication`	Enables text authentication in the specified area. The no command disables authentication in the specified area.
`[no] area IP authentication message-digest`	Enables MD5 authentication in the specified area. The no command disables authentication in the specified area.
`[no] area IP authentication authentication-key authkey`	Sets the password for text authentication in the specified area. The no command clears the password.
`[no] area IP authentication message-digest-key <1..255> md5 authkey`	Sets the MD5 ID and password for MD5 authentication in the specified area. The no command clears the MD5 ID and password.

19.2.4 Virtual Link Commands

This table lists the commands for virtual links in OSPF areas.

Table 90 router Commands: Virtual Links in OSPF Areas

COMMAND	DESCRIPTION
`show ospf area IP virtual-link`	Displays information about virtual links for the specified area.
`router ospf`	
`[no] area IP virtual-link IP`	Creates the specified virtual link in the specified area. The no command removes the specified virtual link.
`[no] area IP virtual-link IP authentication`	Enables text authentication in the specified virtual link. The no command disables authentication in the specified virtual link.
`[no] area IP virtual-link IP authentication message-digest`	Enables MD5 authentication in the specified virtual link. The no command disables authentication in the specified virtual link.
`[no] area IP virtual-link IP authentication authentication-key authkey`	Sets the password for text authentication in the specified virtual link. The no command clears the password in the specified virtual link.
`[no] area IP virtual-link IP authentication message-digest-key <1..255> md5 authkey`	Sets the MD5 ID and password for MD5 authentication in the specified virtual link. The no command clears the MD5 ID and password in the specified virtual link.
`[no] area IP virtual-link IP authentication same-as-area`	Sets the virtual link's authentication method to the area's default authentication.
`[no] area IP virtual-link IP authentication-key authkey`	Sets the password for text authentication in the specified virtual link. The no command clears the password.
`[no] area IP virtual-link IP encrypted-authentication-key <ciphertext>`	Sets the ciphertext for text encryption in the specified virtual link. The no command clears the ciphertext.

Table 90 router Commands: Virtual Links in OSPF Areas (continued)

COMMAND	DESCRIPTION
area IP virtual-link IP message-digest-key <1..255> md5 *authkey*	Sets the MD5 ID and password for MD5 authentication in the specified virtual link.
area IP virtual-link IP message-digest-key <1..255> encrypted-authentication-key	Sets the MD5 ID in the specified virtual link
no area IP virtual-link IP message-digest-key <1..255>	Clears the MD5 ID in the specified virtual link.

19.2.5 Learned Routing Information Commands

This table lists the commands to look at learned routing information.

Table 91 ip route Commands: Learned Routing Information

COMMAND	DESCRIPTION
show ip route [kernel | connected | static | ospf | rip | bgp]	Displays learned routing and other routing information.

19.2.6 Show IP Route Command Example

The following example shows learned routing information on the Zyxel Device.

```
Router> show ip route
Flags: A - Activated route, S - Static route, C - directly Connected
       O - OSPF derived, R - RIP derived, G - selected Gateway
       ! - reject, B - Black hole, L - Loop

IP Address/Netmask    Gateway          IFace           Metric    Flags
Persist
================================================================================
0.0.0.0/0             172.16.1.254     wan1            0         ASG       -
10.59.0.0/24          0.0.0.0          ext-wlan        0         ACG       -
127.0.0.0/8           0.0.0.0          lo              0         ACG       -
172.16.1.0/24         0.0.0.0          wan1            0         ACG       -
192.168.1.0/24        0.0.0.0          lan1            0         ACG       -
192.168.2.0/24        0.0.0.0          lan2            0         ACG       -
192.168.3.0/24        0.0.0.0          dmz             0         ACG       -
```

19.3 BGP (Border Gateway Protocol)

The Zyxel Device supports eBGP (exterior Border Gate Protocol) to route IPv4 traffic between routers in different Autonomous Systems (AS). An AS number is a number from 1 to 4294967295), that identifies an autonomous system. 4200000000 – 4294967294 are private AS numbers.

You must first allow BGP packets to enter the Zyxel Device from the WAN using the following commands.

```
Router(config)# object-group service  Default_Allow_WAN_To_ZyWALL
Router(group-service)# description System Default Allow From WAN To ZyWALL
Router(group-service)# service-object BGP
Router(group-service)# exit
Router(config)# show object-group
Router(config)# show object-group service
Group name                      Reference           Family
Description
================================================================================
CU-SEEME                        0                   Common

DNS                             3                   Common

IRC                             0                   Common

NetBIOS                         2                   Common

ROADRUNNER                      0                   Common

RTSP                            0                   Common

SNMP                            0                   Common

SNMP-TRAPS                      0                   Common

SSH                             0                   Common

Default_Allow_ICMPv6_Group      1                   V6
Default Allow icmpv6 to ZyWALL
Default_Allow_WAN_To_ZyWALL     1                   Common
System Default Allow From WAN To ZyWALL
Default_Allow_DMZ_To_ZyWALL     1                   Common
System Default Allow From DMZ To ZyWALL
Default_Allow_v6_WAN_To_ZyWALL  1                   Common
System Default Allow IPv6 Form WAN To ZyWALL
Default_Allow_v6_DMZ_To_ZyWALL  1                   Common
System Default Allow IPv6 From DMZ to ZyWALL
DHCPv6                          0                   Common

Default_Allow_v6_any_to_ZyWALL  1                   V6
System Default Allow IPv6 From any To ZyWALL
Router(config)#
```

19.3.1 BGP Commands

This table lists the commands for BGP configuration.

Table 92 bgp Commands

COMMAND	DESCRIPTION
`router bgp`	Enters router sub-command mode.
`[no] as-number <1..4294967295>`	Sets the AS number from 1 to 4294967295 in this field. Get the number from your service provider. The Zyxel Device can only belong to one AS at a time. The no command clears the AS number.
`[no] network ipv4_cidr`	Add routes that will be announced to all BGP neighbors. You may configure up to 16 network routes. *ipv4_cidr:* IPv4 subnet in CIDR format, i.e. 192.168.1.0/32 <W.X.Y.Z>/<1..32> The no command clears the network.
`[no] redistribute connected`	Redistributes routes of directly attached devices to the Zyxel Device into the BGP Routing Information Base (RIB) The no command clears the RIB.
`[no] router-id router-id`	Sets the IP address of the interface on the Zyxel Device. This field is optional. The no command clears the router ID.
`quit`	Leaves sub-command mode.
`exit`	Leaves sub-command mode.
`[no] neighbor ipv4`	Sets the IPv4 address of the peer BGP router in a neighboring AS. *ipv4*: IPv4 address <W.X.Y.Z> The no command clears the IPv4 address of the peer BGP router.
`[no] neighbor ipv4 description description`	Sets a neighbor description to identify the neighbor. The no command clears the neighbor description.
`[no] neighbor ipv4 remote-as <1..4294967295>`	Sets the AS number of the neighboring AS. The no command clears the neighbor AS number.
`[no] neighbor ipv4 weight <1..65535>`	Specifies a weight value for all routes learned from this peer BGP router in the specified network. The route with the highest weight gets preference. The no command clears the weight.
`[no] neighbor ipv4 ebgp-multihop hops <1..255>`	Sets the maximum hop count that the Zyxel Device can attempt for BGP connections to external peers on indirectly connected networks. eBGP neighbors must also perform multihop. Multihop is not established if the only route to the multihop peer is a default route. This avoids loop formation. The no command forbids the Zyxel Device from attempting BGP connections to external peers on indirectly connected networks.
`[no] maximum-paths <1..255>`	Sets the maximum number of paths allowed to a peer BGP router in a neighboring AS. The no command clears the maximum paths.

Table 92 bgp Commands (continued)

COMMAND	DESCRIPTION
`[no] neighbor ipv4 timers < 0..65535> < 0..65535>`	Sets the interval between each Keepalive message sent by the Zyxel Device and the maximum time the Zyxel Device waits to receive a Keepalive message from a peer BGP router before it declares that the peer BGP router is dead. The interval should be less than the wait time. The no command clears the timers.
`[no] neighbor ipv4 connect-retry`	Sets the number of times the Zyxel Device tries to connect to a peer BGP router before it declares that the peer BGP router is dead. The no command clears the setting.
`[no] neighbor ipv4 maximum-prefix < 1..4294967295 >`	Sets the maximum number of prefixes, from 1 to 4294967295, of prefixes that can be received from a neighbor. A prefix is a network address (IP/subnet mask) that a BGP router can reach and that it shares with its neighbors. This limits the number of prefixes that the Zyxel Device is allowed to receive from a neighbor. If extra prefixes are received, the Zyxel Device ends the connection with the peer BGP router. You need to edit the peer BGP router configuration to bring the connection back. The no command clears the maximum number of prefixes.
`[no] neighbor ipv4 ttl-security [hops] <1..254>`	Sets the maximum number of hops (1 to 254) between the Zyxel Device and a peer BGP router. The Zyxel Device will only accept incoming IP packets with a TTL value that is equal to or greater than the expected value. If the hop count is 3, then the expected incoming TTL value is at least 252, which is 255 minus the TTL value of 3. The Zyxel Device will only accept incoming IP packets from a peer BGP router if it is up to 3 hops away. The no command clears the hop count.
`[no] neighbor ipv4 default-originate`	Allows the Zyxel Device to send the default route 0.0.0.0 to peer BGP router for use as a default route. The no command sends no route as a default.
`[no] neighbor ipv4 password password`	Sets a default password for MD5 authentication of communication between the Zyxel Device and the peer BGP router. The password can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long. The no command clears the password.
`[no] neighbor ipv4 update-source [ipv4|interface_name]`	Allows BGP sessions to use the specified Zyxel Device gateway IP address or Zyxel Device interface for TCP connections. The no command clears the interface.
`show bgp [global |neighbor]`	Displays configured BGP Zyxel Device and peer router settings.
`show bgp [summary | route | mem]`	Displays BGP run time route and memory status.
`show ip bgp neighbor ipv4 [advertised-routes | prefix-counts | routes]`	Displays route information to the specified peer BGP router.
`show ip route bgp`	Displays IP Address/Netmask, gateway, interface, metric, flags and persist information.

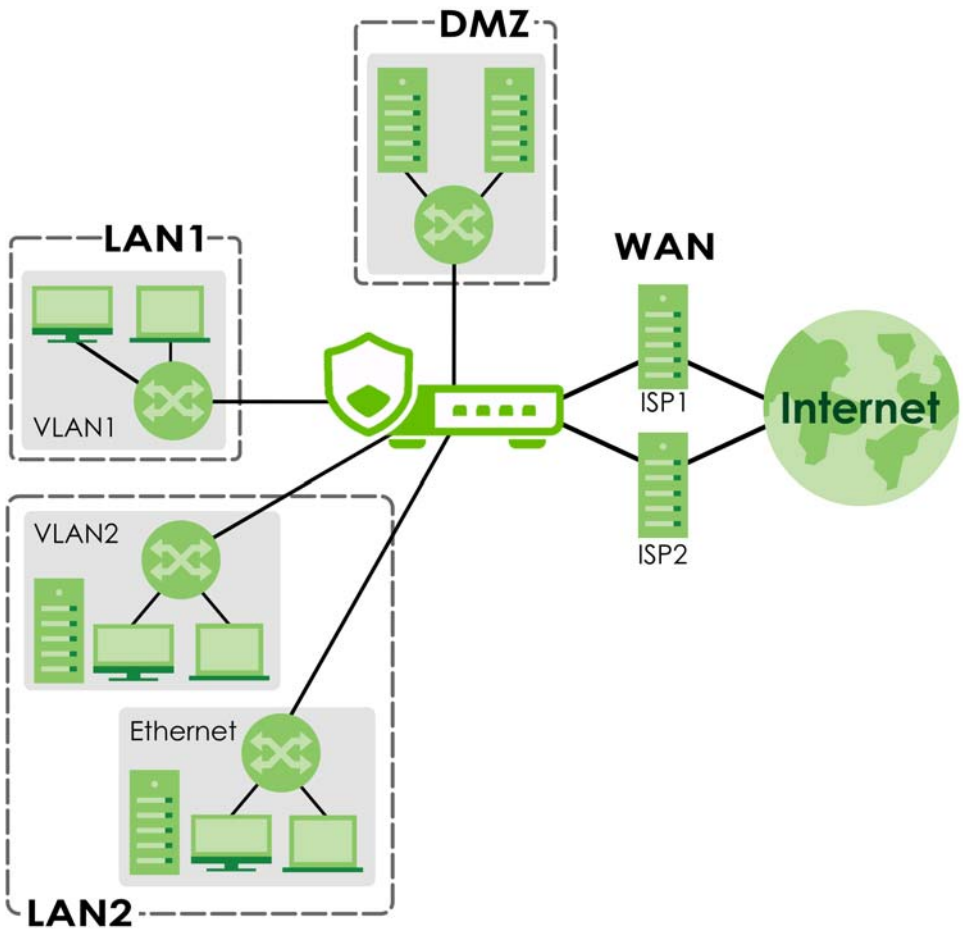
CHAPTER 20
Zones

20.1 Zones Overview

A zone is a group of interfaces and VPN tunnels. The Zyxel Device uses zones, not interfaces, in many security and policy settings, such as firewall rules and remote management.

Zones cannot overlap. Each Ethernet interface, VLAN interface, bridge interface, PPPoE/PPTP interface, and VPN tunnel can be assigned to at most one zone. Virtual interfaces are automatically assigned to the same zone as the interface on which they run.

Figure 18 Example: Zones



20.2 Zone Commands Summary

The following table describes the values required for many zone commands. Other values are discussed with the corresponding commands.

Table 93 Input Values for Zone Commands

LABEL	DESCRIPTION
profile_name	The name of a zone, or the name of a VPN tunnel. For some Zyxel Device models, use up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive. For other Zyxel Devicemodels: • The lan1 interface always belongs to the LAN1 zone. • The lan2 interface always belongs to the LAN2 zone. • The dmz interface always belongs to the DMZ zone. • The wan1, wan2, wan1_ppp, or wan2_ppp interfaces always belong to the WAN zone. • An opt_ppp interface can be added to the WAN or OPT zone.

This table lists the zone commands.

Table 94 zone Commands

COMMAND	DESCRIPTION
`show zone [`*profile_name*`]`	Displays information about the specified zone or about all zones.
`show zone binding-iface`	Displays each interface and zone mappings.
`show zone default-binding`	Displays the pre-configured interface and zone mappings that come with the Zyxel Device.
`show zone none-binding`	Displays the interfaces, tunnels and SSL VPNs that are not associated with a zone yet.
`show zone system-default`	Displays the pre-configured default zones that you cannot delete from the Zyxel Device.
`show zone user-define`	Displays all customized zones.
`[no] zone` *profile_name*	Creates the zone if necessary and enters sub-command mode. The no command deletes the zone.
`zone` *profile_name*	Enter the sub-command mode.
`[no] interface` *interface_name*	Adds the specified interface to the specified zone. The no command removes the specified interface from the specified zone. See Section 16.2 on page 118 for information about interface names.
`[no] crypto` *profile_name*	Adds the specified IPSec VPN tunnel to the specified zone. The no command removes the specified IPSec VPN tunnel from the specified zone.
`[no] sslvpn` *profile_name*	Adds the specified SSL VPN tunnel to the specified zone. The no command removes the specified SSL VPN tunnel from the specified zone.

20.2.1 Zone Command Examples

The following commands add Ethernet interfaces ge1 and ge2 to zone A.

```
Router# configure terminal
Router(config)# zone A
Router(zone)# interface ge1
Router(zone)# interface ge2
Router(zone)# exit
Router(config)# show zone
No. Name                              Member
================================================================================
1   A                                 ge1,ge2
Router(config)# show zone A
No. Type                             Member
================================================================================
1   interface                        ge1
2   interface                        ge2
```

CHAPTER 21
DDNS

21.1 DDNS Overview

DNS maps a domain name to a corresponding IP address and vice versa. Similarly, dynamic DNS maps a domain name to a dynamic IP address. As a result, anyone can use the domain name to contact you (in NetMeeting, CU-SeeMe, etc.) or to access your FTP server or Web site, regardless of the current IP address.

Note: You must have a public WAN IP address to use Dynamic DNS.

Set up a dynamic DNS account with a supported DNS service provider to be able to use Dynamic DNS services with the Zyxel Device. When registration is complete, the DNS service provider gives you a password or key. At the time of writing, the Zyxel Device supports the following DNS service providers. See the listed websites for details about the DNS services offered by each.

Table 95 Network > DDNS

DDNS SERVICE PROVIDER	SERVICE TYPES SUPPORTED	WEBSITE	NOTES
DynDNS	Dynamic DNS, Static DNS, and Custom DNS	www.dyndns.com)	
Dynu	Basic, Premium	www.dynu.com	
No-IP	No-IP	www.no-ip.com	
Peanut Hull	Peanut Hull	www.oray.cn	Chinese website
3322	DynamicDNS, StaticDNS	www.3322.org	Chinese website
Selfhost	Selfhost	selfhoost.de	German website

Note: Record your DDNS account's user name, password, and domain name to use to configure the Zyxel Device.

After, you configure the Zyxel Device, it automatically sends updated IP addresses to the DDNS service provider, which helps redirect traffic accordingly.

21.2 DDNS Commands Summary

The following table describes the values required for many DDNS commands. Other values are discussed with the corresponding commands.

Table 96 Input Values for DDNS Commands

LABEL	DESCRIPTION
profile_name	The name of the DDNS profile. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

The following table lists the DDNS commands.

Table 97 ip ddns Commands

COMMAND	DESCRIPTION
`show ddns [profile_name]`	Displays information about the specified DDNS profile or about all DDNS profiles.
`show ddns-status`	Shows which DDNS profiles are active, inactive or have failed.
`[no] ip ddns profile profile_name`	Creates or edits the specified DDNS profile and enters sub-command mode if necessary. The no command deletes this profile.
`[no]https activate`	Encrypts traffic using SSL (port 443) to the DDNS server. Not all DDNS providers support this option. The no command disables HTTPS.
`[no] service-type {dyndns | dyndns_static | dyndns_custom | dynu-basic | dynu-premium | no-ip | peanut-hull | 3322-dyn | 3322-static | Selfhost | User custom}`	Sets the service type in the specified DDNS profile. The no command clears it.
`[no] username username password password`	Sets the username and password in the specified DDNS profile. The no command clears these fields. *username*: You can use up to 31 alphanumeric characters and the underscore (_). *password*: You can use up to 64 alphanumeric characters and the underscore (_).
`[no] host hostname`	Sets the domain name in the specified DDNS profile. The no command clears the domain name. *hostname*: You may up to 254 alphanumeric characters, dashes (-), or periods (.), but the first character must be alphanumeric.
`[no] ip-select {iface | auto | custom}`	Sets the IP address update policy in the specified DDNS profile. The no command clears the policy.
`[no] ip-select-backup {iface | auto | custom}`	Sets the alternate IP address update policy in the specified DDNS profile. The no command clears the policy.
`[no] custom ip`	Sets the static IP address in the specified DDNS profile. The no command clears it.
`[no] backup-custom ip`	Sets the static IP address for the backup interface in the specified DDNS profile. The no command clears it.
`[no] mx {ip | domain_name}`	Enables the mail exchanger and sets the fully-qualified domain name of the mail server to which mail from this domain name is forwarded. The no command disables the mail exchanger. *domain_name*: You may up to 254 alphanumeric characters, dashes (-), or periods (.), but the first character must be alphanumeric.
`[no] wan-iface interface_name`	Sets the WAN interface in the specified DDNS profile. The no command clears it.
`[no] backup-iface interface_name`	Sets the backup WAN interface in the specified DDNS profile. The no command clears it.
`[no] ha-iface interface_name`	Sets the HA interface in the specified DDNS profile. The no command clears it.
`[no] backmx`	Enables the backup mail exchanger. The no command disables it.
`[no] wildcard`	Enables the wildcard feature. The no command disables it.

Table 97 ip ddns Commands (continued)

COMMAND	DESCRIPTION
[no] url {URL TEXT}	Type the URL that can be used to access the server that will host the DDSN service. For example, # url /api/dynamic/update.php?hostname=home.example.com& ip=10.1.1.1 The no command disables it.
[no] ddns-server {FQDN DNS}	Type the IP address of the server that will host the DDSN service. For example, # ddns-server www.dnspark.net The no command disables it.
[no] additional-ddns-options	Avaialable for User custom. Enter one ofg the following. • --ip_server_name which should be the URL to get the server's public IP address - for example, http://myip.easylife.tw/ • --dyndns_system to specify the DYNDNS Server type - for example, dyndns@dyndns.org

21.3 DDNS Commands Example

The following example sets up a DDNS profile where the interface is wan1 and uses HTTP..

```
Router# configure terminal
Router(config)# ip ddns profile bbb
# activate
# service-type user-custom
# username yjyeh001 password xxxxxx
# host yjye007.dyndns.org
# wan-iface wan1
# url /nic/update?
# ddns-server members.dyndns.org
# additional-ddns-options --dyndns_system dyndns@dyndns.org
```

CHAPTER 22
Virtual Servers

22.1 Virtual Server Overview

This chapter describes how to set up, manage, and remove virtual servers.

Virtual servers are computers on a private network behind the Zyxel Device that you want to make available outside the private network. If the Zyxel Device has only one public IP address, you can make the computers in the private network available by using ports to forward packets to the appropriate private IP address.

Note: Virtual server is also known as port forwarding or port translation.

22.1.1 1:1 NAT and Many 1:1 NAT

1:1 NAT - If the private network server will initiate sessions to the outside clients, use 1:1 NAT to have the Zyxel Device translate the source IP address of the server's outgoing traffic to the same public IP address that the outside clients use to access the server.

Many 1:1 NAT - If you have a range of private network servers that will initiate sessions to the outside clients and a range of public IP addresses, use many 1:1 NAT to have the Zyxel Device translate the source IP address of each server's outgoing traffic to the same one of the public IP addresses that the outside clients use to access the server. The private and public ranges must have the same number of IP addresses.

One many 1:1 NAT rule works like multiple 1:1 NAT rules, but it eases the configuration effort since you only create one rule.

22.2 Virtual Server Commands Summary

The following table describes the values required for many virtual server commands. Other values are discussed with the corresponding commands .

Table 98 Input Values for Virtual Server Commands

LABEL	DESCRIPTION
service_object	The name of a service. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
profile_name	The name of the virtual server. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

The following table lists the virtual server commands

Note: If you create a NAT rule using the IP address of the Web Configurator and set the external port to 80 or 443, the rule will conflict with the Zyxel Device's default HTTP server port. You will not be able to access the Web Configurator through this interface..

Table 99 ip virtual-server Commands

COMMAND	DESCRIPTION
`show ip virtual-server [profile_name]`	Displays information about the specified virtual server or about all the virtual servers.
`no ip virtual-server profile_name`	Deletes the specified virtual server.
`ip virtual-server profile_name interface interface_name source-ip {any | IPv4 | address-object} original-ip {any | ip | address_object} map-to {address_object | ip} map-type any [nat-loopback [nat-1-1-map] [deactivate] | nat-1-1-map [deactivate] | deactivate]`	Creates or modifies the specified virtual server and maps the specified destination IP address (for all destination ports) to the specified destination address object or IP address. The original destination IP is defined by the specified interface (any), the specified IP address (IP), or the specified address object (*address-object*). NAT loopback allows local users to use a domain name to access this virtual server. The source IP is the source IP address of the incoming packets. The original destination IP is defined by the specified interface (any), the specified IP address (IP), or the specified address object (*address-object*). NAT loopback allows local users to use a domain name to access this virtual server. Select what kind of NAT this rule is to perform. `nat-1-1-map`: means the NAT type is either 1:1 NAT or many 1:1 NAT. See Section 22.1.1 on page 189 for more information. Using this command without `nat-1-1-map` means the NAT type is Virtual Server. This makes computers on a private network behind the Zyxel Device available to a public network outside the Zyxel Device (like the Internet). The `deactivate` command disables the virtual server rule.
`ip virtual-server profile_name interface interface_name original-ip {any | IP | address_object} map-to {address_object | ip} map-type port protocol {any | tcp | udp} original-port <1..65535> mapped-port <1..65535> [nat-loopback [nat-1-1-map] [deactivate] | nat-1-1-map [deactivate] | deactivate]`	Creates or modifies the specified virtual server and maps the specified (destination IP address, protocol, and destination port) to the specified (destination IP address and destination port). The original destination IP is defined by the specified interface (any), the specified IP address (IP), or the specified address object (*address-object*). NAT loopback allows local users to use a domain name to access this virtual server. `nat-1-1-map`: means the NAT type is either 1:1 NAT or many 1:1 NAT. See Section 22.1.1 on page 189 for more information. Using this command without `nat-1-1-map` means the NAT type is Virtual Server. This makes computers on a private network behind the Zyxel Device available to a public network outside the Zyxel Device (like the Internet). The `deactivate` command disables the virtual server rule.
`ip virtual-server profile_name interface interface_name original-ip {any | IP | address_object} map-to {address_object | ip} map-type ports protocol {any | tcp | udp} original-port-begin <1..65535> original-port-end <1..65535> mapped-port-begin <1..65535> [nat-loopback [nat-1-1-map] [deactivate] | nat-1-1-map [deactivate] | deactivate]`	Creates or modifies the specified virtual server and maps the specified (destination IP address, protocol, and range of destination ports) to the specified (destination IP address and range of destination ports). The original destination IP is defined by the specified interface (any), the specified IP address (IP), or the specified address object (*address-object*). NAT loopback allows local users to use a domain name to access this virtual server. `nat-1-1-map`: means the NAT type is either 1:1 NAT or many 1:1 NAT. See Section 22.1.1 on page 189 for more information. Using this command without `nat-1-1-map` means the NAT type is Virtual Server. This makes computers on a private network behind the Zyxel Device available to a public network outside the Zyxel Device (like the Internet). The `deactivate` command disables the virtual server rule.

Table 99 ip virtual-server Commands (continued)

COMMAND	DESCRIPTION
`ip virtual-server` *`profile_name`* `interface` *`interface_name`* `original-ip {any | IP |` *`address_object`*`} map-to {`*`address_object`* `|` *`ip`*`} map-type original-service` *`service_object`* `mapped-service` *`service_object`* `[nat-loopback [nat-1-1-map] [deactivate] | nat-1-1-map [deactivate] | deactivate]`	Creates or modifies the specified virtual server and maps the specified (destination IP address, protocol, and service object) to the specified (destination IP address and service object). The original destination IP is defined by the specified interface (any), the specified IP address (IP), or the specified address object (*`address-object`*). NAT loopback allows local users to use a domain name to access this virtual server. `nat-1-1-map`: means the NAT type is either 1:1 NAT or many 1:1 NAT. See Section 22.1.1 on page 189 for more information. Using this command without `nat-1-1-map` means the NAT type is Virtual Server. This makes computers on a private network behind the Zyxel Device available to a public network outside the Zyxel Device (like the Internet). The `deactivate` command disables the virtual server rule.
`ip virtual-server {activate | deactivate}` *`profile_name`*	Activates or deactivates the specified virtual server.
`ip virtual-server delete` *`profile_name`*	Deletes the specified virtual server.
`ip virtual-server flush`	Deletes all virtual servers.
`ip virtual-server rename` *`profile_name profile_name`*	Renames the specified virtual server from the first *`profile_name`* to the second *`profile_name`*.

22.2.1 Virtual Server Command Examples

The following command creates virtual server WAN-LAN_H323 on the wan1 interface that maps IP addresses 10.0.0.8 to 192.168.1.56. for TCP protocol traffic on port 1720. It also adds a NAT loopback entry.

```
Router# configure terminal
Router(config)# ip virtual-server WAN-LAN_H323 interface wan1 original-ip
10.0.0.8 map-to 192.168.1.56 map-type port protocol tcp original-port 1720
mapped-port 1720 nat-loopback
Router(config)#
```

The following command shows information about all the virtual servers in the Zyxel Device.

```
Router(config)# show ip virtual-server
virtual server: WAN-LAN_H323
  Index: 1
  active: yes
  interface: wan1
  NAT-loopback active: yes
  NAT 1-1: no
  original IP: 10.0.0.8
  mapped IP: 192.168.1.56
  mapping type: port
  protocol type: tcp
  original service:
  mapped service:
  original start port: 1720
  original end port:
  mapped start port: 1720
  mapped end port:
Router(config)#
```

22.2.2 Tutorial - How to Allow Public Access to a Server

This is an example of making an HTTP (web) server in the DMZ zone accessible from the Internet (the WAN zone). You will use a public IP address of 1.1.1.2 on the ge2 (or wan1 on some models) interface and map it to the HTTP server's private IP address of 192.168.3.7.

Figure 19 Public Server Example Network Topology

Follow the following steps for the setting.

1 Configure Address object

Create two address objects. One is named DMZ_HTTP for the HTTP server's private IP address of 192.168.3.7. The other one is named ge2_HTTP for the ge2 (wan1) public IP address of 1.1.1.2.

```
Router# configure terminal
Router(config)# address-object DMZ_HTTP 192.168.3.7
Router(config)# address-object ge2_HTTP 1.1.1.2
Router(config)#
```

2 Configure NAT

You need a NAT rule to send HTTP traffic coming to IP address 1.1.1.2 on ge2 (wan1) to the HTTP server's private IP address of 192.168.3.7. Use the following settings:

- This NAT rule is for any HTTP traffic coming in on ge2 (wan1) to IP address 1.1.1.2.
- The NAT rule sends this traffic to the HTTP server's private IP address of 192.168.3.7 (defined in the DMZ_HTTP object).

- HTTP traffic and the HTTP server in this example both use TCP port 80. So you set the port mapping type to “port”, the protocol type to “TCP”, and the original and mapped ports to “80”.

```
Router(config)# ip virtual-server To-VirtualServer-WWW interface ge2
original-ip ge2_HTTP map-to DMZ_HTTP map-type port protocol tcp original-
port 80 mapped-port 80
Router(config)#
```

3 Configure secure policy rule.

Create a firewall rule to allow HTTP traffic from the WAN zone to the DMZ web server.

```
Router(config)# secure-policy insert 1
Router(secure-policy)# description To-VirtualServer-WWW
Router(secure-policy)# from WAN
Router(secure-policy)# to DMZ
Router(secure-policy)# destinationip DMZ_HTTP
Router(secure-policy)# service HTTP
Router(secure-policy)# exit
Router(config)# write
Router(config)#
```

Now the public can go to IP address 1.1.1.2 to access the HTTP server.

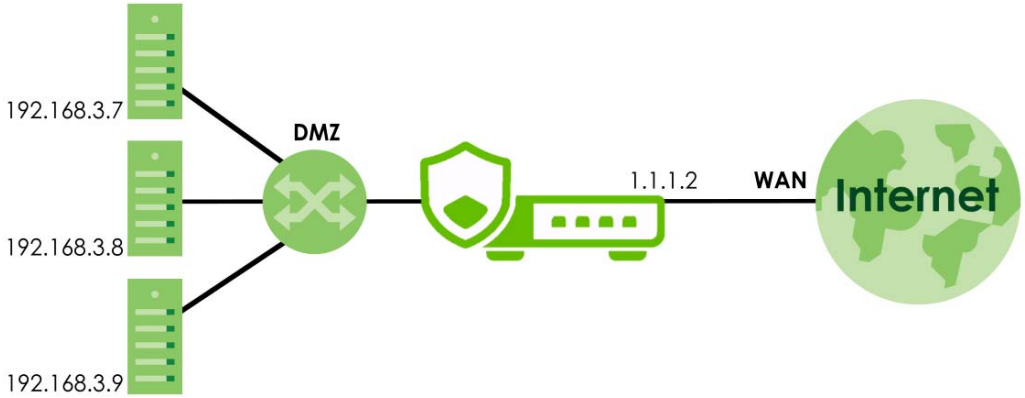
22.3 Virtual Server Load Balancing

Virtual Server Load balancing allows the Zyxel Device to distribute virtual server connection requests between multiple real (physical) servers. This helps reduce each server’s workload and to decrease virtual server response times.

22.3.1 Load Balancing Example 1

You are hosting a very popular website on your network, which attracts a lot of traffic and causes problems with your web server. To resolve this, you set up three identical web servers on the DMZ behind the Zyxel Device (Figure 20 on page 193). The Zyxel Device then distributes incoming requests between the three servers. Clients only see one virtual web server with IP address 1.1.1.2.

Figure 20 Virtual Server with Three Real Servers

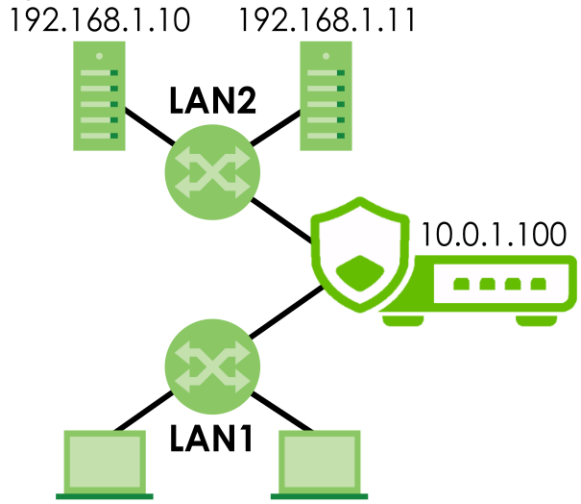


22.3.2 Load Balancing Example 2

You have two internal networks, LAN 1 and LAN 2, that are restricted from accessing each other (Figure 21 on page 194). LAN 2 hosts two duplicate SMTP mail servers. You want clients on LAN 1 to be able to access the SMTP servers on LAN 2.

You create a virtual server load balancing rule using IP address 10.0.1.100 and port 25, and add two SMTP servers from LAN 2 to the rule. Now clients on LAN 1 can access the virtual server's SMTP service by connecting to 10.0.1.100 port 25. Clients see a single mail server.

Figure 21 Virtual Server on LAN



22.3.3 Virtual Server Load Balancing Process

The following gives of an overview of how the Virtual Server Load Balancing process works.

Figure 22 Load Balancing Overview

1 A client connects to the Zyxel Device on IPv4 address 1.1.1.2 (the virtual server external IP address).

2 The Zyxel Device matches the connection request to a set of real servers (1, 2, and 3 in Figure 22 on page 194), and then determines which server will handle the request using a user-specified load balancing algorithm.

3 The Zyxel Device forwards the request to the chosen server using NAT.

4 The server processes the request, and then replies to the Zyxel Device.

5 The Zyxel Device forwards the reply to the client using SNAT.

22.3.4 Load Balancing Rules

In order to use load balancing, you must create a load balancing rule. Each load balancing rule consists of an incoming interface, an external IP address, a service type, a load balancing algorithm, and a list of real servers.

Note: One real server can belong to multiple load-balancing rules.

Note: You can only add one interface, IP address, and port to each load balancing rule.

Note: Virtual servers and real servers only support IPv4.

Only certain Zyxel Device models support virtual server load balancing. There are also limits on the maximum number of rules and real servers per Zyxel Device.

Table 100 Virtual Service Load Balancing Limits

PARAMETER	MODEL	LIMIT
Maximum Number of Load Balancing Rules per Zyxel Device	VPN50, USG FLEX 100, USG FLEX 100W, ATP100, ATP100W	5
	VPN100, USG FLEX 200, ATP200	10
	VPN300, USG FLEX 500, ATP500, USG FLEX 700, ATP700, ATP800, VPN1000	20
Maximum Number of Real Servers Per Load Balancing Rule	All of the above models	4

22.3.5 Virtual Server Load Balancing Algorithms

A rule's load balancing algorithm determines which real server is assigned to an incoming connection request. When creating a load balancing rule, you can assign each server a weight, which indicates the server's processing capacity compared to other servers.

Table 101 Virtual Server Load Balancing Algorithms

ALGORITHM	DESCRIPTION
Round-Robin	The Zyxel Device assigns servers in the reverse order they were added to the rule (Last In First Out). All servers are considered equal, regardless of their weight and current number of connections. For example, if you have three servers, A, B, C and nine requests, the servers are assigned in the following order: CBACBACBA.
Weighted Round-Robin	The Zyxel Device assigns servers based on a user-specified weight. Servers with a higher weight are assigned before servers with a lower weight. Each time a server is assigned a request, the server's weight decreases by one point until it finishes processing the request. The Zyxel Device assigns servers with equal weight in the reverse order they were added to the rule (Last In First Out). Servers with zero connections are given priority over all other servers. For example, if you have three servers A, B, C with weights 4, 3, 2 and nine requests, the servers are assigned in the following order: CBAABACBA. C (Weights: A4, B3, C2) CB (Weights: A4, B3, C1) CBA (Weights: A3, B2, C1) CBAA (Weights: A2, B2, C1) CBAAB (Weights: A2, B1, C1) CBAABA (Weights: A1, B1, C1) CBAABAC (Weights: A1, B1, C0) CBAABACB (Weights: A1, B0, C0) CBAABACBA (Weights: A0, B0, C0)
Least-Connection	The Zyxel Device assigns the server with the least number of current connections.
Source Hashing / Source IP	The Zyxel Device assigns a server by checking a static hash table, which permanently maps each client IP address to a specific real server. Servers are mapped to new client IP addresses in the reverse order the servers were added to the rule (Last In First Out). Each server is added N times during each sequence, where N is equal to the server's weight. For example, if you have two servers A, and B, with weights 1 and 2, the servers are mapped to new client IP addresses in the hash table in the following order: Source_IP_Hash1 = Server B Source_IP_Hash2 = Server B Source_IP_Hash3 = Server A Source_IP_Hash4 = Server B Source_IP_Hash5 = Server B Source_IP_Hash6 = Server A

22.3.6 Virtual Server Load Balancing Commands

The following table describes the virtual server load balancing commands..

Table 102 Virtual Server Load Balancing Commands

Command	DESCRIPTION
`ip virtual-server load-balancer` *name*	Enters subcommand mode for the specified load balancing rule. If you rule does not currently exist, then the Zyxel Device creates the rule. The name must consist of 1–31 characters, and may contain letters, numbers, and the following special characters: - (hyphen), _ (underscore).
`[no] activate`	Enables or disables the load balancing rule.
`virtual-service interface` *interface_name* `external-ip {`*address*`|`*object*`} external-port` *port* `protocol {`*tcp*`|`*udp*`}]`	Links the load balancing rule to an incoming interface, an external IPv4 address, and a port. Incoming requests to the IP4 address and port are processing by the load balancing rule. *interface_name*: The name of a device interface, for example wan1. The interface must be one of the following types: Ethernet, VLAN, bridge, PPPoE/PPTP. *address*`|`*object*: The IPv4 address of the virtual server. You can enter the IP address manually, for example: 192.168.100.100, or you can enter the name of an IPv4 interface object. *port*: The TCP or UDP port to bind this rule to. Valid range is 1–65535.
`virtual-service interface` *interface_name* `external-ip {`*address*`|`*object*`} external-service` *service*	Links the load balancing rule to an incoming interface, an external IPv4 address, and a port. Incoming requests to the IP4 address and port are processing by the load balancing rule. *interface_name*: The name of a device interface, for example wan1. The interface must be one of the following types: Ethernet, VLAN, bridge, PPPoE/PPTP. *address*`|`*object*: An IPv4 address bound to the interface. You can enter the IP address manually, for example: 192.168.100.100, or you can enter the name of an IPv4 interface object. *service*: The name of a service object, for example SMTP. For details on creating service objects, see Chapter 53 on page 467.
`load-balance-algorithm {`*rr*`|`*wrr*`|`*lc*`|`*sh*`}`	Sets the load balancing algorithm for this rule. For information about each algorithm, see Section 22.3.5 on page 196. • *rr*: Round-Robin • *wrr*: Weighted Round-Robin • *lc*: Least-Connection • *sh*: Source Hashing
`persistence timeout` *1-86400*	Sets how long a client/server session with no activity stays open. Timeout is measured in seconds, and the default value is 360. Multiple requests from a client within a short time period are directed to the same real server, as part of a persistent client/server session. If there are no incoming requests from a client within the specified timeout period, then the persistent client/server session is closed. Further requests from the client might be assigned to a different real server, determined by the load balancing algorithm.

Table 102 Virtual Server Load Balancing Commands

Command	DESCRIPTION
persistence granularity *netmask*	Sets the scope of persistent sessions. The default netmask is 255.255.255.255. By default, the Zyxel Device creates persistent sessions between one client and one server. You can set a netmask to allow a range of clients to open a persistent session with a real server. For example, setting a netmask of 255.255.255.0 means all requests from clients on the subnet 192.168.1.x get directed to the same real server within the timeout period.
real-server *address* mapped-port *port* weight *weight* [hash *hash*]	Adds a real server to the load balancing rule. Note: The real server must offer the service specified when running the command `virtual-service interface`. *address*: IPv4 address of a server on the LAN. *port*: The port on the server that connection requests are forwarded to. *weight*: For algorithm Weighted Round Robin, weight represents the processing power of this server compared to other servers. A server with a weight of 2 is considered to be able to handle two times more connection requests than a server with a weight of 1. For algorithm Source Hashing, servers are mapped to source IP addresses in a hash table proportionally based on the server's weights. hash: An MD5 checksum of the webpage specified by `http path` *url*. The Zyxel Device uses this checksum to verify that each HTTP health check request returns the correct webpage, and not an error page.
no real-server *address*	Removes the real server from the set of servers managed by this rule.
[no] health-check activate	Enables or disables server health checks for this rule. When enabled, the Zyxel Device periodically sends a request to each real server. This request ensures that the server is available, and optionally ensures that a specific service on the server is running.
health-check type {*http* | *https* | *tcp* | *smtp* | *dns* | *ping*}	Sets the type of status request to send to each real server. For example, select HTTP and the Zyxel Device periodically sends an HTTP request to each real server, ensuring that the server is available and that its HTTP service is running. • HTTP: Web service • HTTPS: Secure web service • TCP: A general network protocol that shows the server is accepting TCP connections • SMTP: Mail service • DNS: Dynamic Name Service • PING: A general network protocol that shows the server is reachable
check-period *1-86400*	Sets the health check time interval, in seconds. The default is 60.
connect-timeout *1-300*	Sets the period of time in seconds that the Zyxel Device waits after sending a health check request before marking the health check as failed. The default is 5.
retry *1-99*	Sets the number of times the Zyxel Device resends a health check request before marking the server as unavailable. The default is 1.

Table 102 Virtual Server Load Balancing Commands

Command	DESCRIPTION
`http path url`	Sets the URL to request when the health check type is set to HTTP or HTTPS. Note: If an MD5 checksum is set for a real server, the Zyxel Device uses this checksum to verify that each HTTP health check request returns the correct webpage, and not an error page.
`host sni`	Sets the SNI to send to the real server when the health check type is set to HTTPS. A client sends a Server Name Indication (SNI) when they start an HTTPS session with the server. It allows multiple HTTPS sessions to the same IP address and port number with different certificates with different SNIs.
`[no] hash-auto`	Enables or disables auto-hashing. When enabled, the Zyxel Device sends a HTTP request to each real server, and then calculates and stores the MD5 checksum of the returned webpage. The Zyxel Device uses this checksum to verify that each HTTP health check request returns the correct webpage, and not an error page.
`status-code {int|range}`	Sets which status code indicates a successful reply when the health check type is set to HTTP or HTTPS. The default value is range `200-299`.
`[no] https enable-sni`	Enables or disables sending a Server_Name Indication (SNI) as part of the health check request when health check type is set to HTTPS.
`smtp helo-name name`	Sets the HELO string to send to the real server, when the health check type is set to SMTP. Typically, the HELO string contains the fully qualified domain name (FQDN) of the mail server.
`dns query fqdn`	Sets the fully qualified domain name (FQDN) to send to the real server when health check type is set to DNS.
`no ip virtual-server load-balancer name`	Deletes the load balancing rule.
`ip virtual-server load-balancer rename old_name new_name`	Renames the load balancing rule.
`show ip virtual-server load-balancer name`	Displays all of the settings of the specified load balancing rule.
`show ip virtual-server load-balancer name real-server`	Displays all of the real servers managed by this load balancing rule, with details such as their IP address, port, and weight.
`show ip virtual-server load-balancer statistics name`	Displays statistics about how many requests and how much data each load balancing rule has processed.
`show ip virtual-server load-balance statistics rate name`	Displays statistics about the average input and output speed for each load balancing rule.

CHAPTER 23
HTTP Redirect

23.1 HTTP Redirect Overview

HTTP redirect forwards the client's HTTP request (except HTTP traffic destined for the Zyxel Device) to a web proxy server.

23.1.1 Web Proxy Server

A proxy server helps client devices make indirect requests to access the Internet or outside network resources/services. A proxy server can act as a firewall or an ALG (application layer gateway) between the private network and the Internet or other networks. It also keeps hackers from knowing internal IP addresses.

23.2 HTTP Redirect Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 103 Input Values for HTTP Redirect Commands

LABEL	DESCRIPTION
description	The name to identify the rule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
interface_name	The name of the interface. Ethernet interface: For some Zyxel Device models, use ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your Zyxel Device model. For other Zyxel Device models use a name such as wan1, wan2, opt, lan1, or dmz. virtual interface on top of Ethernet interface: add a colon (:) and the number of the virtual interface. For example: ge*x*:*y*, *x* = 1 - N, *y* = 1 - 4 VLAN interface: vlan*x*, *x* = 0 - 4094 virtual interface on top of VLAN interface: vlan*x*:*y*, *x* = 0 - 4094, *y* = 1 - 4 bridge interface: br*x*, *x* = 0 - N, where N depends on the number of bridge interfaces your Zyxel Device model supports. virtual interface on top of bridge interface: br*x*:*y*, *x* = the number of the bridge interface, *y* = 1 - 4 PPPoE/PPTP interface: ppp*x*, *x* = 0 - N, where N depends on the number of PPPoE/PPTP interfaces your Zyxel Device model supports.

The following table describes the commands available for HTTP redirection. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 104 Command Summary: HTTP Redirect

COMMAND	DESCRIPTION
`ip http-redirect` *`description`* `interface` *`interface_name`* `redirect-to` *`w.x.y.z`* `<1..65535>`	Sets a HTTP redirect rule.
`ip http-redirect` *`description`* `interface` *`interface_name`* `redirect-to` *`w.x.y.z`* `<1..65535> deactivate`	Disables a HTTP redirect rule.
`ip http-redirect activate` *`description`*	Enables a rule with the specified rule name.
`ip http-redirect deactivate` *`description`*	Disables a rule with the specified rule name.
`no ip http-redirect` *`description`*	Removes a rule with the specified rule name.
`ip http-redirect flush`	Clears all HTTP redirect rules.
`show ip http-redirect [`*`description`*`]`	Displays HTTP redirect settings.

23.2.1 HTTP Redirect Command Examples

The following commands create a HTTP redirect rule, disable it and display the settings.

```
Router# configure terminal
Router(config)# ip http-redirect example1 interface ge1 redirect-to
10.10.2.3 80
Router(config)# ip http-redirect example1 interface ge1 redirect-to
10.10.2.3 80 deactivate
Router(config)# show ip http-redirect
Name                            Interface    Proxy Server    Port    Active
================================================================================
example1                         ge1          10.10.2.3       80      no
```

CHAPTER 24
Redirect Service

24.1 HTTP Redirect

HTTP redirect forwards the client's HTTP request (except HTTP traffic destined for the Zyxel Device) to a web proxy server. A proxy server helps client devices make indirect requests to access the Internet or outside network resources/services. The web proxy provides caching service to allow quick access and reduce network usage. The proxy checks its local cache for the requested web resource first. If it is not found, the proxy gets it from the specified server and forwards the response to the client.

24.2 SMTP Redirect

SMTP redirect forwards the authenticated client's SMTP message to a SMTP server, that handles all outgoing e-mail messages. The Zyxel Device forwards SMTP traffic using TCP port 25.

24.3 Redirect Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 105 Input Values for HTTP Redirect Commands

LABEL	DESCRIPTION
profile_name	The name to identify the rule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

Table 105 Input Values for HTTP Redirect Commands (continued)

LABEL	DESCRIPTION
interface_name	The name of the interface. Ethernet interface: For some Zyxel Device models, use ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your Zyxel Device model. For other Zyxel Device models use a name such as wan1, wan2, opt, lan1, or dmz. virtual interface on top of Ethernet interface: add a colon (:) and the number of the virtual interface. For example: ge*x*:*y*, *x* = 1 - N, *y* = 1 - 4 VLAN interface: vlan*x*, *x* = 0 - 4094 virtual interface on top of VLAN interface: vlan*x*:*y*, *x* = 0 - 4094, *y* = 1 - 4 bridge interface: br*x*, *x* = 0 - N, where N depends on the number of bridge interfaces your Zyxel Device model supports. virtual interface on top of bridge interface: br*x*:*y*, *x* = the number of the bridge interface, *y* = 1 - 4 PPPoE/PPTP interface: ppp*x*, *x* = 0 - N, where N depends on the number of PPPoE/PPTP interfaces your Zyxel Device model supports.
user_name	This is the user account or user group name to which this rule is applied.

The following table describes the commands available for HTTP redirection. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 106 Command Summary: Redirect

COMMAND	DESCRIPTION
`redirect-service append <1..20>`	Adds a new Redirect rule and enters sub-command mode.
`redirect-service <1..20>`	Edits an existing Redirect rule and enters sub-command mode.
`[no] activate`	Enables the Redirect rule. The no command disables the Redirect rule.
`exit`	Leaves sub-command mode
`[no] interface interface_name`	Names the interface for the Redirect rule. The *no* command restores the interface to `any`.
`[no] name profile_name`	Names the Redirect rule to identify it. The *no* command restores the name to `default`.
`[no] port <1..65535>`	Sets the service port for the Redirect rule. The *no* command restores the `http-redirect` port to `80`, and the `smtp-redirect` port to `25`.
`[no] server <fqdn> <w.x.y.z>`	Sets the fully-qualified domain name or IPv4 address for the Redirect rule. The *no* command clears the server.
`[no] service {http-redirect | smtp-redirect}`	Configures HTTP-redirect or SMTP-redirect as the Redirect rule. The *no* command restores the service to `http-redirect`.
`[no] source profile_name`	Configures the address or address group object. The *no* command restores the source to `any`.

Table 106 Command Summary: Redirect (continued)

COMMAND	DESCRIPTION
`[no] user user_name`	Configures the user account or user group to which this rule is applied. The *no* command restores the user to any.
`redirect-service flush`	Clears all Redirect rules.
`redirect-service insert <1..20>`	Inserts a new Redirect rule at the specified location and enters sub-command mode.
`redirect-service move <1..20> to <1..20>`	Moves a Redirect rule to the specified location.
`show redirect-service <1..20>`	Displays details of the specified Redirect rule.

24.3.1 Redirect Command Example

The following commands show how to create and display Redirect service rules on the Zyxel Device.

```
Router(config)# redirect-service append
Router(redirect-service)# interface ge4
Router(redirect-service)# name test
Router(redirect-service)# port 11111
Router(redirect-service)# service smtp-redirect
Router(redirect-service)# server 1.1.1.1
Router(redirect-service)# user admin
Router(redirect-service)# activate
Router(redirect-service)# exit
Router(config)# show redirect-service
redirect service rule: 1
  active: yes
  name: default
  service: http-redirect
  user: any
  incoming interface: any
  source address: any
  server:
  port: 80
  id: 1
redirect service rule: 2
  active: yes
  name: default
  service: http-redirect
  user: any
  incoming interface: any
  source address: any
  server:
  port: 80
  id: 0
redirect service rule: 3
  active: yes
  name: default
  service: append
  user: any
  incoming interface: any
  source address: any
  server:
  port: 80
  id: 2
redirect service rule: 4
  active: yes
  name: test
  service: smtp-redirect
  user: admin
  incoming interface: ge4
  source address: any
  server: 1.1.1.1
  port: 11111
  id: 3
Router(config)#
```

CHAPTER 25
ALG

25.1 ALG Introduction

This chapter covers how to use the Zyxel Device's ALG feature to allow certain applications to pass through the Zyxel Device.

The Zyxel Device can function as an Application Layer Gateway (ALG) to allow certain NAT un-friendly applications (such as SIP) to operate properly through the Zyxel Device's NAT.

Some applications cannot operate through NAT (are NAT un-friendly) because they embed IP addresses and port numbers in their packets' data payload. The Zyxel Device examines and uses IP address and port number information embedded in the VoIP traffic's data stream. When a device behind the Zyxel Device uses an application for which the Zyxel Device has VoIP pass through enabled, the Zyxel Device translates the device's private IP address inside the data stream to a public IP address. It also records session port numbers and allows the related sessions to go through the firewall so the application's traffic can come in from the WAN to the LAN.

The Zyxel Device only needs to use the ALG feature for traffic that goes through the Zyxel Device's NAT. The firewall allows related sessions for VoIP applications that register with a server. The firewall allows or blocks peer to peer VoIP traffic based on the firewall rules.

You do not need to use a TURN (Traversal Using Relay NAT) server for VoIP devices behind the Zyxel Device when you enable the SIP ALG.

25.2 ALG Commands

The following table lists the `alg` commands. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 107 alg Commands

COMMAND	DESCRIPTION
`[no] alg sip [direct-media | direct-signalling | inactivity-timeout | | media-timeout <1..86400> | signal-timeout <1..86400> | transformation]`	Turns on or configures the ALG. Use `direct-media to` to set the Zyxel Device to allow SIP audio session. Use `direct-signalling` to set the Zyxel Device to allow SIP signaling sessions. Use `inactivity-timeout` to have the Zyxel Device apply SIP media and signaling inactivity time out limits. Use `media-timeout` and a number of seconds (1~86400) for how long to allow a voice session to remain idle (without voice traffic) before dropping it. Use `signal-timeout` and a number of seconds (1~86400) for how long to allow a SIP signaling session to remain idle (without SIP packets) before dropping it. Use `transformation` to have the Zyxel Device modify IP addresses and port numbers embedded in the SIP data payload. You do not need to use this if you have a SIP device or server that will modify IP addresses and port numbers embedded in the SIP data payload. The `no` command turns off the SIP ALG or removes the settings that you specify.
`alg sip defaultport`	Enters ALG SIP default port sub-command
`Router(SIP Signaling Port)# [no] port <1025..65535>`	Enter the custom UDP port number for SIP traffic. The `no` command removes the custom UDP port number for SIP traffic.
`[no] alg <h323 | ftp> [signal-port <1025..65535> | signal-extra-port <1025..65535> | transformation]`	Turns on or configures the H.323 or FTP ALG. Use `signal-port` with a listening port number (1025 to 65535) if you are using H.323 on a TCP port other than 1720 or FTP on a TCP port other than 21. Use `signal-extra-port` with a listening port number (1025 to 65535) if you are also using H.323 or FTP on an additional TCP port number, enter it here. Use `transformation` to have the Zyxel Device modify IP addresses and port numbers embedded in the H.323 or FTP data payload. You do not need to use this if you have an H.323 or FTP device or server that will modify IP addresses and port numbers embedded in the H.323 or FTP data payload. The `no` command turns off the H.323 or FTP ALG or removes the settings that you specify.
`show alg <sip | h323 | ftp>`	Displays the specified ALG's configuration.

25.3 ALG Commands Example

The following example turns on pass through for SIP and turns it off for H.323.

```
Router# configure terminal
Router(config)# alg sip
Router(config)# no alg h323
```

CHAPTER 26
UPnP

26.1 UPnP and NAT-PMP Overview

The Zyxel Device supports both UPnP and NAT-PMP to permit networking devices to discover each other and connect seamlessly.

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use. A gateway that supports UPnP is called Internet Gateway Device (IGD). The standardized Device Control Protocol (DCP) is defined by the UPnP Forum for IGDs to configure port mapping automatically.

NAT Port Mapping Protocol (NAT-PMP), introduced by Apple and implemented in current Apple products, is used as an alternative NAT traversal solution to the UPnP IGD protocol. NAT-PMP runs over UDP port 5351. NAT-PMP is much simpler than UPnP IGD and mainly designed for small home networks. It allows a client behind a NAT router to retrieve the router's public IP address and port number and make them known to the peer device with which it wants to communicate. The client can automatically configure the NAT router to create a port mapping to allow the peer to contact it.

26.2 UPnP and NAT-PMP Commands

The following table lists the `ip upnp` commands. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 108 ip upnp Commands

COMMAND	DESCRIPTION
`ip upnp`	Enters the `config-upnp` sub-command mode to configure the UPnP or NAT-PMP settings.
`[no] bypass-firewall activate`	Allows traffic from UPnP-enabled or NAT-PMP-enabled applications to bypass the firewall. The no command has the firewall block all UPnP or NAT-PMP application packets (for example, MSN packets).
`link-sticking outgoing interface {`*`interface_name`*` | all}`	Specifies through which WAN interface(s) you want to send out traffic from UPnP-enabled or NAT-PMP-enabled applications. If the WAN interface you specified loses its connection, the Zyxel Device attempts to use the other WAN interface. If the other WAN interface also does not work, the Zyxel Device drops outgoing packets from UPnP-enabled or NAT-PMP-enabled applications.
`[no] listen-interface` *`interface_name`*	Enables UPnP and/or NAT-PMP on an internal interface. The no command disables UPnP and/or NAT-PMP on the interface.

Table 108 ip upnp Commands (continued)

COMMAND	DESCRIPTION
[no] nat-pmp activate	Enables NAT-PMP on the Zyxel Device. The no command disables NAT-PMP on the Zyxel Device.
[no] upnp-igd activate	Enables UPnP on the Zyxel Device. The no command disables UPnP on the Zyxel Device.
no ip upnp port-mapping port {<1..65535> type <tcp|udp> | all}	Removes all or a specific port mapping rule.
show ip upnp listen-interface	Displays the name(s) of the internal interface(s) on which the Zyxel Device supports UPnP and/or NAT-PMP.
show ip upnp port-mapping	Displays the UPnP and/or NAT-PMP port mapping rules on the Zyxel Device.
show ip upnp status	Displays the UPnP and/or NAT-PMP configuration.

26.3 UPnP & NAT-PMP Commands Example

The following example turns on UPnP and NAT-PMP on the Zyxel Device and it's two LAN interfaces. It also shows the UPnP and NAT-PMP settings.

```
Router# configure terminal
Router(config)# ip upnp
Router(config-upnp)# nat-pmp activate
Router(config-upnp)# upnp-igd activate
Router(config-upnp)# listen-interface lan1
Router(config-upnp)# listen-interface lan2
Router(config-upnp)# exit
Router(config)# show ip upnp status
upnp active: yes
nat-pmp active: yes
bypass-firewall active: no
link-sticking outgoing: all
Router(config)# show ip upnp listen-interface
interface
================================================================================
lan1
lan2
Router(config)#
```

The following example displays the Zyxel Device's port mapping entries and removes the entry with the specified port number and protocol type.

```
Router# configure terminal
Router(config) # show ip upnp port-mapping
No: 0
  Remote Host: (null)
  Client Type: upnp
  External Port: 1122
  Protocol: tcp
  Internal Port: 1122
  Internal Client: 172.16.1.2
  Description: test1
No: 1
  Remote Host: (null)
  Client Type: upnp
  External Port: 5566
  Protocol: tcp
  Internal Port: 5566
  Internal Client: 172.16.1.2
  Description: test2
Router(config)# no ip upnp port-mapping port 5566 type tcp
Router(config)# show ip upnp port-mapping
No: 0
  Remote Host: (null)
  Client Type: upnp
  External Port: 1122
  Protocol: tcp
  Internal Port: 1122
  Internal Client: 172.16.1.2
  Description: test1
Router(config)#
```

CHAPTER 27
IP/MAC Binding

27.1 IP/MAC Binding Overview

IP address to MAC address binding helps ensure that only the intended devices get to use privileged IP addresses. The Zyxel Device uses DHCP to assign IP addresses and records to MAC address it assigned each IP address. The Zyxel Device then checks incoming connection attempts against this list. A user cannot manually assign another IP to his computer and use it to connect to the Zyxel Device.

Suppose you configure access privileges for IP address 192.168.1.27 and use static DHCP to assign it to Tim's computer's MAC address of 12:34:56:78:90:AB. IP/MAC binding drops traffic from any computer with another MAC address that tries to use IP address 192.168.1.27.

27.2 IP/MAC Binding Commands

The following table lists the `ip-mac-binding` commands. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 109 ip-mac-binding Commands

COMMAND	DESCRIPTION
`[no] ip ip-mac-binding` *`interface_name`* `activate`	Turns on IP/MAC binding for the specified interface. The `no` command turns IP/MAC binding off for the specified interface.
`[no] ip ip-mac-binding` *`interface_name`* `log`	Turns on the IP/MAC binding logs for the specified interface. The `no` command turns IP/MAC binding logs off for the specified interface.
`ip ip-mac-binding exempt` *`name start-ip end-ip`*	Adds a named IP range as being exempt from IP/MAC binding.
`no ip ip-mac-binding exempt` *`name`*	Deletes the named IP range from the list of addresses that are exempt from IP/MAC binding.
`show ip ip-mac-binding` *`interface_name`*	Shows whether IP/MAC binding is enabled or disabled for the specified interface.
`show ip ip-mac-binding all`	Shows whether IP/MAC binding is enabled or disabled for all interfaces.
`show ip ip-mac-binding status` *`interface_name`*	Displays the current IP/MAC bindings for the specified interface.
`show ip ip-mac-binding status all`	Displays the current IP/MAC bindings for all interfaces.
`show ip ip-mac-binding exempt`	Shows the current IP/MAC binding exempt list.
`ip ip-mac-binding clear-drop-count` *`interface_name`*	Resets the packet drop counter for the specified interface.

27.3 IP/MAC Binding Commands Example

The following example enables IP/MAC binding on the LAN1 interface and displays the interface's IP/MAC binding status.

```
Router# configure terminal
Router(config)# ip ip-mac-binding lan1 activate
Router(config)# show ip ip-mac-binding lan1
Name: lan1
Status: Enable
Log: No
Binding Count: 0
Drop Count: 0
Router(config)#
```

CHAPTER 28
Layer 2 Isolation

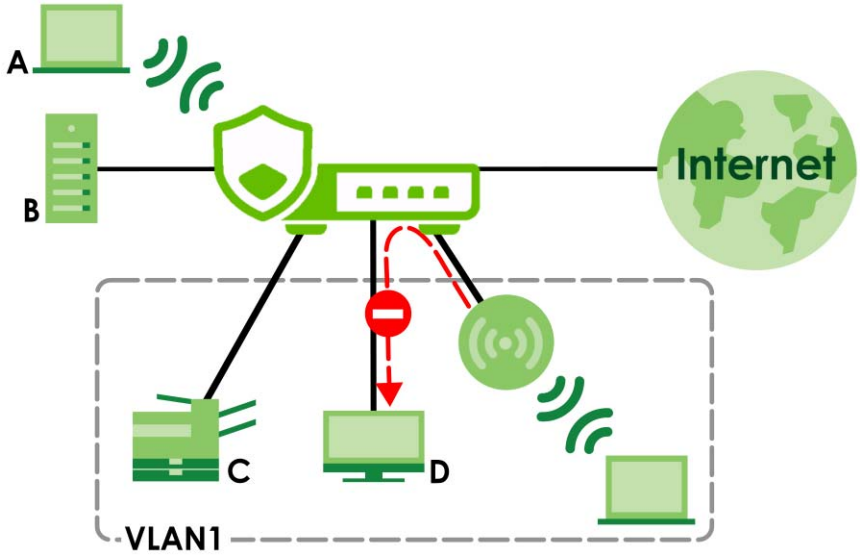
28.1 Layer 2 Isolation Overview

Layer-2 isolation is used to prevent connected devices from communicating with each other in the Zyxel Device's local network(s), on which layer-2 isolation is enabled, except the devices in the white list.

Note: Layer-2 isolation does not check the wireless traffic.

In the following example, layer-2 isolation is enabled on the Zyxel Device's interface Vlan1. A printer, PC and AP are in the Vlan1. The IP address of network printer (C) is added to the white list. The connected AP then cannot communicate with the PC (D), but can access the network printer (C), server (B), wireless client (A) and the Internet.

Figure 23 Layer-2 Isolation Application



28.2 Layer 2 Isolation Commands

The following table lists the `l2-isolation` commands. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 110 l2-isolation Commands

COMMAND	DESCRIPTION
`l2-isolation`	Enters the layer 2 isolation sub-command mode to enable Layer-2 isolation on the Zyxel Device and specific internal interface(s).
`[no] activate`	Turns on Layer-2 isolation on the Zyxel Device. The no command disables Layer-2 isolation on the Zyxel Device.
`[no] interface` *interface_name*	Turns on Layer-2 isolation on a specific internal interface. The no command disables Layer-2 isolation for the specified interface.
`white-list` *rule_number*	Enters the layer 2 isolation white list sub-command mode to set a new rule in the white list. See Table 111 on page 215 for the sub-commands. *rule_number*: 1 - N, where N depends on the Zyxel Device model.
`white-list activate`	Turns on the white list on the Zyxel Device. IP addresses that are not listed in the white list are blocked from communicating with other devices in the layer-2-isolation-enabled internal interface(s) except for broadcast packets.
`white-list append`	Enters the layer 2 isolation white list sub-command mode to add a rule to the end of the white list. See Table 111 on page 215 for the sub-commands.
`white-list flush`	Removes all rules in the white list.
`white-list no activate`	Turns the white list off.
`no l2-isolation activate`	Disables Layer-2 isolation on the Zyxel Device.
`no l2-isolation white-list` *rule_number*	Disables the specified rule in the white list. *rule_number*: 1 - N, where N depends on the Zyxel Device model.
`no l2-isolation white-list activate`	Turns on the white list on the Zyxel Device.
`show l2-isolation`	Displays whether Layer-2 isolation is enabled on an interface.
`show l2-isolation activation`	Displays whether Layer-2 isolation is enabled on the Zyxel Device.
`show l2-isolation white-list [`*rule_number*`]`	Displays all or a specified white list rule settings. *rule_number*: 1 - N, where N depends on the Zyxel Device model.
`show l2-isolation white-list activation`	Displays whether the white list is enabled.

28.2.1 Layer 2 Isolation White List Sub-Commands

The following table describes the sub-commands for `l2-isolation white-list` commands.

Table 111 l2-isolation white-list Sub-commands

COMMAND	DESCRIPTION
`[no] activate`	Enables the rule. The no command disables the rule.

Table 111 l2-isolation white-list Sub-commands (continued)

COMMAND	DESCRIPTION
[no] description *description*	Sets a descriptive name (up to 60 printable ASCII characters) for a rule. The no command removes the descriptive name from the rule.
[no] ip-address *ip*	Sets an IPv4 address associated with this rule. The no command removes the IP address. This is the IP address of device that can be accessed by the devices connected to an internal interface on which layer-2 isolation is enabled.

28.3 Layer 2 Isolation Commands Example

The following example enables Layer-2 isolation on the Zyxel Device and interface lan2. It also creates a rule in the white list to allow access to the device with IP address 172.17.0.66. It then displays the Layer-2 isolation settings.

```
Router# configure terminal
Router(config)# l2-isolation
Router(l2-isolation)# activate
Router(l2-isolation)# interface lan2
Router(l2-isolation)# white-list 1
Router(white-list)# activate
Router(white-list)# description PC
Router(white-list)# ip-address 172.17.0.66
Router(white-list)# exit
Router(config)# show l2-isolation
interface
================================================================================
lan2
Router(config)# show l2-isolation activation
Layer2 Isolation Status: yes
Router(config)# show l2-isolation white-list
layer2 isolation white list rule: 1
  active: yes
  ip address: 172.17.0.66
  description:    PC
Router(config)#
```

CHAPTER 29
Secure Policy

29.1 Secure Policy Overview

This chapter introduces the Zyxel Device's secure policies and shows you how to configure them.

Note: In the guide Secure Policy commands may also be referred to as Firewall in general descriptions.

A secure policy is a template of security settings that can be applied to specific traffic at specific times. The policy can be applied:

- to a specific direction of travel of packets (from / to)
- to a specific source and destination address objects
- to a specific type of traffic (services)
- to a specific user or group of users
- at a specific schedule

The policy can be configured:

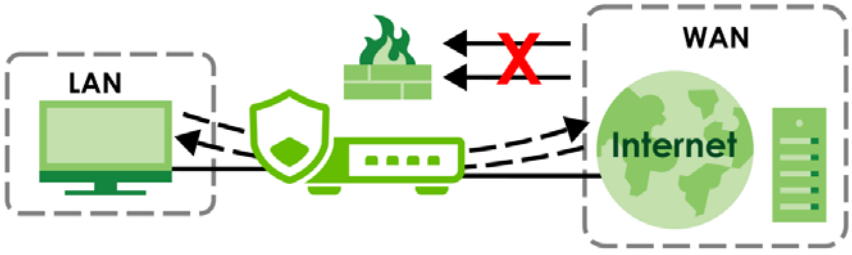
- to allow or deny traffic that matches the criteria above
- send a log or alert for traffic that matches the criteria above
- to apply the actions configured in the UTM profiles (such as application patrol, content filter, IDP, anti-virus, anti-spam) to traffic that matches the criteria above

Note: Secure policies can be applied to both IPv4 and IPv6 traffic

The secure policies can also limit the number of user sessions.

The following example shows the Zyxel Device's default security policies behavior for a specific direction of travel of packets. WAN to LAN traffic and how stateful inspection works. A LAN user can initiate a Telnet session from within the LAN zone and the Zyxel Device allows the response. However, the Zyxel Device blocks incoming Telnet traffic initiated from the WAN zone and destined for the LAN zone.

Figure 24 Default Directional Policy Example



29.2 Secure Policy Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 112 Input Values for Secure Policy Commands

LABEL	DESCRIPTION
address_object	The name of the IP address (or address group) object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
address6_object	The name of the IPv6 address (or address group) object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
user_name	The name of a user (group). You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
zone_object	The name of the zone. For some Zyxel Device models, use up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive. For other Zyxel Devicemodels, use pre-defined zone names like DMZ, LAN1, SSL VPN, IPSec VPN, OPT, and WAN.
rule_number	The priority number of a secure policy. 1 - *X* where *X* is the highest number of rules the Zyxel Device model supports. See the Zyxel Device's User's Guide for details.
schedule_object	The name of the schedule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
service_name	The name of the service (group). You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

The following table describes the commands available for the secure policy. You must use the `configure terminal` command to enter the configuration mode before you can use the configuration commands. Commands that do not have IPv6 specified in the description are for IPv4.

Table 113 Command Summary: Secure Policy

COMMAND	DESCRIPTION
`secure-policy activate`	Enables Secure Policy on the Zyxel Device to perform access control.
`secure-policy backup activate`	Backs up all secure policies configured on the Zyxel Device when you make any configuration changes (insert/modify/delete/append). Type `dir /conf/` to see all configuration files on the Zyxel Device. These files are also visible in Maintenance > File Manager > Configuration File in the web configurator. Filenames beginning with autoback are automatic configuration files created when new firmware is uploaded. `backup-yyyy-mm-dd-hh-mm-ss.conf` is the name of the automatic backup when a secure policy is added or changed. Type `appy` *`config-file-name`* to restore secure policy configuration to what it was before that change.
`show secure-policy _check-exposed-srv`	Displays if only specified IP addresses or Fully Qualified Domain Names (FQDNs) are allowed to access the Zyxel Device remotely. Displays if only SSL VPN clients from specified regions are allowed to access the Zyxel Device.
`show secure-policy backup status`	Displays if backing up of secure policies when changes are done is configured on the Zyxel Device.

Table 113 Command Summary: Secure Policy (continued)

COMMAND	DESCRIPTION
`show secure-policy filter from zone_object to zone_object srcip <ip-address> dstip <ip> service {any | tcp | udp | icmp | gre | esp | user-defined} port-number user user_name sch schedule_object`	Applies IPv4 search filters to find specific IPv4 security policies based on direction, application, user, source, destination and/or schedule.
`[no] secure-policy asymmetrical-route activate`	Allows or disallows asymmetrical route topology.
`secure-policy rule_number`	Enters the secure policy sub-command mode to set a firewall rule. See Table 114 on page 221 for the sub-commands.
`secure-policy zone_object {zone_object|ZyWALL} rule_number`	Enters the secure policy sub-command mode to set a direction specific through-ZyWALL rule or to-ZyWALL rule. See Table 114 on page 221 for the sub-commands.
`secure-policy zone_object {zone_object|ZyWALL} append`	Enters the secure policy sub-command mode to add a direction specific through-ZyWALL rule or to-ZyWALL rule to the end of the global rule list. See Table 114 on page 221 for the sub-commands.
`secure-policy zone_object {zone_object|ZyWALL} delete <1..5000>`	Removes a direction specific through-ZyWALL rule or to-ZyWALL rule. `<1..5000>`: the index number in a direction specific secure policy rule list.
`secure-policy zone_object {zone_object|ZyWALL} flush`	Removes all direction specific through-ZyWALL rule or to-ZyWALL rules.
`secure-policy zone_object {zone_object|ZyWALL} insert rule_number`	Enters the secure policy sub-command mode to add a direction specific through-ZyWALL rule or to-ZyWALL rule before the specified rule number. See Table 114 on page 221 for the sub-commands.
`secure-policy zone_object {zone_object|ZyWALL} move rule_number to rule_number`	Moves a direction specific through-ZyWALL rule or to-ZyWALL rule to the number that you specified.
`[no] secure-policy activate`	Enables the secure policy on the Zyxel Device. The no command disables the secure policy.
`secure-policy append`	Enters the secure policy sub-command mode to add a global secure policy rule to the end of the global rule list. See Table 114 on page 221 for the sub-commands.
`secure-policy default-rule action {allow | deny | reject} { no log | log [alert] }`	Sets how the secure policy handles packets that do not match any other secure policy rule.
`secure-policy delete rule_number`	Removes a secure policy rule.
`secure-policy flush`	Removes all secure policy rules.
`secure-policy insert rule_number`	Enters the secure policy sub-command mode to add a secure policy rule before the specified rule number. See Table 114 on page 221 for the sub-commands.
`secure-policy move rule_number to rule_number`	Moves a secure policy rule to the number that you specified.
`firewall icsa {icmp-destroy-session} {enable | disable}`	During ICSA certification a connection automatically terminates immediately once ICMP unreachable or ICMP TTL expired is received. Use this command to turn off this behavior.

Table 113 Command Summary: Secure Policy (continued)

COMMAND	DESCRIPTION
`show firewall icsa status`	Displays if a ICSA certification connection is automatically terminated immediately once ICMP unreachable or ICMP TTL expired is received.
`show secure-policy`	Displays all Secure Policy settings.
`show secure-policy rule_number`	Displays a secure policy rule's settings.
`show secure-policy zone_object {zone_object|ZyWALL}`	Displays all secure policy rules settings for the specified packet direction.
`show secure-policy zone_object {zone_object|ZyWALL} rule_number`	Displays a specified secure policy rule's settings for the specified packet direction.
`show secure-policy status`	Displays whether or not the secure policy is active, whether or not asymmetrical route topology is allowed, and the default secure policy rule's configuration.
`show secure-policy block_rules`	Displays all the secure policy rules that deny access.
`show secure-policy any ZyWALL`	Shows all the to-Zyxel Device secure policy rules.
`show secure-policy6 filter from zone_object to zone_object srcip6 <ip-address> dstip6 <ip> service {any | tcp | udp | icmp | gre | esp | user-defined} port-number user user_name sch schedule_object`	Applies IPv6 search filters to find specific IPv6 (if enabled) security policies based on direction, application, user, source, destination and/or schedule.
`secure-policy6 rule_number`	Enters the IPv6 secure policy sub-command mode to set a secure policy rule. See Table 114 on page 221 for the sub-commands.
`secure-policy6 zone_object {zone_object|ZyWALL} rule_number`	Enters the IPv6 firewall sub-command mode to set a direction specific through-ZyWALL rule or to-ZyWALL rule. See Table 114 on page 221 for the sub-commands.
`secure-policy6 zone_object {zone_object|ZyWALL} append`	Enters the IPv6 secure policy sub-command mode to add a direction specific through-ZyWALL rule or to-ZyWALL rule to the end of the global rule list. See Table 114 on page 221 for the sub-commands.
`secure-policy6 zone_object {zone_object|ZyWALL} delete <1..5000>`	Removes a direction specific IPv6 through-ZyWALL rule or to-ZyWALL rule. <1..5000>: the index number in a direction specific firewall rule list.
`secure-policy6 zone_object {zone_object|ZyWALL} flush`	Removes all direction specific IPv6 through-ZyWALL rule or to-ZyWALL rules.
`secure-policy6 zone_object {zone_object|ZyWALL} insert rule_number`	Enters the IPv6 secure policy sub-command mode to add a direction specific through-ZyWALL rule or to-ZyWALL rule before the specified rule number. See Table 114 on page 221 for the sub-commands.
`secure-policy6 zone_object {zone_object|ZyWALL} move rule_number to rule_number`	Moves a direction specific IPv6 through-ZyWALL rule or to-ZyWALL rule to the number that you specified.
`[no] secure-policy6 activate`	Enables the IPv6 secure policy on the Zyxel Device. The no command disables the IPv6 firewall.
`secure-policy6 append`	Enters the IPv6 secure policy sub-command mode to add a global firewall rule to the end of the global rule list. See Table 114 on page 221 for the sub-commands.

Table 113 Command Summary: Secure Policy (continued)

COMMAND	DESCRIPTION
`secure-policy6 default-rule action {allow | deny | reject} { no log | log [alert] }`	Sets how the IPv6 secure policy handles packets that do not match any other secure policy rule.
`secure-policy6 delete rule_number`	Removes a IPv6 secure policy rule.
`secure-policy6 flush`	Removes all IPv6 secure policy rules.
`secure-policy6 insert rule_number`	Enters the IPv6 secure policy sub-command mode to add a secure policy rule before the specified rule number. See Table 114 on page 221 for the sub-commands.
`secure-policy6 move rule_number to rule_number`	Moves a IPv6 secure policy rule to the number that you specified.
`show secure-policy6`	Displays all IPv6 secure policy settings.
`show secure-policy6 rule_number`	Displays a IPv6 secure policy rule's settings.
`show secure-policy6 zone_object {zone_object|ZyWALL}`	Displays all IPv6 secure policy rules settings for the specified packet direction.
`show secure-policy6 zone_object {zone_object|ZyWALL} rule_number`	Displays a specified IPv6 secure policy rule's settings for the specified packet direction.
`show secure-policy6 status`	Displays whether or not the IPv6 secure policy is active, whether or not IPv6 asymmetrical route topology is allowed, and the default IPv6 secure policy rule's configuration.
`show secure-policy6 block_rules`	Displays all the IPv6 secure policy rules that deny access.
`show secure-policy6 any ZyWALL`	Shows all the IPv6 to-Zyxel Device secure policy rules.
`[no] secure-policy6 asymmetrical-route activate`	Allows or disallows asymmetrical route topology for IPv6 traffic.
`session-status-update reply-time <5..300>`	Set how many seconds the Zyxel Device will allow a session to remain idle (without traffic) before closing it.
`session-status-update alg {active|inactive}`	Enables or Disables ALG session updates
`show session-status-update reply-time`	Displays idle session timeout

29.2.1 Secure Policy Sub-Commands

The following table describes the sub-commands for several `secure-policy` and `secure-policy6` commands.

Table 114 firewall Sub-commands

COMMAND	DESCRIPTION
`action {allow|deny|reject}`	Sets the action the Zyxel Device takes when packets match this rule.
`[no] activate`	Enables a secure policy rule. The no command disables the rule.

Table 114 firewall Sub-commands (continued)

COMMAND	DESCRIPTION
[no] ctmatch {dnat | snat}	Use dnat to block packets sent from a computer on the Zyxel Device's WAN network from being forwarded to an internal network according to a virtual server rule. Use snat to block packets sent from a computer on the Zyxel Device's internal network from being forwarded to the WAN network according to a 1:1 NAT or Many 1:1 NAT rule. The no command forwards the matched packets. Subcommands cannot be used with secure-policy6.
[no] description *description*	Sets a descriptive name (up to 60 printable ASCII characters) for a secure policy rule. The no command removes the descriptive name from the rule.
[no] destinationip *address_object*	Sets the destination IP address. The no command resets the destination IP address(es) to the default (any). any means all IP addresses.
[no] destinationip6 *address_object*	Sets the destination IPv6 address. The no command resets the destination IP address(es) to the default (any). any means all IP addresses.
[no] from *zone_object*	Sets the zone on which the packets are received. The no command removes the zone on which the packets are received and resets it to the default (any) meaning all interfaces or VPN tunnels.
[no] log [alert]	Sets the Zyxel Device to create a log (and optionally an alert) when packets match this rule. The no command sets the Zyxel Device not to create a log or alert when packets match this rule.
[no] schedule *schedule_object*	Sets the schedule that the rule uses. The no command removes the schedule settings from the rule.
[no] service *service_name*	Sets the service to which the rule applies. The no command resets the service settings to the default (any). any means all services.
[no] sourceip *address_object*	Sets the source IP address(es). The no command resets the source IP address(es) to the default (any). any means all IP addresses.
[no] sourceip6 *address_object*	Sets the source IP address(es). The no command resets the source IP address(es) to the default (any). any means all IP addresses.
[no] sourceport {tcp|udp} {eq <1..65535>|range <1..65535> <1..65535>}	Sets the source port for a secure policy rule. The no command removes the source port from the rule.
[no] to {*zone_object*|ZyWALL}	Sets the zone to which the packets are sent. The no command removes the zone to which the packets are sent and resets it to the default (any). any means all interfaces or VPN tunnels.
[no] user *user_name*	Sets a user-aware secure policy rule. The rule is activated only when the specified user logs into the system. The no command resets the user name to the default (any). any means all users. Subcommands cannot be used with secure-policy6.
secure-policy <*profile name*>	Creates a secure policy rule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

Table 114 firewall Sub-commands (continued)

COMMAND	DESCRIPTION
[no] cf-profile <*profile name*> {[no log]|[log by-profile]} {activate | deactivate}	Applies the (already-created) named anti- x profile to traffic that matches the secure-policy rule. Log by-profile generates a log for all traffic that matches criteria in the anti- x profile. no log does turns off logging and overrides the anti- x profile log setting. The no command does not apply the named anti- x profile to traffic that matches the secure-policy rule.
[no] as-profile <*profile name*> {[no log]|[log by-profile]} {activate | deactivate}	Applies the (already-created) named anti- x profile to traffic that matches the secure-policy rule. Log by-profile generates a log for all traffic that matches criteria in the anti- x profile. no log does turns off logging and overrides the anti- x profile log setting. The no command does not apply the named anti- x profile to traffic that matches the secure-policy rule.
[no] av-profile <*profile name*>{[no log]|[log by-profile]} {activate | deactivate}	Applies the (already-created) named anti- x profile to traffic that matches the secure-policy rule. Log by-profile generates a log for all traffic that matches criteria in the anti- x profile. no log does turns off logging and overrides the anti- x profile log setting. The no command does not apply the named anti- x profile to traffic that matches the secure-policy rule.
[no] idp-profile <*profile name*> {[no log]|[log by-profile]} {activate | deactivate}	Applies the (already-created) named anti- x profile to traffic that matches the secure-policy rule. Log by-profile generates a log for all traffic that matches criteria in the anti- x profile. no log does turns off logging and overrides the anti- x profile log setting. The no command does not apply the named anti- x profile to traffic that matches the secure-policy rule.
[no] ssl-profile <*profile name*> {[no log]|[log by-profile]} {activate | deactivate}	Applies the (already-created) named anti- x profile to traffic that matches the secure-policy rule. Log by-profile generates a log for all traffic that matches criteria in the anti- x profile. no log does turns off logging and overrides the anti- x profile log setting. The no command does not apply the named anti- x profile to traffic that matches the secure-policy rule.
[no] app-profile <*profile name*> {[no log]|[log by-profile]} {activate | deactivate}	Applies the (already-created) named anti- x profile to traffic that matches the secure-policy rule. Log by-profile generates a log for all traffic that matches criteria in the anti- x profile. no log does turns off logging and overrides the anti- x profile log setting. The no command does not apply the named anti- x profile to traffic that matches the secure-policy rule.

29.2.2 Security Services Multiple Profiles

By default, security services such as anti-malware, URL threat filter, and DNS filter, support multiple profiles in the CLI but only a single profile in the Web Configurator. To enable multiple profiles in the Web Configurator, you need to change the Zyxel Device’s display mode.

Table 115 Secure Policy Style Commands

COMMAND	DESCRIPTION
`secure-policy-style {general | advance}`	Enables or disables multiple profiles for the following security services: • Anti-virus • DNS Filter • Threat website • IDP (Intrusion Detection and Prevention • Anti-spam *general:* Multiple profiles are disabled for the listed security services. This is the default option. When the Zyxel Device is set to this mode, a profile named *default_profile* maps to the settings in the Web Configurator UI. *advance:* Multiple profiles are enabled for the listed security services. Note: To change the mode from advance to general, ensure that the inspect policy of each of the listed security services is set to all-traffic.
`secure-policy-style advance all-inspect-by-policy`	Enables multiple profiles for the following security services, and also sets all security services to inspect by policy. • Anti-virus • URL Threat Filter • IDP (Intrusion Detection and Prevention • Anti-spam Inspect by policy means a security service inspects traffic only when its profile is bound to a security policy. For information on binding a security service profile to a security policy, see Section 29.2.1 on page 221.
`show secure-policy-style status`	Displays the current secure policy style setting (general or advanced).
`show security-service inspect status`	Displays the inspect policy setting (all traffic or by policy) for each security service.

29.2.3 Secure Policy Command Examples

These are IPv4 secure policy configuration examples. The IPv6 secure policy commands are similar.

The following example shows you how to add an IPv4 secure policy rule to allow a MyService connection from the WAN zone to the IP addresses Dest_1 in the LAN zone.

- Enter configuration command mode.
- Create an IP address object.
- Create a service object.
- Enter the secure policy sub-command mode to add a secure policy rule.
- Set the direction of travel of packets to which the rule applies.
- Set the destination IP address(es).
- Set the service to which this rule applies.

- Set the action the Zyxel Device is to take on packets which match this rule.

```
Router# configure terminal
Router(config)# service-object MyService tcp eq 1234
Router(config)# address-object Dest_1 10.0.0.10-10.0.0.15
Router(config)# secure-policy insert 3
Router(secure-policy)# from WAN
Router(v)# to LAN
Router(secure-policy)# destinationip Dest_1
Router(secure-policy)# service MyService
Router(secure-policy)# action allow
```

The following command displays the default IPv4 secure policy rule that applies to the WAN to Zyxel Device packet direction. The secure policy rule number is in the rule's priority number in the global rule list.

```
Router(config)# show secure-policy WAN ZyWALL

secure-policy rule: 11
  name: WAN_to_Device
  description:
  user: any, schedule: none
  from: WAN, to: ZyWALL
  source IP: any, source port: any
  destination IP: any, service: Default_Allow_WAN_To_ZyWALL
  log: no, action: allow, status: yes
  connection match: no
  content-filter profile: none
                 enable: no, log: by-profile
  anti-spam      profile: none
                 enable: no, log: by-profile
  anti-virus     profile: none
                 enable: no, log: by-profile
  idp            profile: none
                 enable: no, log: by-profile
  ssl-inspection profile: none
                 enable: no, log: by-profile
  app-patrol     profile: none
                 enable: no, log: by-profile
```

The following command displays the default IPv6 firewall rule that applies to the WAN to Zyxel Device packet direction. The firewall rule number is in the rule's priority number in the global rule list.

```
Router(config)# show secure-policy6 WAN ZyWALL

secure-policy rule: 1
  name: Device_Default_Allow_Service
  description:
  user: any, schedule: none
  from: any, to: ZyWALL
  source IP: any, source port: any
  destination IP: any, service: Default_Allow_v6_any_to_ZyWALL
  log: no, action: allow, status: yes
  content-filter profile: none
                 enable: no, log: by-profile
  anti-spam      profile: none
                 enable: no, log: by-profile
  anti-virus     profile: none
                 enable: no, log: by-profile
  idp            profile: none
                 enable: no, log: by-profile
  ssl-inspection profile: none
                 enable: no, log: by-profile
  app-patrol     profile: none
                 enable: no, log: by-profile
secure-policy rule: 11
  name: WAN_to_Device
  description:
  user: any, schedule: none
  from: WAN, to: ZyWALL
  source IP: any, source port: any
  destination IP: any, service: Default_Allow_v6_WAN_To_ZyWALL
  log: no, action: allow, status: yes
  content-filter profile: none
                 enable: no, log: by-profile
  anti-spam      profile: none
                 enable: no, log: by-profile
  anti-virus     profile: none
                 enable: no, log: by-profile
  idp            profile: none
                 enable: no, log: by-profile
  ssl-inspection profile: none
                 enable: no, log: by-profile
  app-patrol     profile: none
                 enable: no, log: by-profile
```

The following commands activate secure-policy backup, displays its status and then shows where to fond the configuration files. Filenames beginning with autoback are automatic configuration files created when new firmware is uploaded. `backup-2017-12-13-13-34-49.conf` is the name of the automatic backup

when a secure policy was added or changed. Type `apply backup-2017-12-13-13-34-49.conf` to restore secure policy configuration to what it was before that change.

```
Router(config)# secure-policy backup activate
Router(config)# show secure-policy backup status
secure-policy backup status: yes
Router(config)# dir /conf/
File Name                                       Size     Modified Time
================================================
system-default.conf                            70098    2017-11-03 18:02:19
startup-config.conf                            76090    2017-12-13 13:34:49
lastgood.conf                                  74763    2017-11-23 16:24:54
startup-config-bad.conf                        31999    2017-11-03 18:52:14
411AAPH0Preb1-r58726-2015-04-14-06-03-07.conf  22733    2015-04-14 14:03:07
autobackup-0.00.conf                           27782    2016-12-29 10:51:50
420AAPH0b4s2-2016-12-29-02-46-53.conf          27782    2016-12-29 10:46:53
425AAPH0b2-2017-05-22-06-28-12.conf            28815    2017-05-22 14:28:12
autobackup-4.25.conf                           28815    2017-05-22 14:31:16
430AAPH0b1s1-2017-07-20-08-44-45.conf          29538    2017-07-20 16:44:45
autobackup-4.30.conf                           31999    2017-11-03 18:04:22
430AAPH0b2-2017-08-22-06-09-32.conf            30484    2017-08-22 14:09:32
430AAPH0b3-2017-11-03-10-01-27.conf            31999    2017-11-03 18:01:27
backup-2017-12-13-13-34-49.conf                75733    2017-12-13 13:34:49
```

The following command displays `Fail` if HTTP, HTTPS and SSL traffic can access to your Zyxel Device from any IPv4 source on the WAN.

The following command displays `OK` if HTTP, HTTPS and SSL traffic can access to your Zyxel Device only from specified IPv4 sources on the WAN.

```
Router# show secure-policy _check-exposed-srv
HTTPS-HTTP: Fail
SSLVPN: Fail
```

Accessing the Zyxel Device from the WAN

This is an example of configuring security policy settings to allow access to the Zyxel Device from the WAN without deactivating the security policies.

1 Check the Security Policy status. Make sure the Zyxel Device Security Policy is activated to keep your network safe.

```
Router# show secure-policy status
secure-policy status: yes
secure-policy asymmetrical route status: no
secure-policy default rule: deny, log
secure-policy tcp flag detect: yes
```

2 Enter the Default_Allow_WAN_To_ZyWALL service group sub-command mode.

```
Router(config)# object-group service Default_Allow_WAN_To_ZyWALL
Router(group-service)#
;                description      no               service-object
<cr>             exit             object-group     |
```

3 Add HTTP, HTTPS, TELNET and SSH to the service group member list. Exit sub-command mode. Exit configuration mode

```
Router(group-service)# service-object HTTP
Router(group-service)# service-object HTTPS
Router(group-service)# service-object TELNET
Router(group-service)# object-group SSH
Router(group-service)# exit
Router(config)# exit
```

4 Check the Zyxel Device DHCP-assigned IP address for the WAN. Use the IP address to access the Zyxel Device from the WAN.

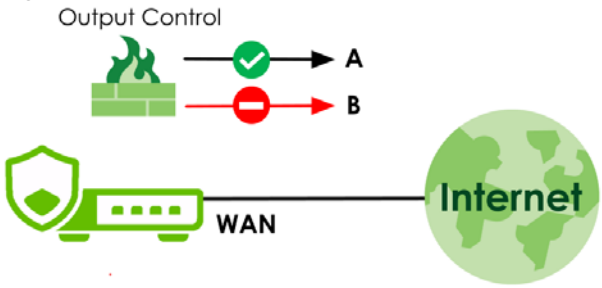
```
Router# show interface all
No. Name           Status              IP Address      Mask            IP Assignment
================================================================================
1   sfp             Down                0.0.0.0         0.0.0.0         Static
2   wan             100M/Full           XXX.XX.XX.XX    255.255.252.0   DHCP client
3   lan1            Down                192.168.1.1     255.255.255.0   Static
4   lan2            Down                192.168.2.1     255.255.255.0   Static
5   dmz             Down                192.168.3.1     255.255.255.0   Static
6   opt             Down                0.0.0.0         0.0.0.0         Static
```

29.3 Output Control Commands

Output control rules only allow outgoing traffic with specific services or specific destinations to travel out from the Zyxel Device. Other outgoing traffic that's not configured in the output control rules will be blocked by the default rule. Note that the ordering of your rules is very important as rules are applied in sequence.

In the example figure shown below, traffic A is the traffic packet allowed in the output control rule. Traffic B is the traffic packet not included or denied in the output control rule.

Figure 25 Output Control Example



Here's the output control process:

1 The outgoing traffic is initiated from the Zyxel Device.

2 The Zyxel Device inspects if the traffic matches the specific services or specific destinations configured in the output control rules.

3 The Zyxel Device decides to:

- Drop the traffic

or

- Permit the passage of the traffic.

The traffic that passes the output control firewall goes to the Internet.

The following table describes the commands available for the output control. You must use the `configure terminal` command to enter the configuration mode before you can use the configuration commands. Commands that do not have IPv6 specified in the description are for IPv4. Output control supports IPv4 only at the time of writing.

Table 116 Command Summary: Output Control

COMMAND	DESCRIPTION
`show firewall-output`	Displays all output control rules settings.
`show firewall-output status`	Displays whether or not output control is active and the default output control rule's configuration.
`[no] firewall-output activate`	Enables the output control on the Zyxel Device. The `no` command disables output control.
`[no] firewall-output default-rule establish enable`	Enables stateful inspection on the Zyxel Device. The `no` command disables stateful inspection. With stateful inspection enabled, the Zyxel Device will respond to all traffic initiated from the WAN. With stateful inspection disabled, the Zyxel Device will not respond to all traffic initiated from the WAN by default. Make sure you configure a rule to allow the Zyxel Device to respond to a specific client on the WAN before disabling this feature.
`firewall-output append`	Adds an output control rule to the end of the rule list.
`firewall-output insert` *`rule_number`*	Adds an output control rule before the specified rule number.
`firewall-output delete` *`rule_number`*	Removes an output control rule.
`firewall-output move` *`rule_number`* `to` *`rule_number`*	Moves an output control rule to the number that you specified.
`firewall-output` *`rule_number`*	Enters the output control sub-command mode to set a firewall rule.

29.3.1 Output Control Sub-Commands

The following table describes the sub-commands for several `firewall-output` commands.

Table 117 firewall Sub-commands

COMMAND	DESCRIPTION
<profile name>	Names an output control rule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
[no] tointerface *<interface name>*	Sets the interface to which the packets are sent. The no command removes the interface to which the packets are sent and resets it to the default (any). any means all interfaces.
[no] destinationip *<profile name>*	Sets the destination IP address. The no command resets the destination IP address(es) to the default (any). any means all IP addresses.
[no] service *<profile name>*	Sets the service to which the rule applies. The no command resets the service settings to the default (any). any means all services.
action {allow|deny|reject}	Sets the action the Zyxel Device takes when packets match this rule.
[no] log [alert]	Sets the Zyxel Device to create a log (and optionally an alert) when packets match this rule. The no command sets the Zyxel Device not to create a log or alert when packets match this rule.
[no] description *<description>*	Sets a descriptive name (up to 60 printable ASCII characters) for an output control rule. The no command removes the descriptive name from the rule.
[no] activate	Enables a secure policy rule. The no command disables the rule.

29.4 Session Limit Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 118 Input Values for General Session Limit Commands

LABEL	DESCRIPTION
rule_number	The priority number of a session limit rule, 1 - 1000.
address_object	The name of the IP address (group) object. You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
address6_object	The name of the IPv6 address (group) object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
user_name	The name of a user (group). You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

The following table describes the session-limit commands. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 119 Command Summary: Session Limit

COMMAND	DESCRIPTION
`[no] session-limit activate`	Turns the session-limit feature on or off.
`session-limit limit <0...20000>`	Sets the default number of concurrent NAT/firewall sessions per host.
`session-limit` *rule_number*	Enters the session-limit sub-command mode to set a session-limit rule.
`[no] activate`	Enables the session-limit rule. The no command disables the session limit rule.
`[no] address` *address_object*	Sets the source IP address. The no command sets this to any, which means all IP addresses.
`[no] description` *description*	Sets a descriptive name (up to 64 printable ASCII characters) for a session-limit rule. The no command removes the descriptive name from the rule.
`exit`	Quits the sub-command mode.
`[no] limit <0...40000>`	Sets the limit for the number of concurrent NAT/firewall sessions this rule's users or addresses can have. 0 means any.
`[no] user` *user_name*	Sets a session-limit rule for the specified user. The no command resets the user name to the default (any). any means all users.
`session-limit append`	Enters the session-limit sub-command mode to add a session-limit rule to the end of the session-limit rule list.
`session-limit delete` *rule_number*	Removes a session-limit rule.
`session-limit flush`	Removes all session-limit rules.
`session-limit insert` *rule_number*	Enters the session-limit sub-command mode to add a session-limit rule before the specified rule number.
`session-limit move` *rule_number* `to` *rule_number*	Moves a session-limit to the number that you specified.
`show session-limit`	Shows the session-limit configuration.
`show session-limit begin` *rule_number* `end` *rule_number*	Shows the settings for a range of session-limit rules.
`show session-limit` *rule_number*	Shows the session-limit rule's settings.
`show session-limit status`	Shows the general session-limit settings.
`[no] session-limit6 activate`	Turns the IPv6 session-limit feature on or off.
`session-limit6 limit <0...20000>`	Sets the default number of concurrent NAT/firewall IPv6 sessions per host.
`session-limit6` *rule_number*	Enters the IPv6 session-limit sub-command mode to set a session-limit rule.
`[no] activate`	Enables the IPv6 session-limit rule. The no command disables the session limit rule.
`[no] address6` *address6_object*	Sets the IPv6 source IP address. The no command sets this to any, which means all IP addresses.

Table 119 Command Summary: Session Limit (continued)

COMMAND	DESCRIPTION
`[no] description` *description*	Sets a descriptive name (up to 64 printable ASCII characters) for a session-limit rule. The no command removes the descriptive name from the rule.
`exit`	Quits the sub-command mode.
`[no] limit <0...40000>`	Sets the limit for the number of concurrent NAT/firewall IPv6 sessions this rule's users or addresses can have. 0 means any.
`[no] user` *user_name*	Sets an IPv6 session-limit rule for the specified user. The no command resets the user name to the default (any). any means all users.
`session-limit6 append`	Enters the IPv6 session-limit sub-command mode to add a session-limit rule to the end of the session-limit rule list.
`session-limit6 delete` *rule_number*	Removes an IPv6 session-limit rule.
`session-limit6 flush`	Removes all IPv6 session-limit rules.
`session-limit6 insert` *rule_number*	Enters the IPv6 session-limit sub-command mode to add a session-limit rule before the specified rule number.
`session-limit6 move` *rule_number* `to` *rule_number*	Moves an IPv6 session-limit to the number that you specified.
`show session-limit6`	Shows the IPv6 session-limit configuration.
`show session-limit6 begin` *rule_number* `end` *rule_number*	Shows the settings for a range of IPv6 session-limit rules.
`show session-limit6` *rule_number*	Shows the IPv6 session-limit rule's settings.
`show session-limit6 status`	Shows the general IPv6 session-limit settings.

29.5 ADP Commands Overview

Anomaly Detection and Prevention (ADP) protects against anomalies based on violations of protocol standards (RFCs – Requests for Comments) and abnormal flows such as port scans. This section introduces ADP, anomaly profiles and applying an ADP profile to a traffic direction.

Traffic Anomalies

Traffic anomaly policies look for abnormal behavior or events such as port scanning, sweeping or network flooding. They operate at OSI layer-2 and layer-3. Traffic anomaly policies may be updated when you upload new firmware.

Protocol Anomalies

Protocol anomalies are packets that do not comply with the relevant RFC (Request For Comments). Protocol anomaly detection includes:

- TCP Decoder
- UDP Decoder

- ICMP Decoder
- IP Decoder

Protocol anomaly policies may be updated when you upload new firmware.

ADP Flood Detection Whitelist

Certain legitimate services, such as IP Sec with NAT traversal, might be erroniously treated as anomalous traffic by ADP flood detection. To prevent this, you can add the clients and/or services to the ADP Flood Detection Whitelist, which means they are not scanned for network flooding.

29.5.1 ADP Command Input Values

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 120 Input Values for ADP Commands

LABEL	DESCRIPTION
zone-rule	The name of a zone. For some Zyxel Device models, use up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case- sensitive. For other Zyxel Device models use pre-defined zone names like DMZ, LAN1, SSL VPN, WLAN, IPSec VPN, OPT, and WAN
adp-profile	The name of an ADP profile. It can consist of alphanumeric characters, the underscore, and the dash, and it is 1-31 characters long. Spaces are not allowed.

29.5.2 ADP Activation Commands

Use these commands to activate ADP and see status.

Table 121 ADP Activation Commands

LABEL	DESCRIPTION
[no] idp anomaly activate	Anomaly detection does not require registration. The no command disables the specified service.
show idp anomaly activation	Displays anomaly detection service status.

29.5.3 ADP Global Profile Commands

These commands apply to all ADP profiles on the Zyxel Device.

Table 122 ADP Global Profile Commands

LABEL	DESCRIPTION
idp rename anomaly *<profile1> <profile2>*	Rename an ADP anomaly profile originally named profile1 to profile2.
no idp anomaly *<profile3>*	Delete an ADP profile named profile3.
show idp anomaly base profile	Displays all anomaly detection base profiles.

Table 122 ADP Global Profile Commands (continued)

LABEL	DESCRIPTION
`show idp anomaly profiles`	Displays all ADP anomaly profiles.
`show idp anomaly rules`	Displays all ADP anomaly rules.

29.5.4 ADP Zone-to-Zone Rule Commands

These commands bind ADP profiles to traffic directions.

Table 123 ADP Zone-to-Zone Rule Commands

LABEL	DESCRIPTION
`idp anomaly rule {append | <1..32> | insert <1..32>}`	Creates an ADP anomaly rule and enters the sub-command mode.
`bind profile`	Binds the ADP anomaly profile to the entry's traffic direction.
`no bind`	Removes the ADP anomaly profile's binding.
`from-zone zone_rule`	Specifies the zone the traffic is coming from.
`[no] activate`	Turns on the ADP anomaly profile to traffic direction binding. The no command turns it off.
`idp anomaly rule {delete <1..32> | move <1..32> to <1..32>}`	Removes or moves an ADP anomaly profile to traffic direction entry.
`no idp anomaly rule <1..32>`	Removes an ADP anomaly profile to traffic direction entry.
`show idp anomaly rules`	Displays the ADP anomaly zone to zone rules.

29.5.5 ADP Add/Edit Profile Sub Commands

These commands create or edit ADP profiles.

Table 124 ADP Add/Edit Profile Commands

LABEL	DESCRIPTION
`idp anomaly` *`adp-profile`* `[base {all | everything | none}]`	Creates a new IDP anomaly profile called *`adp-profile`*. *`adp-profile`* uses the base profile you specify. Enters sub-command mode. All the following commands relate to the new profile. Use exit to quit sub-command mode.
`description` *`description`*	*`description:`* Use up to 60 printable ASCII characters
`no description`	The no command removes the descriptive name from the profile.
`base {all | everything | none}`	Use the base profile you specify. You cannot change the base profile after you specify it.
`scan-detection sensitivity {low | medium | high}`	Sets scan-detection sensitivity.
`no scan-detection sensitivity`	Clears scan-detection sensitivity. The default sensitivity is medium.
`scan-detection block-period <1..3600>`	Sets for how many seconds the ZyWALL / USG blocks all packets from being sent to the victim (destination) of a detected anomaly attack.

Table 124 ADP Add/Edit Profile Commands (continued)

LABEL	DESCRIPTION
`[no] scan-detection {tcp-xxx} {activate | log [alert] | block}`	Activates TCP scan detection options where {tcp-xxx} ={tcp-portscan | tcp-portscan-fin | tcp-portscan-syn tcp-portsweep }. Also sets TCP scan-detection logs or alerts and blocking. no deactivates TCP scan detection, its logs, alerts or blocking.
`[no] scan-detection {udp-portscan} {activate | log [alert] | block}`	Activates or deactivates UDP port scan . Also sets UDP scan-detection logs or alerts and blocking. no deactivates UDP scan detection, its logs, alerts or blocking.
`flood-detection block-period <1..3600>`	Sets for how many seconds the ZyWALL / USG blocks all packets from being sent to the victim (destination) of a detected anomaly attack.
`[no] flood-detection {tcp-flood | udp-flood | icmp-flood | igmp-flood} {activate | log [alert] | block}`	Activates or deactivates TCP, UDP,IGMP or ICMP flood detection. Also sets flood detection logs or alerts and blocking. no deactivates flood detection, its logs, alerts or blocking.
`[no] tcp-decoder {tcp-xxx} activate`	Activates or deactivates tcp decoder options where {tcp-xxx} = {bad-tcp-flag | bad-tcp-l4-size | tcp-fragment | tcp-land}
`tcp-decoder {tcp-xxx} log [alert]`	Sets tcp decoder log or alert options.
`no tcp-decoder {tcp-xxx} log`	Deactivates tcp decoder log or alert options.
`[no] tcp-decoder {tcp-xxx} action {drop | reject- sender | reject-receiver | reject-both}}`	Sets tcp decoder action.
`[no] udp-decoder {bad-udp-l4-size | udp-land | udp-smurf} activate`	Activates or deactivates udp decoder options.
`udp-decoder {bad-udp-l4-size | udp-land | udp-smurf} log [alert]`	Sets udp decoder log or alert options.
`no udp-decoder {bad-udp-l4-size | udp-land | udp-smurf} log`	Deactivates udp decoder log options.
`udp-decoder {bad-udp-l4-size | udp-land | udp-smurf} action {drop | reject-sender | reject-receiver | reject-both}`	Sets udp decoder action.
`no udp-decoder {bad-udp-l4-size | udp-land | udp-smurf} action`	Deactivates udp decoder actions.
`[no] icmp-decoder {bad-icmp-l4-size | icmp-fragment | icmp-smurf} activate`	Activates or deactivates icmp decoder options.

Table 124 ADP Add/Edit Profile Commands (continued)

LABEL	DESCRIPTION
icmp-decoder {bad-icmp-l4-size | icmp-fragment | icmp-smurf} log [alert]	Sets icmp decoder log or alert options.
no icmp-decoder {bad-icmp-l4-size icmp-fragment | icmp-smurf} log	Deactivates icmp decoder log options.
icmp-decoder {bad-icmp-l4-size | icmp-fragment | icmp-smurf} action {drop | reject-sender | reject-receiver | reject-both}	Sets icmp decoder action.
no icmp-decoder {bad-icmp-l4-size | icmp-fragment | icmp-smurf} action	Deactivates icmp decoder actions.
[no] ip-decoder {ip-spoof | ip-teardrop} activate	Activates or deactivates ip decoder options.
[no] ip-decoder {ip-spoof | ip-teardrop} log	Activates or deactivates ip decoder log options.
[no] ip-decoder {ip-spoof | ip-teardrop} action {drop | reject-sender | reject-receiver | reject-both}	Activates or deactivates ip decoder actions.
exit	Use exit to quit sub-command mode.
show idp anomaly profile scan-detection [all details]	Shows all scan-detection settings of the specified ADP profile.
show idp anomaly profile scan-detection {tcp-portscan | tcp-portscan-syn | tcp-portsweep | tcp-portscan-fin} details	Shows selected TCP scan-detection settings for the specified ADP profile.
show idp anomaly profile scan-detection {udp-portscan} details	Shows UDP scan-detection settings for the specified ADP profile.
show idp anomaly profile flood-detection [all details]	Shows all flood-detection settings for the specified ADP profile.
show idp anomaly profile flood-detection {tcp-flood | udp-flood | icmp-flood | icmp-flood} details	Shows flood-detection settings for the specified ADP profile.
show idp anomaly profile tcp-decoder all details	Shows tcp-decoder settings for the specified ADP profile.

Table 124 ADP Add/Edit Profile Commands (continued)

LABEL	DESCRIPTION
`show idp anomaly profile tcp-decoder {bad-tcp-flag | bad-tcp-l4-size | tcp-land} details`	Shows tcp-decoder settings for the specified ADP profile.
`show idp anomaly profile udp-decoder all details`	Shows udp-decoder settings for the specified ADP profile.
`show idp anomaly profile udp-decoder {bad-udp-l4-size | udp-land | udp-smurf} details`	Shows specific udp-decoder settings for the specified ADP profile.
`show idp anomaly profile icmp-decoder all details`	Shows all icmp-decoder settings for the specified ADP profile.
`show idp anomaly profile icmp-decoder {bad-icmp-l4-size | icmp-smurf} details`	Shows specific icmp-decoder settings for the specified ADP profile.
`show idp anomaly` *`adp-profile`* `ip-decoder all details`	Shows all ip-decoder settings for the specified ADP profile.
`show idp anomaly` *`adp-profile`* `ip-decoder {ip-spoof | ip-teardrop} details`	Shows specific ip-decoder settings for the specified ADP profile.

29.5.6 ADP Flood Detection Whitelist Commands

These commands apply add and remove clients/and or services from the ADP Flood Detection Whitelist. .

Table 125 ADP Global Profile Commands

LABEL	DESCRIPTION
`[no] idp anomaly white-list activate`	Enables or disables the ADP Flood Detection Whitelist on the Zyxel Device.
`idp anomaly white-list` *`rule-name`*	Enters the ADP Flood Detection Whitelist subcommand mode for the specified whitelist entry. If the entry does not currently exist, the Zyxel Device creates it.
`activate`	Enables the ADP Flood Detection Whitelist entry.
`deactivate`	Disables the ADP Flood Detection Whitelist entry.
`source {src-ipv4-obj | any} destination {dst-ipv4-obj | any} service {service_obj | any}`	Sets the source IPv4 object, destination IPv4 object, and service object that the entry applies to. Use *any* to match any source, destination, or service.
`no idp anomaly white-list` *`rule-name`*	Deletes the specified ADP Flood Detection Whitelist entry.

Table 125 ADP Global Profile Commands (continued)

LABEL	DESCRIPTION
`idp anomaly white-list rename` *`rule-name new-rule-name`*	Renames the specified ADP Flood Detection Whitelist entry.
`show idp anomaly white-list {all | rule-name}`	Displays information about a single ADP Flood Detection Whitelist entry. All displays the whole whitelist.

CHAPTER 30
Cloud CNM

30.1 Cloud CNM Overview

You need licenses to use Cloud CNM SecuManager, Cloud CNM SecuDeployer and Cloud CNM SecuReporter. You need the SecuManager license to get a CNM ID with which you can access the SecuManager server. It is independent from the Zyxel Devices. The SecuReporter license must be activated on each Zyxel Device. The SecuDeployer license must be activated on the SecuDeployer Zyxel Device server.

- Use SecuManager to enable and configure management of the Zyxel Device by a Central Network Management system.
- Use SecuReporter to enable SecuReporter logging on your Zyxel Device, see license status, type, expiration date and access a link to the SecuReporter web portal. The SecuReporter web portal collects and analyzes logs from your Zyxel Device in order to identify anomalies, alert on potential internal / external threats, and report on network usage.
- Use SecuDeployer to enable SecuDeployer which allows a Zyxel Device SecuDeployer server to mange and apply profile template settings to remote Zyxel Device clients. Provisioning can include the settings of one to multiple LAN/DMZ interfaces, Hub & Spoke IPSec tunnels, and/or static route settings for VTI IPSec VPNs.
- Use Nebula to manage your Zyxel Device using the Nebula Control Center (NCC). NCC is a cloud based network management system that allows you to remotely manage and monitor your Zyxel Device. Use NCC to manage your Zyxel Device with accounts at different privilege levels.

Note: SecuManager and SecuDeployer cannot both be enabled on a Zyxel Device at the same time.

30.2 Cloud CNM SecuManager

Cloud CNM SecuManager is a Virtual Machine-based (VM) management system that uses the TR-069 protocol to encapsulate commands to ZyWALL/USG devices for management and monitoring; these devices must have firmware that supports the TR-069 protocol.

Cloud CNM SecuManager features include:

- Batch import of managed devices at one time using one CSV file
- See an overview of all managed devices and system information in one place
- Monitor and manage devices
- Install firmware to multiple devices of the same model at one time
- Back up and restore device configuration
- View the location of managed devices on a map
- Receive notification for events and alarms, such as when a device goes down

- Graphically monitor individual devices and see related statistics
- Directly access a device for remote configuration
- Create four types of administrators with different privileges
- Perform Site-to-Site, Hub & Spoke, Fully-meshed and Remote Access VPN provisioning.

To allow Cloud CNM SecuManager management of your Zyxel Device:

- You must have a Cloud CNM SecuManager license with CNM ID number or a Cloud CNM SecuManager server URL.
- The Zyxel Device must be able to communicate with the Cloud CNM SecuManager server.

You must configure SecuManager to allow the Zyxel Device to find the Cloud CNM SecuManager server.

30.2.1 Introduction to XMPP

eXtensible Messaging and Presence Protocol (XMPP) allows Zyxel Device to contact managed devices that normally can't be contacted directly due to they are behind a NAT or firewall-enabled gateway.

The managed devices must be able to establish a secure and authenticated connection to an XMPP Server and must be able to maintain a connection to an XMPP Server through which the XMPP Server can send unsolicited messages from a defined set of allowed addresses (Zyxel Device servers. This is defined in RFC 6120.

The general procedure for XMPP to issue a Connection Request to a managed device is as follows:

1. Zyxel Device establishes a connection to an XMPP Server.
2. The device establishes an XMPP connection to the specified XMPP Server.
3. Whenever Zyxel Device wishes to establish a connection to the device, it can send an XMPP Connection Request specifying the 'to' address that matches the device where the Connection Request needs to be sent and a 'from' address that matches one of the allowed Zyxel Device addresses in the XMPP Server.
4. The XMPP Server sends the request to the appropriate device.

Note: There could be multiple XMPP Servers depending on the deployment.

30.2.1.1 Zyxel Device Requirements for XMPP

Both Zyxel Device and the managed device must meet these requirements:

- They must be able to determine the public IP address of the XMPP Server.
- They must be able to open an XML Stream to the XMPP Server and accept an XML Stream from the XMPP Server. XML Streams are unidirectional and this XMPP Connection Request mechanism requires the use of two XML Streams over a single TCP connection.
- They must be able to use Transport Layer Security (TLS) to establish an encrypted and secure TCP connection with the XMPP Server
- They must be able to use Simple Authentication and Security Layer (SASL) to authenticate with the XMPP Server. A Username and Password are used as the credentials for the SASL authentication procedure.
- They must be able to reestablish the connection to the XMPP Server if the connection is lost.

30.2.1.2 Managed Device Additional Requirements

The managed device must also meet these requirements:

- A managed device must be able to maintain the TCP connection to the XMPP Server using 'whitespace keepalive'.
- A managed device must be able to listen for XMPP Connection Request messages sent from an allowed list, and respond to these messages when they arrive. When it receives an XMPP Connection Request message, it must both validate and authenticate the message. It must also continue to listen for HTTP-based Connection Requests.
- Whenever a managed device receives, successfully validates, and authenticates an XMPP Connection Request with an Zyxel Device server from an allowed IP address, it must establish a connection with Zyxel Device server and will respond with a '6 CONNECTION REQUEST' EventCode.
- The managed device may reply with a 'service- unavailable' error, code 503, if the number of connection requests exceeds a certain threshold (to reduce the possibility of a Denial of Service attack) or if it is already in a session with another Zyxel Device server.

30.2.2 Cloud CNM SecuManager Commands

The CNM agent allows communications between the Zyxel Device and Cloud CNM SecuManager server using TR-069 Remote Procedure Calls (RPCs).

You must be in configuration mode (`configure terminal`) to use the indented commands shown below.

Table 126 Command Summary: Cloud CNM SecuManager

COMMAND	DESCRIPTION
`show cnm-agent configuration`	Displays current Cloud CNM SecuManager network management configuration on the Zyxel Device.
`[no] cnm-agent activate`	Allows management of the Zyxel Device by a Cloud CNM SecuManager server. The no command disallows management of the Zyxel Device by a Cloud CNM SecuManager server.
`[no] cnm-agent auto-get-acs activate`	Automatically lets the Zyxel Device get the Cloud CNM SecuManager server URL from myZyxel. The Cloud CNM SecuManager server must be able to access myZyxel and you must have a CNM ID from the Cloud CNM license. The no command disallows the Zyxel Device getting the Cloud CNM SecuManager server URL from myZyxel, so you must manually configure it.
`(no) cnm-agent enable-cnm-id`	Allows Cloud CNM SecuManager to get the URL from myZyxel. The no command means you must provide a CNM URL using `cnm-agent manager {https_url|http_url}`
`[no] cnm-agent cnm-id <ID>`	The CNM ID is used by Cloud CNM SecuManager to get the URL from myZyxel.Enter the CNM ID exactly as on the Cloud CNM SecuManager license. The CNM ID can be from 0 to 80 characters long using these characters:[a-zA-Z0-9-][\.a-zA-Z0-9_-]. The no command removes the CNM ID.

Table 126 Command Summary: Cloud CNM SecuManager (continued)

COMMAND	DESCRIPTION
`[no] cnm-agent manager {https_url|http_url}`	Sets the URL (HTTP or HTTPs) for theCloud CNM SecuManager server. The string must be less than 255 characters. Enter the IPv4 IP address of the Cloud CNM SecuManager server followed by the port number (default 7547 for HTTPS or 7549 for HTPP) followed by the CNM ID from the license in CNM URL. For example, if you installed Cloud CNM SecuManager on a server with IP address 1.1.1.1 and CNM ID V6ABQNTPYGD, then type `1.1.1.1:7547/V6ABQNTPYG` or `1.1.1.1:7549/V6ABQNTPYG` as the CNM URL. The no command removes the URL (HTTP or HTTPs) for the Cloud CNM SecuManager server.
`[no] cnm-agent periodic-inform activate`	Enables the Zyxel Device to send Inform messages to the Cloud CNM SecuManager server informing of its presence at regular intervals. The no command disables the Zyxel Device from sending Inform messages to the Cloud CNM SecuManager server.
`[no] cnm-agent periodic-inform interval <10…86400>`	Sets how often the Zyxel Device should inform the Cloud CNM SecuManager server of its presence. The valid range for the interval is from 10 to 86400 seconds. The no command removes the interval.
`[no] cnm-agent acs username tr069_acs_username`	Sets the Cloud CNM SecuManager connection request user name. The user name can be from 0 to 254 characters long using these characters: [a-zA-Z0-9-][\.a-zA-Z0-9_-]. The no command removes the TR069 account user name.
`[no] cnm-agent acs password tr069_acs_password`	Sets the Cloud CNM SecuManager connection request password associated with the user name. The password can be from 0 to 254 characters long using these characters: [a-zA-Z0-9-][\.a-zA-Z0-9_-]. The no command removes the password.
`[no] cnm-agent password`	Sets the password to authenticate the Zyxel Device. The no command removes the password.
`[no] cnm-agent vantage certificate tr069_cert_file_name`	Sets the Cloud CNM SecuManager server's certificate in HTTPS authentication as TR-069 needs to verify this. The certificate name can be from 1 to 127 characters long using these characters: [a-zA-Z0-9_\.-]. The no command disables using the server's certificate in HTTPS authentication.
`[no] cnm-agent authentication enable`	Sets authentication of the Cloud CNM SecuManager server's certificate. The no command disables authentication.
`cnm-agent server-type [vantage | tr069]`	Sets the management server to be Vantage or Cloud CNM SecuManager. At the time of writing, Vantage is no longer supported.
`[no] cnm-agent auto-get-acs activate`	Allows the Zyxel Device to get the Cloud CNM SecuManager URL from myZyxel. The no command disallows the Zyxel Device from getting the Cloud CNM SecuManager URL from myZyxel.
`[no] cnm-agent trigger-inform <0..8640>`	Specifies the time interval for the Zyxel Device to send Inform messages. The valid range for the interval is in 10-second multiples where 0 means 0 to 10 seconds, 1 means 10 to 20 seconds, and so on. The no command removes the interval.

Table 126 Command Summary: Cloud CNM SecuManager (continued)

COMMAND	DESCRIPTION
[no] cnm-agent username	Creates a Zyxel Device user for Cloud CNM SecuManager authentication. The user name can be from 0 to 254 characters long using these characters: [a-zA-Z0-9-][\.a-zA-Z0-9_-]. The no command removes the Zyxel Device user from Cloud CNM SecuManager authentication.
[no] cnm-agent xmpp-domain *xmpp_domain*	Enter the XMPP domain name of the Cloud CNM SecuManager. The XMPP domain can be from 0 to 80 characters long using these characters:[a-zA-Z0-9-][\.a-zA-Z0-9_-]. The no command removes the domain name of the Cloud CNM SecuManager.
[no] cnm-agent xmpp-host *xmpp_host*	Enter the IP address or FQDN of the Cloud CNM SecuManager. The no command removes the IP address or FQDN of the Cloud CNM SecuManager.
[no] cnm-agent xmpp-password *xmpp_password*	Enter the password of the Cloud CNM SecuManager. The XMPP password can be from 0 to 80 characters long using these characters: [a-zA-Z0-9-][\.a-zA-Z0-9_-]. The no command removes the password of the Cloud CNM SecuManager.
[no] cnm-agent xmpp-resource *xmpp_resource*	Enter the XMPP resource ID of the Cloud CNM SecuManager. The XMPP resource ID can be from 0 to 80 characters long using these characters: [a-zA-Z0-9-][\.a-zA-Z0-9_-]. The no command removes the XMPP resource ID of the Cloud CNM SecuManager.
[no] cnm-agent xmpp-username *xmpp_username*	Enter the XMPP account user name of the Cloud CNM SecuManager. The XMPP account user name can be from 0 to 80 characters long using these characters: [a-zA-Z0-9-][\.a-zA-Z0-9_-] The no command removes the XMPP account user name of the Cloud CNM SecuManager.
[no] cnm-agent encrypted-xmpp-password	Enter the XMPP account encrypted password of the Cloud CNM SecuManager. The no command removes the XMPP account encrypted password of the Cloud CNM SecuManager.
show secumanager status	Displays the active status, server, port and server Certificate Authority (CA) on SecuManager 2. Note: This command is for custom projects only.
[no] secumanager activate	Allows management of the Zyxel Device by a SecuManager 2 server. The no command disallows management of the Zyxel Device by a SecuManager 2 server. Note: This command is for custom projects only.

Table 126 Command Summary: Cloud CNM SecuManager (continued)

COMMAND	DESCRIPTION
`secumanager server {IPv4| FQDN} port <1…65535>`	• Sets the IPv4 address or the FQDN of the SecuManager 2 server • Sets a port number for the SecuManager 2 server. Enter a number between 1 and 65535 Note: This command is for custom projects only.
`secumanager server-ca {default| CERT_NAME}`	Specify the CA certificate for validate the certificate of SecuManager 2 server. • `default`: Use the Zyxel Device's default CA • `CERT_NAME`: Specify the name of a CA for the SecuManager 2 server Note: This command is for custom projects only.

30.2.3 Cloud CNM SecuManager Command Example

The following example shows what Cloud CNM SecuManager configurations you have made.

```
Router# show cnm-agent configuration
Activate: NO
ACS URL:
ACS Username:
ACS Password:
Username:
Password:
Server Type: TR069 ACS
Periodic Inform: DISABLE
Periodic Inform Interval: 3600
HTTPS Authentication: NO
Vantage Certificate:
Auto-get-ACS Activate: NO
CNM-ID:
XMPP Activate: NO
XMPP Username:
XMPP Domain:
XMPP Resource:
XMPP Host:
Router#
```

30.3 Cloud CNM SecuReporter

Cloud CNM SecuReporter is a security analytics portal accessible using a web browser, that collects and analyzes logs from SecuReporter-licensed Zyxel Devices in order to identify anomalies, alert on potential internal / external threats, and report on network usage. You need to buy a SecuReporter license for your Zyxel Device and register it at myZyxel using your myZyxel account. The Zyxel Device must be able to communicate with the myZyxel server.

Cloud CNM SecuReporter can simultaneous support up to 40,000 units at the time of writing.

30.3.1 Cloud CNM SecuReporter Commands

SecuReporter stores logs in a temporary file for uploading to the SecuReporter portal for security analysis. How often to upload is determined by the upload interval (default every 300 seconds) or upload file size (default is when the temporary log file reaches 10 MB). More frequent uploads provides better real-time log analysis, but uses more bandwidth and CPU processing power.

You must be in configuration mode (`configure terminal`) to use the indented commands shown below.

Table 127 Command Summary: Cloud CNM SecuReporter

COMMAND	DESCRIPTION
`secu-reporter activate {no | yes}`	Use `yes` to send security-related logs to the SecuReporter portal. Use `no` to disable SecuReporter logging. SecuReporter must be enabled to collect and analyze logs from this Zyxel Device. • You must read and accept the General Data Protection Regulation (GDPR) privacy policy by enabling SecuReporter in the Web Configurator before you can enable it by using the CLI. • SecuReporter is enabled by default if you have activated a SecuReporter Standard license, • SecuReporter is disabled by default if you have a SecuReporter Trial license. • You cannot enable SecuReporter if you do not have a SecuReporter license.
`show service-register status secu-reporter`	Displays current Cloud CNM SecuReporter registration status at myZyxel.
`show secu-reporter status`	Displays current Cloud CNM SecuReporter status on this Zyxel Device.
`secu-reporter traffic-log {activate | deactivate}`	Use `activate` to send traffic logs to the SecuReporter portal for application usage analysis via this Zyxel Device. This may cause an increase in traffic to SecuReporter from this Zyxel Device. Use `deactivate` to disable sending traffic logs if it impacts Zyxel Device performance.
`secu-reporter upload-filesize <1..10>`	A temporary log file is uploaded to the SecuReporter security analytics portal when it meets the size set here (in megabytes) or the interval defined in the following field. 10 MB is the default. Set it to a smaller number for more frequent uploads.
`secu-reporter upload-interval <60..600>`	A temporary log file is uploaded to the SecuReporter security analytics portal at the interval defined here or when it meets the size setin the previous field. 300 seconds is the default. Set it to a smaller number for more frequent uploads.
`secu-reporter adp {activate|deactivate}`	The `activate` command will have the Zyxel Device send ADP logs to SecuReporter for analysis and trend spotting.
`secu-reporter anti-spam {activate|deactivate}`	The `activate` command will have the Zyxel Device send anti-spam logs to SecuReporter for analysis and trend spotting.
`secu-reporter anti-virus {activate|deactivate}`	The `activate` command will have the Zyxel Device send anti-virus logs to SecuReporter for analysis and trend spotting.
`secu-reporter ap-managed {activate|deactivate}`	The `activate` command will have the Zyxel Device send logs of the APs connected to the Zyxel Device to SecuReporter for analysis and trend spotting.
`secu-reporter app-patrol {activate|deactivate}`	The `activate` command will have the Zyxel Device send application patrol logs to SecuReporter for analysis and trend spotting.
`secu-reporter content-filter {activate|deactivate}`	The `activate` command will have the Zyxel Device send content filtering and URL Threat filtering logs to SecuReporter for analysis and trend spotting.

Table 127 Command Summary: Cloud CNM SecuReporter (continued)

COMMAND	DESCRIPTION
`secu-reporter idp {activate|deactivate}`	The `activate` command will have the Zyxel Device send IDP logs to SecuReporter for analysis and trend spotting.
`secu-reporter interface-statistics {activate|deactivate}`	The `activate` command will have the Zyxel Device send logs of interface statistics to SecuReporter for analysis and trend spotting.
`secu-reporter reputation-filter {activate|deactivate}`	The `activate` command will have the Zyxel Device send IP reputation and URL Threat filter logs to SecuReporter for analysis and trend spotting. Note: This command is for the ATP series.
`secu-reporter sandbox {activate|deactivate}`	The `activate` command will have the Zyxel Device send sandboxing logs to SecuReporter for analysis and trend spotting. Note: This command is for the ATP series.
`secu-reporter traffic-log {activate|deactivate}`	The `activate` command will have the Zyxel Device send traffic logs to SecuReporter for analysis and trend spotting.
`secu-reporter vpn {activate|deactivate}`	The `activate` command will have the Zyxel Device send VPN logs to SecuReporter for analysis and trend spotting.
`secu-reporter anti-botnet {activate|deactivate}`	The `activate` command will have the Zyxel Device send URL Threat filtering logs to SecuReporter for analysis and trend spotting. Note: This command is for the ATP series.
`show secu-reporter category status`	Displays the activation status of each service logged by SecuReporter.
`show {ip-reputation| dns-filter| threat-website} sr-allow-list`	Displays IP reputation, DNS threat filter or URL threat filter allow list settings on SecuReporter. If you want to change the SecuReporter IP reputation, DNS threat filter or URL threat filter allow list settings, go to SecuReporter. For example, if you add 1.1.1.1 to the SecuReporter IP reputation allow list, the Zyxel Device IP reputation will allow incoming packets from 1.1.1.1 and outgoing packets to 1.1.1.1.
`secu-reporter on-cloud-config {dns-threat-filter| ip-reputation| url-threat-filter} update`	Updates IP reputation, DNS threat filter or URL threat filter allow list settings from SecuReporter.

30.3.2 Cloud CNM SecuReporter Commands Example

The following example shows Cloud CNM SecuReporter registration, configurations and configuration status.

```
Router# show service-register status secu-reporter
Service                                Status          Type               Count
Expiration Grace Purchasable Activatable
================================================================================
SecuReporter                         Activated      Standard          N/A   295
0     N/A         0
Router# configure terminal
Router(config)# secu-reporter activate yes
Router(config)# secu-reporter traffic-log activate
Router(config)# secu-reporter upload-filesize 5
Router(config)# secu-reporter upload-interval 100
Router(config)# exit
Router# show secu-reporter status
activate: yes
send-reporter: yes
upload-interval: 100
upload-filesize: 5
banner: yes
last-upload-sync: 2024-03-05 05:32:00
last-upload-status: Success
last-download-allow-list-sync: N/A
last-download-allow-list-status: N/A
utf-last-update: N/A
ipr-last-update: N/A
dtf-last-update: N/A
Router#
```

30.4 Management Modes

You can manage the Zyxel Device in one of the following modes:

- On Premises Mode: monitor and manage the Zyxel Device using the web configurator.
- Nebula Mode: monitor and manage the Zyxel Device mainly using the NCC.
- Cloud Monitoring Mode: monitor the Zyxel Device using the Nebula Control Center (NCC) and manage the Zyxel Device using the web configurator.

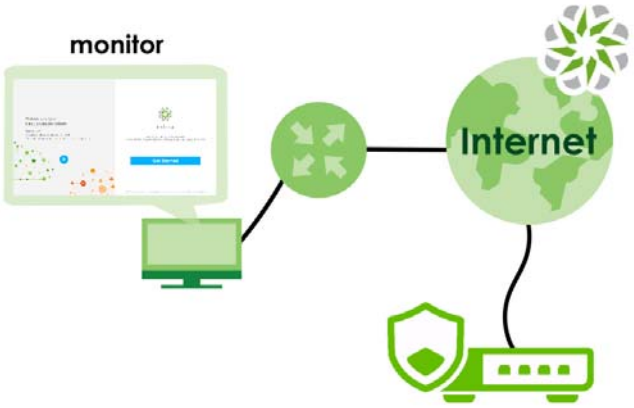
Use Cloud Monitoring Mode to monitor your Zyxel Device using the NCC but configure settings on the web configurator at the same time. You can access the web configurator remotely using SSH or HTTPS.

Note: You cannot set the Zyxel Device to Cloud Monitoring Mode if Device HA is enabled on the Zyxel Device.

30.5 Nebula

The Nebula Control Center (NCC) is a cloud based network management system that allows you to remotely manage and monitor your Zyxel Device with accounts at different privilege levels.

Figure 26 Nebula Mode Example



30.6 Cloud Monitoring Mode

You must have created an organization and a site on the NCC first. Follow the steps below to set the Zyxel Device to Cloud Monitoring Mode.

Figure 27 Cloud Monitoring Mode Example

On Premises Mode to Cloud Monitoring Mode

1. Back up the Zyxel Device configurations.
2. Enable Cloud Monitoring Mode.
3. Enter the Monitor mode ID of an organization you created on Nebula. See the organization Monitor mode ID on Nebula in Organization-wide > Organization-wide manage > Organization settings.
4. Check the result using the `show monitor-mode` command.

The following table explains the possible results that might display.

Table 128 Cloud Monitoring Mode Status

N/A	You've not entered a Monitor mode ID on the Zyxel Device.
Connected	The Zyxel Device is connected to Nebula. Check the Zyxel Device Device Type on Nebula in Organization-wide > License & inventory.
Disconnected - Server is not reachable	The Zyxel Device cannot connect to Nebula. Please make sure the Zyxel Device can access Nebula at *.nebula.zyxel.com and ports 443, 4335 and 6667 are enabled.
Disconnected - Connection failure	The Zyxel Device failed to connect to Nebula. Make sure the Zyxel Device settings match the Nebula settings.
Disconnected - Registration failure	The email registered on myZyxel and the email registered on the Nebula organization to which you want to add the Zyxel Device are different.
Disconnected - Operation modes mismatch	Remove the Zyxel Device from the Nebula organization and site.

Nebula Mode to Cloud Monitoring Mode

First, go from Nebula Mode to On Premises Mode, then use the commands to go to Cloud Monitoring Mode.

1 Remove the Zyxel Device from all organizations and sites.

2 If the Zyxel Device is connected to Nebula, the Zyxel Device will automatically reset after you remove the Zyxel Device from all organizations and sites. If the Zyxel Device is not connected to Nebula, press the reset button.

3 After the PWR LED turns steady green, log into the Zyxel Device and select On Premises Mode in the initial setup wizard.

30.6.1 Nebula Monitor Mode Command

You must be in configuration mode (`configure terminal`) to use the commands shown below.

Table 129 Nebula Monitor Mode Command

COMMAND	DESCRIPTION
`[no] monitor-mode`	Enable or disable cloud monitoring mode.
`monitor-mode id <organization-id>`	Enter the organization ID to which you want to add the Zyxel Device.
`show monitor-mode`	Displays cloud monitoring mode settings; see Section 30.6 on page 248 for more information.

To go to Cloud Monitoring Mode using the commands:

1 Enable Cloud Monitoring Mode.

```
Router> configure terminal
Router(config)# monitor-mode
```

2 Enter the organization ID to which you want to add the Zyxel Device.

```
Router(config)# monitor-mode id xxxxxxxxxx
```

3 Check the result using `show monitor-mode`.

```
Router(config)# show monitor-mode
active: yes
ID: xxxxxxxxxx
status: connected
is_connected: yes
```

CHAPTER 31
Web Authentication

31.1 Web Authentication Overview

Web authentication intercepts network traffic, according to the authentication policies, until the user authenticates his or her connection through a specifically designated login web page. This means all web page requests can initially be redirected to a special web page that requires users to authenticate their sessions. Once authentication is successful, the user can then connect to the rest of the network or Internet.

As soon as a user attempt to open a web page, the Zyxel Device reroutes the user's browser to a web portal page that prompts the user to log in.

31.1.1 User Two-Factor Authentication

Two-factor authentication adds an extra layer of security for users logging into the Zyxel Device. When two-factor authentication is enabled, a user has to first enter their username and password, and then enter a second one-time password when logging in.

Web authentication supports two-factor authentication using Google Authenticator. When enabled, the web authentication page first prompts the user to enter their username and password (factor 1), and then prompts them to enter a time-limited code from the Google Authenticator app (factor 2).

Note: It is also possible to configure two-factor authentication for VPN and admin users. For details, see Section 56.4 on page 481.

Note: The admin two-factor authentication settings override the web authentication two-factor authentication settings if both are configured.

31.1.1.1 Google Authenticator

The following is a list of specifications and limitations on using Google Authenticator for two-factor authentication.

- ext-users (external users) are not supported.
- A user must setup Google Authenticator on their mobile device before they can successfully authenticate with the Zyxel Device.
- Verification code length: 6 digits.
- Maximum verification code failed attempts: 3
- Backup code length: 8 digits
- Google authenticator is supported in device High Availability (HA) mode. The secret keys are synchronized between all Zyxel Devices.

31.1.2 802.1X Single Sign-On

802.1X Single Sign-On allows the Zyxel Device to use the same username and password for 802.1X WiFi authentication and web authentication. When enabled, a user logs into a WiFi network on the Zyxel Device that has 802.1X (WPA Enterprise) enabled. The Zyxel Device then reuses the 802.1X username and password for web authentication, preventing the user from having to log in twice.

Note: Active Directory Single Sign-On takes priority over 802.1X Single Sign-On, if both are enabled.

31.1.3 Summary of User Authentication Methods

The following table summarizes how users authenticate with the Zyxel Device when web authentication is enabled.

Table 130 User Authentication Methods

CLIENT	SINGLE SIGN-ON	GOOGLE AUTHENTICATOR	USER AUTHENTICATION STEPS
802.1X	No	No	1. 802.1X - Username/password 2. Web Authentication Portal - Username/password
	No	Yes	1. 802.1X - Username/password 2. Web Authentication Portal - Username/password 3. Web Authentication Portal - Google Authenticator code
	Yes (802.1X SSO)	No	1. 802.1X - Username/password
	Yes (802.1X SSO)	Yes	1. 802.1X - Username/password 2. Web Authentication Portal - Google Authenticator code
Non-802.1X	No	No	1. Web Authentication Portal - Username/password
	No	Yes	1. Web Authentication Portal - Username/password 2. Web Authentication Portal - Google Authenticator code
	Yes (Active Directory SSO)	No	None needed (if user is using Windows)
	Yes (Active Directory SSO)	Yes	None needed (if user is using Windows)

31.2 Web Authentication Commands

This table lists the commands for forcing user authentication. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 131 web-auth Commands

COMMAND	DESCRIPTION
`[no] web-auth activate`	Enables force user authentication that force users to log in to the Zyxel Device before the Zyxel Device routes traffic for them. The no command means the user authentication is not required.
`web-auth default-rule authentication {required | unnecessary} {no log | log [alert]}`	Sets the default authentication policy that the Zyxel Device uses on traffic that does not match any exceptional service or other authentication policy. `required`: Users need to be authenticated. They must manually go to the Zyxel Device's login screen. The Zyxel Device will not redirect them to the login screen. `unnecessary`: Users do not need to be authenticated. `no log | log [alert]`: Select whether to have the Zyxel Device generate a log (`log`), log and alert (`log alert`) or not (`no log`) for packets that match this default policy.
`web-auth [no] exceptional-service` *`service_name`*	Sets a service which you want users to be able to access without user authentication. The no command removes the specified service from the exceptional list.
`web-auth google-auth valid-time <`*`1..5`*`>`	Sets maximum time, in minutes, that a user has to authenticate using Google Authenticator before the authentication attempt fails. The setting only takes effect if Google Authenticator is enabled in the web authentication policy.
`web-auth login setting`	Sets the login web page through which the user authenticates his or her connection before he or she can then connect to the rest of the network or Internet. See Table 133 on page 256 for the sub-commands.
`web-auth method portal`	Sets a client to authenticate with the Zyxel Device through the specifically designated web portal.
`web-auth policy <1..1024>`	Creates the specified condition for forcing user authentication, if necessary, and enters sub-command mode. The conditions are checked in sequence, starting at 1. See Table 133 on page 256 for the sub-commands.
`web-auth policy append`	Creates a new condition for forcing user authentication at the end of the current list and enters sub-command mode. See Table 133 on page 256 for the sub-commands.
`web-auth policy insert <1..1024>`	Creates a new condition for forcing user authentication at the specified location, renumbers the other conditions accordingly, and enters sub-command mode. See Table 133 on page 256 for the sub-commands.
`web-auth policy delete <1..1024>`	Deletes the specified condition. To modify a condition, you can insert a new condition (N) and then delete the one (N+1) that you want to modify.
`web-auth policy flush`	Deletes every condition.
`web-auth policy move <1..1024> to <1..1024>`	Moves the specified condition to the specified location and renumbers the other conditions accordingly.
`[no] web-auth redirect-fqdn` *`host_str`*	Set the Fully-Qualified Domain Name (FQDN) of the Zyxel Device interface to which the clients connect. The no command removes the specified FQDN. *`host_str`*: the fully qualified domain name for the host.

Table 131 web-auth Commands (continued)

COMMAND	DESCRIPTION
`show web-auth redirect-fqdn`	Displays the FQDN of the Zyxel Device interface to which the clients connect to authenticate through the internal web portal page
`web-auth redirect-parameter`	Enters redirect parameter subcommand mode, and change the names of the following parameters. • `ap_ip` • `ap_mac` • `client_ip` • `client_mac` • `ssid_name` • `vlan_id` To use an external web portal for web authentication, you need to use the parameters' names that are adopted by the external web portal. Thus, you can be directed successfully to the external web portal. The Zyxel Device will automatically add these parameters to the URL of the external web portal when you're directed to the web portal for web authentication.
`{ap_ip|ap_mac|client_ip|client_mac|ssid_name|vlan_id } new_parameter`	Changes the name of the following parameters. You can only change a parameter's name at a time. {ap_ip|ap_mac|client_ip|client_mac|ssid_name| vlan_id}: Enters the parameter of which you want to change the name. *new_parameter*: Enters a new name for the parameter.
`mac_delimiter {colon|hyphen}`	Specifies the separator the external server uses for the two-character pairs within MAC addresses used. For example, use `mac delimiter hyphen` if you need to use a MAC address formatted like 00-11-AC-01-A0-11.
`no web-auth redirect-parameter`	Resets the names of the parameters to the default settings.
`show web-auth redirect-parameter`	Displays the names of the following parameters: • `ap_ip` • `ap_mac` • `client_ip` • `client_mac` • `ssid_name` • `vlan_id`
`web-auth web-portal`	Enters web portal subcommand mode.
`session-page {activate | deactivate}`	Redirects to a 'Welcome page' after login when activated.
`show web-auth activation`	Displays whether forcing user authentication is enabled or not.
`show web-auth default-rule`	Displays settings of the default web authentication policy.
`show web-auth exceptional-service`	Displays services that users can access without user authentication.
`show web-auth method`	Displays whether a client is to authenticate with the Zyxel Device through the specifically designated web portal when web authentication is enabled.
`show web-auth policy {<1..1024> | all}`	Displays details about the policies for forcing user authentication.

Table 131 web-auth Commands (continued)

COMMAND	DESCRIPTION
`show web-auth portal status`	Displays the web portal page settings.
`show web-auth status`	Displays the web portal page settings.

31.2.1 web-auth login setting Sub-commands

The following table describes the sub-commands for the web-auth login setting command.

Table 132 web-auth login setting Sub-commands

COMMAND	DESCRIPTION
`exit`	Leaves the sub-command mode.
`type {external | internal}`	Sets the login page appears whenever the web portal intercepts network traffic, preventing unauthorized users from gaining access to the network. `internal`: Use the default login page built into the Zyxel Device. `external`: Use a custom login page from an external web portal instead of the default one built into the Zyxel Device. You can configure the look and feel of the web portal page. Note: If you select the external option, you cannot use endpoint security to make sure that users' computers meet specific security requirements before they can access the network.
`[no] error-url` *`url`*	Sets the error page's URL; for example, http://IIS server IP Address/error.html. You can use up to 255 characters (0-9a-zA-Z;/?:@&=+$\.-_!~'()%,) in quotes. The no command removes the URL. The Internet Information Server (IIS) is the web server on which the web portal files are installed.
`[no] internal-welcome-url` *`url`*	Sets the welcome page's URL when you select to use the default login page built into the Zyxel Device; for example, http://IIS server IP Address/welcome.html. You can use up to 255 characters (0-9a-zA-Z;/?:@&=+$\.-_!~'()%,) in quotes. The no command removes the URL. The Internet Information Server (IIS) is the web server on which the web portal files are installed.
`[no] login-url` *`url`*	Sets the login page's URL; for example, http://IIS server IP Address/login.html. You can use up to 255 characters (0-9a-zA-Z;/?:@&=+$\.-_!~'()%,) in quotes. The no command removes the URL. The Internet Information Server (IIS) is the web server on which the web portal files are installed.
`[no] logout-ip` *`ipv4_address`*	Sets an IP address that users can use to terminate their sessions manually by entering the IP address in the address bar of the web browser. The no command removes the IP address.

Table 132 web-auth login setting Sub-commands (continued)

COMMAND	DESCRIPTION
`[no] logout-url url`	Sets the logout page's URL; for example, http://IIS server IP Address/logout.html. You can use up to 255 characters (0-9a-zA-Z;/?:@&=+$\-_!~'()%,) in quotes. The no command removes the URL. The Internet Information Server (IIS) is the web server on which the web portal files are installed.
`[no] session-url url`	Sets the session page's URL; for example, http://IIS server IP Address/session.html. You can use up to 255 characters (0-9a-zA-Z;/?:@&=+$\-_!~'()%,) in quotes. The no command removes the URL. The Internet Information Server (IIS) is the web server on which the web portal files are installed.
`[no] terms-of-service`	Forces users to agree to the terms before they can use the service. An agreement checkbox will display in the login page. The no command allows users to use the service without agreeing to the terms.
`[no] welcome-url url`	Sets the welcome page's URL; for example, http://IIS server IP Address/welcome.html. You can use up to 255 characters (0-9a-zA-Z;/?:@&=+$\-_!~'()%,) in quotes. The no command removes the URL. The Internet Information Server (IIS) is the web server on which the web portal files are installed.

31.2.2 web-auth policy Sub-commands

The following table describes the sub-commands for an web-auth policy (`web-auth policy 1-1024`). Note that not all rule commands use all the sub-commands listed here.

Table 133 web-auth policy Sub-commands

COMMAND	DESCRIPTION
`[no] activate`	Activates the specified condition. The no command deactivates the specified condition.
`[no] authentication {force | required}`	Selects the authentication requirement for users when their traffic matches this policy. The no command means user authentication is not required. `force`: Users need to be authenticated and the Zyxel Device automatically display the login screen when users who have not logged in yet try to send HTTP traffic. `required`: Users need to be authenticated. They must manually go to the login screen. The Zyxel Device will not redirect them to the login screen.
`authentication-type {<profile name> | default-user-agreement | default-web-portal | facebook-wifi}`	Select the authentication type profile you want to use in this policy. facebook-wifi is available when you enable Facebook Wi-Fi on the Zyxel Device. Note: If you set the authentication type to `facebook-wifi`, the destination address must be `any`. Note: You can configure the web-portal and user-agreement profile using the `web-auth type profile` commands.

Table 133 web-auth policy Sub-commands (continued)

COMMAND	DESCRIPTION
`[no] description description`	Sets the description for the specified condition. The no command clears the description. *description*: You can use alphanumeric and ( )+/:=?!*#@$_%- characters, and it can be up to 60 printable ASCII characters long.
`[no] destination {address_object | group_name}`	Sets the destination criteria for the specified condition. The no command removes the destination criteria, making the condition effective for all destinations.
`[no] force`	Forces users to log in to the Zyxel Device if the specified condition is satisfied. The no command means that users do not log in to the Zyxel Device.
`interface interface_name`	Sets an interface on which packets for the policy must be received.
`[no] schedule schedule_name`	Sets the time criteria for the specified condition. The no command removes the time criteria, making the condition effective all the time.
`[no] source {address_object | group_name}`	Sets the source criteria for the specified condition. The no command removes the source criteria, making the condition effective for all sources.
`[no] sso`	Enables single sign-on (SSO) web authentication using Microsoft Active Directory. When enabled, a user logs into a Windows computer using their Active Directory (AD) username and password. The Zyxel Device then uses these AD credentials for web authentication, through an SSO Agent server. The no command disables SSO web authentication.
`[no] 8021x-sso`	Enables single sign-on (SSO) web authentication using 8021x. When enabled, a user logs into a WiFi network on the Zyxel Device that has 8021.x (WPA Enterprise) enabled. The Zyxel Device then uses the user's 8021.x username and password for web authentication. The no command disables SSO web authentication using 8021x.
`[no] google-auth`	Enables 2-factor authentication using Google Authenticator. When enabled, a user must first authenticate on the web authentication page using their Zyxel Device username and password (this step can be bypassed if SSO or 8021.x-SSO is enabled), The user must then authenticate again by entering a code from the Google Authenticator app. To successfully authenticate, Google Authentication must already be enabled on the user's account and configured on their mobile device. For details, see Section 56.4 on page 481.
`show sso { agent | port | presharekey}`	Displays information about the specified condition.

31.2.3 Facebook Wi-Fi Commands

This table lists the commands for Facebook Wi-Fi. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 134 fbwifi Commands

COMMAND	DESCRIPTION
`[no] fbwifi activate`	Turns on Facebook Wi-Fi on the Zyxel Device. The no command disables it.
`[no] fbwifi idle-detection`	Sets the Zyxel Device to monitor how long each user (authenticated via Facebook Wi-Fi) is idle. The no command disables the idle detection feature.
`fbwifi idle-detection timeout <1..60>`	Specifies the user idle timeout between 1 and 60 minutes. The Zyxel Device automatically disconnects a user (authenticated via Facebook Wi-Fi) from the network after a period of inactivity.
`fbwifi reset-fbpage`	Removes the Facebook Page settings.
`fbwifi security {high |low}`	Sets when guests have to check into a business owner's Facebook Page. • `fbwifi security high` (default) only allows HTTP traffic, and blocks all other Internet traffic (HTTPS, FTP, SSH, and so on). Guests can browse using HTTP without checking in to the business owner's Facebook Page. Check-in is necessary for other Internet services such as WeChat, Line and so on. • `fbwifi security low` only blocks HTTP traffic, and allows all other Internet traffic (HTTPS, FTP, SSH, and so on). Guests that browse using HTTP will be redirected to the business owner's Facebook Page, and will need to check-in to continue browsing the Internet. Check-in is not necessary for other Internet services such as WeChat, Line and so on.
`show fbwifi activate`	Displays whether Facebook Wi-Fi is enabled on the Zyxel Device.
`show fbwifi service-register status`	Displays whether the Zyxel Device has been registered with myZyXEL.com.
`show fbwifi status`	Displays Facebook Wi-Fi settings on the Zyxel Device.

31.3 SSO Overview

SSO (Single Sign-On) integrates Domain Controller and Zyxel Device authentication mechanisms, so that users just need to log in once (single login) to get access to permitted resources.

- The Zyxel Device, the DC, the SSO agent and the LDAP or AD server must all be in the same domain and be able to communicate with each other.
- SSO does not support IPv6 or RADIUS; you must use it in an IPv4 network environment with Windows AD (Active Directory) or LDAP (Lightweight Directory Access Protocol) authentication databases.
- You must enable Web Authentication to use SSO.

31.3.1 SSO Configuration Commands

Use these commands to configure the Zyxel Device to communicate with SSO.

Table 135 SSO Commands and Subcommnds

COMMAND	DESCRIPTION
`sso agent primary`	Enters SSO primary agent subcommand mode.
`sso agent secondary`	Enters secondary agent subcommand mode. A secondary agent is an optional backup SSO agent.
`router(config-sso-primary)# router(config-sso-secondary)# [no] ip <w.x.y.z>`	Sets the primary or secondary SSO agent *ipv4 address.* Use *[no]* to disable the IPv4 address. Type the IPv4 address of the SSO agent. The Zyxel Device and the SSO agent must be in the same domain and be able to communicate with each other.
`router(config-sso-primary)# router(config-sso-secondary)# [no] port <1025..65535>`	Sets the primary or secondary agent port *<1025..65535>.* Use *[no]* to disable the port. Type the same port number here as in the Agent Listening Port field on the SSO agent. Type a number ranging from 1025 to 65535.
`sso presharekey <preshared key>`	Sets the SSO pre-shared key. Type 8-32 printable ASCII characters or exactly 32 hex characters (0-9; a-f). The Agent PreShareKey is used to encrypt communications between the Zyxel Device and the SSO agent
`sso encrypted-presharekey <ciphertext>`	Sets the SSO encrypted pre-shared key.
`sso_port <1025..65535>`	Sets the SSO listening port. This port is used to wait for receiving information from Agent. Type a number ranging from 1025 to 65535.

31.3.2 SSO Show Commands

You don't need to enter the configuration mode before you can use these commands. Use them to see SSO configurations done.

Table 136 SSO Show Commands

COMMAND	DESCRIPTION
`show sso agent`	Displays primary and secondary agent IP and Port configurations.
`show sso agent primary`	Displays primary agent IP and Port configurations.
`show sso agent secondary`	Displays secondary agent IP and Port configurations.
`show sso agent status`	Displays primary and secondary agent status.
`show sso port`	Displays the ZySSO port configured.
`show sso presharekey`	Shows the configured ZySSO presharekey.

31.3.3 Command Setup Sequence Example

The following commands show how to configure the Zyxel Device to communicate with an an SSO agent at IP address '1.1.1.1', using port '2158' and preshared key '12345678'.

```
Router(config)# sso agent primary
Router(config-sso-primary)# ip 1.1.1.1
Router(config-sso-primary)# port 2158
Router(config-sso-primary)# exit
Router(config)# sso presharekey 12345678
Router(config)# sso port 2158
Router(config)# exit
Router# show sso agent
Agent: primary
  IP Address: 1.1.1.1
  Port: 2158
Agent: secondary
  IP Address:
  Port: 0
Router# show sso agent primary
Agent: primary
  IP Address: 1.1.1.1
  Port: 2158
Router# show sso agent secondary
Agent: secondary
  IP Address:
  Port: 0
Router# show sso agent status
ZySSO Primary Agent: Offline
ZySSO Primary Agent: Offline
Router# show sso port
ZySSO port: 2158
Router# show sso presharekey
ZySSO presharekey: 12345678
Router#
```

31.3.4 Two-Factor Web Authentication Command Example

The following example shows how to enable web authentication with two-factor authentication for clients on LAN1, and then configure Google Authenticator for a user account.

Note: After running `show username <USERNAME> google-auth qrcode`, the owner of account TestUser needs to add the QRCode key manually to their Google Authenticator app..

```
Router# show web-auth policy all
force authentication policy: 1
  active: yes
  description: LAN1
  incoming interface: lan1
  source address: any
  destination address: any
  authentication: force
  sso: no
  schedule: none
  authentication type: default-web-portal
  ieee8021x sso: no
  google auth: no
Router# configure terminal
Router(config)# web-auth activate
Router(config)# web-auth policy 1
Router(config-web-auth-1)# google-auth
Router(config-web-auth-1)# exit
Router(config)# username TestUser google-auth
Router(config)# show username TestUser google-auth qrcode
qrcode-url# otpauth://totp/
admin?secret=XXXXXXXXXXXXXXXXXXXXXXXXXX&issuer=atp100w
Router(config)# username TestUser google-auth verify-code 123456
Verify: Success
```

CHAPTER 32
Hotspot

32.1 Hotspot Overview

See the Introduction chapter of the ZyWALL USG Series User's Guide for a list of models that support Hotspot management.

32.2 Billing Overview

You can use the built-in billing function to set up billing profiles. A billing profile describes how to charge users. This chapter also shows you how to select an accounting method or configure a discount price plan.

32.3 Billing Commands

This table lists the `billing` commands. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 137 billing Commands

COMMAND	DESCRIPTION
`billing accounting-method {accumulation | time-to-finish }`	Sets how the Zyxel Device accounts the time. `accumulation`: to allow each user a one-time login. Once the user logs in, the system starts counting down the pre-defined usage even if the user stops the Internet access before the time period is finished. If a user disconnects and reconnects before the allocated time expires, the user does not have to enter the user name and password to access the Internet again `time-to-finish`: to allow each user multiple re-login until the time allocated is used up. The Zyxel Device accounts the time that the user is logged in for Internet access
`billing accumulation idle-detection timeout <1..60>`	Specifies the idle timeout between 1 and 60 minutes. The Zyxel Device automatically disconnects a computer from the network after a period of inactivity. The user may need to enter the username and password again before access to the network is allowed.
`billing accumulation-expire {day <1..360> | hour <1..24>}`	Specifies a time unit and number to set how long to wait before the Zyxel Device deletes an idle account.
`billing currency {eur | gbp | usd | user-define` *`currency_code`* `}`	Sets the appropriate currency unit. *`currency_code`*: enter a three-letter alphabetic code, such as TWD or JPY.
`billing decimal-places <2>`	Sets the number of decimal places to be used for billing.
`billing decimal-symbol {comma | dot}`	Sets the Zyxel Device to use a dot (.) or a comma (,) for the decimal point.

Table 137 billing Commands (continued)

COMMAND	DESCRIPTION
`[no] billing discount activate`	Activates the discount price plan. The no command disables the discount price plan.
`billing discount button {a | b | c} [charge-by-level]`	Specifies a button to assign the base charge. `charge-by-level`: to charge the rate at each successive level from the first level (most expensive per unit) to the highest level (least expensive per unit) that the total purchase reaches.
`[no] billing discount unit <2..10> price price`	Creates a new discount level by setting the duration of the billing period that should be reached before the Zyxel Device charges users at this level and defining this level's charge per time unit. The no command removes this discount level.
`[no] billing profile profile_name`	Creates a billing profile and enters the `billing profile` sub-command mode to set the price and the duration of the billing period. See Table 138 on page 264 for the sub-commands. The no command removes the specified profile. *profile_name*: use up to 31 alphanumeric characters (A-Z, a-z, 0-9) and underscores (_). Spaces are not allowed. The first character must be a letter.
`billing profile rename profile_name profile_name`	Renames the specified billing profile (first *profile_name*) to the specified name (second *profile_name*).
`billing tax-rate <0..100>`	Sets the tax rate. For example, type 6 for a 6% sales tax.
`[no] billing tax-rate activate`	Sets the Zyxel Device to charge sales tax for the account. The no command sets the Zyxel Device to not charge sales tax for the account.
`billing unused-expire {minute <30..60> | hour <1..24> | day <1..365>}`	Specifies a time unit and number to set how long to wait before the Zyxel Device deletes an account that has not been used.
`billing username-password-length <4..6>`	Sets how many characters the username and password of a newly-created dynamic guest account will have.
`[no] billing wlan-ssid-profile profile_name`	Sets the name of the SSID profile to which you can apply the general billing settings. The no command sets the Zyxel Device to not apply the billing settings to the SSID profile.
`[no] billing replenish activate`	Allows dynamic-guest accounts to purchase additional time units for their accounts before their accounts expire.
`show billing discount default rule`	Displays settings of the default discount price plan.
`show billing discount rule`	Displays settings of the custom discount price plan(s).
`show billing discount status`	Displays billing discount settings.
`show billing profile [profile_name]`	Displays settings for all or the specified billing profile.
`show billing status`	Displays the general billing settings, such as the accounting method or tax rate.

32.3.1 Billing Profile Sub-commands

The following table describes the sub-commands for the `billing profile` command.

Table 138 billing profile Sub-commands

COMMAND	DESCRIPTION
`[no] activate`	Enables the billing profile. The no command disables the profile.
`bandwidth {upload | download} <0..1048576> priority <1..7>`	Specifies the maximum bandwidth allowed for the user account in kilobits per second and types a number between 1 and 7 to set the priority for the user's traffic. The smaller the number, the higher the priority. `upload` refers to the traffic the Zyxel Device sends out from a user. `download` refers to the traffic the Zyxel Device sends to a user.
`[no] bandwidth activate`	Turns on bandwidth management for the user account. The no command disables bandwidth management for the user account.
`price` *price*	Defines each profile's price, up to 999999.99, per time unit.
`quota {total | upload | download} megabytes <0..1023>`	Sets how much downstream and/or upstream data in Megabytes can be transmitted through the external interface before the account expires. 0 means there is no data limit for the user account.
`quota {total | upload | download} gigabytes <0..100>`	Sets how much downstream and/or upstream data in Gigabytes can be transmitted through the external interface before the account expires. 0 means there is no data limit for the user account.
`quota type {total | upload-download}`	Sets a limit for the user account. This only applies to user's traffic that is received or transmitted through the external interface. Note: When the limit is exceeded, the user is not allowed to access the Internet through the Zyxel Device. `total`: set a limit on the total traffic in both directions. `upload-download`: set a limit on the upstream traffic and downstream traffic respectively.
`time-period {day <1..365> | hour <1..24> | minute <30..60>}`	Sets the duration of the billing period. When this period expires, the user's access will be stopped.

32.3.2 Billing Command Example

This example sets the accounting method to `time-to-finish` and configures the idle timeout that elapses before the Zyxel Device disconnects a user.

```
Router# configure terminal
Router(config)# billing accounting-method time-to-finish
Router(config)# billing accumulation idle-detection timeout 30
Router(config)#
```

This example enables and creates a custom discount pricing plan. It uses button A to assign the base charge and also shows the discount status and plan settings.

```
Router# configure terminal
Router(config)# billing discount activate
Router(config)# billing discount button a charge-by-level
Router(config)# billing discount unit 3 price 1.9
Router(config)# show billing discount status
Billing discount status:
  activate: yes
  button: a
  charge_by_level: yes
Router(config)#show billing discount rule
No.  Conditions          Unit            Unit price
================================================================================
====
1    when >=             3               eur  1,90
Router(config)#
```

This example creates a billing profile named `billing_1hour` and displays the profile settings.

```
Router# configure terminal
Router(config)# billing profile billing_1hour
Router(billing profile button-a)# activate
Router(billing profile button-a)# price 2
Router(billing profile button-a)# time-period hour 1
Router(billing profile button-a)# exit
Router(config)# show billing profile
Billing Profile: billing_30mins
  activate: yes
  time period: 30 minute
  price: eur 0,00
Billing Profile: billing_1hour
  activate: yes
  time period: 1 hour
  price: eur 2,00
Router(config)#
```

This example applies the billing profile `billing_1hour` to button A of the web-based account generator and button A on a connected statement printer. It also displays the default discount price plan settings, that is, the billing profile settings for button A when it is selected as the button to assign the base charge.

```
Router# configure terminal
Router(config)# printer-manager button a billing_1hour
Router(config)# show billing discount default rule
No.        Conditions          Unit            Unit price
================================================================================
====
default    when >=             1               eur  2,00
Router(config)#
```

32.3.3 Payment Service

Use these commands to use a credit card service to authorize, process, and manage credit card transactions directly through the Internet. You must register with the supported credit card service before you can configure the Zyxel Device to handle credit card transactions.

This table lists the `payment-service` commands. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 139 payment-service Commands

COMMAND	DESCRIPTION
`payment-service provider select` *`provider`*	Selects a payment provider. For example, `payment-service provider select` *`paypal`*.
`payment-service provider paypal`	Enters payment-service sub-command mode for PayPal.
`payment-service provider paypal exit`	Exits payment-service sub-command mode.
`[no] payment-service activate`	Activates payment service to use PayPal to authorize credit card payments. The no command disables payment service.
`payment-service account-delivery` *`delivery_method`* `{deactivate | activate}`	Enables or disables how the Zyxel Device provides dynamic guest account information after the user's online payment is done. *`delivery_method`*: type *`onscreen`* or *`sms`*. *`onscreen`* displays the user account information in the web configurator screen. *`sms`* uses Short Message Service (SMS) to send account information in a text message to the user's mobile device. You should have enabled SMS to send text messages to the user's mobile device.
`[no] payment-service page-customization`	Enables customization of desktop online payment service pages that displays after an unauthorized user clicks the link in the Web Configurator login screen to purchase access time. The no commands disables customization and uses the default page.
`[no] payment-service mobile-page-customization`	Enables customization of mobile online payment service pages that displays after an unauthorized user clicks the link in the Web Configurator login screen to purchase access time. The no commands disables customization and uses the default page.
`payment-service fail-page failed-message` *`message`*	Creates a message if a desktop payment transaction fails. *`message`*: The message must be from 1 to 256 characters long and can contain spaces and the following characters ([0-9a-zA-Z '`()+,/:;=~!*#@$_%-\.\&\?\[\]\{\}*|\^\\\<\>\+\"]) The default message is "Sorry! We can't handle your payment transaction at this time."
`payment-service mobile-fail-page failed-message` *`message`*	Creates a message if a mobile payment transaction fails. *`message`*: The message must be from 1 to 256 characters long and can contain spaces and the following characters ([0-9a-zA-Z '`()+,/:;=~!*#@$_%-\.\&\?\[\]\{\}*|\^\\\<\>\+\"]) The default message is "Sorry! We can't handle your payment transaction at this time."

Table 139 payment-service Commands (continued)

COMMAND	DESCRIPTION
`payment-service mobile-profile-page selection-message` *`message`*	Creates a message prompting mobile payment service plan selection. *`message`*: The message must be from 1 to 256 characters long and can contain spaces and the following characters ([0-9a-zA-Z '`()+,/:;=~!*#@$_%-\.\&\?\[\]\{\}*|\^\\\<\>\+\"]) The default message is “Please choose the service plan from the following profile table.”
`payment-service mobile-sms-page info-message` *`message`*	Creates a mobile view customized SMS page when a new account is created. *`message`*: The message must be from 1 to 256 characters long and can contain spaces and the following characters ([0-9a-zA-Z '`()+,/:;=~!*#@$_%-\.\&\?\[\]\{\}*|\^\\\<\>\+\"]) The default message is “Please check your mobile phone for the account information.”
`payment-service mobile-success-page {`*`notification-message`* `|` *`successful-message`* `| notification-message-color {#00FF00 |` *`color_name`* `| rgb(0,0,255)}`	Creates custom colored mobile view messages when a new account is created successfully. *`message`*: The message must be from 1 to 256 characters long and can contain spaces and the following characters ([0-9a-zA-Z '`()+,/:;=~!*#@$_%-\.\&\?\[\]\{\}\*|\^\\\<\>\+\"]) The default `notification-message` is “IMPORTANT! Make a note for your case-sensitive username and password for logging later. This will be your only opportunity to do so.” The default `successful-message` is “You may now use the Internet.“ `notification-message-color`: Defines the message color by selecting RGB (0,0,255), or type a *`color_name`* such as red, or enter the hex color format (#00FF00).
`payment-service profile-page selection-message` *`message`*	Creates a message prompting payment service plan selection. *`message`*: The message must be from 1 to 256 characters long and can contain spaces and the following characters ([0-9a-zA-Z '`()+,/:;=~!*#@$_%-\.\&\?\[\]\{\}*|\^\\\<\>\+\"]) The default message is “Please choose the service plan from the following profile table.”
`payment-service success-page {account-message` *`message`* `| format-date {dd-mm-yyyy | mm-dd-yyyy | yyyy-mm-dd} | notification-message` *`message`* `| notification-message-color {#00FF00 |` *`color_name`* `| rgb(0,0,255)} | successful-message` *`message}`*	Creates custom colored, date-formatted desktop view messages when a new account is created successfully. *`message`*: The message must be from 1 to 256 characters long and can contain spaces and the following characters ([0-9a-zA-Z '`()+,/:;=~!*#@$_%-\.\&\?\[\]\{\}\*|\^\\\<\>\+\"]) The default `account-message` is ”This is your account information, please keep this for your internet service.” The default `notification-message` is “IMPORTANT! Make a note for your case-sensitive username and password for logging later. This will be your only opportunity to do so.” The default `successful-message` is “You may now use the Internet.“ `notification-message-color`: Defines the message color by selecting RGB (0,0,255), or type a *`color_name`* such as red, or enter the hex color format (#00FF00).
`show payment-service account-delivery`	Displays how the Zyxel Device provides dynamic guest account information after the user’s online payment is done (*`onscreen`* or *`sms`*).

Table 139 payment-service Commands (continued)

COMMAND	DESCRIPTION
`show payment-service check payment-all-currency`	Checks if the billing currency is different from the payment currency configured.
`show payment-service activation`	Displays if payment service is active.
`show payment-service provider select`	Displays the payment service provider selected.
`show payment-service provider paypal`	Displays account, currency, identity token, and payment gateway details of the PayPal payment service provider.
`show payment-service page-customization`	Displays whether customization of desktop online payment service is enabled.
`show payment-service profile-page settings`	Displays the message prompting payment service plan selection
`show payment-service success-page settings`	Displays the settings for messages for when a new account is created successfully.
`show payment-service fail-page settings`	Displays the message for if a desktop payment transaction fails.
`show payment-service sms-page settings`	Displays the SMS message in Desktop View when a new account is created.
`show payment-service mobile-page-customization`	Displays whether customization of mobile online payment service pages that displays after an unauthorized user clicks the link in the Web Configurator login screen to purchase access time, is enabled.
`show payment-service mobile-profile-page settings`	Displays the message prompting mobile payment service plan selection.
`show payment-service mobile-success-page settings`	Displays whether customization for mobile view messages when a new account is created successfully is enabled.
`show payment-service mobile-fail-page settings`	Displays the settings for messages if a mobile payment transaction fails.
`show payment-service mobile-sms-page settings`	Displays the SMS message in Mobile View when a new account is created.

The following table describes the sub-commands for the `payment-service` command.

Table 140 payment-service paypal Sub-commands

COMMAND	DESCRIPTION
`payment-service provider paypal account e-mail`	Configures an e-mail address for the PayPal account. *e-mail*: type a valid e-mail address for this account
`payment-service provider paypal no account`	Removes the PayPal account.
`payment-service provider paypal currency paypal_currency`	Defines the currency in which payments are made *paypal_currency*: Select the currency that PayPal supports. For example, *aud, cad, chf, czk, dkk, eur, gbp, hkd, huf, ils, jpy, mxn, nok, nzd, php, pln, sek, sgd, thb, twd, usd*.
`payment-service provider paypal identity-token paypal_token`	Defines the PayPal ID token. *paypal_token*: Enter the ID token provided to you by PayPal after successfully applying for your PayPal account.
`payment-service provider paypal no identity-token`	Removes the PayPal ID token.

Table 140 payment-service paypal Sub-commands (continued)

COMMAND	DESCRIPTION
`payment-service provider paypal gateway payment_gw_url`	Defines the PayPal gateway. *payment_gw_url*: Enter the address of the PayPal gateway provided to you by PayPal after applying for your PayPal account.
`payment-service check paypal-currency`	Displays the currency in which PayPal payments are made.

32.4 Printer Manager Overview

You can create dynamic guest accounts and print guest account information by pressing the button on an external statement printer, such as SP350E. Make sure that the printer is connected to the appropriate power and the Zyxel Device, and that there is printing paper in the printer. Refer to the printer's documentation for details.

32.5 Printer-manager Commands

This table lists the `printer-manager` commands. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 141 printer-manager Commands

COMMAND	DESCRIPTION
`[no] printer-manager activate`	Allows the Zyxel Device to manage and moniter the printer status. The no command disables printer management on the Zyxel Device.
`printer-manager discover`	Detects the printer(s) that is connected to the Zyxel Device and display the printer information.
`printer-manager button {a | b | c} profile_name`	Applies the specified billing profile to a button of the web-based account generator and/or the button on a connected statement printer
`[no] printer-manager encrypt activate`	Turns on data encryption. Data transmitted between the Zyxel Device and the printer will be encrypted with a secret key. The no command disables data encryption.
`printer-manager encrypt secret-key secret_key`	Sets a key for data encryption. *secret_key*: four alphanumeric characters (A-Z, a-z, 0-9)
`printer-manager multi-printout <1..3>`	Sets how many copies of subscriber statements you want to print (1 is the default).
`printer-manager port <1..65535>`	Sets the number of port on which the Zyxel Device sends data to the printer for it to print.
`[no] printer-manager printer <1..10>`	Enters the `printer-manager printer` sub-command mode to configure a printer that can be managed by the Zyxel Device. See Table 138 on page 264 for the sub-commands. The no command removes the specified printer from the printer list.
`printer-manager printer append`	Enters the `printer-manager printer` sub-command mode to add a printer to the end of the printer list. See Table 138 on page 264 for the sub-commands.

Table 141 printer-manager Commands (continued)

COMMAND	DESCRIPTION
`printer-manager printout-type {customized | default}`	Sets to use the default account printout format built into the Zyxel Device or use a custom account printout format.
`show printer-manager button`	Displays the name of billing profile that is applied to each button.
`show printer-manager discover-printer-status`	Displays information of the printer that is connected to and detected by the Zyxel Device.
`show printer-manager printer [<1..10>]`	Displays settings of all or the specified printer that can be managed by the Zyxel Device.
`show printer-manager printer-status`	Displays information about the printers that are connected and can be managed by the Zyxel Device.
`show printer-manager printerfw version`	Displays the version of the printer firmware currently uploaded to the Zyxel Device. The Zyxel Device automatically installs it in the connected printers to make sure the printers are upgraded to the same version.
`show printer-manager printout-type`	Displays the current account printout format.
`show printer-manager settings`	Displays the printer management settings.
`show printer-manager workableIP`	Displays the number and IP address(s) of printer(s) that can synchronize with the Zyxel Device successfully.

32.5.1 Printer-manager Printer Sub-commands

The following table describes the sub-commands for the `printer-manager printer` command.

Table 142 printer-manager printer Sub-commands

COMMAND	DESCRIPTION
`activate`	Enables the entry.
`deactivate`	Disables the entry.
`description` *`description`*	Sets a descriptive name for the printer.
`printer-ip` *`ipv4_address`*	Sets the IP address of the printer.

32.5.2 Printer-manager Command Example

This example adds a printer to the managed printer list and displays the printer settings.

```
Router# configure terminal
Router(config)# printer-manager printer 1
Router(printer-manager)# activate
Router(printer-manager)# description cafe
Router(printer-manager)# printer-ip 172.16.0.123
Router(printer-manager)# exit
Router(config)# show printer-manager printer
printer: 1
  activate: yes
  IPv4 address: 172.16.0.123
  description:  cafe
Router(config)#
```

32.6 Free Time Overview

With Free Time, the Zyxel Device can create dynamic guest accounts that allow users to browse the Internet free of charge for a specified period of time.

32.7 Free-Time Commands

The following table lists the `free-time` commands. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 143 free-time Commands

COMMAND	DESCRIPTION
`[no] free-time activate`	Turns on the free time feature to allow users to get a free account for Internet surfing during the specified time period. The no command disables the free time feature.
`[no] free-time auto-login`	Allow users to log into their free account directly without having to enter their user name and password. The no command requires users to enter their user name and password, and click login to access their free account.
`[no] free-time deliver-method onscreen`	Sets the Zyxel Device to display the user account information in the web screen. The no command sets the Zyxel Device to not display the user account information in the web screen.
`[no] free-time deliver-method sms`	Sets the Zyxel Device to send account information in an SMS text message to the user's mobile device. The no command sets the Zyxel Device to not send account information in an SMS text message to the user's mobile device.
`[no] free-time maximum-allowed-account <1..2000>`	Specifies the maximum number of the free user accounts that users can create. The Zyxel Device rejects prevents users from creating a free account after this limit is reached. The no command resets the setting to its default value of `1000`.
`[no] free-time maximum-register-number <1..5>`	Specifies the maximum number of the users that are allowed to log in for Internet access simultaneously with a free guest account before the time specified using the `free-time reset-register` command. The no command resets the setting to its default value (`1`).
`[no] free-time reset-register` *`hh:mm`*	Sets the time in 24-hour format at which the new free time account is allowed to access the Internet. The no command resets the setting to its default value (`00:00`).
`[no] free-time time-period` *`time_period`*	Sets the duration of time period (in minutes) for which the free time account is allowed to access the Internet. *`time_period`*: x - y, where x and y depend on the Zyxel Device model. The no command resets the setting to its default value (`30`).
`show free-time status`	Displays the free time settings.

32.8 Free-Time Commands Example

The following example enables the free time feature and sets the Zyxel Device to provide user account information in the web screen and also sent account information via SMS text messages. It then displays the free time settings.

```
Router# configure terminal
Router(config)# free-time activate
Router(config)# free-time deliver-method onscreen
Router(config)# free-time deliver-method sms
Router(config)# show free-time status
Activate: yes
Time Period: 30
Reset Time: 00:00
Maximum registration number before reset time: 1
Delivery Method: onscreen-sms
Router(config)#
```

32.9 IPnP Overview

IP Plug and Play (IPnP) allows a computer to access the Internet without changing the network settings (such as IP address and subnet mask) of the computer, even when the IP addresses of the computer and the Zyxel Device are not in the same subnet.

When you disable the IPnP feature, only computers with dynamic IP addresses or static IP addresses in the same subnet as the Zyxel Device's LAN IP address can connect to the Zyxel Device or access the Internet through the Zyxel Device.

The IPnP feature does not apply to a computer using either a dynamic IP address or a static IP address that is in the same subnet as the Zyxel Device's IP address.

Note: You must enable NAT to use the IPnP feature.

32.10 IPnP Commands

The following table lists the `ipnp` commands. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 144 ipnp Commands

COMMAND	DESCRIPTION
`[no] ip ipnp activate`	Enables IPnP on the Zyxel Device. The `no` command disables IPnP.
`ip ipnp config`	Enters the IPnP sub-command mode to enable IPnP on specific internal interface(s).
`[no] interface` *`interface_name`*	Enables IPnP on a specific internal interface. The `no` command disables IPnP for the specified interface.

Table 144 ipnp Commands (continued)

COMMAND	DESCRIPTION
`show ip ipnp activation`	Displays whether IPnP is enabled on the Zyxel Device.
`show ip ipnp interface`	Displays whether IPnP is enabled on an interface.

32.11 IPnP Commands Example

The following example enables IPnP on the Zyxel Device and interface lan1. It also displays the IPnP settings.

```
Router# configure terminal
Router(config)# ip ipnp activate
Router(config)# ip ipnp config
Router(ipnp)# interface lan1
Router(ipnp)# exit
Router(config)# show ip ipnp activation
IPnP Status: yes
Router(config)# show ip ipnp interface
interface
================================================================================
lan1
Router(config)#
```

32.12 Walled Garden Overview

A user must log in before the Zyxel Device allows the user's access to the Internet. However, with a walled garden, you can define one or more web site addresses that all users can access without logging in. These can be used for advertisements for example.

32.13 Walled Garden Commands

This table lists the `walled-garden` commands. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 145 walled-garden Commands

COMMAND	DESCRIPTION
`[no] walled-garden activate`	Enables the walled garden feature. The no command disables the walled garden feature.
`[no] walled-garden rule <1..50>`	Creates a walled garden URL link entry (URLs that use the HTTP or HTTPS protocol) for web site that all users are allowed to access without logging in, and enters sub-command mode. See Section Table 146 on page 274 for the rule sub-commands.
`walled-garden rule append`	Creates a new walled garden URL entry at the end of the current list and enters sub-command mode. See Table 146 on page 274 for the sub-commands.

Table 145 walled-garden Commands (continued)

COMMAND	DESCRIPTION
`walled-garden rule flush`	Deletes all walled garden URL entries.
`walled-garden rule insert <1..50>`	Creates a new walled garden URL entry at the specified location, renumbers the other entries accordingly, and enters sub-command mode. See Table 146 on page 274 for the sub-commands.
`walled-garden rule move <1..50> to <1..50>`	Moves the specified walled garden URL entry to the specified location and renumbers the other entries accordingly.
`walled-garden domain-ip rule <1..50>`	Creates a walled garden web site link entry, which uses a (wildcard) domain name or an IP address for web site that all users are allowed to access without logging in, and enters sub-command mode. See Section Table 147 on page 275 for the rule sub-commands.
`walled-garden domain-ip rule append`	Creates a new walled garden domain name or IP address entry at the end of the current list and enters sub-command mode. See Table 147 on page 275 for the sub-commands.
`walled-garden domain-ip rule flush`	Deletes all walled garden domain name or an IP address entries.
`show walled-garden activation`	Displays whether the walled garden feature is enabled or not.
`show walled-garden rule <1..50>`	Displays settings of the specified walled garden URL entry.

32.13.1 walled-garden rule Sub-commands

The following table describes the sub-commands for several `walled-garden rule` commands. Note that not all rule commands use all the sub-commands listed here.

Table 146 walled-garden rule Sub-commands

COMMAND	DESCRIPTION
`[no] activate`	Enables this entry. The `no` command disables the entry.
`[no] name` *`description`*	Sets a descriptive name for the walled garden link to be displayed in the login screen. The `no` command clears the description. *`description`*: You can use up to 31 alphanumeric characters (A-Z, a-z, 0-9) and underscores (_). Spaces are not allowed. The first character must be a letter.
`[no] hidden`	Sets the Zyxel Device to not display the web site link in the user login screen. This is helpful if a user's access to a specific web site is required to stay connected but he or she does not need to visit that web site. The `no` command displays the web site link in the user login screen.
`[no] url` *`url`*	Sets the URL or IP address of the web site. Use "http://" followed by up to 262 characters (0-9a-zA-Z;/?:@&=+$\.-_!~*'()%). For example, http://www.example.com or http://172.16.1.35. The `no` command removes the web site address.

32.13.2 walled-garden domain-ip rule Sub-commands

The following table describes the sub-commands for several `walled-garden domain-ip rule` commands. Note that not all rule commands use all the sub-commands listed here.

Table 147 walled-garden domain-ip rule Sub-commands

COMMAND	DESCRIPTION
`[no] activate`	Enables this entry. The no command disables the entry.
`[no] name` *description*	Sets a descriptive name for the walled garden link to be displayed in the login screen. The no command clears the description. *description*: You can use up to 31 alphanumeric characters (A-Z, a-z, 0-9) and underscores (_). Spaces are not allowed. The first character must be a letter.
`[no] type {domain|ip}`	Sets the rule type to be a domain name or an IPv4 IP address.
`[no] domain-name` *walled_garden_fqdn*	Sets a fully qualified name for the `domain` type rule. *walled_garden_fqdn*: Type a valid fully qualified name for this rule. The no command removes the fully qualified name.
`[no] ip-address` *<w.x.y.z>/<1..32>*	Sets the IPv4 subnet in CIDR format for the `ip` type rule. For example, 192.168.1.0/32. The no command removes the web site address.

32.13.3 Walled Garden Command Example

This example shows how to enable the walled garden feature and insert a walled garden link rule at position 1 of the checking order. This example also displays the rule settings. The link rule uses the following settings:

- Activate: yes
- Name: Example1
- URL: www.example.com

```
Router# configure terminal
Router(config)# walled-garden activate
Router(config)# walled-garden rule insert 1
Router(walled-garden)# activate
Router(walled-garden)# name Example1
Router(walled-garden)# url http://www.example.com
Router(walled-garden)# exit
Router(config)# show walled-garden
walled garden rule: 1
  active: yes
  url: http://www.example.com
  name: Example1
Router(config)#
```

32.14 Advertisement Overview

You can set the Zyxel Device to display an advertisement web page as the first web page whenever the user connects to the Internet.

32.15 Advertisement Commands

This table lists the `advertisement` commands. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 148 advertisement Commands

COMMAND	DESCRIPTION
`[no] advertisement activate`	Enables the advertisement feature. The no command disables the advertisement feature.
`advertisement flush`	Deletes all advertisement rules.
`[no] advertisement name` *`description`* `url` *`url`*	Sets a descriptive name for the advertisement web page and enters the web site address to create a new rule. The no command removes the advertisement rule. *`description`*: You can use up to 31 alphanumeric characters (A-Z, a-z, 0-9) and underscores (_). Spaces are not allowed. The first character must be a letter. *`url`*: the URL or IP address of the web site. Use "http://" followed by up to 262 characters (0-9a-zA-Z;/?:@&=+$\.-_!~*'()%). For example, http://www.example.com or http://172.16.1.35.
`advertisement rename` *`description_old description_new`*	Gives an existing rule a new name.
`show advertisement`	Displays settings of advertisement rule(s).
`show advertisement activation`	Displays whether the advertisement feature is enabled or not.

32.15.1 Advertisement Command Example

This example shows how to set an advertisement rule and displays the rule settings.

```
Router# configure terminal
Router(config)# advertisement activate
Router(config)# advertisement name example url http://www.example.com
Router(config)# show advertisement
advertisement rule: 1
  name: example
  url: http://www.example.com
Router(config)#
```

CHAPTER 33
IPSec VPN

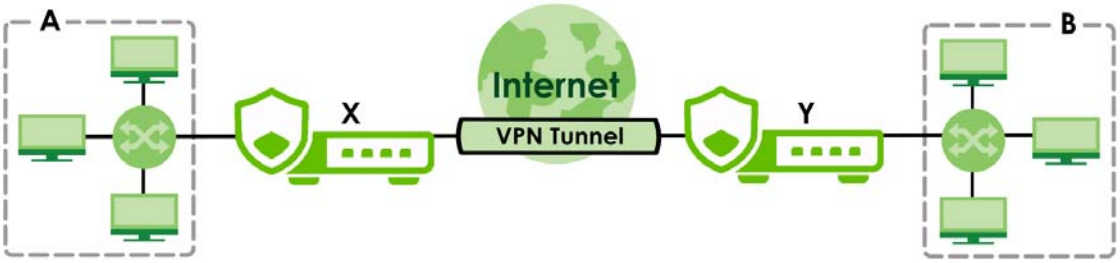
33.1 IPSec VPN Overview

A virtual private network (VPN) provides secure communications between sites without the expense of leased site-to-site lines. A secure VPN is a combination of tunneling, encryption, authentication, access control and auditing. It is used to transport traffic over the Internet or any insecure network that uses TCP/IP for communication.

Internet Protocol Security (IPSec) is a standards-based VPN that offers flexible solutions for secure data communications across a public network like the Internet. IPSec is built around a number of standardized cryptographic techniques to provide confidentiality, data integrity and authentication at the IP layer.

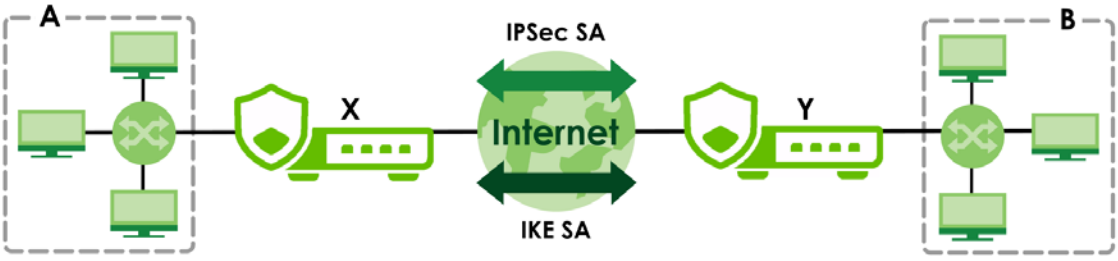
The following figure is one example of a VPN tunnel. Here local Zyxel Device X uses an IPSec VPN runnel to remote (peer) Zyxel Device Y to connect the local (A) and remote (B) networks.

Figure 28 VPN: Example



A VPN tunnel is usually established in two phases. Each phase establishes a security association (SA), a contract indicating what security parameters the Zyxel Device and the remote IPSec router will use. The first phase establishes an Internet Key Exchange (IKE) SA between the Zyxel Device and remote IPSec router. The second phase uses the IKE SA to securely establish an IPSec SA through which the Zyxel Device and remote IPSec router can send data between computers on the local network and remote network. This is illustrated in the following figure.

Figure 29 VPN: IKE SA and IPSec SA



In this example, a computer in network A is exchanging data with a computer in network B. Inside networks A and B, the data is transmitted the same way data is normally transmitted in the networks. Between routers X and Y, the data is protected by tunneling, encryption, authentication, and other security features of the IPSec SA. The IPSec SA is secure because routers X and Y established the IKE SA first.

33.2 IPSec VPN Commands Summary

The following table describes the values required for many IPSec VPN commands. Other values are discussed with the corresponding commands.

Table 149 Input Values for IPSec VPN Commands

LABEL	DESCRIPTION
profile_name	The name of a VPN concentrator. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
policy_name	The name of an IKE SA. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
map_name	The name of an IPSec SA. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
domain_name	Fully-qualified domain name. You may use up to 254 alphanumeric characters, dashes (-), or periods (.), but the first character cannot be a period.
e_mail	An e-mail address. You can use up to 63 alphanumeric characters, underscores (_), dashes (-), or @ characters.
distinguished_name	A domain name. You can use up to 511 alphanumeric, characters, spaces, or `.@=,_-` characters.

sort_order	Sort the list of currently connected SAs by one of the following classifications.
	`algorithm`
	`encapsulation`
	`inbound`
	`name`
	`outbound`
	`policy`
	`timeout`
	`uptime`

auth_method	The name of the authentication profile.

The following sections list the IPSec VPN commands.

33.2.1 IPv4 IKEv1 SA Commands

This table lists the commands for IKE SAs (VPN gateways).

Table 150 IPv4 IKEv1 SA Commands

COMMAND	DESCRIPTION
`show vpn-service status`	Displays if IPSec VPN and UDP ports 500/4500 are enabled.
`[no] vpn-service enable`	Enables or disables IPSec VPN.
`[no] vpn-service auto-disable`	Disables UDP ports 500 and 4500 when no IPSec VPN rules are configured on the Zyxel Device. This prevents hackers from attacking the Zyxel Device through UDP 500 and 4500 when you're not using IPSec VPN.
`[no] crypto boost-tcp`	Enhances TCP throughput traffic performance. This command must be applied on both local Zyxel Device and peer Zyxel Device. The `no` command disables this feature.

Table 150 IPv4 IKEv1 SA Commands (continued)

COMMAND	DESCRIPTION
`show crypto boost-tcp`	Displays if TCP throughput traffic performance is enhanced or not.
`show isakmp keepalive`	Displays the Dead Peer Detection period.
`show isakmp policy [policy_name]`	Shows the specified IKE SA or all IKE SAs.
`[no] isakmp policy policy_name`	Creates the specified IKE SA if necessary and enters sub-command mode. The no command deletes the specified IKE SA.
`activate` `deactivate`	Activates or deactivates the specified IKE SA.
`authentication {pre-share | rsa-sig | user-base-psk}`	Specifies whether to use a pre-shared key, a certificate, or a user-based pre-shared key for authentication.
`certificate certificate-name`	Sets the certificate that can be used for authentication.
`[no] dpd`	Enables Dead Peer Detection (DPD). The no command disables DPD. DPD has the Zyxel Device make sure the remote IPSec device is there before transmitting data through the IKE SA. If there has been no traffic for at least 15 seconds, the Zyxel Device sends a message to the remote IPSec device. If it responds, the Zyxel Device transmits the data. If it does not respond, the Zyxel Device shuts down the IKE SA. Disabling DPD might cause the Zyxel Device to transmit data to a remote IPSec device that is not available.
`dpd-interval <15..60>`	Sets the Dead Peer Detection (DPD) period.
`[no] fall-back`	Set this to have the Zyxel Device reconnect to the primary address when it becomes available again and stop using the secondary connection, if the connection to the primary address goes down and the Zyxel Device changes to using the secondary connection. Users will lose their VPN connection briefly while the Zyxel Device changes back to the primary connection. To use this, the peer device at the secondary address cannot be set to use a nailed-up VPN connection.
`fall-back-check-interval <60..86400>`	Sets how often (in seconds) the Zyxel Device checks if the primary address is available.
`mode {main | aggressive}`	Sets the negotiating mode.
`transform-set isakmp-algo [isakmp_algo [isakmp_algo]]`	Sets the encryption and authentication algorithms for each IKE SA proposal. *isakmp_algo*: {des-md5 | des-sha | 3des-md5 | 3des-sha | aes128-md5 | aes128-sha | aes192-md5 | aes192-sha | aes256-md5 | aes256-sha | aes256-sha256 | aes256-sha512}
`lifetime <180..3000000>`	Sets the IKE SA life time to the specified value.

`group1`
`group2`
`group5`
`group14`
	Sets the DH*x* group to the specified group.

`[no] natt`	Enables NAT traversal. The no command disables NAT traversal.

Table 150 IPv4 IKEv1 SA Commands (continued)

COMMAND	DESCRIPTION
`local-ip {ip {ip | domain_name} | interface interface_name}`	Sets the local gateway address to the specified IP address, domain name, or interface.
`peer-ip {ip | domain_name} [ip | domain_name]`	Sets the remote gateway address(es) to the specified IP address(es) or domain name(s).
`keystring pre_shared_key`	Sets the pre-shared key of up to 128 characters that can be used for authentication. The *pre_shared_key* can be: • Alphanumeric characters or ,;|`~!@#$%^&*()_+\{}':./<>=-". • Hexadecimal (0-9, A-F) characters, preceded by "0x". The pre-shared key is case-sensitive.
`local-id type {ip ip | fqdn domain_name | mail e_mail | dn distinguished_name}`	Sets the local ID type and content to the specified IP address, domain name, or e-mail address.
`peer-id type {any | ip ip | fqdn domain_name | mail e_mail | dn distinguished_name}`	Sets the peer ID type and content to any value, the specified IP address, domain name, or e-mail address.
`[no] twofa-auth`	Enables two-factor authentication. The no command disables two-factor authentication. See Section 56.4 on page 481 and Section 56.5 on page 484 for more information on configuring two-factor authentication settings.
`xauth type {server auth_method [user-id {username | any}] | client name username password password} [deactivate]`	Enables extended authentication and specifies whether the Zyxel Device is the server or client. If the Zyxel Device is the server, it also specifies the extended authentication method (`aaa authentication profile_name`); if the Zyxel Device is the client, it also specifies the username and password to provide to the remote IPSec router. The `deactivate` command disables extended authentication. *auth_method:* The name of the authentication profile the VPN configuration provisioning service uses to authenticate users. `user-id`: A user or user group allowed to use the IKE SA. `any` allows any user with a valid user account and password on the Zyxel Device to use the IKE SA. *username*: You can use alphanumeric characters, underscores (_), and dashes (-), and it can be up to 31 characters long. *password*: You can use most printable ASCII characters. You cannot use square brackets [ ], double quotation marks ("), question marks (?), tabs or spaces. It can be up to 31 characters long.
`isakmp policy rename policy_name policy_name`	Renames the specified IKE SA (first *policy_name*) to the specified name (second *policy_name*).

33.2.2 IPv4 IPSec SA Commands (except Manual Keys)

This table lists the commands for IPSec SAs, excluding manual keys (VPN connections using VPN gateways).

Table 151 crypto Commands: IPSec SAs

COMMAND	DESCRIPTION
`[no] crypto ignore-df-bit`	Fragment packets larger than the MTU (Maximum Transmission Unit) that have the "don't" fragment" bit in the header turned on. The `no` command has the Zyxel Device drop packets larger than the MTU that have the "don't" fragment" bit in the header turned on.
`show crypto map [map_name]`	Shows the specified IPSec SA or all IPSec SAs.
`crypto map dial map_name`	Dials the specified IPSec SA manually. This command does not work for IPSec SAs using manual keys or for IPSec SAs where the remote gateway address is 0.0.0.0.
`[no] crypto map map_name`	Creates the specified IPSec SA if necessary and enters sub-command mode. The `no` command deletes the specified IPSec SA.
`crypto map rename map_name map_name`	Renames the specified IPSec SA (first *map_name*) to the specified name (second *map_name*).
`activate` `deactivate`	Activates or deactivates the specified IPSec SA.
`adjust-mss {auto | <200..1500>}`	Set a specific number of bytes for the Maximum Segment Size (MSS) meaning the largest amount of data in a single TCP segment or IP datagram for this VPN connection or use `auto` to have the ZyWALL automatically set it.
`ipsec-isakmp policy_name`	Specifies the IKE SA for this IPSec SA and disables manual key.
`encapsulation {tunnel | transport}`	Sets the encapsulation mode.
`transform-set crypto_algo_esp [crypto_algo_esp [crypto_algo_esp]]`	Sets the active protocol to ESP and sets the encryption and authentication algorithms for each proposal. *crypto_algo_esp*: esp-null-md5 | esp-null-sha | esp-null-sha256 | esp-null-sha512 | esp-des-md5 | esp-des-sha | esp-des-sha256 | esp-des-sha512 | esp-3des-md5 | esp-3des-sha | esp-3des-sha256 | esp-3des-sha512 | esp-aes128-md5 | esp-aes128-sha | esp-aes128-sha256 | esp-aes128-sha512 | esp-aes192-md5 | esp-aes192-sha | esp-aes192-sha256 | esp-aes192-sha512 | esp-aes256-md5 | esp-aes256-sha | esp-aes256-sha256 | esp-aes256-sha512
`transform-set crypto_algo_ah [crypto_algo_ah [crypto_algo_ah]]`	Sets the active protocol to AH and sets the encryption and authentication algorithms for each proposal. *crypto_algo_ah*: ah-md5 | ah-sha | ah-sha256 | ah-sha512

Table 151 crypto Commands: IPSec SAs (continued)

COMMAND	DESCRIPTION
`scenario {site-to-site-static|site-to-site-dynamic|remote-access-server|remote-access-client}`	Select the scenario that best describes your intended VPN connection. `Site-to-site`: The remote IPSec router has a static IP address or a domain name. This Zyxel Device can initiate the VPN tunnel. `site-to-site-dynamic`: The remote IPSec router has a dynamic IP address. Only the remote IPSec router can initiate the VPN tunnel. `remote-access-server`: Allow incoming connections from IPSec VPN clients. The clients have dynamic IP addresses and are also known as dial-in users. Only the clients can initiate the VPN tunnel. `remote-access-client`: Connects to an IPSec server. This Zyxel Device is the client (dial-in user) and can initiate the VPN tunnel. `vpn-tunnel-interface:` Sets up a VPN tunnel interface to bind with a VPN connection. The Zyxel Device can use the interface to do load balancing using a specific Trunk. The remote IPsec router should have a static IP address or a domain name.
`set security-association lifetime seconds <180..3000000>`	Sets the IPSec SA life time.
`set pfs {group1 | group2 | group5 | none}`	Enables Perfect Forward Secrecy group.
`local-policy` *address_name*	Sets the address object for the local policy (local network).
`remote-policy` *address_name*	Sets the address object for the remote policy (remote network).
`[no] policy-enforcement`	Drops traffic whose source and destination IP addresses do not match the local and remote policy. This makes the IPSec SA more secure. The `no` command allows traffic whose source and destination IP addresses do not match the local and remote policy. Note: You must allow traffic whose source and destination IP addresses do not match the local and remote policy, if you want to use the IPSec SA in a VPN concentrator.
`[no] nail-up`	Automatically re-negotiates the SA as needed. The `no` command does not.
`[no] replay-detection`	Enables replay detection. The `no` command disables it.
`[no] netbios-broadcast`	Enables NetBIOS broadcasts through the IPSec SA. The `no` command disables NetBIOS broadcasts through the IPSec SA.
`[no] out-snat activate`	Enables out-bound traffic SNAT over IPSec. The `no` command disables out-bound traffic SNAT over IPSec.
`out-snat source` *address_name* `destination` *address_name* `snat` *address_name*	Configures out-bound traffic SNAT in the IPSec SA.

Table 151 crypto Commands: IPSec SAs (continued)

COMMAND	DESCRIPTION
[no] in-snat activate	Enables in-bound traffic SNAT in the IPSec SA. The no command disables in-bound traffic SNAT in the IPSec SA.
in-snat source *address_name* destination *address_name* snat *address_name*	Configures in-bound traffic SNAT in the IPSec SA.
[no] in-dnat activate	Enables in-bound traffic DNAT in the IPSec SA. The no command disables in-bound traffic DNAT in the IPSec SA.
in-dnat delete <1..10>	Deletes the specified rule for in-bound traffic DNAT in the specified IPSec SA.
in-dnat move <1..10> to <1..10>	Moves the specified rule (first rule number) to the specified location (second rule number) for in-bound traffic DNAT.
in-dnat append protocol {all | tcp | udp} original-ip *address_name* <0..65535> <0..65535> mapped-ip *address_name* <0..65535> <0..65535>	Maps the specified IP address and port range (original-ip) to the specified IP address and port range (mapped-ip) and appends this rule to the end of the rule list for in-bound traffic DNAT.
in-dnat insert <1..10> protocol {all | tcp | udp} original-ip *address_name* <0..65535> <0..65535> mapped-ip *address_name* <0..65535> <0..65535>	Maps the specified IP address and port range (original-ip) to the specified IP address and port range (mapped-ip) and inserts this rule before the specified rule.
in-dnat <1..10> protocol {all | tcp | udp} original-ip *address_name* <0..65535> <0..65535> *mapped-ip* *address_name* <0..65535> <0..65535>	Creates or revises the specified rule and maps the specified IP address and port range (original-ip) to the specified IP address and port range (mapped-ip).
[no] configuration-payload-provide activate	Enables configuration payload in server role. The no command disables it.
configuration-payload-provide address- {}	Sets configuration payload address . The no command disables it
[no] configuration-payload-provide {first-dns IPv6|second-dns IPv6}	Sets configuration payload address dns server. The no command disables it
[no] narrowed	Enables policy narrowed. The no command disables it.
[no] protocol gre	Enables GRE over IPSec to allow traffic using the Generic Routing Encapsulation (GRE) tunneling protocol through an IPSec tunnel. The no protocol command disables it.
mode-config activate	Allows the IPSec VPN client to receive an IP address, DNS and WINS information from the Zyxel Device when the scenario is Remote Access (Server Role) and VPN Gateway uses IKEv1. remote-access-server allows incoming connections from IPSec VPN clients with dynamic IP addresses.
mode-config address- *profile_name*	Sets the IP address to be included in the VPN setup data. *profile_name*: an address or address group object
[no] mode-config {first-dns | second-dns}	Specifies the DNS server IP address to assign to the remote users. The second-dns server's IP address is checked if first-dns is unavailable. The no command removes the setting.

Table 151 crypto Commands: IPSec SAs (continued)

COMMAND	DESCRIPTION
`[no] mode-config {first-wins | second-wins}`	Sets the IP address of the WINS (Windows Internet Naming Service) server that you want to send to the remote users. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using. The `second-wins` server's IP address is checked if `first-wins` is unavailable. The `no` command removes the setting.
`conn-check {`*`ip address ip address`*` | first-and-last} method {icmp | tcp} period <5...3600> timeout <1...10> fail-tolerance <1...10> action {log | no-log} probe-condition {all | any}`	Enables the IPSec VPN connection check. The Zyxel Device can regularly check the VPN connection to the gateway to specified to make sure it is still available. *`ip address`*: Specifies one or two domain names or IP addresses for the connectivity check. You can use one IP address and one domain name. Separate them with a comma, for example, 1.1.1.1,www.zyxel.com. `first-and-last`: Checks the connection to the first and last IP addresses in the connection's remote policy. Remote policy is the addresses of the devices behind the remote IPSec router. Make sure one of these is the peer gateway's LAN IP address. `method`: Sets how the Zyxel Device checks the connection. The peer must be configured to respond to the method you select. Sets the method to `icmp` to have the Zyxel Device regularly ping the address you specify to make sure traffic can still go through the connection. You may need to configure the peer to respond to pings. Sets the method to `tcp` to have the Zyxel Device regularly perform a TCP handshake with the address you specify to make sure traffic can still go through the connection You may need to configure the peer to accept the TCP connection. `period`: Sets the number of seconds between connection check attempts. `time-out`: Sets the number of seconds to wait for a response before the attempt is a failure. `fail-tolerance`: Sets the number of consecutive failures allowed before the Zyxel Device disconnects the VPN tunnel. The Zyxel Device resumes using the first peer gateway address when the VPN connection passes the connectivity check. `action`: Sets the action to log to have the Zyxel Device generate a log every time it checks this VPN. Sets the action to no-log to have the Zyxel Device take no action when it checks this VPN. `probe-condition`: Sets the probe-condition to any if you want the check to pass when at least one of the domain names or IP addresses responds. Sets the probe-condition `all` if you want the check to pass only when both domain names or IP addresses respond.
`debug conntrack flush`	Clears a blocked connection.

33.2.3 IPv4 IPSec SA Commands (for Manual Keys)

This table lists the additional commands for IPSec SAs using manual keys (VPN connections using manual keys).

Table 152 crypto map Commands: IPSec SAs (Manual Keys)

COMMAND	DESCRIPTION
`crypto map` *map_name*	
`set session-key {ah <256..4095>` *auth_key* `| esp <256..4095> [cipher` *enc_key*`] authenticator` *auth_key*`}`	Sets the active protocol, SPI (<256..4095>), authentication key and encryption key (if any). *auth_key*: You can use any alphanumeric characters or `,;|`~!@#$%^&*()_+\{}':./<>=-"`. The length of the key depends on the algorithm. md5 - 16-20 characters sha - 20 characters sha256 - 32 characters sha512 - 64 characters *enc_key*: You can use any alphanumeric characters or `,;\|`~!@#$%^&*()_+\{}':./<>=-"`. The length of the key depends on the algorithm. des - 8-32 characters 3des - 24-32 characters aes128 - 16-32 characters aes192 - 24-32 characters aes256 - 32 characters If you want to enter the key in hexadecimal, type “0x” at the beginning of the key. For example, "0x0123456789ABCDEF" is in hexadecimal format; in “0123456789ABCDEF” is in ASCII format. If you use hexadecimal, you must enter twice as many characters. The Zyxel Device automatically ignores any characters above the minimum number of characters required by the algorithm. For example, if you enter `1234567890XYZ` for a DES encryption key, the Zyxel Device only uses `12345678`. The Zyxel Device still stores the longer key.
`local-ip` *ip*	Sets the local gateway address to the specified IP address.
`peer-ip` *ip*	Sets the remote gateway address to the specified IP address.

33.2.4 VPN Concentrator Commands

This table lists the commands for the VPN concentrator.

Table 153 vpn-concentrator Commands: VPN Concentrator

COMMAND	DESCRIPTION
`show vpn-concentrator [profile_name]`	Shows the specified VPN concentrator or all VPN concentrators.
`[no] vpn-concentrator profile_name`	Creates the specified VPN concentrator if necessary and enters sub-command mode. The no command deletes the specified VPN concentrator.
`[no] crypto map_name`	Adds the specified IPSec SA to the specified VPN concentrator. The no command removes the specified IPSec SA from the specified VPN concentrator.
`vpn-concentrator rename profile_name profile_name`	Renames the specified VPN concentrator (first *profile_name*) to the specified name (second *profile_name*).

33.2.5 VPN Configuration Provisioning Commands

This table lists the commands for VPN configuration provisioning.

Table 154 vpn-configuration-provision Commands: VPN Configuration Provisioning

COMMAND	DESCRIPTION
`vpn-configuration-provision rule { append | conf_index | insert conf_index }`	Enters the VPN configuration provisioning sub-command mode to add or edit a rule. *conf_index*: The index number of a VPN configuration provisioning rule, 1 to the Zyxel Device's maximum number of VPN connection rules.
`[no] activate`	Turns the VPN configuration provisioning rule on or off.
`crypto map_name`	Specifies the name of the IPSec VPN connection (*map_name*) to bind to this VPN configuration provisioning rule's user or group.
`user username`	Specifies a user or group of users allowed to use the Zyxel Device IPSec VPN client to retrieve the associated VPN rule settings. A user may belong to a number of groups. If VPN configuration provisioning rules are configured for different groups, the Zyxel Device will allow VPN rule setting retrieval based on the first match found. Admin or limited-admin users are not allowed.
`no user`	Removes the VPN configuration provisioning rule's user or user group configuration. In other words, any users can match the rule. In the GUI "any" will display in the Allowed User field.
`[no] ul-bandwidth-limit <1...1048576>`	Sets the maximum bandwidth for uploading traffic from IPsec VPN clients over IPSec VPN tunnels. This feature is available for Zyxel subscription-based SecuExtender IPSec VPN clients with Window version 5.6.80.007 or later or macOS version 1.2.0.7 or later.
`exit`	Leaves sub-command mode.
`vpn-configuration-provision rule { delete conf_index | move conf_index to conf_index }`	Deletes or moves the specified VPN configuration provisioning rule.
`[no] vpn-configuration-provision activate`	Turns the VPN configuration provisioning service on or off.

Table 154 vpn-configuration-provision Commands: VPN Configuration Provisioning

COMMAND	DESCRIPTION
`vpn-configuration-provision port <1...65535>`	Sets a new port between 1024 to 65535 that is not in use by other services. This change the default port that IPSec VPN clients use to retrieve VPN rule settings from the Zyxel Device. The default is 443 which is already in use for remote management by default. If you change the default IPSec VPN port on the Zyxel Device, make sure to make the same change to the Zyxel IPSec VPN client.
`no vpn-configuration-provision port`	Sets the VPN configuration provisioning port back to default.
`show vpn-configuration-provision port`	Displays the current VPN configuration provisioning port.
`vpn-configuration-provision authentication` *`auth_method`*	Sets the authentication method the VPN configuration provisioning service uses to authenticate users.
`show vpn-configuration-provision activation`	Displays whether or not the VPN configuration provisioning service is activated.
`show vpn-configuration-provision authentication`	Displays the authentication method the VPN configuration provisioning service uses to authenticate users.
`show vpn-configuration-provision rules`	Displays the settings of the configured VPN configuration provisioning rules.
`show vcp allowed users`	Displays available users who can be configured as allowed users (using `user` *`username`*) of a VPN Configuration Provision (VCP) rule.
`show vcp allowed crypto map`	Displays IPv4 VPN Connection rules which can be used in a VPN Configuration Provision (VCP) rule. Nothing displays if no suitable rules are available.
`show vcp allowed crypto map6`	Displays IPv6 VPN Connection rules which can be used in a VPN Configuration Provision (VCP) rule. Nothing displays if no suitable rules are available.
`[no] vpn-configuration-provision iosfilter`	Enables over-the-air VPN provisioning for mobile Apple (iOS) devices. The Apple (iOS) user must log into the Zyxel Device web configurator using a Safari browser to be authenticated. The user can then set up a VPN connection by visiting a link in the Safari browser to install an XML VPN configuration file. The VPN rule for the Apple (iOS) device must be configured first. Each VPN rule must have a separate link. Types of VPN supported are: • L2TP • IKEv1 Cisco VPN • IKEv2 (for iOS 9.3 and later) The `no` command disables over-the-air VPN provisioning for mobile Apple (iOS) devices using a Safari browser.

Table 154 vpn-configuration-provision Commands: VPN Configuration Provisioning

COMMAND	DESCRIPTION
`show vpn-configuration-provision iosfilter`	Displays if over-the-air VPN provisioning for mobile Apple (iOS) devices is enabled on the Zyxel Device.
`vpn-configuration-provision generate {ios | windows | android} ikev2-wizard profile <profile name>`	Downloads a VPN configuration script to send to VPN clients using a supported operating system. Uses *profile name* to set the file name for the downloaded configuration script. To use the download script, your device needs to support: • Windows 8 and later version. • iOS 13 and later version. • MAC OS 10.12.2 and later version. • Android 10.0 and later version. Install strongSwan VPN client version 2.3.3 or later on your device first.

33.2.6 SA Monitor Commands

This table lists the commands for the SA monitor.

Table 155 sa Commands: SA Monitor

COMMAND	DESCRIPTION
`show sa monitor [{begin <1..1000>} | {end <1..1000>} | {crypto-map regexp} | {policy regexp} |{rsort sort_order} | {sort sort_order}]`	Displays the current IPSec SAs and the status of each one. You can specify a range of SA entries to display. You can also control the sort order of the display and search by VPN connection or (local or remote) policy. *regexp*: A keyword or regular expression. Use up to 30 alphanumeric and _+-.()!$*^:?|{}[]<>/ characters. A question mark (?) lets a single character in the VPN connection or policy name vary. For example, use “a?c” (without the quotation marks) to specify abc, acc and so on. Wildcards (*) let multiple VPN connection or policy names match the pattern. For example, use “*abc” (without the quotation marks) to specify any VPN connection or policy name that ends with “abc”. A VPN connection named “testabc” would match. There could be any number (of any type) of characters in front of the “abc” at the end and the VPN connection or policy name would still match. A VPN connection or policy name named “testacc” for example would not match. A * in the middle of a VPN connection or policy name has the Zyxel Device check the beginning and end and ignore the middle. For example, with “abc*123”, any VPN connection or policy name starting with “abc” and ending in “123” matches, no matter how many characters are in between. The whole VPN connection or policy name has to match if you do not use a question mark or asterisk. See Table 149 on page 278 for other parameter description.
`show isakmp sa`	Displays current IKE SA and the status of each one.
`no sa spi spi`	Deletes the SA specified by the SPI. *spi*: 2-8 hexadecimal (0-9, A-F) characters
`no sa tunnel-name map_name`	Deletes the specified IPSec SA.
`show sa counter`	Displays the IPSec VPN tunnels that are currently established.
`show vpn-counters`	Displays VPN traffic statistics.

33.2.7 IPv4 IKEv2 SA Commands

This table lists the commands for the IPv4 IKEv2 SA.

Table 156 sa Commands: IPv4 IKEv2

COMMAND	DESCRIPTION
`show ikev2 policy [policy_name]`	Shows the specified IKEv2 SA or all IKEv2 SAs.
`[no] ikev2 policy policy_name`	Creates the specified IKEv2 SA if necessary and enters sub-command mode. The no command deletes the specified IKEv2 SA.
`activate` `deactivate`	Activates or deactivates the specified IKEv2 SA.
`authentication {pre-share | rsa-sig}`	Specifies whether to use a pre-shared key or a certificate for authentication
`certificate certificate-name`	Sets the certificate that can be used for authentication.
`[no] fall-back`	Set this to have the Zyxel Device reconnect to the primary address when it becomes available again and stop using the secondary connection, if the connection to the primary address goes down and the Zyxel Device changes to using the secondary connection. Users will lose their VPN connection briefly while the Zyxel Device changes back to the primary connection. To use this, the peer device at the secondary address cannot be set to use a nailed-up VPN connection.
`fall-back-check-interval <60..86400>`	Sets how often (in seconds) the Zyxel Device checks if the primary address is available.
`transform-set isakmp-algo [isakmp_algo [isakmp_algo]]`	Sets the encryption and authentication algorithms for each IKEv2 SA proposal. `isakmp_algo`: `{des-md5 | des-sha | 3des-md5 | 3des-sha | aes128-md5 | aes128-sha | aes192-md5 | aes192-sha | aes256-md5 | aes256-sha | aes256-sha256 | aes256-sha512}`
`lifetime <180..3000000>`	Sets the IKEv2 SA life time to the specified value.

`group1`
`group2`
`group5`
`group14`
`group15`
`group16`
`group17`
`group18`
	Sets the DH group to the specified group.
	Different operating systems may support different DH key groups. Check your operating system documentation.
	• For Windows VPN clients, Zyxel SecuExtender perpetual VPN clients versions 3.8.203.61.32 and earlier support DH1 to DH14.
	• For macOS VPN clients, Zyxel SecuExtender subscription VPN clients versions 1.2.0.7 and later support DH14 to DH21. For Windows VPN clients, Zyxel SecuExtender subscription VPN clients versions 5.6.80.007 and later support DH14 to DH21.
	• Windows versions 7, 10, 11 built-in IKEv2 VPN clients support DH2 by default.
	• macOS versions 14.2 and later built-in IKEv2 VPN clients support DH14 by default.
	• iOS versions 10.15 and later built-in IKEv2 VPN clients support DH14 by default.

`local-ip {ip {ip | domain_name} | interface interface_name}`	Sets the local gateway address to the specified IP address, domain name, or interface.
`peer-ip {ip | domain_name} [ip | domain_name]`	Sets the remote gateway address(es) to the specified IP address(es) or domain name(s).

Table 156 sa Commands: IPv4 IKEv2 (continued)

COMMAND	DESCRIPTION
keystring pre_shared_key	Sets the pre-shared key of up to 128 characters that can be used for authentication. The pre_shared_key can be: • Alphanumeric characters or ,;|`~!@#$%^&*()_+\{}':./<>=-". • Hexadecimal (0-9, A-F) characters, preceded by "0x". The pre-shared key is case-sensitive.
local-id type {ip ip | fqdn domain_name | mail e_mail | dn distinguished_name}	Sets the local ID type and content to the specified IP address, domain name, or e-mail address.
peer-id type {any | ip ip | fqdn domain_name | mail e_mail | dn distinguished_name}	Sets the peer ID type and content to any value, the specified IP address, domain name, or e-mail address.
eap auth_method AUTH_METHOD	Sets auth method for EAP. Default value is Mschapv2.
[no] eap type {server AAA_method user-id {name|any}| client name username {password PASSWORD| encrypted-password PASSWORD}	Enables extended authentication and specifies whether the ZyWALL/ USG is the server or client. If the Zyxel Device is the server, it also specifies the AAA authentication method (aaa authentication profile_name); if the Zyxel Device is the client, it also specifies the username and password to provide to the remote IPSec router. The no command disables extended authentication. • username: You can use alphanumeric characters, underscores (_), and dashes (-), and it can be up to 31 characters long. • password: You can use most printable ASCII characters. You cannot use square brackets [ ], double quotation marks ("), question marks (?), tabs or spaces. It can be up to 31 characters long.
ikev2 policy rename policy_name policy_name	Renames the specified IKEv2 SA (first policy_name) to the specified name (second policy_name).
[no] twofa-auth	Enables two-factor authentication. The no command disables two-factor authentication.

33.2.8 IPv6 IKEv2 SA Commands

This table lists the commands for the IPv4 IKEv2 SA.

Table 157 sa Commands: IPv6 IKEv2

COMMAND	DESCRIPTION
show ikev2 policy6 [*policy_name*]	Shows the specified IKEv2 SA or all IKEv2 SAs.
[no] ikev2 policy6 *policy_name*	Creates the specified IKEv2 SA if necessary and enters sub-command mode. The no command deletes the specified IKEv2 SA.
activate deactivate	Activates or deactivates the specified IKEv2 SA.
authentication {pre-share | rsa-sig}	Specifies whether to use a pre-shared key or a certificate for authentication
certificate certificate-name	Sets the certificate that can be used for authentication.

Table 157 sa Commands: IPv6 IKEv2 (continued)

COMMAND	DESCRIPTION
`[no] fall-back`	Set this to have the Zyxel Device reconnect to the primary address when it becomes available again and stop using the secondary connection, if the connection to the primary address goes down and the Zyxel Device changes to using the secondary connection. Users will lose their VPN connection briefly while the Zyxel Device changes back to the primary connection. To use this, the peer device at the secondary address cannot be set to use a nailed-up VPN connection.
`fall-back-check-interval <60..86400>`	Sets how often (in seconds) the Zyxel Device checks if the primary address is available.
`transform-set isakmp-algo [isakmp_algo [isakmp_algo]]`	Sets the encryption and authentication algorithms for each IKEv2 SA proposal. `isakmp_algo`: {`des-md5 | des-sha | 3des-md5 | 3des-sha | aes128-md5 | aes128-sha | aes192-md5 | aes192-sha | aes256-md5 | aes256-sha | aes256-sha256 | aes256-sha512`}
`lifetime <180..3000000>`	Sets the IKEv2 SA life time to the specified value.

`group1`
`group2`
`group5`
	Sets the DH group to the specified group.

`local-ip {ip IPv6}`	Sets the local gateway address to the specified IP address.
`peer-ip {ip IPv6]`	Sets the remote gateway address(es) to the specified IP address(es).
`keystring pre_shared_key`	Sets the pre-shared key of up to 128 characters that can be used for authentication. The pre_shared_key can be: • Alphanumeric characters or ,;|`~!@#$%^&*()_+\{}':./<>=-". • Hexadecimal (0-9, A-F) characters, preceded by "0x". The pre-shared key is case-sensitive.
`local-id type {ip IPv6 | fqdn domain_name | mail e_mail | dn distinguished_name}`	Sets the local ID type and content to the specified IP address, domain name, or e-mail address.
`peer-id type {any | ip IPv6 | fqdn domain_name | mail e_mail | dn distinguished_name}`	Sets the peer ID type and content to any value, the specified IP address, domain name, or e-mail address.
`eap auth_method` *`auth_method`*	Sets auth method for EAP. Default value is `Mschapv2`.
`[no] eap type {server` *`auth_method`* `user-id {name|any}| client name username {password PASSWORD| encrypted-password` *`password`*`}`	Enables extended authentication and specifies whether the ZyWALL/ USG is the server or client. If the Zyxel Device is the server, it also specifies the AAA authentication method (aaa authentication profile_name); if the Zyxel Device is the client, it also specifies the username and password to provide to the remote IPSec router. The no command disables extended authentication. • *`username`*: You can use alphanumeric characters, underscores (_), and dashes (-), and it can be up to 31 characters long. • *`password`*: You can use most printable ASCII characters. You cannot use square brackets [ ], double quotation marks ("), question marks (?), tabs or spaces. It can be up to 31 characters long.
`ikev2 policy rename policy_name policy_name`	Renames the specified IKEv2 SA (first policy_name) to the specified name (second policy_name).
`[no] twofa-auth`	Enables two-factor authentication. The `no` command disables two-factor authentication.

33.2.9 IPv6 IPSec SA Commands

This table lists the commands for IPv6 IPSec SAs.

Table 158 crypto Commands: IPv6 IPSec SAs

COMMAND	DESCRIPTION
`show crypto map6 [map_name]`	Shows the specified IPSec SA or all IPSec SAs.
`crypto map6 dial map_name`	Dials the specified IPSec SA manually. This command does not work for IPSec SAs using manual keys or for IPSec SAs where the remote gateway address is 0.0.0.0.
`[no] crypto map map_name`	Creates the specified IPSec SA if necessary and enters sub-command mode. The no command deletes the specified IPSec SA.
`crypto map rename map_name map_name`	Renames the specified IPSec SA (first *map_name*) to the specified name (second *map_name*).
`crypto map map_name`	
`activate` `deactivate`	Activates or deactivates the specified IPSec SA.
`adjust-mss {auto | <200..1500>}`	Set a specific number of bytes for the Maximum Segment Size (MSS) meaning the largest amount of data in a single TCP segment or IP datagram for this VPN connection or use `auto` to have the ZyWALL automatically set it.
`ipsec-isakmp policy_name`	Specifies the IKE SA for this IPSec SA and disables manual key.
`encapsulation {tunnel | transport}`	Sets the encapsulation mode.
`transform-set crypto_algo_esp [crypto_algo_esp [crypto_algo_esp]]`	Sets the active protocol to ESP and sets the encryption and authentication algorithms for each proposal. *crypto_algo_esp*: esp-null-md5 | esp-null-sha | esp-null-sha256 | esp-null-sha512 | esp-des-md5 | esp-des-sha | esp-des-sha256 | esp-des-sha512 | esp-3des-md5 | esp-3des-sha | esp-3des-sha256 | esp-3des-sha512 | esp-aes128-md5 | esp-aes128-sha | esp-aes128-sha256 | esp-aes128-sha512 | esp-aes192-md5 | esp-aes192-sha | esp-aes192-sha256 | esp-aes192-sha512 | esp-aes256-md5 | esp-aes256-sha | esp-aes256-sha256 | esp-aes256-sha512
`transform-set crypto_algo_ah [crypto_algo_ah [crypto_algo_ah]]`	Sets the active protocol to AH and sets the encryption and authentication algorithms for each proposal. *crypto_algo_ah*: ah-md5 | ah-sha | ah-sha256 | ah-sha512

Table 158 crypto Commands: IPv6 IPSec SAs (continued)

COMMAND	DESCRIPTION
`scenario {site-to-site-static|site-to-site-dynamic|remote-access-server|remote-access-client}`	Select the scenario that best describes your intended VPN connection. `Site-to-site`: The remote IPSec router has a static IP address or a domain name. This Zyxel Device can initiate the VPN tunnel. `site-to-site-dynamic`: The remote IPSec router has a dynamic IP address. Only the remote IPSec router can initiate the VPN tunnel. `remote-access-server`: Allow incoming connections from IPSec VPN clients. The clients have dynamic IP addresses and are also known as dial-in users. Only the clients can initiate the VPN tunnel. `remote-access-client`: Choose this to connect to an IPSec server. This Zyxel Device is the client (dial-in user) and can initiate the VPN tunnel.
`set security-association lifetime seconds <180..3000000>`	Sets the IPSec SA life time.
`set pfs {group1 | group2 | group5 | none}`	Enables Perfect Forward Secrecy group.
`local-policy` *address_name*	Sets the address object for the local policy (local network).
`remote-policy` *address_name*	Sets the address object for the remote policy (remote network).
`[no] policy-enforcement`	Drops traffic whose source and destination IP addresses do not match the local and remote policy. This makes the IPSec SA more secure. The `no` command allows traffic whose source and destination IP addresses do not match the local and remote policy. Note: You must allow traffic whose source and destination IP addresses do not match the local and remote policy, if you want to use the IPSec SA in a VPN concentrator.
`[no] nail-up`	Automatically re-negotiates the SA as needed. The `no` command does not.
`[no] replay-detection`	Enables replay detection. The `no` command disables it.
`[no] configuration-payload-provide activate`	Enables configuration payload in server role. The no command disables it.
`configuration-payload-provide address- {}`	Sets configuration payload address . The no command disables it
`[no] configuration-payload-provide {first-dns IPv6|second-dns IPv6}`	Sets configuration payload address dns server. The no command disables it
`[no] narrowed`	Enables policy narrowed. The no command disables it

33.2.10 IPv6 VPN Concentrator Commands

This table lists the commands for the IPv6 VPN concentrator.

Table 159 vpn-concentrator Commands: VPN Concentrator

COMMAND	DESCRIPTION
`show vpn-concentrator6 [profile_name]`	Shows the specified IPv6 VPN concentrator or all IPv6 VPN concentrators.
`[no] vpn-concentrator6 profile_name`	Creates the specified IPv6 VPN concentrator if necessary and enters sub-command mode. The no command deletes the specified IPv6 VPN concentrator.
`[no] crypto map_name`	Adds the specified IPSec SA to the specified IPv6 VPN concentrator. The no command removes the specified IPSec SA from the specified IPv6 VPN concentrator.
`vpn-concentrator6 rename profile_name profile_name`	Renames the specified IPv6 VPN concentrator (first *profile_name*) to the specified name (second *profile_name*).

CHAPTER 34
SSL VPN

34.1 SSL Access Policy

An SSL access policy allows the Zyxel Device to perform the following tasks:

- limit user access to specific applications or files on the network.
- allow user access to specific networks.
- assign private IP addresses and provide DNS/WINS server information to remote users to access internal networks.

34.1.1 SSL Application Objects

SSL application objects specify an application type and server that users are allowed to access through an SSL tunnel. See Chapter 60 on page 501 for how to configure SSL application objects.

34.1.2 SSL Access Policy Limitations

You cannot delete an object that is used by an SSL access policy. To delete the object, you must first unassociate the object from the SSL access policy.

34.2 SSL VPN Commands

The following table describes the values required for some SSL VPN commands. Other values are discussed with the corresponding commands.

Table 160 Input Values for SSL VPN Commands

LABEL	DESCRIPTION
profile_name	The descriptive name of an SSL VPN access policy. You may use up to 31 characters (“a-z”, A-Z”, “0-9”) with no spaces allowed.
address_object	The name of an IP address (group) object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
application_object	The name of an SSL application object. You may use up to 31 characters (“0-9”, “a-z”, “A-Z”, “-” and “_”). No spaces are allowed.
user_name	The name of a user (group). You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

The following sections list the SSL VPN commands.

34.2.1 SSL VPN Commands

This table lists the commands for SSL VPN. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 161 SSL VPN Commands

COMMAND	DESCRIPTION
`sslvpn login message <description>`	Sets the login message that users see after logging into the Zyxel Device using SSL VPN.
`sslvpn login-port <1..65535>`	Sets the SSL VPN server port of the Zyxel Device for full tunnel mode SLL VPN access. Leave this field to default settings unless it conflicts with another interface.
`no sslvpn login-port`	Resets the SSL VPN server port of the Zyxel Device back to its default setting,
`show sslvpn login-port`	Displays the SSL VPN server port of the Zyxel Device.
`sslvpn logout message <description>`	Sets the login message that users see after logging out of the Zyxel Device using SSL VPN.
`show sslvpn policy [profile_name]`	Displays the settings of the specified SSL VPN access policy.
`show ssl-vpn network-extension local-ip`	Displays the IP address that-t the Zyxel Device uses in setting up the SSL VPN.
`show sslvpn monitor`	Displays a list of the users who are currently logged into the VPN SSL client portal.
`sslvpn network-extension local-ip ip`	Sets the IP address that the Zyxel Device uses in setting up the SSL VPN.
`sslvpn policy {profile_name | profile_name append | profile_name insert <1..16>}`	Enters the SSL VPN sub-command mode to add or edit an SSL VPN access policy.
`[no] activate`	Turns the SSL VPN access policy on or off.
`[no] application application_object`	Adds the SSL application object to the SSL VPN access policy.
`[no] description description`	Adds information about the SSL VPN access policy. Use up to 60 characters (“0-9”, “a-z”, “A-Z-”, “-” and “_”).
`[no] network-extension {activate | ip-address_object | 1st-dns {address_object | ip } | 2nd-dns {address_object | ip } | 1st-wins {address_object | ip } | 2nd-wins {address_object | ip } | network address_object}`	Use this to configure for a VPN tunnel between the authenticated users and the internal network. This allows the users to access the resources on the network as if they were on the same local network. `ip-`: specify the name of the IP addresses to assign to the user computers for the VPN connection. `1st/2nd-dns/sins`: specify the name of the DNS or WINS servers to assign to the remote users. This allows them to access devices on the local network using domain names instead of IP addresses. `network`: specify a network users can access.
`[no] network-extension traffic-enforcement`	Forces all SSL VPN client traffic to be sent through the SSL VPN tunnel. The no command disables this setting.
`[no] network-extension netbios-broadcast`	Allows netbios broadcast packets to pass through the SSL VPN tunnel.
`[no] user user_name`	Specifies the user or user group that can use the SSL VPN access policy.

Table 161 SSL VPN Commands

COMMAND	DESCRIPTION
`sslvpn policy move <1..16> to <1..16>`	Moves the specified SSL VPN access policy to the number that you specified.
`sslvpn no connection username user_name`	Terminates the user's SSL VPN connection and deletes corresponding session information from the Zyxel Device.
`no sslvpn policy profile_name`	Deletes the specified SSL VPN access policy.
`sslvpn policy rename profile_name profile_name`	Renames the specified SSL VPN access policy.
`show workspace application`	Displays the SSLVPN resources available to each user when logged into SSLVPN.
`show workspace cifs`	Displays the shared folders available to each user when logged into SSLVPN.

34.2.2 Setting an SSL VPN Rule Tutorial

Here is an example SSL VPN configuration. The SSL VPN rule defines:

- Only users using the "tester" account can use the SSL VPN.
- The Zyxel Device will assign an IP address from 192.168.100.1 to 192.168.100.10 (defined in object "IP-") to the computers which match the rule's criteria.
- The Zyxel Device will assign two DNS server settings (172.16.1.1 and 172.16.1.2 defined in objects DNS1 and DNS2) to the computers which match the rule's criteria.
- The SSL VPN users are allowed to access the Zyxel Device's local network, 172.16.10.0/24 (defined in object "Network1").

1 First of all, configure 10.1.1.254/24 for the IP address of interface ge2 which is an external interface for public SSL VPN to access. Configure 172.16.10.254/24 for the IP address of interface ge3 which is an internal network.

```
Router(config)# interface ge2
Router(config-if-ge)# ip address 10.1.1.254 255.255.255.0
Router(config-if-ge)# exit
Router(config)# interface ge3
Router(config-if-ge)# ip address 172.16.10.254  255.255.255.0
Router(config-if-ge)# exit
```

2 Create four address objects for the SSL VPN DHCP , DNS servers and the local network for SSL VPN authenticated users to access.

```
Router(config)# address-object IP- 192.168.100.1-192.168.100.10
Router(config)# address-object DNS1 172.16.5.1
Router(config)# address-object DNS2 172.16.5.2
Router(config)# address-object NETWORK1 172.16.10.0/24
```

3 Create the SSL VPN user account named tester with password 1234.

```
Router(config)# username tester password 1234 user-type user
```

4 Create an SSL VPN rule named SSL_VPN_TEST. Enable it and apply objects you just created.

```
Router(config)# sslvpn policy SSL_VPN_TEST
Router(policy SSL_VPN_TEST)# activate
Router(policy SSL_VPN_TEST)# user tester
Router(policy SSL_VPN_TEST)# network-extension activate
Router(policy SSL_VPN_TEST)# network-extension ip- IP-
Router(policy SSL_VPN_TEST)# network-extension 1st-dns DNS1
Router(policy SSL_VPN_TEST)# network-extension 2nd-dns DNS2
Router(policy SSL_VPN_TEST)# network-extension network NETWORK1

Router(policy SSL_VPN_TEST)# exit
```

5 Displays the SSL VPN rule settings.

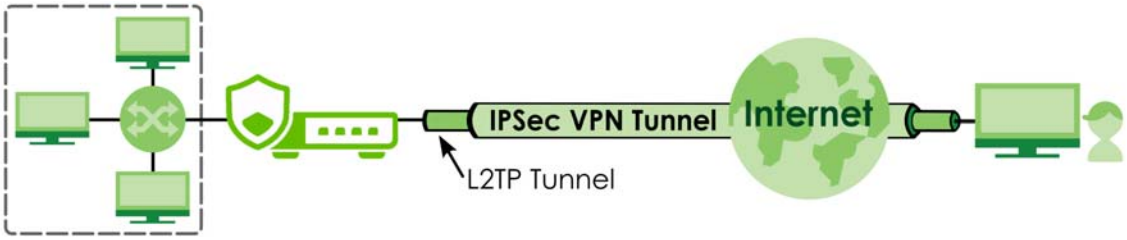
```
Router(config)# show sslvpn policy SSL_VPN_TEST
index: 1
  active: yes
  name: SSL_VPN_TEST
  description:
  user: tester
  ssl application: none
  network extension: yes
  traffic enforcement:no
  netbios broadcast: no
  ip : IP-
  dns server 1: DNS1
  dns server 2: DNS2
  wins server 1: none
  wins server 2: none
  network: NETWORK1

  reference count: 0
```

CHAPTER 35
L2TP VPN

35.1 L2TP VPN Overview

L2TP VPN lets remote users use the L2TP and IPSec client software included with their computers' operating systems to securely connect to the network behind the Zyxel Device. The remote users do not need their own IPSec gateways or VPN client software.

Figure 30 L2TP VPN Overview



The Layer 2 Tunneling Protocol (L2TP) works at layer 2 (the data link layer) to tunnel network traffic between two peers over another network (like the Internet). In L2TP VPN, an IPSec VPN tunnel is established first (see Chapter 33 on page 277 for information on IPSec) and then an L2TP tunnel is built inside it.

Note: At the time of writing the L2TP remote user must have a public IP address in order for L2TP VPN to work (the remote user cannot be behind a NAT router or a firewall).

35.2 IPSec Configuration

You must configure an IPSec VPN connection for L2TP VPN to use (see Chapter 33 on page 277 for details). The IPSec VPN connection must:

- Be enabled.
- Use transport mode.
- Not be a manual key VPN connection.
- Use Pre-Shared Key authentication.
- Use a VPN gateway with the Secure Gateway set to 0.0.0.0 if you need to allow L2TP VPN clients to connect from more than one IP address.

35.2.1 Using the Default L2TP VPN Connection

Default_L2TP_VPN_Connection is pre-configured to be convenient to use for L2TP VPN. If you use it, edit the following.

Configure the local and remote policies as follows.

- For the Local Policy, create an address object that uses host type and contains the My Address IP address that you configured in the Default_L2TP_VPN_GW. Use this address object in the local policy.
- For the Remote Policy, create an address object that uses host type and an IP address of 0.0.0.0. Use this address object in the remote policy.

You must also edit the Default_L2TP_VPN_GW gateway entry.

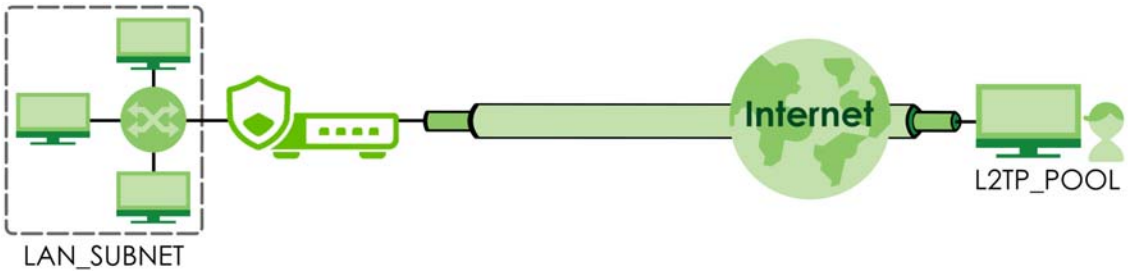
- Configure the My Address setting according to your requirements.
- Replace the default Pre-Shared Key.

35.3 LAN Policy Route

You must configure a policy route to let VPN users access resources on a network behind the Zyxel Device.

- Set the policy route's Source Address to the address object that you want to allow the remote users to access (LAN_SUBNET in the following figure).
- Set the Destination Address to the IP address that the Zyxel Device assigns to the remote users (L2TP_ in the following figure).

Figure 31 Policy Route for L2TP VPN



35.4 WAN Policy Route

You must configure a policy route with SNAT to let VPN users send traffic out through the WAN interface, for example to the Internet.

In firmware 5.0 and later, the Zyxel Device has a default policy route that forwards traffic from the VPN interface to the WAN and applies SNAT. This default policy route is applied to all VPN profiles in the zone VPN_To_WAN_SNAT. VPN_To_WAN_SNAT is a hidden zone and does not appear in the Web Configurator or when listing zones in the CLI.

Note: The Web Configurator automatically adds a VPN profile to zone VPN_To_WAN_SNAT when you enable setting "Allow Traffic Through WAN Zone". In the CLI, you must add each VPN profiles to the VPN_To_WAN_SNAT zone manually.

35.5 L2TP VPN Commands

The following table describes the values required for some L2TP VPN commands. Other values are discussed with the corresponding commands.

Table 162 Input Values for L2TP VPN Commands

LABEL	DESCRIPTION
address_object	The name of an IP address (group) object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
interface_name	The name of the interface. Ethernet interface: For some Zyxel Device models, use ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your Zyxel Device model. For other Zyxel Device models, use a name such as wan1, wan2, opt, lan1, or dmz. VLAN interface: vlan*x*, *x* = 0 - 4094 bridge interface: br*x*, *x* = 0 - N, where N depends on the number of bridge interfaces your Zyxel Device model supports.
ppp_interface	PPPoE/PPTP interface: ppp*x*, *x* = 0 - N, where N depends on the number of PPPoE/PPTP interfaces your Zyxel Device model supports.
map_name	The name of an IPSec SA. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
user_name	The name of a user (group). You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
domain_name	Fully-qualified domain name. You may use up to 254 alphanumeric characters, dashes (-), or periods (.), but the first character cannot be a period.
profile_name	The name of an L2TP VPN account. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

The following sections list the L2TP VPN commands.

35.5.1 L2TP VPN Commands

This table lists the commands for L2TP VPN. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 163 L2TP VPN Commands

COMMAND	DESCRIPTION
`l2tp-over-ipsec recover default-ipsec-policy`	If the default L2TP IPSec policy has been deleted, use this command to recreate it (with the default settings).
`[no] l2tp-over-ipsec activate;`	Turns L2TP VPN on. The `no` command turns it off.
`l2tp-over-ipsec crypto` *`map_name`*	Specifies the IPSec VPN connection the Zyxel Device uses for L2TP VPN. It must meet the requirements listed in Section 35.2 on page 299. Note: Modifying this VPN connection (or the VPN gateway that it uses) disconnects any existing L2TP VPN sessions.
`l2tp-over-ipsec` *`address-object`*	Specifies the address object that defines the of IP addresses that the Zyxel Device uses to assign to the L2TP VPN clients.

Table 163 L2TP VPN Commands

COMMAND	DESCRIPTION
`l2tp-over-ipsec authentication` *`authentication profile_name`*	Specifies how the Zyxel Device authenticates a remote user before allowing access to the L2TP VPN tunnel. The authentication method has the Zyxel Device check a user's user name and password against the Zyxel Device's local database, a remote LDAP, RADIUS, a Active Directory server, or more than one of these.
`certificate` *`cert_name`*	Select the certificate to use to identify the Zyxel Device for L2TP VPN connections. The certificate is used with the EAP, PEAP, and MSCHAPv2 authentication protocols. The certificate must already be configured.
`[no] l2tp-over-ipsec user user_name`	Specifies the user or user group that can use the L2TP VPN tunnel. If you do not configure this, any user with a valid account and password on the Zyxel Device to log in. The `no` command removes the user name setting.
`[no] l2tp-over-ipsec keepalive-timer <1..180>`	The Zyxel Device sends a Hello message after waiting this long without receiving any traffic from the remote user. The Zyxel Device disconnects the VPN tunnel if the remote user does not respond. The `no` command returns the default setting.
`[no] l2tp-over-ipsec first-dns-server {`*`ip`* `|` *`interface_name`*`} {1st-dns|2nd-dns|3rd-dns}| {`*`ppp_interface`*`}{1st-dns|2nd-dns}}`	Specifies the first DNS server IP address to assign to the remote users. You can specify a static IP address, or a DNS server that an interface received from its DHCP server. The `no` command removes the setting.
`[no] l2tp-over-ipsec second-dns-server {`*`ip`* `|` *`interface_name`*`} {1st-dns|2nd-dns|3rd-dns}| {`*`ppp_interface`*`}{1st-dns|2nd-dns}}`	Specifies the second DNS server IP address to assign to the remote users. You can specify a static IP address, or a DNS server that an interface received from its DHCP server. The `no` command removes the setting.
`[no] l2tp-over-ipsec first-wins-server` *`ip`*	Specifies the first WINS server IP address to assign to the remote users. The `no` command removes the setting.
`[no] l2tp-over-ipsec second-wins-server` *`ip`*	Specifies the second WINS server IP address to assign to the remote users. The `no` command removes the setting.
`no l2tp-over-ipsec session tunnel-id <0..65535>`	Deletes the specified L2TP VPN tunnel.
`show l2tp-over-ipsec`	Displays the L2TP VPN settings.
`show l2tp-over-ipsec session`	Displays current L2TP VPN sessions.

35.5.2 L2TP Account Commands

This table lists the commands to create, remove, display and bind L2TP VPN accounts. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

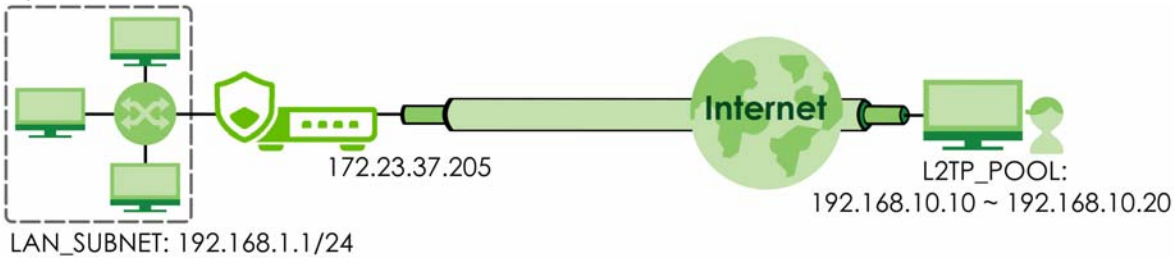
Table 164 L2TP VPN Commands

COMMAND	DESCRIPTION
`[no] account l2tp` *`profile_name`*	Creates an L2TP account and enters sub-command mode.
`authentication {chap | chap-pap | mschap | mschap-v2 | pap}`	Selects how the Zyxel Device authenticates a remote user before allowing access to the L2TP VPN tunnel. PAP (Password Authentication Protocol) is more readily available than CHAP (Challenge Handshake Authentication Protocol), but CHAP is more secure than PAP. • `chap-pap` - Your Zyxel Device accepts either CHAP or PAP when requested by this remote node. • `chap` - Your Zyxel Device accepts CHAP only. • `pap` - Your Zyxel Device accepts PAP only. • `mschap` - Your Zyxel Device accepts MSCHAP only. • `mschap-v2` - Your Zyxel Device accepts MSCHAP-V2 only.
`encrypted-password` *`ciphertext`*	Sets the password to encrypt L2TP traffic. *`ciphertext`*: The encryption password.
`idle <0..360>`	Specifies the number of seconds (0 to 360) that must elapse without traffic before the Zyxel Device automatically disconnects the L2TP tunnel. 0 (zero) means the timeout is disabled.
`password` *`isp_account_password`*	Sets the password given by the ISP for this account. *`isp_account_password`*: Password as given by ISP.
`server {`*`domain_name`* `|` *`w.x.y.z`*`}`	Specifies the fully-qualified domain name (*`domain_name`*) or IP address for the ISP account.
`user` *`isp_account_username`*	Displays the activity log for the specified user. *`isp_account_username`*: User name as given by ISP.
`show account l2tp [`*`profile_name`*`]`	Displays above details of all L2TP accounts or the one specified.
`Interface` *`interface_name`*	Specifies a PPP interface (see Section 16.2 on page 118) and enters that interface sub-command mode to bind an L2TP account to it.
`account` *`profile_name`*	Specifies the L2TP account to bind to this interface.
`local-address` *`w.x.y.z`*	Specifies the IP address of this interface.
`Interface disconnect`	Disconnects the L2TP tunnel on this interface.
`Interface dial wan1_ppp`	Connects the L2TP tunnel on this interface.
`show interface ppp`	Displays details of each PPP interface connection.

35.6 L2TP VPN Examples

This example uses the following settings in creating a basic L2TP VPN tunnel. See the Web Configurator User's Guide for how to configure L2TP in remote user computers using Windows XP and Windows 2000.

Figure 32 L2TP VPN Example



- The Zyxel Device has a static IP address of 172.23.37.205 for the ge3 interface.
- The remote user has a dynamic public IP address and connects through the Internet.
- You configure an IP address object named L2TP_ to assign the remote users IP addresses from 192.168.10.10 to 192.168.10.20 for use in the L2TP VPN tunnel.
- The VPN rule allows the remote user to access the LAN_SUBNET which covers the 192.168.1.1/24 subnet.

35.6.1 Configuring the Default L2TP VPN Gateway Example

The following commands configure the Default_L2TP_VPN_GW entry.

- Configure the My Address setting. This example uses interface ge3 with static IP address 172.23.37.205.
- Configure the Pre-Shared Key. This example uses “top-secret”.

```
Router(config)# isakmp policy Default_L2TP_VPN_GW
Router(config-isakmp Default_L2TP_VPN_GW)# local-ip interface ge3
Router(config-isakmp Default_L2TP_VPN_GW)# authentication pre-share
Router(config-isakmp Default_L2TP_VPN_GW)# keystring top-secret
Router(config-isakmp Default_L2TP_VPN_GW)# activate
Router(config-isakmp Default_L2TP_VPN_GW)# exit
Router(config)#
```

35.6.2 Configuring the Default L2TP VPN Connection Example

The following commands configure the Default_L2TP_VPN_Connection entry.

Enforce and configure the local and remote policies.

- For the Local Policy, create an address object that uses host type and contains the My Address IP address that you configured in the Default_L2TP_VPN_GW. The address object in this example uses IP address 172.23.37.205 and is named L2TP_IFACE.
- For the Remote Policy, create an address object that uses host type and an IP address of 0.0.0.0. It is named L2TP_HOST in this example.

```
Router(config)# crypto map Default_L2TP_VPN_Connection
Router(config-crypto Default_L2TP_VPN_Connection)# policy-enforcement
Router(config-crypto Default_L2TP_VPN_Connection)# local-policy L2TP_IFACE
Router(config-crypto Default_L2TP_VPN_Connection)# remote-policy L2TP_HOST
Router(config-crypto Default_L2TP_VPN_Connection)# activate
Router(config-crypto Default_L2TP_VPN_Connection)# exit
Router(config)#
```

35.6.3 Configuring the L2TP VPN Settings Example

The following commands configure and display the L2TP VPN settings.

- Set it to use the Default_L2TP_VPN_Connection VPN connection.
- Configure an IP address for the range of 192.168.10.10 to 192.168.10.20. In this example it is already created and called L2TP_.
- This example uses the default authentication method (the Zyxel Device's local user data base).
- Select a user or group of users that can use the tunnel. Here a user account named L2TP-test has been created.
- The other settings are left to the defaults in this example.
- Enable the connection.

```
Router(config)# l2tp-over-ipsec crypto Default_L2TP_VPN_Connection
Router(config)# l2tp-over-ipsec  L2TP_
Router(config)# l2tp-over-ipsec authentication default
Router(config)# l2tp-over-ipsec user L2TP-test
Router(config)# l2tp-over-ipsec activate
Router(config)# show l2tp-over-ipsec
L2TP over IPSec:
  activate          : yes
  crypto            : Default_L2TP_VPN_Connection
  address       : L2TP_
  authentication    : default
  user              : L2TP-test
  keepalive timer   : 60
  first dns server  : aux 1st-dns
  second dns server : aux 1st-dns
  first wins server :
  second wins server:
```

35.6.4 Configuring the LAN Policy Route for L2TP Example

The following commands configure and display the policy route for the L2TP VPN connection entry.

- Set the policy route's Source Address to the address object that you want to allow the remote users to access (LAN_SUBNET in this example).
- Set the Destination Address to the IP address that the Zyxel Device assigns to the remote users (L2TP_ in this example).
- Set the next hop to be the Default_L2TP_VPN_Connection tunnel.

- Enable the policy route.

```
Router(config)# policy 3
Router(policy-route)# source LAN_SUBNET
Router(policy-route)# destination L2TP_
Router(policy-route)# service any
Router(policy-route)# next-hop tunnel
Default_L2TP_VPN_ConnectionRouter(policy-route)# no deactivate
Router(policy-route)# exit
Router(config)# show policy-route 3
index: 3
  active: yes
  description: WIZ_VPN
  user: any
  schedule: none
  interface: ge1
  tunnel: none
  sslvpn: none
  source: PC_SUBNET
  destination: L2TP_
  service: any
  nexthop type: Tunnel
  nexthop: Default_L2TP_VPN_Connection
  bandwidth: 0
  bandwidth priority: 0
  maximize bandwidth usage: no
  SNAT: none
  amount of port trigger: 0
```

35.6.5 Configuring the WAN Policy Route for L2TP Example

Firmware 5.0 or later: The following commands configure the L2TP profile so that VPN clients to access the Internet through the WAN when connected to the Zyxel Device.

- Check that the default zone VPN_To_WAN_SNAT exists.
- Add the L2TP VPN profile to the VPN_To_WAN_SNAT zone.

```
Router# show zone VPN_To_WAN_SNAT
No. Type                              Member
=========================================================================
Router# configure terminal
Router(config)# zone VPN_To_WAN_SNAT
Router(zone)# crypto WIZ_VPN
```

CHAPTER 36
Bandwidth Management

36.1 Bandwidth Management Overview

Bandwidth management provides a convenient way to manage the use of various services on the network. It manages general protocols (for example, HTTP and FTP) and applies traffic prioritization to enhance the performance of delay-sensitive applications like voice and video.

36.1.1 BWM Type

The Zyxel Device supports two types of bandwidth management: shared, per-user and per-source-ip.

The shared BWM type is selected by default in a bandwidth management rule. All users to which the rule is applied need to share the bandwidth configured in the rule. If the BWM type is set to per-user in a rule, every user that matches the rule can use up to the configured bandwidth by his/her own. Set the BWM type set to per-source-ip in a rule,when you want to set the maximum bandwidth for traffic from an individual source IP address.

36.2 Bandwidth Management Commands

The following table lists the `bwm` commands. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 165 bwm Commands

COMMAND	DESCRIPTION
`bwm <1..127>`	Enters the `config-bwm` sub-command mode to configure a bandwidth management policy. See Table 166 on page 308 for the sub-commands.
`[no] bwm activate`	Enables bandwidth management on the Zyxel Device. The no command disabled bandwidth management.
`bwm append`	Enters the `config-bwm` sub-command mode to add a policy to the end of the policy list. See Table 166 on page 308 for the sub-commands.
`bwm default inbound priority <1..7>`	Specifies a number between 1 and 7 to set the priority for incoming traffic that matches the default policy. The smaller the number, the higher the priority. Traffic with a higher priority is given bandwidth before traffic with a lower priority.
`bwm default outbound priority <1..7>`	Specifies a number between 1 and 7 to set the priority for outgoing traffic that matches the default policy.
`bwm delete <1..127>`	Removes a policy.

Table 165 bwm Commands (continued)

COMMAND	DESCRIPTION
`[no] bwm highest sip bandwidth priority`	Maximizes the throughput of SIP traffic to improve SIP-based VoIP call sound quality. This has the Zyxel Device immediately send SIP traffic upon identifying it. When this option is enabled the Zyxel Device ignores any other application patrol rules for SIP traffic (so there is no bandwidth control for SIP traffic) and does not record SIP traffic bandwidth usage statistics. The `[no]` command clears this setting.
`bwm insert <1..127>`	Enters the `config-bwm` sub-command mode to add a policy before the specified policy number. See Table 166 on page 308 for the sub-commands.
`bwm <1..127>`	Enters the `config-bwm` sub-command mode to create a bandwidth management policy. See Table 166 on page 308 for the sub-commands.
`bwm modify <1..127>`	Enters the `config-bwm` sub-command mode to edit a bandwidth management policy. See Table 166 on page 308 for the sub-commands.
`bwm move <1..127> to <1..127>`	Moves a policy to the number that you specified.
`show bwm activation`	Displays whether bandwidth management is enabled.
`show bwm all`	Displays all bandwidth management policies.
`show bwm applications list`	Displays all applications supported by bandwidth management.
`show bwm default`	Displays the default bandwidth management policy.
`show bwm highest sip bandwidth priority`	Displays whether the Zyxel Device is set maximize the throughput of SIP traffic to improve SIP-based VoIP call sound quality.

36.2.1 Bandwidth Sub-Commands

The following table describes the sub-commands for several `bwm` commands.

Table 166 bwm Sub-commands

COMMAND	DESCRIPTION
`[no] activate`	Enables a policy. The no command disables the policy.
`[no] description` *`description`*	Sets a descriptive name (up to 60 printable ASCII characters) for a policy. The no command removes the descriptive name from the policy.
`[no] destination` *`address_object`*	Sets the destination IP address or address group for whom this policy applies. The no command resets the destination IP address(es) to the default (any). any means all IP addresses.
`[no] dscp {<0..63> | any | class {af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs0 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | default | wmm_be0 | wmm_be24 | wmm_bk16 | wmm_bk8 | wmm_vi32 | wmm_vi40 | wmm_vo48 | wmm_vo56}}`	Specifies a DSCP code point value or sets an AF class or QoS access class of incoming or outgoing packets to which this policy applies. any means all DSCP value or no DSCP marker. The no command resets the DSCP code to the default (any).

Table 166 bwm Sub-commands (continued)

COMMAND	DESCRIPTION
`[no] inbound ceiling {<0..1048576> | maximize-bandwidth-usage}`	Sets the maximum bandwidth allowed for incoming traffic or enables maximize bandwidth usage to let the traffic matching this policy "borrow" any unused bandwidth on the incoming interface. The no command resets the inbound maximum bandwidth to the default (0).
`[no] inbound guarantee-bandwidth <0..1048576> priority <1..7>`	Sets how much inbound bandwidth, in kilobits per second, this policy allows the traffic to use and also sets a number between 1 and 7 to set the priority for traffic that matches this policy. The smaller the number, the higher the priority. Inbound refers to the traffic the Zyxel Device sends to a connection's initiator. The no command resets the inbound guarantee bandwidth to the default (0).
`[no] inbound-dscp-mark {<0..63> | class {af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs0 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | default | wmm_be0 | wmm_be24 | wmm_bk16 | wmm_bk8 | wmm_vi32 | wmm_vi40 | wmm_vo48 | wmm_vo56}}`	Sets the DSCP value to apply to the incoming packets that match this policy. `default`: to have the Zyxel Device set the DSCP value of the packets to 0. The no command resets the incoming DSCP code to the default (`preserve`) and have the Zyxel Device keep the packets' original DSCP value.
`[no] incoming-interface {interface` *`interface_name`* `| trunk` *`group_name`*`}`	Sets the source interface of the traffic to which this policy applies. *`interface_name`*: The name of the interface. This depends on the Zyxel Device model. See Table 52 on page 118 for detailed information about the interface name. *`group_name`*: A descriptive name for the trunk. The name cannot start with a number. This value is case-sensitive. The no command resets the incoming interface to the default (any).
`[no] log [alert]`	Sets the Zyxel Device to generate a log (and alert) for packets that match the policy. The no command sets the Zyxel Device to not generate a log and alert for packets that match the policy.
`[no] outbound ceiling {<0..1048576> | maximize-bandwidth-usage}`	Sets the maximum bandwidth allowed for outgoing traffic or enables maximize bandwidth usage to let the traffic matching this policy "borrow" any unused bandwidth on the out-going interface. The no command resets the outbound maximum bandwidth to the default (0).
`[no] outbound guarantee-bandwidth <0..1048576> priority <1..7>`	Sets how much outbound bandwidth, in kilobits per second, this policy allows the traffic to use and also sets a number between 1 and 7 to set the priority for traffic that matches this policy. The smaller the number, the higher the priority. Outbound refers to the traffic the UAG sends out from a connection's initiator. The no command resets the outbound guarantee bandwidth to the default (0).

Table 166 bwm Sub-commands (continued)

COMMAND	DESCRIPTION
`[no] outbound-dscp-mark {<0..63> | class {af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs0 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | default | wmm_be0 | wmm_be24 | wmm_bk16 | wmm_bk8 | wmm_vi32 | wmm_vi40 | wmm_vo48 | wmm_vo56}}`	Sets the DSCP value to apply to the outgoing packets that match this policy. `default`: to have the Zyxel Device set the DSCP value of the packets to 0. The no command resets the outgoing DSCP code to the default (`preserve`) and have the Zyxel Device keep the packets' original DSCP value.
`[no] outgoing-interface {interface` *`interface_name`* `| trunk` *`group_name`*`}`	Sets the destination interface of the traffic to which this policy applies. *`interface_name`*: The name of the interface. This depends on the Zyxel Device model. See Table 52 on page 118 for detailed information about the interface name. *`group_name`*: A descriptive name for the trunk. The name cannot start with a number. This value is case-sensitive. The no command resets the outgoing interface to the default (`any`).
`[no] schedule` *`schedule_object`*	Specifies a schedule that defines when the policy applies. The no command resets the schedule to the default (`none`) to make the policy always effective.
`[no] service application-group` *`app_name`*	Specifies an Application Patrol service to identify the type pf traffic to which this policy applies. The no command resets the acation to the default (`any`).
`[no] service service-object {`*`service_name`*` | any}`	Specifies a service or service group to identify the type of traffic to which this policy applies. `any`: the policy is effective for every service. The no command resets the service to the default (`any`).
`show`	Displays the policy settings.
`[no] source` *`address_object`*	Sets the source IP address or address group for whom this policy applies. The no command resets the source IP address(es) to the default (`any`). `any` means all IP addresses.
`[no] type {per-user | shared | per-ip-source}`	Sets the type of bandwidth management. `per-user`: to allow every user that matches this policy to use up to the bandwidth configured in this policy. `shared`: to have users that match this policy to share the bandwidth configured in this policy. `per-ip-source`: tset the maximum bandwidth for traffic from an individual source IP address. The no command resets the bandwidth management type to the default (`shared`).
`[no] user` *`user_name`*	Sets a user name or user group to which to apply the policy. The `no` command resets the user name to the default (`any`). `any` means all users.

Table 166 bwm Sub-commands (continued)

COMMAND	DESCRIPTION
`priority-code <0..7>`	Priority code is applied to outgoing traffic. The BWM policy priority code setting overwrites the VLAN priority code setting. Sets the priority code for the specified VLAN from 0 (lowest, background traffic) to 7 (highest, network control traffic). This is the priority code for packets in the specified VLAN that don't match the BWM rule.
`vlan-priority-code <0..7>`	Sets the priority code for matching outgoing traffic in the specfied VLAN.
`marked-interface interface vlan<1..4064>`	When a packet matches BWM criteria, choose the VLAN interface(s) to which to apply the priority code using a `marked-interface` command. Marks matching outgoing traffic from the specfied VLAN with the configured priority code.
`marked-interface any`	Marks matching outgoing traffic from any VLAN with the configured priority code.
`marked-interface trunk` *`trunk_name`*	Marks matching outgoing traffic from the specfied trunk with the configured priority code.
`marked-interface none`	Doesn't mark outgoing traffic with priority code for this BWM rule.

36.3 Bandwidth Management Commands Examples

The following example sets the priority code to 3 for packets in VLAN 1 that don't match any other BWM rule. BWM rule 1 marks matching outgoing traffic from VLAN 1 to priority code 4.

```
Router(config)# interface vlan1
Router(config-if-vlan)# priority-code 3
Router(config-if-vlan)# exit
Router(config)# bwm 1
Router(config-bwm modify 1)# vlan-priority-code 4
Router(config-bwm modify 1)# marked-interface interface vlan1
Router(config-bwm modify 1)# exit
Router(config)#
```

The following example adds a new bandwidth management policy for trial-users to limit incoming and outgoing bandwidth and sets the traffic priority to 3. It then displays the policy settings.

```
Router# configure terminal
Router(config)# bwm append
Router(config-bwm append 6)# activate
Router(config-bwm append 6)# description example
Router(config-bwm append 6)# user trial-users
Router(config-bwm append 6)# inbound guarantee-bandwidth 800 priority 3
Router(config-bwm append 6)# outbound guarantee-bandwidth 700 priority 3
Router(config-bwm append 6)# show
Current Configuration:
index: 6
   Activate: yes
   Description: example
   BWM Type: shared
   Schedule: none
   User: trial-users
   Incoming_Type: any
   Incoming_Interface: any
   Outgoing_Type: any
   Outgoing_Interface: any
   Src: any
   Dst: any
   Service_Type: service-object
   Service_Name: any
   Inbound_Excess: no
   Inbound_Prio: 3
   Inbound: 800
   Inbound_Ceiling: 0
   Outbound_Excess: no
   Outbound_Prio: 3
   Outbound: 700
   Outbound_Ceiling: 0
   DSCP_Code: any
   DSCP_Inbound: preserve
   DSCP_Outbound: preserve
   Log: no
Router(config-bwm append 6)# exit
Router(config)#
```

CHAPTER 37
Application Patrol

37.1 Application Patrol Overview

Application patrol provides a convenient way to manage the use of various applications on the network. It manages general protocols (for example, http and ftp) and instant messenger (IM), peer-to-peer (P2P), Voice over IP (VoIP), and streaming (RSTP) applications. You can even control the use of a particular application's individual features (like text messaging, voice, video conferencing, and file transfers). Application patrol also has powerful bandwidth management including traffic prioritization to enhance the performance of delay-sensitive applications like voice and video.

Note: The Zyxel Device checks firewall rules before application patrol rules for traffic going through the Zyxel Device. To use a service, make sure both the firewall and application patrol allow the service's packets to go through the Zyxel Device.

Application patrol examines every TCP and UDP connection passing through the Zyxel Device and identifies what application is using the connection. Then, you can specify, by application, whether or not the Zyxel Device continues to route the connection.

37.2 Application Patrol Commands Summary

The following table describes the values required for many application patrol commands. Other values are discussed with the corresponding commands.

Table 167 Input Values for Application Patrol Commands

LABEL	DESCRIPTION
<profile-name>	Type the name of the profile. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
description	This is a description of the App Patrol Profile.

The following sections list the application patrol commands.

37.2.1 Application Patrol Commands

This table lists the application patrol commands.

Table 168 app Commands: Application Patrol

COMMAND	DESCRIPTION
`[no] app <profile-name>`	Creates a profile with the specified name. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. The no command disables it.
`[no] description DESCRIPTION`	Write a description of the App Patrol Profile.

Table 168 app Commands: Application Patrol

COMMAND	DESCRIPTION
application <*profile-name*> action {forward|drop|reject} {no log|log [alert]}	Sets the action and generates a log, log and alert or neither (no) when traffic matches a signature in this profile. Actions are: • forward - routes packets that matches these signatures. • Drop - silently drops packets that matches these signatures without notification. • Reject - drops packets that matches these signatures and sends notification.
[no] app log_sid	Generate a log when traffic matches a signature in this category. The no command disables it.
app reload signatures	Re-downloads signatures from the update server.
app rename <*profile-name*> <*profile-name*>	Renames an existing profile
[no] app statistics collect	Enables application patrol statistics gathering. The no command disables it.
app statistics flush	Clears all application patrol statistics.
app update	Immediately downloads signatures from an update server.
[no] app update auto	Enables (disables) automatic signature downloads at regular times and days.
app update daily <0..23>	Enables automatic signature download every day at the time specified.
app update hourly	Enables automatic signature download every hour.
app update weekly {sun | mon | tue | wed | thu | fri | sat} <0..23>	Enables automatic signature download once-a-week at the time and day specified.
no application-object <*profile-name*>	Removes the application object from the named profile.
[no] security-service app-patrol activate	Turns on application patrol on the Zyxel Device. The no command disables application patrol.
show app category <*category_id*>	Shows tag IDs for a specific category.
show app profiles	Shows the description, application name, and object reference number for all application patrol profiles on the Zyxel Device.
show app profiles <*profile-name*>	Shows the description, application name, and object reference number associated with the named profile.
show app profiles <*profile-name*> application	Shows the application name, action and log associated with the named profile.
show app profiles <*profile-name*> application category {*category_id* | all}	Shows the description, application name, and object reference number associated with the named profile within a specific or all categories.
show app search-name <*application_keyword*>	Searches for applications that contain the specified keyword.
show app signature update	Displays signature update schedule.
show app signatures date	Displays the date (yyyy-mm-dd) and time the set was released.
show app signatures status	Displays details about the current application patrol signature set.
show app signatures version	Displays the App Patrol signature set version number. This number gets larger as the set is enhanced.
show app statistics collect	Shows if application patrol statistics gathering is enabled and if yes, when.
show app statistics summary	Shows a summary of application patrol statistics (if any).

Table 168 app Commands: Application Patrol

COMMAND	DESCRIPTION
`show app tag info`	Displays the ID and name of tags for applications.
`show app update status`	Displays signature update status.
`show security-service signature status`	Displays details about all current signature sets.
`show security-service status`	Displays whether the security services are enabled on the Zyxel Device.

37.2.1.1 Application Patrol Command Examples

This command shows details of an application patrol profile created.

```
Router# show app profiles
APP-patrol: 1
  profile name: app1
  description:
  application: ultrasurf_app
  ref: 1
```

These are some other example application patrol usage commands

```
Router(config)# show app statistics collect
collect statistics: yes
collect statistics time: since 2014-06-03 05:39:59 to 2014-06-10 06:20:17
Router(config)# show app signatures version
version: 3.1.4.049
Router(config)# show app signatures date
date: 2013-12-05 18:09:51
Router(config)# app john
Router(config-app-patrol-profile-john)# description this is a dummy
profile
Router(config-app-patrol-profile-john)# exit
Router(config)# show app profiles
APP-patrol: 1
  profile name: testfb
  description:
  application: tests
  ref: 0
APP-patrol: 2
  profile name: test
  description: this is a test
  application:
  ref: 0
APP-patrol: 3
  profile name: john
  description: this is a dummy profile
  application:
  ref: 0
Router(config)#
```

CHAPTER 38
Anti-Virus

38.1 Anti-Virus Overview

This chapter introduces and shows you how to configure the anti-virus scanner.

Note: This feature is called Anti-Malware on some Zyxel Device models.

A computer virus is a small program designed to corrupt and/or alter the operation of other legitimate programs. A worm is a self-replicating virus that resides in active memory and duplicates itself. The effect of a virus attack varies from doing so little damage that you are unaware your computer is infected to wiping out the entire contents of a hard drive to rendering your computer inoperable.

38.2 Anti-Virus Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 169 Input Values for General Anti-Virus Commands

LABEL	DESCRIPTION
<profile-name>	The name of the profile. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
av_file_pattern	Use up to 80 characters to specify a file pattern. Alphanumeric characters, underscores (_), dashes (-), question marks (?) and asterisks (*) are allowed. A question mark (?) lets a single character in the file name vary. For example, use “a?.zip” (without the quotation marks) to specify aa.zip, ab.zip and so on. Wildcards (*) let multiple files match the pattern. For example, use “*a.zip” (without the quotation marks) to specify any file that ends with “a.zip”. A file named “testa.zip” would match. There could be any number (of any type) of characters in front of the “a.zip” at the end and the file name would still match. A file named “test.zipa” for example would not match. A * in the middle of a pattern has the Zyxel Device check the beginning and end of the file name and ignore the middle. For example, with “abc*.zip”, any file starting with “abc” and ending in “.zip” matches, no matter how many characters are in between. The whole file name has to match if you do not use a question mark or asterisk. If you do not use a wildcard, the Zyxel Device checks up to the first 80 characters of a file name.

38.2.1 General Anti-Virus Commands

The following table describes general anti-virus commands. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Note: You must register for the anti-virus service in order to use it (see Chapter 5 on page 53).

Table 170 General Anti-Virus Commands

COMMAND	DESCRIPTION
`[no] anti-virus activate`	Enables the anti-virus service. The Anti-Virus service depends on anti-virus service registration.
`show anti-virus eicar activation`	Displays anti-virus eicar status.
`[no] anti-virus cloud-query activate`	Enables the cloud-query service. The no command disables the cloud-query service.
`show anti-virus cloud-query status`	`Displays the status of anti-virus cloud-query.` Note: This command was removed in firmware version 4.5.0
`[no] anti-virus eicar activate`	Turns detection of the EICAR test file on or off.
`anti-virus scan mode {express | hybrid | stream}`	Sets the anti-virus scan mode. • Express: The Zyxel Device scans files that match the list of user-defined file types using cloud query. This is the fastest scan mode. • Hybrid: The Zyxel Device scans files that match the list of user-defined file types using cloud query, anti-malware signatures, and Threat Intelligence Machine Learning (if supported). This mode offers a balance of speed and security. • Stream: The Zyxel Device scans all files using anti-malware signatures and Threat Intelligence Machine Learning (if supported). This is the deepest scan mode. Note: Some device models do not support hybrid mode.
`show anti-virus scan mode status`	Displays the current anti-virus scan mode.
`[no] anti-virus cloud-query ftype-identify file_type`	Adds or removes a file type from the list of user-defined file types that cloud query will scan. Allowed values: 7z, AVI, BMP, BZ2, EXE, Flash, GIF, Gz, JPG, MOV, MP3, MPG, “MS Office”, PNG, RAR, RM, TIFF, WAV, ZIP.
`show anti-virus cloud-query ftype-identify status`	Displays the list of user-defined file types that cloud query will scan.
`anti-virus reload signatures`	Recovers anti-virus signatures. You only need to do this if instructed by a support technician.
`[no] anti-virus skip-unknown-file-type activate`	Sets whether or not anti-virus checks unknown file types.
`show anti-virus skip-unknown-file-type activation`	Displays whether or not anti-virus checks unknown file types.
`anti-virus mail-infect-ext activate`	Has the Zyxel Device add a notification text file to an e-mail after modifying a virus-infected e-mail attachment.
`no anti-virus mail-infect-ext activate`	Has the Zyxel Device not add a notification text file to an e-mail after identifying an infected file.
`[no] security-service anti-virus activate`	Turns on anti-virus on the Zyxel Device. The no command disables anti-virus.

Table 170 General Anti-Virus Commands (continued)

COMMAND	DESCRIPTION
`security-service anti-virus inspect {all-traffic | by-policy}`	Sets how the security service inspects traffic. *all-traffic*: The security service inspects all traffic passing through the Zyxel Device. *by-policy*: The security service inspects traffic only when its profile is bound to a security policy. For information on binding a security service profile to a security policy, see Section 29.2.1 on page 221. Note: This command is only available when secure-policy-style is set to advanced. For details, see Section 29.2.2 on page 223.
`show security-service status`	Displays whether the security services are enabled on the Zyxel Device.

38.2.2 Anti-Virus Profile

On Zyxel Devices that do not support multiple profiles, edit the profile named default_profile to change settings in the Web Configurator UI.

Table 171 Anti-Virus Profile Commands

COMMAND	DESCRIPTION
`anti-virus rename old_profile_name new_profile_name`	Renames the AV profile.
`anti-virus profile_name`	Enters the anti-virus sub-command mode to edit the specified anti-virus profile.
`[no] bypass {white-list | black-list}`	When enabled, files are not checked against the white-list and/or black-list.
`description profile_description`	Adds a description to the profile.
`[no] file-decompression [unsupported destroy]`	Enable file decompression to have the Zyxel Device attempt to decompress zipped files for further scanning. `unsupported destroy:` Have the Zyxel Device "destroy" (overwrite the infected portion of the file with zeros before forwarding to the user) zipped files it cannot decompress due to encryption or system resource limitations. Note: The Zyxel Device cannot decompress compressed files within a compressed file.
`[no] infected-action {destroy | send-win-msg}`	Sets the action to take when the Zyxel Device detects a virus in a file. The file can be "destroyed" (overwrite a portion of the file with zeros before forwarding to the user). The Zyxel Device can also send a message alert to the user using a Microsoft Windows computer connected to the to interface.
`[no] log [alert]`	Set whether the Zyxel Device should create a log message and an optional alert if it finds a virus in a file.
`[no] scan {http | ftp | imap4 | smtp | pop3}`	Sets the traffic protocols you want to scan for viruses.
`show [all]`	Displays the details of the anti-virus rule you are configuring or all the rules.
`exit`	Leaves the sub-command mode.

Table 171 Anti-Virus Profile Commands

COMMAND	DESCRIPTION
`show anti-virus profile [profile_name]`	Displays details of the named profile.
`show anti-virus profile`	Displays all anti-virus profiles.

38.2.2.1 Anti-Virus Profile Command Example

This is an example of anti-virus profile commands.

```
Router(config)# anti-virus office1
Router(config-av-profile-office1)# infected-action destroy
Router(config-av-profile-office1)# file-decompression
Router(config-av-profile-office1)# no file-decompression unsupported
destroy
Router(config-av-profile-office1)# exit
Router(config)# show an
anti-spam    anti-virus
Router(config)# show anti-virus profile office1
Anti-Virus Rule: 3
  name: office1
  description:
  log: log
  file decompression: yes
  destroy unsupported compressed file: no
  destroy infected compressed file: yes
  reference count: 0
```

38.2.3 White and Black Lists

The following table describes the commands for configuring the white list and black list. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 172 Commands for the Anti-Virus Black List

COMMAND	DESCRIPTION
`[no] anti-virus black-list activate`	Activates or deactivates the black list. When activated, the Zyxel Device logs and deletes files with names that match any of the black list file patterns.
`show anti-virus black-list status`	Displays whether the black list is currently activated or deactivated.
`show anti-virus black-list`	Displays a list of patterns in the black list. The list also displays each pattern's index number, and whether the pattern is currently activated.
`anti-virus black-list {md5-hash` *`md5-pattern`* `| sha256-hash` *`sha256-pattern`* `| file-pattern` *`file-pattern`*`} {activate|deactivate}`	Adds an MD5 hash pattern, SHA-256 hash pattern or file pattern to the black list if it did not already exist, and then activates or deactivates the pattern.

Table 172 Commands for the Anti-Virus Black List (continued)

COMMAND	DESCRIPTION
`no anti-virus black-list {md5-hash *md5-pattern* | sha256-hash *sha256-pattern* | file-pattern *file-pattern*}`	Removes an MD5 hash pattern, SHA-256 hash pattern or file pattern from the black list.
`anti-virus black-list {replace <1..256> | file-pattern *file-pattern* md5-hash *md5-pattern* | sha256-hash *sha256-pattern*}`	Replaces the black list pattern that has the specified index number with a new pattern. The new pattern can be a file pattern, an MD5 or a SHA-256 hash pattern. `<1..256>`: The index number of the file pattern, MD5 or SHA-256 hash pattern that you want to replace. *file-pattern*: The new file pattern. *md5-pattern*: The new MD5 hash pattern. *sha256-pattern*: The new SHA-256 hash pattern.

Table 173 Commands for the Anti-Virus White List

COMMAND	DESCRIPTION
`[no] anti-virus white-list activate`	Activates or deactivates the white list. When activated, the Zyxel Device does not perform anti-virus checks on files that match any of the white list file patterns.
`show anti-virus white-list status`	Displays whether the white list is currently activated or deactivated.
`show anti-virus white-list`	Displays a list of patterns in the white list. The list also displays each pattern's index number, and whether the pattern is currently activated.
`anti-virus white-list {md5-hash *md5-pattern* | sha256-hash *sha256-pattern* | file-pattern *file-pattern*} {activate|deactivate}`	Adds an MD5 hash pattern, SHA-256 hash pattern or file pattern to the white list if it did not already exist, and then activates or deactivates the pattern.
`no anti-virus white-list {md5-hash *md5-pattern* | sha256-hash *sha256-pattern* | file-pattern *file-pattern*}`	Removes an MD5 hash pattern, SHA-256 hash pattern or file pattern from the white list.
`anti-virus white-list {replace <1..256> | file-pattern *file-pattern* md5-hash *md5-pattern* | sha256-hash *sha256-pattern*}`	Replaces the white list pattern that has the specified index number with a new pattern. The new pattern can be a file pattern, an MD5 or a SHA-256 hash pattern. `<1..256>`: The index number of the file pattern, MD5 or SHA-256 hash pattern that you want to replace. *file-pattern*: The new file pattern. *md5-pattern*: The new MD5 hash pattern. *sha256-pattern*: The new SHA-256 hash pattern.

38.2.3.1 White and Black Lists Example

This example shows how to enable the white list and configure an active white list entry for files with a .exe extension. It also enables the black list and configures an inactive black list entry for files with a .exe extension.

```
Router(config)# anti-virus white-list activate
Router(config)# anti-virus white-list file-pattern
Router(config)# anti-virus white-list file-pattern *.exe activate
Router(config)# anti-virus black-list activate
Router(config)# anti-virus black-list file-pattern *.exe deactivate
Router(config)# show anti-virus white-list status
anti-virus white-list status: yes
Router(config)# show anti-virus white-list
No.  Status
File-Pattern
================================================================================
1    yes
*.exe
Router(config)# show anti-virus black-list status
anti-virus black-list status: yes
Router(config)# show anti-virus black-list
No.  Status
File-Pattern
================================================================================
1    no
*.exe
```

38.2.4 Signature Search Anti-Virus Command

The following table describes the command for searching for signatures. You must use the `configure terminal` command to enter the configuration mode before you can use this command.

Table 174 Command for Anti-Virus Signature Search

COMMAND	DESCRIPTION
`show anti-virus search signature {all | name virus_name} [{from id to id}]`	Searches for signatures by name.Type the ID or part of the ID that you want to find.

38.2.4.1 Signature Search Example

This example shows how to search for anti-virus signatures with MSN in the name.

```
Router(config)# anti-virus search signature name MSN
signature: 1
  virus name: MSN
```

38.3 Update Anti-Virus Signatures

Use these commands to update new signatures. You should be registered for anti-virus service to use these.

Table 175 Update Signatures

COMMAND	DESCRIPTION
`[no] anti-virus update auto`	Enables (disables) automatic signature downloads at regular times and days.
`anti-virus update ctdb`	Immediately downloads the Cloud Threat Database signature from an update server.
`anti-virus update daily <0..23>`	Enables automatic signature download every day at the time specified.
`anti-virus update hourly`	Enables automatic signature download every hour.
`anti-virus update signatures`	Immediately downloads the anti-virus signatures from an update server.
`anti-virus update weekly {sun | mon | tue | wed | thu | fri | sat} <0..23>`	Enables automatic signature download once-a-week at the time and day specified.
`show anti-virus update`	Displays the signature update schedule.
`show anti-virus update status`	Displays the signature update status.
`show anti-virus signatures status`	Displays details about the current anti-virus signature set.
`show security-service signature status`	Displays details about all current signature sets.

38.3.1 Update Signature Examples

These examples show how to enable/disable automatic anti-virus downloading, schedule updates, display the schedule, display the update status, show the (new) updated signature version number, show the total number of signatures and show the date/time the signatures were created.

```
Router# configure terminal
Router(config)# anti-virus update signatures
ANTI-VIRUS signature update in progress.
Please check system log for future information.
Router(config)# anti-virus update auto
Router(config)# no anti-virus update auto
Router(config)# anti-virus update hourly
Router(config)# anti-virus update daily 10
Router(config)# anti-virus update weekly fri 13
Router(config)# show anti-virus update
auto: yes
schedule: weekly at Friday 13 o'clock
Router(config)# show anti-virus update status
current status: Anti-Virus Current signature version 1.046 on device is
latest at Tue Apr 17 10:18:00 2007
last update time: 2007/04/07 10:41:01
Router(config)# show anti-virus signatures status
current version : 1.046
release date    : 2007/04/06 10:41:29
signature number: 686000
SSII (signature) number: 6000
SSII(md5 checksum) number: 680000
```

38.4 Anti-Virus Statistics

The following table describes the commands for collecting and displaying anti-virus statistics. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 176 Commands for Anti-Virus Statistics

COMMAND	DESCRIPTION
`[no] anti-virus statistics collect`	Turns the collection of anti-virus statistics on or off.
`anti-virus statistics flush`	Clears the collected statistics.
`show anti-virus statistics summary`	Displays the collected statistics.
`show anti-virus statistics collect`	Displays whether the collection of anti-virus statistics is turned on or off.
`show anti-virus statistics ranking {destination | destination6 | source | source6 | virus-name}`	Queries and sorts anti-virus statistics entries by destination IP address, source IP address, or virus name. `virus-name`: lists the most common viruses detected. `source(6)`: lists the source IP addresses (IPv4 or IPv6) having the most number virus-infected files. `destination(6)`: lists the most common destination IP addresses (IPv4 or IPv6) for virus-infected files.

38.4.1 Anti-Virus Statistics Example

This example shows how to collect and display anti-virus statistics. It also shows how to sort the display by the most common destination IP addresses.

```
Router(config)# anti-virus statistics collect
Router(config)# show anti-virus statistics collect
collect statistics: yes
Router(config)# show anti-virus statistics summary
virus detected: 0
Router(config)# show anti-virus statistics ranking destination
Router(config)# show anti-virus statistics ranking virus-name
ranking: 1
  virus name: Malicious Virus
  hash-type: sha256
  hash: 275A021BBFB6489E54D471899F7DB9D1663FC695EC2FE2A2C4538AABF651FD0F
  occurrence: 2
```

CHAPTER 39
RTLS

39.1 RTLS Overview

Ekahau RTLS (Real Time Location Service) tracks battery-powered Wi-Fi tags attached to APs managed by the Zyxel Device to create maps, alerts, and reports.

The Ekahau RTLS Controller is the centerpiece of the RTLS system. This server software runs on a Windows computer to track and locate Ekahau tags from Wi-Fi signal strength measurements. Use the Zyxel Device with the Ekahau RTLS system to take signal strength measurements at the APs (Integrated Approach / Blink Mode).

You need:

- At least three APs managed by the Zyxel Device (the more APs the better since it increases the amount of information the Ekahau RTLS Controller has for calculating the location of the tags)
- IP addresses for the Ekahau Wi-Fi tags
- A dedicated RTLS SSID is recommended
- Ekahau RTLS Controller in blink mode with TZSP Updater enabled
- Secure policies to allow RTLS traffic if the Zyxel Device Secure Policy control is enabled or the Ekahau RTLS Controller is behind a firewall.

For example, if the Ekahau RTLS Controller is behind a firewall, open ports 8550, 8553, and 8569 to allow traffic the APs send to reach the Ekahau RTLS Controller.

The following table lists default port numbers and types of packets RTLS uses.

Table 177 RTLS Traffic Port Numbers

PORT NUMBER	TYPE	DESCRIPTION
8548	TCP	Ekahau T201 location update.
8549	UDP	Ekahau T201 location update.
8550	TCP	Ekahau T201 tag maintenance protocol and Ekahau RTLS Controller user interface.
8552	UDP	Ekahau Location Protocol
8553	UDP	Ekahau Maintenance Protocol
8554	UDP	Ekahau T301 firmware update.
8560	TCP	Ekahau Vision web interface
8562	UDP	Ekahau T301W firmware update.
8569	UDP	Ekahau TZSP Listener Port

39.1.1 RTLS Configuration Commands

Use these commands to configure RTLS on the Zyxel Device.

Table 178 RTLS Commands

COMMAND	DESCRIPTION
`[no] rtls ekahau activate`	Enables RTLS to use Wi-Fi to track the location of Ekahau Wi-Fi tags. The no command disables tracking.
`rtls ekahau ip address <ip>`	Specifies the IP address of the Ekahau RTLS Controller.
`rtls ekahau ip port <1..65535>`	Specifies the server port of the Ekahau RTLS Controller.
`show rtls ekahau config`	Displays RTLS configuration details.
`show rtls ekahau cli`	Displays commands run on the AP. The AP runs the flush command before executing other commands.

39.1.2 RTLS Configuration Examples

The following commands show how to enable RTLS to use Wi-Fi to track the location of Ekahau Wi-Fi tags, specify the IP address of the Ekahau RTLS Controller and then show the configuration settings.

```
Router# configure terminal
Router(config)# rtls ekahau activate
Router(config)# rtls ekahau ip address 1.1.1.1
Router(config)# exit
Router# show rtls ekahau config
ekahau activate: yes
ekahau address: 1.1.1.1
ekahau port: 8569
Router#
```

The following command displays the commands run on the AP.

```
Router(config)# show rtls ekahau cli
!
rtls ekahau flush
!
rtls ekahau ip port 11111
rtls ekahau ip address 1.1.1.1
rtls ekahau activate
!
Router(config)#
```

CHAPTER 40
Reputation Filter

40.1 Overview

IP Reputation

IP reputation checks the reputation of an IP address from a database. An IP address with bad reputation associates with suspicious activities, such as spam, virus, and/or phishing. The Zyxel Device will respond when there are packets coming from an IPv4 address with bad reputation.

URL Threat Filter

URL filtering compares access to specific URLs against a database of blocked or allowed sites. Sites on the database are sorted into categories such as:

Anonymizers	Browser Exploits
Malicious Downloads	Malicious Sites
Phishing	Spam URLs
Spyware Adware Keyloggers	

Note: This feature was previously called Anti-Botnet Filter.

DNS Threat Filter

DNS threat filtering inspects DNS queries made by clients on your network and compares the queries against a database of blocked or allowed Fully Qualified Domain Names (FQDNs). The Zyxel Device DNS Threat Filter will either drop the DNS query or reply to the user with a fake DNS response.

The following types of DNS queries are inspected by the Zyxel Device:
- Type "A" ...
- Type "AAAA" ...
- Type "NS" ...
- Type "MX" ...
- Type "CNAME" ...
- Type "PTR" ...
- Type "SOA" ...

The Zyxel Device replies with a DNS reply packet containing a fake IP address for type "A", and replies with a DNS reply packet with server failure code for remaining types.

40.1.1 Signature Database Priority

The Zyxel Device checks the URL Threat Filter signature databases in the following order:

1. White List
2. Black List
3. External Black List
4. Local Signature Database
5. Cloud Query Cache
6. Cloud Query

The Zyxel Device checks the DNS Threat Filter signature databases in the following order:

1. White List
2. Black List
3. Local Signature Database
4. Cloud Query Cache
5. Cloud Query

40.2 IP Reputation Commands

The following table describes general IP reputation commands. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 179 IP Reputation Commands

COMMAND	DESCRIPTION
`[no] security-service ip-reputation activate`	Enables the IP reputation filtering service on the Zyxel Device. The no command disables the IP reputation filtering service.
`show security-service status`	Displays whether security services such as IP reputation filtering are enabled on the Zyxel Device.
`ip-reputation action {block | pass}`	Sets what action the Zyxel Device takes when a packet arrives from an IPv4 address with a bad reputation. `pass`: The Zyxel Device allows the packet to go through. `block`: The Zyxel Device denies the packet, and then sends a TCP RST to both the packet sender and receiver.
`ip-reputation action-level {high | medium | low}`	Sets the threshold threat level to which the Zyxel Device will take action (high, medium, and low). The threat level is determined by the IP reputation engine. which grades IPv4 addresses. • high: An IPv4 address that scores 0 to 20 points. • medium: An IPv4 address that scores 0-60 points. • low: An IPv4 address that scores 0-80 points.
`[no] ip-reputation log [alert]`	The Zyxel Device creates a log message and sends an optional alert when packets arrive from an IPv4 address with a bad reputation.
`[no] ip-reputation log-all`	The Zyxel Device creates a log message each time an IPv4 address is scanned using IP reputation.
`[no] ip-reputation system-protect activate`	Enables IP reputation system-protect to scan the IPv4 address reputation of the packets that are destined for or sent out by the Zyxel Device.
`show ip-reputation status`	Displays the action and log settings for IP reputation.

Table 179 IP Reputation Commands (continued)

COMMAND	DESCRIPTION
`show ip-reputation signatures date`	Displays the date and time the signature set was released.
`show ip-reputation signatures number`	Displays the number of signatures in this set.
`show ip-reputation signatures version`	Displays the signature set version number currently used by the Zyxel Device. This number gets larger as new signatures are added.
`[no] ip-reputation white-list activate`	Turns on the IP reputation white list, and the Zyxel Device will allow the incoming packets that come from the listed IPv4 addresses.
`ip-reputation white-list` *{IPv4|IPv4CIDR}* `{activate|deactivate}`	Activates or deactivates the specified IPv4 address on the IP reputation white list. You can also add an IP address block using CIDR notation, for example 192.168.0.1/24.
`ip-reputation white-list replace <1..256>` *IPv4* `{activate|deactivate}`	Replaces the IPv4 address of the specified entry with a new one on the IP reputation white list.
`no ip-reputation white-list` *IPv4*	Removed the specified IPv4 address from the IP reputation white list.
`[no] ip-reputation black-list activate`	Turns on the IP reputation black list, and the Zyxel Device will block the incoming packets that come from the listed IPv4 addresses.
`ip-reputation black-list` *{IPv4|IPv4CIDR}* `{activate|deactivate}`	Activates or deactivates the specified IPv4 address on the IP reputation black list. You can also add an IP address block using CIDR notation, for example 192.168.0.1/24.
`ip-reputation black-list replace <1..256>` *IPv4* `{activate|deactivate}`	Replaces the IPv4 address of the specified entry with a new one on the IP reputation black list.
`no ip-reputation black-list` *IPv4*	Removed the specified IPv4 address from the IP reputation black list.
`show ip-reputation {white-list|black-list}`	Displays the current IP reputation white or black list.
`show ip-reputation {white-list|black-list} status`	Displays if the IP reputation white or black list is turned on or not.
`[no] ip-reputation webroot incoming-category {botnets | denial-of-service | exploits | phishing | proxy | reputation | scanners | spam-sources | tor-proxy | web-attacks}`	Select the categories of packets coming from the Internet that the Zyxel Device applies IP reputation filtering to.
`[no] ip-reputation webroot outgoing-category {botnets | phishing}`	Select the categories of packets coming from the Internet or local networks that the Zyxel Device applies IP reputation filtering to. Note: In Firmware v4.55 or later, the phishing option does nothing and is only included for compatibility.
`show ip-reputation webroot {incoming-category | outgoing-category}`	Displays whether each category of packet coming from the Internet or Internet and local networks is filtered.

40.2.1 Update IP Reputation Signatures

Use these commands to update new signatures. You should have already registered for IP reputation service.

Table 180 Update Signatures

COMMAND	DESCRIPTION
`ip-reputation update signatures`	Immediately downloads signatures from an update server.
`[no] ip-reputation update auto`	Enables (disables) automatic signature downloads at regular times and days.
`ip-reputation update daily <0..23>`	Enables automatic signature download every day at the time specified.
`ip-reputation update hourly`	Enables automatic signature download every hour.
`ip-reputation update weekly {sun | mon | tue | wed | thu | fri | sat} <0..23>`	Enables automatic signature download once-a-week at the time and day specified.
`show ip-reputation signature update`	Displays signature update schedule.
`show ip-reputation update status`	Displays signature update status.
`show ip-reputation search {Ipv6Address | Ipv4Address}`	Searches for the specified IPv4 or IPv6 address in the Zyxel Device's internal and external IP reputation databases, and then displays the IP address's threat level.

40.2.2 IP Reputation Statistics

The following table describes the commands for collecting and displaying IP reputation statistics. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 181 Commands for IP Reputation Statistics

COMMAND	DESCRIPTION
`ip-reputation statistics flush`	Clears the collected IP reputation statistics.
`[no] ip-reputation statistics collect`	Turns the collection of IP reputation statistics on or off.
`show ip-reputation statistics recent-activities`	Displays a list of connection attempts to or from the IP reputation addresses.
`show ip-reputation statistics collect status`	Displays whether the collection of IP reputation statistics is turned on or off.
`show ip-reputation statistics summary`	Displays the collected IP reputation statistics.

40.2.3 IP Reputation External Black List

The following table describes the commands for enabling and configuring an external database of black listed IP addresses. The Zyxel Device blocks incoming and outgoing packets from the addresses in this

file.

- The external black list file must be in text format (*.txt) with each entry separated by a new line.
- The external black list file must be stored on a web server that supports HTTP or HTTPS, and that is reachable from the Zyxel Device.
- Each entry consists of a single IPv4/IPv6 IP address, a IPv4/IPv6 subnet in CIDR (Classless Inter-Domain Routing) format, or an IPv4/IPv6 IP address range. For example:
  104.244.79.43
  188.68.0.266/31
  1.1.1.1-1.1.1.3
  2001:b000:168::1
- The external black list file can contain a maximum of 50,000 entries.
- If the external black list file contains any invalid entries, the Zyxel Device will not use the file.

Table 182 Commands for IP Reputation Statistics

COMMAND	DESCRIPTION
`[no] ip-reputation ebl activate`	Enables or disables the IP Reputation external black list. When enabled, the Zyxel Device blocks incoming packets that come from the listed addresses in the black list file.
`ip-reputation ebl <profile name>`	Enters the subcommand mode for the specified external black list profile. If the profile does not exist, the Zyxel Device creates it. Note: After creating a new profile, you must add a source URL. Failure to do so might result in an error when starting the Zyxel Device.
description <*description*>	Enter a description of the external black list file. The description must consist of 1–60 characters, and may include letters, numbers, and the following special characters: ( )+/:=?!*#@$_%- Use the no command to delete the description for this profile.
source <*url*>	Adds the exact file name, path and IP address of the server containing the external black list file. For example, http://172.16.107.20/blacklist-files/myip-ebl.txt The server must be reachable from the Zyxel Device.
`no ip-reputation ebl <profile name>`	Deletes the specified external black list profile.
`ip-reputation ebl rename old_profile_name new_profile_name`	Renames the specified external black list profile.
`[no] ip-reputation ebl update auto`	Sets the Zyxel Device to automatically check for updates to the external black list at the time and day specified. You should select a time when your network is not busy for minimal interruption. The [no] command disables the automatic updates.
`ip-reputation ebl update hourly`	Sets the Zyxel Device to check for updates to the external black list every hour.

Table 182 Commands for IP Reputation Statistics (continued)

COMMAND	DESCRIPTION
`ip-reputation ebl update daily <0..23>`	Sets the Zyxel Device to check for updates to the external black list once per day, at the specified hour. For example, the time format is the 24 hour clock, so '23' means 11 PM.
`ip-reputation ebl update weekly {sun |mon|tue|wed|thu|fri|sat} <0..23>`	Sets the Zyxel Device to check for updates to the external black list once per week, on the specified day at the specified hour.
`ip-reputation ebl update`	Checks for updates to the external black list immediately.
`show ip-reputation ebl`	Shows all IP Reputation external black list profiles.
`show ip-reputation ebl <profile name>`	Shows the specified IP Reputation external black list profile.
`show ip-reputation ebl signature update`	Shows whether automatic external black list updates are enabled, and the schedule for the updates.
`show ip-reputation ebl <1..4> {date | number}`	Shows how many addresses are in the specified external black list profile, or the date that the external black list file was last updated. The profile is identified by its ID number, which can be viewed by running the command `show ip-reputation ebl`.

40.3 URL Threat Filter Commands

The following table describes general URL Threat Filter commands. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 183 URL Threat Filter Commands

COMMAND	DESCRIPTION
`anti-botnet action {forward | reject-both | reject-receiver | reject-sender}`	Sets what action the Zyxel Device takes when a packet contains a malicious URL. `forward`: The Zyxel Device allows the packet to go through. `reject-sender`: The Zyxel Device blocks the packet and sends a TCP RST to the sender. `reject-receiver`: The Zyxel Device denies the packet and sends a TCP RST to the receiver. `reject-both`: The Zyxel Device denies the packets and sends a TCP RST to both the sender and receiver.
`[no] anti-botnet log [alert]`	Creates a log on the Zyxel Device (and sends an optional alert) when the packet contains a malicious URL.
`[no] security-service anti-botnet-IP activate`	Enables the URL Threat Filter service on the Zyxel Device. The no command disables the service.
`[no] threat-website trust-list activate`	Enables or disables the URL Threat Filter whitelist.
`[no] threat-website forbid-list activate`	Enables or disables the URL Threat Filter black list.

Table 183 URL Threat Filter Commands (continued)

COMMAND	DESCRIPTION
`show anti-botnet signatures date`	Displays the date and time the signature set was released.
`show anti-botnet signatures number`	Displays the number of signatures in this set.
`show anti-botnet signatures version`	Displays the signature set version number currently used by the Zyxel Device. This number gets larger as new signatures are added.
`show anti-botnet status`	Displays the action and log settings for the URL Threat Filter service.
`show security-service status`	Displays whether security services such as anti-malware are enabled on the Zyxel Device.
`show threat-website status`	Displays the action, log, message and category settings for the URL Threat Filter service.
`show threat-website {trust|forbid}`	Displays the current URL Threat Filter white list (trust) or black list (forbid).
`[no] threat-website action {block | log | pass | warn}`	Sets what action the Zyxel Device takes when it detects a connection attempt to or from the web pages of the specified categories. `block`: The Zyxel Device blocks access to the web pages that match the categories that you specified. `log`: The Zyxel Device creates a log when it detects a connection attempt to or from the web pages of the specified categories. `warn`: The Zyxel Device displays a warning message to the access requesters for the web pages before allowing users to access web pages that match the categories that you specified. `pass`: The Zyxel Device allows access to the web pages that match the categories that you specified.
`[no] threat-website block message` *`message`*	Sets a message to be displayed when the URL Threat Filter blocks access to a web page. *`message`*: Use up to 127 characters (0-9a-zA-Z;/?:@&=+$\.-_!~*'()%,"). For example, "Access to this web page is not allowed. Please contact the network administrator".
`[no] threat-website block redirect` *`url`*	Sets the URL of the web page to which you want to send users when their web access is blocked by the URL Threat Filter. The web page you specify here opens in a new frame below the denied access message. *`url`*: Use "http://" or "https://" followed by up to 262 characters (0-9a-zA-Z;/?:@&=+$\.-_!~*'()%). For example, http://192.168.1.17/blocked access.
`[no] threat-website category {anonymizers | browser-exploits | botnets | compromised | malicious-downloads | malicious-sites | malware | phishing | phishing-fraud | spam-sites | spam-urls | spyware-adware-keyloggers}`	The Zyxel Device blocks the specified web page categories. The *no* command unblocks the specified category. For compatibility, legacy categories are still included as options and map to the following new categories: • `phishing-fraud -> phishing` • `spam-sites -> spam-urls` • `compromised, malware, botnets -> malicious-sites`
`threat-website {trust | forbid}`	Enters sub command mode, where you can add or remove web site entries in the white list (trust) or black list (forbid).

Table 183 URL Threat Filter Commands (continued)

COMMAND	DESCRIPTION
`[no] {ipv4 | ipv4_cidr | ipv4_range | wildcard_domainname | top_level_domain}`	*ipv4*: IPv4 address <W.X.Y.Z> *ipv4_cidr*: IPv4 subnet in CIDR format, i.e. 192.168.1.0/32<W.X.Y.Z>/<1..32> *ipv4_range*: Range of IPv4 addresses. <W.X.Y.Z>-<W.X.Y.Z> *wildcard_domainname*: Wildcard domain name, in the format *String1.String2*. For example: zyxel*.co* • String 1 must consist of 1–63 characters, and may include letters, numbers, and the following special characters: - (hyphen), . (period), * (wildcard character). • String 2 must consist of 1–63 characters, and may include letters, numbers, and the following special characters: - (hyphen), * (wildcard character). *top_level_domain*: Top level domain. for example: zyxel.com.
`exit`	Leaves the sub-command mode.
`security-service threat-website inspect {all-traffic | by-policy}`	Sets how the security service inspects traffic. *all-traffic*: The security service inspects all traffic passing through the Zyxel Device. *by-policy*: The security service inspects traffic only when its profile is bound to a security policy. For information on binding a security service profile to a security policy, see Section 29.2.1 on page 221.

40.3.1 URL Threat Filter Command Examples

Use these commands to block users in your network from accessing URLs that are categorized as browser exploits, malicious downloads, malicious sites, phishing or spam URLs. Use these commands if you also want to create a trusted list of URLs to make sure the Zyxel Device will allow incoming packets from these URLs even if they are categorized as URL threats.

The example uses the parameters given below.

Table 184 URL Threat Filter Example

ACTION	LOG	DENIED ACCESS MESSAGE	THREAT CATEGORIES	TRUST LIST
block	log-alert	Access to this website is not allowed.	• Browser Exploits • Malicious Downloads • Malicious Sites • Phishing • Spam URLs	• www.google.com • www.yahoo.com

1 Configure the URL threat filer settings as the parameters given above.

```
Router# configure terminal
Router(config)# security-service anti-botnet-url activate
Router(config)# threat-website action block
Router(config)# anti-botnet log alert
Router(config)# threat-website block message Access to this website is not allowed.
Router(config)# threat-website category browser-exploits
Router(config)# threat-website category malicious-downloads
Router(config)# threat-website category malicious-sites
Router(config)# threat-website category phishing
Router(config)# threat-website category spam-urls
```

2 Enable URL threat filter trust list.

```
Router(config)# threat-website trust-list activate
```

3 Enter the sub-command mode. Configure the URL threat filter trust list as the parameters given above.

```
Router(config)# threat-website trust
Router(Host)# www.google.com
Router(Host)# www.yahoo.com
```

4 Save the current configuration to the Zyxel Device.

```
Router(Host)# exit
Router(config)# write
```

40.3.2 URL Threat Filter Profile Commands

On Zyxel Devices that do not support multiple URL threat filter profiles, edit the profile named default_profile to change settings in the Web Configurator UI.

Table 185 URL Threat Filter Profile Commands

COMMAND	DESCRIPTION
`threat-website rename` *`old_profile_name new_profile_name`*	Renames the URL Threat Filter profile.
`threat-website profile` *`profile_name`*	Creates the specified URL Threat Filter profile, if it does not already exist.
`threat-website profile` *`<profile name>`* `action` *`{block | pass | warn}`*	Sets what action the Zyxel Device takes when it detects a connection attempt to or from the web pages of the specified categories. `block`: The Zyxel Device blocks access to the web pages that match the categories that you specified. `pass`: The Zyxel Device allows access to the web pages that match the categories that you specified. `warn`: The Zyxel Device displays a warning message to the person trying to access a website in the profile before allowing users to access web pages that match the categories that you specified.

Table 185 URL Threat Filter Profile Commands

COMMAND	DESCRIPTION
`[no] threat-website profile <profile name> description <description>`	Adds a description to the profile.
`[no] threat-website profile <profile name> {forbid | trust| ebl}`	Enables or disables the the black list (forbid), the whitelist (trust) and the external black list (ebl) for this profile.
`[no] threat-website profile <profile name> log`	Set whether the Zyxel Device should create a log message if it detects a hit.
`[no] threat-website profile <profile name> category {anonymizers | malware | botnets | phishing | browser-exploits | phishing-fraud | compromised | spam-sites | malicious-downloads | spam-urls | malicious-sites | spyware-adware-keyloggers}`	The profile blocks the specified web page categories. The *no* command unblocks the specified category. For compatibility, legacy categories are still included as options and map to the following new categories: • `phishing-fraud -> phishing` • `spam-sites -> spam-urls` • `compromised, malware, botnets -> malicious-sites`

40.3.3 URL Threat Filter External Black List

The following table describes the commands for enabling and configuring an external database of blacklisted URLs. The Zyxel Device blocks incoming and outgoing packets from the addresses in this file.

- The external black list file must be in text format (*.txt) with each entry separated by a new line.
- The external black list file must be stored on a web server that supports HTTP or HTTPS, and that is reachable from the Zyxel Device.
- Each entry consists of a URL, domain name, or domain name with wildcard *. For example:
  https://www.zyxel.com/products_services/smb.shtml?t=s
  www.zyxel.com
  .zyxel.
- The external black list file can contain a maximum of 50,000 entries.
- If the external black list file contains any invalid entries, the Zyxel Device will not use the file.

Table 186 Commands for URL Threat Filter External Black List

COMMAND	DESCRIPTION
`[no] threat-website ebl activate`	Enables or disables the URL Threat Filter external black list. When enabled, the Zyxel Device blocks incoming packets that come from the listed addresses in the black list file.
`threat-website ebl <profile name>`	Enters the subcommand mode for the specified external black list profile. If the profile does not exist, the Zyxel Device creates it. Note: After creating a new profile, you must add a source URL. Failure to do so might result in an error when starting the Zyxel Device.

Table 186 Commands for URL Threat Filter External Black List (continued)

COMMAND	DESCRIPTION
description <*description*>	Enter a description of the external black list file. The description must consist of 1–60 characters, and may include letters, numbers, and the following special characters: ( )+/:=?!*#@$_%- Use the no command to delete the description for this profile.
source <*url*>	Adds the URL of the external black list file. For example, https://zyxel.com.tw/blacklist-files/myip-ebl.txt. The server must be reachable from the Zyxel Device.
no threat-website ebl <*profile name*>	Deletes the specified external black list profile.
threat-website ebl rename *old_profile_name new_profile_name*	Renames the specified external black list profile.
[no] threat-website ebl update auto	Sets the Zyxel Device to automatically check for updates to the URL Threat Filter external black list at the time and day specified. You should select a time when your network is not busy for The [no] command disables the automatic updates.
threat-website ebl update hourly	Sets the Zyxel Device to automatically check for updates to the URL Threat Filter external black list once per day, at the specified hour.
threat-website ebl update daily <*0..23*>	Sets the Zyxel Device to update the URL Threat Filter external black list every day at the specified time. For example, the time format is the 24 hour clock, so '23' means 11 PM.
threat-website ebl update weekly *{sun |mon|tue|wed|thu|fri|sat}* <*0..23*>	Sets the Zyxel Device to automatically check for updates to the URL Threat Filter external black list file once per week, on the specified day at the specified hour.
threat-website ebl update	Checks for updates to the URL Threat Filter external black list file immediately.
show threat-website ebl	Shows all URL Threat Filter external black list profiles.
show threat-website ebl <*profile name*>	Shows the specified URL Threat Filter external black list profile.
show threat-website ebl signature update	Shows whether automatic external black list updates are enabled, and the schedule for the updates.
show threat-website ebl <*1..4*> *{date | number}*	Shows how many addresses are in the specified URL Threat Filter external black list profile, or the date that the external black list file was last updated. The profile is identified by its ID number, which can be viewed by running the command show threat-website ebl.
show threat-website search {*ipv6address | ipv4address*}	Searches for the specified IPv4 or IPv6 address in the internal and external URL Threat Filter databases, and then displays the IP address's threat level.

40.3.4 Update URL Threat Filter Signatures

Use these commands to update new signatures. You must have already registered for the URL Threat Filter service.

Table 187 Update Signatures

COMMAND	DESCRIPTION
`anti-botnet update signatures`	Immediately downloads signatures from an update server.
`[no] anti-botnet update auto`	Enables (disables) automatic signature downloads at regular times and days.
`anti-botnet update daily <0..23>`	Enables automatic signature download every day at the time specified.
`anti-botnet update hourly`	Enables automatic signature download every hour.
`anti-botnet update weekly {sun | mon | tue | wed | thu | fri | sat} <0..23>`	Enables automatic signature download once-a-week at the time and day specified.
`show anti-botnet signature update`	Displays signature update schedule.
`show anti-botnet update status`	Displays signature update status.
`show security-service signature status`	Displays details about all current signature sets.

40.3.5 Update Signature Examples

These examples show how to enable/disable automatic URL Threat Filter signature downloading, schedule updates, display the schedule, display the update status, show the (new) updated signature version number and show the date/time the signatures were created.

```
Router# configure terminal
Router(config)# anti-botnet update signatures
Anti-Botnet signature update in progress.
Please check system log for more information.
Router(config)# anti-botnet update auto
Router(config)# no anti-botnet update auto
Router(config)# anti-botnet update hourly
Router(config)# anti-botnet update daily 10
Router(config)# anti-botnet update weekly fri 13
Router(config)# show anti-botnet signature update
auto: no
schedule: weekly at Friday 13 o'clock
Router(config)# show anti-botnet update status
current status: Botnet Filter signature download has failed. (failed) at Mon Jul 9
18:01:32 2018
last update time: 2018/07/09 18:01:32
Router(config)# show security-service signature status
Feature         Type                      Current Version   Released Date
            Last Sync
================================================================================
====================================
Anti-Malware    Anti-Malware Signature    1.0.0.000         2018-01-01 00:00:00
(UTC+08:00) 2018-07-08 23:26:01
Anti-Malware    Cloud Threat Database     1.0.0.20171211.1  2017-12-11 13:46:40
(UTC+08:00) 2018-07-08 23:26:01
App-Patrol      App-Patrol                1.0.0.20180125.0  2018-01-25 09:45:25
(UTC+08:00) 2018-07-08 00:46:01
IDP             IDP                       3.1.4.050         2013-12-05 18:09:51
(UTC+08:00) 2018-07-08 01:11:01
Botnet Filter   Botnet Filter             1.0.0.000         2017-04-01 11:25:37
(UTC+08:00) 2018-07-09 18:01:19
```

40.3.6 URL Threat Filter Statistics

The following table describes the commands for collecting and displaying URL Threat Filter statistics. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 188 Commands for URL Threat Filter Statistics

COMMAND	DESCRIPTION
`[no] anti-botnet statistics collect`	Turns the collection of URL Threat Filter IP blocking statistics on or off.
`anti-botnet statistics flush`	Clears the collected IP blocking statistics.
`[no] threat-website statistics collect`	Turns the collection of URL Threat Filter URL blocking statistics on or off.
`threat-website statistics flush`	Clears the collected URL blocking statistics.

Table 188 Commands for URL Threat Filter Statistics (continued)

COMMAND	DESCRIPTION
`show anti-botnet statistics summary`	Displays the collected URL Threat Filter IP blocking statistics.
`show anti-botnet statistics collect status`	Displays whether the collection of URL Threat Filter IP blocking statistics is turned on or off.
`show anti-botnet statistics recent-activities`	Displays a list of connection attempts to or from the URL Threat Filter IP addresses.
`show threat-website statistics collect`	Displays whether the collection of URL Threat Filter blocking statistics is turned on or off.
`show threat-website statistics list`	Displays a list of connection attempts to or from the web pages of the specified categories.
`show threat-website statistics summary`	Displays the collected URL Threat Filter blocking statistics.

40.3.7 URL Threat Filter Statistics Example

This example shows how to collect and display URL Threat Filter statistics.

```
Router(config)# anti-botnet statistics collect
Router(config)# show anti-botnet statistics collect status
Anti-BotNet Statistics Status: yes
duration: since 2018-07-09 17:38:15 to 2018-07-09 18:17:15
Router(config)# show anti-botnet statistics summary
enable: 1
scan: 0
total_threat: 0
high: 0
medium: 0
low: 0
Router(config)#
```

40.3.7.1 Security Threat Category Definitions

The following table contains a list of URL Threat Filter (previously Anti-Botnet Filter) categories in firmware version 4.50 or earlier.

Table 189 Legacy Category Descriptions

CATEGORY	DESCRIPTION
Anonymizers	Sites and proxies that act as an intermediary for surfing to other Web sites in an anonymous fashion, whether to circumvent web filtering or for other reasons.
Botnets	A botnet is a network consisting of computers that are infected with malware and remotely controlled. The infected computers will contact and wait for instructions from a command and control (C&C) server. An attacker can control the botnet by setting up a C&C server and then sending commands to the infected computers. Alternatively, a peer-to-peer network approach is used. The infected computer scans and communicates with the peer devices in the same botnet to share commands or malware sent by the C&C server. These are botnet sites including command-and-control (C&C) servers

Table 189 Legacy Category Descriptions (continued)

Compromised	Sites that have been compromised by someone other than the site owner in order to install malicious programs without the user's knowledge. Includes sites that may be vulnerable to a particular high-risk attack.
Malware	Sites that install unwanted software on a user's computer with the intent to enable third-party monitoring or make system changes without the user's consent.
Phishing & Fraud	Sites that are used for deceptive or fraudulent purposes (e.g. phishing), such as stealing financial or other user account information. These sites are most often designed to appear as legitimate sites in order to mislead users into entering their credentials.
Spam Sites	Sites that have been promoted through spam techniques.

The following table contains a list of URL Threat Filter categories in firmware version 4.55 or later.

Table 190 Current Category Descriptions

CATEGORY	DESCRIPTION
Anonymizers	Sites and proxies that act as an intermediary for surfing to other Web sites in an anonymous fashion, whether to circumvent web filtering or for other reasons.
Browser Exploits	Sites that contain browser exploits. A browser exploit is any content that forces a web browser to perform operations that you do not explicitly intend.
Malicious Downloads	Sites that host files containing malicious content, such as viruses, spyware, rootkits, and ransomware.
Malicious Sites	Sites that install unwanted software on a user's computer with the intent to enable third-party monitoring or make system changes without the user's consent.
Phishing	Sites that are used for deceptive or fraudulent purposes (e.g. phishing), such as stealing financial or other user account information. These sites are most often designed to appear as legitimate sites in order to mislead users into entering their credentials.
Spam URLs	Sites that have been promoted through spam techniques.
Spyware Adware Keyloggers	Sites that contain spyware, adware, or keyloggers. Spyware is a program installed on your computer, usually without your explicit knowledge, that captures and transmits personal information or Internet browsing habits and details to companies. Companies use this information to analyze browsing habits, to gather marketing data, and to sell your information to others. Key logger programs try to capture and steal your passwords and watch and record everything you do on your computer. Adware programs typically display blinking advertisements or pop-up windows when you perform a certain action. Adware programs are often installed in exchange for another service, such as the right to use a program without paying for it.

40.4 DNS Threat Filter Commands

The following table describes general DNS Threat Filter commands. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 191 DNS Threat Filter Commands

COMMAND	DESCRIPTION
`[no] dns-filter black-list activate`	Enables or disables the DNS Threat Filter black list. The Zyxel Device treats all FQDNs in the blacklist as malicious, and applies DNS Threat Filter rules when they are queried.
`dns-filter black-list` *`FQDN`* `{activate|deactivate}`	Activates or deactivates the specified Fully Qualified Domain Name (FQDN) in the DNS Threat Filter black list. If the FQDN is not already in the black list, the Zyxel Device adds it. FQDN example: www.zyxel.com.tw
`no dns-filter black-list` *`FQDN`*	Removes the specified Fully Qualified Domain Name (FQDN) from the DNS Threat Filter black list.
`dns-filter black-list replace <1..256>` *`FQDN`* `{activate|deactivate}`	Replaces the Fully Qualified Domain Name (FQDN) of the specified entry with a new one in the DNS Threat Filter black list.
`[no] dns-filter drop-malform-packet activate`	Sets the Zyxel Device to drop a DNS query packet if the DNS query is invalid, or if the device cannot read the packet. A DNS query is invalid under any of the following conditions: • The number of entries in the DNS header question count field is 0 • An error occurs while parsing the domain name in the question field • The length of the domain name exceeds 255 characters Use the [no] command to allow malformed DNS packets to pass through the Zyxel Device.
`[no] dns-filter drop-malform-packet log`	Have the Zyxel Device log a DNS query if the DNS query packet is not a standard DNS query, or if the device cannot read the packet. Use the [no] command to stop logging.
`dns-filter profile` *`profilename`*	Enter subcommand mode and edit the specified DNS Threat Filter configuration profile. If the profile does not currently exist, the Zyxel Device creates it. Note: Only certain Zyxel Device models and firmware versions support multiple profiles in the Web Configurator. On Zyxel Devices that do not support multiple profiles, edit the profile named default_profile to change settings in the Web Configurator UI.
action *`{pass|redirect}`*	Choose what the Zyxel Device does when it detects a malicious DNS query packet. *`pass`*: Have the Zyxel Device allow the DNS query packet and not reply a DNS reply packet with a fake IP for it. *`redirect`*: Have the Zyxel Device reply with a DNS reply packet containing a default or custom-defined IP address. The default redirect IP is the IP address of the DNS Threat Filter server (dnsft.cloud.zyxel.com).
[no] black-list activate	Enables or disables the DNS Threat Filter black list for this profile.

Table 191 DNS Threat Filter Commands (continued)

COMMAND	DESCRIPTION
[no] category {anonymizers | phishing | browser-exploits | spam-urls | malicious-downloads | spyware-adware-keyloggers | malicious-sites}	The Zyxel Device considers DNS queries that match the specified category to be malicious. The *no* command means the Zyxel Device ignores DNS queries that match the specified category.
description *description*	Sets a description for the profile. You can use up to 60 printable ASCII characters.
[no] description	Deletes the description for this profile.
[no] log	The Zyxel Device generates a log message when it detects a malicious DNS query packet. The *no* command means the Zyxel Device does not generate a log message or alert when it detects a malicious DNS query packet.
log-alert	The Zyxel Device generates a log message and an alert when it detects a malicious DNS query packet.
[no] white-list activate	Enables or disables the DNS Threat Filter white list for this profile.
`dns-filter rename` *old_profile_name new_profile_name*	Renames the DNS Threat Filter profile.
`dns-filter redirect-ip default`	Sets the redirect IPv4 address for malicious DNS queries to the default, which is the IP address of the DNS Threat Filter server (dnsft.cloud.zyxel.com). This setting is used when `dns-filter profile > action` is set to `redirect`.
`dns-filter redirect-ip custom` *IPv4*	Sets the redirect IP address for malicious DNS queries to the specified IPv4 address. This setting is used when `dns-filter profile > action` is set to `redirect`.
`[no] dns-filter statistics collect`	Turns the collection of DNS Threat Filter blocking statistics on or off.
`dns-filter statistics flush`	Clears the collected IP blocking statistics.
`[no] dns-filter white-list activate`	Enables or disables the DNS Threat Filter white list. The Zyxel Device treats all FQDNs in the white list as non-malicious, and does not apply DNS Threat Filter rules when they are queried.
`dns-filter white-list` *FQDN* `{activate|deactivate}`	Activates or deactivates the specified Fully Qualified Domain Name (FQDN) in the DNS Threat Filter white list. If the FQDN is not already in the white list, the Zyxel Device adds it. FQDN example: www.zyxel.com.tw
`no dns-filter white-list` *FQDN*	Removes the specified Fully Qualified Domain Name (FQDN) from the DNS Threat Filter white list.
`dns-filter white-list replace <1..256>` *FQDN* `{activate|deactivate}`	Replaces the Fully Qualified Domain Name (FQDN) of the specified entry with a new one in the DNS Threat Filter white list.
`show dns-filter {white-list|black-list}`	Displays the current DNS Threat Filter white or black list.

Table 191 DNS Threat Filter Commands (continued)

COMMAND	DESCRIPTION
`show dns-filter dashboard statistics summary`	Displays the total number of Fully Qualified Domain Names (FQDNs) that the Zyxel Device has scanned, and the number of malicious FQDNs detected, as displayed on the Web Configurator dashboard.
`show dns-filter profile {all | profilename}`	Shows the name and settings of each DNS Threat Filter profiles, or the specified DNS Threat Filter profile.
`show dns-filter search FQDN`	Runs a DNS query for the specified Fully Qualified Domain Name (FQDN) and returns the result according to the current DNS Threat Filter rules.
`show dns-filter statistics collect`	Displays whether the collection of DNS Threat Filter statistics is turned on or off.
`show dns-filter statistics list`	Displays the collected DNS Threat Filter statistics.
`show dns-filter statistics summary`	Displays the total number of Fully Qualified Domain Names (FQDNs) that the Zyxel Device has scanned, and the number of malicious FQDNs detected.
`show dns-filter status`	Displays the action and log settings for the `dns-filter` service.
`[no] security-service dns-filter activate`	Turns on the DNS Threat Filter service on the Zyxel Device. The no command disables the DNS Threat Filter service.
`security-service dns-filter inspect {all-traffic | by-policy}`	Sets how the security service inspects traffic. *all-traffic*: The security service inspects all traffic passing through the Zyxel Device. *by-policy*: The security service inspects traffic only when its profile is bound to a security policy. For information on binding a security service profile to a security policy, see Section 29.2.1 on page 221.
`show security-service status`	Displays whether the security services are enabled on the Zyxel Device.
`dns-filter fake-dns-response-ttl <300...86400>`	Sets the time period in seconds for redirecting clients to a default or custom-defined IP address when the clients try to access a blocked FQDN. If you remove an FQDN from the block list before the response time-to-live (TTL) time is up, the clients will still be redirected to a default or custom-defined IP address when they try to access the FQDN.
`show dns-filter fake-dns-response-ttl`	Displays how long the clients will be redirected to a default or custom-defined IP address when the clients try to access a blocked FQDN.
`dns-filter secure-dns action {drop | pass}`	Sets what action the Zyxel Device takes when there is an encrypted DNS query packet. An encrypted DNS query packet might endanger your network because the Zyxel Device cannot inspect it to check if a user on your network is trying to access a suspect site. `pass`: Use this command to have the Zyxel Device allow the DNS query packet through the Zyxel Device. `drop`: Use this command to have the Zyxel Device discard the encrypted DNS query packet. Please note that if you enable Use secure DNS in your browser (with Google Chrome as the example) in Customize and control > Privacy and security > Security > Advanced, the Zyxel Device will discard all the DNS query packets over HTTPS you send to the DoH server that's in the Zyxel Device database.
`dns-filter secure-dns {log | no log}`	Sets if you want to have the Zyxel Device create a log when there is an encrypted DNS query packet.

Table 191 DNS Threat Filter Commands (continued)

COMMAND	DESCRIPTION
`[no] utm-manager {doh| dot| system-protect} defaultport` *`port number`*	Sets the default port used to transmit packets for the specified service. The no command sets the value you configure back to default.
`show utm-manager {doh| dot| system-protect} defaultport`	Displays the port used to transmit packets for the specified service.
`show secure-dns search {`*`FQDN`*`|`*`IP Address`*`}`	Enters an IP address or FQDN to check if the associated DoH or DoT server is included in the Zyxel Device database.

40.5 Blocking Secure DNS Query Packets Command Examples

You want to:

- Make sure users in your Zyxel Device network cannot access malicious sites through DNS query packets that the Zyxel Device cannot inspect, such as an HTTPS site.

  DNS over HTTPS/TLS packets are DNS query packets encrypted by HyperText Transfer Protocol Secure (HTTPS) or Transport Layer Security (TLS). When a client accesses an HTTPS site, the client is sending out an encrypted DNS query packet that the Zyxel Device cannot inspect.
- Have the Zyxel Device generate logs when users try to access suspect sites through encrypted DNS packets.

When a user sends out encrypted DNS over HTTPS or DNS over TLS query packets, the Zyxel Device will check the DNS over HTTPS or DNS over TLS server IP address to which the query packets are sent. If the DNS over HTTPS or DNS over TLS server IP address is in the Zyxel Device database, the Zyxel Device will block these packets. If not, the Zyxel Device will not block these packets.

The DNS threat filter general settings use the parameters in the table below. General settings are for all traffic in the Zyxel Device network.

Table 192 DNS Threat General Settings Example

ACTION WHEN DETECTING DNS OVER HTTPS/TLS PACKETS
drop/log

1 Configure the DNS threat filter general settings.

```
Router# configure terminal
Router(config)#
Router(config)# dns-filter secure-dns action drop
Router(config)# dns-filter secure-dns log
```

CHAPTER 41
Sandboxing

41.1 Sandboxing Overview

The Zyxel Device sandboxing is a security mechanism, which provides a safe environment to separate running programs from your network and host devices. Unknown or untrusted programs/codes are executed within an isolated virtual machine (VM) to monitor and analyze the zero-day malware and advanced persistent threats (APTs) that may evade the Zyxel Device protection, such as anti-malware. When a file with malicious or suspicious codes is detected, the Zyxel Device can take specific actions on the threats.

41.2 Sandbox Commands

The following table describes general sandbox commands. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 193 Sandbox Commands

COMMAND	DESCRIPTION
`sandbox dashboard statistics flush`	Clears the collected sandboxing statistics displayed on the web GUI dashboard.
`sandbox file-scanning-log {log | log-alert | no}`	Generates a log, log and alert or neither (no) when a file is being scanned.
`sandbox file-send-log {log | log-alert | no}`	Generates a log, log and alert or neither (no) when a file is sent for sandboxing inspection.
`[no] sandbox file-type {archives | chm | eicar | executables | macromedia-flash-data | ms-office-document | pdf | rtf | unknow-type}`	Specifies the type of files to be sent for sandboxing inspection. The no command sets the Zyxel Device to not send the specified type of files for sandboxing inspection.
`sandbox malicious-action malicious {allow | destroy} {log | log-alert | no}`	Sets whether the Zyxel Device deletes (`destroy`) or forwards (`allow`) malicious files. This also sets the Zyxel Device to generate a log, log and alert or neither (no) when a malicious file is detected.
`sandbox malicious-action suspicious {allow | destroy} {log | log-alert | no}`	Sets whether the Zyxel Device deletes (`destroy`) or forwards (`allow`) suspicious files. This also sets the Zyxel Device to generate a log, log and alert or neither (no) when a suspicious file is detected.
`sandbox mdb flush`	Removes sandboxing MDB files.

Table 193 Sandbox Commands (continued)

COMMAND	DESCRIPTION
`[no] sandbox queue-packet`	Has the Zyxel Device hold the downloaded file for up to two seconds if the downloaded file has never been inspected before. The Zyxel Device will wait for the could server's result and forward the file in two seconds. Sandbox detection may take longer than two seconds, so infected files could still possibly be forwarded to the user. The no command clears the setting. Note: The Zyxel Device only checks the file types you specified for sandbox inspction. The scan result will be removed from the Zyxel Device cache after the Zyxel Device restarts.
`sandbox response-clean-log {log | log-alert | no}`	Generates a log, log and alert or neither (no) when no malicious or suspicious files are detected.
`sandbox server-file {delete | keep}`	The Zyxel Device tells the sandboxing host server to keep or delete a file after scanning it. Note: This feature is deprecated.
`[no] sandbox statistics collect`	Turns the collection of sandboxing statistics on or off.
`sandbox statistics flush`	Clears the collected sandboxing statistics.
`sandbox dashboard statistics flush`	Clears the collected sandboxing statistics on the web GUI dashboard.
`[no] security-service sandbox activate`	Turns on sandboxing on the Zyxel Device. The no command disables sandboxing.
`show sandbox file-type all`	Displays all the file types and whether a type of files is to be sent for sandboxing inspection.
`show sandbox file-type status`	Displays only the types of files that are set to be sent for sandboxing inspection.
`show sandbox statistics collect`	Displays whether the collection of sandboxing statistics is turned on or off.
`show sandbox statistics ranking file-name`	Queries and sorts the sandboxing statistics entries by file name.
`show sandbox statistics summary`	Displays the collected sandboxing statistics.
`show sandbox statistics dashboard summary`	Displays the collected sandboxing statistics that are currently displayed on the web GUI dashboard.
`show sandbox status`	Displays the action and log settings for sandboxing.
`show security-service status`	Displays whether the security services are enabled on the Zyxel Device.

41.2.1 Sandbox Command Examples

This command shows how to enable sandboxing on the Zyxel Device and displays the status of security services.

```
Router# configure terminal
Router(config)# security-service sandbox activate
Router(config)# show security-service status
ips activation: no
sandbox activation: yes
anti-virus activation: yes
anti-botnet-ip activation: no
anti-botnet-url activation: no
anti-spam activation: no
content-filter activation: yes
app-patrol activation: yes
Router(config)#
```

This command sets the Zyxel Device to delete malicious files and generate a log when a malicious file is detected.

```
Router# configure terminal
Router(config)# sandbox malicious-action malicious destroy log
Router(config)#
```

CHAPTER 42
IDP Commands

42.1 Overview

IDP (Intrusion Detection and Prevention) protects against network-based intrusions, by detecting malicious or suspicious packets and responding instantaneously.
The IDP commands mostly mirror web configurator features. It is recommended you use the web configurator for IDP features such as searching for web signatures, creating/editing an IDP profile or creating/editing a custom signature. Some web configurator terms may differ from the command-line equivalent.

Packet Inspection Signatures

A signature is a pattern of malicious or suspicious packet activity. You can specify an action to be taken if the system matches a stream of data to a malicious signature. You can change the action in the profile screens. Packet inspection examine OSI (Open System Interconnection) layer-4 to layer-7 packet contents for malicious data. Generally, packet inspection signatures are created for known attacks while anomaly detection looks for abnormal behavior.

Rate Based Signatures

Rate based signatures are IDP signatures that allow the Zyxel Device to just respond when a certain number of malicious packets are identified within a specific time.

Figure 33 IDP Signatures Example

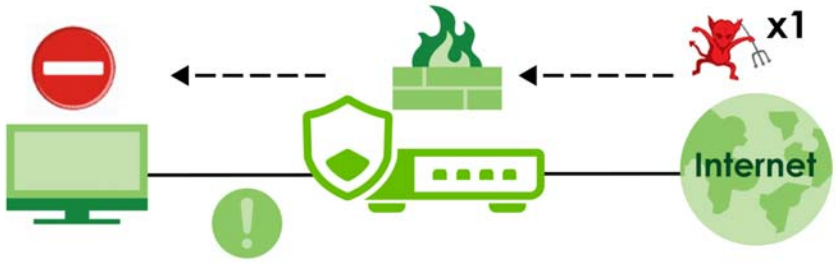
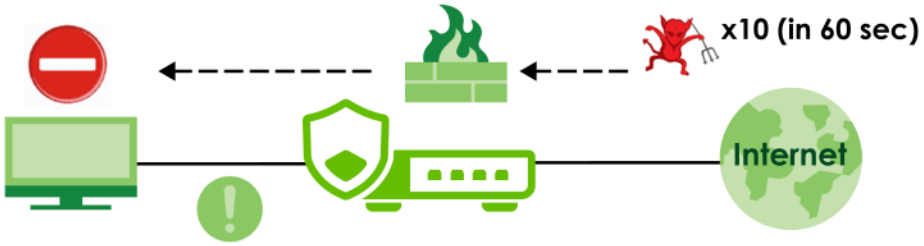


Figure 34 Rate Based Signatures Example



Note: The no command negates the action or returns it to the default value.

The following table lists valid input for IDP commands.

Table 194 Input Values for IDP Commands

LABEL	DESCRIPTION
zone_profile	The name of a zone. For some Zyxel Device models, use up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive. For other Zyxel Device models, use pre-defined zone names like DMZ, LAN1, SSL VPN, IPSec VPN, OPT, and WAN.
idp_profile	The name of an IDP profile. It can consist of alphanumeric characters, the underscore, and the dash, and it is 1-31 characters long. Spaces are not allowed.

42.2 General IDP Commands

42.2.1 IDP Activation

Note: You must register for the IDP/AppPatrol signature service (at least the trial) before you can use it. See Chapter 5 on page 53.

This table shows the IDP signature, and system-protect activation commands.

Table 195 IDP Activation

COMMAND	DESCRIPTION
`[no] security-service ips activate`	Turns on IDP on the Zyxel Device. The no command disables IDP.
`show security-service status`	Displays whether the security services such as IDP are enabled on the Zyxel Device.
`security-service ips inspect {all-traffic | by-policy}`	Sets how the security service inspects traffic. *all-traffic*: The security service inspects all traffic passing through the Zyxel Device. *by-policy*: The security service inspects traffic only when its profile is bound to a security policy. For information on binding a security service profile to a security policy, see Section 29.2.1 on page 221.
`[no] idp {anomaly | signature} activate`	Enables IDP signatures or anomaly detection. IDP signatures use requires IDP service registration. If you don't have a standard license, you can register for a once-off trial one. The no command disables the specified service.
`idp system-protect {activate| deactivate}`	Enables IDP system-protect to scan the packets that are destined for or sent out by the Zyxel Device for malicious or suspicious activities.
`show idp {anomaly | signature | system-protect} activation`	Displays the activation status of the anomaly detection, IDP signature, or system protect service.
`show idp rate_based_sig <profile name>`	Displays the specified rate based signature profile.
`idp reload`	Recovers the IDP signatures. You should only need to do this if instructed to do so by a support technician.

Table 195 IDP Activation

COMMAND	DESCRIPTION
`idp session-block {activate | deactivate}`	Activate a specific RDP signature. Note: This command is aimed at regular users. You should only use it if instructed to do so.
`idp session-block period {1-3600}`	Sets the time in seconds that the Zyxel Device blocks an IP address which matches the `idp session-block signature`.

42.2.1.1 Activate/Deactivate IDP Example

This example shows how to activate and deactivate signature-based IDP on the Zyxel Device.

```
Router# configure terminal
Router(config)# idp signature activate
Router(config)# show idp signature activation
idp signature activation: yes
Router(config)# no idp signature activate
Router(config)# show idp signature activation
idp signature activation: no
```

42.3 IDP Profile Commands

42.3.1 Global Profile Commands

Use these commands to rename or delete existing profiles and show IDP base profiles.

Table 196 Global Profile Commands

COMMAND	DESCRIPTION
`idp rename signature` *`profile1 profile2`*	Rename an IDP signature originally named *`profile1`* to *`profile2`*.
`no idp signature` *`profile3`*	Delete an IDP signature or system protect profile named *`profile3`*.
`idp signature profile signature sid {activate | log [alert] | action {drop | reject-sender | reject-receiver | reject-both}}`	Sets the action and log for the specified signature.
`idp signature mode {detection | prevention}`	Sets what the Zyxel Device does when a stream of data matches a malicious signature. • detection: The Zyxel Device only creates a log message. The default IDP profile changes to default_detect_only. • prevention: The Zyxel Device performs a user-specified action. The default IDP profile changes to default_profile.
`show idp signature` *`profile`* `signature all details`	Lists the settings for all of the specified profile's signatures. Use `|more` to display the settings page by page.
`show idp signature all details`	Lists the settings for all of the signatures. Use `|more` to display the settings page by page.
`show idp {signature | anomaly} base profile`	Displays all IDP signature or system protect base profiles.

Table 196 Global Profile Commands

COMMAND	DESCRIPTION
`show idp signature base profile {all|none|wan|lan|dmz} settings`	Lists the specified signature base profile's settings. Use `|more` to display the settings page by page.
`show idp signature profiles`	Displays IDP profiles created.
`show idp signature mode`	Displays the IDP scan mode.
`show idp engine version`	Displays the IDP engine version.
`show idp signature profile signature sid details`	Displays specified signature details.

42.3.1.1 Example of Global Profile Commands

In this example we rename an IDP signature profile from "old_profile" to "new_profile", delete the "bye_profile" and show all base profiles available.

```
Router# configure terminal
Router(config)# idp rename signature old_profile new_profile
Router(config)# no idp signature bye_profile
Router(config)# show idp signature base profile
No.  Base Profile Name
============================================================
1    none
2    all
3    wan
4    lan
5    dmz
Router(config)#
```

42.3.2 Editing/Creating IDP Signature Profiles

Use these commands to create a new IDP signature profile or edit an existing one. It is recommended you use the web configurator to create/edit profiles. If you do not specify a base profile, the default base profile is none.

Note: You cannot change the base profile later!

Table 197 Editing/Creating IDP Signature Profiles

COMMAND	DESCRIPTION
`idp signature *newpro* [base {all | lan | wan | dmz | none}]`	Creates a new IDP signature profile called *newpro*. *newpro* uses the base profile you specify. Enters sub-command mode. All the following commands relate to the new profile. Use `exit` to quit sub-command mode.
`[no] signature *sid* activate`	Activates or deactivates an IDP signature.
`signature *sid* log [alert]`	Sets log or alert options for an IDP signature
`no signature *sid* log`	Deactivates log options for an IDP signature
`signature *sid* action {drop | reject-sender | reject-receiver | reject-both}`	Sets an action for an IDP signature

Table 197 Editing/Creating IDP Signature Profiles (continued)

COMMAND	DESCRIPTION
`no signature sid action`	Deactivates an action for an IDP signature.
`description description2`	Describes the signature profile.

42.3.3 Editing Rate Based Signatures Profiles

IDP signatures identify traffic packets with suspicious malicious patterns. The Zyxel Device can then respond instantaneously according to the action you define. If you do not want the Zyxel Device to respond instantaneously for each suspicious packet detected, use rate based signatures.

Use these commands to edit rate based signatures profiles. It is recommended you use the web configurator to create/edit profiles. You must use the `configure terminal` commands to enter the configuration mode before you can use the configuration commands.

Table 198 Editing Rate Based Signatures Profiles

COMMAND	DESCRIPTION
`idp signature default_profile`	Enters configuration mode for the rate based signatures default profiles.
`signature sid seconds`	Sets the length of time in seconds the event should occur from a client the counts number of times to trigger an action. For example, counts is set to 5, and seconds is set to 60. If the Zyxel Device detects 5 or more occurrences of malicious traffic in less than 60 seconds, then action is triggered.
`signature sid counts`	Sets the number of security events that need to occur within the defined seconds to trigger an action.
`signature sid block_period`	Sets the time period the attacker's IP will be blocked.
`signature sid action {drop | reject-sender | reject-receiver | reject-both}`	Sets an action for a rate based signature.
`no signature sid action`	Deactivates an action for a rate based signature.

42.3.3.1 IDP Rate-Based Signature Example

This example shows how to configure a rate-based signature settings.

```
Router# configure terminal
Router(config)# idp signature default_profile
Router(config-idp-signature-profile-default_profile)# signature 130009
action         activate       block_period   counts         log
seconds
Router(config-idp-signature-profile-default_profile)# signature 130009
seconds
<1..120>
Router(config-idp-signature-profile-default_profile)# signature 130009
seconds 60
Router(config-idp-signature-profile-default_profile)# signature 130009
counts
<1..300>
Router(config-idp-signature-profile-default_profile)# signature 130009
counts 250
Router(config-idp-signature-profile-default_profile)# signature 130009
block_period
<0..86400>
Router(config-idp-signature-profile-default_profile)# signature 130009
block_period 500
Router(config-idp-signature-profile-default_profile)# signature 130009
action
drop              reject-both       reject-receiver   reject-sender
Router(config-idp-signature-profile-default_profile)# signature 130009
action drop
```

42.3.4 Signature Search

Use this command to search for signatures in the named profile.

Note: It is recommended you use the web configurator to search for signatures.

Table 199 Signature Search Command

COMMAND	DESCRIPTION
`idp search signature` *`my_profile`* `name` *`quoted_string`* `sid SID severity` *`severity_mask`* `platform` *`platform_mask`* `classtype` *`classtype_mask`* `service` *`service_mask`* `activate {any | yes | no} log {any | no | log | log-alert} action` *`action_mask`*	Searches for signature(s) in a profile by the parameters specified. The quoted string is any text within the signature name in quotes, for example, [idp search LAN_IDP name "WORM" sid 0 severity 0 platform 0 classtype 0 service 0 activate any log any action] searches for all signatures in the LAN_IDP profile containing the text “worm” within the signature name.
`show idp search signature` *`my_profile`* `name` *`quoted_string`* `sid SID severity` *`severity_mask`* `platform` *`platform_mask`* `classtype` *`classtype_mask`* `service` *`service_mask`* `activate {any | yes | no} log {any | no | log | log-alert} action` *`action_mask`*	Searches for signature(s) in a profile by the parameters specified. The quoted string is any text within the signature name in quotes, for example, [idp search LAN_IDP name "WORM" sid 0 severity 0 platform 0 classtype 0 service 0 activate any log any action] searches for all signatures in the LAN_IDP profile containing the text “worm” within the signature name.

42.3.4.1 Search Parameter Tables

The following table displays the command line severity, platform and class type equivalent values. If you want to combine platforms in a search, then add their respective numbers together. For example, to search for signatures for Windows NT, Windows XP and Windows 2000 computers, then type “12” as the platform parameter.

Table 200 Severity, Platform and Class Type Command Values

SEVERITY	PLATFORM	CLASS TYPE
1 = Very Low	1 = All	1 = DoS
2 = Low	2 = Win95/98	2 = Buffer-Overflow
3 = Medium	4 = WinNT	3 = Access-Control
4 = High	8 = WinXP/2000	4 = Scan
5 = Severe	16 = Linux	5 = Backdoor/Trojan
	32 = FreeBSD	6 = Others
	64 = Solaris	7 = P2P
	128 = SGI	8 = IM
	256 = Other-Unix	9 = Virtus/Worm
	512 = Network-Device	10 = Botnet
		11 = Web-Attack
		12 = Spam

The following table displays the command line service and action equivalent values. If you want to combine services in a search, then add their respective numbers together. For example, to search for signatures for DNS, Finger and FTP services, then type “7” as the service parameter.

Table 201 Service and Action Command Values

SERVICE	SERVICE	ACTION
1 = DNS	65536 = SMTP	1 = None
2 = FINGER	131072 = SNMP	2 = Drop
4 = FTP	262144 = SQL	4 = Reject-sender
8 = MYSQL	524288 = TELNET	8 = Reject-receiver
16 = ICMP	1048576 = TFTP	16 = Reject-both
32 = IM	2097152 = n/a	
64 = IMAP	4194304 = WEB_ATTACKS	
128 = MISC	8388608 = WEB_CGI	
256 = NETBIOS	16777216 = WEB_FRONTPAGE	
512 = NNTP	33554432 = WEB_IIS	
1024 = ORACLE	67108864 = WEB_MISC	
2048 = P2P	134217728 = WEB_PHP	
4096 = POP2	268435456 = MISC_BACKDOOR	
8192 = POP3	536870912 = MISC_DDOS	
16384 = RPC	1073741824 = MISC_EXPLOIT	
32768 = RSERVICES		

42.3.4.2 Signature Search Example

This example command searches for all signatures in the LAN_IDP profile:

- Containing the text “worm” within the signature name
- With an ID of 12345
- Has a very low severity level
- Operates on the Windows NT platform
- Is of class type: DNS service
- Is enabled
- Generates logs.

```
Router# configure terminal
Router(config)#
Router(config)# idp search signature LAN_IDP name “worm” sid 12345 severity
1 platform 4 type 4 service 1 activate yes log log action 2
```

42.4 IDP Custom Signatures

Use these commands to create a new signature or edit an existing one.

Note: It is recommended you use the web configurator to create/edit signatures using the web configurator Anti-X > UTM Profile > Custom Signatures screen.

Note: You must use the web configurator to import a custom signature file.

Table 202 Custom Signatures

COMMAND	DESCRIPTION
`idp customize signature` *quoted_string*	Create a new custom signature. The quoted string is the signature command string enclosed in quotes. for example. "alert tcp any any <> any any (msg: \"test\"; sid: 9000000 ;)".
`idp customize signature edit` *quoted_string*	Edits an existing custom signature.
`no idp customize signature` *custom_sid*	Deletes a custom signature.
`idp customize_import name sig_name`	Edits an existing signature.
`show idp signatures custom-signature` *custom_sid* `{details | contents | non-contents}`	Displays custom signature information.
`show idp signatures custom-signature all details`	Displays all custom signatures' information.
`show idp signatures custom-signature number`	Displays the total number of custom signatures.

42.4.1 Custom Signature Examples

These examples show how to create a custom signature, edit one, display details of one, all and show the total number of custom signatures.

```
Router# configure terminal
Router(config)# idp customize signature "alert tcp any any <> any any
(msg: \"test\"; sid: 9000000 ;  )"
sid: 9000000
  message: test
  class type:
  severity:
  platform:
    all: no
    Win95/98: no
    WinNT: no
    WinXP/2000: no
    Linux: no
    FreeBSD: no
    Solaris: no
    SGI: no
    other-Unix: no
    network-device: no
  service:
  outbreak: no
```

This example shows you how to edit a custom signature.

```
Router(config)# idp customize signature edit "alert tcp any any <> any any
(msg : \"test edit\"; sid: 9000000 ;  )"
sid: 9000000
  message: test edit
  class type:
  severity:
  platform:
    all: no
    Win95/98: no
    WinNT: no
    WinXP/2000: no
    Linux: no
    FreeBSD: no
    Solaris: no
    SGI: no
    other-Unix: no
    network-device: no
  service:
  outbreak: no
```

This example shows you how to display custom signature details.

```
Router(config)# show idp signatures custom-signature 9000000 details
sid: 9000000
  message: test edit
  class type:
  severity:
  platform:
    all: no
    Win95/98: no
    WinNT: no
    WinXP/2000: no
    Linux: no
    FreeBSD: no
    Solaris: no
    SGI: no
    other-Unix: no
    network-device: no
  service:
  outbreak: no
```

This example shows you how to display custom signature contents.

```
Router(config)# show idp signatures custom-signature 9000000 contents
sid: 9000000
Router(config)# show idp signatures custom-signature 9000000 non-contents
sid: 9000000
  ack:
  dport: 0
  dsize:
  dsize_rel:
  flow_direction:
  flow_state:
  flow_stream:
  fragbits_reserve:
  fragbits_dontfrag:
  fragbits_morefrag:
  fragoffset:
  fragoffset_rel:
  icmp_id:
  icmp_seq:
  icode:
  icode_rel:
  id:
  ipopt:
  itype:
  itype_rel:
  sameip:
  seq:
  sport: 0
  tcp_flag_ack:
  tcp_flag_fin:
  tcp_flag_push:
  tcp_flag_r1:
  tcp_flag_r2:
  tcp_flag_rst:
  tcp_flag_syn:
  tcp_flag_urg:
  threshold_type:
  threshold_track:
  threshold_count:
  threshold_second:
  tos:
  tos_rel:
  transport: tcp
  ttl:
  ttl_rel:
  window:
  window_rel:
```

This example shows you how to display all details of a custom signature.

```
Router(config)# show idp signatures custom-signature all details
sid: 9000000
  message: test edit
  class type:
  severity:
  platform:
    all: no
    Win95/98: no
    WinNT: no
    WinXP/2000: no
    Linux: no
    FreeBSD: no
    Solaris: no
    SGI: no
    other-Unix: no
    network-device: no
  service:
  outbreak: no
```

This example shows you how to display the number of custom signatures on the Zyxel Device.

```
Router(config)# show idp signatures custom-signature number
signatures:  1
```

42.5 Update IDP Signatures

Use these commands to update new signatures. You register for IDP service before you can update IDP signatures, although you do not have to register in order to update system-protect signatures.

Note: You must use the web configurator to import a custom signature file.

Table 203 Update Signatures

COMMAND	DESCRIPTION
`idp signature update signatures`	Immediately downloads IDP signatures from an update server.
`[no] idp signature update auto`	Enables (disables) automatic signature downloads at regular times and days.
`idp signature update hourly`	Enables automatic signature download every hour.
`idp signature update daily <0..23>`	Enables automatic signature download every day at the time specified.
`idp signature update weekly {sun | mon | tue | wed | thu | fri | sat} <0..23>`	Enables automatic signature download once-a-week at the time and day specified.
`show idp signature update`	Displays signature update schedule.
`show idp signature update status`	Displays signature update status.
`show idp signature signatures {version | date | number}`	Displays signature information

Table 203 Update Signatures

COMMAND	DESCRIPTION
`show idp signatures date`	Displays the date and time the signature set was released.
`show idp signatures number`	Displays the number of signatures in this set.
`show idp signatures version`	Displays the signature set version number currently used by the Zyxel Device. This number gets larger as new signatures are added.

42.5.1 Update Signature Examples

These examples show how to enable/disable automatic IDP downloading, schedule updates, display the schedule, display the update status, show the (new) updated signature version number, show the total number of signatures and show the date/time the signatures were created.

```
Router# configure terminal
Router(config)# idp signature update signatures
IDP signature update in progress.
Please check system log for future information.
Router(config)# idp signature update auto
Router(config)# no idp signature update auto
Router(config)# idp signature update hourly
Router(config)# idp signature update daily 10
Router(config)# idp signature update weekly fri 13
Router(config)# show idp signature update
auto: yes
schedule: weekly at Friday 13 o'clock
Router(config)# show idp signature update status
current status: IDP signature download failed, do 1 retry at Sat Jan  4
22:47:47  2003
last update time: 2003-01-01 01:34:39
Router(config)# show idp signature signatures version
version: 1.2000
Router(config)# show idp signature signatures number
signatures: 2000
Router(config)# show idp signature signatures date
date: 2005/11/13 13:56:03
```

42.6 IDP Statistics

The following table describes the commands for collecting and displaying IDP statistics. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 204 Commands for IDP Statistics

COMMAND	DESCRIPTION
`[no] idp statistics collect`	Turn the collection of IDP statistics on or off.
`idp statistics flush`	Clears the collected statistics.
`show idp statistics summary`	Displays the collected statistics.

Table 204 Commands for IDP Statistics (continued)

COMMAND	DESCRIPTION
`show idp statistics collect`	Displays whether the collection of IDP statistics is turned on or off.
`show idp statistics collect status`	Displays the status of collected statistics.
`show idp statistics ranking {signature-name | source | source6 | destination |destination6 | rate-based}`	Query and sort the IDP statistics entries by signature name, source IP address, or destination IP address. `signature-name`: lists the most commonly detected signatures. `source(6)`: lists the source IP addresses (IPv4 or IPv6) from which the Zyxel Device has detected the most intrusion attempts. `destination(6):` lists the most common destination IP addresses (IPv4 or IPv6) for detected intrusion attempts. `rate-based`: lists the detected rate based signatures.

42.6.1 IDP Statistics Example

This example shows how to collect and display IDP statistics. It also shows how to sort the display by the most common signature name, source IP address, or destination IP address.

```
Router# configure terminal
Router(config)# idp statistics collect
Router(config)# no idp statistics activate
Router(config)# idp statistics flush
Router(config)# show idp statistics collect status
IDP collect statistics status: yes
Router(config)# show idp statistics summary
scanned session : 268
packet dropped: 0
packet reset: 0
Router(config)# show idp statistics ranking signature-name
ranking: 1
  signature id: 8003796
  signature name: ICMP L3retriever Ping
  type: Scan
  severity: verylow
  occurence: 22
ranking: 2
  signature id: 8003992
  signature name: ICMP Large ICMP Packet
  type: DDOS
  severity: verylow
  occurence: 4
Router(config)# show idp statistics ranking destination
ranking: 1
  destination ip: 172.23.5.19
  occurence: 22
ranking: 2
  destination ip: 172.23.5.1
  occurence: 4
Router(config)# show idp statistics ranking source
ranking: 1
  source ip: 192.168.1.34
  occurence: 26
```

42.7 IDP White List

The Zyxel Device will exclude the incoming packets of the signature(s) in the IDP white list. These packets won't be intercepted and will be passed through uninspected.

You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 205 Commands for IDP White List

COMMAND	DESCRIPTION
`idp white-list`	Enter IDP white list sub-command mode.
`[no] sid {1–4294967295}`	Adds the specified signature to the IDP white list. The no command removes the specified signature from the IDP white list.
`exit`	Exit IDP white list sub-command mode.
`show idp white-list`	Displays all signatures in the IDP white list.

42.8 IDP Packet Capture

The following table describes the commands for configuring IDP packet capture settings. Use IDP packet capture to capture network traffic that triggers IDP signatures.

Table 206 Commands for IDP Statistics

COMMAND	DESCRIPTION
`idp packet-capture {enable | disable}`	Enables or disables IDP packet capture.
`idp packet-capture show status`	Displays current IDP packet capture settings.
`idp packet-capture select {enable | disable}`	Captures network traffic that triggers the specified IDP signatures.
`idp packet-capture select {add-id` *`sid`* `| del-id` *`sid`*`}`	Captures network traffic that triggers the specified IDP signature. You can select up to 10 signature SIDs. Use the `del` command to stop the Zyxel Device from capturing network traffic that triggers the specified signature.
`idp packet-capture default setting`	Returns IDP packet capture settings to factory defaults. This command will: • Enable IDP packet capture. • Disable IDP packet capture select. • Clear all selected signature SIDs.

42.8.1 IDP Packet Capture Example

This example shows how to capture network traffic that triggers the specified IDP signature.

```
Router# idp packet-capture enable
Router# idp packet-capture select enable
Router# idp packet-capture select add-id
<0..4294967295>
Router# idp packet-capture select add-id 12345
Router# idp packet-capture show status
ips pkt capture status info:
    enable: 1
    user select sig_id enable: 1
-------------------------------------------------------------
    current pkt count: 0
    current sig count: 0
    current session count: 0
    current mem size: 0
    current file size: 0
-------------------------------------------------------------
    user select sig id count: 1
    12345,
```

This example shows how to return IDP packet capture settings to factory defaults.

```
Router# idp packet-capture default setting
Router# idp packet-capture
default   disable   enable    select    show
Router# idp packet-capture show status
ips pkt capture status info:
    enable: 1
    user select sig_id enable: 0
-------------------------------------------------------------
    current pkt count: 0
    current sig count: 0
    current session count: 0
    current mem size: 0
    current file size: 0
-------------------------------------------------------------
    user select sig id count: 0
```

CHAPTER 43
Content Filtering

43.1 Content Filtering Overview

Content filtering allows you to block certain web features, such as cookies, and/or block access to specific web sites. It can also block access to specific categories of web site content. You can create different content filtering policies for different addresses, schedules, users or groups and content filtering profiles. For example, you can configure one policy that blocks John Doe's access to arts and entertainment web pages during the workday and another policy that lets him access them after work.

43.1.1 Web Content Filter

The Web Content Filter allows the Zyxel Device to block specific web features, such as cookies or ActiveX, by inspecting the web pages that users are visiting. The Zyxel Device can also block access to specific websites, by inspecting the URL or Server Name Indication (SNI) that the user's web browser sends to the web server.

43.1.1.1 Web Content Filter Process

1. A user enters a URL into their web browser.
2. The user's computer sends a DNS query for the URL.
3. DNS server returns an IP address for the URL.
4. The user's web browser connects to the IP address.
5. The Web Content Filter detects an HTTP connection, and inspects the website send using Server Name Indication (SNI).
6. If the website contains prohibited material, the HTTP request is redirected to a block page.

Note: If the user's web browser is using encryption, then you must enable SSL Inspection for Web Content Filter to work.
If the user's web browser is using Encrypted Server Name Indication (ESNI), DNS Content Filter will not work.

43.1.2 DNS Content Filter

The DNS Content Filter allows the Zyxel Device to block access to specific websites by inspecting DNS queries made by users on your network. If the website in the DNS query contains prohibited material, then the Zyxel Device replies to the DNS query with a IP address that points to the block page.
Unlike the Web Content Filter, the DNS Content Filter works if the user is using TLS 1.3 with ESNI.

43.1.2.1 DNS Content Filter Process

1. A user enters a URL into their web browser.
2. The user's computer sends a DNS query for the URL.
3. The DNS Content Filter detects DNS query, and inspects the website in the DNS query packet.
4. If website contains prohibited material, the DNS reply is redirected to a block page.

43.2 External Web Filtering Service

When you register for and enable the external web filtering service, your Zyxel Device accesses an external database that has millions of web sites categorized based on content. You can have the Zyxel Device block, block and/or log access to web sites based on these categories.

See the web configurator User's Guide to see how to view content filtering reports after you have activated the category-based content filtering subscription service.

Table 207 content-filter Report Commands

COMMAND	DESCRIPTION
content-filter report deactivate	Sets the message to display when content filtering blocks access to a web page. The no command clears the setting.
content-filter report server {ip_address | hostname}	Sets the URL of the web page to which to send users when their web access is blocked by content filtering. The no command clears the setting.

43.3 Content Filter Command Input Values

The following table explains the values you can input with the content-filter and dns-content-filter commands.

Table 208 Content Filter Command Input Values

LABEL	DESCRIPTION
filtering_profile	The filtering profile defines how to filter web URLs or content. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
category_name	The name of a web category. For a list of category definitions, see Section 43.7 on page 382. Firmware v4.50 or earlier: {advertisements-pop-ups | job-search | alcohol-tobacco | leisure-recreation | anonymizers | malware | arts | network-errors | botnets | news | business | non-profits-ngos | chat | nudity | child-abuse-images | parked-domains | compromised | peer-to-peer | computers-technology | personal-sites | criminal-activity | phishing-fraud |cults | politics | dating-personals | pornography-sexually-explicit | download-sites | private-ip-addresses | education | real-estate | entertainment | religion | fashion-beauty | restaurants-dining | finance | school-cheating | forums-newsgroups | search-engines-portals | gambling | sex-education | games | shopping | general | social-networking | government | spam-sites | greeting-cards | sports | hacking | streaming-media-downloads | hate-intolerance | tasteless | health-medicine | translators | illegal-drugs | transportation | illegal-software | travel | image-sharing | violence | information-security | weapons | instant-messaging | web-based-email } Firmware v4.55 or later: {adult-topics | alcohol | anonymizing-utilities | art-culture-heritage | auctions-classifieds | blogs-wiki | business | chat | computing-internet | consumer-protection | content-server | controversial-opinions | cult-occult | dating-personals | dating-social-networking | digital-postcards | discrimination | drugs | education-reference | entertainment | extreme | fashion-beauty | finance-banking | for-kids | forum-bulletin-boards | gambling | gambling-related | game-cartoon-violence | games | general-news | government-military | gruesome-content | health | historical-revisionism | history | humor-comics | illegal-uk | incidental-nudity | information-security | information-security-new | instant-messaging | interactive-web-applications | internet-radio-tv | internet-services | job-search | major-global-religions | marketing-merchandising | media-downloads | media-sharing | messaging | mobile-phone | moderated | motor-vehicles | non-profit-advocacy-ngo | nudity | online-shopping | p2p-file-sharing | parked-domain | personal-network-storage | personal-pages | pharmacy | politics-opinion | pornography | portal-sites | potential-criminal-activities | potential-hacking-computer-crime | potential-illegal-software | private-ip-addresses | profanity | professional-networking | provocative-attire | public-information | pups | real-estate | recreation-hobbies | religion-ideology | remote-access | reserved | residential-ip-addresses | resource-sharing | restaurants | school-cheating-information | search-engines | sexual-materials | shareware-freeware | social-networking | software-hardware | sports | stock-trading | streaming-media | technical-business-forums | technical-information | text-spoken-only | text-translators | tobacco | travel | usenet-news | violence | visual-search-engine | weapons | web-ads | web-mail | web-meetings | web-phone}

Table 208 Content Filter Command Input Values (continued)

LABEL	DESCRIPTION
trust_hosts	The IP address or domain name of a trusted web site. Use a host name such as www.good-site.com. Do not use the complete URL of the site – that is, do not include “http://”. All subdomains are allowed. For example, entering “zyxel.com” also allows “www.zyxel.com”, “partner.zyxel.com”, “press.zyxel.com”, etc. Use up to 63 case-insensitive characters (0-9a-z-). You can enter a single IP address in dotted decimal notation like 192.168.2.5. You can enter a subnet by entering an IP address in dotted decimal notation followed by a slash and the bit number of the subnet mask of an IP address. The range is 0 to 32. To find the bit number, convert the subnet mask to binary and add all of the 1’s together. Take “255.255.255.0” for example. 255 converts to eight 1’s in binary. There are three 255’s, so add three eights together and you get the bit number (24). An example is 192.168.2.1/24 You can enter an IP address range by entering the start and end IP addresses separated by a hyphen, for example 192.168.2.5-192.168.2.23. IPv6 support format like: Single ip - 2001::1 Range format - 2001::1-2001::5 Prefix format - 2001::1/64
forbid_hosts	The IP address or domain name of a forbidden web site. Use a host name such as www.bad-site.com into this text field. Do not use the complete URL of the site – that is, do not include “http://”. All subdomains are also blocked. For example, entering “bad-site.com” also blocks “www.bad-site.com”, “partner.bad-site.com”, “press.bad-site.com”, etc. Use up to 63 case-insensitive characters (0-9a-z-). You can enter a single IP address in dotted decimal notation like 192.168.2.5. You can enter a subnet by entering an IP address in dotted decimal notation followed by a slash and the bit number of the subnet mask of an IP address. The range is 0 to 32. To find the bit number, convert the subnet mask to binary and add all of the 1’s together. Take “255.255.255.0” for example. 255 converts to eight 1’s in binary. There are three 255’s, so add three eights together and you get the bit number (24). An example is 192.168.2.1/24 You can enter an IP address range by entering the start and end IP addresses separated by a hyphen, for example 192.168.2.5-192.168.2.23. IPv6 support format like: Single ip - 2001::1 Range format - 2001::1-2001::5 Prefix format - 2001::1/64
keyword	A keyword or a numerical IP address to search URLs for and block access to if they contain it. Use up to 63 case-insensitive characters (0-9a-zA-Z;/?:@&=+$\-_!~*'()%,) in double quotes. For example enter “Bad_Site” to block access to any web page that includes the exact phrase “Bad_Site”. This does not block access to web pages that only include part of the phrase (such as “Bad” in this example).
message	The message to display when a web site is blocked. Use up to 255 characters (0-9a-zA-Z;/?:@&=+$\-_!~*'()%,) in quotes. For example, “Access to this web page is not allowed. Please contact the network administrator.”

Table 208 Content Filter Command Input Values (continued)

LABEL	DESCRIPTION
redirect_url	The URL of the web page to which you want to send users when their web access is blocked by content filtering. The web page you specify here opens in a new frame below the denied access message. Use "http://" followed by up to 255 characters (0-9a-zA-Z;/?:@&=+$\.-_!~*'()%) in quotes. For example, "http://192.168.1.17/blocked access". IPv6 format support: http://[2001::1]/blocked_access
service_timeout	The value specifies the maximum querying time in seconds <1...60>
url	The URL of a web site in http://xxx.xxx.xxx format.
query_timeout	The value specifies the maximum querying time when testing the connection to an external content filtering server or checking its rating for a URL. <1..60> seconds.

43.4 Web Content Filter

The following section describes the commands for the web content filter.

43.4.1 General Web Content Filter Commands

The following table lists the commands that you can use for general web content filter configuration, such as creating a denial of access message or specifying a redirect URL and checking your external web filtering service registration status. Use the `configure terminal` command to enter the configuration mode to be able to use these commands. See Table 208 on page 367 for details about the values you can input with these commands.

Table 209 content-filter General Commands

COMMAND	DESCRIPTION
`[no] content-filter block message` *message*	Sets the message to display when the Web Content Filter blocks access to a web page. The `no` command clears the setting.
`[no] content-filter block redirect` *redirect_url*	Sets the URL of the web page to which to send users when their web access is blocked by the Web Content Filter. The `no` command clears the setting.
`content-filter passed warning flush`	Clears the Zyxel Device's record of sessions for which it has given the user a warning before allowing access.
`content-filter passed warning timeout <1..1440>`	Sets how long to keep records of sessions for which the Zyxel Device has given the user a warning before allowing access.
`content-filter url-cache clear`	Clears all URLs from the Zyxel Device's local Web Content Filter cache.
`content-filter url-cache clear` *url*	Deletes the specified URL from the Zyxel Device's local Web Content Filter cache.
`content-filter url-server test commtouch`	Firmware v4.50 or earlier Enters the sub-command mode for testing URLs with the legacy external Web Content Filter.

Table 209 content-filter General Commands (continued)

COMMAND	DESCRIPTION
`content-filter url-server test`	Firmware v4.55 or later Enters the sub-command mode for testing URLSs with the Web Content Filter.
`url` [timeout *query_timeout*]	Checks which Web Content Filter category a web page belongs to. Enter the page's full URL including the protocol, for example: http://www.zyxel.com.tw. The query fails if the content filter is not active. `timeout:` Specify how long to wait for a response from the Web Content Filter server, in seconds.
`exit`	Leaves the sub-command mode.
`content-filter common-list {trust|forbid}`	Enters the sub-command for configuring a common list of trusted or forbidden web sites. The Web Content Filter profile commands let you configure trusted or forbidden URLs for individual profiles. URL checking is applied in the following order: profile trusted web sites, common trusted web sites, profile forbidden web sites, common forbidden web sites, and then profile keywords.
[no] {*ipv4* | *ipv4_cidr* | *ipv4_range* | *wildcard_domainname* | *tld* |*ipv6* | *ipv6_range* | *ipv6_prefix* }	Adds or removes a common trusted or forbidden web site entry. *ipv4*: IPv4 address <W.X.Y.Z> • *ipv4_cidr*: IPv4 subnet in CIDR format, i.e. 192.168.1.0/32 <W.X.Y.Z>/<1..32> *ipv4_range*: Range of IPv4 addresses. <W.X.Y.Z>-<W.X.Y.Z> *wildcard_domainname*: Wildcard domain name, in the format *String1.String2*. For example: zyxel*.co* • String 1 must consist of 1–63 characters, and may include letters, numbers, and the following special characters: - (hyphen), . (period), * (wildcard character). • String 2 must consist of 1–63 characters, and may include letters, numbers, and the following special characters: - (hyphen), * (wildcard character). *tld*: top level domain. ipv6: IPv6 address, i.e. 2001::1 ipv6_range: Range of IPv6 address, < IPv6 Address >-< IPv6 Address > ipv6_prefix: IPv6 prefix formant, <IPv6 Address>/<Prefix Length>
`exit`	Leaves the sub-command mode.
`content-filter cf-queue flush`	Clears content filter queuing packets.
`[no] content-filter https-domain-filter activate`	Enables HTTPs Domain Filter which lets the ZyWALL/USG take action on HTTPS web pages using the category service. In an HTTPS connection, the Zyxel Device can extract the Server Name Indication (SNI) from a client request, check if it matches a category in the Web Content Filter and then take appropriate action. The keyword match is for the domain name only. The `no` command disables the HTTPs Domain Filter.

Table 209 content-filter General Commands (continued)

COMMAND	DESCRIPTION
`show content-filter passed warning`	Displays the Zyxel Device's record of sessions for which it has given the user a warning before allowing access.
`show content-filter settings`	Displays the general content filtering settings.
`show content-filter common-list {trust|forbid}`	Displays the common list of trusted or forbidden web sites.
`show content-filter https-domain-filter status`	Displays HTTPs Domain Filter content filtering settings.
`[no] content-filter sslv3 action block`	Block HTTPS web pages that are using SSL version 3 or earlier.

43.4.2 Web Content Filter Profile Commands

The following table lists the commands that you can use to configure a web content filter profile. Use the `configure terminal` command to enter the configuration mode to be able to use these commands. See Table 208 on page 367 for details about the values you can input with these commands.

Table 210 content-filter Filtering Profile Commands Summary

COMMAND	DESCRIPTION
`[no] content-filter profile` *`filtering_profile`*	Creates a Web Content Filter profile. The no command removes the profile.
`[no] content-filter profile` *`filtering_profile`* `url-server`	Enables the Content Filter Category Service for this profile. The no command disables the service.
`[no] content-filter profile` *`filtering_profile`* `custom`	Sets a Web Content Filter profile to use a profile's custom settings (lists of trusted web sites and forbidden web sites and blocking of certain web features). The no command has the profile not use the custom settings.
`[no] content-filter profile` *`filtering_profile`* `custom activex`	Sets a Web Content Filter profile to block ActiveX controls. The no command sets the profile to allow ActiveX.
`[no] content-filter profile` *`filtering_profile`* `custom cookie`	Sets a Web Content Filter profile to block Cookies. The no command sets the profile to allow Cookies.
`[no] content-filter profile` *`filtering_profile`* `log-level-info`	Enables this to has the Zyxel Device generate logs at the info level. A log at the info level is a log to inform you of network events that are not serious or critical. For example, the Zyxel Device will generate an info level log when an admin level account user logs in to the Zyxel Device through the web configurator. Use the no command to have the Zyxel Device generate logs at the alert level. A log at the alert level is a log for serious events that may need more immediate attention. For example, you may want to know right away if there are clients in your networks that try to access adult topics or drugs related web pages. Use the command `show logging entries [priority` *`pri`*`]` to display the specified level logs.
`content-filter profile` *`filtering_profile`* `custom-list forbid`	Enters the sub-command for configuring the Web Content Filter profile's list of forbidden hosts.
`[no]` *`forbid_hosts`*	Adds a forbidden host to the Web Content Filter profile's list. The no command removes it.

Table 210 content-filter Filtering Profile Commands Summary (continued)

COMMAND	DESCRIPTION
exit	Leaves the sub-command mode.
[no] content-filter profile *filtering_profile* custom java	Sets a Web Content Filter profile to block Java. The no command sets the profile to allow Java.
content-filter profile *filtering_profile* custom-list keyword	Enters the sub-command for configuring the Web Content Filter profile's list of forbidden keywords. This has the content filtering profile block access to Web sites with URLs that contain the specified keyword or IP address in the URL.
[no] *keyword*	Adds a forbidden keyword or IP address to the Web Content Filter profile's list. The no command removes it.
exit	Leaves the sub-command mode.
[no] content-filter profile *filtering_profile* custom proxy	Sets a Web Content Filter profile to block access to web proxy servers. The no command sets the profile to allow access to proxy servers.
content-filter profile *filtering_profile* custom-list trust	Enters the sub-command for configuring the Web Content Filter profile's list of trusted hosts.
[no] *trust_hosts*	Adds a trusted host to the Web Content Filter profile's list. The no command removes it.
exit	Leaves the sub-command mode.
[no] content-filter profile *filtering_profile* custom trust-allow-features	Sets a Web Content Filter profile to permit Java, ActiveX and Cookies from sites on the trusted list. The no command has the content filtering profile not permit Java, ActiveX and Cookies from sites on the trusted list
[no] content-filter profile *filtering_profile* custom trust-only	Sets a Web Content Filter profile to only allow access to web sites that are on the trusted list. The no command has the profile allow access to web sites that are not on the trusted list.
[no] content-filter service-timeout *service_timeout*	Sets how many seconds the Zyxel Device is to wait for a response from the external content filtering server. The no command clears the setting.
[no] content-filter profile *filtering_profile* commtouch-url category {category_name}	Firmware v4.50 or earlier Sets a Web Content Filter profile to check for specific legacy web site categories. The no command has the profile not check for the specified categories.
[no] content-filter profile *filtering_profile* category {category_name}	Firmware v4.55 or later Sets a Web Content Filter profile to check for specific web site categories. The no command has the profile not check for the specified categories.
content-filter profile *filtering_profile* commtouch-url match-unsafe {block | log | warn |pass}	Firmware v4.50 or earlier Sets the action for attempted access to web pages that match the Web Content Filter profile's selected legacy unsafe categories. Block access, log access, or allow access.
content-filter profile *filtering_profile* commtouch-url match {block | log | pass}	Firmware v4.50 or earlier Sets the action for attempted access to web pages that match the Web Content Filter profile's selected legacy managed categories. Block access, allow and log access, display a warning message before allowing access, or allow access.

Table 210 content-filter Filtering Profile Commands Summary (continued)

COMMAND	DESCRIPTION
`content-filter profile *filtering_profile* [commtouch-url] match {block | log | pass}`	Firmware v4.55 or later Sets the action for attempted access to web pages that match the profile's selected managed categories. Block access, allow and log access, display a warning message before allowing access, or allow access. The *commtouch-url* option has no effect, and is only included for compatibility.
`content-filter profile *filtering_profile* commtouch-url offline {block | log | warn | pass}`	Firmware v4.50 or earlier Sets the action for attempted access to web pages if the legacy external web filtering database is unavailable. Block access, allow and log access, display a warning message before allowing access, or allow access.
`content-filter profile *filtering_profile* [commtouch-url] offline {block | log | warn | pass}`	Firmware v4.55 or later Sets the action for attempted access to web pages if the external web filtering database is unavailable. Block access, allow and log access, display a warning message before allowing access, or allow access. The *commtouch-url* option has no effect, and is only included for compatibility.
`content-filter profile *filtering_profile* commtouch-url unrate {block | log | warn | pass}`	Firmware v4.50 or earlier Sets the action for attempted access to web pages that the legacy external web filtering service has not categorized. Block access, allow and log access, display a warning message before allowing access, or allow access.
`content-filter profile *filtering_profile* [commtouch-url] unrate {block | log | warn | pass}`	Firmware v4.55 or later Sets the action for attempted access to web pages that the external web filtering service has not categorized. Block access, allow and log access, display a warning message before allowing access, or allow access. The *commtouch-url* option has no effect, and is only included for compatibility.
`content-filter profile *filtering_profile* commtouch-url log-all`	Firmware 4.50 or earlier. The Zyxel Device creates a log message each time an IPv4 address is scanned by the Web Content Filter service.
`content-filter profile *filtering_profile* [commtouch-url] log-all`	Firmware v4.55 or later The Zyxel Device creates a log message each time an IPv4 address is scanned by the Web Content Filter service. The *commtouch-url* option has no effect, and is only included for compatibility.
`no content-filter profile *filtering_profile* commtouch-url match-unsafe {log}`	Has the Zyxel Device not log attempted access to web pages that match the profile's selected legacy unsafe categories.

Table 210 content-filter Filtering Profile Commands Summary (continued)

COMMAND	DESCRIPTION
`no content-filter profile filtering_profile commtouch-url match {log}`	Firmware v4.50 or earlier Has the Zyxel Device not log attempted access to web pages that match the profile's selected legacy managed categories.
`no content-filter profile filtering_profile [commtouch-url] match {log}`	Firmware v4.55 or later Has the Zyxel Device not log attempted access to web pages that match the profile's selected managed categories. The *commtouch-url* option has no effect, and is only included for compatibility.
`no content-filter profile filtering_profile commtouch-url offline {log}`	Firmware v4.50 or earlier Has the Zyxel Device not log access to web pages if the legacy external Web Content Filter database is unavailable.
`no content-filter profile filtering_profile [commtouch-url] offline {log}`	Firmware v4.55 or later Has the Zyxel Device not log access to web pages if the external Web Content Filter database is unavailable. The *commtouch-url* option has no effect, and is only included for compatibility.
`no content-filter profile filtering_profile commtouch-url unrate {log}`	Firmware v4.50 or earlier Has the Zyxel Device not log access to web pages that the legacy external Web Content Filter has not categorized.
`no content-filter profile filtering_profile [commtouch-url] unrate {log}`	Firmware v4.55 or later Has the Zyxel Device not log access to web pages that the external Web Content Filter service has not categorized. The *commtouch-url* option has no effect, and is only included for compatibility.
`[no] content-filter sslv3 action block`	Has the Zyxel Device block HTTPS web pages using SSL V3 or a previous version. The no command allows HTTPS web pages using SSL V3 or a previous version.
`[no] content-filter https-domain-filter block-page activate`	Has the ZyWALL/USG display a warning page instead of a blank page when an HTPPS connection is redirected. The no command has the ZyWALL/USG display a blank page when an HTTPS connection is blocked.
`content-filter https-domain-filter block-page port <port>`	Changes the port number of the HTTPS Domain Filter blocking page. The default port is 54088.
`content-filter https-domain-filter block-cache-ttl <1~60>`	Sets how many seconds (1-60) to keep blocked HTTPS pages in the cache. The default value is 5.
`content-filter https-domain-filter forward-cache-ttl <1~1440>`	Sets how many minutes (1-1440) to keep forwarded HTTPS pages in the cache. The default value is 60.
`[no] content-filter profile <filtering_profile> safesearch`	Enables SafeSearch in the specified Web Content Filter profile. SafeSearch is a feature of a search engine that can automatically filter sexually explicit videos and images from the search result without overloading the Zyxel Device. Supported search engines at the time of writing are: Yahoo, Google, MSN Live Bing, Yandex

Table 210 content-filter Filtering Profile Commands Summary (continued)

COMMAND	DESCRIPTION
`[no] content-filter safesearch <name>`	Creates a Web Content Filter safesearch rule and enters sub-command mode. The no command removes the rule.
`domain match <string>`	Sets a string that the domain name should (partially) match in a safesearch rule. For example, domain-match: .google.
`domain not-match <string>`	Sets a string that the domain name should not match in a safesearch rule.
`url match <string>`	Sets a string that the URL should (partially) match in a safesearch rule. For example, url-match: search
`url not-match <string>`	Sets a string that the URL should not match in a safesearch rule.
`url parameter <string>`	Sets a parameter that updates the URL when there is a safesearch rule match. Values in URL Parameters are set dynamically in a page's URL. Example url-parameter: safe=
`url value <string>`	Sets a value that updates the URL when there is a safesearch rule match. Example url-value: active
`cookie match <string>`	Sets a string that the cookie should (partially) match in a safesearch rule. A cookie is a small piece of data sent from a website and stored in the user's web browser.
`cookie parameter <string>`	Sets a parameter that updates the cookie when there is a safesearch rule match. Parameters store information such as the cookie's expiration, domain, and flags.
`cookie value <string>`	Sets a value that updates the cookie when there is a safesearch rule match. The value of a cookie can be modified by the server in response to a page request.
`show content-filter safesearch`	Displays all safesearch rules created and their sub-command contents.
`show content-filter profile commtouch`	Firmware v4.50 or earlier Displays a list of all Web Content Filter profiles.
`show content-filter profile`	Firmware v4.55 or later Displays a list of all Web Content Filter profiles.
`show content-filter profile [filtering_profile] commtouch`	Firmware v4.50 or earlier Displays the settings of the specified Web Content Filter profile, including which categories it blocks.
`show content-filter profile [filtering_profile]`	Firmware v4.55 or later Displays the settings of the specified Web Content Filter profile, including which categories it blocks.

43.4.3 Web Content Filtering Statistics

The following table describes the commands for collecting and displaying web content filtering statistics. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 211 Commands for Content Filtering Statistics

COMMAND	DESCRIPTION
`[no] content-filter statistics collect`	Turn the collection of Web Content Filter statistics on or off.
`content-filter statistics flush`	Clears the collected Web Content Filter statistics.
`show content-filter statistics summary`	Displays the collected Web Content Filter statistics.
`show content-filter statistics collect`	Displays whether the collection of Web Content Filter statistics is turned on or off.
`show content-filter statistics summary`	Displays the current Web Content Filter statistics.

43.4.4 Web Content Filtering Statistics Example

This example shows how to collect and display Web Content Filter statistics.

```
Router(config)# content-filter statistics collect
Router(config)# show content-filter statistics summary
total web pages inspected               : 0
  web pages warned by category service : 0
  web pages blocked by category service: 0
  web pages blocked by custom service  : 0
    restricted web features            : 0
    forbidden web sites                : 0
    url keywords                       : 0
    web pages passed                   : 0

  unsafe web pages                     : 0
  other web pages                      : 0
```

43.5 DNS Content Filter

The following section describes the commands for the DNS content filter.

43.5.1 DNS Content Filter Commands

The following table lists the commands that you can use for general DNS content filter configuration, Use the `configure terminal` command to enter the configuration mode to be able to use these commands. See Table 208 on page 367 for details about the values you can input with these commands.

Table 212 DNS Content Filter Commands

COMMAND	DESCRIPTION
`dns-content-filter black-list` *`FQDN`* `{activate | deactivate}`	Activates or deactivates the specified Fully Qualified Domain Name (FQDN) in the DNS Content Filter black list. If the FQDN is not already in the black list, the Zyxel Device adds it. FQDN example: www.zyxel.com.tw
`no dns-content-filter black-list` *`FQDN`*	Removes the specified Fully Qualified Domain Name (FQDN) from the DNS Content Filter black list.
`[no] dns-content-filter black-list activate`	Enables or disables the DNS Content Filter black list. The Zyxel Device treats all FQDNs in the blacklist as prohibited, and applies DNS Content filter rules when they are queried.
`dns-content-filter black-list replace <1..256>` *`FQDN`* `{activate | deactivate}`	Replaces the Fully Qualified Domain Name (FQDN) of the specified entry with a new one in the DNS Content Filter black list.
`dns-content-filter redirect-ip custom` *`IPv4`*	Sets the redirect IP address for prohibited DNS queries to the specified IPv4 address. This setting is used when `dns-content-filter profile > action` is set to `redirect`.
`dns-content-filter redirect-ip default`	Sets the redirect IPv4 address for prohibited DNS queries to the default, which is the IP address of the DNS Content Filter server (dnsft.cloud.zyxel.com). This setting is used when `dns-content-filter profile > action` is set to `redirect`.
`dns-content-filter white-list` *`FQDN`* `{activate | deactivate}`	Activates or deactivates the specified Fully Qualified Domain Name (FQDN) in the DNS Content Filter white list. If the FQDN is not already in the white list, the Zyxel Device adds it. FQDN example: www.zyxel.com.tw
`no dns-content-filter white-list` *`FQDN`*	Removes the specified Fully Qualified Domain Name (FQDN) from the DNS Content Filter white list.
`[no] dns-content-filter white-list activate`	Enables or disables the DNS Content Filter white list. The Zyxel Device treats all FQDNs in the white list as non-prohibited, and does not apply DNS Content Filter rules when they are queried.
`dns-content-filter white-list replace <1..256>` *`FQDN`* `{activate | deactivate}`	Replaces the Fully Qualified Domain Name (FQDN) of the specified entry with a new one in the DNS Content Filter white list.
`show dns-content-filter {white-list | black-list}`	Displays the current DNS Content Filter white or black list.
`show dns-content-filter dashboard statistics summary`	Displays the total number of Fully Qualified Domain Names (FQDNs) that the Zyxel Device has scanned, and the number of prohibited FQDNs detected, as displayed on the Web Configurator dashboard.
`show dns-content-filter profile {all | profileName}`	Shows the name and settings of each DNS Content Filter profiles, or the specified DNS Content Filter profile.

Table 212 DNS Content Filter Commands (continued)

COMMAND	DESCRIPTION
`show dns-content-filter search FQDN`	Runs a DNS query for the specified Fully Qualified Domain Name (FQDN) and returns the result according to the current DNS Content Filter rules.
`show dns-content-filter status`	Displays the action and log settings for the `dns-content-filter` service.
`dns-content-filter fake-dns-response-ttl <300...86400>`	Sets the time period in seconds for redirecting clients to a default or custom-defined IP address when the clients try to access a blocked FQDN. If you remove an FQDN from the block list before the response time-to-live (TTL) time is up, the clients will still be redirected to a default or custom-defined IP address when they try to access the FQDN.
`show dns-content-filter fake-dns-response-ttl`	Displays how long the clients will be redirected to a default or custom-defined IP address when the clients try to access a blocked FQDN.

43.5.2 DNS Content Filter Profile Commands

The following table lists the commands that you can use to configure a DNS content filter profile. Use the `configure terminal` command to enter the configuration mode to be able to use these commands. See Table 208 on page 367 for details about the values you can input with these commands.

Table 213 dns-content-filter Profile Commands Summary

COMMAND	DESCRIPTION
`dns-content-filter profile <profilename>`	Enter subcommand mode and edit the specified DNS Content Filter configuration profile. If the profile does not currently exist, the Zyxel Device creates it.
`action {pass | redirect}`	Choose what the Zyxel Device does when it detects a prohibited DNS query packet. *pass*: Have the Zyxel Device allow the DNS query packet and not reply a DNS reply packet with a fake IP for it. *redirect*: Have the Zyxel Device reply with a DNS reply packet containing a default or custom-defined IP address. The default redirect IP is the IP address of the DNS Content Filter server (dnsft.cloud.zyxel.com).
`[no] black-list activate`	Enables or disables the DNS Content Filter black list for this profile.
`[no] category category_name`	The Zyxel Device considers DNS queries that match the specified category to be prohibited. The *no* command means the Zyxel Device ignores DNS queries that match the specified category.
`description description`	Sets a description for the profile. You can use up to 60 printable ASCII characters.
`[no] description`	Deletes the description for this profile.
`[no] log`	The Zyxel Device generates a log message when it detects a prohibited DNS query packet. The *no* command means the Zyxel Device does not generate a log message or alert when it detects a DNS query packet.
`log-alert`	The Zyxel Device generates a log message and an alert when it detects a prohibited DNS query packet.

Table 213 dns-content-filter Profile Commands Summary (continued)

COMMAND	DESCRIPTION
`[no] white-list activate`	Enables or disables the DNS Content Filter white list for this profile.
`safesearch [no] activate`	Enables SafeSearch in the specified DNS Content Filter profile. SafeSearch is a feature of a search engine that can automatically filter sexually explicit videos and images from the search result without overloading the Zyxel Device. The Zyxel Device can filter the following: YouTube, Google, MSN Live Bing The no command disables SafeSearch.
`safesearch youtube {moderate| strict}`	`strict` prevents the Zyxel Device clients from seeing pornography, and offensive or inappropriate videos on YouTube. `moderate` allows YouTube to display more videos in the search result.

43.5.3 DNS Content Filtering Statistics

The following table describes the commands for collecting and displaying DNS Content Filter statistics. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 214 Commands for DNS Content Filter Statistics

COMMAND	DESCRIPTION
`[no] dns-content-filter statistics collect`	Turn the collection of DNS Content Filter statistics on or off.
`dns-content-filter statistics flush`	Clears the collected DNS Content Filter statistics.
`show dns-content-filter statistics collect`	Displays whether the collection of DNS Content Filter statistics is turned on or off.
`show dns-content-filter statistics list`	Displays the collected DNS Content Filter statistics.
`show dns-content-filter statistics summary`	Displays the total number of Fully Qualified Domain Names (FQDNs) that the Zyxel Device has scanned, and the number of prohibited FQDNs detected.

43.6 Web Content Filtering Example

The following example shows how to limit the web access for a sales group using the web content filter.

1 First, create a sales address object. This example uses a subnet that covers IP addresses 172.21.3.1 to 172.21.3.254.

2 Then create a schedule for all day.

3 Create a filtering profile for the group.

4 You can use the following commands to block sales from accessing job search websites.

5 Enable the external web filtering service.

Note: You must register for the external web filtering service before you can use it (see Chapter 5 on page 53).

6 You can also customize the filtering profile. The following commands block active-X, java and proxy access.

7 Append a Secure Policy with content filter profile.

```
Router# configure terminal
Router(config)# address-object sales 172.2.3.0/24
Router(config)# schedule-object all_day 00:00 23:59
Router(config)# content-filter profile sales_CF_PROFILE
Router(config)# content-filter profile sales_CF_PROFILE category job-search
Router(config)# content-filter profile sales_CF_PROFILE url-server
Router(config)# content-filter profile sales_CF_PROFILE custom java
Router(config)# content-filter profile sales_CF_PROFILE custom activex
Router(config)# content-filter profile sales_CF_PROFILE custom proxy
Router(config)# content-filter profile sales_CF_PROFILE custom
Router(config)# secure-policy insert 1
Router(config)# name UTM
Router(config)# from LAN1
Router(config)# schedule all_day
Router(config)# sourceip sales
Router(config)# no app-profile
Router(config)# cf-profile sales_CF_PROFILE log by-profile activate
Router(config)# exit
```

Use this command to display the settings of the profile.

```
Router(config)# show content-filter profile sales_CF_PROFILE
safesearch active :  no
service active :  yes
url match unsafe: action:   warn, log:  no
url match other : action:  block, log:  no
url unrate      : action:   warn, log:  no
service offline : action:   warn, log:  no
all log active :  no

category settings:
Art/Culture/Heritage            :  no, Alcohol                          :  no
Anonymizers                     : yes, Adult Topics                     :  no
Anonymizing Utilities           :  no, Business                         : yes
Chat                            :  no, Computing/Internet               :  no
Public Information              :  no, Potential Criminal Activities    :  no
Drugs                           :  no, Education/Reference              :  no
Entertainment                   :  no, Extreme                          :  no
Finance/Banking                 :  no, Gambling                         :  no
Games                           :  no, Government/Military              :  no
Potential Hacking/Computer Crime:  no, Health                           :  no
Humor/Comics                    :  no, Discrimination                   :  no
Instant Messaging               :  no, Stock Trading                    :  no
Internet Radio/TV               :  no, Job Search                       : yes
Information Security            :  no, Dating/Social Networking         :  no
Mobile Phone                    :  no, Media Downloads                  :  no
Malicious Sites                 : yes, Usenet News                      :  no
Nudity                          :  no, Non-Profit/Advocacy/NGO          :  no
...
```

43.7 Content Filter Category Definitions

Table 215 Legacy Category Descriptions (Firmware v4.50 or earlier)

CATEGORY	DESCRIPTION
Advertisements & Pop-Ups	Sites that provide advertising graphics or other ad content files such as banners and pop-ups.
Alcohol & Tobacco	Sites that promote or sell alcohol- or tobacco-related products or services.
Arts	Sites with artistic content or relating to artistic institutions such as theaters, museums, galleries, dance companies, photography, and digital graphic resources.
Business	Sites that provide business related information such as corporate Web sites. Information, services, or products that help businesses of all sizes to do their day-to-day commercial activities.
Transportation	Sites that provide information about motor vehicles such as cars, motorcycles, boats, trucks, RVs and the like. Includes manufacturer sites, dealerships, review sites, pricing,, online purchase sites, enthusiasts clubs, etc.
Chat	Sites that enable web-based exchange of real time messages through chat services or chat rooms.
Forums & Newsgroups	Sites for sharing information in the form of newsgroups, forums, bulletin boards.
Computers & Technology	Sites that contain information about computers, software, hardware, IT, peripheral and computer services, such as product reviews, discussions, and IT news.
Criminal Activity	Sites that offer advice on how to commit illegal or criminal activities, or to avoid detection. These can include how to commit murder, build bombs, pick locks, etc. Also includes sites with information about illegal manipulation of electronic devices, hacking, fraud and illegal distribution of software.
Dating & Personals	Sites that promote networking for interpersonal relationships such as dating and marriage. Includes sites for match-making, online dating, spousal introduction.
Download Sites	Sites that contain downloadable software, whether shareware, freeware, or for a charge. Includes peer-to-peer sites.
Education	Sites sponsored by educational institutions and schools of all types including distance education. Includes general educational and reference materials such as dictionaries, encyclopedias, online courses, teaching aids and discussion guides.
Entertainment	Sites related to television, movies, music and video (including video on demand), such as program guides, celebrity sites, and entertainment news.
Finance	Sites related to banking, finance, payment or investment, including banks, brokerages, online stock trading, stock quotes, fund management, insurance companies, credit unions, credit card companies, and so on.
Gambling	Sites that offer or are related to online gambling, lottery, casinos and betting agencies involving chance.
Games	Sites relating to computer or other games, information about game producers, or how to obtain cheat codes. Game-related publication sites.
Government	Sites run by governmental organizations, departments, or agencies, including police departments, fire departments, customs bureaus, emergency services, civil defense, counter-terrorism organizations, military and hospitals.
Hate & Intolerance	Sites that promote a supremacist political agenda, encouraging oppression of people or groups of people based on their race, religion, gender, age, disability, sexual orientation or nationality.
Health & Medicine	Sites containing information pertaining to health, healthcare services, fitness and well-being, including information about medical equipment, hospitals, drugstores, nursing, medicine, procedures, prescription medications, etc.

Table 215 Legacy Category Descriptions (Firmware v4.50 or earlier)

Illegal Drugs	Sites with information on the purchase, manufacture, and use of illegal or recreational drugs and their paraphernalia, and misuse of prescription drugs and other compounds.
Job Search	Sites containing job listings, career information, assistance with job searches (such as resume writing, interviewing tips, etc.), employment agencies or head hunters.
Streaming Media & Downloads	Sites that deliver streaming content, such as Internet radio, Internet TV or MP3 and live or archived media download sites. Includes fan sites, or official sites run by musicians, bands, or record labels.
News	Sites covering news and current events such as newspapers, newswire services, personalized news services, broadcasting sites, and magazines.
Non-profits & NGOs	Sites devoted to clubs, communities, unions, and non-profit organizations. Many of these groups exist for educational or charitable purposes.
Nudity	Sites that contain full or partial nudity that are not necessarily overtly sexual in intent. Includes sites that advertise or sell lingerie, intimate apparel, or swim wear.
Personal Sites	Sites about or hosted by personal individuals, including those hosted on commercial sites.
Politics	Sites that promote political parties or political advocacy, or provide information about political parties, interest groups, elections, legislation or lobbying. Also includes sites that offer legal information and advice.
Pornography/Sexually Explicit	Sites that contain explicit sexual content. Includes adult products such as sex toys, CD-ROMs, and videos, adult services such as videoconferencing, escort services, and strip clubs, erotic stories and textual descriptions of sexual acts.
Real Estate	Sites relating to commercial or residential real estate services, including renting, purchasing, selling or financing homes, offices, etc.
Religion	Sites that deal with faith, human spirituality or religious beliefs, including sites of churches, synagogues, mosques and other houses of worship.
Restaurants & Dining	Sites that list, review, promote or advertise food, dining or catering services. Includes sites for recipes, cooking instruction and tips, food products, and wine advisors.
Search Engines & Portals	Sites enabling the searching of the Web, newsgroups, images, directories, and other online content. Includes portal and directory sites such as white/yellow pages.
Shopping	Sites for online shopping, catalogs, online ordering, auctions, classified ads. Excludes shopping for products and services exclusively covered by another category such as health & medicine.
Social Networking	Sites that enable social networking for online communities of various topics, for friendship, dating, or professional reasons.
Sports	Sites relating to sports teams, fan clubs, scores and sports news. Relates to all sports, whether professional or recreational.
Translators	Sites that translate Web pages or phrases from one language to another. These sites may be used to attempt to bypass a filtering system.
Travel	Sites that provide travel and tourism information or online booking of travel services such as airlines, accommodations, car rentals. Includes regional or city information sites.
Violence	Sites that contain images or text depicting or advocating physical assault against humans, animals, or institutions. Sites of a particularly gruesome nature such as shocking depictions of blood or wounds, or cruel animal treatment.
Weapons	Sites that depict, sell, review or describe guns and weapons, including for sport.
Web-based Email	Sites that enable users to send and receive email through a web-accessible email account.
General	Sites that do not clearly fall into other categories, for example, blank Web pages.

Table 215 Legacy Category Descriptions (Firmware v4.50 or earlier)

Leisure & Recreation	Sites relating to recreational activities and hobbies including zoos, public recreation centers, pools, amusement parks, and hobbies such as gardening, literature, arts & crafts, home improvement, home decor, family, etc.
Cults	Sites relating to non-traditional religious practice typically known as "cults," that is, considered to be false, unorthodox, extremist, or coercive, with members often living under the direction of a charismatic leader.
Fashion & Beauty	Sites concerning fashion, jewelry, glamour, beauty, modeling, cosmetics or related products or services. Includes product reviews, comparisons, and general consumer information.
Greeting cards	Sites that allow people to send and receive greeting cards and postcards.
Hacking	Sites that promote or give advice about how to gain unauthorized access to proprietary computer systems, for the purpose of stealing information, perpetrating fraud, creating viruses, or committing other illegal activity related to theft of digital information.
Illegal Software	Sites that illegally distribute software or copyrighted materials such as movies or music, software cracks, illicit serial numbers, illegal license key generators.
Image Sharing	Sites that host digital photographs and images, online photo albums and digital photo exchanges.
Information Security	Sites that provide legitimate information about data protection, including newly discovered vulnerabilities and how to block them.
Instant Messaging	Sites that enable logging in to instant messaging services such as ICQ, AOL Instant Messenger, IRC, MSN, Jabber, Yahoo Messenger, and the like.
Peer-to-Peer	Sites that enable direct exchange of files between users without dependence on a central server.
Private IP Addresses	Sites that are private IP addresses as defined in RFC 1918, that is, hosts that do not require access to hosts in other enterprises (or require just limited access) and whose IP address may be ambiguous between enterprises but are well defined within a certain enterprise.
School Cheating	Sites that promote unethical practices such as cheating or plagiarism by providing test answers, written essays, research papers, or term papers.
Sex Education	Sites relating to sex education, including subjects such as respect for partner, abortion, gay and lesbian lifestyle, contraceptives, sexually transmitted diseases, and pregnancy.
Tasteless	Sites with offensive or tasteless content such as bathroom humor or profanity.
Child Abuse Images	Sites that portray or discuss children in sexual or other abusive acts.
Unknown	URLs unknown to the content filtering database.

Table 216 New Managed Category Descriptions (Firmware v4.55 or later)

CATEGORY	DESCRIPTION
Adult Topics	Web pages that contain content or themes that are generally considered unsuitable for children.
Alcohol	Web pages that mainly sell, promote, or advocate the use of alcohol, such as beer, wine, and liquor. This category also includes cocktail recipes and home-brewing instructions.

Table 216 New Managed Category Descriptions (Firmware v4.55 or later) (continued)

Anonymizing Utilities	Web pages that result in anonymous web browsing without the explicit intent to provide such a service. This category includes URL translators, web-page caching, and other utilities that might function as anonymizers, but without the express purpose of bypassing filtering software. This category does not include text translation.
Art Culture Heritage	Web pages that contain virtual art galleries, artist sites (including sculpture and photography), museums, ethnic customs, and country customs. This category does not include online photograph albums.
Auctions Classifieds	Web pages that provide online bidding and selling of items or services. This category includes web pages that focus on bidding and sales. This category does not include classified advertisements such as real estate postings, personal ads, or companies marketing their auctions.
Blogs Wiki	Web pages containing dynamic content, which often changes because users can post or edit content at any time. This category covers the risks with dynamic content that might range from harmless to offensive.
Business	Web pages that provide business-related information, such as corporate overviews or business planning and strategies. This category also includes information, services, or products that help other businesses plan, manage, and market their enterprises, and multi-level marketing. This category does not include personal pages and web-hosting web pages.
Chat	Web pages that provide web-based, real-time social messaging in public and private chat rooms. This category includes IRC. This category does not include instant messaging.
Computing Internet	Web pages containing reviews, information, buyer's guides of computers, computer parts and accessories, computer software and Internet companies, industry news and magazines, and pay-to-surf sites.
Consumer Protection	Websites that try to rob or cheat consumers. Some examples of their activities include selling counterfeit products, selling products that were originally provided for free, or improperly using the brand of another company. This category also includes sites where many consumers reported being cheated or not receiving services. This category does not include phishing, which tries to perpetrate fraud or theft by stealing account information.
Content Server	URLs for servers that host images, media files, or JavaScript for one or more sites and are intended to speed up content retrieval for existing web servers, such as Apache. This category includes domain-level and sub-domain-level URLs that function as content servers. This category does not include: • Web pages for businesses that provide the content servers • Web pages that allow users to browse photographs. See the Media Sharing category. • URLs for servers that serve only advertisements. See the Web Ads category.

Table 216 New Managed Category Descriptions (Firmware v4.55 or later) (continued)

Controversial Opinions	Web pages that contain opinions that are likely to offend political or social sensibilities and incite controversy. Much of this content is at the extremes of public opinion. This category does not include opinion or language clearly intended to promote hate or discrimination.
Cult Occult	Sites relating to non-traditional religious practices considered to be false, unorthodox, extremist, or coercive.
Dating Personals	Web pages that provide networking for online dating, matchmaking, escort services, or introductions to potential spouses. This category does not include sites that provide social networking that might include dating, but are not specific to dating.
Dating Social Networking	Web pages that focus on social interaction such as online dating, friendship, school reunions, pen-pals, escort services, or introductions to potential spouses. This category does not include wedding-related content, dating tips, or related marketing.
Digital Postcards	Web pages that allow people to send and receive digital postcards and greeting cards via the Internet.
Discrimination	Web pages, which provide information that explicitly encourages the oppression or discrimination of a specific group of individuals. This category does not include jokes and humor, unless the focus of the entire site is considered discriminatory.
Drugs	Websites that provide information on the purchase, manufacture, and use of illegal or recreational drugs. This category does not include sites with exclusive health or political themes.
Education Reference	Web pages devoted to academic-related content such as academic subjects (mathematics, history), school or university web pages, and education administration pages (school boards, teacher curriculum).
Entertainment	Web pages that provide information about cinema, theater, music, television, infotainment, entertainment industry gossip-news, and sites about celebrities such as actors and musicians. This category also includes sites where the content is devoted to providing entertainment on the web, such as horoscopes or fan clubs.
Extreme	Web pages that provide content considered gory, perverse, or horrific.
Fashion Beauty	Web pages that market clothing, cosmetics, jewelry, and other fashion-oriented products, accessories, or services. This category also includes product reviews, comparisons, and general consumer information, and services such as hair salons, tanning salons, tattoo studios, and body-piercing studios. This category does not include fashion-related content such as modeling or celebrity fashion unless the site focuses on marketing the product line.
Finance Banking	Web pages that provide financial information or access to online financial accounts. This category includes stock information (but not stock trading), home finance, and government-related financial information.
For Kids	Web pages that are family-safe, specifically for children of approximate ages ten and under. This category can also be used as an exception to allow web pages that do not pose a risk to children, or to access sites that have a primary educational or recreational focus for children, but are in other categories such as Games, Humor/Comics, Recreation/Hobbies, or Entertainment.

Table 216 New Managed Category Descriptions (Firmware v4.55 or later) (continued)

Forum Bulletin Boards	Web pages that provide access (http://) to Usenet newsgroups or hold discussions and post user-generated content, such as real-time message posting for an interest group. This category also includes archives of files uploaded to newsgroups. This category does not include message forums with a business or technical support focus.
Gambling	Web pages that allow users to wager or place bets online, or provide gambling software that allows online betting, such as casino games, betting pools, sports betting, and lotteries. This category does not include web pages related to gambling that do not allow betting online.
Gambling Related	Web pages that offer information about gambling, without providing the means to gamble. This category includes casino-related web pages that do not offer online gambling, gambling links, tips, sports picks, lottery results, and horse, car, or boat racing.
Game Cartoon Violence	Web pages that provide fantasy or fictitious representations of violence within the context of games, comics, cartoons, or graphic novels. This category includes images and textual descriptions of physical assaults or hand-to-hand combat, and grave injury and destruction caused by weapons or explosives.
Games	Web pages that offer online games and related information such as cheats, codes, demos, emulators, online contests or role-playing games, gaming clans, game manufacturer sites, fantasy or virtual sports leagues, and other gaming sites without chances of profit. This category includes gaming consoles.
General News	Web pages that provide online news media, such as international or regional news broadcasting and publication. This category includes portal sites that provide news content.
Government Military	Web pages that contain content maintained by governmental or military organizations, such as government branches or agencies, police departments, fire departments, civil defense, counter-terrorism organizations, or supranational organizations, such as the United Nations or the European Union. This category includes military and veterans' medical facilities.
Gruesome Content	Web pages with content that can be considered tasteless, gross, shocking, or gruesome. This category does not include web pages with content pertaining to physical assault.
Health	Web pages that cover all health-related information and health care services. This category does not include cosmetic surgery, marketing/selling pharmaceuticals, or animal-related medical services.
Historical Revisionism	Web pages that denounce, or offer different interpretations of, significant historical facts, such as holocaust denial. This category does not include all re-examination of historical facts, only historical events that are highly sensitive.
History	Web pages that provide content about historical facts. This category includes content suitable for higher education, but the Education category includes content for primary education. For example, a site with Holocaust photographs might be offensive, but have academic value.

Table 216 New Managed Category Descriptions (Firmware v4.55 or later) (continued)

Humor Comics	Web pages that provide comical or funny content. This category includes sites with jokes, sketches, comics, and satire pages. This category might also include graphic novel content, which is often associated with comics.
Illegal UK	Web pages that contain child sexual abuse content hosted anywhere in the world, and criminally obscene and incitement to racial hatred content hosted in the UK.
Incidental Nudity	Web pages that contain non-pornographic images of the bare human body like those in classic sculpture and paintings, or medical images. This category enables you to allow or block sites in order to address cultural or geographic differences in opinion about nudity. For example, you can use this category to block access to nudity, but allow access when nudity is not the primary focus of a site, such as news sites or major portals.
Information Security	Web pages that legitimately provide information about data protection. This category includes detailed information for safeguarding business or personal data, intellectual property, privacy, and infrastructure on the Internet, private networks, or in other bandwidth services such as telecommunications. This category does not include: • Legitimate information security companies and security software providers, such as virus protection companies. • Sites that intend to exploit security or teach how to bypass security.
Information Security New	Web pages that legitimately provide information about data protection. This category includes detailed information for safeguarding business or personal data, intellectual property, privacy, and infrastructure on the Internet, private networks, or in other bandwidth services such as telecommunications. This category does not include: • Legitimate information security companies and security software providers, such as virus protection companies. • Sites that intend to exploit security or teach how to bypass security.
Instant Messaging	Web pages that provide software for real-time communication over a network exclusively for users who joined a member's contact list or an instant-messaging session. Most instant-messaging software includes features such as file transfer, PC-to-PC phone calls, and can track when other people log on and off.
Interactive Web Applications	Web pages that provide access to live or interactive web applications, such as browser-based office suites and groupware. This category includes sites with business, academic, or individual focus. This category does not include sites providing access to interactive web applications that do not take critical user data or offer security risks, such as Google Maps.
Internet Radio TV	Web pages that provide software or access to continuous audio or video broadcasting, such as Internet radio, TV programming, or podcasting. Quick downloads and shorter streams that consume less bandwidth are in the Streaming Media or Media Downloads categories.
Internet Services	Web pages that provide services for publication and maintenance of Internet sites such as web design, domain registration, Internet Service Providers, and broadband and telecommunications companies that provide web services. This category includes web utilities such as statistics and access logs, and web graphics like clip art.

Table 216 New Managed Category Descriptions (Firmware v4.55 or later) (continued)

Job Search	Web pages related to a job search including sites concerned with resume writing, interviewing, changing careers, classified advertising, and large job databases. This category also includes corporate web pages that list job openings, salary comparison sites, temporary employment, and company job-posting sites. This category does not include make-money-at-home sites.
Major Global Religions	Web pages with content about religious topics and information related to major religions. This category includes sites that cover religious content such as discussion, beliefs, non-controversial commentary, articles, and information for local congregations such as a church or synagogue homepage. The religions in this category are Baha'i, Buddhism, Chinese Traditional, Christianity, Hinduism, Islam, Jainism, Judaism, Shinto, Sikhism, Tenrikyo, Zoroastrianism.
Marketing Merchandising	Web pages that promote individual or business products or services on the web, but do not sell their products or services online. This category includes websites that are generally a company overview, describing services or products that cannot be purchased directly from these sites. Examples include automobile manufacturer sites, wedding photography services, or graphic design services. This category does not include: • Other categories that imply marketing such as Alcohol, Auctions/Classifieds, Drugs, Finance/Banking, Mobile Phone, Online Shopping, Real Estate, School Cheating Information, Software/Hardware, Stock Trading, Tobacco, Travel, and Weapons. • Sites that market their services only to other businesses. See the Business category. • Sites that rob or cheat consumers. See the Consumer Protection category.
Media Downloads	Web pages that provide audio or video files for download such as MP3, WAV, AVI, and MPEG formats. The files are saved to, and played from, the user's computer. This category does not include audio or video files that are played directly through a browser window. See the Streaming Media category.
Media Sharing	Web pages that allow users to upload, search for, and share media files and photographs, such as online photograph albums.
Messaging	Examples include text messaging to mobile phones, PDAs, fax machines, and internal website user-to-user messaging or site-to-site messaging. This category does not include real-time chat or instant messaging, or message posts that can be viewed by anyone but the intended recipient.
Mobile Phone	Web pages that sell media, software, or utilities for mobile phones that can be downloaded and delivered to mobile phones. Examples include ringtones, logos/skins, games, screen-savers, text-based tunes, and software for SMS, MMS, WAP, and other mobile phone protocols.
Moderated	Bulletin boards, chat rooms, search engines, or web mail sites that are monitored by an individual or group who has the authority to block messages or content considered inappropriate. This category does not include sites with posted rules against offensive content. See the Forum/Bulletin Boards category.

Table 216 New Managed Category Descriptions (Firmware v4.55 or later) (continued)

Motor Vehicles	Websites for manufacturers and dealerships of consumer transportation vehicles, such as cars, vans, trucks, SUVs, motorcycles, and scooters. This category also includes sites that provide product marketing, reviews, comparisons, pricing information, auto fairs, auto expos, and general consumer information about motor vehicles. This category does not include automotive accessories, mechanics, auto-body shops, and recreational hobby pages. This category does not include sites that provide business-to-business-only content regarding motor vehicles.
Non Profit Advocacy NGO	Web pages from charitable or educational groups that fulfill a stated mission, benefiting the larger community, such as clubs, lobbies, communities, non-profit organizations, labor unions, and advocacy groups. Examples are Masons, Elks, Boy and Girl Scouts, or Big Brothers.
Nudity	Web pages that have non-pornographic images of the bare human body. This category includes classic sculpture and paintings, artistic nude photographs, some naturism pictures, and detailed medical illustrations. This category does not include high-profile sites where nudity is not a concern for visitors. See the Incidental Nudity category.
Online Shopping	Web pages that sell products or services online. Web pages selling a broad range of products might pose a risk to users by offering access to items that are normally in other categories such as Pornography, Weapons, Nudity, or Violence. Web pages selling such content exclusively are in their respective categories.
P2P File Sharing	Web pages that allow the exchange of files between computers and users for business or personal use, such as downloadable music. P2P clients allow users to search for and exchange files from a peer-user network. They often include spyware or real-time chat capabilities. This category includes BitTorrent web pages.
Parked Domain	Web pages that once served content, but their domains have been sold or abandoned and are no longer registered. Parked domains do not host their own content, but usually redirect users to a generic page that states the domain name is for sale, or redirect users to a generic search engine and portal page, some of which provide valid search engine results.
Personal Network Storage	Web pages that allow users to upload folders and files to an online network server in order to backup, share, edit, or retrieve files or folders from any web browser.
Personal Pages	Personal home pages that share a common domain such as those hosted by ISPs, university/education servers, or free web page hosts. This category also includes unique domains that contain personal information, such as a personal home page. This category does not include home pages of public figures.
Pharmacy	Web pages that provide reviews, descriptions, and market or sell prescription-based drugs, over-the-counter drugs, birth control, or dietary supplements.
Politics Opinion	Web pages covering political parties, individuals in political life, and opinion on various topics. This category might also cover laws and political opinion about drugs. This category includes URLs for political parties, political campaigning, and opinions on various topics, including political debates.
Pornography	Web pages, which provide materials intended to be sexually arousing or erotic. This category includes fetish pages, animation, cartoons, stories, and illegal pornography.

Table 216 New Managed Category Descriptions (Firmware v4.55 or later) (continued)

Portal Sites	Web pages that serve as major gateways or directories to content on the web. Many portal sites also provide a variety of internal site features or services such as search engines, email, news, and entertainment. Mailing list sites with a variety of content are in this category. This category does not include sites with topic-specific content.
Potential Criminal Activities	Web pages, which provide instructions to commit illegal or criminal activities. Instructions include committing murder or suicide, sabotage, bomb-making, lock-picking, service theft, evading law enforcement, or spoofing drug tests. This category might also include information on how to distribute illegal content, perpetrate fraud, or consumer scams. This category does not include computer-related fraud.
Potential Hacking Computer Crime	Web pages, which provide instructions, or otherwise enable, fraud, crime, or malicious activity that is computer-oriented. This category includes web pages related to computer crime include malicious hacking information or tools that help individuals gain unauthorized access to computers and networks (root kits, kiddy scripts). This category also includes other areas of electronic fraud such as dialer scams and illegal manipulation of electronic devices. This category does not include illegal software.
Potential Illegal Software	Web pages, which the filter believes offer information to potentially 'pirated' or illegally distribute software or electronic media, such as copyrighted music or film, distribution of illegal license key generators, software cracks, and serial numbers. This category does not include peer-to-peer web pages.
Private IP Addresses	Sites that are private IP addresses as defined in RFC 1918, that is, hosts that do not require access to hosts in other enterprises (or require just limited access) and whose IP address may be ambiguous between enterprises but are well defined within a certain enterprise.
Profanity	Web pages that contain crude, vulgar, or obscene language or gestures.
Professional Networking	Web pages that provide social networking exclusively for professional or business purposes. This category includes sites that provide personal or group profiles, and enable their members to interact through real-time communication, message posting, public bulletins, and media sharing. This category also contains alumni sites that have a networking function. This category does not include social networking sites where the focus might vary, but include friendship, dating, or professional focuses.
Provocative Attire	Web pages with pictures that include alluring or revealing attire, lingerie and swimsuits, or supermodel or celebrity photograph collections, but do not involve nudity. This category does not include sites with swimwear or similar attire that is not intended to be provocative. For example, Olympic swimming sites are not in this category.
Public Information	Web pages that provide general reference information such as public service providers, regional information, transportation schedules, maps, or weather reports.
PUPs	Web pages that contain Potentially Unwanted Programs (PUPs). PUPs are often made for a beneficial purpose but they alter the security of a computer or the computer user's privacy. Computer users who are concerned about security or privacy might want to be informed about this software, and in some cases, they might want to remove this software from their computers.

Table 216 New Managed Category Descriptions (Firmware v4.55 or later) (continued)

Real Estate	Web pages that provide commercial or residential real estate services and information. Service and information includes sales and rental of living space or retail space and guides for apartments, housing, and property, and information on appraisal and brokerage. This category includes sites that allow you to browse model homes. This category does not include content related to personal finance, such as credit applications.
Recreation Hobbies	Web pages for recreational organizations and facilities that include content devoted to recreational activities and hobbies. This category includes information about public swimming pools, zoos, fairs, festivals, amusement parks, recreation guides, hiking, fishing, bird watching, or stamp collecting. This category does not include activities that need no active participation, such as watching a movie or reading celebrity gossip.
Religion Ideology	Web pages with content related to religious topics and beliefs in human spirituality that are not within the major religions. This category includes religious discussion, beliefs, articles, and information for local congregations or groups such as a church homepage, unless the site is already in the Major Global Religions category. This category also includes comparative religion, or sites that include religions and ideologies. This category does not include astrology and horoscope sites
Remote Access	Web pages that provide remote access to a program, online service, or an entire computer system. Although remote access is often used legitimately to run a computer from a remote location, it creates a security risk, such as backdoor access. Backdoor access, written by the original programmer, allows the system to be controlled by another party without the user's knowledge.
Reserved	This category is reserved for future use.
Residential IP Addresses	IP addresses (and any domains associated with them) that access the Internet by DSL modems or cable modems. Because this content is not generally intended for Internet access via HTTP, access to the Internet through these IP addresses can indicate suspicious behavior. This behavior might be related to malware located on the home computer or homegrown gateways set up to allow anonymous Internet access.
Resource Sharing	Web pages that harness idle or unused computer resources to focus on a common task. The task can be on a company or an international basis. Well known examples are the SETI program and the Human Genome Project, which use the idle time of thousands of volunteered computers to analyze data.
Restaurants	Web pages that provide information about restaurants, bars, catering, take-out and delivery, including online ordering. This category includes sites that provide information about location, hours, prices, menus and related dietary information. This category also includes restaurant guides and reviews, and cafes and coffee shops. This category does not include groceries, wholesale food, non-profit and charitable food organizations, or bars that do not focus on serving food.
School Cheating Information	Web pages that promote plagiarism or cheating by providing free or fee-based term papers, written essays, or exam answers. This category does not include sites that offer student help, discuss literature, films, or books, or other content that is often the subject of research papers.

Table 216 New Managed Category Descriptions (Firmware v4.55 or later) (continued)

Search Engines	Web pages that provide search results that enable users to find information on the Internet based on key words. This category does not include site-specific search engines.
Sexual Materials	Web pages that describe or depict sexual acts, but are not intended to be arousing or erotic. Examples of sexual materials include sex education, sexual innuendo, humor, or sex related merchandise. This category does not include web pages with content intended to arouse.
Shareware Freeware	Web pages that are repositories of downloadable copies of shareware and freeware. This category does not include subscription-based software.
Social Networking	Web pages that enable social networking for a variety of purposes, such as friendship, dating, professional, or topics of interest. These sites provide personal or group profiles and enable interaction among their members through real-time communication, message posting, public bulletins, and media sharing. This category does not include sites that are exclusive to dating, matchmaking, or a specific professional networking focus.
Software Hardware	Web pages related to computing software and hardware, including vendors, product marketing and reviews, deployment and maintenance of software and hardware, and software updates and add-ons such as scripts, plug-ins, or drivers. Hardware includes computer parts, accessories, and electronic equipment used with computers and networks. This category includes the marketing of software and hardware, and magazines focused on software or hardware product reviews or industry trends.
Sports	Web pages related to professional or organized recreational sports. This category includes sporting news, events, and information such as playing tips, strategies, game scores, or player trades. This category does not include fantasy leagues, sports centers, athletic clubs, fitness or martial arts clubs, and non-league billiards, darts, or other such activities.
Stock Trading	Web pages that offer purchasing, selling, or trading of shares online. This category also includes ticker-tape information that enables viewing of real-time stock prices and financial spread betting in the stock market. Other betting is in the Gambling category. This category does not include sites that offer information about stocks, but do not offer purchasing, selling, or trading of shares.
Streaming Media	Web pages that provide streaming media, or contain software plug-ins for displaying audio and visual data before the entire file has been transmitted. This category does not include audio or video files that are downloaded to a user's computer before being played.
Technical Business Forums	Web pages with a technical or business focus that provide online message posting or real-time chatting, such as technical support or interactive business communication. Although users can post any type of content, these forums tend to present less risk of containing offensive content. Sites that offer a variety of forums with themes, including technical and business content, are only in the categories of Forum/Bulletin Boards or Chat.

Table 216 New Managed Category Descriptions (Firmware v4.55 or later) (continued)

Technical Information	Web pages that provide computing information with an educational focus in areas such as Information Technology, computer programming, and certification. Examples include Linux user groups, UNIX commands, software tutorials, or dictionaries of technical terms. Most sites in this category might be subdirectories of larger domains. For example, a software site with a tutorial page is in this category only at the tutorial page URL. This category does not include content about information security.
Text Spoken Only	Content that is text or audio only, and does not contain pictures. This category can be used as an exception to allow explicit text and recorded material to be accessed when you want pictures blocked using the Pornography, Violence, or Sexual Materials categories. Libraries or universities can use this category to prevent the display of offensive graphics in their public facilities.
Text Translators	Web pages that allow users to type phrases or a block of text to translate it from one language into another. This category also includes language identifier web pages. URL translation is in the Anonymizing Utilities category.
Tobacco	Web pages that sell, promote, or advocate the use of tobacco products, tobacco paraphernalia, including cigarettes, cigars, pipes, snuff and chewing tobacco.
Travel	Web pages that promote personal or business travel, such as hotels, resorts, airlines, ground transportation, car rentals, travel agencies, and general tourist and travel information. This category also includes sites for buying tickets or accommodation. This category does not include personal vacation photographs.
Usenet News	Web pages that provide access (http://) to Usenet newsgroups and archives of files uploaded to newsgroups. This category also includes online groups that offer similar community-oriented content posting.
Violence	Web pages that contain real or lifelike images or text that portray, describe, or advocate physical assaults against people, animals, or institutions, such as depictions of war, suicide, mutilation, or dismemberment.
Visual Search Engine	Web pages that provide image-specific search results such as thumbnail pictures. This category does not include sites that offer site-specific visual search engines.
Weapons	Web pages that provide information about buying, making, modifying, or using weapons, such as guns, knives, swords, paintball guns, and ammunition, explosives, and weapon accessories. This category also includes sites that contain content for: weapons for personal or military use, homemade weapons, non-lethal weapons such as mace, pepper spray, or Taser guns, weapons facilities, such as shooting ranges, and government or military oriented weapons. This category does not include political action groups, such as the NRA.
Web Ads	Web pages that provide advertisement-hosting or programs that create advertisements. Examples include links, source code or applets for banners, popups, and other kinds of static or dynamically generated advertisements that appear on web pages. This category is intended to block advertisements on web pages, not the companies that provide the advertisements or advertising services. This category does not include aggressive advertising adware. See the Spyware/ Adware category.
Web Mail	Web pages that enable users to send or receive email through the Internet.

Table 216 New Managed Category Descriptions (Firmware v4.55 or later) (continued)

Web Meetings	Web pages that host live meetings, video conferences, and interactive presentations mainly for businesses. Web meetings generally include streaming audio and video, and allow data transfer or office-oriented application sharing, such as online presentations.
Web Phone	Web pages that enable users to make telephone calls via the Internet or obtain information or software for this purpose. Web Phone service is also called Internet Telephony, or VoIP. Web phone service includes PC-to-PC, PC-to-phone, and phone-to-phone services connecting via TCP/IP networks.

43.8 Web Content Filter Example

This is an example of using the Zyxel Device to block access to a specific network service. A company wants to prevent its employees from using Facebook during their time in the office, but still allows access to other web pages, such as Office 365, Google, Wikipedia... The company wants to make sure any traffic going from the LAN to the Internet cannot access Facebook whether the traffic goes through the Zyxel Device or not.

Figure 35 Web Content Filter Example

Follow the steps below to block the Zyxel Device LAN users from accessing Facebook.

1 Create a web content filter profile named facebook_block.

```
Router# configure terminal
Router(config)# content-filter profile facebook_block
```

2 You then enter sub-command mode for the facebook_block profile to configure the web content filter profile's list of forbidden keywords.

```
Router(config)# content-filter profile facebook_block custom-list keyword
Router(Host)#
;      <cr>   exit   no     url    |
```

3 Enter *.facebook*.com to block access to websites with URLs that contain facebook. Use asterisks (*) as a wildcard to match any string in trusted and forbidden websites. Exit sub-command mode.

```
Router(Host)# url *.facebook*.com
Router(Host)# exit
```

4 To block traffic that goes through the Zyxel Device from the LAN to the Internet, you need to apply the web content filter profile facebook_block to the security policies LAN1_Outgoing and LAN2_Outgoing. Enter sub-command mode for configuring the security policy LAN1_Outgoing.

```
Router(config)# secure-policy 1
```

5 Apply the web content filter profile facebook_block to the security policies' web content filter profile. Set the log to log by-profile to generate a log for all traffic that matches criteria in the profile. Exit sub-command mode.

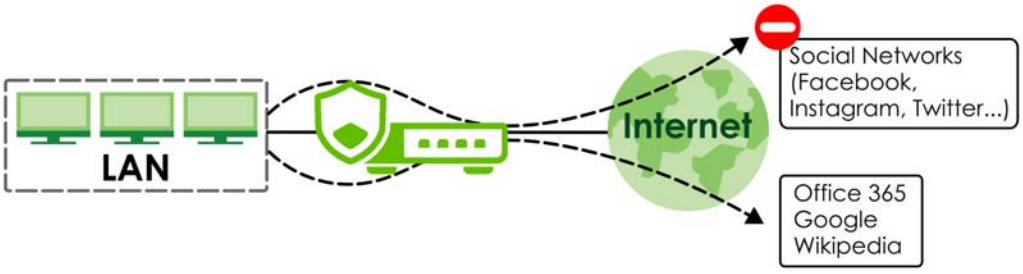
```
Router(secure-policy)# cf-profile
<profile name>
Router(secure-policy)# cf-profile facebook_block
log   no
Router(secure-policy)# cf-profile facebook_block log by-profile
activate     deactivate
Router(secure-policy)# cf-profile facebook_block log by-profile activate
Router(secure-policy)# exit
```

6 Repeat step 7 and step 8 to apply the web content filter profile facebook_block to the security policy LAN2_Outgoing.

43.9 DNS Content Filter Example

This is an example of using the Zyxel Device to block access to a specific network service. A company wants to prevent its employees from using social networks during their time in the office, such as Facebook, Instagram, Twitter... The company wants to make sure any traffic going from the LAN to the Internet cannot access social networks whether the traffic goes through the Zyxel Device or not.

Figure 36 DNS Content Filter Example



Follow the steps below to block the Zyxel Device LAN users from accessing social networks.

1 Create a DNS content filter profile named SocialNetworks.

```
Router# configure terminal
Router(config)# dns-content-filter profile SocialNetworks
```

2 You then enter sub-command mode for the SocialNetworks profile to configure the DNS content filter profile's forbidden categories. Sets the category to social-networking to block all social networks.

```
Router(config-dns-content-filter-profile-SocialNetworks)# category
adult-topics                      cult-occult                       forum-bulletin-
boards            illegal-uk                      media-sharing
pharmacy                          pups                              shareware-
freeware                usenet-news
alcohol                  dating-personals             gambling
incidental-nudity                 messaging                         politics-
opinion              real-estate                  social-networking
violence
anonymizing-utilities             dating-social-networking          gambling-
related              information-security           mobile-phone
pornography                       recreation-hobbies                software-
hardware                 visual-search-engine
art-culture-heritage              digital-postcards                 game-cartoon-
violence           information-security-new        moderated
portal-sites               religion-ideology            sports
weapons
auctions-classifieds         discrimination             games
instant-messaging                 motor-vehicles                    potential-
criminal-activities    remote-access                stock-trading
web-ads
blogs-wiki                  drugs                     general-news
interactive-web-applications      non-profit-advocacy-ngo           potential-
hacking-computer-crime  reserved                    streaming-media
web-mail
business                          education-reference               government-
military             internet-radio-tv              nudity
potential-illegal-software        residential-ip-addresses          technical-
business-forums          web-meetings
chat                              entertainment                     gruesome-
content              internet-services             online-shopping
private-ip-addresses              resource-sharing                  technical-
information              web-phone
computing-internet           extreme                   health
job-search                p2p-file-sharing            profanity
restaurants                       text-spoken-only
consumer-protection               fashion-beauty                    historical-
revisionism          major-global-religions         parked-domain
professional-networking           school-cheating-information       text-
translators
content-server              finance-banking             history
marketing-merchandising           personal-network-storage          provocative-
attire                 search-engines                    tobacco
controversial-opinions        for-kids                  humor-comics
media-downloads                   personal-pages                    public-
information                sexual-materials                 travel
Router(config-dns-content-filter-profile-SocialNetworks)# category social-
networking
```

3 Sets the action to redirect to redirect users that try to access FQDNs that are categorized as social networks. Sets the log to log to generate a log for all traffic that matches criteria in the profile. Exit sub-command mode.

```
Router(config-dns-content-filter-profile-SocialNetworks)# action redirect
Router(config-dns-content-filter-profile-SocialNetworks)# log
Router(Host)# exit
```

4 To block traffic that goes through the Zyxel Device from the LAN to the Internet, you need to apply the DNS content filter profile SocialNetworks to security policies LAN1_Outgoing and LAN2_Outgoing. Enter sub-command mode for configuring the security policy LAN1_Outgoing.

```
Router(config)# secure-policy 1
```

5 Apply the DNS content filter profile SocialNetworks to the security policies' DNS content filter profile. Set the log to log by-profile to generate a log for all traffic that matches criteria in the profile. Exit sub-command mode.

```
Router(secure-policy)# dns-cf-profile
<profile name>
Router(secure-policy)# dns-cf-profile SocialNetworks
log   no
Router(secure-policy)# dns-cf-profile SocialNetworks log by-profile
activate     deactivate
Router(secure-policy)# dns-cf-profile SocialNetworks log by-profile
activate
Router(secure-policy)# exit
```

6 Repeat step 7 and step 8 to apply the DNS content filter profile SocialNetworks to the security policy LAN2_Outgoing.

CHAPTER 44
Anti-Spam

44.1 Anti-Spam Overview

The anti-spam feature marks or discards spam. Activate the anti-spam subscription service for sender IP reputation checking, mail content analysis, and virus outbreak detection. Use the white list to identify legitimate e-mail. Use the black list to identify spam e-mail. You can also check e-mail against a DNS black list (DNSBL) of IP addresses of servers suspected of being used by spammers.

Note: From firmware version 4.60 onwards, the anti-spam provider is McAfee. This means some anti-spam commands changed in firmware versions 4.60 and later.

44.2 Anti-Spam Commands

The following table identifies the values used in some of these commands. Other input values are discussed with the corresponding commands.

Table 217 Input Values for General Anti-Spam Commands

LABEL	DESCRIPTION
xheader-name	The name (part that comes before the colon) of a field to add to an e-mail header. Use up to 16 ASCII characters.
xheader-value	The value (part that comes after the colon) of a field to add to an e-mail header. Use up to 16 ASCII characters.

44.2.1 Anti-Spam Profile Rules

The following table describes the commands for configuring the zone to zone rules. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 218 Commands for Anti-Spam Profile Rules

COMMAND	DESCRIPTION
`anti-spam profile append`	Enters the anti-spam sub-command mode to append a profile.
`anti-spam profile insert` *`rule_number`*	Enters the anti-spam sub-command mode to insert a profile.
`anti-spam profile` *`rule_number`*	Enters the anti-spam sub-command mode to edit the specified direction specific rule.
`[no] log [alert]`	Sets the Zyxel Device to create a log (and optionally an alert) when packets match this rule and are found to be spam. The `no` command sets the Zyxel Device not to create a log or alert when packets match this rule.
`[no] scan {smtp | pop3}`	Sets the protocols of traffic to scan for spam.

Table 218 Commands for Anti-Spam Profile Rules (continued)

COMMAND	DESCRIPTION
[no] match-action pop3 {forward | forward-with-tag}	Sets the action to take when the Zyxel Device detects a spam POP3 e-mail. The file can be forwarded or forwarded with a spam tag.
[no] match-action smtp {drop | forward | forward-with-tag}	Sets the action to take when the Zyxel Device detects a spam SMTP e-mail. The file can be deleted, forwarded, or forwarded with a spam tag.
[no] bypass {white-list | black-list | dnsbl}	Bypassing has the Zyxel Device not check files against your configured white (allowed) list, black (spam) list, or DNSBL servers list.
[no] bypass {ip-reputation | mail-content | virus-outbreak}	Firmware 4.55 or earlier Has the Zyxel Device not check mail's IP reputation, content, or for viruses.
[no] bypass mail-phishing	Firmware 4.60 or later Has the Zyxel Device not check emails for suspicious links.
show	Displays the details of the anti-spam rule you are configuring.
anti-spam profile move *rule_number* to *rule_number*	Moves an anti-spam profile to the number that you specified.
anti-spam profile delete *rule_number*	Removes an anti-spam profile.
show anti-spam profile [*rule_number*]	Displays the details of all the configured anti-spam profiles.
[no] anti-spam ip-reputation activate	Firmware 4.55 or earlier Sets whether or not to use IP reputation to identify spam by the sender's IP address.
anti-spam ip-reputation query-timeout time [*timeout*]	Firmware 4.55 or earlier Sets how many seconds the Zyxel Device waits for a reply when checking the IP reputation of a sender's IP address.
anti-spam ip-reputation statistics flush	Firmware 4.55 or earlier Clears the anti-spam statistics showing how many emails were detected as spam using the IP Reputation filter.
[no] anti-spam ip-reputation private-check activate	Firmware 4.55 or earlier Sets whether or not to check the IP reputation of private sender IP addresses.
[no] anti-spam mail-content activate	Firmware 4.55 or earlier Sets whether or not to identify spam by content, such as malicious content.
[no] anti-spam mail-phishing activate	Sets whether or not to identify emails sent from suspicious websites known for phishing.
anti-spam tag {mail-content | mail-phishing | virus-outbreak} [*tag*]	Firmware 4.55 or earlier Specifies the labels to add to the beginning of the mail subject if content-analysis identified it as spam, the e-mail has suspicious websites links or it contains a virus.
anti-spam tag mail-phishing [*tag*]	Firmware 4.60 or later Specifies the label to add to the beginning of an email subject if the email contains suspicious websites links.

Table 218 Commands for Anti-Spam Profile Rules (continued)

COMMAND	DESCRIPTION
`[no] anti-spam virus-outbreak activate`	Firmware 4.55 or earlier Sets whether or not to scan emails for attached viruses.
`anti-spam xheader {mail-content | virus-outbreak} xheader-name xheader-value`	Firmware 4.55 or earlier Specifies the name and value for the X-Header to add to content-analysis identified spam or e-mails containing a virus.
`no anti-spam xheader {mail-content | virus-outbreak}`	Firmware 4.55 or earlier The Zyxel Device does not add an X-header to content-analysis identified spam or e-mails containing a virus.
`anti-spam xheader mail-phishing xheader-name xheader-value`	Firmware 4.60 or later Specifies the name and value for the X-Header to emails containing suspicious websites links.
`no anti-spam xheader mail-phishing`	Firmware 4.60 or later The Zyxel Device does not add an X-header to content-analysis identified spam or e-mails containing a virus.
`anti-spam mail-scan query-timeout pop3 {forward | forward-with-tag}`	Selects how to handle POP3 mail if querying the mail scan server times out. Use `forward` to send it or `forward-with-tag` to add a tag to the mail subject and send it.
`anti-spam mail-scan query-timeout smtp {drop | forward | forward-with-tag}`	Selects how to handle SMTP mail if querying the mail scan server times out. Use `drop` to discard the SMTP mail, `forward` to send it, or `forward-with-tag` to add a tag to the mail subject and send it.
`anti-spam mail-phishing query-timeout smtp {drop | forward | forward-with-tag}`	Firmware 4.60 or later Selects how to handle SMTP mail if querying the mail phishing scan server times out. Use `drop` to discard the SMTP mail, `forward` to send it, or `forward-with-tag` to add a tag to the mail subject and send it.
`anti-spam mail-phishing query-timeout pop3 {forward | forward-with-tag}`	Firmware 4.60 or later Selects how to handle POP3 mail if querying the mail phishing scan server times out. Use `drop` to discard the POP3 mail, `forward` to send it, or `forward-with-tag` to add a tag to the mail subject and send it.
`anti-spam mail-phishing query-timeout time [timeout]`	Firmware 4.60 or later Sets how many seconds the Zyxel Device waits for a reply from the phishing scan server before taking the relevant timeout action.
`anti-spam mail-scan query-timeout time [timeout]`	Sets how many seconds the Zyxel Device waits for a reply from the mail scan server before taking the relevant timeout action.
`anti-spam tag query-timeout [tag]`	Specifies the label to add to the mail subject of e-mails the Zyxel Device tags and forwards when queries to the mail scan servers time out.
`[no] anti-spam xheader query-timeout xheader-name xheader-value`	Specifies the name and value for the X-Header to add to e-mails the Zyxel Device forwards when queries to the mail scan servers time out.
`show anti-spam ip-reputation query-timeout time`	Firmware 4.55 or earlier Displays how many seconds the Zyxel Device waits for a reply when checking the IP reputation of a sender's IP address.

Table 218 Commands for Anti-Spam Profile Rules (continued)

COMMAND	DESCRIPTION
`show anti-spam ip-reputation private-check`	Firmware 4.55 or earlier Displays the setting for checking the IP reputation of private sender IP addresses.
`show anti-spam ip-reputation high-sensitivity`	Firmware 4.55 or earlier Displays whether IP reputation high sensitivity mode is enabled or not.
`show anti-spam mail-scan query-timeout smtp`	Displays the action the Zyxel Device takes on SMTP mail if querying the mail scan server times out.
`show anti-spam mail-scan query-timeout pop3`	Displays the action the Zyxel Device takes on POP3 mail if querying the mail scan server times out.
`show anti-spam mail-scan query-timeout time`	Displays how many seconds the Zyxel Device waits for a reply from the mail scan server before taking the relevant timeout action.
`show anti-spam mail-phishing query-timeout smtp`	Firmware 4.60 or later Displays the action the Zyxel Device takes on SMTP mail if querying the phishing scan server times out.
`show anti-spam mail-phishing query-timeout pop3`	Firmware 4.60 or later Displays the action the Zyxel Device takes on POP3 mail if querying the phishing scan server times out.
`show anti-spam mail-phishing query-timeout time`	Firmware 4.60 or later Displays how many seconds the Zyxel Device waits for a reply from the phishing scan server before taking the relevant timeout action.
`show anti-spam mail-scan status`	Firmware 4.55 or earlier Displays the Zyxel Device's settings for IP reputation, mail content, and virus outbreak checking.
`show anti-spam mail-phishing status`	Firmware 4.60 or later Displays whether the Zyxel Device scans emails for suspicious websites links.
`show anti-spam tag {mail-content | mail-phishing | virus-outbreak}`	Firmware 4.55 or earlier Displays the labels for content-analysis identified spam, e-mails that have suspicious websites links or emails containing a virus.
`show anti-spam tag mail-phishing`	Firmware 4.60 or later Displays the labels for content-analysis identified emails containing suspicious websites links.
`show anti-spam tag query-timeout`	Displays the label the Zyxel Device adds to the mail subject of e-mails that it tags and forwards when queries to the mail scan servers time out.
`show anti-spam xheader {mail-content | mail-phishing | virus-outbreak}`	Firmware 4.55 or earlier Displays the name and value for the X-Header to add to content-analysis identified spam, e-mails containing suspicious websites links or e-mails containing a virus.
`show anti-spam xheader mail-phishing`	Firmware 4.60 or later Displays the name and value for the X-Header to add to content-analysis identified e-mails containing suspicious websites links.

Table 218 Commands for Anti-Spam Profile Rules (continued)

COMMAND	DESCRIPTION
`show anti-spam xheader query-timeout`	Displays the name and value for the X-Header the Zyxel Device adds to e-mails that it tags and forwards when queries to the mail scan servers time out.
`[no] security-service anti-spam activate`	Turns on anti-spam/email security on the Zyxel Device. The no command disables anti-spam/email security.
`security-service anti-spam inspect {all-traffic | by-policy}`	Sets how the security service inspects traffic. *all-traffic*: The security service inspects all traffic passing through the Zyxel Device. *by-policy*: The security service inspects traffic only when its profile is bound to a security policy. For information on binding a security service profile to a security policy, see Section 29.2.1 on page 221.
`show security-service status`	Displays whether the security services are enabled on the Zyxel Device.

44.2.1.1 Anti-Spam Profile Example

This example shows how to configure (and display) a WAN to DMZ anti-spam profile to scan POP3 and SMTP traffic. SMTP spam is forwarded. POP3 spam is marked with a spam tag. The Zyxel Device logs the event when an e-mail matches the DNSBL (see Section 44.2.3 on page 406 for more on DNSBL). The white and black lists are ignored.

```
Router(config)# anti-spam 1
Router(config-as-rule-1)# activate
Router(config-as-rule-1)# scan smtp
Router(config-as-rule-1)# scan pop3
Router(config-as-rule-1)# match-action smtp forward
Router(config-as-rule-1)# match-action pop3 forward-with-tag
Router(config-as-rule-1)# log
Router(config-as-rule-1)# bypass white-list
Router(config-as-rule-1)# bypass black-list
Router(config-as-rule-1)# exit
Router(config)# show anti-spam 1
Anti-Spam Rule: 1
  profile name: AS_profile_default_SXI
  description:
  log: log
  scan protocols:
    smtp: yes
    pop3: yes
  match action:
    smtp: forward-with-tag
    pop3: forward-with-tag
  bypass white list: no
  bypass black list: no
  bypass ip reputation: no
  bypass mail content: no
  bypass virus outbreak: no
  bypass dnsbl: no
  ref: 0
```

44.2.2 White and Black Lists

The following table identifies values used in these commands. Other input values are discussed with the corresponding commands.

Table 219 Input Values for White and Black list Anti-Spam Commands

LABEL	DESCRIPTION
mail_header	The name part of an e-mail header (the part that comes before the colon). Use up to 63 ASCII characters. For example, if you want the entry to check the "Received:" header for a specific mail server's domain, use "Received".
mail_header_value	The value part of an e-mail header (the part that comes after the colon). Use up to 63 ASCII characters. For example, if you want the entry to check the "Received:" header for a specific mail server's domain, specify the mail server's domain. See Section 44.2.2.2 on page 406 for more details.
rule_number	The index number of an anti-spam white or black list entry. 1 - *X* where *X* is the highest number of entries the Zyxel Device model supports. See the Zyxel Device's User's Guide for details.
subject	A keyword in the content of the e-mail Subject headers. Use up to 63 ASCII characters. Spaces are not allowed, although you could substitute a question mark (?). See Section 44.2.2.2 on page 406 for more details.

Use the white list to identify legitimate e-mail and the black list to identify spam e-mail. The following table describes the commands for configuring the white list and black list. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 220 Commands for Anti-Spam White and Black Lists

COMMAND	DESCRIPTION
`[no] anti-spam white-list activate`	Turns the white list checking on or off. Turn on the white list to forward e-mail that matches (an active) white list entry without doing any more anti-spam checking on that individual e-mail.
`[no] anti-spam white-list [`*rule_number*`] ip-address` *ip subnet_mask* `{activate|deactivate}`	Adds, edits, or removes a white list entry to check e-mail for a specific source or relay IPv4 address. Also turns the entry on or off.
`[no] anti-spam white-list [rule_number] ip6-address ipv6_subnet {activate|deactivate}`	Adds, edits, or removes a white list entry to check e-mail for a specific source or relay IPv6 address. Also turns the entry on or off.
`[no] anti-spam white-list [`*rule_number*`] e-mail` *email* `{activate|deactivate}`	Adds, edits, or removes a white list entry to check e-mail for a specific source e-mail address or domain name. Also turns the entry on or off.
`[no] anti-spam white-list [`*rule_number*`] mail-header` *mail-header mail-header-value* `{activate|deactivate}`	Adds, edits, or removes a white list entry to check e-mail for specific header fields and values. Also turns the entry on or off.
`[no] anti-spam white-list [`*rule_number*`] subject` *subject* `{activate|deactivate}`	Adds, edits, or removes a white list entry to check e-mail for specific content in the subject line. Also turns the entry on or off.
`[no] anti-spam black-list activate`	Turns the black list checking on or off. Turn on the black list to treat e-mail that matches (an active) black list entry as spam.

Table 220 Commands for Anti-Spam White and Black Lists (continued)

COMMAND	DESCRIPTION
`[no] anti-spam black-list [rule_number] ip-address ip subnet_mask {activate|deactivate}`	Adds, edits, or removes a black list entry to check e-mail for a specific source or relay IPv4 address. Also turns the entry on or off.
`[no] anti-spam black-list [rule_number] ip6-address ipv6_subnet {activate|deactivate}`	Adds, edits, or removes a black list entry to check e-mail for a specific source or relay IPv6 address. Also turns the entry on or off.
`[no] anti-spam black-list [rule_number] e-mail email {activate|deactivate}`	Adds, edits, or removes a black list entry to check e-mail for a specific source e-mail address or domain name. Also turns the entry on or off.
`[no] anti-spam black-list [rule_number] mail-header mail-header mail-header-value {activate|deactivate}`	Adds, edits, or removes a black list entry to check e-mail for specific header fields and values. Also turns the entry on or off.
`[no] anti-spam black-list [rule_number] subject subject {activate|deactivate}`	Adds, edits, or removes a black list entry to check e-mail for specific content in the subject line. Also turns the entry on or off.
`anti-spam tag black-list [tag]`	Configures a message or label (up to 15 ASCII characters) to add to the mail subject of e-mails that match an anti-spam black list entry.
`show anti-spam white-list [status]`	Displays the current anti-spam white list. Use `status` to show the activation status only.
`show anti-spam black-list [status]`	Displays the current anti-spam black list. Use `status` to show the activation status only.
`show anti-spam tag black-list`	Shows the configured anti-spam black list tag.
`[no] anti-spam xheader {white-list | black-list} mail-header mail-header-value`	Specifies the name and value for the X-Header to add to e-mails that match the Zyxel Device's spam white list or black list.
`show anti-spam xheader {white-list | black-list}`	Displays the name and value for the X-Header to add to e-mails that match the Zyxel Device's spam white list or black list.

44.2.2.1 White and Black Lists Example

This example shows how to configure and enable a white list entries for e-mails with “testwhite” in the subject, e-mails from whitelist@ourcompany.com, e-mails with the Date header set to 2007, and e-mails from (or forwarded by) IP address 192.168.1.0 with subnet 255.255.255.0.

```
Router(config)# anti-spam white-list subject testwhite activate
Router(config)# anti-spam white-list e-mail whitelist@ourcompany.com
activate
Router(config)# anti-spam white-list mail-header Date 2007 activate
Router(config)# anti-spam white-list ip-address 192.168.1.0 255.255.255.0
activate
Router(config)# show anti-spam white-list
No.   Type        Status
Content
================================================================================
1     subject     yes
testwhite
2     e-mail      yes
whitelist@ourcompany.com
3     mail-header yes
Date : 2007
4     ip-address  yes
192.168.1.0 / 255.255.255.0
```

44.2.2.2 Regular Expressions in Black or White List Entries

The following applies for a black or white list entry based on an e-mail subject, e-mail address, or e-mail header value.

- Use a question mark (?) to let a single character vary. For example, use “a?c” (without the quotation marks) to specify abc, acc and so on.
- You can also use a wildcard (*). For example, if you configure *def.com, any e-mail address that ends in def.com matches. So “mail.def.com” matches.
- The wildcard can be anywhere in the text string and you can use more than one wildcard. You cannot use two wildcards side by side, there must be other characters between them.
- The Zyxel Device checks the first header with the name you specified in the entry. So if the e-mail has more than one “Received” header, the Zyxel Device checks the first one.

44.2.3 DNSBL Anti-Spam Commands

This section describes the commands for checking the sender and relay IP addresses in e-mail headers against DNS (Domain Name Service)-based spam Black Lists (DNSBLs). You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 221 Input Values for DNSBL Commands

LABEL	DESCRIPTION
dnsbl_domain	A domain that is maintaining a DNSBL. You may use 0-254 alphanumeric characters, or dashes (-).

This table describes the DNSBL commands.

Table 222 DNSBL Commands

COMMAND	DESCRIPTION
`[no] anti-spam dnsbl activate`	Turns DNSBL checking on or off.
`anti-spam dnsbl [1..5] domain` *`dnsbl_domain`* `{activate|deactivate}`	Adds or edits a DNSBL domain for checking e-mail header IP addresses.
`no anti-spam dnsbl domain` *`dnsbl_domain`*	Removes the specified DNSBL domain.
`anti-spam dnsbl query-timeout smtp {drop | forward | forward-with-tag}`	Sets how the Zyxel Device handles SMTP mail (mail going to an e-mail server) if the queries to the DNSBL domains time out.
`anti-spam dnsbl query-timeout pop3 {forward | forward-with-tag}`	Sets how the Zyxel Device handles POP3 mail (mail coming to an e-mail client) if the queries to the DNSBL domains time out.
`anti-spam dnsbl max-query-ip [1..5]`	Sets up to how many sender and relay server IP addresses in the mail header to check against the DNSBL.
`anti-spam dnsbl ip-check-order {forward | backward}`	Configures the order in which anti-spam checks e-mail header IP addresses against the DNSBLs. • `forward` checks the first N IP addresses. Checking starts from the first IP address in the mail header. This is the IP of the sender or the first server that forwarded the mail. • `backward` checks the last N IP addresses. Checking starts from the last IP address in the mail header. This is the IP of the last server that forwarded the mail.
`anti-spam tag {dnsbl | dnsbl-timeout}` [*`tag`*]	`dnsbl` configures the message or label to add to the beginning of the mail subject of e-mails that have a sender or relay IP address in the header that matches a black list maintained by a DNSBL domain listed in the Zyxel Device. `dnsbl-timeout` configures the message or label to add to the mail subject of e-mails that the Zyxel Device forwards if queries to the DNSBL domains time out. Use up to 15 alphanumeric characters, underscores (_), colons (:), or dashes (-).
`show anti-spam dnsbl status`	Displays the activation status of the anti-spam DNSBL checking.
`show anti-spam dnsbl domain`	Displays the Zyxel Device's configured anti-spam DNSBL domain entries.
`show anti-spam dnsbl max-query-ip`	Displays how many sender and relay server IP addresses in the mail header anti-spam checks against the DNSBL.
`show anti-spam dnsbl ip-check-order`	Displays the order in which anti-spam checks e-mail header IP addresses against the DNSBLs.
`show anti-spam dnsbl query-timeout {smtp | pop3}`	Displays how the Zyxel Device handles SMTP or POP3 mail if the queries to the DNSBL domains time out.
`show anti-spam tag {dnsbl | dnsbl-timeout}`	`dnsbl` displays the anti-spam tag for e-mails that have a sender or relay IP address in the header that matches a black list maintained by a DNSBL domain. `dnsbl-timeout` displays the message or label to add to the mail subject of e-mails that the Zyxel Device forwards if queries to the DNSBL domains time out.
`show anti-spam dnsbl statistics`	Displays anti-spam DNSBL statistics for each configured DNSBL domain.
`anti-spam dnsbl statistics flush`	Clears the anti-spam DNSBL statistics for each configured DNSBL domain.

Table 222 DNSBL Commands

COMMAND	DESCRIPTION
`anti-spam dnsbl query-timeout time [1..10]`	Sets how long the Zyxel Device waits for a reply from the DNSBL domains.
`show anti-spam dnsbl query-timeout time`	Displays how long the Zyxel Device waits for a reply from the DNSBL domains.
`[no] anti-spam xheader dnsbl` *`mail-header mail-header-value`*	Specify the name and value for the X-Header to add to e-mails with a sender or relay IP address in the header that matches a black list maintained by a DNSBL domain in the Zyxel Device's list
`show anti-spam xheader dnsbl`	Display the name and value for the X-Header to add to e-mails with a sender or relay IP address in the header that matches a black list maintained by a DNSBL domain in the Zyxel Device's list

44.2.3.1 DNSBL Example

This example:

- Sets the Zyxel Device to use "DNSBL-example.com" as a DNSBL.
- Turns DNSBL checking on.
- Sets the Zyxel Device to forward POP3 mail with a tag if the queries to the DNSBL domains time out.
- Sets the Zyxel Device to check up to 4 sender and relay server IP addresses in e-mail headers against the DNSBL.
- Sets the Zyxel Device to start DNSBL checking from the first IP address in the mail header.
- Sets the DNSBL tag to "DNSBL".
- Sets the DNSBL timeout tag to "DNSBL-timeout".

- Displays the DNSBL statistics.

```
Router(config)# anti-spam dnsbl domain DNSBL-example.com activate
Router(config)# show anti-spam dnsbl domain
No.   Status
Domain
================================================================================
1     yes
DNSBL-example.com
Router(config)# anti-spam dnsbl activate
Router(config)# show anti-spam  dnsbl status
anti-spam dnsbl status: yes
Router(config)# anti-spam dnsbl query-timeout pop3 forward-with-tag
Router(config)# show anti-spam  dnsbl query-timeout pop3
dnsbl query timeout action: forward-with-tag
Router(config)# anti-spam dnsbl max-query-ip 4
Router(config)# show anti-spam  dnsbl max-query-ip
dnsbl max query ip: 4
Router(config)# anti-spam dnsbl ip-check-order forward
Router(config)# show anti-spam  dnsbl ip-check-order
anti-spam dnsbl IP check order: forward
Router(config)# anti-spam tag dnsbl DNSBL
Router(config)# show anti-spam tag dnsbl
dnsbl tag: DNSBL
Router(config)# anti-spam tag dnsbl-timeout DNSBL-timeout
Router(config)# show anti-spam tag dnsbl-timeout
dnsbl-timeout tag: DNSBL-timeout
Router(config)# show anti-spam dnsbl statistics
DNSBL domain: 1
  domain: DNSBL-example.com
  average time: 0.00
  total query: 0
    spam: 0
    clear: 0
    no timeout: 0
    timeout: 0
    no response: 0
```

44.3 Anti-Spam Statistics

The following table describes the commands for collecting and displaying anti-spam statistics. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 223 Commands for Anti-Spam Statistics

COMMAND	DESCRIPTION
`[no] anti-spam statistics collect`	Turn the collection of anti-spam statistics on or off.
`anti-spam statistics flush`	Clears the collected statistics.
`show anti-spam statistics summary`	Displays an overview of the collected statistics.
`show anti-spam statistics collect`	Displays whether the collection of anti-spam statistics is turned on or off.

Table 223 Commands for Anti-Spam Statistics (continued)

COMMAND	DESCRIPTION
`show anti-spam statistics ranking {source | mail-address}`	Query and sort the anti-spam statistics entries by source IP address or mail address. `source`: lists the source IP addresses of the most spam. `mail-address`: lists the most common source mail address for spam.
`show anti-spam ip-reputation statistics`	Firmware 4.55 or earlier Displays the mail sender IP reputation checking statistics.
`show anti-spam mail-scan statistics`	Displays the mail scan statistics.

44.3.1 Anti-Spam Statistics Example

This example shows how to collect anti-spam statistics and display a summary.

```
Router(config)# anti-spam statistics collect
Router(config)# show anti-spam statistics collect
collect statistics: yes
collect statistics time: since 2008-03-11 07:16:01 to 2008-03-11 07:16:13
Router(config)# show anti-spam statistics summary
total mails scanned: 0
total clear mails: 0
clear mail by whitelist: 0
total spam mails: 0
spam detected by blacklist: 0
spam detected by ip reputation: 0
spam detected by mail content: 0
spam detected by dnsbl: 0
spam detected with virus: 0
total virus mails: 0
dnsbl timeout: 0
mail session forwarded: 0
mail session dropped: 0
```

CHAPTER 45
Collaborative Detection & Response

45.1 Overview

Collaborative Detection & Response (CDR) allows you to detect wired and WiFi clients that are sending malicious traffic in your network and then block or quarantine traffic coming from them. In this way, malicious traffic is not spread throughout the network. Secure policies can block malicious traffic for specific traffic flows, but CDR can block malicious traffic from the sender. Malicious traffic is identified using a combination of Web Filtering, Anti-Malware and IPS (IDP) signatures.

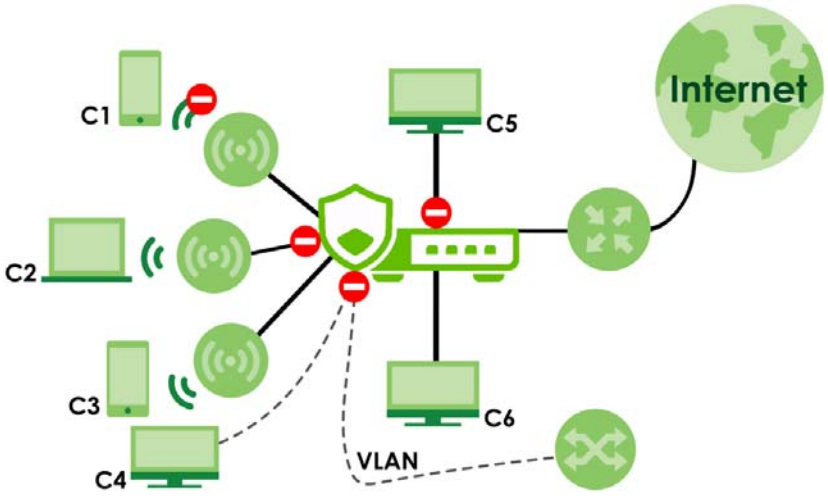
45.1.1 CDR Example Scenario

In the following example scenario, clients C1 to C6 are connected to the network. Intrusion Prevention (IPS) or Anti-Malware signatures have identified malicious traffic coming from clients C1, C2, C4 and C5.

You have configured CDR to take the following actions:

- Traffic from WiFi client C1 is blocked at the AP.
- Traffic from WiFi client C2 is blocked at the Zyxel Device.
- Traffic from wired client C5 is blocked at the Zyxel Device. This traffic can still be broadcast to other clients in the same subnet, such as C6.
- Traffic from WiFi client C4 is isolated from the network through a quarantine VLAN. Quarantined traffic in a VLAN isolates traffic from other clients in the same subnet, and only broadcasts to other clients in that same VLAN.

Figure 37 CDR Example Scenario



This the graphic key.

Table 224 CDR Example Scenario Graphic Key

LABEL	DEFINITION
C1 to C4	WiFi clients
C5 to C6	Wired clients
VLAN	VLAN configured to isolate traffic from a quarantined client

45.2 Before You Begin

- You must have active and up-to-date Web Filtering, Anti-Malware, IPS (Intrusion Prevention System), and CDR (Collaborative Detection & Response) licenses.
- Malicious traffic is detected in two phases.
  - Web Filtering (URL Threat Filtering), Anti-Malware (Anti-Virus) and IPS (IDP) signatures first identify malicious traffic and inform the CDR daemon. If these licenses have expired or are not active, then no checking for malicious traffic is done.
  - CDR signatures are a subset of the above license signatures. If a specific number of signature matches are detected within a defined time period, then the CDR containment policy is triggered. These are the signatures that apply to CDR at the time of writing:

Table 225 Security Signatures Applied to CDR

SECURITY SIGNATURES	SIGNATURES APPLIED TO CDR
Web Filtering	URL Threat Filter Categories: Browser Exploits, Malicious Downloads, Malicious Sites, Phishing
IPS	IDP Signatures: • CVE-2019-0708 (117760, 130797, 130801) • CVE-2020-0796(130822,130823,130824,130825) • 117723, 117724, 117726
Anti-Malware	All signatures

- Blocking traffic from an infected client causes the Zyxel Device to drop all traffic received from the client. This traffic can still be broadcast to other clients in the same subnet as the infected client.
- Blocking traffic from an infected WiFi client causes the AP it is connected with to drop all traffic received from the client if you run command `cdr block block-wireless-client`.
- The Zyxel Device can only block traffic from Nebula-managed APs in your network using CDR.
- Quarantining traffic from an infected WiFi client blocks traffic at the Zyxel Device or AP and also isolates traffic from other clients in the same subnet. Traffic from the infected WiFi is only broadcast to other clients in the quarantine VLAN. You must configure the quarantine VLAN on the Zyxel Device and any switches or routers in your network through which you want to route the VLAN traffic.
- There are 2 requirements to block or quarantine WiFi clients:
  - The AP must be managed by the Zyxel Device.
  - The AP must be in the Zyxel Device's supported list. At the time of writing, there are 5 supported AP models:

Table 226 Zyxel Device Managed APs

MANAGED AP MODELS
• WAX650S
• WAX610D

Table 226 Zyxel Device Managed APs

MANAGED AP MODELS
• WAX510D
• WAC500
• WAC500H

Note: Please see your AP product page at the Zyxel web site to see if it can be managed by the Zyxel Device.

- You must decide how long to contain (block or quarantine) a suspect client, before allowing traffic to be sent from it again. This will depend on how quickly you can contact the owner of the suspect client and how long they need to remove the malicious software from their device.
- You must also decide if there are trusted clients in your network that are exempt from CDR and never have their traffic blocked or quarantined.
- You can use the`cdr unblock` commands to prematurely release a blocked or quarantined client, and the `cdr white-list commands` to add a client to a list exempt from CDR checking.
- If you disable CDR or your CDR license expires, then all blocked and quarantined clients are released.
- If you restart the Zyxel Device or restart an AP connected to the Zyxel Device, blocked and quarantined clients are still blocked until the block or quarantine period expires.

45.3 CDR Commands

The following describes the commands for CDR.

45.3.1 CDR General Commands

This table shows the commands for activating and configuring CDR..

Table 227 CDR General Commands

COMMAND	DESCRIPTION
`[no] cdr activate`	Enables CDR on the Zyxel Device. The no command disables CDR.
`[no] cdr counter-reset activate`	Enables CDR counter reset to automatically reset the number of security occurrences within the defined duration when it reaches the threshold value so as to reduce alert emails. For example, if you set the CDR settings for a security event as below: • Occurrence: 10 • Duration: 60 • Containment: Alert • Counter Reset: Enable You will only receive one alert email every hour if the security event hit count reaches ten times within 60 minutes. The no command disables CDR counter reset.
`[no] cdr block block-wireless-client`	Has traffic from the suspect client blocked at the AP. Use the no command to have traffic from the suspect client blocked at the Zyxel Device.

Table 227 CDR General Commands

COMMAND	DESCRIPTION
`cdr block http-service-port <1..65535>`	Changes the port number of the CDR HTTP blocking page.
`cdr block https-service-port <1..65535>`	Changes the port number of the CDR HTTPS blocking page.
`cdr block message denied_message`	Sets the message that is displayed on the default Zyxel Device notification page. The client is redirected here when a Block or Quarantine action is triggered. The message must be less than 127 characters.
`cdr block period <0..1440>`	Sets how long the client is blocked after a block action is triggered. 0 means the client is blocked forever. This should be at least twice the DHCP server lease time, in order to prevent false positives.
`cdr block redirect <url>`	Sets a URL in “http://domain” or “https://domain” format to an external notification page. The client is redirected here when a Block or Quarantine action is triggered. Make sure the external notification page is accessible from the Zyxel Device.
`cdr block url {message|redirect}`	Sets the notification web page that is displayed when a Block or Quarantine action is triggered. • message: The Zyxel Device displays the default Zyxel Device notification page, with a message set by command `cdr block message`. • redirect: The Zyxel Device displays a custom external notification page, set by command cdr block redirect.
`cdr blocked-by {ip|mac}`	Sets how CDR blocks suspected clients after a block or quanratine action is triggered. • IP: The suspect client’s IP address is blocked. However, the suspected client can access network resources again if it changes IP addresses, for example by picking up a new DHCP lease. • MAC: The suspect client’s MAC address is blocked. However, the suspected client can access network resources again if it changes MAC address, for example by using a different source Ethernet port. Note: If you have a switch between the client and the Zyxel Device, then blocking by MAC address could block all traffic from the switch if the client MAC address is not forwarded through the switch.
`cdr quarantine period <0..1440>`	Sets how long the client is quarantined after a quarantine action is triggered. 0 means the client is quarantined forever.
`cdr quarantine vlan-id <1..4094>`	Sets a previously configured VLAN as the quarantine VLAN. When a client is quarantined, the client’s traffic is isolated and is broadcast only to members in the VLAN.

Table 227 CDR General Commands

COMMAND	DESCRIPTION
`cdr rule rule_id threshold occurence duration duration action {alert| block| quarantine| block-alert| quarantine-alert}`	Edits a CDR policy with the following values: • rule_id: The category of the policy. At the time of writing, 1 = Malware, 2 = IDP, 3 = Web Threat. • Occurrence: The number of security events that need to occur within the defined Duration to trigger a CDR containment action. The valid range is 1 to 100. • Duration: The length of time, in minutes, that events needs to occur within the Occurrence number of times in order to trigger a CDR containment action. The valid range is 1 to 1440. • Action: The action to be taken when the number of security events exceed the threshold within the defined duration. A suspect client is the wired or WiFi device that is sending malicious traffic in your network. A suspect client owner is the person who owns the wired or WiFi device that is sending malicious traffic in your network. - Alert: Send an email to the suspect client owner or Zyxel Device admin. Please note that traffic from the suspect client will not be blocked when this action is triggered. - Block: Block traffic from a suspect client at the Zyxel Device, or from a suspect WiFi client at the AP connected to the Zyxel Device. Please note that no alert will be sent to the suspect client owner when the suspect client is blocked. Traffic is still broadcast to other clients in the same subnet. A 'notification' web page is displayed when this action is triggered. - Quarantine: Isolate traffic from a suspect client at the Zyxel Device in a quarantine VLAN. Please note that no alert will be sent to the suspect client owner when the suspect client is blocked. Traffic is not broadcast to other clients in the same subnet. A 'notification' web page is displayed to the client when this action is triggered. - Block-Alert: Use this command if you want to both Block and Alert. - Quarantine-Alert: Use this command if you want to both Quarantine and Alert.
`cdr send-alerts-to email_address`	Sets an email address in the user@domain.com format of the owner of the suspect client or another person who should be informed that a CDR action was triggered.
`cdr unblock ipv4 ip_address`	Unblocks an IP address that is currently being blocked or quarantined. This removes the address from the CDR containment list.
`cdr unblock mac mac_address`	Unblocks an MAC address that is currently being blocked or quarantined. This removes the address from the CDR containment list.
`[no] cdr white-list ipv4 ip_address`	Adds the IPv4 address to the exempt list. CDR will check traffic sent from the IP address and always flag it as PASS. The no command removes the IP address from the whitelist.
`[no] cdr white-list mac mac_address`	Adds the MAC address to the exempt list. CDR will check traffic sent from the MAC address and always flag it as PASS. The no command removes the MAC address from the whitelist.
`cdr white-list replace <1..512> ipv4 ip_address`	Replaces the numbered entry in the whitelist with the specified IPv4 address.
`cdr white-list replace <1..512> mac mac_address`	Replaces the numbered entry in the whitelist with the specified MAC address.

45.3.2 CDR Show Commands

This table shows the commands for showing CDR settings..

Table 228 CDR Show Activation

COMMAND	DESCRIPTION
`show cdr block-list`	Displays the CDR containment list. This list contains all devices currently being blocked or quarantined.
`show cdr event-list`	Displays the CDR event (history) list. This list contains up to 1024 devices that were previously blocked, quarantined, or triggered an alert.
`show cdr rules`	Displays all current CDR policies.
`show cdr signature`	Displays the version number and release date of the current CDR signatures.
`show cdr status`	Displays all CDR settings, such as block period, block message, and quarantine VLAN ID.
`show cdr update`	Displays the signature update schedule.
`show cdr white-list`	Displays all entries in the CDR exempt list. This consists of IPv4 and MAC addresses.

45.3.3 Update CDR Signatures

This table shows the commands for updating the CDR signatures..

Table 229 CDR Update Commands

COMMAND	DESCRIPTION
`cdr signature reload`	Recovers CDR signatures. You only need to do this if instructed by a support technician.
`cdr signature update`	Immediately downloads the latest CDR signatures.
`[no] cdr update auto`	Enables automatic CDR signature downloads, at the time and date set by the daily/hourly/weekly command. Use the no command to disable auto updates.
`cdr update daily <0..23>`	Enables automatic CDR signature downloads every day at the time specified.
`cdr update hourly`	Enables automatic CDR signature download every hour.
`cdr update weekly {sun | mon | tue | wed | thu | fri | sat} <0..23>`	Enables automatic CDR signature downloads once a week at the time and day specified.

45.3.3.1 Update Signature Examples

This examples shows how to enable automatic CDR signature updates daily at midnight, and then check that it is configured corrected.

```
Router(config)# configure terminal
Router(config)# cdr update auto
Router(config)# cdr update daily 0
Router(config)# show cdr update
auto: yes
schedule: daily at 0 o'clock
```

45.3.3.2 Configure CDR Settings Examples

The example below shows you how to block clients that have tried to access malicious websites more than 10 times in 60 minutes. The example uses the parameters in this table.

Table 230 CDR Settings Configuration Example

OCCURRENCE	DURATION	CONTAINMENT	SEND ALERT EMAIL TO	DENIED ACCESS MESSAGE
10	60	block-alert	abcd@gmail.com	Your device is trying to access malicious websites, so you are temporarily blocked. Please contact the network admin.

1 Enable CDR. Follow the parameters given above to configure the occurrence, duration and containment actions for rule 3 (Web Threat).

```
Router(config)# configure terminal
Router(config)# cdr activate
Router(config)# cdr rule 3 threshold 10 duration 60 action block-alert
```

2 Enable counter reset to automatically reset the number of security occurrences within the defined duration when it reaches the threshold value so as to reduce alert email. An alert email will only be sent once within the duration for the first occurrence of the threshold reached, not for every occurrence over the threshold.

```
Router(config)# cdr counter-reset activate
```

3 Follow the parameters given above to configure the email address to receive an alert email when the CDR containment action is triggered.

```
Router(config)# cdr send-alerts-to abcd@gmail.com
```

4 Follow the parameters given above to configure the block message that will show in the default Zyxel Device notification page.

```
Router(config)# cdr block message Your device is trying to access
malicious websites, so you are temporarily blocked. Please contact the
network admin.
```

5 Save the current configuration to the Zyxel Device.

```
Router(config)# write
```

CHAPTER 46
SSL Inspection

46.1 SSL Inspection Overview

Secure Socket Layer (SSL) traffic, such as HTTPS, FTPS, POP3+SSL, and SMTPS, is encrypted and therefore cannot be inspected using Unified Threat Management (UTM) profiles such as App Patrol, Content Filter, Intrusion, Detection and Prevention (IDP), or Anti-Virus. The Zyxel Device uses SSL Inspection to decrypt SSL traffic, sends it to the UTM engines for inspection, then encrypts traffic that passes inspection and forwards it to the destination server, such as Google.

The Zyxel Device supports the following SSL/TLS versions and cipher suites:

- SSLv3 AES-CBC
- TLS1.0 AES-CBC
- TLS1.2 AES-CBC/AES-GCM
- TLS1.3 AES-GCM

SSL Inspection does not support the following:

- Compression
- Client Authentication
- TLS1.3 Key updates -)
- TLS1.3 Zero Round Trip Time Resumption (0-RTT)

46.2 SSL Inspection Commands Summary

The following table describes the values required for many SSL inspection commands. Other values are discussed with the corresponding commands.

Table 231 Input Values for SSL Inspection Commands

LABEL	DESCRIPTION
ssi_profile_name	This is the name of the profile. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
description	This is additional information about this SSL Inspection profile. You can enter up to 60 characters ("0-9", "a-z", "A-Z", "-" and "_").
cert_name	This is a name of a certificate.

The following sections list the commands.

46.2.1 SSL Inspection General Settings

Table 232 SSL Inspection General Settings

COMMAND	DESCRIPTION
`ssl-inspection server-sign-cert mode {default | rsa-1024 | rsa-2048}`	Select how to validate a client accessing a HTTPS website using RSA encryption through the Zyxel Device. The Zyxel Device must check that the client's certificate and public key are valid and were issued by a Certificate Authority (CA) listed in the Zyxel Device's list of trusted CAs. The default value is 1024. Note: You should flush the SSL inspection certificate cache after changing the server signing mode.
`ssl-inspection server-sign-cert mode {ecdsa-rsa-1024|ecdsa-rsa-2048}`	Select how to validate a client accessing a HTTPS website using ECDSA encryption through the Zyxel Device. ECDSA is required by certain clients such as iOS 13. • `ecdsa-rsa-1024` means the Zyxel Device uses ECDSA-256 if the client supports ECDSA-256, or RSA-1024 if the client does not support ECDSA-256. • `ecdsa-rsa-2048` means the Zyxel Device uses ECDSA-256 if the client supports ECDSA-256, or RSA-2048 if the client does not support ECDSA-256.
`ssl-inspection pkt-enc-mss <536..1460>`	Sets the maximum TCP packet size that the Zyxel Device will encrypt, in bytes. If a packet's size is greater than this value, then the Zyxel Device splits the packet into two or more packets. The default value is 1460.
`show ssl-inspection status`	Displays the current configuration of SSL inspection.

46.2.2 SSL Inspection Exclusion Command Input Values

The following table explains the values you can input with the SSL inspection exclusion commands.

Table 233 Content Filter Command Input Values

LABEL	DESCRIPTION
category_name	The name of a web category. For a list of category definitions, see Section 43.7 on page 382. Firmware v4.50 or earlier: {advertisements-pop-ups | job-search | alcohol-tobacco | leisure-recreation | anonymizers | malware | arts | network-errors | botnets | news | business | non-profits-ngos | chat | nudity | child-abuse-images | parked-domains | compromised | peer-to-peer | computers-technology | personal-sites | criminal-activity | phishing-fraud |cults | politics | dating-personals | pornography-sexually-explicit | download-sites | private-ip-addresses | education | real-estate | entertainment | religion | fashion-beauty | restaurants-dining | finance | school-cheating | forums-newsgroups | search-engines-portals | gambling | sex-education | games | shopping | general | social-networking | government | spam-sites | greeting-cards | sports | hacking | streaming-media-downloads | hate-intolerance | tasteless | health-medicine | translators | illegal-drugs | transportation | illegal-software | travel | image-sharing | violence | information-security | weapons | instant-messaging | web-based-email } Firmware v4.55 or later: {adult-topics | alcohol | anonymizing-utilities | art-culture-heritage | auctions-classifieds | blogs-wiki | business | chat | computing-internet | consumer-protection | content-server | controversial-opinions | cult-occult | dating-personals | dating-social-networking | digital-postcards | discrimination | drugs | education-reference | entertainment | extreme | fashion-beauty | finance-banking | for-kids | forum-bulletin-boards | gambling | gambling-related | game-cartoon-violence | games | general-news | government-military | gruesome-content | health | historical-revisionism | history | humor-comics | illegal-uk | incidental-nudity | information-security | information-security-new | instant-messaging | interactive-web-applications | internet-radio-tv | internet-services | job-search | major-global-religions | marketing-merchandising | media-downloads | media-sharing | messaging | mobile-phone | moderated | motor-vehicles | non-profit-advocacy-ngo | nudity | online-shopping | p2p-file-sharing | parked-domain | personal-network-storage | personal-pages | pharmacy | politics-opinion | pornography | portal-sites | potential-criminal-activities | potential-hacking-computer-crime | potential-illegal-software | private-ip-addresses | profanity | professional-networking | provocative-attire | public-information | pups | real-estate | recreation-hobbies | religion-ideology | remote-access | reserved | residential-ip-addresses | resource-sharing | restaurants | school-cheating-information | search-engines | sexual-materials | shareware-freeware | social-networking | software-hardware | sports | stock-trading | streaming-media | technical-business-forums | technical-information | text-spoken-only | text-translators | tobacco | travel | usenet-news | violence | visual-search-engine | weapons | web-ads | web-mail | web-meetings | web-phone}

46.2.3 SSL Inspection Exclusion Commands

There may be privacy and legality issues regarding inspecting a user's encrypted session. The legal issues may vary by locale, so it's important to check with your legal department to make sure that it’s OK to intercept SSL traffic from your Zyxel Device users.

To ensure individual privacy and meet legal requirements, you can configure an exclusion list to exclude matching sessions to destination servers. This traffic is not intercepted and passes through the Zyxel Device uninspected.

This table lists the SSL Inspection exclusion-related commands.

Table 234 SSL Inspection Exclusion Commands

COMMAND	DESCRIPTION
`ssl-inspection exclude-list`	Enter SSL Inspection exclude list sub-command mode. In this mode you can add and remove the servers that are excluded from SSL Inspection.
`[no] entry {IPv4 | IPv4_CIDR | IPv4_RANGE | IPv6 | IPv6_PREFIX | IPv6_RANGE | SSL_INSPECTION_WILDCARD_CNAME}`	Identify the certificate in one of the following ways: • Type an IPv4 or IPv6 address. For example, type 192.168.1.35, or 2001:7300:3500::1 • Type an IPv4/IPv6 block in CIDR notation. For example, type 192.168.1.1/24, or 2001:7300:3500::1/64 • Type an IPv4/IPv6 address range by entering the start and end addresses separated by a hyphen (-). For example, type 192.168.1.1-192.168.1.35, or 2001:7300:3500::1-2001:7300:3500::35 • Type a DNS name. For example, type www.zyxel.com.tw. • Type a common name (wildcard char: '*', escape char: '\'). Use up to 127 case-insensitive characters (0-9a-zA-Z`~!@#$%^&*()-_=+[]{}|;:',.<>/?). '*' can be used as a wildcard to match any string. Use '*' to indicate a single wildcard character. • Type an email address. For example, type abc@zyxel.com.tw The no command removes the SSL entry.
`[no] category <category_name>`	Sets the web categories to let SSL traffic destined for websites that belong to these categories pass through the Zyxel Device without been inspected. The no command removes the web categories so that SSL traffic to these sites is inspected.
`exit`	Exit the sub-command mode.
`show ssl-inspection exclude-list`	Displays all entries in the SSL exclusion list.
`ssl-inspection exclude-list-settings`	Enter SSL Inspection exclude list settings sub-command mode. In this mode you can configure settings for the SSL Inspection exclude list.
`[no] log`	Create a log for traffic that bypasses SSL Inspection. The no command disables SSL exclusion list logging.
`exit`	Exit the sub-command mode.
`show ssl-inspection exclude-list settings`	Displays all SSL exclusion list settings, such as whether logging is enabled.
`show ssl-inspection exclude-list address`	Displays all SSL exclusion list entry settings, such as the certificate IP addresses or DNS names.
`show ssl-inspection exclude-list web-category`	Displays the web categories that lets SSL traffic destined for websites that belong to these categories pass through the Zyxel Device without been inspected.

46.2.4 SSL Inspection Profile Settings

This table lists the SSL Inspection profile setting commands.

Table 235 SSL Inspection Profile Commands

COMMAND	DESCRIPTION
`ssl-inspection profile` *`ssi_profile_name`*	Creates an SSL Inspection profile, and then enters the SSL Inspection profile sub-command mode. The profile name may consist of 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
`bind-ipv4-addr` *`ipv4`*	Request a certificate using the specified IPv4 source address. This command is for debugging purposes.
`bind-ipv6-addr` *`ipv6`*	Request a certificate using the specified IPv6 source address. This command is for debugging purposes.
`[no] certificate` *`cert_name`*	Enter the default certificate or one already created for this profile. The no command removes the certificate from this profile.
`[no] description` *`description`*	Enter additional information about this SSL Inspection entry. You can enter up to 60 characters ("0-9", "a-z", "A-Z", "-" and "_"). The no command removes the description.
`exit`	Exit sub-command mode.
`follow-real-client-routing {yes | no}`	When an SSL session is detected by SSL inspection, the Zyxel Device creates another independent session in order to get information such as the certificate chain. However, because traffic for this new session is sent from the Zyxel Device, it may not match the same routing policy of the original SSL session and may not reach the destination server. Enable this command to allow the session sent from the Zyxel Device to follow the routing policy of the original session. The no command does not allow the session sent from the Zyxel Device to follow the routing policy of the original session.
`sslv2 action {pass | block} {no log | log [alert]}`	SSL Inspection supports SSLv3 and TLS1.0. This command sets the action and log event for when the Zyxel Device encounters SSLv2 traffic. • Pass: SSLv2 traffic is allowed to pass through the Zyxel Device uninspected. • Block: SSLv2 traffic is blocked. You can also set the logging events. • no log: Do not log SSLv2 traffic events. • log: Create a log message when SSLv2 traffic is passed through or blocked. • log: Create a log message and issue an alert email when SSLv2 traffic is passed through or blocked.
`support-version-max {ssl3 | tls1_0 | tls1_1 | tls1_2 | tls1_3}`	The Zyxel Device only inspects SSL traffic if the SSL version is equal to this value or lower.
`support-version-min {ssl3 | tls1_0 | tls1_1 | tls1_2 | tls1_3}`	The Zyxel Device only inspects SSL traffic if the SSL version is equal to this value or higher.
`unsupported-suite action {pass | block} {no log | log [alert]}`	Select to pass or block unsupported traffic, such as traffic using unsupported cipher suites, compression, or client authentication.

Table 235 SSL Inspection Profile Commands

COMMAND	DESCRIPTION
`untrusted-cert-chain action {block | inspect | pass} {no log | log [alert]}`	A certificate chain is a certification process that involves the following certificates between the SSL/TLS server and a client. A certificate chain will fail if one of the following certificates is not correct. • A certificate owned by a user • The certificate signed by a certification authority • A root certificate Select to pass, inspect, or block an untrusted certification chain.
`ssl-inspection profile rename` *`ssi_profile_name1 ssi_profile_name2`*	Renames an SSL Inspection profile.
`no ssl-inspection profile` *`ssi_profile_name`*	Deletes an SSL Inspection profile.
`show ssl-inspection profile [`*`ssi_profile_name`*`]`	Displays SSL Inspection profile settings.
`ssl-inspection tls1-3 {activate | deactivate}`	Enables or disables support for TSL 1.3 on the Zyxel Device.
`ssl-inspection tls1-2 aesgcm {activate | deactivate}`	Enables or disables support for cipher TSL 1.2 AES-GCM on the Zyxel Device.

46.2.5 SSL Inspection Certificate Cache

This table lists the SSL Inspection certificate cache commands.

Table 236 SSL Inspection Certificate Cache Commands

COMMAND	DESCRIPTION
`ssl-inspection cache flush`	Clears SSL Inspection cached entries.
`show ssl-inspection cert-list`	Displays certificates used in SSL Inspection.

46.2.6 SSL Inspection Certificate Update

Use these commands to update the latest certificates of servers using SSL connections to the Zyxel Device network. You must have Internet access and have activated SSL Inspection on the Zyxel Device at myZyxel.com.

This table lists the SSL Inspection certificate cache commands.

Table 237 SSL Inspection Certificate Update Commands

COMMAND	DESCRIPTION
`[no] ssl-inspection cert-update auto`	The Zyxel Device automatically updates the certificate set when a new one becomes available on myZyxel.com.
`ssl-inspection cert-update now`	Download the latest certificate set from the myZyxel.com and update it on the Zyxel Device.

Table 237 SSL Inspection Certificate Update Commands

COMMAND	DESCRIPTION
`show ssl-inspection default-cert version`	Displays the default certificate update status.
`show ssl-inspection default-cert update`	Shows the current certificate update status.
`show ssl-inspection cert-update status`	Shows if automatically updating the certificate set is configured on the Zyxel Device.

These are some example SSL Inspection certificate update usage commands.

```
Router(config)# show ssl-inspection cert-update status
update auto     : no
Router(config)# ssl-inspection cert-update auto
Router(config)# show ssl-inspection cert-update status
update auto     : yes
Router(config)# show ssl-inspection default-cert update
/tmp/sslinsp_certs/default_trusted /
current status: Connecting to update server to get SSL certificate. at Fri Apr 10
03:47:37 2015

Router(config)# show ssl-inspection default-cert update
current status: SSL Certificate update has succeeded. (success) at Fri Apr 10
03:47:49 2015
Router(config)#
```

46.2.7 SSL Inspection Statistics

This table lists the SSL Inspection statistics commands.

Table 238 SSL Inspection Statistics Commands

COMMAND	DESCRIPTION
`[no] ssl-inspection statistics collect`	Enables SSL inspection statistics collection. The no command disables SSL exclusion statistics collection.
`ssl-inspection statistics flush`	Clears SSL inspection statistics.
`show ssl-inspection statistics collect`	Shows if SSL inspection statistics collection is enabled.
`show ssl-inspection statistics summary`	Shows SSL inspection statistics such as concurrent sessions, total ssl sessions, sessions inspected, decrypted Kbytes, encrypted Kbytes, sessions blocked, and sessions passed.

46.2.8 SSL Inspection Command Examples

These are some other example SSL Inspection usage commands.

```
Router(config)#Router(config)# ssl-inspection exclude-list-settings
Router(ssl-inspection-exclude-list-settings)# no log
Router(ssl-inspection-exclude-list-settings)# exit
Router(config)# ssl-inspection exclude-list
Router(ssl-inspection-exclude-list)# entry 1.1.1.1
Router(ssl-inspection-exclude-list)# entry abc@zyxel.com.tw
Router(ssl-inspection-exclude-list)# exit
Router(config)# show ssl-inspection exclude-list settings
SSL Inspection Exclude List Global Information
  Log: no
Router(config)# show ssl-inspection exclude-list
No.  Exclude list of Certificate Identity
================================================================================
0    1.1.1.1
1    abc@zyxel.com.tw
Router(config)# ssl-inspection profile dummy
Router(config-ssl-inspection-profile-dummy)# description this is a dummy profile
Router(config-ssl-inspection-profile-dummy)# certificate default
Router(config-ssl-inspection-profile-dummy)# sslv2 action block log
Router(config-ssl-inspection-profile-dummy)# unsupported-suite action block log
Router(config-ssl-inspection-profile-dummy)# untrusted-cert-chain action block log
Router(config-ssl-inspection-profile-dummy)# exit
Router(config)# show ssl-inspection profile dummy
SSL-Inspection: 3
  profile name: dummy
  description: this is a dummy profile
  Certificate: default
  Follow_real_client_routing: yes
  SSLv2_action: block
  SSLv2_log: log
  Unsupported_suite_action: block
  Unsupported_suite_log: log
  Untrusted_cert_chain_action: block
  Untrusted_cert_chain_action_log: log
  Reference: 0
Router(config)# ssl-inspection statistics collect
Router(config)# show ssl-inspection statistics collect
collect statistics: yes
collect statistics time: since 2014-06-20 05:47:37 to 2014-06-20 05:47:55
Router(config)# show ssl-inspection statistics summary
maximum concurrent sessions  : 1000
concurrent sessions          : 0

total ssl sessions           : 0
  sessions inspected         : 0
     decrypted Kbytes        : 0
     encrypted Kbytes        : 0
  sessions blocked           : 0
  sessions passed            : 0

Router(config)#
```

CHAPTER 47
IP Exception

47.1 IP Exception Overview

IP Exception allows incoming IP packets to bypass specific security services based on the packet's source or destination address. Bypassing a security service means the security service does not intercept or inspect the packet. IP Exception supports bypassing the following security services:

- Antivirus (including sandboxing)
- Intrusion Detection and Prevention (IDP)
- IP Reputation
- URL Threat Filter

47.2 IP Exception Commands

The Zyxel Device excludes incoming packets that match any IP Exception rule. Each IP Exception rule contains a source address, destination address, and a list of bypassed services. The following table identifies the values required for many IP Exception commands..

Table 239 General Input Values for IP Exception List Commands

LABEL	DESCRIPTION
<profile-name>	The name of an IP Exception rule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
address_name	The source or destination address of an IP packet. The address name can be any of the following: • Address object name • Address group object name • FQDN object name • Geo IP object name For details on addresses, see Chapter 52 on page 458.

Table 240 Commands for IP Exception

COMMAND	DESCRIPTION
`security-service ip-exception {profile_name}`	Configure an IPv4 rule. If the rule does not currently exist, then the Zyxel Device creates it.
`source {address_name | any} destination {address_name | any} {log | no-log}`	*address_name*: Apply this rule to IPv4 packets with the specified source or destination address. any: Apply this rule to IPv4 packets with any source or destination address. `log`: Create a log message each time an incoming IPv4 packet matches this rule. `no-log`: Do not create any log messages.

Table 240 Commands for IP Exception

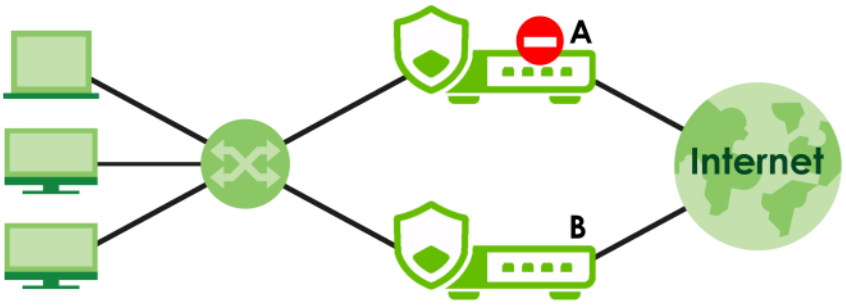
COMMAND	DESCRIPTION
[no] {anti-virus| ip-reputation | ips | threat-website} bypass	Sets the service that IPv4 packets will bypass. To bypass multiple services, run the command multiple times. ips is IDP. Use the no command to stop bypassing a service.
[no] description {*DESCRIPTION*}	{*DESCRIPTION*}: Sets a description for the IP Exception rule. You can use up to 60 printable ASCII characters. Use the no command to delete the description for this profile.
security-service ip6-exception {*profile_name*}	Configure an IPv6 rule. If the rule does not currently exist, then the Zyxel Device creates it.
source {*address_name* | any} destination {*address_name* | any} {log | no-log}	*address_name*: Apply this rule to IPv6 packets with the specified source or destination address. any: Apply this rule to IPv6 packets with any source or destination address. log: Create a log a log message each time an incoming IPv6 packet matches this rule. no-log: Do not create any log messages.
[no] {anti-virus | ip-reputation | ips | threat-website} bypass	Sets a service that IPv6 packets will bypass. You can run this command multiple times to bypass multiple services. ips is IDP. Use the no command to stop bypassing a service.
[no] description {*DESCRIPTION*}	{*DESCRIPTION*}: Sets a description for the IP Exception rule. You can use up to 60 printable ASCII characters. Use the no command to delete the description for this profile.
no security-service ip-exception *profile_name*	Removes the specified IPv4 rule.
no security-service ip6-exception *profile_name*	Removes the specified IPv6 rule.
show security-service ip-exception	Displays all IPv4 rules.
show security-service ip6-exception	Displays all IPv6 rules.

CHAPTER 48
Device HA

48.1 Device HA Overview

Use device HA to increase network reliability. Device HA lets a backup Zyxel Device (B) automatically take over if a master Zyxel Device (A) fails.

Figure 38 Device HA Backup Taking Over for the Master



Active-Passive Mode

- Active-passive mode lets a backup Zyxel Device take over if the master Zyxel Device fails.
- The Zyxel Devices must all support and be set to use the same device HA mode (either active-passive or legacy).

Management Access

You can configure a separate management IP address for each interface. You can use it to access the Zyxel Device for management whether the Zyxel Device is the master or a backup. The management IP address should be in the same subnet as the interface IP address.

Synchronization

Use synchronization to have a backup Zyxel Device copy the master Zyxel Device's configuration, signatures (anti-virus, IDP/application patrol, and system protect), and certificates.

Note: Only Zyxel Devices of the same model and firmware version can synchronize.

Otherwise you must manually configure the master Zyxel Device's settings on the backup (by editing copies of the configuration files in a text editor for example).

48.1.1 Before You Begin

- Configure a static IP address for each interface that you will have device HA monitor.

Note: Subscribe to services on the backup Zyxel Device before synchronizing it with the master Zyxel Device.

- Synchronization includes updates for services to which the master and backup Zyxel Devices are both subscribed. For example, a backup subscribed to IDP/AppPatrol, but not anti-virus, gets IDP/AppPatrol updates from the master, but not anti-virus updates. It is highly recommended to subscribe the master and backup Zyxel Devices to the same services.

48.1.2 Device HA and Device HA Pro

Refer to the Introduction chapter of the ZyWALL USG Series User's Guide for a list of device models that support Device HA Pro.

The following table shows some differences between Device HA and Device HA Pro.

Table 241 Device HA Vs Device HA Pro

FEATURE	DEVICE HA	DEVICE HA PRO
Role	Role of Master and Backup is configurable. Master takes over from Backup if the Master goes down and then becomes the Master again if it comes back online again (failback).	Role of active and passive is not configurable. The active model is the one whose heartbeat interface comes online first. passive becomes active if active goes down and stays active even if the previous active comes online again.
Firmware Upgrade	Master remains Master by default when new firmware is uploaded.	New firmware is first uploaded to the passive device and then uploaded to the active device. By default, the passive device reboots after firmware upload making it become the active device. Clear the Reboot prompt in the Web Configurator after uploading firmware to the passive device if you want the passive device to remain passive when new firmware is uploaded.
What is synchronized	Configuration file	Configuration file, device time, IPv4/v6 TCP sessions, IPSec VPN tunnels, user login/logout information, AV/IDP signatures, DHCP table, IP/MAC binding table.
Maximum Failover Count	0	5 (default) to 50. Can be reset by command.
Best case Failover delay	10~30 seconds to rebuild connections.	0~1 seconds.
Monitored Interfaces	Ethernet	Ethernet, VLAN, Bridge, LAG
Dedicated monitor port	No	Heartbeat interface. Note: Remove Ethernet, VLAN, Bridge, LAG configurations from this port first.

48.2 General Device HA Commands

This table lists the general commands for device HA.

Table 242 device-ha General Commands

COMMAND	DESCRIPTION
`show device-ha status`	Displays whether or not device HA is activated, the configured device HA mode, and the status of the monitored interfaces.
`[no] device-ha activate`	Turns device HA on or off.
`device-ha mode active-passive`	Sets the Zyxel Device to use active-passive device HA.

48.3 Active-Passive Mode Device HA

Virtual Router

The master and backup Zyxel Device form a single 'virtual router'.

Cluster ID

You can have multiple Zyxel Device virtual routers on your network. Use a different cluster ID to identify each virtual router.

Monitored Interfaces in Active-Passive Mode Device HA

You can select which interfaces device HA monitors. If a monitored interface on the Zyxel Device loses its connection, device HA has the backup Zyxel Device take over.

Enable monitoring for the same interfaces on the master and backup Zyxel Devices. Each monitored interface must have a static IP address and be connected to the same subnet as the corresponding interface on the backup or master Zyxel Device.

Virtual Router and Management IP Addresses

- If a backup takes over for the master, it uses the master's IP addresses. These IP addresses are know as the virtual router IP addresses.
- Each interface can also have a management IP address. You can connect to this IP address to manage the Zyxel Device regardless of whether it is the master or the backup.

48.4 Active-Passive Mode Device HA Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 243 Input Values for device-ha Commands

LABEL	DESCRIPTION
interface_name	The name of the interface. This depends on the Zyxel Device model. For some Zyxel Device models, use ge*x*, *x* = 1 ~ N, where N equals the highest numbered Ethernet interface for your Zyxel Device model. For other Zyxel Device models, use a name such as wan1, wan2, opt, lan1, or dmz. Besides, in HA AP mode, the interface can also be a bridge interface. In HA Legacy mode, the interface can also be a VLAN interface.

The following sections list the `device-ha` commands.

48.4.1 Active-Passive Mode Device HA Commands

This table lists the commands for configuring active-passive mode device HA.

Table 244 device-ha ap-mode Commands

COMMAND	DESCRIPTION
`[no] device-ha ap-mode preempt`	Turn on preempt if this Zyxel Device should become the master Zyxel Device if a lower-priority Zyxel Device is the master when this Zyxel Device is enabled.
`device-ha ap-mode role {master|backup}`	Sets the Zyxel Device to be the master or a backup in the virtual router.
`device-ha ap-mode cluster-id <1..32>`	Sets the cluster ID number. A virtual router consists of a master Zyxel Device and all of its backup Zyxel Devices. If you have multiple Zyxel Device virtual routers on your network, use a different cluster ID for each virtual router.
`device-ha ap-mode priority <1..254>`	Sets backup Zyxel Device's priority. The backup Zyxel Device with the highest value takes over the role of the master Zyxel Device if the master Zyxel Device becomes unavailable. The priority must be between 1 and 254. (The master interface has priority 255.)
`[no] device-ha ap-mode authentication {string` *key* `| ah-md5` *key*`}`	Sets the authentication method the virtual router uses. Every interface in a virtual router must use the same authentication method and password. The no command disables authentication. `string`: Use a plain text password for authentication. *key* - Use up to eight characters including alphanumeric characters, the underscore, and some punctuation marks (+-/*= :; .! @$&%#~ ' \ ()). `ah-md5`: Use an encrypted MD5 password for authentication. *key* - Use up to eight characters including alphanumeric characters, the underscore, and some punctuation marks (+-/*= :; .! @$&%#~ ' \ ()).
`[no] device-ha ap-mode` *interface_name* `manage-ip` *ip subnet_mask*	Sets the management IP address for an interface.
`[no] device-ha ap-mode` *interface_name* `activate`	Has device HA monitor the status of an interface's connection.

Table 244 device-ha ap-mode Commands (continued)

COMMAND	DESCRIPTION
`[no] device-ha ap-mode master sync authentication password` *password*	This is for a master Zyxel Device. It specifies the password to require from synchronizing backup Zyxel Devices. Every router in the virtual router must use the same password. The `no` command sets the password setting to blank (which means no backups can synchronize with this master). *password*: Use 4-63 alphanumeric characters, underscores (_), dashes (-), and #%^*={}:,.~ characters.
`[no] device-ha ap-mode backup sync authentication password` *password*	Sets the password the backup Zyxel Device uses when synchronizing with the master. The `no` command sets the password setting to blank (which means this backup Zyxel Device cannot synchronize with the master). *password*: Use 4-63 alphanumeric characters, underscores (_), dashes (-), and #%^*={}:,.~ characters.
`[no] device-ha ap-mode backup sync auto`	Turns on automatic synchronization according to the interval you specify in `device-ha ap-mode backup sync interval`. The first synchronization begins after the specified interval (not immediately).
`[no] device-ha ap-mode backup sync interval <5..1440>`	When you use automatic synchronization, this sets how often (in minutes) the Zyxel Device synchronizes with the master.
`[no] device-ha ap-mode backup sync from` *master_address* `port` *port*	Sets the address of the master Zyxel Device with which this backup Zyxel Device is to synchronize. *master_address*: The master Zyxel Device's IP address or fully-qualified domain name (FQDN). *port*: The master Zyxel Device's FTP port number.
`device-ha ap-mode backup sync now`	Synchronize now.
`show device-ha ap-mode interfaces`	Displays the device HA AP mode interface settings and status.
`show device-ha ap-mode next-sync-time`	Displays the next time and date (in hh:mm yyyy-mm-dd format) the Zyxel Device will synchronize with the master.
`show device-ha ap-mode status`	Displays the Zyxel Device's key device HA settings.
`show device-ha ap-mode master sync`	Displays the master Zyxel Device's synchronization settings.
`show device-ha ap-mode backup sync`	Displays the backup Zyxel Device's synchronization settings.
`show device-ha ap-mode backup sync status`	Displays the backup Zyxel Device's current synchronization status.
`show device-ha ap-mode backup sync summary`	Displays the backup Zyxel Device's synchronization settings.
`show device-ha ap-mode forwarding-port` *interface_name*	If you apply Device HA on a bridge interface on a backup Zyxel Device, you can use this command to see which port in the bridge interface is chosen to receive VRRP packets used to monitor if the master Zyxel Device goes down. *interface_name*: This is a bridge interface, For example, brx.
`show device-ha mode`	Displays whether this Zyxel Device is in active-passive mode.

48.4.2 Active-Passive Mode Device HA Command Example

This example configures a Zyxel Device to be a master Zyxel Device for active-passive mode device HA. There is a management IP address of 192.168.1.3 on lan1. wan1 and lan1 are monitored. The synchronization password is set to “mySyncPassword”.

```
Router(config)# device-ha ap-mode lan1 manage-ip 192.168.1.3 255.255.255.0
Router(config)# device-ha ap-mode role master
Router(config)# device-ha ap-mode master sync authentication password
mySyncPassword
Router(config)# device-ha ap-mode wan1 activate
Router(config)# device-ha ap-mode lan1 activate
Router(config)# device-ha activate
```

48.5 Device HA Pro

You need a license to use Device HA Pro. Device HA Pro is easier to deploy than Device HA, is more reliable (no risk of overloading), and faster (Device HA causes a connection break of 10~30 seconds while Device HA Pro just has 1~2 seconds). In addition to configuration file backup in Device HA, device time, TCP sessions (IPv4/IPv6), IPSec VPN sessions, login/logout information and license status can also be backed up using Device HA Pro.

Active and Passive Devices

Device HA Pro uses a dedicated heartbeat link between an active device and a passive device for dynamic syncing and backup to the passive device. On the passive device, all ports are disabled except for the port with the heartbeat link.

Note: The dedicated heartbeat link port must be the highest-numbered port on each Zyxel Device for Device HA Pro to work.

Failover from the active Zyxel Device to the passive Zyxel Device is activated when:

- A monitored interface is down
- A monitored service (daemon) is down
- The hearbeat link exceeds the failure tolerance.

After failover, the initial active Zyxel Device becomes the passive Zyxel Device after it recovers.

See Section 48.1.2 on page 429 for differences between Device HA and Device HA Pro.

48.5.1 Deploying Device HA Pro

1. Register either the active or passive Zyxel Device with a Device HA Pro license at MyZyxel.com. Check that it’s properly licensed in Licensing > Registration > Service in the active Zyxel Device.
2. Make sure the passive Zyxel Device is offline, then enable Device HA in Device HA > General in the passive Zyxel Device.

3 Must make sure the FTP port in System > FTP (default 21) is the same on both Zyxel Devices. FTP is used for transferring files in the event of failover from active to passive Zyxel Device.

4 Connect the passive Zyxel Device to the active Zyxel Device using the highest-numbered ports on both Zyxel Devices.

Note: If both Zyxel Devices are turned on at the same time with Device HA enabled, then they may send the heartbeat at the same time. In this case, the Zyxel Device with the bigger MAC address becomes the passive Zyxel Device.

5 When using Device HA Pro to synchronize firmware, the location of the running firmware must be the same in both active and passive Zyxel Devices. For example, if the running firmware is in partition 1 in the active Zyxel Device (standby firmware in partition 2), then the running firmware must also be in partition 1 in the passive Zyxel Device (standby firmware in partition 2).

6 When using Device HA Pro to update new firmware, the new firmware is downloaded to the active device. The active device sends a ping to the passive device to see if it is alive. If the active device receives a reply from the passive device, it uploads the new firmware to the passive device.
The passive device uploads the new firmware and then reboots. The active device then repeatedly pings the passive device again as it reboots. The active device waits from 1-3,600 seconds `check-timeout` (with 1,800 as the default) for a reply from the passive device indicating it has fully rebooted. If the active device does not receive a reply within the check-timeout, it will not update its own firmware.
If it receives a reply, the active device again waits from 1-300 seconds `delay` (with 10 as the default) before updating its own firmware. The passive device becomes the active device after a successful reboot with the new firmware.

48.5.2 Device HA Pro Commands

This table lists the commands for Device HA Pro (`device-ha2`).

Table 245 `device-ha2` (Device HA Pro) Commands

COMMAND	DESCRIPTION
`[no] device-ha2 activate`	Turns Device HA Pro on or off (no).
`[no] device-ha2 interface_name activate`	Turns Device HA Pro monitoring on or off (no) on the specified interface.
`[no] device-ha2 manage-ip ip1 ip2 subnet_mask`	Sets or removes (no) the IPv4 address and subnet mask of the heartbeat dedicated link port (the highest-numbered port) on the active and passive Zyxel Device. *ip1*: IPv4 address of the active Zyxel Device. *ip2*: IPv4 address of the passive Zyxel Device.
`device-ha2 sync password password`	Sets a synchronization password of between 1 and 32 single-byte printable characters.
`[no] device-ha2 sync password`	Enables or disables (no) being prompted for the password before synchronization takes place.
`device-ha2 sync_to_passive`	Manually synchronizes the passive and active devices. Use this command on the active device. This command is available in User or Privilege mode.
`device-ha2 sync_from_active`	Manually synchronizes the passive and active devices. Use this command on the passive device. This command is available in User or Privilege mode.
`[no] device-ha2 disable-session-sync`	Disables or enables (no) connection tracking session synchronization.

Table 245 device-ha2 (Device HA Pro) Commands (continued)

COMMAND	DESCRIPTION
[no] device-ha2 srv-monitor	Enables or disables (no) service monitoring. When enabled, the passive Zyxel Device takes over when a monitored service daemon on the active Zyxel Device fails.
[no] device-ha2 connchk-monitor	Enables or disables (no) connection check monitoring. When enabled, the passive Zyxel Device takes over when a monitored interface on the active Zyxel Device fails.
device-ha2 failover connchk-hold-time <60..86400>	Sets a minimum time period between failovers to mitigate failover flapping. Failover flapping occurs when the active and passive devices keep switching due for example to a faulty up-link connection.
device-ha2 heartbeat period <1..10> fail-tolerance <1..10>	Sets when failover is activated on the passive Zyxel Device. Zyxel Device will change to active mode if it doesn't receive a heartbeat after heartbeat period x fail-tolerance seconds. heartbeat period: the number of seconds (1-10) allowed for absence of a heartbeat signal. fail-tolerance: the number of heartbeat failures allowed.
device-ha2 license-sync *serial_number*	Sets the serial number of the Zyxel Device (active or passive) with the Device HA Pro subscribed license.
device-ha2 virtual-mac *zynos_style_mac_address*	Specifies the Virtual MAC address of a port on the active Zyxel Device. Virtual MAC is a shared MAC address which is owned by the active Zyxel Device. All traffic can communicate with this shared MAC address, allowing the backup Zyxel Device to pick up traffic seamlessly. *zynos_style_mac_address*: The first (wan0) MAC address of the Zyxel Device. A Zyxel-style MAC address must use the Zyxel OUI (Organizationally Unique Identifier) such as 00-13-49-XX-XX-XX.
device-ha2 failover-count <5 ..50>	Sets the maximum number of times a Zyxel Device can change from active to passive mode. The Zyxel Device won't change to passive mode if it's already changed to passive mode failover-count times. This is to prevent too many changes between active and passive mode.
device-ha2 failover reset-interval <1..30>	Sets the time period after which the failover counter can be reset (1-30 days). The default is 5 days. For example, if the failover-count is 5 and the failover reset-interval is 30, then Zyxel Device can change from active to passive mode at most 5 times within 30 days.
device-ha2 ap-firmware-sync	Sets the active device to upload the latest AP firmware to the passive device after the active device discovers and downloads the latest AP firmware from the cloud server.
device-ha2 firmware-update check-timeout	Sets how long the active device will wait for a reply ping from the passive device indicating it has fully rebooted. check-timeout: 1 - 3,600 seconds with 1,800 as the current default
device-ha2 firmware-update delay	Sets how long the active device will wait before updating its firmware after receiving a reply ping from the passive device. delay time: 1 - 300 seconds with 10 as the current default
show device-ha2 activation	Displays whether or not Device HA Pro is activated.
show device-ha2 mode	Displays whether this Zyxel Device is the active or passive device. HA mode: Active | Passive.
show device-ha2 device-status	Displays if this Zyxel Device is active or passive, heartbeat link status, this Zyxel Device serial number, Virtual MAC address and synchronization progress.
show device-ha2 passive device-status	Displays the passive Zyxel Device heartbeat link status, the passive Zyxel Device serial number, Virtual MAC address and synchronization progress.

Table 245 `device-ha2` (Device HA Pro) Commands (continued)

COMMAND	DESCRIPTION
`show device-ha2 passive log`	Displays High Availability logs for the passive Zyxel Device.
`show device-ha2 interfaces`	Displays Device HA Pro monitored interfaces.
`show device-ha2 log`	Displays Device HA Pro logs.
`show device-ha2 trace-log`	Displays the active device's Device HA Pro trace logs.
`show device-ha2 passive trace-log`	Displays the passive device's Device HA Pro trace logs.
`show device-ha2 mgnt-iface`	Displays the Device HA Pro management interface.
`show device-ha2 sync status`	Displays Device HA Pro synchronization status.
`show device-ha2 sync summary`	Displays Device HA Pro synchronization result.
`show device-ha2 virtual-mac`	Displays Device HA Pro virtual router MAC address. The active and passive Zyxel Devices form a single 'virtual router' with the MAC address of the active device being the virtual MAC address.
`show device-ha2 status`	Displays whether or not device HA is activated, the IP addresses of the active and passive devices, heartbeat parameters, failover parameters and monitored interfaces.
`show device-ha2 firmware-update check-timeout`	Displays how long the active device will wait for a reply ping from the passive device indicating it has fully rebooted. `check-timeout`: 1 - 3,600 seconds with 1,800 as the current default
`show device-ha2 firmware-update delay`	Displays how long the active device will wait before updating its firmware after receiving a reply ping from the passive device. `delay time`: 1 - 300 seconds with 10 as the current default
`show device-ha2 firmware-update status`	Displays the firmware update status.

48.5.3 Device HA2 Command Example

This command shows whether Device HA2 is activated and related parameters. Srv-monitor shows if a monitored service daemon on the active Zyxel Device fails. Conn-chk monitor shows if there is connection

check monitoring. When enabled, the passive Zyxel Device takes over when a monitored interface on the active Zyxel Device fails.

```
Router# show device-ha2 activation
active: yes
Router# show device-ha2 status
Active: yes
Srv-monitor: no
Conn-chk monitor: no
Password: 1234
Active Device Management IP: 192.168.177.100
Passive Device Management IP: 192.168.177.101
Subnet Mask: 255.255.255.0
Heartbeat Interval: 2
Heartbeat Fail Tolerence: 2
License-Sync: S122L23030003
Max Failover Count: 5
Current Failover Count: 0
Failover Reset Interval (days): 5
Failover Conn-chk Hold Time: 300
Virtual mac: B0B2DC69A5FE
AP-Image-Sync: no
Disable Session Sync: yes
Router(config)#
```

CHAPTER 49
Device Insight

49.1 Device Insight Overview

Device Insight displays the status of the clients connected to the Zyxel Device internal interface or IPSec VPN, such as if a client is sending traffic to the Zyxel Device or if a client's MAC address is in the CDR block list.

It also displays the basic information of the clients. The clients shown may include clients connected to the Zyxel Device:

- A - Using wired connections.
- B - Through access points (APs) using wired connections.
- C - Through access points (APs) using WiFi connections.
- D- Through built-in access points using WiFi connections.
- E- Using SecuExtender (IPSec VPN clients).

Use Device Insight to identify and monitor clients connected to the internal LAN/VLAN DMZ networks of the Zyxel Device in the same IP subnet. This feature collects client information, including:

- Hostname
- IP address and MAC address
- Operating system
- Category, such as mobile phones or computers
- Connected interface

You can create a profile based on clients' categories and operating systems, and then apply the created profile to the Zyxel Device security policies. For example, company A on the Zyxel Device LAN1 wants to block its subsidiary employees on LAN2 from accessing the company A local networks with their mobile phones. Company A can create a profile that includes all operating systems mobile phones, and then apply it to the LAN2_To_LAN1 policy. Clients using mobile phones on the Zyxel Device LAN2 will be blocked from accessing the Zyxel Device LAN1.

Note: To collect clients' information using Device Insight, the clients must be in the same IP subnet in the LAN/VLAN/DMZ networks behind the Zyxel Device. Information from clients that are in different IP subnets in the LAN/VLAN/DMZ networks might not be collected correctly as traffic must pass through another router or a layer-3 switch to the Zyxel Device.

49.1.1 Device Insight Commands

This table lists the commands for Device Insight.

Table 246 Command Summary: Device Insight

COMMAND	DESCRIPTION
`show device info all`	Displays all connected clients status and information.
`show device info mac <mac address>`	Displays information of a client with the specified MAC address.
`show device info ip <ip address>`	Displays information of a client with the specified IP address.
`[no] device identify activate`	Enables Device Insight to identify connected clients. Use the `no` command to disable this feature.
`show device identify status`	Displays whether Device Insight is on or off.
`[no] device block mac <mac address>`	Blocks a client with the specified MAC address. Use the `no` command to unblock an MAC address.
`device remove mac <mac address>`	Removes a client with the specified MAC address that's no longer connected to your network.
`[no] device mac <mac address> description <description>`	Enters a client MAC address to set a description for the client. Use the `no` command to delete the description for this client.
`show device profile all`	Displays all device insight profiles settings.
`show device profile <profile name>`	Enters a profile name to show the specified profile settings.

The following table describes the commands available for Device Insight. You must use the `configure terminal` commands to enter the configuration mode before you can use the configuration commands. Commands that do not have IPv6 specified in the description are for IPv4.

Table 247 Command Summary: Device Insight Profiles

COMMAND	DESCRIPTION
`[no] device profile <profile name>`	Creates a Device Insight profile. You may use 1-31 alphanumeric character, underscores (_), or dashes (-), but the first character cannot be a number. Spaces and duplicate names are not allowed. This value is case-sensitive Use the `no` command to delete the specified profile.
`device profile rename <profile name> <profile name>`	Renames the specified Device Insight profile (first *profile name*) to the specified Device Insight profile name (second *profile name*).
`show reference object device <profile name>`	Displays which configuration settings reference the specified Device Insight profile.
`device remove mac <mac address>`	Removes a client from the table that's no longer connected to your network. For example, guest A visited your company over a month ago. Guest A used his cellphone to connect to your Zyxel Device networks. Guest A has left for over a month and you're sure he will not return in the near future. You can remove his device using this command. Please note that clients that are blocked cannot be removed. Make sure to unblock clients before you remove them.

Table 247 Command Summary: Device Insight Profiles (continued)

COMMAND	DESCRIPTION
`device feedback mac <mac address> category <category> os <os> type <type>`	Reports on a client that is wrongly identified regarding its category, operating system or type. Enter the category, operating system or type you believe is correct for the client.
`[no] device profile <profile name> description <description>`	Sets a description for the specified Device Insight profile. You can use up to 60 printable ASCII characters. Use the `no` command to delete the description for this profile.
`[no] device profile <profile name> category <category>`	Configures the type of device used by the connected client for the specified profile. The category includes: • Computer • Firewall • Game Consoles • IP Camera • IP Phone • IoT: A device with sensors and software that collects and analyzes data. It exchanges the data it collects with other devices over the Internet. • Media Player • Mobile Phone/Tablet • Network Storage • Printer • Projector • Router • Smart TV • Switch • Wireless AP • Others: A device will be sorted as others when the Zyxel Device cannot sort the device into the categories above.
`[no] device profile <profile name> os <os>`	Configures the device operating system used by the connected client for the specified profile.
`secure policy <1...500> device <profile name>`	Applies the specified profile to the specified secure policy.

49.1.2 Device Insight Command Examples

Here's the process to use a Device Insight profile in a Zyxel Device security policy. Th example below uses the parameters in this table.

Table 248 Device Insight Profile Configuration Example

PROFILE NAME	DESCRIPTION	CATEGORY	OPERATING SYSTEM	APPLIED POLICY
MobilePhone	profile for mobile clients	mobile-phone-tablet	• Windows • macOS • Linux • OS • Android • Others	LAN2_To_LAN1

The security policy LAN2_To_LAN1 uses the parameters in this table.

Table 249 Security Policy Configuration Example

TO	FROM	ACTION	DEVICE INSIGHT PROFILE
LAN1	LAN2	deny	MobilePhone

1 Create a Device Insight profile, for example, clients connected to the Zyxel Device LAN using mobile phones.

```
Router# configure terminal
Router(config)# device profile MobilePhone
Router(config)# device profile MobilePhone description profile for mobile clients
Router(config)# device profile MobilePhone category
computer            gaming-consoles      ip-camera           media-player
network-storage       printer               router               switch
firewall              iot                   ip-phone             mobile-phone-
tablet   others              projector           smart-tv            wireless-ap
Router(config)# device profile MobilePhone category mobile-phone-tablet
Router(config)# device profile MobilePhone os
android   ios       linux     macos     others    windows
Router(config)# device profile MobilePhone os android
Router(config)# device profile MobilePhone os ios
Router(config)# device profile MobilePhone os linux
Router(config)# device profile MobilePhonee os macos
Router(config)# device profile MobilePhone os others
Router(config)# device profile MobilePhone os windows
```

2 Create a new security policy. Name it as LAN2_To_LAN1.

```
Router(config)# secure-policy 14
Router(secure-policy)# name LAN2_To_LAN1
```

3 Configure the traffic direction for the security policy LAN2_To_LAN1. Add the created Device Insight profile to the security policy.

```
Router(secure-policy)# from LAN2
Router(secure-policy)# to LAN1
Router(secure-policy)# device MobilePhone
```

4 The Zyxel Device will block clients if they match the settings you configure in the Device Insight profile and the security policy action is set to deny.

```
Router(secure-policy)# action deny
Router(secure-policy)# exit
```

To remove a blocked client's device from the Device Insight database, you need to unblock the client's device first.

```
Router(config)# no device block mac 00:00:5e:00:53:af
% Set device unblock success
Router(config)# device remove mac 00:00:5e:53:af
```

CHAPTER 50
User/Group

This chapter describes how to set up user accounts, user groups, and user settings for the Zyxel Device. You can also set up rules that control when users have to log in to the Zyxel Device before the Zyxel Device routes traffic for them.

50.1 User Account Overview

A user account defines the privileges of a user logged into the Zyxel Device. User accounts are used in firewall rules and application patrol, in addition to controlling access to configuration and services in the Zyxel Device.

50.1.1 User Types

There are the types of user accounts the Zyxel Device uses.

Table 250 Types of User Accounts

TYPE	ABILITIES	LOGIN METHOD(S)
Admin Users		
Admin	Change Zyxel Device configuration (web, CLI)	WWW, TELNET, SSH, FTP
Limited-Admin	Look at Zyxel Device configuration (web, CLI) Perform basic diagnostics (CLI)	WWW, TELNET, SSH
Access Users		
User	Access network services Browse user-mode commands (CLI)	WWW, TELNET, SSH
Guest	Access network services	WWW
Ext-User	External user account	WWW
ext-group-user	External group user account	WWW

Note: The default admin account is always authenticated locally, regardless of the authentication method setting. (See Chapter 56 on page 479 for more information about authentication methods.)

50.2 User/Group Commands Summary

The following table identifies the values required for many `username/groupname` commands. Other input values are discussed with the corresponding commands.

Table 251 username/groupname Command Input Values

LABEL	DESCRIPTION
username	The name of the user (account). You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
groupname	The name of the user group. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. It cannot be the same as the user name.

The following sections list the `username/groupname` commands.

50.2.1 User Commands

The first table lists the commands for users.

Table 252 username/groupname Commands Summary: Users

COMMAND	DESCRIPTION
`show username [`*username*`]`	Displays information about the specified user or about all users set up in the Zyxel Device.
`username` *username* `nopassword user-type {admin | guest | limited-admin | user}`	Creates the specified user (if necessary), disables the password, and sets the user type for the specified user.
`username` *username* `password` *password* `user-type {admin | guest | limited-admin | user}`	Creates the specified user (if necessary); enables and sets the password; and sets the user type for the specified user. *password*: You can use 1-63 printable ASCII characters, except double quotation marks (") and question marks (?).
`username` *username* `user-type ext-user`	Creates the specified user (if necessary) and sets the user type to Ext-User.
`username` *username* `user-type mac-address`	Creates the specified user (if necessary) and sets the user type to mac-address.
`username` *username* `user-type ext-group-user associated-aaa-server` *server_profile* `group-id` *id*	Specifies the value of the AD or LDAP server's Group Membership Attribute that identifies the group to which the specified ext-group-user type user account belongs.
`username username encrypted-password` *<password>*	Sets the password for the specified user.
`no username` *username*	Deletes the specified user.
`username rename` *username username*	Renames the specified user (first *username*) to the specified username (second *username*).
`username` *username* `[no] description` *description*	Sets the description for the specified user. The `no` command clears the description. *description*: You can use alphanumeric and `()+/:=?!*#@$_%-` characters, and it can be up to 60 characters long.

Table 252 username/groupname Commands Summary: Users (continued)

COMMAND	DESCRIPTION
`username username logon-time-setting <default | manual>`	Sets the account to use the factory default lease and reauthentication times or custom ones.
`username username [no] logon-lease-time <0..1440>`	Sets the lease time for the specified user. Set it to zero to set unlimited lease time. The *no* command sets the lease time to five minutes (regardless of the current default setting for new users).
`username username [no] logon-re-auth-time <0..1440>`	Sets the reauthorization time for the specified user. Set it to zero to set unlimited reauthorization time. The no command sets the reauthorization time to thirty minutes (regardless of the current default setting for new users).
`username username [no] email <1..2> email-address`	Specifies up to two email addresses for a user account. The *no* command removes the specified email address for this account. *email-address:* Should be in the <user@domainname> format.
`username username [no] phone phone_number`	Sets the mobile phone number for the account. The *no* command removes the specified mobile phone number for this account. *phone_number:* 20 character length, including numbers 1~9 and characters +*#()-
`username username vlan activate`	Enables dynamic VLAN assignment for the user account. Dynamic VLAN assignment allows you to assign a user to a specific VLAN based on the user credentials.
`username username vlan id <1..4094>`	Sets the ID number of the VLAN to which this user account is assigned after authentication is successful.
`username username [no] {email1-verify|email2-verify}`	Sends an authorization email with a code of six digits. The authorization email will be sent to the email address set for the account.
`_two-factor-auth-send email email user username verification-code verification_code`	Enters the authorization code to verify your email address for the account.
`username username [no] phone-verify`	Sends an SMS message with a code of six digits. The SMS message will be sent to the mobile phone number set for the account.
`sms-service _two-factor-auth-admin-send phone phone user username verification-code verification_code`	Enters the authorization code to verify your mobile telephone number for the account.
`[no] pwd-expiry force-to-change-pwd activate`	Enforces a periodic password change. The *no* command removes the requirement.
`[no] pwd-expiry expiration days <1..365>`	Sets how often users must change their password when they log into the Zyxel Device. You can choose from once a day to once a year. The *no* command removes the requirement.
`pwd-expiry link-to-device custom {myrouter | <FQDN> | <IPv6 Address> | <W.X.Y.X>}`	Set the host part of the hyperlink in the password expiration notice email. Please note that myrouter is accessible only if the user is in the LAN of this Zyxel Device, and there are no other Zyxel gateways in between.
`pwd-expiry expiration send-now`	Sends a password expiration e-mail immediately.

Table 252 username/groupname Commands Summary: Users (continued)

COMMAND	DESCRIPTION
`[no] password complexity-verify`	Enforces a complex user password consisting of at least 8 characters and at most 64. At least 1 character must be a number, at least 1 a lower case letter, at least 1 an upper case letter and at least one special character from the keyboard, such as `~!@#$%^&*()_+={}|;:'<,>./\"- The *no* command removes the requirement.
`show pwd-expiry {all | expiration | force-to-change-pwd | link-to-device}`	Displays if a password must be changed (`force-to-change-pwd`), when a password will expire (`expiration`) and the host part of the hyperlink in the password expiration notice email (`link-to-device`).
`show password complexity-verify status`	Displays if a complex user password as defined above is required.

50.2.2 User Group Commands

This table lists the commands for groups.

Table 253 username/groupname Commands Summary: Groups

COMMAND	DESCRIPTION
`show groupname [`*`groupname`*`]`	Displays information about the specified user group or about all user groups set up in the Zyxel Device.
`[no] groupname` *`groupname`*	Creates the specified user group if necessary and enters sub-command mode. The no command deletes the specified user group.
`[no] description` *`description`*	Sets the description for the specified user group. The no command clears the description for the specified user group.
`[no] groupname` *`groupname`*	Adds the specified user group (second *`groupname`*) to the specified user group (first *`groupname`*).
`[no] user` *`username`*	Adds the specified user to the specified user group.
`groupname rename` *`groupname groupname`*	Renames the specified user group (first *`groupname`*) to the specified group-name (second *`groupname`*).

50.2.3 User Setting Commands

This table lists the commands for user settings, except for forcing user authentication.

Table 254 username/groupname Commands Summary: Settings

COMMAND	DESCRIPTION
`show users default-setting {all | user-type {admin|user|guest|limited-admin|ext-user| ext-group-user}}`	Displays the default lease and reauthentication times for the specified type of user accounts.
`users default-setting [no] logon-lease-time <0..1440>`	Sets the default lease time (in minutes) for each new user. Set it to zero to set unlimited lease time. The no command sets the default lease time to five.

Table 254 username/groupname Commands Summary: Settings (continued)

COMMAND	DESCRIPTION
`users default-setting [no] logon-re-auth-time <0..1440>`	Sets the default reauthorization time (in minutes) for each new user. Set it to zero to set unlimited reauthorization time. The no command sets the default reauthorization time to thirty.
`users default-setting [no] user-type <admin |ext-user|guest|limited-admin|user|ext-group-user>`	Sets the default user type for each new user. The no command sets the default user type to user.
`users default-setting [no] user-type <admin |ext-user|guest|limited-admin|user|ext-group-user> logon-lease-time <0..1440>`	Sets the default lease time (in minutes) for each type of new user. Set it to zero for unlimited lease time. The no command sets the default lease time to five.
`users default-setting [no] user-type <admin |ext-user|guest|limited-admin|user|ext-group-user> logon-re-auth-time <0..1440>`	Sets the default reauthorization time (in minutes) for each type of new user. Set it to zero for unlimited reauthorization time. The no command sets the default reauthorization time to thirty.
`show users retry-settings`	Displays the current retry limit settings for users.
`[no] users retry-limit`	Enables the retry limit for users. The no command disables the retry limit.
`[no] users retry-count <1..99>`	Sets the number of failed login attempts a user can have before the account or IP address is locked out for lockout-period minutes. The no command sets the retry-count to five.
`[no] users lockout-period <1..65535>`	Sets the amount of time, in minutes, a user or IP address is locked out after retry-count number of failed login attempts. The no command sets the lockout period to thirty minutes.
`show users simultaneous-logon-settings`	Displays the current settings for simultaneous logins by users.
`[no] users simultaneous-logon {administration | access} enforce`	Enables the limit on the number of simultaneous logins by users of the specified account-type. The no command disables the limit, or allows an unlimited number of simultaneous logins.
`[no] users simultaneous-logon {administration | access} limit <1..1024>`	Sets the limit for the number of simultaneous logins by users of the specified account-type. The no command sets the limit to one.
`show users update-lease-settings`	Displays whether or not access users can automatically renew their lease time.
`[no] users update-lease automation`	Lets users automatically renew their lease time. The no command prevents them from automatically renewing it.
`show users idle-detection-settings`	Displays whether or not users are automatically logged out, and, if so, how many minutes of idle time must pass before they are logged out.
`[no] users idle-detection`	Enables logging users out after a specified number of minutes of idle time. The no command disables logging them out.
`[no] users idle-detection timeout <1..60>`	Sets the number of minutes of idle time before users are automatically logged out. The no command sets the idle-detection timeout to three minutes.

50.2.3.1 User Setting Command Examples

The following commands show the current settings for the number of simultaneous logins.

```
Router# configure terminal
Router(config)# show users simultaneous-logon-settings
enable simultaneous logon limitation for administration account: yes
maximum simultaneous logon per administration account          : 1
enable simultaneous logon limitation for access account        : yes
maximum simultaneous logon per access account                  : 3
```

50.2.3.2 Create User Accounts Command Examples

Lease time is the idle timeout for a specific user. A logged in user must use the web configurator or CLI before he is logged out.

Reauthentication time is the number of minutes the user can be logged into the Zyxel Device in one session before the user has to log in again.

For example, suppose you've set the lease time to 30 minutes and the reauthentication time to 60 minutes. See the comparison table below for more information on the differences between lease time and reauthentication time.

Table 255 Lease Time and Reauthentication Time Comparison Table

	USER ACTION	RESULT
Lease Time	The user has used the Zyxel Device web configurator or CLI within 30 minutes.	The user will not be logged out.
	The user has not used the Zyxel Device web configurator or CLI for over 30 minutes.	The user will be logged out.
Reauthentication Time	The user has used the Zyxel Device web configurator or CLI within 60 minutes.	After 60 minutes, the user will be logged out. He must log in again.
	The user has not used the Zyxel Device web configurator or CLI for over 60 minutes.	

You want to log the admin account Max out if 60 minutes of idle time have passed, that is, he has not been using the Zyxel Device web configurator or CLI.

You want to make the number of minutes unlimited so the admin account Max will not have to log in again after a certain time period.

Table 256 Create User Account Example

USER NAME	PASSWORD	USER TYPE
Max	1234	admin

1 Create an admin account using the parameters given above.

```
Router# configure terminal
Router(config)# username Max password 1234 user-type admin
Router(config)# username Max logon-lease-time 60
Router(config)# username Max logon-re-auth-time 0
```

2 Save the current configuration to the Zyxel Device.

```
Router(config)# write
```

50.2.4 MAC Auth Commands

This table lists the commands for creating a list of MAC addresses. Only WiFi clients using the MAC addresses you specified can access the Internet or the network behind the Zyxel Device. Please note that you need to first configure an SSID security profile MAC authentication settings to have the AP authenticate WiFi clients by their MAC addresses.

Table 257 MAC-Auth Commands Summary

COMMAND	DESCRIPTION
`[no] mac-auth database mac` *`mac_address`* `type ext-mac-address mac-role` *`mac-users`* `description` *`description`*	Maps the specified MAC address authenticated by an external server to the specified MAC role. The MAC role is a MAC address user account. The MAC address you set here will be mapped to the MAC address user account. When a WiFi client connects to the Zyxel Device, the Zyxel Device will check the WiFi client MAC address to see if the WiFi client MAC address has been mapped with the MAC address user account. The `no` command deletes the mapping between the MAC address and the MAC role.
`[no] mac-auth database mac` *`mac_address`* `type int-mac-address mac-role` *`mac-users`* `description` *`description`*	Maps the specified MAC address authenticated by the Zyxel Device's local user database to the specified MAC role. The MAC role is a MAC address user account. The MAC address you set here will be mapped to the MAC address user account. When a WiFi client connects to the Zyxel Device, the Zyxel Device will check the WiFi client MAC address to see if the WiFi client MAC address has been mapped with the MAC address user account. The `no` command deletes the mapping between the MAC address and the MAC role.

Table 257 MAC-Auth Commands Summary (continued)

COMMAND	DESCRIPTION
`[no] mac-auth database mac` *`oui`* `type ext-oui mac-role` *`mac-users`* `description` *`description`*	Maps the specified OUI (Organizationally Unique Identifier) authenticated by an external server to the specified MAC role. The MAC role is a MAC address user account. The MAC address you set here will be mapped to the MAC address user account. When a WiFi client connects to the Zyxel Device, the Zyxel Device will check the WiFi client MAC address to see if the WiFi client MAC address has been mapped with the MAC address user account. The OUI is the first three octets in a MAC address and uniquely identifies the manufacturer of a network device. The no command deletes the mapping between the OUI and the MAC role.
`[no] mac-auth database mac` *`oui`* `type int-oui mac-role` *`mac-users`* `description` *`description`*	Maps the specified OUI (Organizationally Unique Identifier) authenticated by the Zyxel Device's local user database to the specified MAC role. The MAC role is a MAC address user account. The MAC address you set here will be mapped to the MAC address user account. When a WiFi client connects to the Zyxel Device, the Zyxel Device will check the WiFi client MAC address to see if the WiFi client MAC address has been mapped with the MAC address user account. The OUI is the first three octets in a MAC address and uniquely identifies the manufacturer of a network device. The no command deletes the mapping between the OUI and the MAC role.

50.2.4.1 MAC Auth Example

This example uses an external server to authenticate wireless clients by MAC address. After authentication the Zyxel Device maps the wireless client to a mac-address user account (MAC role). Configure user-aware features to control MAC address user access to network services.

The following commands:

- Create a MAC role (mac-address user type user account) named Zyxel-mac
- Map a wireless client's MAC address of 00:13:49:11:a0:c4 to the Zyxel-mac MAC role (MAC address user account)
- Modify the WLAN security profile named secureWLAN1 as follows:
  - Turn on MAC authentication
  - Use the authentication method named Auth1
  - Use colons to separate the two-character pairs within account MAC addresses

- Use upper case letters in the account MAC addresses

```
Router(config)# username Zyxel-mac user-type mac-address
Router(config)# mac-auth database mac 00:13:49:11:a0:c4 type ext-mac-address
mac-role Zyxel-mac description zyxel mac

3. Modify wlan-security-profile
Router(config)# wlan-security-profile secureWLAN1
Router(config-wlan-security default)# mac-auth activate
Router(config-wlan-security default)# mac-auth auth-method Auth1
Router(config-wlan-security default)# mac-auth delimiter account colon
Router(config-wlan-security default)# mac-auth case account upper
Router(config-wlan-security default)# exit
```

50.2.5 Additional User Commands

This table lists additional commands for users.

Table 258 username/groupname Commands Summary: Additional

COMMAND	DESCRIPTION
`show users {`*`username`*` | all | current}`	Displays information about the users logged onto the system.
`show lockout-users`	Displays users who are currently locked out.
`unlock lockout-users {`*`ip`*` | console|` *`ipv6_addr`*`}`	Unlocks the specified IP address.
`users force-logout {`*`username`*` |` *`ip`*` |` *`ipv6_addr`*`}`	Logs out the specified login.

50.2.5.1 Additional User Command Examples

The following commands display the users that are currently logged in to the Zyxel Device and forces the

logout of all logins from a specific IP address.

```
Router# configure terminal
Router(config)# show users all
No: 1
  Name: admin
  Type: admin
  From: 172.21.40.9
  Country_Code: RIP
  Country_Name: Private IP
  MAC: DC:4A:3E:40:EC:67
  Associated AP: -
  Service: http/https
  Login_Time: 03:59:48
  Idle_Time: unlimited
  Lease_Timeout: 21:59:49
  Re_Auth_Timeout: 20:00:12
  Remaining_Time: n/a
  Total_Quota: -
  Upload_quota: -
  Download_quota: -
  Upload_Bandwidth: unlimited
  Upload_Bandwidth_Priority: 7
  Download_Bandwidth: unlimited
  Download_Bandwidth_Priority: 7
  Session_Timeout: unlimited
  Acct. Status: -
  Profile Name: N/A
  User_Info: admin(admin)
  Mobile: N/A
  Email: N/A
No: 2
  Name: admin
  Type: admin
  From: console
  Country_Code: -
  Country_Name: -
  MAC: -
  Associated AP: -
  Service: console
  Login_Time: 02:07:23
  Idle_Time: unlimited
  Lease_Timeout: 24:00:00
  Re_Auth_Timeout: 21:52:37
  Remaining_Time: n/a
  Total_Quota: -
  Upload_quota: -
  Download_quota: -
  Upload_Bandwidth: unlimited
  Upload_Bandwidth_Priority: 7
  Download_Bandwidth: unlimited
  Download_Bandwidth_Priority: 7
  Session_Timeout: unlimited
  Acct. Status: -
  Profile Name: N/A
  User_Info: admin(admin)
  Mobile: N/A
  Email: N/A
```

The following commands display the users that are currently locked out and then unlocks the user who is displayed.

```
Router# configure terminal
Router(config)# show lockout-users
No.  Username Tried                  From            Lockout Time Remaining
================================================================================
No.  From            Failed Login Attempt    Record Expired Timer
================================================================================
1    172.16.1.5             2                       46

Router(config)# unlock lockout-users 172.16.1.5
User from 172.16.1.5 is unlocked
Router(config)# show lockout-users
No.  Username Tried                  From            Lockout Time Remaining
================================================================================
No.  From            Failed Login Attempt    Record Expired Timer
================================================================================
```

CHAPTER 51
Application Object

Check that you have the latest IDP and App Patrol signatures.

51.1 Application Object Commands Summary

The following table describes the values required for many application object commands. Other values are discussed with the corresponding commands.

Table 259 Input Values for Application Object Commands

LABEL	DESCRIPTION
<object>	Type the name of the object.
<description>	This is a description of the object
<sid>	This is the associated IDP and App Patrol signature ID number.

51.1.1 Application Object Commands

This table lists the application object commands.

Table 260 `application-object` Commands

COMMAND	DESCRIPTION
`show application-object <object>`	Displays information on the named application object.
`application-object <object>`	Creates an object with the specified name. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. The no command disables it.
`[no] description <description>`	Write a description of the object.
`[no] application <sid>`	Write a valid signature ID for the object. The no command disables it.
`no application-object <object>`	Deletes the object with the specified name.
`application-object rename <object> <object>`	Renames the specified object with a new name.

51.1.1.1 Application Object Examples

These are some example usage commands.

```
Router(config)# show application-object
Name
Description                                                    Ref
Content
================================================================================
======
tests
New Create                                                     1
Facebook Game (access)
Router(config)# show application-object tests
Name: tests
Description: New Create
Category                        Application
Application ID
================================================================================
======
Social Network                  Facebook Game (access)
402685702
Router(config)#
```

51.1.2 Application Object Group Commands

This table lists the application object group commands.

Table 261 `object-group application` Commands

COMMAND	DESCRIPTION
`show object-group application <object>`	Displays information on the named application object group.
`object-group application <object>`	Creates an object group. with the specified name. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. The no command disables it.
`[no] description <description>`	Write a description of the object group.
`[no] application-object <object>`	Adds the named application object to the object group. The no command removes it.
`[no] object-group <object>`	Creates an object group. The no command removes it.
`no object-group application <object>`	Deletes the object group with the specified name.
`object-group application rename <object> <object>`	Renames the specified object group with a new name.

51.1.2.1 Object Group Application Examples

These are some example usage commands.

```
Router(config)# show object-group application
Name
Description                                                     Ref
Member
================================================================================
======
Router(config)# object-group application may
Router(group-application)# description rinse after use
Router(group-application)# exit
Router(config)# show object-group application
Name
Description                                                     Ref
Member
================================================================================
======
may
rinse after use                                                 0
tests
Router(config)#
```

CHAPTER 52
Addresses

This chapter describes how to set up addresses and address groups for the Zyxel Device.

52.1 Address Overview

Address objects can represent a single IP address or a range of IP addresses. Address groups are composed of address objects and other address groups.

You can create IP address objects based on an interface's IP address, subnet, or gateway. The Zyxel Device automatically updates these objects whenever the interface's IP address settings change. This way every rule or setting that uses the object uses the updated IP address settings. For example, if you change the LAN1 interface's IP address, the Zyxel Device automatically updates the corresponding interface-based, LAN1 subnet address object. So any configuration that uses the LAN1 subnet address object is also updated.

Address objects and address groups are used in dynamic routes, firewall rules, application patrol, content filtering, and VPN connection policies. For example, addresses are used to specify where content restrictions apply in content filtering. Please see the respective sections for more information about how address objects and address groups are used in each one.

Address groups are composed of address objects and address groups. The sequence of members in the address group is not important.

52.2 Address Commands Summary

The following table describes the values required for many address object and address group commands. Other values are discussed with the corresponding commands.

Table 262 Input Values for Address Commands

LABEL	DESCRIPTION
object_name	The name of the address. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
group_name	The name of the address group. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
interface_name	The name of the interface. This depends on the Zyxel Device model. For some models, use ge*x*, *x* = 1 ~ N, where N equals the highest numbered Ethernet interface for your Zyxel Device model. For other models, use a name such as wan1, wan2, opt, lan1, or dmz.

The following sections list the address object and address group commands.

52.2.1 Address Object Commands

There are the types of address objects:

- HOST - the object uses an IP Address to define a host address
- RANGE - the object uses a range address defined by a Starting IP Address and an Ending IP Address
- SUBNET - the object uses a network address defined by a Network IP address and Netmask subnet mask
- INTERFACE IP - the object uses the IP address of one of the Zyxel Device's interfaces
- INTERFACE SUBNET - the object uses the subnet mask of one of the Zyxel Device's interfaces
- INTERFACE GATEWAY - the object uses the gateway IP address of one of the Zyxel Device's interfaces
- GEOGRAPHY - the object uses the IP addresses of a country to represent a country
- FQDN - the object uses a FQDN (Fully Qualified Domain Name). An FQDN consists of a host and domain name. For example, www.zyxel.com is a fully qualified domain name. FQDN in address objects can be used in Security Policy, Policy Route, BWM and Web Authentication profiles as source and destination criteria. FQDN with a wildcard (for example, *.zyxel.com) can be used in these profiles as destination criteria only. An FQDN is resolved to its IP address using the DNS server configured on the Zyxel Device. If the Zyxel Device receives a DNS query for an FQDN and the Zyxel Device has an FQDN cache entry, the Zyxel Device can map the IP address in a DNS response without having to query a DNS name server.

This table lists the commands for address objects.

Table 263 address-object and address6-object Commands

COMMAND	DESCRIPTION
`show {address-object | address6-object | service-object | schedule-object} [object_name]`	Displays information about the specified object or all the objects of the specified type.
`address-object object_name {ip | ip_range | ip_subnet | fqdn fqdn| geography country code | interface-ip | interface-subnet | interface-gateway} {interface_name | virtual interface name}`	Creates the specified IPv4 address object using the specified parameters. *ip* <W.X.Y.Z> Enter an IPv4 address. *ip_range* <W.X.Y.Z>-<W.X.Y.Z> Enter an IPv4 address range. *ip_subnet* <W.X.Y.Z>/<1..32> Enter an IPv4 subnet in CIDR format. For example, 192.168.1.0/32. fqdn Enter a fully-qualified domain name. *country code* Enter a country or continent code (represents an IP address for that country/continent). *interface-gateway / interface-ip / interface-subnet* Enter an *interface_name* or a *virtual_interface_name*
`address-object object_name geography <country code> all`	Creates a GEOGRAPHY object representing all IPv4 address of the specified country. Use the command, `geo-ip [no] geography <country_code> all address {ipv4 | ip6}`, to configure the custom country-to-IP/continent-to-IP address mappings for a GEOGRAPHY object.
`no address-object object_name`	Deletes the specified address object.

Table 263 address-object and address6-object Commands (continued)

COMMAND	DESCRIPTION
`address-object rename object_name object_name`	Renames the specified address (first *object_name*) to the second *object_name*.
`address6-object object_name {ip | ip_range | ip_subnet | fqdn fqdn| geography country code | interface-ip | interface-subnet | interface-gateway} {interface_name | virtual interface name}`	Creates the specified IPv6 address object using the specified parameters. *ip* <W.X.Y.Z> Enter an IPv6 address. *ip_range* <W.X.Y.Z>-<W.X.Y.Z> Enter an IPv6 address range. *ip_subnet* <W.X.Y.Z>/<1..32> Enter an IPv6 subnet. For example, 192.168.1.0/32. fqdn Enter a fully-qualified domain name. *country code* Enter a country or continent code (represents an IP address for that country/continent). *interface-gateway / interface-ip /interface-subnet* Enter an *interface_name* or a *virtual_interface_name*
`address6-object object_name geography <country code> all`	Creates a GEOGRAPHY object representing all IPv6 address of the specified country. Use the command, `geo-ip [no] geography <country_code> all address {ipv4 | ip6}`, to configure the custom country-to-IP/continent-to-IP address mappings for a GEOGRAPHY object.
`[no] address6-object object_name {ipv6_address | ipv6_range | ipv6_subnet}`	Creates the specified IPv6 address object using the specified parameters. The no command removes the specified address object. *ipv6_address*: IPv6 address *ipv6_range*: IPv6 address range. For example: fe80:1234::1-fe80:1234::ffff *ipv6_subnet*: IPv6 prefix format. For example: fe80::211:85ff:fe0e:dec/128
`[no] address6-object OBJECT_NAME interface-ip interface {dhcpv6 | link-local | slaac | static} {addr_index}`	Creates the specified IPv6 address object based on the specified interface object. Specify whether it is a DHCPv6 server, link-local IP address, StateLess Address Auto Configuration IP address (slaac), or static IPv6 address. The no command removes the specified address object.
`[no] address6-object object_name interface-subnet interface {dhcpv6 | slaac | static} {addr_index}`	Creates the specified IPv6 address object based on the specified interface subnet object. Specify whether it is a DHCPv6 server, SLAAC, or static IPv6 address. The no command removes the specified address object.
`[no]address6-object object_name interface-gateway interface {slaac | static} {addr_index}`	Creates the specified IPv6 address object based on the specified interface gateway object. Specify whether it is a SLAAC or static IPv6 address. The no command removes the specified address object.
`fqdn-object query-period <1..1440>`	Configures how long (1-1440 seconds) the Zyxel Device should wait for a reply from the DNS server configured on the Zyxel Device in order to update FQDN - IP cache entries.
`fqdn-object sync-period <1..5>`	Configures how often (1-5 seconds) the Zyxel Device should query the DNS server configured on the Zyxel Device to update FQDN - IP cache entries.

Table 263 address-object and address6-object Commands (continued)

COMMAND	DESCRIPTION
`fqdn-object test fqdn`	*fqdn* Tests an FQDN object by entering a fully-qualified domain name.
`show fqdn-object all`	Displays all FQDN objects with IPv4 addresses configured on the Zyxel Device.
`show fqdn-object6 all`	Displays all FQDN objects with IPv6 addresses configured on the Zyxel Device.
`show fqdn`	Displays the FQDN host name and domain name configured on the Zyxel Device.
`show fqdn-object query-period`	Displays how often (1-5 seconds) the Zyxel Device should query the DNS server configured on the Zyxel Device to update FQDN - IP cache entries.
`show fqdn-object sync-period`	Displays how often (1-5 seconds) the Zyxel Device should query the DNS server configured on the Zyxel Device to update FQDN - IP cache entries.

52.2.1.1 Address Object Command Examples

The following example creates three IPv4 address objects and then deletes one.

```
Router# configure terminal
Router(config)# address-object A0 192.168.1.1
Router(config)# address-object A1 192.168.1.1-192.168.1.20
Router(config)# address-object A2 192.168.1.0/24
Router(config)# show address-object
Object name                    Type    Address                         Ref.
=====================================================================
A0                             HOST    192.168.1.1                       0
A1                             RANGE   192.168.1.1-192.168.1.20      0
A2                             SUBNET 192.168.1.0/24                  0
Router(config)# no address-object A2
Router(config)# show address-object
Object name                    Type    Address                         Ref.
=====================================================================
A0                             HOST    192.168.1.1                       0
A1                             RANGE   192.168.1.1-192.168.1.20      0
```

The following example shows FQDN command usage.

```
Router# show fqdn
host name  : usg110
domain name: none
FQDN       : usg110
Router# show fqdn-object query-period
FQDN Object Query Period: 2
Router# show fqdn-object sync-period
FQDN Object Sync Period: 1
Router(config)# fqdn-object test usg110
FQDN: usg110
Address
================================================================================
127.0.0.1

Router(config)#
```

The following example creates host, range, subnet, and link local IPv6 address objects and then deletes the subnet IPv6 address object.

```
> enable
Router# configure terminal
Router(config)# address6-object B0 fe80::211:85ff:fe0e:cdec
Router(config)# address6-object B1 fe80::211:85ff:fe0e:1-fe80::211:85ff:fe0e:ff
Router(config)# address6-object B2 fe80::211:85ff:fe0e:cdec/128
Router(config)# address6-object B3 interface-ip ge1 link-local
Router(config)# show address6-object
Object name                    Type              Address Type               Index
Address
Note            Ref.
==============================================================================
B0                             HOST
fe80::211:85ff:fe0e:cdec
                0
B1                             RANGE
fe80::211:85ff:fe0e:1-fe80::211:85ff:fe0e:ff
                0
B2                             SUBNET
fe80::211:85ff:fe0e:cdec/128
                0
B3                             INTERFACE IP       LINK LOCAL                1
fe80::213:49ff:feaa:cb88
ge1             0

Router(config)# no address6-object B2
Router(config)# show address6-object
Object name                    Type              Address Type               Index
Address
Note            Ref.
==============================================================================
B0                             HOST
fe80::211:85ff:fe0e:cdec
                0
B1                             RANGE
fe80::211:85ff:fe0e:1-fe80::211:85ff:fe0e:ff
                0
B3                             INTERFACE IP       LINK LOCAL                1
fe80::213:49ff:feaa:cb88
ge1             0
```

52.2.2 Address Group Commands

This table lists the commands for address groups.

Table 264 object-group Commands: Address Groups

COMMAND	DESCRIPTION
`show object-group {address | address6} [group_name]`	Displays information about the specified address group or about all address groups.
`[no] object-group address group_name`	Creates the specified address group if necessary and enters sub-command mode. The no command deletes the specified address group.
`[no] address-object object_name`	Adds the specified address to the specified address group. The no command removes the specified address from the specified group.

Table 264 object-group Commands: Address Groups (continued)

COMMAND	DESCRIPTION
[no] object-group *group_name*	Adds the specified address group (second *group_name*) to the specified address group (first *group_name*). The no command removes the specified address group from the specified address group.
[no] description *description*	Sets the description to the specified value. The no command clears the description. *description*: You can use alphanumeric and ()+/ :=?!*#@$_%- characters, and it can be up to 60 characters long.
object-group address rename *group_name group_name*	Renames the specified address group from the first *group_name* to the second *group_name*.

52.2.2.1 Address Group Command Examples

The following commands create three address objects A0, A1, and A2 and add A1 and A2 to address group RD.

```
Router# configure terminal
Router(config)# address-object A0 192.168.1.1
Router(config)# address-object A1 192.168.1.2-192.168.2.20
Router(config)# address-object A2 192.168.3.0/24
Router(config)# object-group address RD
Router(group-address)# address-object A1
Router(group-address)# address-object A2
Router(group-address)# exit
Router(config)# show object-group address
Group name                      Reference
Description
================================================================================
TW_TEAM                         5

RD                              0

Router(config)# show object-group address RD
Object/Group name               Type   Reference
================================================================================
A1                              Object 1
A2                              Object 1
```

52.2.3 FQDN Object

If the Zyxel Device receives a DNS query for an FQDN and the Zyxel Device has an FQDN cache entry, the Zyxel Device can map the IP address in a DNS response without having to query a DNS name server.

FQDN can be used in Security Policy, Policy Route, BWM and Web Authentication profiles as source and destination criteria. FQDN with a wildcard (for example, *.zyxel.com) can be used in these profiles as destination criteria only.

52.2.4 Geo IP

Use these commands to update the database of country-to-IP address mappings and manually configure custom country-to-IP address mappings in geographic address objects. You can then use geographic address objects in security policies to forward or deny traffic to whole countries or regions.

Note: You need to have a registered Content Filter 2.0 Service license to use the country-to-IP and continent-to-IP address database.

52.2.5 FQDN / Geo IP Commands

You must be in configuration mode (`configure terminal`) to use the indented commands shown below.

Table 265 `FQDN / Geo IP` Commands

COMMAND	DESCRIPTION
`[no] geo-ip database update auto`	Enables the Zyxel Device to automatically check for the latest country-to-IP-address database version on myZyxel.com and allows it to be automatically updated when there is newer version available. The no command disallows the Zyxel Device automatically checking for the latest country-to-IP-address database version on myZyxel.com.
`geo-ip database update country`	Updates the country-to-IP-address database for all countries.
`geo-ip database update weekly {fri | mon | sat | sun | thu | tue | wed} <0..23>`	Specifies the weekly day and time the Zyxel Device should check for the latest country-to-IP-address database version on myZyxel.com if automatic checking is enabled.
`geo-ip [no] geography <country_code> all address {ipv4 | ip6}`	Creates a new geography-to-IP-address mapping for the specified country. Use `show geo-ip country-code` to see the 2-letter abbreviation for each country. The no command removes the new geography-to-IP-address mapping for the specified country.
`show geo-ip database update`	Shows if the country-to-IP address database is automatically updated and the schedule.
`show geo-ip database version`	Shows the latest and current country-to-IP-address database version.
`show geo-ip database version country`	Shows the latest and current country-to-IP-address database version.
`show geo-ip country-code`	Shows the 2-letter abbreviation for each country.
`show geo-ip country-list region code`	Shows the countries that belong to the continent.
`show geo-ip region-code`	Shows the 2-letter abbreviation for each continent.
`show geo-ip geography`	Shows customized country-to-IPv4-address mappings.
`show geo-ip geography6`	Shows customized country-to-IPv6-address mappings.

52.2.6 Geo IP Command Examples

The following shows Geo IP command examples.

```
Router(config)# geo-ip database update auto
Router(config)# geo-ip database update weekly thu 17
Router(config)# exit
Router# show geo-ip database update
auto: yes
schedule: weekly at Thursday 17 o'clock
Router# show geo-ip database version
country latest version : 20150921
country current version : 20150921
Router# show geo-ip database version country
country latest version : 20150921
country current version : 20150921
Router# show geo-ip geography
Customize IPv4 to Geolocation:
Geolocation     Type       Address
Note
================================================================================
Router# show geo-ip geography6
Customize IPv6 to Geolocation:
Geolocation     Type       Address
Note
================================================================================
Router#
```

CHAPTER 53
Services

Use service objects to define TCP applications, UDP applications, and ICMP messages. You can also create service groups to refer to multiple service objects in other features.

53.1 Services Overview

See the appendices in the web configurator's User Guide for a list of commonly-used services.

53.2 Services Commands Summary

The following table describes the values required for many service object and service group commands. Other values are discussed with the corresponding commands.

Table 266 Input Values for Service Commands

LABEL	DESCRIPTION
group_name	The name of the service group. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
object_name	The name of the service. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

The following sections list the service object and service group commands.

53.2.1 Service Object Commands

The first table lists the commands for service objects.

Table 267 service-object Commands: Service Objects

COMMAND	DESCRIPTION
`show service-object [`*`object_name`*`]`	Displays information about the specified service or about all the services.
`no service-object` *`object_name`*	Deletes the specified service.
`service-object` *`object_name`* `{tcp | udp} {eq <1..65535> | range <1..65535> <1..65535>}`	Creates the specified TCP service or UDP service using the specified parameters.

Table 267 service-object Commands: Service Objects (continued)

COMMAND	DESCRIPTION
`service-object object_name icmp icmp_value`	Creates the specified ICMP message using the specified parameters. *icmp_value*: <0..255> | alternate-address | conversion-error | echo | echo-reply | information-reply | information-request | mask-reply | mask-request | mobile-redirect | parameter-problem | redirect | router-advertisement | router-solicitation | source-quench | time-exceeded | timestamp-reply | timestamp-request | unreachable
`service-object object_name protocol <1..255>`	Creates the specified user-defined service using the specified parameters.
`service-object rename object_name object_name`	Renames the specified service from the first *object_name* to the second *object_name*.
`service-object object_name icmpv6 {<0..255> | neighbor-solicitation | router-advertisement | echo | packet-toobig | router-solicitation | echo-reply | parameter-problem | time-exceeded | neighbor-advertisement | redirect | unreachable}`	Creates the specified ICMPv6 message using the specified parameters.

53.2.1.1 Service Object Command Examples

The following commands create four services, displays them, and then removes one of them.

```
Router# configure terminal
Router(config)# service-object TELNET tcp eq 23
Router(config)# service-object FTP tcp range 20 21
Router(config)# service-object ICMP_ECHO icmp echo
Router(config)# service-object MULTICAST protocol 2
Router(config)# show service-object
Object name                Protocol         Minmum port  Maxmum port  Ref.
=========================================================================TELNET
TCP               23            23             0
FTP                          TCP             20             21             0
ICMP_ECHO                   ICMP             0              0              0
MULTICAST                   2                 0              0              0
Router(config)# no service-object ICMP_ECHO
Router(config)# show service-object
Object name                Protocol         Minmum port  Maxmum port  Ref.
=========================================================================TELNET
TCP               23            23             0
FTP                          TCP             20             21             0
MULTICAST                   2                 0              0              0
```

53.2.2 Service Group Commands

The first table lists the commands for service groups.

Table 268 object-group Commands: Service Groups

COMMAND	DESCRIPTION
`show object-group service group_name`	Displays information about the specified service group.
`[no] object-group service group_name`	Creates the specified service group if necessary and enters sub-command mode. The `no` command removes the specified service group.
`[no] service-object object_name`	Adds the specified service to the specified service group. The `no` command removes the specified service from the specified group.
`[no] object-group group_name`	Adds the specified service group (second *`group_name`*) to the specified service group (first *`group_name`*). The `no` command removes the specified service group from the specified service group.
`[no] description description`	Sets the description to the specified value. The `no` command removes the description. *`description`*: You can use alphanumeric and `()+/:=?!*#@$_%-` characters, and it can be up to 60 characters long.
`object-group service rename group_name group_name`	Renames the specified service group from the first *`group_name`* to the second *`group_name`*.

53.2.2.1 Service Group Command Examples

The following commands create service ICMP_ECHO, create service group SG1, and add ICMP_ECHO to SG1.

```
Router# configure terminal
Router(config)# service-object ICMP_ECHO icmp echo
Router(config)# object-group service SG1
Router(group-service)# service-object ICMP_ECHO
Router(group-service)# exit
Router(config)# show service-object ICMP_ECHO
Object name                    Protocol        Minmum port  Maxmum port  Ref.
=============================================================================
ICMP_ECHO                        ICMP             8            8            1
Router(config)# show object-group service SG1
Object/Group name              Type   Reference
=============================================================================
ICMP_ECHO                        Object 1
```

CHAPTER 54
Schedules

Use schedules to set up one-time and recurring schedules for policy routes, firewall rules, application patrol, and content filtering.

54.1 Schedule Overview

The Zyxel Device supports two types of schedules: one-time and recurring. One-time schedules are effective only once, while recurring schedules usually repeat.

Note: Schedules are based on the current date and time in the Zyxel Device.

One-time schedules begin on a specific start date and time and end on a specific stop date and time. One-time schedules are useful for long holidays and vacation periods.

Recurring schedules begin at a specific start time and end at a specific stop time on selected days of the week (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday). Recurring schedules always begin and end in the same day. Recurring schedules are useful for defining the workday and off-work hours.

54.2 Schedule Commands Summary

The following table describes the values required for many schedule commands. Other values are discussed with the corresponding commands.

Table 269 Input Values for Schedule Commands

LABEL	DESCRIPTION
object_name	The name of the schedule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
time	24-hour time, hours and minutes; <0..23>:<0..59>.

The following table lists the schedule commands.

Table 270 schedule Commands

COMMAND	DESCRIPTION
`show schedule-object`	Displays information about the schedules in the Zyxel Device.
`no schedule-object` *object_name*	Deletes the schedule object.

Table 270 schedule Commands (continued)

COMMAND	DESCRIPTION
schedule-object *object_name date time date time*	Creates or updates a one-time schedule. *date*: yyyy-mm-dd date format; yyyy-<01..12>-<01..31>
schedule-object *object_name time time* [*day*] [*day*] [*day*] [*day*] [*day*] [*day*] [*day*]	Creates or updates a recurring schedule. *day*: 3-character day of the week; sun | mon | tue | wed | thu | fri | sat

54.2.1 Schedule Command Examples

The following commands create recurring schedule SCHEDULE1 and one-time schedule SCHEDULE2 and then delete SCHEDULE1.

```
Router# configure terminal
Router(config)# schedule-object SCHEDULE1 11:00 12:00 mon tue wed thu fri
Router(config)# schedule-object SCHEDULE2 2006-07-29 11:00 2006-07-31 12:00
Router(config)# show schedule-object
Object name                    Type      Start/End                        Ref.
=============================================================================
SCHEDULE1                       Recurring 11:00/12:00 ===MonTueWedThuFri=== 0
SCHEDULE2                       Once      2006-07-29 11:00/2006-07-31 12:00 0

Router(config)# no schedule-object SCHEDULE1
Router(config)# show schedule-object
Object name                    Type      Start/End                        Ref.
=============================================================================
SCHEDULE2                       Once      2006-07-29 11:00/2006-07-31 12:00 0
```

CHAPTER 55
AAA Server

This chapter introduces and shows you how to configure the Zyxel Device to use external authentication servers.

55.1 AAA Server Overview

You can use an AAA (Authentication, Authorization, Accounting) server to provide access control to your network.

The following lists the types of authentication server the Zyxel Device supports.

- Local user database

  The Zyxel Device uses the built-in local user database to authenticate administrative users logging into the Zyxel Device's web configurator or network access users logging into the network through the Zyxel Device. You can also use the local user database to authenticate VPN users.
- Directory Service (LDAP/AD)

  LDAP (Lightweight Directory Access Protocol)/AD (Active Directory) is a directory service that is both a directory and a protocol for controlling access to a network. The directory consists of a database specialized for fast information retrieval and filtering activities. You create and store user profile and login information on the external server.
- RADIUS

  RADIUS (Remote Authentication Dial-In User Service) authentication is a popular protocol used to authenticate users by means of an external or built-in RADIUS server. RADIUS authentication allows you to validate a large number of users from a central location.

55.2 Authentication Server Command Summary

This section describes the commands for authentication server settings.

55.2.1 ad-server Commands

The following table lists the `ad-server` commands you use to set the default AD server.

Table 271 ad-server Commands

COMMAND	DESCRIPTION
`show ad-server`	Displays the default AD server settings.
`[no] ad-server basedn` *basedn*	Sets a base distinguished name (DN) for the default AD server. A base DN identifies an AD directory. The no command clears this setting.

Table 271 ad-server Commands (continued)

COMMAND	DESCRIPTION
`[no] ad-server binddn` *`binddn`*	Sets the user name the Zyxel Device uses to log into the default AD server. The no command clears this setting.
`[no] ad-server cn-identifier` *`uid`*	Sets the unique common name (cn) to identify a record. The no command clears this setting.
`[no] ad-server host` *`ad_server`*	Sets the AD server address. Enter the IP address (in dotted decimal notation) or the domain name. The no command clears this setting.
`[no] ad-server password` *`password`*	Sets the bind password. This password will be encrypted when you use the `show ad-server` command to display. The no command clears this setting.
`[no] ad-server password-encrypted` *`password`*	Sets the encrypted password (less than 32 alphanumerical characters) in order to hide the real password from people behind you when you are configuring AD server password. This password is displayed as what you typed when you use the `show ad-server` command.
`[no] ad-server port` *`port_no`*	Sets the AD port number. Enter a number between 1 and 65535. The default is 389. The no command clears this setting.
`[no] ad-server search-time-limit` *`time`*	Sets the search timeout period (in seconds). Enter a number between 1 and 300. The no command clears this setting.
`[no] ad-server ssl`	Enables the Zyxel Device to establish a secure connection to the AD server. The no command disables this feature.

55.2.2 ldap-server Commands

The following table lists the `ldap-server` commands you use to set the default LDAP server.

Table 272 ldap-server Commands

COMMAND	DESCRIPTION
`show ldap-server`	Displays current LDAP server settings.
`[no] ldap-server basedn` *`basedn`*	Sets a base distinguished name (DN) for the default LDAP server. A base DN identifies an LDAP directory. The no command clears this setting.
`[no] ldap-server binddn` *`binddn`*	Sets the user name the Zyxel Device uses to log into the default LDAP server. The no command clears this setting.
`[no] ldap-server cn-identifier` *`uid`*	Sets the unique common name (cn) to identify a record. The no command clears this setting.
`[no] ldap-server host` *`ldap_server`*	Sets the LDAP server address. Enter the IP address (in dotted decimal notation) or the domain name. The no command clears this setting.
`[no] ldap-server password` *`password`*	Sets the bind password. The no command clears this setting.
`[no] ldap-server password-encrypted` *`password`*	Sets an encrypted bind password. The no command clears this setting.
`[no] ldap-server port` *`port_no`*	Sets the LDAP port number. Enter a number between 1 and 65535. The default is 389. The no command clears this setting.
`[no] ldap-server search-time-limit` *`time`*	Sets the search timeout period (in seconds). Enter a number between 1 and 300. The no command clears this setting.
`[no] ldap-server ssl`	Enables the Zyxel Device to establish a secure connection to the LDAP server. The no command disables this feature.

55.2.3 radius-server Commands

The following table lists the `radius-server` commands you use to set the default RADIUS server.

Table 273 radius-server Commands

COMMAND	DESCRIPTION
`show radius-server`	Displays the default RADIUS server settings.
`[no] radius-server host` *`radius_server`* `auth-port` *`auth_port`*	Sets the RADIUS server address and service port number. Enter the IP address (in dotted decimal notation) or the domain name of a RADIUS server. The no command clears the settings.
`[no] radius-server key` *`secret`*	Sets a password (up to 15 alphanumeric characters) as the key to be shared between the RADIUS server and the Zyxel Device. The no command clears this setting.
`[no] radius-server timeout` *`time`*	Sets the search timeout period (in seconds). Enter a number between 1 and 300. The no command clears this setting.

55.2.4 radius-server Command Example

The following example sets the secret key and timeout period of the default RADIUS server (172.23.10.100) to "87643210" and 80 seconds.

```
Router# configure terminal
Router(config)# radius-server host 172.23.10.100 auth-port 1812
Router(config)# radius-server key 876543210
Router(config)# radius-server timeout 80
Router(config)# show radius-server
host               : 172.23.10.100
authentication port: 1812
key                : 876543210
timeout            : 80
Router(config)#
```

55.2.5 aaa group server ad Commands

The following table lists the `aaa group server ad` commands you use to configure a group of AD servers.

Table 274 aaa group server ad Commands

COMMAND	DESCRIPTION
`clear aaa group server ad [`*`group-name`*`]`	Deletes all AD server groups or the specified AD server group. Note: You can NOT delete a server group that is currently in use.
`show aaa group server ad` *`group-name`*	Displays the specified AD server group settings.
`[no] aaa group server ad` *`group-name`*	Sets a descriptive name for an AD server group. Use this command to enter the sub-command mode. The no command deletes the specified server group.
`aaa group server ad rename` *`group-name group-name`*	Changes the descriptive name for an AD server group.

Table 274 aaa group server ad Commands (continued)

COMMAND	DESCRIPTION
`aaa group server ad group-name`	Enter the sub-command mode to configure an AD server group.
`[no] case-sensitive`	Specify whether or not the server checks the username case. Set this to be the same as the server's behavior.
`[no] server alternative-cn-identifier uid`	Sets the second type of identifier that the users can use to log in if any. For example "name" or "e-mail address". The no command clears this setting.
`[no] server basedn basedn`	Sets the base DN to point to the AD directory on the AD server group. The no command clears this setting.
`[no] server binddn binddn`	Sets the user name the Zyxel Device uses to log into the AD server group. The no command clears this setting.
`[no] server cn-identifier uid`	Sets the user name the Zyxel Device uses to log into the AD server group. The no command clears this setting.
`[no] server description description`	Sets the descriptive information for the AD server group. You can use up to 60 printable ASCII characters. The no command clears the setting.
`[no] server group-attribute group-attribute`	Sets the name of the attribute that the Zyxel Device is to check to determine to which group a user belongs. The value for this attribute is called a group identifier; it determines to which group a user belongs. You can add ext-group-user user objects to identify groups based on these group identifier values. For example you could have an attribute named "memberOf" with values like "sales", "RD", and "management". Then you could also create an ext-group-user user object for each group. One with "sales" as the group identifier, another for "RD" and a third for "management". The no command clears the setting.
`[no] server host ad_server`	Enter the IP address (in dotted decimal notation) or the domain name of an AD server to add to this group. The no command clears this setting.
`[no] server password password`	Sets the bind password (up to 15 alphanumerical characters). The no command clears this setting.
`[no] server port port_no`	Sets the AD port number. Enter a number between 1 and 65535. The default is 389. The no command clears this setting.
`[no] server search-time-limit time`	Sets the search timeout period (in seconds). Enter a number between 1 and 300. The no command clears this setting and set this to the default setting of 5 seconds.
`[no] server ssl`	Enables the Zyxel Device to establish a secure connection to the AD server. The no command disables this feature.

55.2.6 aaa group server ldap Commands

The following table lists the `aaa group server ldap` commands you use to configure a group of LDAP servers.

Table 275 aaa group server ldap Commands

COMMAND	DESCRIPTION
`clear aaa group server ldap [group-name]`	Deletes all LDAP server groups or the specified LDAP server group. Note: You can NOT delete a server group that is currently in use.
`show aaa group server ldap group-name`	Displays the specified LDAP server group settings.

Table 275 aaa group server ldap Commands (continued)

COMMAND	DESCRIPTION
`[no] aaa group server ldap group-name`	Sets a descriptive name for an LDAP server group. Use this command to enter the sub-command mode. The no command deletes the specified server group.
`aaa group server ldap rename group-name group-name`	Changes the descriptive name for an LDAP server group.
`aaa group server ldap group-name`	Enter the sub-command mode.
`[no] case-sensitive`	Specify whether or not the server checks the username case. Set this to be the same as the server's behavior.
`[no] server alternative-cn-identifier uid`	Sets the second type of identifier that the users can use to log in if any. For example "name" or "e-mail address". The no command clears this setting.
`[no] server basedn basedn`	Sets the base DN to point to the LDAP directory on the LDAP server group. The no command clears this setting.
`[no] server binddn binddn`	Sets the user name the Zyxel Device uses to log into the LDAP server group. The no command clears this setting.
`[no] server cn-identifier uid`	Sets the user name the Zyxel Device uses to log into the LDAP server group. The no command clears this setting.
`[no] server description description`	Sets the descriptive information for the LDAP server group. You can use up to 60 printable ASCII characters. The no command clears this setting.
`[no] server group-attribute group-attribute`	Sets the name of the attribute that the Zyxel Device is to check to determine to which group a user belongs. The value for this attribute is called a group identifier; it determines to which group a user belongs. You can add ext-group-user user objects to identify groups based on these group identifier values. For example you could have an attribute named "memberOf" with values like "sales", "RD", and "management". Then you could also create an ext-group-user user object for each group. One with "sales" as the group identifier, another for "RD" and a third for "management". The no command clears the setting.
`[no] server host ldap_server`	Enter the IP address (in dotted decimal notation) or the domain name of an LDAP server to add to this group. The no command clears this setting.
`[no] server password password`	Sets the bind password (up to 15 characters). The no command clears this setting.
`[no] server port port_no`	Sets the LDAP port number. Enter a number between 1 and 65535. The default is 389. The no command clears this setting.
`[no] server search-time-limit time`	Sets the search timeout period (in seconds). Enter a number between 1 and 300. The no command clears this setting and set this to the default setting of 5 seconds.
`[no] server ssl`	Enables the Zyxel Device to establish a secure connection to the LDAP server. The no command disables this feature.

55.2.7 aaa group server radius Commands

The following table lists the `aaa group server radius` commands you use to configure a group of RADIUS servers.

Table 276 aaa group server radius Commands

COMMAND	DESCRIPTION
`clear aaa group server radius` *`group-name`*	Deletes all RADIUS server groups or the specified RADIUS server group. Note: You can NOT delete a server group that is currently in use.
`show aaa group server radius` *`group-name`*	Displays the specified RADIUS server group settings.
`[no] aaa group server radius` *`group-name`*	Sets a descriptive name for the RADIUS server group. The no command deletes the specified server group.
`aaa group server radius rename` {*`group-name-old`*} *`group-name-new`*	Sets the server group name.
`aaa group server radius` *`group-name`*	Enter the sub-command mode.
`[no] case-sensitive`	Specify whether or not the server checks the username case. Set this to be the same as the server's behavior.
`[no] server description` *`description`*	Sets the descriptive information for the RADIUS server group. You can use up to 60 printable ASCII characters. The no command clears the setting.
`[no] server group-attribute` <1-255>	Sets the value of an attribute that the Zyxel Device is used to determine to which group a user belongs. This attribute's value is called a group identifier. You can add ext-group-user user objects to identify groups based on different group identifier values. For example, you could configure attributes 1,10 and 100 and create a ext-group-user user object for each of them. The no command clears the setting.
`[no] server host` *`radius_server`*	Enter the IP address (in dotted decimal notation) or the domain name of a RADIUS server to add to this server group. The no command clears this setting.
`[no] server key` *`secret`*	Sets a password (up to 15 alphanumeric characters) as the key to be shared between the RADIUS server(s) and the Zyxel Device. The no command clears this setting.
`[no] server timeout` *`time`*	Sets the search timeout period (in seconds). Enter a number between 1 and 300. The no command clears this setting and set this to the default setting of 5 seconds.

55.2.8 aaa group server Command Example

The following example creates a RADIUS server group with two members and sets the secret key to "12345678" and the timeout to 100 seconds. Then this example also shows how to view the RADIUS group settings.

```
Router# configure terminal
Router(config)# aaa group server radius RADIUSGroup1
Router(group-server-radius)# server host 192.168.1.100 auth-port 1812
Router(group-server-radius)# server host 172.23.22.100 auth-port 1812
Router(group-server-radius)# server key 12345678
Router(group-server-radius)# server timeout 100
Router(group-server-radius)# exit
Router(config)# show aaa group server radius RADIUSGroup1
key                : 12345678
timeout            : 100
description        :
group attribute    : 11

No.  Host Member                                                    Auth. Port

==========================================================================
1    192.168.1.100                                                   1812

2    172.23.22.100                                                   1812
```

CHAPTER 56
Authentication Objects

This chapter shows you how to select different authentication methods for user authentication using the AAA servers or the internal user database.

56.1 Authentication Objects Overview

After you have created the AAA server objects, you can specify the authentication objects (containing the AAA server information) that the Zyxel Device uses to authenticate users (using VPN or managing through HTTP/HTTPS).

56.2 aaa authentication Commands

The following table lists the `aaa authentication` commands you use to configure an authentication profile.

Table 277 aaa authentication Commands

COMMAND	DESCRIPTION
`aaa authentication rename` *`profile-name-old profile-name-new`*	Changes the profile name. *`profile-name`*: You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
`clear aaa authentication` *`profile-name`*	Deletes all authentication profiles or the specified authentication profile. Note: You can NOT delete a profile that is currently in use.
`show aaa authentication {`*`group-name`*`|default}`	Displays the specified authentication server profile settings.
`[no] aaa authentication` *`profile-name`*	Sets a descriptive name for the authentication profile. The `no` command deletes a profile.
`aaa authentication default` *`member1`* `[`*`member2`*`] [`*`member3`*`] [`*`member4`*`]`	Sets the default profile to use the authentication method(s) in the order specified. *`member`* = group ad, group ldap, group radius, or local. Note: You must specify at least one member for each profile. Each type of member can only be used once in a profile.

Table 277 aaa authentication Commands (continued)

COMMAND	DESCRIPTION
`aaa authentication` *`profile-name member1`* `[`*`member2`*`] [`*`member3`*`] [`*`member4`*`]`	Sets the profile to use the authentication method(s) in the order specified. *`member`* = group ad, group ldap, group radius, or local. Note: You must specify at least one member for each profile. Each type of member can only be used once in a profile.
`aaa authentication [no] match-default-group`	Enable this to treat a user successfully authenticated by a remote auth server as a defat-ext-user. If the remote authentication server is LDAP, the default-ext-user account is an ldap-user. If the remote authentication server is AD, the default-ext-user account is an ad-user. If the remote authentication server is RADIUS, the default-ext-user account is a radius-user.

56.2.1 aaa authentication Command Example

The following example creates an authentication profile to authentication users using the LDAP server group and then the local user database.

```
Router# configure terminal
Router(config)# aaa authentication LDAPuser group ldap local
Router(config)# show aaa authentication LDAPuser
No.  Method
================================================================================
0    ldap
1    local
Router(config)#
```

56.3 test aaa Command

The following table lists the `test aaa` command you use to teat a user account on an authentication server.

Table 278 test aaa Command

COMMAND	DESCRIPTION
`test aaa {server|secure-server} {ad|ldap} host {`*`hostname`*`|`*`ipv4-address`*`} [host {`*`hostname`*`|`*`ipv4-address`*`}] port <1..65535> base-dn `*`base-dn-string`*` [bind-dn `*`bind-dn-string`*` password `*`password`*`] login-name-attribute `*`attribute`*` [alternative-login-name-attribute `*`attribute`*`] account `*`account-name`*	Tests whether a user account exists on the specified authentication server.

56.3.1 Test a User Account Command Example

The following example shows how to test whether a user account named userABC exists on the AD authentication server which uses the following settings:

- IP address: 172.16.50.1
- Port: 389
- Base-dn: DC=Zyxel,DC=com
- Bind-dn: zyxel\engineerABC
- Password: abcdefg
- Login-name-attribute: sAMAccountName

The result shows the account exists on the AD server. Otherwise, the Zyxel Device responds an error.

```
Router> test aaa server ad host 172.16.50.1 port 389 base-dn DC=Zyxel,DC=com
bind-dn zyxel\engineerABC password abcdefg login-name-attribute
sAMAccountName account userABC

dn:: Q049MTIzNzco546L5aOr56uRKSxPVT1XaXRoTWFpbCxEQz1aeVhFTCxEQz1jb20=
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn:: MTIzNzco546L5aOr56uRKQ==
sn: User
l: 2341100
-------------------------SNIP!-----------------------------------------
```

56.4 VPN/Admin Two-Factor Authentication

Two-factor authentication adds an extra layer of security for users logging into the Zyxel Device. When two-factor authentication is enabled, a user has to first enter their username and password, and then click on a temporary link or enter a one-time password when logging in.

You can enable two-factor authentication for users who are logging into the Zyxel Device to create a VPN tunnel (VPN access), and for administrator and limited admin users who are logging into the Web Configurator or CLI (admin access) to configure the Zyxel Device.

Note: You can also configure two-factor authentication for non-VPN and non-admin users in web authentication. For details, see Section 31.1 on page 251.

Note: The admin two-factor authentication settings override the web authentication two-factor authentication settings if both are configured.

56.4.1 Two-Factor Authentication Methods

The following tables lists the methods for two-factor authentication.

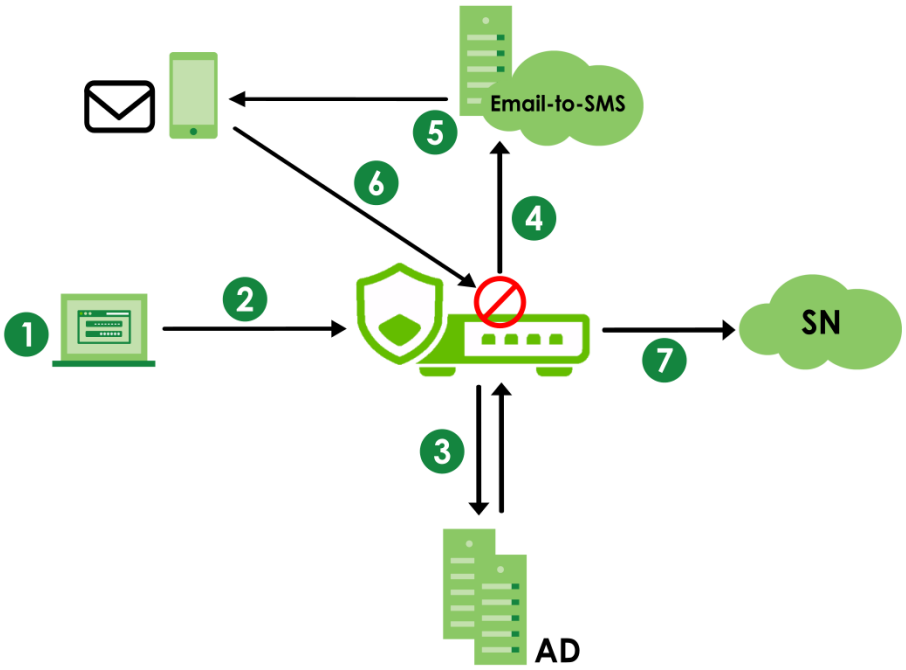
Table 279 Two Factor Authentication Methods

ACCESS TYPE	TWO-FACTOR AUTHENTICATION METHOD	FACTOR 2 PASSWORD
VPN	SMS	Link
VPN	Email	Link
Admin	SMS	Code
Admin	Email	Code
Admin	Google Authenticator app	Code

56.4.2 Two-Factor Authentication with SMS/Email

This section introduces how SMS/email two-factor authentication works.

Figure 39 SMS/Email Two-Factor Authentication



VPN Access

1. A user runs a VPN client and enters their VPN user name and password.
2. A VPN connection is created from the VPN client device to the Zyxel Device.
3. The Zyxel Device requests the user's user-name, password and mobile phone number or email address from the Active Directory (AD), RADIUS server or local Zyxel Device database in order to authenticate this user's use of the VPN tunnel (factor 1). If they are not found, then the Zyxel Device terminates the VPN connection.

4 If all correct credentials are found, then the Zyxel Device requests the Email-to-SMS Provider to send an authorization SMS, or the Zyxel Device sends an email to the client requesting VPN access (factor 2).

5 The client must open the authorization link sent via SMS or email within a user-specified time period (Valid Time).

6 If the authorization is correct and received on time, the client can access the secured network (SN) through the VPN tunnel.

Admin Access (Web Configurator, SSH, Telnet)

1 An admin user connects to the Zyxel Device through the Web Configurator, SSH, or Telnet.

2 The Zyxel Device requests the admin user's user-name, password and mobile phone number or email address from the Active Directory (AD), RADIUS server or local Zyxel Device database in order to authenticate this admin user.

3 If all correct credentials are found, then the Zyxel Device requests the Email-to-SMS Provider to send an authorization SMS, or the Zyxel Device sends an email to the client requesting VPN access (factor 2).

4 The client must enter the code sent via SMS or email within a user-specified time period (Valid Time).

5 If the authorization is correct and received on time, the admin user can log into Zyxel Device.

56.4.3 SMS/Email Configuration

Before enabling SMS/email Two-Factor Authentication, you must:

- Set up the user's user-name, password and email address or mobile number in the Active Directory, RADIUS server or local Zyxel Device database
- Configure the VPN tunnel for this user on the Zyxel Device
- Have an account with an Email-to-SMS Provider to be able to send SMS authorization requests
- Enable HTTP and/or HTTPS
- Enable SSH and/or Telnet
- Configure SMS and a mail server.

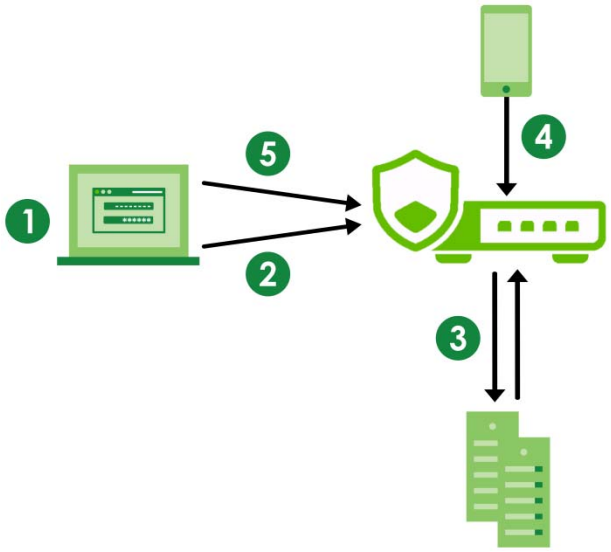
Two-Factor authentication may fail if one of the above is not configured or one of the below occurred.

- The user did not receive the authorization SMS or email. Check if the mobile telephone number or email address of the user in the Active Directory, RADIUS Server or local Zyxel Device database is configured correctly.
- Email-to-SMS Provider Authentication failed and no SMS was sent. Check that SMS is enabled on the Zyxel Device and credentials are correct.
- Mail server authentication failed. Check if the mail server settings are correct on the Zyxel Device.
- The authorization timed out. Extend the Valid Time.

56.4.4 Two-Factor Authentication with Google Authenticator

This section introduces how Google Authenticator two-factor authentication works.

Figure 40 Google Authenticator Two-Factor Authentication



Admin Access (Web Configurator, SSH, Telnet)

1 An admin user connects to the Zyxel Device through the Web Configurator, SSH, or Telnet.

2 The Zyxel Device requests the admin user's username and password.

3 The Zyxel Device authenticates the admin user's username and password using an Active Directory server, a RADIUS server, or a local Zyxel Device database. If this authentication is successful, the Zyxel Device requests the admin user's Google Authenticator code.

4 The admin user enters the code displayed in the Google Authenticator app.

5 If the Google Authenticator code is correct, the admin user can log into the Zyxel Device.

56.5 Two-Factor Authentication Commands

56.5.1 Two-Factor Authentication VPN Access

Use the following commands to configure which users and services require two-factor authentication for VPN access.

Table 280 Two-Factor Authentication Commands: VPN Access

COMMAND	DESCRIPTION
`[no] two-factor-auth activate`	Enables two-factor authentication to access a secured network behind the Zyxel Device via a VPN tunnel. The no command disables double-layer security.
`[no] two-factor-auth valid-time <1..15>`	Sets the maximum time (1-15 minutes) that the VPN client user must click or tap the authorization link in the SMS or email in order to get authorization for the VPN connection. The no command sets the maximum time to 3.

Table 280 Two-Factor Authentication Commands: VPN Access (continued)

COMMAND	DESCRIPTION
`two-factor-auth server interface` *`interface_name`*	Sets the Zyxel Device WAN interface to be used for two-factor authentication. This is part of the link that the VPN client user will receive in the SMS or email. The VPN client user must be able to access the link. *`interface_name:`* See Section 16.2 on page 118 for information about interface names.
`two-factor-auth server user-defined {`*`ipv4`*`|`*`domain_name`*`}`	Sets the WAN IPv4 address or domain name to be used for two-factor authentication. This is part of the link that the VPN client user will receive in the SMS or email. The VPN client user must be able to access the link. *`domain_name`*: This name can be up to 254 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted. *`ipv4`*: IPv4 address <W.X.Y.Z>
`two-factor-auth sms message {`*`message_quoted	message`*`}`	Sets the SMS message the VPN client user will receive by SMS for two-factor authentication. Use <user>, <host>, <url>, and <time> (in angular brackets) as variables to display dynamic information. The message must contain the <url> variable. *`message_quoted:`* Put the actual message in quotes. *`message:`* Put the name of a file with the message. The message file must be named '2FA-msg.txt' and be in UTF-8 format.
`two-factor-auth message {`*`message_quoted	message`*`}`	Sets the SMS message the VPN client user will receive by email for two-factor authentication. Use <user>, <host>, <url>, and <time> (in angular brackets) as variables to display dynamic information. The message must contain the <url> variable. *`message_quoted:`* Put the actual message in quotes. *`message:`* Put the name of a file with the message. The message file must be named '2FA-msg.txt' and be in UTF-8 format.
`two-factor-auth message-type {default	file}`	Sets which message to be used for two-factor authentication. `default`: a message edited using the `two-factor-auth message` command or via the web configurator. `file`: a message file uploaded from your computer using the `two-factor-auth message` command or via the web configurator.
`[no] two-factor-auth deliver-method {sms	email	google-auth}`	Sets the method to be used for two-factor authentication delivery to the VPN client user. The `no` command removes the method. • `SMS`: must contain a valid mobile telephone number. A valid mobile telephone number can be up to 20 characters in length, including the numbers 1~9 and the following characters in the square brackets [+*#()-]. • `email`: must contain a valid email address. A valid email address must contain the @ character. For example, this is a valid email address: abc@example.com. • `google-auth`: must first set up your Zyxel Device on the Google Authenticator app, see Section 56.5.3 on page 487 for more information. Then enter a time-limited code from the Google Authenticator app.
`[no] two-factor-auth service {sslvpn|ipsec|l2tp}`	Sets which kinds of VPN tunnels require Two-Factor Authentication. You should have configured the VPN tunnel first. The `no` command removes the VPN tunnel type. • SSL VPN Access • IPSec VPN Access • L2TP/IPSec VPN Access
`[no] two-factor-auth user` *`username`*	Sets the users or user groups that require two-factor authentication. The user or user group accounts should be already created. The `no` command removes the users or user groups that require two-factor authentication.

Table 280 Two-Factor Authentication Commands: VPN Access (continued)

COMMAND	DESCRIPTION
`two-factor-auth allow-access-url-thru-tunnel [activate | deactivate]`	Allows access to the link that the user will receive in the SMS or email. The user must be able to access the link and the Zyxel Device must have http/https enabled with a WAN interface/IP address/domain-name defined. The no command removes access to the link.
`[no] two-factor-auth http activate`	Enables the VPN client user to access the two-factor authorization page using the http protocol. Use the no command to require the VPN client user to access the two-factor authorization page using the https protocol.
`two-factor-auth http port <1...65535>`	Sets a new port between 1 to 65535 that is not in use by other services. Use this port for two-factor authentication of VPN clients to access the network behind the Zyxel Device. VPN clients do not need to change the port number on their devices, because the link to access the network behind the Zyxel Device will contain the new port number. For example, if you change this to port 8008 and the link is using a.b.c.d, the VPN clients will see this link in their email or SMS to access the network behind the Zyxel Device: https://a.b.c.d:8008.
`show two-factor-auth`	Displays current two-factor command settings for the VPN connection.

56.5.2 VPN Access Two-Factor Command Example

The following example shows current two-factor command settings.

```
Router# show two-factor-auth
 Activate : yes
 Valid Time : 3
 Auth Server Type : interface
 Auth Server : wan1
 Send Http Link : no
 Allow Access URL thru Tunnel : enable
 Deliver-Method-SMS : enable
 Deliver-Method-Email : enable
 Message-Type : default
 Message : <user>. You have initiated a VPN connection to a secured network
behind the <host>. Please click or tap the following link within <time>
minutes to get authorization for the VPN connection.
 Service : ipsec,sslvpn,l2tp
 Allowed User : any,
Router#
```

56.5.3 Admin Access

Use the following commands to configure whether Web, SSH, and TELNET require two-factor authentication for the admin user.

Table 281 two-factor Authentication Commands

COMMAND	DESCRIPTION
`[no] two-factor-auth admin-access activate`	Enables two-factor authentication to access a secured network behind the Zyxel Device via the Web Configurator, SSH, or Telnet as the admin user. The no command disables double-layer security.
`two-factor-auth admin-access auth-method {google-auth|pin-code}`	Sets the default two-factor authentication method for new admin accounts to either Google Authenticator or SMS/email).
`[no] two-factor-auth admin-access valid-time <1..5>`	Sets the maximum time (1-5 minutes) that the admin user must enter the code from the SMS or email in order to get authorization for logins via the Web Configurator, SSH, or Telnet. The no command sets the maximum time to 3.
`[no] two-factor-auth admin-access deliver-method {sms|email}`	Sets the method to be used for two-factor authentication pin code delivery to the admin user. The no command removes the method. • `SMS`: must contain a valid mobile telephone number. A valid mobile telephone number can be up to 20 characters in length, including the numbers 1~9 and the following characters in the square brackets [+*#()-]. • `email`: must contain a valid email address. A valid email address must contain the @ character. For example, this is a valid email address: abc@example.com.
`[no] two-factor-auth admin-access user` *`username`*	Uses this command and the admin user requires two-factor authentication for admin access. The no command means the admin user does not require two-factor authentication.
`[no] two-factor-auth admin-access service {ssh|telnet|web}`	Sets which services require Two-Factor Authentication for the admin user. The no command removes disables two-Factor Authentication for the specified access type. • SSH • Telnet • Web
`username` *`username`* `2fa-auth-method {default|google-auth|pin-code}`	Sets the two-factor authentication method for the user to either Google Authenticator or SMS/email. Default sets the authentication method to the default method set by the command `two-factor-auth admin-access auth-method.`
`username` *`username`* `[no] google-auth`	Enables two-factor authentication by Google Authenticator for the user account. The Zyxel Device creates a Google Authenticator QR code, and a set of backup codes for the account. The no command disables two-factor authentication by Google Authenticator for the user account, and also deletes the account's Google Authenticator QR code, secret key file, and backup codes.
`username` *`username`* `google-auth verify-code <verification code>`	Verifies whether the code currently displayed in the Google Authenticator app is correct or not. The Zyxel Device also creates a secret key file if one does not already exist.

Table 281 two-factor Authentication Commands (continued)

COMMAND	DESCRIPTION
`username` *`username`* `google-auth backup-code create`	Generates five new Google Authenticator backup codes. All previously generated backup codes become invalid. You can use Google Authenticator backup codes to log into the Zyxel Device if you are unable to access the Google Authenticator app.
`username` *`username`* `[no] {email1-verify|email2-verify}`	Verifies that the specified email address for the specified user name is valid. Use the no command and the specified email address for the specified user name will be invalid.
`username` *`username`* `[no] phone-verify`	Verifies that the specified mobile telephone number for the specified user name is valid. Use the no command and the specified mobile telephone number for the specified user name will be invalid.
`show two-factor-auth admin-access`	Displays current two-factor command settings for logins via the Web Configurator, SSH, or Telnet.
`show username` *`username`* `google-auth qrcode`	Displays the Google Authenticator QR code for this account. You can link this user account with Google Authenticator by pressing Enter Provided Key in the Google Authenticator app.
`show username` *`username`* `google-auth backup-code`	Displays the Google Authenticator backup codes for this user account. You can use Google Authenticator backup codes to log into the Zyxel Device if you are unable to access the Google Authenticator app.
`show two-factor-auth admin-access`	Displays the default two-factor authentication method for new admin accounts

56.5.4 Admin Access Two-Factor Command Examples

The following example shows how to set up two-factor authentication for an admin user.

56.5.4.1 Admin Access Two-Factor Command Example: Email

Follow the steps below to enable two-factor authentication for a Zyxel Device account. The example uses the parameters below.

Table 282 Admin Account Example

USER NAME	PASSWORD	USER TYPE
Mary	1234	admin

Table 283 Two-Factor Authentication Settings Example

AUTHENTICATION METHOD	DELIVERY METHOD	VALID TIME
pin code	email	5 minutes

1 Create an admin account using the parameters given above.

```
Router(config)# username Mary password 1234 user-type admin
```

2 Set an email for the account. Then verify the email.

```
Router(config)# username Mary email 1 abcd@zyxel.com.tw
Router(config)# username Mary email1-verify
```

3 Enable two-factor authentication for the admin account Mary.

```
Router(config)# two-factor-auth admin-access user Mary
```

4 Configure the two-factor authentication settings using the parameters given above.

```
Router(config)# username Mary 2fa-auth-method pin-code
Router(config)# two-factor-auth deliver-method email
Router(config)# two-factor-auth admin-access valid-time 5
```

5 Save the current configuration to the Zyxel Device.

```
Router(config)# write
```

56.5.4.2 Admin Access Two-Factor Command Example: QR Code

Please note that you need to add the QR code key generated by the Zyxel Device (secret=XXXXXXXXXXX) manually to the Google Authenticator app after running `show username <USERNAME> google-auth qrcode`.

To add the QR code manually, open your Google Authenticator app. Tap the plus icon then select Enter Key Manually.

```
Router(config)# two-factor-auth admin-access activate
Router(config)# two-factor-auth admin-access user admin
Router(config)# username admin google-auth
Router(config)# show username admin google-auth qrcode
qrcode-url# otpauth://totp/
admin?secret=XXXXXXXXXXXXXXXXXXXXXXXXXX&issuer=atp100w
Router(config)# username admin google-auth verify-code 123456
Verify: Success
Router(config)# write
```

CHAPTER 57
Authentication Server

This chapter shows you how to configure the Zyxel Device as an authentication server for access points.

57.1 Authentication Server Overview

The Zyxel Device can also work as a RADIUS server to exchange messages with other APs for user authentication and authorization.

57.2 Authentication Server Commands

The following table lists the authentication server commands you use to configure the Zyxel Device's built-in authentication server settings.

Table 284 Command Summary: Authentication Server

COMMAND	DESCRIPTION
`[no] auth-server activate`	Sets the Zyxel Device to act as an authentication server for other RADIUS clients, such as APs. The `no` command sets the Zyxel Device to not act as an authentication server for other APs.
`auth-server authentication` *`auth_method`*	Specifies an authentication method used by the authentication server.
`no auth-server authentication`	Resets the authentication method used by the authentication server to the factory default (`default`).
`[no] auth-server cert` *`certificate_name`*	Specifies a certificate used by the authentication server (Zyxel Device). The `no` command resets the certificate used by the authentication server to the factory default (`default`). *`certificate_name`*: The name of the certificate. You can use up to 31 alphanumeric and ;'~!@#$%^&()_+[]{}',.=- characters.
`[no] auth-server trusted-client` *`profile_name`*	Creates a trusted RADIUS client profile. The `no` command deletes the specified profile. *`profile-name`*: You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
`[no] activate`	Enables the client profile. The `no` command disables the profile.
`[no] ip address` *`ip subnet_mask`*	Sets the client's IP address and subnet mask. The `no` command clears this setting.
`[no] secret` *`secret`*	Sets a password as the key to be shared between the Zyxel Device and the client. The `no` command clears this setting.

Table 284 Command Summary: Authentication Server (continued)

COMMAND	DESCRIPTION
`[no] description` *description*	Sets the description for the profile. The `no` command clears this setting. *description*: You can use alphanumeric and `()+/:=?!*#@$_%-` characters, and it can be up to 60 characters long.
`show auth-server status`	Displays the Zyxel Device's authentication server settings.
`show auth-server trusted-client`	Displays all RADIUS client profile settings.
`show auth-server trusted-client` *profile_name*	Displays the specified RADIUS client profile settings.

57.2.1 Authentication Server Command Examples

The following example shows you how to enable the authentication server feature on the Zyxel Device and sets a trusted RADIUS client profile. This example also shows you the authentication server and client profile settings.

```
Router# configure terminal
Router(config)# auth-server activate
Router(config)# auth-server trusted-client AP-1
Router(config-trusted-client-AP-1)# activate
Router(config-trusted-client-AP-1)# ip address 10.10.1.2 255.255.255.0
Router(config-trusted-client-AP-1)# secret 12345678
Router(config-trusted-client-AP-1)# exit
Router(config)# show auth-server status
activation: yes
authentication method: default
certificate: default
Router(config)# show auth-server trusted-client AP-1
Client: AP-1
  Activation: yes
  Description:
  IP: 10.10.1.2
  Netmask: 255.255.255.0
  Secret: VQEq907jWB8=
Router(config)#
```

CHAPTER 58
Certificates

This chapter explains how to use the Certificates.

58.1 Certificates Overview

The Zyxel Device can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities. You can use the Zyxel Device to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

58.2 Certificate Commands

This section describes the commands for configuring certificates.

58.3 Certificates Commands Input Values

The following table explains the values you can input with the `certificate` commands.

Table 285 Certificates Commands Input Values

LABEL	DESCRIPTION
certificate_name	The name of a certificate. You can use up to 31 alphanumeric and ;'~!@#$%^&()_+[]{}',.=- characters.
cn_ipv4_address	A common name IP version 4 address identifies the certificate's owner.
cn_ipv6_address	A common name IP version 6 address identifies the certificate's owner.
cn_domain_name	A common name domain name identifies the certificate's owner. The domain name is for identification purposes only and can be any string. The domain name can be up to 255 characters. You can use alphanumeric characters, the hyphen and periods.
cn_email	A common name e-mail address identifies the certificate's owner. The e-mail address is for identification purposes only and can be any string. The e-mail address can be up to 63 characters. You can use alphanumeric characters, the hyphen, the @ symbol, periods and the underscore.
organizational_unit	Identifies the organizational unit or department to which the certificate owner belongs. You can use up to 31 characters. You can use alphanumeric characters, hyphen (-) and underscore (_).

Table 285 Certificates Commands Input Values (continued)

LABEL	DESCRIPTION
organization	Identifies the company or group to which the certificate owner belongs. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
country	A two-letter country code, which identifies the nation where the certificate owner is located. For example US, UK, ES, FR.
key_type	Sets the certificate's encryption algorithm and signature hash algorithm. Encryption algorithms: • RSA: Rivest, Shamir and Adleman public-key algorithm. • DSA: Digital Signature Algorithm public-key algorithm. • ECDSA: Elliptic Curve Digital Signature Algorithm. Signature hash algorithms: • SHA256 • SHA384 • SHA512 If you set an encryption algorithm without specifiying a signature hash algorithm (for example, *key_type rsa*), then . Note: RSA and SHA256 are less secure but more compatible with different clients and applications. ECDSA and SHA512 are the more secure but less compatible.
key_length	Specifiy the length of the key, in bits. Allowed values:. • ECDSA: 256, 384 • RSA/DSA: 512, 768, 1024, 1536, 2048, 4096 Typically, the longer the key, the more secure it is. A longer key also uses more PKI storage space. ECDSA keys are significant shorter than RSA and DSA keys, while offering equal or higher security.
password	When you have the Zyxel Device enroll for a certificate immediately online, the certification authority may want you to include a key (password) to identify your certification request. Use up to 31 of the following characters. a-zA-Z0-9;|`~!@#$%^&*()_+\{}':,./<>=-
ca_name	When you have the Zyxel Device enroll for a certificate immediately online, you must have the certification authority's certificate already imported as a trusted certificate. Specify the name of the certification authority's certificate. It can be up to 31 alphanumeric and ;'~!@#$%^&()_+[]{}',.=- characters.
url	When you have the Zyxel Device enroll for a certificate immediately online, enter the IP address (or URL) of the certification authority server. You can use up to 511 of the following characters. a-zA-Z0-9'()+,/:.=?;!*#@$_%-
town	Identifies the city or town in which the certificate owner is located. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore. You can add multiple words by enclosing them in double quotes, for example "New York".
state	Identifies the state, province, or region in which the certificate owner is located. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore. You can add multiple words by enclosing them in double quotes, for example "New Mexico".
user_definition	Not used at the time of writing.

Table 285 Certificates Commands Input Values (continued)

LABEL	DESCRIPTION
extend_key	Add extended use cases for the certificate. • client: The Zyxel Device generates and stores a request for a client authentication certificate. • ike: The Zyxel Device generates and stores a request for an IKE Intermediate authentication certificate. • svr: The Zyxel Device generates and stores a request for a server authentication certificate. • client-ike, svr-client, svr-ike, svr-client-ike: Enable a combination of client, ike, and svr settings. For example, client-ike generates and stores a request for a client authentication certificate and also an IKE Intermediate authentication certificate.
lifetimes	Sets how long the certificate is valid, in years. The value must be between 2 and 10. Note: Software such as web browsers might not trust a certificate that has a long lifetime.

58.4 Certificates Commands Summary

The following table lists the commands that you can use to display and manage the Zyxel Device's summary list of certificates and certification requests. You can also create certificates or certification requests. Use the `configure terminal` command to enter the configuration mode to be able to use these commands.

Table 286 ca Commands Summary

COMMAND	DESCRIPTION
`ca generate pkcs10 name` *certificate_name* `cn-type {ip cn` *cn_ipv4_address* `| ipv6 cn` *cn_ipv6_address* `|fqdn cn` *cn_domain_name* `| mail cn` *cn_email*`} [ou` *organizational_unit*`] [o` *organization*`] [l` *town*`] [s` *state*`] [c` *country*`] [usr-def` *user_definition*`] key-type {dsa | dsa-sha256 | ecdsa | ecdsa-sha256 | ecdsa-sha384 | rsa | rsa-sha256 | rsa-sha512} key-len` *key_length* `[extend-key` *extend_key*`] year` *lifetimes*	Generates a PKCS#10 certification signing request (CSR).
`ca generate pkcs12 name` *name* `password` *password*	Encrypts the named certificate using the specified password. This CLI command is for debugging purposes only; it is not possible to download the resulting file. To encrypt a certificate and download the resulting CRT file, use the Web Configurator.
`ca generate x509 name` *certificate_name* `cn-type {ip cn` *ipv4* `| ipv6 cn` *cn_ipv6_address* `| fqdn cn` *cn_domain_name* `| mail cn` *cn_email*`} [ou` *organizational_unit*`] [o` *organization*`] [l` *town*`] [s` *state*`] [c` *country*`] [usr-def` *user_definition*`] key-type {dsa | dsa-sha256 | ecdsa | ecdsa-sha256 | ecdsa-sha384 | rsa | rsa-sha256 | rsa-sha512} key-len` *key_length*	Generates a self-signed x509 certificate.
`ca rename category {local|remote}` *old_name new_name*	Renames a local (my certificates) or remote (trusted certificates) certificate.

Table 286 ca Commands Summary (continued)

COMMAND	DESCRIPTION
`ca validation` *`remote_certificate`*	Enters the sub command mode for validation of certificates signed by the specified remote (trusted) certificates. Note: At the time of writing, it is not possible to validate ECDSA certificates on the Zyxel Device.
`cdp {activate|deactivate}`	Turns certificate revocation on or off. When it is turned on, the Zyxel Device validates a certificate by getting a Certificate Revocation List (CRL) through HTTP or LDAP (can be configured after activating the LDAP checking option) and online responder (can be configured after activating the OCSP checking option). You also need to configure the OSCP or LDAP server details.
`ldap {activate|deactivate}`	Has the Zyxel Device check (or not check) incoming certificates that are signed by this certificate against a Certificate Revocation List (CRL) on a LDAP (Lightweight Directory Access Protocol) directory server.
`ldap ip {`*`ip`*`|`*`fqdn`*`} port <1..65535> [id` *`name`* `password` *`password`*`] [deactivate]`	Sets the validation configuration for the specified remote (trusted) certificate where the directory server uses LDAP. *`ip`*: Type the IP address (in dotted decimal notation) or the domain name of the directory server. The domain name can use alphanumeric characters, periods and hyphens. Up to 255 characters. `port`: Specify the LDAP server port number. You must use the same server port number that the directory server uses. 389 is the default server port number for LDAP. The Zyxel Device may need to authenticate itself in order to access the CRL directory server. Type the login name (up to 31 characters) from the entity maintaining the server (usually a certification authority). You can use alphanumeric characters, the underscore and the dash. Type the password (up to 31 characters) from the entity maintaining the CRL directory server (usually a certification authority). You can use the following characters: a-zA-Z0-9;|`~!@#$%^&*()_+\{}':,./<>=-
`ocsp {activate|deactivate}`	Has the Zyxel Device check (or not check) incoming certificates that are signed by this certificate against a directory server that uses OCSP (Online Certificate Status Protocol).

Table 286 ca Commands Summary (continued)

COMMAND	DESCRIPTION
ocsp url *url* [id *name* password *password*] [deactivate]	Sets the validation configuration for the specified remote (trusted) certificate where the directory server uses OCSP. *url*: Type the protocol, IP address and pathname of the OCSP server. name: The Zyxel Device may need to authenticate itself in order to access the OCSP server. Type the login name (up to 31 characters) from the entity maintaining the server (usually a certification authority). You can use alphanumeric characters, the underscore and the dash. password: Type the password (up to 31 characters) from the entity maintaining the OCSP server (usually a certification authority). You can use the following characters: a-zA-Z0-9;|`~!@#$%^&*()_+\{}':,./<>=-
no ca category {local|remote} *certificate_name*	Deletes the specified local (my certificates) or remote (trusted certificates) certificate.
no ca validation *name*	Removes the validation configuration for the specified remote (trusted) certificate.
show ca category {local|remote}	Displays a summary of all local (my certificates) or remote (trusted certificates) certificates in readable text.
show ca category {local|remote} name *certificate_name* format {text|pem}]	Displays information about the local or remote certificate with the specified name. Under format, use text to display the certificate's information in readable text, or pem to display the certificate in PEM (Base-64) encoded format.
show ca category {local|remote} name *certificate_name* certpath	Displays the certificate path of the specified the local or remote certificate.
show ca hierarchy name *certificate_name* [format all | cn | file]	Displays the hierarchy of certification authorities that validate the certificate, and the certificate itself. Format dertmines..
show ca validation name *name*	Displays the validation configuration for the specified remote (trusted) certificate.
show ca spaceusage	Displays the storage space in use by certificates.

58.5 Certificates Commands Examples

The following example creates a self-signed X.509 certificate with IP address 10.0.0.58 as the common name. It uses the RSA key type with SHA512. Then it displays the list of local certificates. Finally it deletes the pkcs12request certification request.

```
Router# configure terminal
Router(config)# ca generate x509 name test_x509 cn-type ip cn 10.0.0.58 key-
type rsa key-len 512
Router(config)# show ca category local
certificate: default
  type: SELF
  subject: CN=ZyWALL-1050_Factory_Default_Certificate
  issuer: CN=ZyWALL-1050_Factory_Default_Certificate
  status: VALID
  ID: ZyWALL-1050_Factory_Default_Certificate
    type: EMAIL
  valid from: 2003-01-01 00:38:30
  valid to: 2022-12-27 00:38:30
certificate: test
  type: REQ
  subject: CN=1.1.1.1
  issuer: none
  status: VALID
  ID: 1.1.1.1
    type: IP
  valid from: none
  valid to: none
certificate: pkcs12request
  type: REQ
  subject: CN=1.1.1.2
  issuer: none
  status: VALID
  ID: 1.1.1.2
    type: IP
  valid from: none
  valid to: none
certificate: test_x509
  type: SELF
  subject: CN=10.0.0.58
  issuer: CN=10.0.0.58
  status: VALID
  ID: 10.0.0.58
    type: IP
  valid from: 2006-05-29 10:26:08
  valid to: 2009-05-28 10:26:08
Router(config)# no ca category local pkcs12request
```

CHAPTER 59
ISP Accounts

Use ISP accounts to manage Internet Service Provider (ISP) account information for PPPoE, PPTP and cellular interfaces.

59.1 ISP Accounts Overview

An ISP account is a profile of settings for Internet access using PPPoE, PPTP, or cellular.

59.1.1 PPPoE and PPTP Account Commands

The following table lists the PPPoE and PPTP ISP account commands.

Table 287 PPPoE and PPTP ISP Account Commands

COMMAND	DESCRIPTION
`show account [pppoe` *`profile_name`* `| pptp` *`profile_name`*`]`	Displays information about the specified account(s).
`[no] account {pppoe | pptp}` *`profile_name`*	Creates a new ISP account with name *`profile_name`* if necessary and enters sub-command mode. The no command deletes the specified ISP account. *`profile_name`*: use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
`encrypted-password` *`ciphertext`*	Sets a encrypted secret for the specified account. *`ciphertext`*:
`[no] user` *`username`*	Sets the username for the specified ISP account. The no command clears the username. *`username`*: You can use alphanumeric, underscores (_), dashes (-), commas (,), and /@$ characters, and it can be up to 64 characters long.
`[no] password` *`password`*	Sets the password for the specified ISP account. The no command clears the password. *`password`*: You can use up to 63 printable ASCII characters. Spaces are not allowed.
`[no] authentication {chap-pap | chap | pap | mschap | mschap-v2}`	Sets the authentication for the specified ISP account. The no command sets the authentication to chap-pap.
`[no] compression {yes | no}`	Turns compression on or off for the specified ISP account. The no command turns off compression.
`[no] idle <0..360>`	Sets the idle timeout for the specified ISP account. The no command sets the idle timeout to zero.

Table 287 PPPoE and PPTP ISP Account Commands (continued)

COMMAND	DESCRIPTION
`[no] service-name {ip | hostname | service_name}`	Sets the service name for the specified PPPoE ISP account. The no command clears the service name. *hostname*: You may up to 63 alphanumeric characters, dashes (-), or periods (.), but the first character cannot be a period. *service_name*: You can use up to 63 alphanumeric characters, underscores (_), dashes (-), and @$./ characters.
`[no] server ip`	Sets the PPTP server for the specified PPTP ISP account. The no command clears the server name.
`[no] encryption {nomppe | mppe-40 | mppe-128}`	Sets the encryption for the specified PPTP ISP account. The no command sets the encryption to nomppe.
`[no] connection-id connection_id`	Sets the connection ID for the specified PPTP ISP account. The no command clears the connection ID. *connection_id*: You can use up to 31 alphanumeric characters, underscores (_), dashes (-), and colons (:).

59.1.2 Cellular Account Commands

The following table lists the cellular ISP account commands.

Table 288 Cellular Account Commands

COMMAND	DESCRIPTION
`show account cellular profile_name`	Displays information about the specified account.
`[no] account cellular profile_name`	Creates a new cellular ISP account with name *profile_name* if necessary and enters sub-command mode. The no command deletes the specified ISP account. *profile_name*: the cellular ISP account name format is “cellularx” where “x” is a number. For example, cellular1.
`[no] apn access_point_name`	Sets the Access Point Name (APN) for the cellular ISP account. The no command clears the APN. *access_point_name*: Use up to 63 alphanumeric characters and underscores (_), dashes (-), periods (.), and /@\$#.
`[no] dial-string isp_dial_string`	Sets the dial string for the specified ISP account. The no command clears the dial-string. *isp_dial_string*: Use up to 63 alphanumeric characters and underscores (_), dashes (-), periods (.), and /@\$#.
`[no] user username`	Sets the username for the specified ISP account. The no command clears the username. *username*: Use up to 64 alphanumeric characters and underscores (_), dashes (-), periods (.), and /@\$#.
`[no] password password`	Sets the password for the specified ISP account. The no command clears the password. *password*: Use up to 63 printable ASCII characters. Spaces are not allowed.

Table 288 Cellular Account Commands (continued)

COMMAND	DESCRIPTION
`[no] authentication {none | pap | chap}`	Sets the authentication for the cellular account. The no command sets the authentication to none.
`[no] idle <0..360>`	Sets the idle timeout for the cellular account. Zero disables the idle timeout. The no command sets the idle timeout to zero.

CHAPTER 60
SSL Application

This chapter describes how to configure SSL application objects for use in SSL VPN.

60.1 SSL Application Overview

Configure an SSL application object to specify a service and a corresponding IP address of the server on the local network. You can apply one or more SSL application objects in the VPN > SSL VPN screen for a user account/user group.

60.1.1 SSL Application Object Commands

This table lists the commands for creating SSL application objects. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 289 SSL Application Object Commands

COMMAND	DESCRIPTION
`show sslvpn application [application_object]`	Displays SSL VPN application objects.
`[no] sslvpn application application_object`	Enters the sub-command mode to create an SSL VPN application object.
`server-type {file-sharing | owa | web-server} url URL [entry-point entry_point]`	Specify the type of service for this SSL application. `file-sharing`: create a file share application for SSL VPN. `owa`: (Outlook Web Access) to allow users to access e-mails, contacts, calenders via an Microsoft Outlook-like interface using supported web browsers. The Zyxel Device supports one OWA object. `web-server`: to allow access to the specified web site hosted on the local network. `url`: Enter the fully qualified domain name (FQDN) or IP address of the application server. You must enter the “http://” or “https://” prefix. Remote users are restricted to access only files in this directory. For example, if you enter “\remote\” in this field, remote users can only access files in the “remote” directory. *`entry-point`*: optional. Specify the name of the directory or file on the local server as the home page or home directory on the user screen.

Table 289 SSL Application Object Commands

COMMAND	DESCRIPTION
`server-type file-sharing share-path` *`share-path`*	Specifies the IP address, domain name or NetBIOS name (computer name) of the file server and the name of the share to which you want to allow user access. Enter the path in one of the following formats. "\\<IP address>\<share name>" "\\<domain name>\<share name>" "\\<computer name>\<share name>" For example, if you enter "\\my-server\Tmp", this allows remote users to access all files and/or folders in the "\Tmp" share on the "my-server" computer.
`server-type rdp server-address` *`server-address`* `[starting-port <1..65535> ending-port <1..65535>] [program-path` *`program-path`*`]`	Creates an SSL application object to allow users to manage LAN computers that have Remote Desktop Protocol remote desktop server software installed. Specify the listening ports of the LAN computer(s) running remote desktop server software. The Zyxel Device uses a port number from this range to send traffic to the LAN computer that is being remotely managed. *`program-path`*: specify an application to open when a remote user logs into the remote desktop application.
`server-type vnc server-address` *`server-address`* `[starting-port <1..65535> ending-port <1..65535>]`	Creates an SSL application object to allow users to manage LAN computers that have Virtual Network Computing remote desktop server software installed. Specify the listening ports of the LAN computer(s) running remote desktop server software. The Zyxel Device uses a port number from this range to send traffic to the LAN computer that is being remotely managed.
`server-type weblink url` *`url`*	Sets this to create a link to a web site you specified that you expect the SSL VPN users to commonly use. *`url`*: Enter the fully qualified domain name (FQDN) or IP address of the application server. You must enter the "http://" or "https://" prefix. For example, `https://1.2.3.4`. SSL VPN users are restricted to access only web pages or files in this directory. For example, if you enter "\remote\" in this field, remote users can only access web pages or files in the "remote" directory. If a link contains a file that is not within this domain, then SSL VPN users cannot access it.
`no server-type`	Remove the type of service configuration for this SSL application.
`[no] webpage-encrypt`	Turn on web encrypt to prevent users from saving the web content.

60.1.2 SSL Application Command Examples

The following commands create and display a server-type SSL application object named ZW5 for a web server at IP address 192.168.1.12.

```
Router(config)# sslvpn application ZW5
Router(sslvpn application)# server-type web-server url http://192.168.1.12
Router(sslvpn application)# exit
Router(config)# show sslvpn application
SSL Application: ZW5
  Server Type: web-server
  URL: http://192.168.1.12
  Entry Point:
  Encrypted URL: ~aHR0cDovLzE5Mi4xNjguMS4xMi8=/
  Web Page Encryption: yes
  Reference: 1
```

CHAPTER 61
DHCPv6 Objects

This chapter describes how to configure and view DHCPv6 request and lease objects.

61.1 DHCPv6 Object Commands Summary

The following table identifies the values required for many DHCPv6 object commands. Other input values are discussed with the corresponding commands.

Table 290 DHCPv6 Object Command Input Values

LABEL	DESCRIPTION
dhcp6_profile	The name of a DHCPv6 request object. Use a string of less than 31 characters.
interface_name	The name of the interface. This depends on the Zyxel Device model. For some models, use ge*x*, *x* = 1 ~ N, where N equals the highest numbered Ethernet interface for your Zyxel Device model. For other models, use a name such as wan1, wan2, opt, lan1, or dmz.

The following sections list the DHCPv6 object commands.

61.1.1 DHCPv6 Object Commands

This table lists the commands for DHCPv6 objects. Use the `configure terminal` command to enter the configuration mode to be able to use the commands that configure settings.

Table 291 DHCPv6 Object Commands

COMMAND	DESCRIPTION
`show ipv6 dhcp6 binding`	Displays the server side IPv6/DUID binding lease.
`show dhcp6 interface`	Displays all DHCPv6 server, client and relay interfaces.
`show dhcp6 lease-object [`*`dhcp6_profile`*`]`	Displays the specified DHCPv6 lease object or all of them.
`show dhcp6 object-binding` *`interface_name`*	Displays the DHCPv6 object bound to the specified interface.
`show dhcp6 request-object [`*`dhcp6_profile`*`]`	Displays the specified DHCPv6 request object or all of them.
`dhcp6-lease-object` *`dhcp6_profile`* `address` *`ipv6_addr`* `duid` *`duid`*	Creates or edits the specified DHCP lease object with the specified IPv6 address and DHCP Unique IDentifier (DUID).
`dhcp6-lease-object` *`dhcp6_profile`* `prefix-delegation` *`ipv6_addr_prefix`* `duid` *`duid`*	Creates or edits the specified pre-fix delegation DHCP lease object with the specified IPv6 address prefix and DUID.

Table 291 DHCPv6 Object Commands (continued)

COMMAND	DESCRIPTION
`dhcp6-lease-object` *`dhcp6_profile`* `address-` *`ipv6_addr ipv6_addr`*	Creates or edits the specified DHCP lease object address with the specified IPv6 address range.
`dhcp6-lease-object` *`dhcp6_profile`* `{ sip-server | ntp-server | dns-server } {` *`ipv6_addr`* `|` *`dhcp6_profile`* `}`	Creates or edits the specified SIP server, NTP server, or DNS server DHCP lease object with the specified IPv6 address. When you assign a request object, the lease object value will be the request object value retrieved from the DHCPv6 server.
`dhcp6-lease-object rename` *`dhcp6_profile dhcp6_profile`*	Renames the specified DHCPv6 lease object to the specified name.
`no dhcp6-lease-object` *`dhcp6_profile`*	Deletes the specified DHCPv6 lease object.
`dhcp6-request-object` *`dhcp6_profile`* `{ dns-server | ntp-server | prefix-delegation | sip-server }`	Creates or edits the specified SIP server, DNS server, NTP server, prefix-delegation, or SIP server DHCP request object.
`dhcp6-request-object rename` *`dhcp6_profile dhcp6_profile`*	Renames the specified DHCPv6 request object to the specified name.
`no dhcp6-request-object` *`dhcp6_profile`*	Deletes the specified DHCPv6 request object.

61.1.2 DHCPv6 Object Command Examples

This example creates and displays a DHCPv6 lease object named “test1” for IPv6 address 2003::1 with DUID 00:01:02:03:04:05:06:07.

```
Router(config)# dhcp6-lease-object test1 address 2003::1 duid
00:01:02:03:04:05:06:07
Router(config)# show dhcp6 lease-object
DHCP6 Lease Object: test1
  Object Type: address
  Object Value: 2003::1
  DUID: 00:01:02:03:04:05:06:07
  Bind Iface:
  REFERENCE: 0
```

This example makes “test1” into a DHCPv6 address lease object for IPv6 addresses 2004::10 to 2004::40.

```
Router(config)# dhcp6-lease-object test1 address- 2004::10 2004::40
Router(config)# show dhcp6 lease-object
DHCP6 Lease Object: test1
  Object Type: address-
  Object Value: 2004::10
  Ext Object Value: 2004::40
  Bind Iface:
  REFERENCE: 0
```

This example creates and displays a DHCPv6 prefix delegation lease object named “pfx” for IPv6 address prefix 2005::/64 and DUID 00:01:02:03:04:05:06:07, then renames it to “pd”.

```
Router(config)# dhcp6-lease-object pfx prefix-delegation 2005::/64 duid
00:01:02:03:04:05:06:07
Router(config)# show dhcp6 lease-object pfx
DHCP6 Lease Object: pfx
  Object Type: prefix-delegation
  Object Value: 2005::/64
  DUID: 00:01:02:03:04:05:06:07
  Bind Iface:
  REFERENCE: 0
Router(config)# dhcp6-lease-object rename pfx pd
Router(config)# show dhcp6 lease-object pd
DHCP6 Lease Object: pd
  Object Type: prefix-delegation
  Object Value: 2005::/64
  DUID: 00:01:02:03:04:05:06:07
  Bind Iface:
  REFERENCE: 0
```

This example deletes the “test1” DHCPv6 lease object.

```
Router(config)# no dhcp6-lease-object test1
```

This example creates a DHCPv6 prefix delegation request object named “pfx” and displays its settings.

```
Router(config)# dhcp6-request-object pfx prefix-delegation
Router(config)# show dhcp6 request-object
DHCP6 Request Object: pfx
  Object Type: prefix-delegation
  Object Value: 2089:3::/48
  Bind Iface: ge2
  REFERENCE: 1
```

CHAPTER 62
Dynamic Guest Accounts

62.1 Dynamic Guest Accounts Overview

Dynamic guest accounts are guest accounts, but are created dynamically and stored in the Zyxel Device's local user database. A dynamic guest account has a dynamically-created user name and password. A dynamic guest account user can access the Zyxel Device's services only within a given period of time and will become invalid after the expiration date/time.

There are three types of dynamic guest accounts depending on how they are created or authenticated: billing-users, ua-users and trial-users.

billing-users are guest account created with the `dynamic-guest generate` command or the guest manager account or an external printer and paid by cash or created and paid via the on-line payment service.

ua-users are users that log in from the user agreement page.

trial-users are free guest accounts that are created with the `dynamic-guest generate-freeuser` command or the Free Time function.

62.2 Dynamic-guest Commands

This table lists the `dynamic-guest` commands. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 292 dynamic-guest Commands

COMMAND	DESCRIPTION
`dynamic-guest freeuser` *`user_name`*	Creates a free dynamic guest account (trial-user) with the specified user name and enters the dynamic-guest sub-command mode to set the password and timeout settings. See Table 293 on page 508 for the sub-commands.
`dynamic-guest generate`	Sets the Zyxel Device to automatically create a dynamic guest account (billing-user) and enters the dynamic-guest sub-command mode to set the password and timeout settings. See Table 293 on page 508 for the sub-commands.
`dynamic-guest generate-freeuser`	Sets the Zyxel Device to automatically create a free dynamic guest account (trial-user) and enters the dynamic-guest sub-command mode to set the password and timeout settings. See Table 293 on page 508 for the sub-commands.
`dynamic-guest keep-user-logged-in`	

Table 292 dynamic-guest Commands (continued)

COMMAND	DESCRIPTION
`[no] dynamic-guest user_name`	Creates a dynamic guest account (billing-user) with the specified user name and enters the dynamic-guest sub-command mode to set the password and timeout settings. See Table 293 on page 508 for the sub-commands. The no command removes the specified dynamic-guest account.
`show dynamic-guest log`	Displays all the dynamic guest accounts which are either active or expired.
`show dynamic-guest log create-time begin yyyy-mm-dd hh:mm end yyyy-mm-dd hh:mm`	Displays all the active and/or expired dynamic guest accounts that were generated within a specified period of time.
`show dynamic-guest users`	Displays all the active dynamic guest accounts on the Zyxel Device.

62.2.1 dynamic-guest Sub-commands

The following table describes the sub-commands for several `dynamic-guest` commands. Note that not all rule commands use all the sub-commands listed here.

Table 293 dynamic-guest Sub-commands

COMMAND	DESCRIPTION
`bandwidth {upload | download} <0..1048576> priority <1..7>`	Specifies the maximum bandwidth allowed for the user account in kilobits per second and types a number between 1 and 7 to set the priority for the user's traffic. The smaller the number, the higher the priority. `upload` refers to the traffic the Zyxel Device sends out from a user. `download` refers to the traffic the Zyxel Device sends to a user.
`[no] bandwidth activate`	Turns on bandwidth management for the user account. The no command disables bandwidth management for the user account.
`charge price`	Sets the account's price, up to 99999999.99, per time unit.
`create-time yyyy-mm-dd hh:mm`	Sets the date and time the account is created.
`currency {eur |gbp |usd | user-define curreny_code}`	Sets the currency for the charge, which is displayed in the UI. • eur: Euros. • gbp: British pounds • USD: American dollars • user-define: Specify any three-letter currency name
`e-mail email_address`	Sets an email address for the guest user.
`encrypted-password password`	Sets a new password for the dynamic user.
`expire-time yyyy-mm-dd hh:mm`	Sets the date and time the account becomes invalid.
`login-mac mac_address`	Sets the MAC address of the guest's device. The guest account can then only log in from this device.
`name description`	Sets a human-readable description for the dynamic user.
`password password`	Sets the password for the account.
`payment-info {cash | payment-service}`	Sets the method of payment for the account.

Table 293 dynamic-guest Sub-commands (continued)

COMMAND	DESCRIPTION
phone *phone_number*	Sets the mobile phone number for the account.
printer-ip *ip_address*	
quota {total | upload | download} megabytes <0..1023>	Sets how much downstream and/or upstream data in Megabytes can be transmitted through the external interface before the account expires. 0 means there is no data limit for the user account.
quota {total | upload | download} gigabytes <0..100>	Sets how much downstream and/or upstream data in Gigabytes can be transmitted through the external interface before the account expires. 0 means there is no data limit for the user account.
quota type {total | upload-download}	Sets a limit for the user account. This only applies to user's traffic that is received or transmitted through the external interface. Note: When the limit is exceeded, the user is not allowed to access the Internet through the Zyxel Device. total: set a limit on the total traffic in both directions. upload-download: set a limit on the upstream traffic and downstream traffic respectively.
remaining-time <1..25920000>	Sets the amount of Internet access time (in seconds) remaining for the account.
time-period <1..432000>	Sets the total account of time (in minutes) the account can use to access the Internet through the Zyxel Device.
replenish enable	Reloads the quota of a specific dynamic user's account.
serial-number *number*	

62.2.2 Dynamic-guest Command Example

This example shows how to create a dynamic guest account, configure the account related settings and displays the account information.

```
Router# configure terminal
Router(config)# dynamic-guest generate
[dynamic guest] username:gn0ti7, password:ihzun7
Router(config-dynamic-guest)# charge 5
Router(config-dynamic-guest)# expire-time 2013-06-26 14:00
Router(config-dynamic-guest)# payment-info cash
Router(config-dynamic-guest)# phone 0912345678
Router(config-dynamic-guest)# time-period 1440
Router(config-dynamic-guest)# remaining-time 86400
Router(config-dynamic-guest)# create-time 2013-06-25 14:03
Router(config-dynamic-guest)# exit
Router(config)# show dynamic-guest users
No.   Status     Username   Create Time            Expiration Time
     Time Period          Remaining Time       Charge        ayment Info
Phone Num
     User Role
================================================================================
=========
1     Unused     gn0ti7    2013-06-25 14:03        2013-06-26 14:00
     1day 00:00:00        1day 00:00:00        eur 5,00        cash
0912345678
     billing-users
Router(config)#
```

CHAPTER 63
System

63.1 System Overview

Use these commands to configure general Zyxel Device information, the system time and the console port connection speed for a terminal emulation program. They also allow you to configure DNS settings and determine which services/protocols can access which Zyxel Device zones (if any) from which computers.

63.2 Customizing the WWW Login Page

Use these commands to customize the Web Configurator login screen. You can also customize the page that displays after an access user logs into the Web Configurator to access network services like the Internet. See Chapter 49 on page 438 for more on access user accounts.

The following figures identify the parts you can customize in the login and access pages.

Figure 41 Login Page Customization

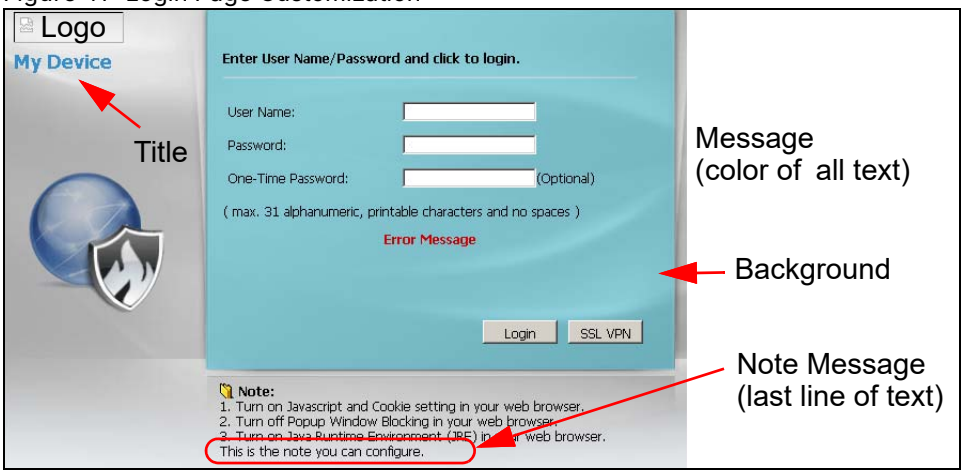
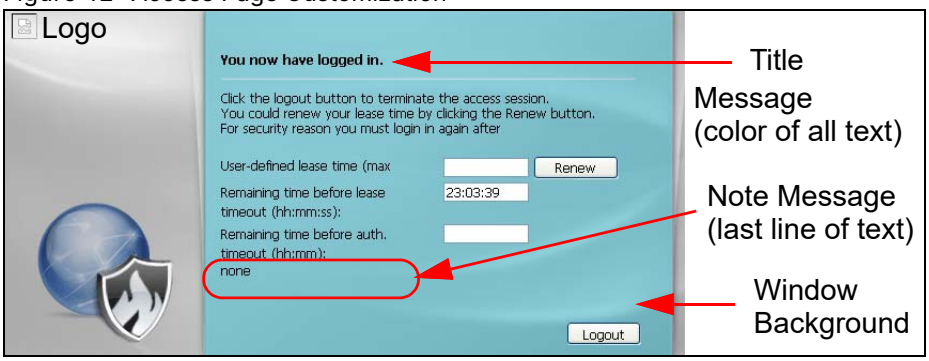


Figure 42 Access Page Customization



You can specify colors in one of the following ways:

- *color-rgb*: Enter red, green, and blue values in parenthesis and separate by commas. For example, use "rgb(0,0,0)" for black.
- *color-name*: Enter the name of the desired color.
- *color-number*: Enter a pound sign (#) followed by the six-digit hexadecimal number that represents the desired color. For example, use "#000000" for black.

The following table describes the commands available for customizing the Web Configurator login screen and the page that displays after an access user logs into the Web Configurator to access network services like the Internet. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 294 Command Summary: Customization

COMMAND	DESCRIPTION
`[no] access-page color-window-background`	Sets whether or not the access page uses a colored background.
`access-page message-color {color-rgb | color-name | color-number}`	Sets the color of the message text on the access page.
`[no] access-page message-text message`	Sets a note to display below the access page's title. Use up to 64 printable ASCII characters. Spaces are allowed.
`access-page title title`	Sets the title for the top of the access page. Use up to 64 printable ASCII characters. Spaces are allowed.
`access-page window-color {color-rgb | color-name | color-number}`	Sets the color of the access page's colored background.
`login-page background-color {color-rgb | color-name | color-number}`	Sets the color of the login page's background.
`[no] login-page color-background`	Sets the login page to use a solid colored background.
`[no] login-page color-window-background`	Sets the login page's window to use a solid colored background.
`login-page message-color {color-rgb | color-name | color-number}`	Sets the color of the message text on the login page.
`[no] login-page message-text % message`	Sets a note to display at the bottom of the login screen. Use up to 64 printable ASCII characters. Spaces are allowed.

Table 294 Command Summary: Customization (continued)

COMMAND	DESCRIPTION
`login-page title` *`title`*	Sets the title for the top of the login screen. Use up to 64 printable ASCII characters. Spaces are allowed.
`login-page title-color` {*`color-rgb`* | *`color-name`* | *`color-number`*}	Sets the title text color of the login page.
`login-page window-color` {*`color-rgb`* | *`color-name`* | *`color-number`*}	Sets the color of the login page's window border.
`logo background-color` {*`color-rgb`* | *`color-name`* | *`color-number`*}	Sets the color of the logo banner across the top of the login screen and access page.
`show access-page settings`	Lists the current access page settings.
`show login-page default-title`	Lists the factory default title for the login page.
`show login-page settings`	Lists the current login page settings.
`show logo settings`	Lists the current logo background (banner) and floor (line below the banner) settings.
`show page-customization`	Lists whether the Zyxel Device is set to use custom login and access pages or the default ones.

63.3 Host Name Commands

The following table describes the commands available for the hostname and domain name. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 295 Command Summary: Host Name

COMMAND	DESCRIPTION
`[no] domainname` *`domain_name`*	Sets the domain name. The `no` command removes the domain name. *`domain_name`*: This name can be up to 254 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
`[no] hostname` *`hostname`*	Sets a descriptive name to identify your Zyxel Device. The `no` command removes the host name.
`show fqdn`	Displays the fully qualified domain name.

63.4 Time and Date

For effective scheduling and logging, the Zyxel Device system time must be accurate. The Zyxel Device's Real Time Chip (RTC) keeps track of the time and date. There is also a software mechanism to set the time manually or get the current time and date from an external server.

63.4.1 Date/Time Commands

The following table describes the commands available for date and time setup. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 296 Command Summary: Date/Time

COMMAND	DESCRIPTION
`clock date` *`yyyy-mm-dd`* `time` *`hh:mm:ss`*	Sets the new date in year, month and day format manually and the new time in hour, minute and second format.
`[no] clock daylight-saving`	Enables daylight savings. The `no` command disables daylight saving.
`[no] clock saving-interval begin {apr|aug|dec|feb|jan|jul|jun|mar|may|nov|oct|sep} {1|2|3|4|last} {fri|mon|sat|sun|thu|tue|wed} hh:mm end {apr|aug|dec|feb|jan|jul|jun|mar|may|nov|oct|sep} {1|2|3|4|last} {fri|mon|sat|sun|thu|tue|wed} hh:mm offset`	Configures the day and time when daylight saving time starts and ends. The `no` command removes the day and time when daylight savings time starts and ends. offset: a number from 1 to 5.5 (by 0.5 increments)
`clock time` *`hh:mm:ss`*	Sets the new time in hour, minute and second format.
`[no] clock time-zone {-|+hh:mm} [+|-]HH:MM.`	Sets your time zone where `hh: hour 0-14, mm: minute 0-59`). The `no` command removes time zone settings.
`[no] ntp`	Saves your date and time and time zone settings and updates the data and time every 24 hours. The `no` command stops updating the data and time every 24 hours.
`[no] ntp server {fqdn|w.x.y.z}`	Sets the IP address or URL of your NTP time server. The `no` command removes time server information.
`ntp sync`	Gets the time and date from an NTP time server.
`[no] clock auto-sync-timezone`	Allows the Zyxel Device to automatically update its time zone from the cloud server after the set and get commands below are issued. The `no` command disables the Zyxel Device from automatically updating its time zone from the cloud server.
`[no] clock auto-sync-daylight-saving`	Allows the Zyxel Device to automatically update its daylight savings adjusted time from the cloud server after the set and get commands below are issued. The `no` command disables the Zyxel Device from automatically updating daylight savings adjusted time from the cloud server.
`myzyxel-service get-cloud-timezone`	Sends a query to the cloud server to get both time-zone and daylight-savings information for where the Zyxel Device is located. The Zyxel Device keeps the result in a temporary file.
`myzyxel-service set-timezone-according-cloud`	Applies time-zone and daylight-savings settings according the information received from `myzyxel-service get-cloud-timezone` and if `clock auto-sync-timezone` and/or `clock auto-sync-daylight-saving` were issued. For example, if `clock auto-sync-timezone` was not issued, then Zyxel Device will not automatically update the time-zone.
`show myzyxel-service get-cloud-timezone`	Displays the time-zone, daylight savings time start-date, daylight savings time end-date and daylight savings time offset from the cloud server.
`show clock date`	Displays the current date of your Zyxel Device.

Table 296 Command Summary: Date/Time (continued)

COMMAND	DESCRIPTION
`show clock status`	Displays your time zone and daylight saving settings.
`show clock time`	Displays the current time of your Zyxel Device.
`show ntp server`	Displays time server settings.

63.5 Console Port Speed

This section shows you how to set the console port speed when you connect to the Zyxel Device via the console port using a terminal emulation program. The following table describes the console port commands. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 297 Command Summary: Console Port Speed

COMMAND	DESCRIPTION
`[no] console baud` *`baud_rate`*	Sets the speed of the console port. The no command resets the console port speed to the default (115200). *`baud_rate`*: 9600, 19200, 38400, 57600 or 115200.
`show console`	Displays console port speed.

63.6 DNS Overview

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it.

63.6.1 Domain Zone Forwarder

A domain zone forwarder contains a DNS server's IP address. The Zyxel Device can query the DNS server to resolve domain zones for features like VPN, DDNS and the time server. A domain zone is a fully qualified domain name without the host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name.

A name query begins at a client computer and is passed to a resolver, a DNS client service, for resolution. The Zyxel Device can be a DNS client service. The Zyxel Device can resolve a DNS query locally using cached Resource Records (RR) obtained from a previous query (and kept for a period of time). If the Zyxel Device does not have the requested information, it can forward the request to DNS servers. This is known as recursion.

The Zyxel Device can ask a DNS server to use recursion to resolve its DNS client requests. If recursion on the Zyxel Device or a DNS server is disabled, they cannot forward DNS requests for resolution.

A Domain Name Server (DNS) amplification attack is a kind of Distributed Denial of Service (DDoS) attack that uses publicly accessible open DNS servers to flood a victim with DNS response traffic. An open DNS server is a DNS server which is willing to resolve recursive DNS queries from anyone on the Internet.

In a DNS amplification attack, an attacker sends a DNS name lookup request to an open DNS server with the source address spoofed as the victim's address. When the DNS server sends the DNS record response, it is sent to the victim. Attackers can request as much information as possible to maximize the amplification effect.

63.6.2 DNS Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 298 Input Values for General DNS Commands

LABEL	DESCRIPTION
address_object	The name of the IP address (group) object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
interface_name	The name of the interface. Ethernet interface: For some Zyxel Device models, use ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your Zyxel Device model. For other Zyxel Device models, use a name such as wan1, wan2, opt, lan1, or dmz. virtual interface on top of Ethernet interface: add a colon (:) and the number of the virtual interface. For example: ge*x*:*y*, *x* = 1 - N, *y* = 1 - 4 VLAN interface: vlan*x*, *x* = 0 - 4094 virtual interface on top of VLAN interface: vlan*x*:*y*, *x* = 0 - 4094, *y* = 1 - 12 bridge interface: br*x*, *x* = 0 - N, where N depends on the number of bridge interfaces your Zyxel Device model supports. virtual interface on top of bridge interface: br*x*:*y*, *x* = the number of the bridge interface, *y* = 1 - 4 PPPoE/PPTP interface: ppp*x*, *x* = 0 - N, where N depends on the number of PPPoE/PPTP interfaces your Zyxel Device model supports.

The following table describes the commands available for DNS. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 299 Command Summary: DNS

COMMAND	DESCRIPTION
`[no] ip dns server a-record` *`fqdn w.x.y.z`*	Sets an A record that specifies the mapping of a fully qualified domain name (FQDN) to an IP address. The `no` command deletes an A record.
`ip dns server cache-flush`	Clears the DNS.
`[no] ip dns server mx-record` *`domain_name`* `{`*`w.x.y.z`*`|`*`fqdn`*`}`	Sets a MX record that specifies a mail server that is responsible for handling the mail for a particular domain. The `no` command deletes a MX record.
`ip dns server rule {<1..32>|append|insert <1..32>} access-group {ALL|`*`address_object`*`} zone {ALL|`*`address_object`*`} action {accept|deny}`	Sets a service control rule for DNS requests.
`ip dns server rule move <1..32> to <1..32>`	Changes the number of a service control rule.

Table 299 Command Summary: DNS (continued)

COMMAND	DESCRIPTION
`[no] ip dns server zone-forwarder {<1..32>|append|insert <1..32>} {domain_zone_name|*} interface interface_name`	Sets a domain zone forwarder record that specifies a fully qualified domain name. You can also use a star (*) if all domain zones are served by the specified DNS server(s). *domain_zone_name*: This is a domain zone, not a host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name. For example, whenever the Zyxel Device receives needs to resolve a zyxel.com.tw domain name, it can send a query to the recorded name server IP address. *interface_name*: This is the interface through which the ISP provides a DNS server. The interface should be activated and set to be a DHCP client. The no command deletes a zone forwarder record.
`ip dns server zone-forwarder {<1..32>|append|insert <1..32>} {domain_zone_name|*} user-defined w.x.y.z {ip_type} [private | interface {interface_name | auto}]`	Sets a domain zone forwarder record that specifies a DNS server's IP address. `private | interface`: Use `private` if the Zyxel Device connects to the DNS server through a VPN tunnel. Otherwise, use the `interface` command to set the interface through which the Zyxel Device sends DNS queries to a DNS server. The `auto` means any interface that the Zyxel Device uses to send DNS queries to a DNS server according to the routing rule.
`ip dns server zone-forwarder move <1..32> to <1..32>`	Changes the index number of a zone forwarder record.
`no ip dns server rule <1..32>`	Deletes a service control rule.
`show ip dns server`	Displays all DNS entries.
`show ip dns server database`	Displays all configured records.
`show ip dns server status`	Displays whether this service is enabled or not.
`show ip dns security-options all`	Displays security options configured for the customized and default rules.
`ip dns server aaaa-record {FQDN_DNS | FQDN_WILDCARD_DNS} IPv6`	An address record contains the mapping of a Fully-Qualified Domain Name (FQDN) to an IP address. Type a Fully-Qualified Domain Name (FQDN) of a server. An FQDN starts with a host name and continues all the way up to the top-level domain name. For example, www.zyxel.com.tw is a fully qualified domain name, where "www" is the host, "zyxel" is the third-level domain, "com" is the second-level domain, and "tw" is the top level domain. Underscores are not allowed. Use "*." as a prefix in the FQDN for a wildcard domain name (for example, *.example.com).
`ip dns server cname-record {FQDN_DNS | FQDN_WILDCARD_DNS} {FQDN_DNS}`	A Canonical Name Record or CNAME record is a type of resource record in the Domain Name System (DNS) that specifies that the domain name is an alias of another, canonical domain name. Type a Fully-Qualified Domain Name (FQDN) of a server. An FQDN starts with a host name and continues all the way up to the top-level domain name. For example, www.zyxel.com.tw is a fully qualified domain name, where "www" is the host, "zyxel" is the third-level domain, "com" is the second-level domain, and "tw" is the top level domain. Underscores are not allowed. Use "*." as a prefix in the FQDN for a wildcard domain name (for example, *.example.com).
`ip dns security-options {default | 1}]`	Selects to use the default security option or profile '1'. The default allows any address to use `additional-from-cache` and `recursion`.
`name DNS_OPTIONS_NAME`	Names the DNS security options profile.

Table 299 Command Summary: DNS (continued)

COMMAND	DESCRIPTION
`no address-object-group {any | PROFILE}`	Sets the address object to be any or a previously created one. no removes the address object from this DNS security options profile.
`no additional-from-cache activate`	Activated allows the Zyxel Device to reply to queries with previously cached DNS requests. Deactivated (no) does not.
`no recursion activate`	Activated recursion allows the Zyxel Device to forward queries it can't find in its DNS database. Deactivated (no) does not.

63.6.3 DNS Command Examples

This command sets an A record that specifies the mapping of a fully qualified domain name (www.abc.com) to an IP address (210.17.2.13).

```
Router# configure terminal
Router(config)# ip dns server a-record www.abc.com 210.17.2.13
```

This command displays security options configured for the customized and default rules.

```
Router# configure terminal
Router(config)# show ip dns security-options all
security option rule: 1
   Name: Customize
   Address Object: RFC1918_1, RFC1918_2, RFC1918_3
   Additional Info from Cache: allow
   Recursion Query: deny
security option rule: default
   Name: Default
   Address Object: any
   Additional Info from Cache: allow
   Recursion Query: allow
Router(config)#
```

63.7 Authentication Server Overview

The Zyxel Device can also work as a RADIUS server to exchange messages with other APs for user authentication and authorization.

63.7.1 Authentication Server Commands

The following table lists the authentication server commands you use to configure the Zyxel Device's built-in authentication server settings.

Table 300 Command Summary: Authentication Server

COMMAND	DESCRIPTION
`[no] auth-server activate`	Sets the Zyxel Device to act as an authentication server for other RADIUS clients, such as APs. The `no` command sets the Zyxel Device to not act as an authentication server for other APs.
`auth-server authentication` *`auth_method`*	Specifies an authentication method used by the authentication server.
`no auth-server authentication`	Resets the authentication method used by the authentication server to the factory default (`default`).
`[no] auth-server cert` *`certificate_name`*	Specifies a certificate used by the authentication server (Zyxel Device). The `no` command resets the certificate used by the authentication server to the factory default (`default`). *`certificate_name`*: The name of the certificate. You can use up to 31 alphanumeric and ;'~!@#$%^&()_+[]{}',.=- characters.
`[no] auth-server trusted-client` *`profile_name`*	Creates a trusted RADIUS client profile. The `no` command deletes the specified profile. *`profile-name`*: You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
`[no] activate`	Enables the client profile. The `no` command disables the profile.
`[no] ip address` *`ip subnet_mask`*	Sets the client's IP address and subnet mask. The `no` command clears this setting.
`[no] secret` *`secret`*	Sets a password as the key to be shared between the Zyxel Device and the client. The `no` command clears this setting.
`[no] description` *`description`*	Sets the description for the profile. The `no` command clears this setting. *`description`*: You can use alphanumeric and `()+/:=?!*#@$_%-` characters, and it can be up to 60 characters long.
`show auth-server status`	Displays the Zyxel Device's authentication server settings.
`show auth-server trusted-client`	Displays all RADIUS client profile settings.
`show auth-server trusted-client` *`profile_name`*	Displays the specified RADIUS client profile settings.

63.7.2 Authentication Server Command Examples

The following example shows you how to enable the authentication server feature on the Zyxel Device and sets a trusted RADIUS client profile. This example also shows you the authentication server and client profile settings.

```
Router# configure terminal
Router(config)# auth-server activate
Router(config)# auth-server trusted-client AP-1
Router(config-trusted-client-AP-1)# activate
Router(config-trusted-client-AP-1)# ip address 10.10.1.2 255.255.255.0
Router(config-trusted-client-AP-1)# secret 12345678
Router(config-trusted-client-AP-1)# exit
Router(config)# show auth-server status
activation: yes
authentication method: default
certificate: default
Router(config)# show auth-server trusted-client AP-1
Client: AP-1
  Activation: yes
  Description:
  IP: 10.10.1.2
  Netmask: 255.255.255.0
  Secret: VQEq907jWB8=
Router(config)#
```

63.8 Notification

The notification commands allow you to configure the Zyxel Device to send you event notifications by SMS and email. You can also configure how the Zyxel Device notifies clients that they have accessed a restricted web page.

63.8.1 Mail Server Commands

The mail server commands allow you configure a mail server, so you can receive reports and notification emails such as when your password is about to expire.

Table 301 mail-server commands

COMMAND	DESCRIPTION
`mail-server`	Enters mail-server sub-command mode for configuring e-mail server settings and notification email settings.
`[no] mail-from` *`email_address`*	Sets the email address from which the notification email is sent.
`[no] mail-subject append system-name`	Determines whether the system name will be appended to the subject of the notification e-mails.
`[no] mail-subject append date-time`	Determines whether the sending date-time will be appended at subject of the notification e-mails.
`schedule hour <0..23> minute <00..59>`	Sets the time for sending out the notification e-mails.
`show`	Displays mail server settings.

Table 301 mail-server commands

COMMAND	DESCRIPTION
[no] smtp-address {*ip* | *hostname*}	Sets the SMTP mail server IP address or domain name. The *no* command removes the mail server IP address or domain name.
[no] smtp-auth activate	Enables or disables (*no* command) SMTP authentication.
[no] smtp-auth username *username* password *password*	Sets or removes (*no* command) the username and password for SMTP authentication. The password can be up to 63 characters long.
[no] smtp-port <1..65535>	Sets the SMTP port. The no command deletes the setting.
[no] smtp-tls activate	Sets the mail server to use or not use (*no* command) Transport Layer Security (TLS) for encrypted communications between the mail server and the Zyxel Device.
[no] smtp-tls authenticate-server	Sets the Zyxel Device to authenticates the mail server in the TLS handshake or not (*no* command).
[no] smtp-tls starttls-off	The mail server uses SSL or TLS for encrypted communications between the mail server and the Zyxel Device. This command turns off STARTTLS and uses the TLS protocol. The no command enables the default STARTTLS protocol (SSL) for encrypted communications between the mail server and the Zyxel Device.

63.8.2 SMS Service Commands

The Zyxel Device supports Short Message Service (SMS) to send short text messages to mobile devices.

Note: Support for ViaNett on ZyWALL devices will end soon. In firmware version 4.60, all ViaNett configuration settings have been removed from the Web Configurator UI. You can still configure ViaNett using the CLI, but commands related to ViaNett will be removed from the CLI in a future firmware update. We recommend not purchasing any new ViaNett credits.

Table 302 sms-service Commands

COMMAND	DESCRIPTION
sms-service account-send phone *phone_number* account *user_name* password *password*	Specifies the guest account information and the number of mobile device to which you want to send a text message.
[no] sms-service activate	Enables the SMS service on the Zyxel Device. The no command disabled the SMS service.
sms-service default-country-code *country_code*	Sets the default country code for the mobile phone number to which you want to send SMS messages. *country_code*: one to four digits
sms-service provider vianett	Enters the sms-service-vianett sub-command mode to configure your ViaNett account information.
[no] password *password*	Sets the password for your ViaNett account.
[no] username *e-mail*	Sets the user name for your ViaNett account.
sms-service provider-select vianett {vianett|email-to-sms}	Selects vianett if you use ViaNett to help forward SMS messages. Selects email-to-sms if you use another SMS gateway to help forward SMS messages.

Table 302 sms-service Commands (continued)

COMMAND	DESCRIPTION
`sms-service provider email-to-sms`	Enters email-to-SMS subcommand mode.
`provider-domain` *`domain_name`*	Sets the domain name of your SMS service provider. The domain name can be of up to 252 characters.
`auto-append`	Adds the domain name of your SMS service provider after the receiver's mobile phone number.
`mail-subject` *`mail-subject`*	Sets the subject line of up to 128 characters for outgoing e-mail from the Zyxel Device.
`mail-from` *`user@domainname`*	Sets the sender's email address of up to 64 characters. This email address needs to be in your SMS provider's allowed sender address list. If you leave this field blank, the Zyxel Device will use the IP address or domain name configured using the command, `smtp-address {ip | hostname}`.
`mail-to` *`mobile_number@provider_domain`*	Sets the mobile phone number of up to 80 characters. You can only have one receiver. Use this variable in brackets [$mobile_number$], and the Zyxel Device will use the mobile phone number of the user logging in. Use the command, `username` *`username`* `phone` *`phone_number`*, to add a valid mobile telephone number for a user.
`no {provider-domain|auto-append|mail-subject|mail-from|mail-to}`	Clears the settings.
`sms-service test-send phone` *`phone_number`* `msg` *`message`*	Specifies the mobile phone number and message to test whether the Zyxel Device can use SMS to send a text message.
`show sms-service`	Displays the SMS settings.
`show sms-service activation`	Displays whether the SMS service is enabled.
`show sms-service default-country-code`	Displays the default country code for the mobile phone number to which you want to send SMS messages.
`show sms-service provider vianett`	Displays the ViaNett account information.
`show sms-service provider email-to-sms`	Displays the settings of the SMS service provider you use.

63.8.2.1 SMS Commands Example

The following example enables the SMS service on the Zyxel Device to provide and configures the ViaNett account information. It then displays the SMS settings.

```
Router# configure terminal
Router(config)# sms-service activate
Router(config)# sms-service provider vianett
Router(sms-service-vianett)# username test@example.com
Router(sms-service-vianett)# password 12345
Router(sms-service-vianett)# exit
Router(config)# show sms-service
enable sms service: yes
SMS Country-Code: 0
SMS Provider-Selected: vianett
SMS Service: Vianett
  username: test@example.com
  password: 12345
Router(config)#
```

63.8.3 Response Message Commands

When a webpage is blocked by a service such as URL threat filter or content filter, the Zyxel Device displays an HTML block page. The HTML block page informs the user that the page was blocked and why. You can use the response message commands to customize the look of this block page.

Table 303 Commands for Response Message

COMMAND	DESCRIPTION
`[no] respmsg url-filter block-page customized activate`	Use a custom block page when a page is blocked. The no command tells the Zyxel Device to use the default block page.
`respmsg url-filter block-page message-color {<rgb(0,0,255)> | <color name> | <#00FF00>}`	Sets the color of the message on the block page. You can specify the color as an RGB value, a Hex value, or as a CSS color name.
`respmsg url-filter block-page background-color {<rgb(0,0,255)> | <color name> | <#00FF00>}`	Sets the color of the background on the block page. You can specify the color as an RGB value, a Hex value, or as a CSS color name.
`respmsg url-filter block-page banner-color {<rgb(0,0,255)> | <color name> | <#00FF00>}`	Sets the color of the banner at the bottom of the block page. You can specify the color as an RGB value, a Hex value, or as a CSS color name.
`respmsg url-filter block-page banner-message-color {<rgb(0,0,255)> | <color name> | <#00FF00>}`	Sets the color of the banner message at the bottom of the block page. You can specify the color as an RGB value, a Hex value, or as a CSS color name.
`show respmsg url-filter block-page`	Shows the current response message settings.

63.9 Language Commands

Use the `language` commands to display what language the web configurator is using or change it. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 304 Command Summary: Language

COMMAND	DESCRIPTION
`language` *`language_name`*	Specifies the language used in the web configurator screens. To view a list of supported language names, run the command `show language all`.
`[no] language update auto`	Enables (disables) automatic language pack updates at regular times and days. Note: To save network resources, periodically run the "language update package" command instead of enabling automatic updates.
`language update daily <0..23>`	Enables automatic language pack updates every day at the time specified.
`language update hourly`	Enables automatic language pack updates every hour.
`language update package`	Immediately updates the language pack from the update server.
`language update weekly {sun | mon | tue | wed | thu | fri | sat} <0..23>`	Enables automatic language pack updates once-a-week at the time and day specified.
`show language {setting | all}`	`setting` displays the current display language in the web configurator screens. `all` displays the languages available on the Zyxel Device.

63.10 IPv6 Commands

Use the `ipv6` commands to enable or disable IPv6 support. You must use the `configure terminal` command to enter the configuration mode before you can use the commands that configure settings.

Table 305 Command Summary: IPv6

COMMAND	DESCRIPTION
`[no] ipv6 activate`	Enables or disables IPv6 support.
`show ipv6 status`	Displays whether IPv6 support is enabled or disabled.

63.11 ZON Overview

The Zyxel One Network (ZON) utility uses the Zyxel Discovery Protocol (ZDP) for discovering and configuring ZDP-aware Zyxel devices in the same broadcast domain as the computer on which ZON is installed.

The ZON Utility issues requests via ZDP and in response to the query, the Zyxel device responds with basic information including IP address, firmware version, location, system and model name. The information is then displayed in the ZON Utility screen and you can perform tasks like basic configuration of the devices and batch firmware upgrade in it. You can download the ZON Utility at www.zyxel.com and install it on a computer.

63.11.1 LLDP

LLDP is a layer-2 protocol that allows a network device to advertise its identity and capabilities on the local network. It also allows the device to maintain and store information from adjacent devices which are directly connected to the network device. This helps you discover network changes and perform necessary network reconfiguration and management.

63.11.2 ZON Commands

The following table describes the commands available for ZON. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 306 Command Summary: ZON

COMMAND	DESCRIPTION
`zon lldp server`	Activates LLDP discovery on the Zyxel Device. This allows you to use Link Layer Discovery Protocol (LLDP) for discovering and configuring LLDP-aware devices in the same broadcast domain as the Zyxel Device that you are logged into using the web configurator.
`zon lldp server tx-hold <1..10>`	Sets the multiplier used to calculate the TTL (Time To Live) value for the transmitted LLDP packets. The TTL value determines how long the device information can be saved on the neighbors. LLDP TTL = the multi pl er * the LLDP transmission interval
`zon lldp server tx-interval <1..600>`	Sets the interval (in seconds) at which the Zyxel Device sends a LLDP packet to the neighbor.
`zon zdp server`	Activates ZDP discovery on the Zyxel Device.
`show zon lldp neighbors`	Displays the Zyxel Device's neighboring devices via LLDP.
`show zon lldp server config`	Displays the LLDP settings.
`show zon lldp server statistics`	Displays the LLDP traffic statistics.
`show zon lldp server status`	Displays whether LLDP discovery is enabled.
`show zon zdp server status`	Displays whether ZDP discovery is enabled.

63.11.3 ZON Examples

This example enables LLDP discovery and displays whether LLDP discovery is enabled on the Zyxel Device.

```
Router(config)# zon lldp server
Router(config)# zon lldp server status
status: active
Router(config)#
```

63.12 Fast Forwarding

Fast Forwarding maximizes the network performance of the Zyxel Device, by enabling a faster packet switching method which uses a trie (prefix tree).

When Fast Forwarding is enabled, essential network services such as NAT, routing, firewall, and VPN work as expected. However, security and logging services such as UTM, web authentication, MAC address binding, BWM, and traffic statistics are bypassed. This means traffic passes through theZyxel Device unchecked and unlogged.

Note: Enabling fast forward might expose your network to security threats. We recommend enabling fast forwarding temporarily and only when it is needed

63.12.1 Fast Forwarding Technical Overview

When switching a packet, a network device examines the packet's destination and then searches its local route cache to determine the output interface and the next hop to the destination. The route cache must be periodically cleared of old and invalid entries, to prevent the cache from consuming too much memory.

Fast Forwarding improves route cache performance by using a trie (prefix tree). A trie is a 256-way binary tree that does not store any data. Instead, each leaf in the tree contains a pointer to data in a separate adjacency table. The routing cache stores destination information in the search tree, and information about how to reach each destination in the adjacency table. Separating the routing cache into two data structures offers several advantages:

- The search tree and adjacency table can be created and recreated separately.
- Modifying entries in the adjacency table does not invalidate entries in the search tree.
- Entries in the adjacency table can point to each other, speeding up recursive routing. Recursive routing is where a device looks up a packet's next hop in the routing cache but does not know how to reach the next hop, requiring another lookup.
- The adjacency table can be updated directly from the device's ARP cache and routing table. This eliminates the need to periodically clear old and invalid entries from the cache.

63.12.2 Fast Forwarding Commands

The following table describes the commands available for fast forwarding. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 307 Command Summary: Fast Forwarding

COMMAND	DESCRIPTION
`fast forwarding {`*`activate`* `|` *`deactivate`*`}`	Enables or disables fast forwarding on the Zyxel Device.
`show fast forwarding status`	Displays whether fast forwarding is currently enabled.

CHAPTER 64
System Remote Management

This chapter shows you how to determine which services/protocols can access which Zyxel Device zones (if any) from which computers.

Note: To access the Zyxel Device from a specified computer using a service, make sure no service control rules or to-Zyxel Device firewall rules block that traffic.

64.1 Remote Management Overview

You may manage your Zyxel Device from a remote location via:

- Internet (WAN only)
- LAN only
- ALL (LAN&WAN&DMZ)
- DMZ only

To disable remote management of a service, deselect Enable in the corresponding service screen.

64.1.1 Remote Management Limitations

Remote management will not work when:

1. You have disabled that service in the corresponding screen.
2. The accepted IP address in the Service Control table does not match the client IP address. If it does not match, the Zyxel Device will disconnect the session immediately.
3. There is a firewall rule that blocks it.

64.1.2 System Timeout

There is a lease timeout for administrators. The Zyxel Device automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling.

Each user is also forced to log in the Zyxel Device for authentication again when the reauthentication time expires.

64.2 Common System Command Input Values

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 308 Input Values for General System Commands

LABEL	DESCRIPTION
address_object	The name of the IP address (group) object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
rule_number	The number of a service control rule. 1 - *X* where *X* is the highest number of rules the Zyxel Device model supports.
zone_object	The name of the zone. For some Zyxel Device models, use up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive. For other Zyxel Device models, use pre-defined zone names like DMZ, LAN1, SSL VPN, IPSec VPN, OPT, and WAN.

64.3 HTTP/HTTPS Commands

The following table describes the commands available for HTTP/HTTPS. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 309 Command Summary: HTTP/HTTPS

COMMAND	DESCRIPTION
`[no] ip http authentication` *auth_method*	Sets an authentication method used by the HTTP/HTTPS server. The `no` command resets the authentication method used by the HTTP/HTTPS server to the factory default (`default`). *auth_method*: The name of the authentication method. You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
`[no] ip http content-security-policy`	Sets the content-security-policy header to frame-ancestors 'none'. It prevents loading the web page in an iframe from any source. The content-security-policy HTTP response header is a security header that can help avoid clickjacking attacks by defining which resources are allowed to loaded or executed. The `no` command removes the header directive. Note: This security is provided only for browsers that support content-security-policy (CSP).
`[no] ip http port <1..65535>`	Sets the HTTP service port number. The `no` command resets the HTTP service port number to the factory default (80).
`[no] ip http secure-port <1..65535>`	Sets the HTTPS service port number. The `no` command resets the HTTPS service port number to the factory default (443).
`[no] ip http secure-server`	Enables HTTPS access to the Zyxel Device web configurator. The `no` command disables HTTPS access to the Zyxel Device web configurator.
`[no] ip http secure-server auth-client`	Sets the client to authenticate itself to the HTTPS server. The `no` command sets the client not to authenticate itself to the HTTPS server.

Table 309 Command Summary: HTTP/HTTPS (continued)

COMMAND	DESCRIPTION
[no] ip http secure-server cert *certificate_name*	Specifies a certificate used by the HTTPS server. The no command resets the certificate used by the HTTPS server to the factory default (default). *certificate_name*: The name of the certificate. You can use up to 31 alphanumeric and ;'~!@#$%^&()_+[]{}',.=- characters.
[no] ip http secure-server force-redirect	Redirects all HTTP connection requests to a HTTPS URL. The no command disables forwarding HTTP connection requests to a HTTPS URL.
[no] ip http secure-server sslv3	Turns on SSLv3 support in the HTTP server. The no command turns SSLv3 support off.
ip http secure-server table {admin|user} rule {*rule_number*|append|insert *rule_number*} access-group {ALL|*address_object*} zone {ALL|*zone_object*} action {accept|deny}	Sets a service control rule for HTTPS service.
ip http secure-server table {admin|user} rule move *rule_number* to *rule_number*	Changes the index number of a HTTPS service control rule.
ip http secure-server cipher-suite {aes| rc4| des| 3des| dhe}	Has the Zyxel Device use or not use the specified encryption algorithm for the SSL in HTTPS connections. rc4: RC4 (RC4 may impact the Zyxel Device's CPU performance since the Zyxel Device's encryption accelerator does not support it). aes: AES des: DES 3des: Triple DES dhe: DHE (Diffie-Hellman Ephemeral)
[no] ip http server	Allows HTTP access to the Zyxel Device web configurator. The no command disables HTTP access to the Zyxel Device web configurator.
ip http server table {admin|user} rule {*rule_number*|append|insert *rule_number*} access-group {ALL|*address_object*} zone {ALL|*zone_object*} action {accept|deny}	Sets a service control rule for HTTP service.
ip http server table {admin|user} rule move *rule_number* to *rule_number*	Changes the number of a HTTP service control rule.
no ip http secure-server table {admin|user} rule *rule_number*	Deletes a service control rule for HTTPS service.
no ip http server table {admin|user} rule *rule_number*	Deletes a service control rule for HTTP service.

Table 309 Command Summary: HTTP/HTTPS (continued)

COMMAND	DESCRIPTION
ip http skip-csrf-check	Omits cross-site request forgery (CSRF) checking. CSRF exploits the trust that a site has in a user's browser to transmit unauthorized commands as if they are from a user that the website trusts.
no ip http skip-csrf-check	Performs cross-site request forgery (CSRF) checking.
[no] ip http x-frame-options	Sets the x-frame-options header to SAMEORIGIN. The web page can only be displayed in a frame on the same origin (from the site/host which is the same as the one serving the page). The x-frame-options HTTP response header is a security header that can help avoid clickjacking attacks by indicating whether a browser is allowed to load a page in a frame. The no command removes the header directive. Note: This security is provided only for browsers that support x-frame-options.
show ip http server status	Displays HTTP settings.
show ip http server secure status	Displays HTTPS settings.
show ip http skip-csrf-check	Shows whether cross-site request forgery (CSRF) checking is done or not.

64.3.1 HTTP/HTTPS Command Examples

This following example adds a service control rule that allowed an administrator from the computers with the IP addresses matching the Marketing address object to access the WAN zone using HTTP service.

```
Router# configure terminal
Router(config)# ip http server table admin rule append access-group
Marketing zone WAN action accept
```

This command sets an authentication method Example used by the HTTP/HTTPS server to authenticate the client(s).

```
Router# configure terminal
Router(config)# ip http authentication Example
```

This following example sets a certificate named MyCert used by the HTTPS server to authenticate itself to the SSL client.

```
Router# configure terminal
Router(config)# ip http secure-server cert MyCert
```

64.4 SSH

Unlike Telnet or FTP, which transmit data in clear text, SSH (Secure Shell) is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network.

64.4.1 SSH Implementation on the Zyxel Device

Your Zyxel Device supports SSH using RSA authentication and the following encryption methods: AES, 3DES, Archfour, Blowfish. The SSH server is implemented on the Zyxel Device for remote management on port 22 (by default).

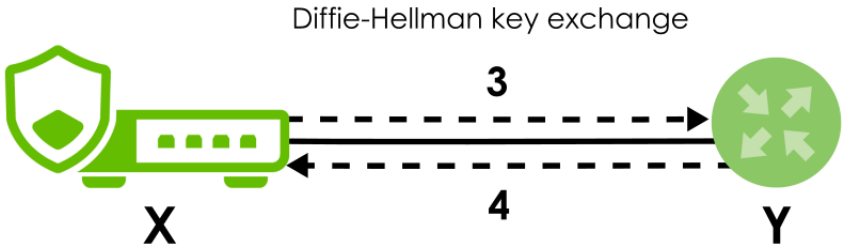
64.4.2 Requirements for Using SSH

You must install an SSH client program on a client computer (Windows or Linux operating system) that is used to connect to the Zyxel Device over SSH.

64.4.3 Diffie-Hellman (DH) Key Exchange

The Zyxel Device and the remote IPSec router use DH public-key cryptography to establish a shared secret. The shared secret is then used to generate encryption keys for the IKE SA and IPSec SA. In main mode, this is done in steps 3 and 4, as illustrated next.

Figure 43 IKE SA: Main Negotiation Mode, Steps 3 - 4: DH Key Exchange



DH public-key cryptography is based on DH key groups. Each key group is a fixed number of bits long. The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. For example, DH2 keys (1024 bits) are more secure than DH1 keys (768 bits), but DH2 keys take longer to encrypt and decrypt.

Note: Ensure both The Zyxel Device and the remote IPSec router use the same DH key group.

The available DHx options on the Zyxel Device are:

- DH1 - uses a 768-bit random number to create an encryption key.
- DH2 - uses a 1024-bit random number to create an encryption key.
- DH5 - uses a 1536-bit random number to create an encryption key.
- DH14 - uses a 2048-bit random number to create an encryption key.
- DH15 - uses a 3072-bit random number to create an encryption key.
- DH16 - uses a 4096-bit random number to create an encryption key.
- DH17 - uses a 6144-bit random number to create an encryption key.

- DH18 - uses a 8192-bit random number to create an encryption key.
- DH19 - uses a 256-bit elliptic curve to create an encryption key, offering stronger security than the random number-based method.
- DH20 - uses a 384-bit elliptic curve to create an encryption key, offering stronger security than the random number-based method.
- DH21 - uses a 521-bit elliptic curve to create an encryption key, offering stronger security than the random number-based method.

Elliptic Curve Diffie-Hellman provides a higher level of protection using elliptic curve mathematical principles (recommeded).

Different operating systems may support different DH key groups. Check your operating system documentation.

- For Windows VPN clients, Zyxel SecuExtender perpetual VPN clients versions 3.8.203.61.32 and earlier support DH1 to DH14.
- For macOS VPN clients, Zyxel SecuExtender subscription VPN clients versions 1.2.0.7 and later support DH14 to DH21. For Windows VPN clients, Zyxel SecuExtender subscription VPN clients versions 5.6.80.007 and later support DH14 to DH21.
- Windows versions 7, 10, 11 built-in IKEv2 VPN clients support DH2 by default.
- macOS versions 14.2 and later built-in IKEv2 VPN clients support DH14 by default.
- iOS versions 10.15 and later built-in IKEv2 VPN clients support DH14 by default.

64.4.4 SSH Commands

The following table describes the commands available for SSH. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 310 Command Summary: SSH

COMMAND	DESCRIPTION
`ssh {user@W.X.Y.Z | or W.X.Y.Z)`	Sets the user name where W.X.Y.Z is an IPv4 address or domain of an SSH client.
`[no] ip ssh server`	Allows SSH access to the Zyxel Device CLI. The no command disables SSH access to the Zyxel Device CLI.
`[no] ip ssh server cert` *`certificate_name`*	Sets a certificate whose corresponding private key is to be used to identify the Zyxel Device for SSH connections. The no command resets the certificate used by the SSH server to the factory default (`default`). *`certificate_name`*: The name of the certificate. You can use up to 31 alphanumeric and ;'~!@#$%^&()_+[]{}',.=- characters.
`[no] ip ssh server port <1..65535>`	Sets the SSH service port number. The no command resets the SSH service port number to the factory default (22).
`ip ssh server rule {`*`rule_number`*`|append|insert` *`rule_number`*`} access-group {ALL|`*`address_object`*`} zone {ALL|`*`zone_object`*`} action {accept|deny}`	Sets a service control rule for SSH service. *`address_object`*: The name of the IP address (group) object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. *`zone_object`*: The name of the zone. For some Zyxel Device models, use up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive. For other Zyxel Device models, use pre-defined zone names like DMZ, LAN1, SSL VPN, IPSec VPN, OPT, and WAN.

Table 310 Command Summary: SSH (continued)

COMMAND	DESCRIPTION
`ip ssh server rule move` *`rule_number`* `to` *`rule_number`*	Changes the index number of a SSH service control rule.
`[no] ip ssh server v1`	Enables remote management using SSH v1. The no command stops the Zyxel Device from using SSH v1. This command has been removed from firmware version 4.60 and later, because SSH v1 is no longer supported.
`no ip ssh server rule` *`rule_number`*	Deletes a service control rule for SSH service.
`[no] ip ssh server kexalg dhe`	Enables or disables the SSH server to use the key exchange algorithm DHE (Diffie-Hellman Ephemeral).
`show ip ssh server status`	Displays SSH settings.

64.4.5 SSH Command Examples

This command sets a service control rule that allowed the computers with the IP addresses matching the specified address object to access the specified zone using SSH service.

```
Router# configure terminal
Router(config)# ip ssh server rule 2 access-group Marketing zone WAN action
accept
```

This command sets a certificate (Default) to be used to identify the Zyxel Device.

```
Router# configure terminal
Router(config)# ip ssh server cert Default
```

64.5 Telnet

You can configure your Zyxel Device for remote Telnet access.

64.6 Telnet Commands

The following table describes the commands available for Telnet. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 311 Command Summary: Telnet

COMMAND	DESCRIPTION
`[no] ip telnet server`	Allows Telnet access to the Zyxel Device CLI. The no command disables Telnet access to the Zyxel Device CLI.
`[no] ip telnet server port <1..65535>`	Sets the Telnet service port number. The no command resets the Telnet service port number back to the factory default (23).

Table 311 Command Summary: Telnet (continued)

COMMAND	DESCRIPTION
`ip telnet server rule {rule_number|append|insert rule_number} access-group {ALL|address_object} zone {ALL|zone_object} action {accept|deny}`	Sets a service control rule for Telnet service. *address_object*: The name of the IP address (group) object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. *zone_object*: The name of the zone. For some Zyxel Device models, use up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive. For other Zyxel Device models, use pre-defined zone names like DMZ, LAN1, SSL VPN, IPSec VPN, OPT, and WAN.
`ip telnet server rule move rule_number to rule_number`	Changes the index number of a service control rule.
`no ip telnet server rule rule_number`	Deletes a service control rule for Telnet service.
`show ip telnet server status`	Displays Telnet settings.

64.6.1 Telnet Commands Examples

This command sets a service control rule that allowed the computers with the IP addresses matching the specified address object to access the specified zone using Telnet service.

```
Router# configure terminal
Router(config)# ip telnet server rule 11 access-group RD zone LAN action
accept
```

This command displays Telnet settings.

```
Router# configure terminal
Router(config)# show ip telnet server status
active     : yes
port       : 23
service control:
No.  Zone                        Address                    Action
================================================================================
Router(config)#
```

64.7 Configuring FTP

You can upload and download the Zyxel Device's firmware and configuration files using FTP. To use this feature, your computer must have an FTP client.

64.7.1 FTP Commands

The following table describes the commands available for FTP. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 312 Command Summary: FTP

COMMAND	DESCRIPTION
`[no] ip ftp server`	Allows FTP access to the Zyxel Device. The no command disables FTP access to the Zyxel Device.
`[no] ip ftp server cert` *`certificate_name`*	Sets a certificate to be used to identify the Zyxel Device. The no command resets the certificate used by the FTP server to the factory default.
`[no] ip ftp server port <1..65535>`	Sets the FTP service port number. The no command resets the FTP service port number to the factory default (21).
`[no] ip ftp server tls-required`	Allows FTP access over TLS. The no command disables FTP access over TLS.
`ip ftp server rule {`*`rule_number`*`|append|insert` *`rule_number`*`} access-group {ALL|`*`address_object`*`} zone {ALL|`*`zone_object`*`} action {accept|deny}`	Sets a service control rule for FTP service. *`address_object`*: The name of the IP address (group) object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. *`zone_object`*: The name of the zone. For some Zyxel Device models, use up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive. For other Zyxel Device models, use pre-defined zone names like DMZ, LAN1, SSL VPN, IPSec VPN, OPT, and WAN.
`ip ftp server rule move` *`rule_number`* `to` *`rule_number`*	Changes the index number of a service control rule.
`no ip ftp server rule` *`rule_number`*	Deletes a service control rule for FTP service.
`[no] ip ftp server cipher-suite {3des| des| rc4| dhe}`	Enables or disables the following ciphers for the FTP service: 3DES, DES, RC4, DHE. These ciphers are considered weak, so from firmware version 4.60 onwards, they are disables by default.
`show ip ftp server status`	Displays FTP settings.

64.7.2 FTP Commands Examples

This command sets a service control rule that allowed the computers with the IP addresses matching the specified address object to access the specified zone using FTP service.

```
Router# configure terminal
Router(config)# ip ftp server rule 4 access-group Sales zone WAN action
accept
```

This command displays FTP settings.

```
Router# configure terminal
Router(config)# show ip ftp server status
active     : yes
port       : 21
certificate: default
TLS        : no
service control:
No.  Zone                    Address                     Action
================================================================================
```

64.8 SNMP

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. Your Zyxel Device supports SNMP agent functionality, which allows a manager station to manage and monitor the Zyxel Device through the network. The Zyxel Device supports SNMP version one (SNMPv1) version two (SNMPv2c) and version 3 (SNMPv3).

SNMP v3 enhances security for SNMP management using authentication and encryption. SNMP managers can be required to authenticate with agents before conducting SNMP management sessions.

Security can be further enhanced by encrypting the SNMP messages sent from the managers. Encryption protects the contents of the SNMP messages. When the contents of the SNMP messages are encrypted, only the intended recipients can read them.

64.8.1 Supported MIBs

The Zyxel Device supports MIB II that is defined in RFC-1213 and RFC-1215. The Zyxel Device also supports private MIBs to collect information about CPU and memory usage and VPN total throughput. The focus of the MIBs is to let administrators collect statistical data and monitor status and performance. You can download the Zyxel Device's MIBs from www.zyxel.com.

64.8.2 SNMP Traps

The Zyxel Device will send traps to the SNMP manager when any one of the following events occurs:

Table 313 SNMP Traps

OBJECT LABEL	OBJECT ID	DESCRIPTION
Cold Start	1.3.6.1.6.3.1.1.5.1	This trap is sent when the Zyxel Device is turned on or an agent restarts.
linkDown	1.3.6.1.6.3.1.1.5.3	This trap is sent when the Ethernet link is down.
linkUp	1.3.6.1.6.3.1.1.5.4	This trap is sent when the Ethernet link is up.
authenticationFailure	1.3.6.1.6.3.1.1.5.5	This trap is sent when an SNMP request comes from non-authenticated hosts.
vpnTunnelDisconnected	1.3.6.1.4.1.890.1.6.22.2.3	This trap is sent when an IPSec VPN tunnel is disconnected.

Table 313 SNMP Traps (continued)

OBJECT LABEL	OBJECT ID	DESCRIPTION
vpnTunnelName	1.3.6.1.4.1.890.1.6.22 .2.2.1.1	This trap is sent along with the vpnTunnelDisconnected trap. This trap carries the disconnected tunnel's IPSec SA name.
vpnIKEName	1.3.6.1.4.1.890.1.6.22 .2.2.1.2	This trap is sent along with the vpnTunnelDisconnected trap. This trap carries the disconnected tunnel's IKE SA name.
vpnTunnelSPI	1.3.6.1.4.1.890.1.6.22 .2.2.1.3	This trap is sent along with the vpnTunnelDisconnected trap. This trap carries the security parameter index (SPI) of the disconnected VPN tunnel.

64.8.3 SNMP Commands

The following table describes the commands available for SNMP. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 314 Command Summary: SNMP

COMMAND	DESCRIPTION
`[no] snmp-server`	Allows SNMP access to the Zyxel Device. The no command disables SNMP access to the Zyxel Device.
`[no] snmp-server community` *`community_string`* `{ro|rw}`	Enters up to 64 characters to set the password for read-only (ro) or read-write (rw) access. The no command resets the password for read-only (ro) or read-write (rw) access to the default.
`[no] snmp-server contact` *`description`*	Sets the contact information (of up to 60 characters) for the person in charge of the Zyxel Device. The no command removes the contact information for the person in charge of the Zyxel Device.
`[no] snmp-server enable {informs|traps}`	Enables all SNMP notifications (informs or traps). The no command disables all SNMP notifications (informs or traps).
`[no] snmp-server host {`*`w.x.y.z|fqdn|ipv6 address`*`} [`*`community_string`*`]`	Sets the IPv4 or IPv6 address of the host that receives the SNMP notifications. The no command removes the host that receives the SNMP notifications.
`[no] snmp-server location` *`description`*	Sets the geographic location (of up to 60 characters) for the Zyxel Device. The no command removes the geographic location for the Zyxel Device.
`[no] snmp-server port <1..65535>`	Sets the SNMP service port number. The no command resets the SNMP service port number to the factory default (161).
`snmp-server rule {`*`rule_number`*`|append|insert` *`rule_number`*`} access-group {ALL|`*`address_object`*`} zone {ALL|`*`zone_object`*`} action {accept|deny}`	Sets a service control rule for SNMP service. *`address_object`*: The name of the IP address (group) object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. *`zone_object`*: The name of the zone. For some Zyxel Device models, use up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive. For other Zyxel Device models, use pre-defined zone names like DMZ, LAN1, SSL VPN, IPSec VPN, OPT, and WAN.
`snmp-server rule move` *`rule_number`* `to` *`rule_number`*	Changes the index number of a service control rule.
`no snmp-server rule` *`rule_number`*	Deletes a service control rule for SNMP service.

Table 314 Command Summary: SNMP (continued)

COMMAND	DESCRIPTION
`snmp-server v3user username description authentication {md5 | sha} privacy {none | des | aes} privilege {ro | rw}`	Sets the authentication, privacy and privilege for an SNMPv3 user.
`snmp-server version {v2c | v3}`	Sets the SNMP version for the Zyxel Device. The SNMP version on the Zyxel Device must match the version on the SNMP manager.
`show snmp status`	Displays SNMP Settings.
`show snmp-server v3user status`	Displays authentication, privacy and privilege for configured SNMPv3 users.

64.8.4 SNMP Commands Examples

The following command sets a service control rule that allowed the computers with the IP addresses matching the specified address object to access the specified zone using SNMP service.

```
Router# configure terminal
Router(config)# snmp-server rule 11 access-group Example zone WAN action
accept
```

The following command sets the password (secret) for read-write (`rw`) access.

```
Router# configure terminal
Router(config)# snmp-server community secret rw
```

The following command sets the IP address of the host that receives the SNMP notifications to 172.23.15.84 and the password (sent with each trap) to qwerty.

```
Router# configure terminal
Router(config)# snmp-server host 172.23.15.84 qwerty
```

The following commands create an SNMPv3 rule and then displays the configured settings.

```
Router# configure terminal
Router(config)# snmp-server v3user username john authentication md5 privacy
none privilege rw
Router(config)# show snmp-server v3user status
SNMPv3 user profile: 1
  username: john
  authentication: md5
  privacy: none
  privilege: rw
Router(config)#
```

64.9 ICMP Filter

The `ip icmp-filter` commands are obsolete. See Chapter 29 on page 217 to configure secure policy rules for ICMP traffic going to the Zyxel Device to discard or reject ICMP packets destined for the Zyxel Device.

Configure the ICMP filter to help keep the Zyxel Device hidden from probing attempts. You can specify whether or not the Zyxel Device is to respond to probing for unused ports.

You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 315 Command Summary: ICMP Filter

COMMAND	DESCRIPTION
`[no] ip icmp-filter activate`	Turns the ICMP filter on or off.
`ip icmp-filter rule {<1..32>|append|insert <1..32>} access-group {ALL|ADDRESS_OBJECT} zone {ALL|ZONE_OBJECT} icmp-type {ALL |echo-reply |destination-unreachable |source-quench|redirect|echo-request| router-advertisement|router-solicitation |time-exceeded | parameter-problem| timestamp-request|timestamp-reply| address-mask-request| address-mask-reply} action {accept|deny}`	Sets an ICMP filter rule. ADDRESS_OBJECT: The name of the IP address (group) object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. ZONE_OBJECT: The name of the zone. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
`no ip icmp-filter rule <1..64>`	Deletes an ICMP filter rule.
`ip icmp-filter rule move <1..64> to <1..64>`	Changes the index number of an ICMP filter rule.
`show ip icmp-filter status`	Displays ICMP filter settings.

CHAPTER 65
File Manager

65.1 File Directories

The Zyxel Device stores files in the following directories.

Table 316 FTP File Transfer Notes

DIRECTORY	FILE TYPE	FILE NAME EXTENSION
A	Firmware (upload only)	bin
cert	Non-PKCS#12 certificates	cer
conf	Configuration files	conf
idp	IDP custom signatures	rules
packet_trace	Packet trace results (download only)	
script	Shell scripts	.zysh
tmp	Temporary system maintenance files and crash dumps for technical support use (download only)	

A. After you log in through FTP, you do not need to change directories in order to upload the firmware.

65.2 Configuration Files and Shell Scripts Overview

You can store multiple configuration files and shell script files on the Zyxel Device.

When you apply a configuration file, the Zyxel Device uses the factory default settings for any features that the configuration file does not include. Shell scripts are files of commands that you can store on the Zyxel Device and run when you need them. When you run a shell script, the Zyxel Device only applies the commands that it contains. Other settings do not change.

You can edit configuration files or shell scripts in a text editor and upload them to the Zyxel Device. Configuration files use a .conf extension and shell scripts use a .zysh extension.

These files have the same syntax, which is also identical to the way you run CLI commands manually. An example is shown below.

Figure 44 Configuration File / Shell Script: Example

```
# enter configuration mode
configure terminal
# change administrator password
username admin password 4321 user-type admin
# configure ge3
interface ge3
ip address 172.23.37.240 255.255.255.0
ip gateway 172.23.37.254 metric 1
exit
# create address objects for remote management / to-ZyWALL firewall rules
# use the address group in case we want to open up remote management later
address-object TW_SUBNET 172.23.37.0/24
object-group address TW_TEAM
address-object TW_SUBNET
exit
# enable Telnet access (not enabled by default, unlike other services)
ip telnet server
# open WAN-to-ZyWALL firewall for TW_TEAM for remote management
secure-policy insert 4
from WAN
to ZyWALL
sourceip TW_TEAM
service TELNET
action allow
exit
write
```

While configuration files and shell scripts have the same syntax, the Zyxel Device applies configuration files differently than it runs shell scripts. This is explained below.

Table 317 Configuration Files and Shell Scripts in the Zyxel Device

Configuration Files (.conf)	Shell Scripts (.zysh)
• Resets to default configuration. • Goes into CLI Configuration mode. • Runs the commands in the configuration file.	• Goes into CLI Privilege mode. • Runs the commands in the shell script.

You have to run the example in Table 44 on page 540 as a shell script because the first command is run in Privilege mode. If you remove the first command, you have to run the example as a configuration file because the rest of the commands are executed in Configuration mode. (See Section 1.5 on page 33 for more information about CLI modes.)

65.2.1 Comments in Configuration Files or Shell Scripts

In a configuration file or shell script, use “#” or “!” as the first character of a command line to have the Zyxel Device treat the line as a comment.

Your configuration files or shell scripts can use “exit” or a command line consisting of a single “!” to have the Zyxel Device exit sub command mode.

Note: “exit” or “!'” must follow sub commands if it is to make the Zyxel Device exit sub command mode.

Line 3 in the following example exits sub command mode.

```
interface ge1
ip address dhcp
!
```

Lines 1 and 3 in the following example are comments and line 4 exits sub command mode.

```
!
interface ge1
# this interface is a DHCP client
!
```

Lines 1 and 2 are comments. Line 5 exits sub command mode.

```
! this is from Joe
# on 2006/06/05
interface ge1
ip address dhcp
!
```

65.2.2 Errors in Configuration Files or Shell Scripts

When you apply a configuration file or run a shell script, the Zyxel Device processes the file line-by-line. The Zyxel Device checks the first line and applies the line if no errors are detected. Then it continues with the next line. If the Zyxel Device finds an error, it stops applying the configuration file or shell script and generates a log.

You can have the Zyxel Device to ignore errors and apply the valid parts of the configuration file every time you upload configuration files or only for the specific file you’re uploading.

Use `setenv stop-on-error off` if you want the Zyxel Device to ignore errors and apply the valid parts of the configuration file every time you upload configuration files to the Zyxel Device.

Use `apply/conf/`*`file_name`*`.conf ignore-error`, for example, `apply/conf/ATPConfigFile.conf ignore-error`, to:

- Apply the valid parts of the configuration file.
- Generate error logs for all of the configuration file’s errors.

This lets the Zyxel Device apply most of your configuration in the configuration file you just uploaded. You can refer to the logs for what to fix.

Use `apply/conf/`*`file_name`*`.conf ignore-error rollback`, for example, `apply/conf/ATPConfigFile.conf ignore-error rollback`, to:

- Generate error logs for all of the configuration file's errors.
- Start the Zyxel Device with the last fully valid configuration file.

This lets the Zyxel Device apply your current configuration file (the startup-config.conf file) instead of the configuration file you just uploaded. You can refer to the logs for what to fix.

See the table below for the comparison between these commands.

Table 318 Commands Comparison Table

COMMAND	EFFECTIVE	RESULT
`setenv stop-on-error off`	every time you upload configuration files (until you apply the command `setenv stop-on-error on`)	• ignore errors • apply the valid parts of the configuration file • generate error logs
`apply/conf/`*`file_name`*`.conf ignore-error`	only for the specific file	• ignore errors • apply the valid parts of the configuration file • generate error logs
`apply/conf/`*`file_name`*`.conf ignore-error rollback`	only for the specific file	• ignore errors • apply the startup-config.conf file • generate error logs

65.2.3 Zyxel Device Configuration File Details

You can store multiple configuration files on the Zyxel Device. You can also have the Zyxel Device use a different configuration file without the Zyxel Device restarting.

- When you first receive the Zyxel Device, it uses the system-default.conf configuration file of default settings.
- When you change the configuration, the Zyxel Device creates a startup-config.conf file of the current configuration.
- The Zyxel Device checks the startup-config.conf file for errors when it restarts. If there is an error in the startup-config.conf file, the Zyxel Device copies the startup-config.conf configuration file to the startup-config-bad.conf configuration file and tries the existing lastgood.conf configuration file.
- When the Zyxel Device reboots, if the startup-config.conf file passes the error check, the Zyxel Device keeps a copy of the startup-config.conf file as the lastgood.conf configuration file for you as a back up file. If you upload and apply a configuration file with an error, you can apply lastgood.conf to return to a valid configuration.

65.2.4 Configuration File Flow at Restart

If there is not a startup-config.conf when you restart the Zyxel Device (whether through a management interface or by physically turning the power off and back on), the Zyxel Device uses the system-default.conf configuration file with the Zyxel Device's default settings.

If there is a startup-config.conf, the Zyxel Device checks it for errors and applies it. If there are no errors, the Zyxel Device uses it and copies it to the lastgood.conf configuration file. If there is an error, the Zyxel Device generates a log and copies the startup-config.conf configuration file to the startup-config-bad.conf configuration file and tries the existing lastgood.conf configuration file. If there isn't a lastgood.conf configuration file or it also has an error, the Zyxel Device applies the system-default.conf configuration file.

You can change the way the startup-config.conf file is applied. Include the `setenv-startup stop-on-error off` command. The Zyxel Device ignores any errors in the startup-config.conf file and applies all of the valid commands. The Zyxel Device still generates a log for any errors.

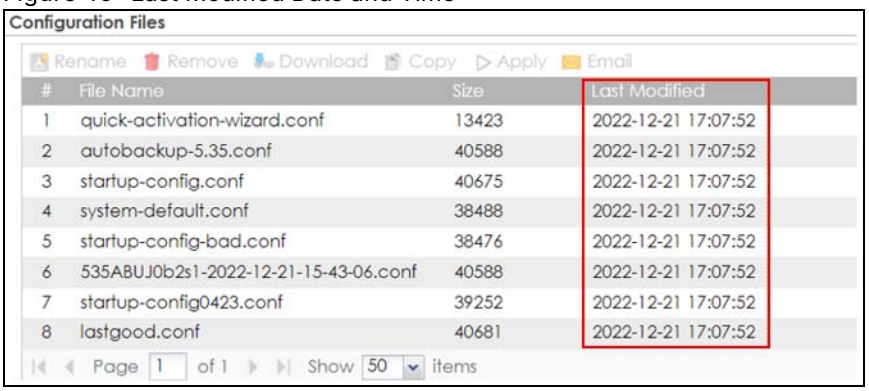
65.2.5 Sensitive Data Protection

The Zyxel Device by default encrypts local admin and user account passwords for web configurator and CLI.

Enable Sensitive Data Protection to better protect local admin and user account passwords for web configurator and CLI.

When you change the private key, the date and time shown in Maintenance > File Manager > Configuration File > Configuration > Last Modified for all configuration files will change to the date and time you changed the private key.

Figure 45 Last Modified Date and Time



Note: You can only upload configuration files using FTP that are using the current private key of the Zyxel Device.

The following examples describe the situations you might come across using Sensitive Data Protection.

Example 1:

1 Download a configuration file (file1).

2 Enable Sensitive Data Protection.

3 Create a private key (key1).

4 When you upload file1 to the Zyxel Device through the Zyxel Device web configurator, you do not need to enter the private key (key1). Configuration file1 is not encrypted by the private key (key1).

Example 2:

1 Enable Sensitive Data Protection.

2 Create a private key (key1).

3 Download a configuration file (file2).

4 You must use key1 to upload file2 to the Zyxel Device because file2 is encrypted by key1.

Example 3:

1 Change the private key from key1 to key2.

2 Download another configuration file (file3).

3 You must use key2 to upload file3 to the Zyxel Device.

Note: You must still use key1 to upload file2 to the Zyxel Device. Make a note of the key to use when you change the private key and then download a configuration file.

Example 4:

1 Enable Sensitive Data Protection on Zyxel Device1 and create a private key.

2 Download a configuration file from Zyxel Device1.

3 You must upload this configuration file using the private key you created on Zyxel Device1 to Zyxel Device2 even if Sensitive Data Protection is not enabled on Zyxel Device2.

65.3 File Manager Commands Input Values

The following table explains the values you can input with the file manager commands.

Table 319 File Manager Command Input Values

LABEL	DESCRIPTION
file_name	The name of a file. Use up to 25 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-).

65.4 File Manager Commands Summary

The following table lists the commands that you can use for file management.

Table 320 File Manager Commands Summary

COMMAND	DESCRIPTION
`apply /conf/file_name.conf [ignore-error] [rollback]`	Has the Zyxel Device use a specific configuration file. You must still use the `write` command to save your configuration changes to the flash (“non-volatile” or “long term”) memory. Use this command without specify both `ignore-error` and `rollback`: this is not recommended because it would leave the rest of the configuration blank. If the interfaces were not configured before the first error, the console port may be the only way to access the device. Use `ignore-error` without `rollback`: this applies the valid parts of the configuration file and generates error logs for all of the configuration file’s errors. This lets the Zyxel Device apply most of your configuration and you can refer to the logs for what to fix. Use both `ignore-error` and `rollback`: this applies the valid parts of the configuration file, generates error logs for all of the configuration file’s errors, and starts the Zyxel Device with a fully valid configuration file. Use `rollback` without `ignore-error`: this gets the Zyxel Device started with a fully valid configuration file as quickly as possible. You can use the “`apply /conf/system-default.conf`” command to reset the Zyxel Device to go back to its system defaults.
`[no] private-encryption-key <encryption-key>`	Enables sensitive data protection on the Zyxel Device and sets the encryption key. You need this key to upload configuration files. Write down the key you set and keep it in a safe place. Uses the no command to disable sensitive data protection.
`show private-encryption-key status`	Displays whether sensitive data protection is enabled on the Zyxel Device.
`copy {/conf | /idp | /packet_trace | /script | /tmp}file_name-a.conf {/conf | /idp | /packet_trace | /script | /tmp}/file_name-b.conf`	Saves a duplicate of a file on the Zyxel Device from the source file name to the target file name. Specify the directory and file name of the file that you want to copy and the directory and file name to use for the duplicate. Always copy the file into the same directory.
`copy running-config startup-config`	Saves your configuration changes to the flash (“non-volatile” or “long term”) memory. The Zyxel Device immediately uses configuration changes made via commands, but if you do not use this command or the write command, the changes will be lost when the Zyxel Device restarts.
`copy running-config /conf/file_name.conf`	Saves a duplicate of the configuration file that the Zyxel Device is currently using. You specify the file name to which to copy.
`delete {/conf | /idp | /packet_trace | /script | /tmp}/file_name`	Removes a file. Specify the directory and file name of the file that you want to delete.
`dir {/conf | /idp | /packet_trace | /script | /tmp}`	Displays the list of files saved in the specified directory.

Table 320 File Manager Commands Summary (continued)

COMMAND	DESCRIPTION
`rename {/conf | /idp | /packet_trace | /script | /tmp}/old-file_name {/conf | /idp | /packet_trace | /script | /tmp}/new-file_name`	Changes the name of a file. Specify the directory and file name of the file that you want to rename. Then specify the directory again followed by the new file name.
`rename /script/old-file_name /script/new-file_name`	Changes the name of a shell script.
`run /script/file_name.zysh`	Has the Zyxel Device execute a specific shell script file. You must still use the `write` command to save your configuration changes to the flash (“non-volatile” or “long term”) memory.
`schedule-run 1 file_name.zysh {daily | monthly | weekly} time {date | sun | mon | tue | wed | thu | fri | sat}`	Has the Zyxel Device execute the specified specific shell script file at the the specified time. You must still use the `write` command to save your configuration changes to the flash (“non-volatile” or “long term”) memory.
`show running-config`	Displays the settings of the configuration file that the system is using.
`setenv-startup stop-on-error off`	Has the Zyxel Device ignore any errors in the startup-config.conf file and apply all of the valid commands.
`show setenv-startup`	Displays whether or not the Zyxel Device is set to ignore any errors in the startup-config.conf file and apply all of the valid commands.
`write`	Saves your configuration changes to the flash (“non-volatile” or “long term”) memory. The Zyxel Device immediately uses configuration changes made via commands, but if you do not use the `write` command, the changes will be lost when the Zyxel Device restarts.

65.5 File Manager Dual Firmware Commands

The following table lists the commands that you can use for managing dual firmware. Firmware uploaded using FTP goes to the Running partition. Use the web configurator to upload firmware to the Standby partition. The Zyxel Device reboots automatically when you upload firmware to the Running partition.

Table 321 File Manager Dual Firmware Commands

COMMAND	DESCRIPTION
`set firmware boot option <0..1>`	Sets the behavior of the Zyxel Device when firmware is uploaded to the Standby partition. (This command does not upload firmware.) Use 0 to have the Zyxel Device reboot immediately after firmware is uploaded to the Standby partition and become the Running firmware. Use 1 to not have the Zyxel Device reboot immediately after a firmware is uploaded to the Standby partition.
`show firmware image boot option`	Shows the behavior of the Zyxel Device when firmware is uploaded to the Standby partition.
`set firmware boot number <1..2>`	Reboots the Zyxel Device immediately with firmware in partition 1 or 2. If 2 is the Standby partition, then it becomes the Running partition after reboot. Use `show version` to see which partition is Standby and which is Running.

65.6 File Manager Command Examples

These are examples of the dual firmware commands .

```
Router(config)# set firmware boot option 0
Router(config)#
Router(config)# show firmware image boot option
boot option: 0
Router(config)#
Router(config)# set firmware boot number 2

Welcome to USG110

Username:
Terminate All Processes: OK
kill_process_and_umountfs() returns -7
Restarting system.

<snipped>

Welcome to USG110
Username: admin
Password:
Router> configure terminal
Router(config)# show version
Zyxel Communications Corp.
image number model                  firmware version
build date           boot status
================================================================================
1        USG110                  V4.11(AAPH.0)b3s1
2015-01-11 21:53:44  Standby
2        USG110                   V4.11(AAPH.0)
2015-03-13 03:47:52  Running
```

This example saves a back up of the current configuration before applying a shell script file.

```
Router(config)# copy running-config /conf/backup.conf
Router(config)# run /script/vpn_setup.zysh
```

These commands run the aaa.zysh script at noon every day, on the first day of every month, and on every Monday, Wednesday, and Friday.

```
Router> configure terminal
Router(config)# schedule-run 1 aaa.zysh daily 12:00
Router(config)# schedule-run 1 aaa.zysh monthly 12:00 01
Router(config)# schedule-run 1 aaa.zysh weekly 12:00 mon wed fri
Router(config)#
```

65.7 FTP File Transfer

You can use FTP to transfer files to and from the Zyxel Device for advanced maintenance and support.

65.7.1 Command Line FTP File Upload

1. Connect to the Zyxel Device.
2. Enter “bin” to set the transfer mode to binary.
3. You can upload the firmware after you log in through FTP. To upload other files, use “cd” to change to the corresponding directory.
4. Use “put” to transfer files from the computer to the Zyxel Device.[1] For example:

   In the conf directory, use "put config.conf today.conf” to upload the configuration file (config.conf) to the Zyxel Device and rename it “today.conf”.

   "put 1.00(XL.0).bin” transfers the firmware (1.00(XL.0).bin) to the Zyxel Device.

   The firmware update can take up to five minutes. Do not turn off or reset the Zyxel Device while the firmware update is in progress! If you lose power during the firmware upload, you may need to refer to Section 65.10 on page 555 to recover the firmware.

65.7.2 Command Line FTP Configuration File Upload Example

The following example transfers a configuration file named tomorrow.conf from the computer and saves it on the Zyxel Device as next.conf.

Note: Uploading a custom signature file named "custom.rules”, overwrites all custom signatures on the ZyWALL.

1. When you upload a custom signature, the Zyxel Device appends it to the existing custom signatures stored in the "custom.rules” file.

Figure 46 FTP Configuration File Upload Example

```
C:\>ftp 192.168.1.1
Connected to 192.168.1.1.
220 FTP Server (ZyWALL) [192.168.1.1]
User (192.168.1.1:(none)): admin
331 Password required for admin.
Password:
230 User admin logged in.
ftp> cd conf
250 CWD command successful
ftp> bin
200 Type set to I
ftp> put tomorrow.conf next.conf
200 PORT command successful
150 Opening BINARY mode data connection for next.conf
226-Post action ok!!
226 Transfer complete.
ftp: 20231 bytes sent in 0.00Seconds 20231000.00Kbytes/sec.
```

65.7.3 Command Line FTP File Download

1. Connect to the Zyxel Device.
2. Enter “bin” to set the transfer mode to binary.
3. Use “cd” to change to the directory that contains the files you want to download.
4. Use “dir” or “ls” if you need to display a list of the files in the directory.
5. Use "get” to download files. For example:

   “get vpn_setup.zysh vpn.zysh” transfers the vpn_setup.zysh configuration file on the Zyxel Device to your computer and renames it “vpn.zysh.”

65.7.4 Command Line FTP Configuration File Download Example

The following example gets a configuration file named today.conf from the Zyxel Device and saves it on the computer as current.conf.

Figure 47 FTP Configuration File Download Example

```
C:\>ftp 192.168.1.1
Connected to 192.168.1.1.
220 FTP Server (ZyWALL) [192.168.1.1]
User (192.168.1.1:(none)): admin
331 Password required for admin.
Password:
230 User admin logged in.
ftp> bin
200 Type set to I
ftp> cd conf
250 CWD command successful
ftp> get today.conf current.conf
200 PORT command successful
150 Opening BINARY mode data connection for conf/today.conf
(20220 bytes)
226 Transfer complete.
ftp: 20220 bytes received in 0.03Seconds 652.26Kbytes/sec.
```

65.8 Cloud Helper Commands

Cloud Helper lets you know if there is a later firmware available on the Cloud Helper server and lets you download it one is available.

Note: To use this feature, you must register your Zyxel Device at myZyxel.com.

Table 322 Cloud Helper Commands

COMMAND	DESCRIPTION
`show cloud-helper autoupdate firmware`	Shows if automatically updating firmware is enabled, the schedule and if automatically rebooting the Zyxel Device is enabled (meaning the uploaded firmware becomes the running firmware.
`show cloud-helper firmware`	Displays latest firmware information available on the Cloud Helper server.
`show cloud-helper highlight`	Displays the number of unread notifications.
`show cloud-helper notify_all`	Displays all notifications on the Zyxel Device, including the name, description, and URL.
`show cloud-helper remind`	Displays whether the popup reminder about new available firmware is enabled or disabled.
`show cloud-helper retry`	Shows the number of retry_times, retry_period and retry_fail_period. `retry_times`: The number of attempts allowed to download items. `retry_period`: The length of time between download attempts. `retry_fail_period`: The retry interval after retry attempts have expired.
`cloud-helper check all`	Sends a query to the Cloud Helper Server to get the latest firmware, Geo IP, IDP signature and SSL CA certificate information.
`cloud-helper check app`	Sends a query to the Cloud Helper Server to get the latest App Patrol signature information.
`cloud-helper check app_incr`	Sends a query to the Cloud Helper Server to get the latest incremental App Patrol signature information.

Table 322 Cloud Helper Commands (continued)

COMMAND	DESCRIPTION
`cloud-helper check av`	Sends a query to the Cloud Helper Server to get the latest Antivirus signature information.
`cloud-helper check botnet`	Sends a query to the Cloud Helper Server to get the latest URL Threat Filter signature information.
`cloud-helper check ctdb`	Sends a query to the Cloud Helper Server to get the latest Content Filter signature information.
`cloud-helper check firmware`	Sends a query to the Cloud Helper Server to get the latest firmware information.
`cloud-helper check geoip`	Sends a query to the Cloud Helper Server to get the latest Geo IP information.
`cloud-helper check idp`	Sends a query to the Cloud Helper Server to get the latest IDP signature information.
`cloud-helper check rf`	Sends a query to the Cloud Helper Server to get the latest Reputation Filter signature information.
`cloud-helper check sslca`	Sends a query to the Cloud Helper Server to get the latest SSL CA certificate information.
`cloud-helper check-notify new_features_cdr`	Checks for new notifications relating to CDR.
`cloud-helper check-notify new_features_dns_cf`	Checks for new notifications relating to DNS Content Filtering.
`cloud-helper check-notify new_features_rap`	Checks for new notifications relating to Remote Access Points (RAP).
`cloud-helper check-notify now`	Checks for all new notifications.
`cloud-helper check-notify service_expired`	Checks for new notifications relating to relating to services that are expired on the Zyxel Device.
`cloud-helper check-notify whats_new`	Checks for new notifications relating to Remote Access Points (RAP).
`cloud-helper clean-download firmware`	Stops and removes a firmware being downloaded to the Zyxel Device.
`[no] cloud-helper firmware update auto`	Lets the Zyxel Device automatically check for and download new firmware to the standby partition at the time and day specified. The no command disallows the Zyxel Device automatically checking for and downloading new firmware.
`cloud-helper firmware update daily <0..23> reboot {no | yes}`	Has the Zyxel Device check for new firmware every day at the specified time. The time format is the 24 hour clock, so '0' means midnight, 01 means 1AM and so on. Configure `reboot yes` to have the Zyxel Device automatically restart making the newly downloaded firmware in the standby partition become the running firmware.
`cloud-helper firmware update weekly {fri | mon | sat | sun | thu | tue | wed} <0..23> reboot {no | yes}`	Has the Zyxel Device check for new firmware once a week on the day and at the time specified. Configure `reboot yes` to have the Zyxel Device automatically restart making the newly downloaded firmware in the standby partition become the running firmware. If you configure both weekly and daily commands, then the command that takes effect is the last one configured.
`cloud-helper get app`	Downloads the latest App Patrol signatures from the Cloud Helper server to the Zyxel Device.

Table 322 Cloud Helper Commands (continued)

COMMAND	DESCRIPTION
`cloud-helper get av`	Downloads the latest Antivirus signatures from the Cloud Helper server to the Zyxel Device.
`cloud-helper get botnet`	Downloads the latest URL Threat Filter signatures from the Cloud Helper server to the Zyxel Device.
`cloud-helper get firmware <1..2>`	Downloads the latest firmware on the Cloud Helper server to the specified system space on the Zyxel Device.
`cloud-helper get idp`	Downloads the latest IDP signature on the Cloud Helper server to the Zyxel Device.
`cloud-helper get sslca`	Downloads the latest SSL certificate on the Cloud Helper server to the Zyxel Device.
`cloud-helper pause-download firmware <1..2>`	Temporarily stops a firmware being downloaded to the specified system space on the Zyxel Device.
`cloud-helper set {[retry_times <1..10>]} {[retry_period <2..60>]} {[retry_fail_period <180..720>]}`	Specifies criteria for how the Zyxel Device should download firmware, security service signatures, and SSL certificates from the Cloud Helper server. `retry_times:` Up to 10 attempts are allowed to download items. `retry_period:` The retry interval must be between 2 and 60 seconds. `retry_fail_period:` The retry interval after retry attempts have expired must be between 180 and 720 seconds.
`cloud-helper set remind {every-time | never}`	Enables or disables a notificaton that appears when logging in, reminding the Zyxel Device admin that new firmware is available.
`cloud-helper set-read new_features_cdr`	Marks all CDR notifications as read.
`cloud-helper set-read new_features_dns_cf`	Marks all DNS Content Filter notifications as read.
`cloud-helper set-read service_expired`	Marks all Service Expired notifications as read.
`cloud-helper set-read whats_new`	Marks all What's New notifications as read.
`cloud-helper update firmware <1..2>`	Resumes a firmware being downloaded to the specified system space on the Zyxel Device.
`[no] cloud-helper-notify activate`	Enables the Cloud Helper notifications service, which checks for new new, app updates, and firmware updates. The `no` command disables the service and hides notifications.

65.8.1 Cloud Helper Command Examples

These are examples of Cloud Helper commands.

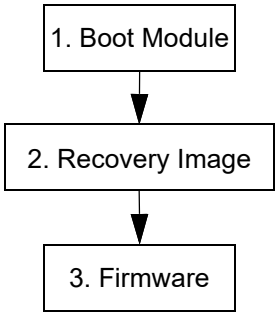
```
Router(config)#
Router(config)# cloud-helper check firmware
================================================================================
Cloud status      : NORMAL
firmware version  : 4.20(AAPL.0)b5
firmware release  : 2016-07-15T02:29:11Z
firmware md5      : 752ed3f2d8296e669ea2146c29523bda
firmware news file: YES
firmware note file: YES
firmware message file: NO
boot status       : Running
================================================================================
Cloud status      : NORMAL
firmware version  : 4.20(AAPL.0)b5
firmware release  : 2016-07-15T02:29:11Z
firmware md5      : 752ed3f2d8296e669ea2146c29523bda
firmware news file: YES
firmware note file: YES
firmware message file: NO
boot status       : Standby
Router(config)#
```

```
Router(config)#
Router# show cloud-helper autoupdate firmware
auto: no
schedule: daily at 18 o'clock
autoreboot: no
Router(config)# cloud-helper set retry_times 5 retry_period 6 retry_fail_period 200
Router# show cloud-helper retry
retry_times: 5
retry_period: 6 min
retry_fail_period: 200 min
Router(config)#
Router# show cloud-helper firmware
WARNING: can not get fw fw_md5 info
================================================================================
Cloud status      : NORMAL
firmware version  : 4.20(AAKZ.2)
firmware release  : 2016-11-29T01:42:39Z
firmware md5      :
firmware news file: YES
firmware note file: YES
firmware message file: YES
boot status       : Running
WARNING: can not get fw fw_md5 info
================================================================================
Cloud status      : NORMAL
firmware version  : 4.20(AAKZ.2)
firmware release  : 2016-11-29T01:42:39Z
firmware md5      :
firmware news file: YES
firmware note file: YES
firmware message file: YES
boot status       : Standby
Router(config)#
```

65.9 Zyxel Device File Usage at Startup

The Zyxel Device uses the following files at system startup.

Figure 48 Zyxel Device File Usage at Startup



1 The boot module performs a basic hardware test. You cannot restore the boot module if it is damaged. The boot module also checks and loads the recovery image. The Zyxel Device notifies you if the recovery image is damaged.

2 The recovery image checks and loads the firmware. The Zyxel Device notifies you if the firmware is damaged.

65.10 Notification of a Damaged Recovery Image or Firmware

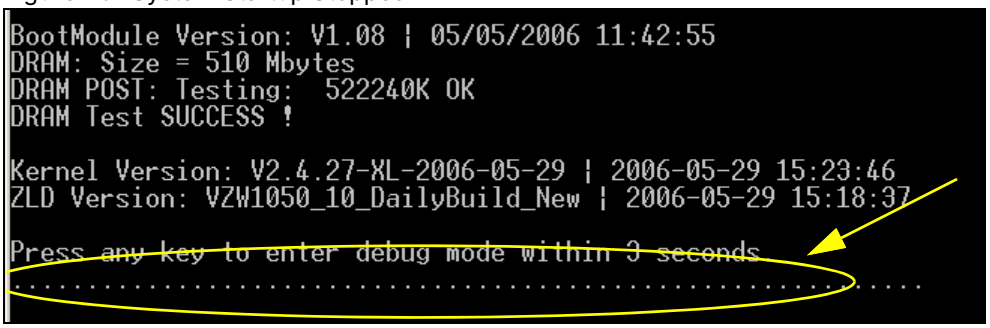
The Zyxel Device's recovery image and/or firmware could be damaged, for example by the power going off during a firmware upgrade. This section describes how the Zyxel Device notifies you of a damaged recovery image or firmware file. Use this section if your device has stopped responding for an extended period of time and you cannot access or ping it. Note that the Zyxel Device does not respond while starting up. It takes less than five minutes to start up with the default configuration, but the start up time increases with the complexity of your configuration.

1 Use a console cable and connect to the Zyxel Device via a terminal emulation program (such as HyperTerminal). Your console session displays the Zyxel Device's startup messages. If you cannot see any messages, check the terminal emulation program's settings (see Section 1.2.1 on page 28) and restart the Zyxel Device.

2 The system startup messages display followed by "Press any key to enter debug mode within 3 seconds."

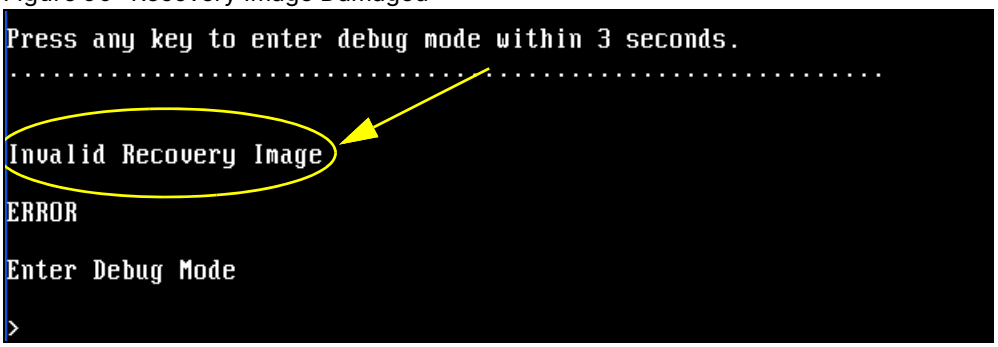
Note: Do not press any keys at this point. Wait to see what displays next.

Figure 49 System Startup Stopped



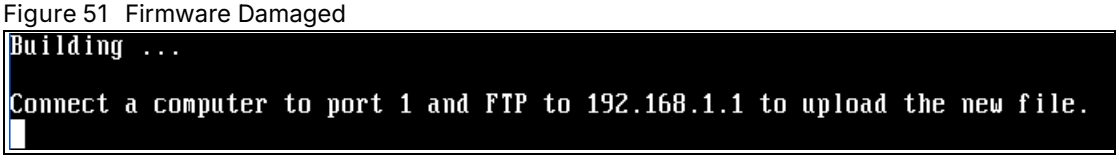
3 If the console session displays "Invalid Firmware", or "Invalid Recovery Image", or the console freezes at "Press any key to enter debug mode within 3 seconds" for more than one minute, go to Section 65.11 on page 556 to restore the recovery image.

Figure 50 Recovery Image Damaged



4 If "Connect a computer to port 1 and FTP to 192.168.1.1 to upload the new file" displays on the screen, the firmware file is damaged. Use the procedure in Section 65.12 on page 558 to restore it. If the message does not display, the firmware is OK and you do not need to use the firmware recovery procedure.

Figure 51 Firmware Damaged



65.11 Restoring the Recovery Image

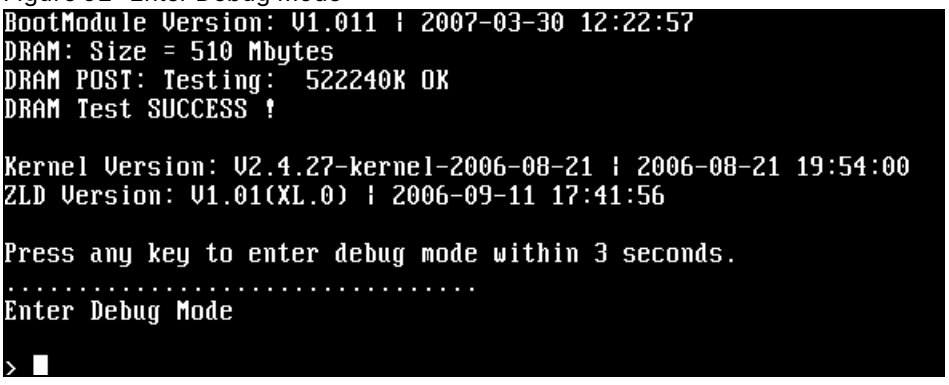
This procedure requires the Zyxel Device's recovery image. Download the firmware package from www.zyxel.com and unzip it. The recovery image uses a .ri extension, for example, "1.01(XL.0)C0.ri". Do the following after you have obtained the recovery image file.

Note: You only need to use this section if you need to restore the recovery image.

1 Restart the Zyxel Device.

2 When "Press any key to enter debug mode within 3 seconds." displays, press a key to enter debug mode.

Figure 52 Enter Debug Mode



3 Enter `atuk` to initialize the recovery process. If the screen displays "ERROR", enter `atur` to initialize the recovery process.

Note: You only need to use the `atuk` or `atur` command if the recovery image is damaged.

Figure 53 atuk Command for Restoring the Recovery Image

```
> atuk
This command is for restoring the "recovery image" (xxx.ri).
Use This command only when
1) the console displays "Invalid Recovery Image" or
2) the console freezes at "Press any key to enter debug mode within 3 seconds"
   for more than one minute.

Note:
Please exit this command immediately if you do not need to restore the
"recovery image".

Do you want to start the recovery process (Y/N)? (default N)
```

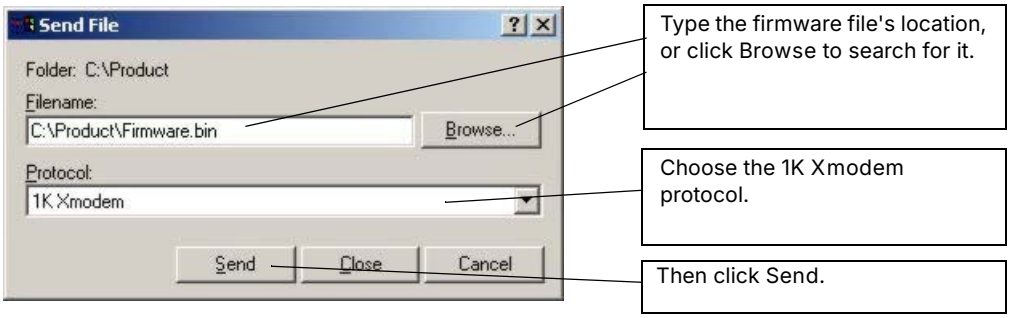
4 Enter `Y` and wait for the "Starting XMODEM upload" message before activating XMODEM upload on your terminal.

Figure 54 Starting Xmodem Upload

```
Do you want to start the recovery process (Y/N)? (default N)
Starting XMODEM upload (CRC mode)....
C
```

5 This is an example Xmodem configuration upload using HyperTerminal. Click Transfer, then Send File to display the following screen.

Figure 55 Example Xmodem Upload



6 Wait for about three and a half minutes for the Xmodem upload to finish.

Figure 56 Recovery Image Upload Complete

```
Total  1867264 bytes received.
programming ..................................................
..............................................................
..............................................................
..............................................................
..............................................................
..............................................................

OK


> 
```

7 Enter `atgo`. The Zyxel Device starts up. If "Connect a computer to port 1 and FTP to 192.168.1.1 to upload the new file" displays on the screen, the firmware file is damaged and you need to use the procedure in Section 65.12 on page 558 to recover the firmware.

Figure 57 atgo Debug Command

```
> atgo
Booting...
```

65.12 Restoring the Firmware

This procedure requires the Zyxel Device's firmware. Download the firmware package from www.zyxel.com and unzip it. The firmware file uses a .bin extension, for example, "1.01(XL.0)C0.bin". Do the following after you have obtained the firmware file.

Note: This section is not for normal firmware uploads. You only need to use this section if you need to recover the firmware.

1 Connect your computer to the Zyxel Device's port 1 (only port 1 can be used).

2 The Zyxel Device's FTP server IP address for firmware recovery is 192.168.1.1, so set your computer to use a static IP address from 192.168.1.2 ~192.168.1.254.

3 Use an FTP client on your computer to connect to the Zyxel Device. For example, in the Windows command prompt, type `ftp 192.168.1.1`. Keep the console session connected in order to see when the firmware recovery finishes.

4 Hit enter to log in anonymously.

5 Set the transfer mode to binary (type `bin`).

6 Transfer the firmware file from your computer to the Zyxel Device. Type `put` followed by the path and name of the firmware file. This examples uses `put e:\ftproot\ZLD FW \1.01(XL.0)C0.bin`.

Figure 58 FTP Firmware Transfer Command

```
C:\>ftp 192.168.1.1
Connected to 192.168.1.1.
220-=(<*>)=-.:. (( Welcome to PureFTPd 1.0.11 )) .:.-=(<*>)=-
220-You are user number 1 of 50 allowed
220-Local time is now 21:33 and the load is 0.01. Server port: 21.
220-Only anonymous FTP is allowed here
220 You will be disconnected after 15 minutes of inactivity.
User (192.168.1.1:(none)):
230 Anonymous user logged in
ftp> bi
200 TYPE is now 8-bit binary
ftp> put E:\ftproot\ZLD_FW\100XL0c0\1.00(XL.0)C0.bin_
```

7 Wait for the file transfer to complete.

Figure 59 FTP Firmware Transfer Complete

```
200 PORT command successful
150 Connecting to port 1564
226-87.0 Mbytes free disk space
226-File successfully transferred
226 3.231 seconds (measured here), 10.83 Mbytes per second
ftp: 36708858 bytes sent in 3.23Seconds 11350.91Kbytes/sec.
ftp> _
```

8 After the transfer is complete, “Firmware received” or “ZLD-current received” displays. Wait (up to four minutes) while the Zyxel Device recovers the firmware.

Figure 60 Firmware Received and Recovery Started

```
Firmware received ...

[Update Filesystem]
       Updating Code
       ..
```

9 The console session displays “done” when the firmware recovery is complete. Then the Zyxel Device automatically restarts.

Figure 61 Firmware Recovery Complete and Restart

```
.....
.....
.....
.....
.....
.....
.....
       done

[Update Kernel]
       Extracting Kernel Image
       ..
       done
       Writing Kernel Image ... done

[Update BootModule]
       Extracting BootModule Image
       .
       done
       Writing BootModule
       .....
.....                                  done
Restarting system.
```

10 The username prompt displays after the Zyxel Device starts up successfully. The firmware recovery process is now complete and the Zyxel Device is ready to use.

Figure 62 Restart Complete

```
Setting the System Clock using the Hardware Clock as reference...
System Clock set. Local time: Sun Jan 26 21:40:24 UTC 2003

Cleaning: /tmp /var/lock /var/run.
Initializing random number generator... done.
Initializing Debug Account Authentication Seed (DAAS)... done.
Lionic device init successfully
cavium nitrox device CN1005 init complete
INIT: Entering runlevel: 3
Starting zylog daemon: zylogd zylog starts.
Starting syslog-ng.
Starting uam daemon.
Starting app patrol daemon.
Starting periodic command scheduler: cron.
Start ZyWALL system daemon....
Got LINK_CHANGE
Port [0] is up --> Group [0] is up
Applying system configuration file, please wait...
ZyWALL system is configured successfully with startup-config.conf

Welcome to ZyWALL 1050

Username:
```

65.13 Restoring the Default System Database

The default system database stores information such as the default anti-virus or IDP signatures. The Zyxel Device can still operate if the default system database is damaged or missing, but related features (like anti-virus or IDP) may not function properly.

If the default system database file is not valid, the Zyxel Device displays a warning message in your console session at startup or when reloading the anti-virus or IDP signatures. It also generates a log. Here are some examples. Use this section to restore the Zyxel Device's default system database.

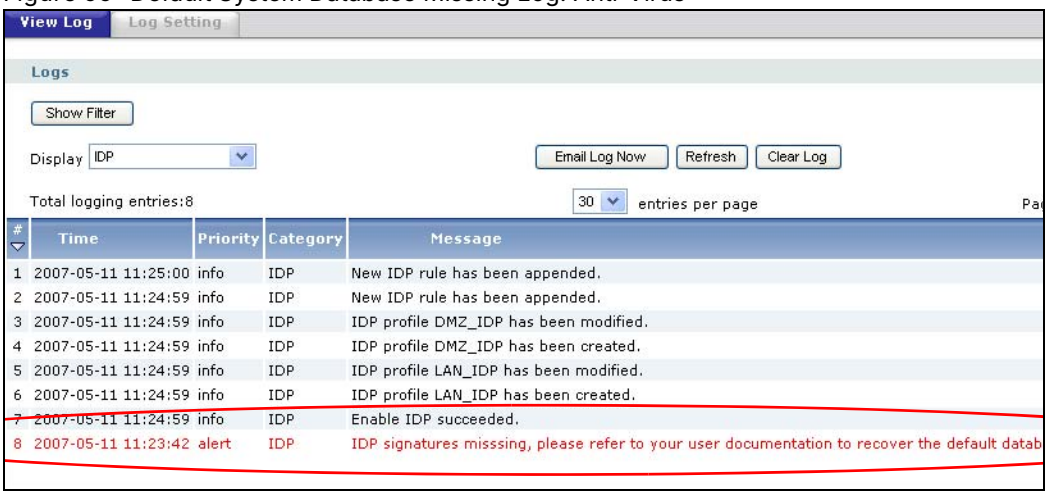
Figure 63 Default System Database Console Session Warning at Startup: Anti-Virus

```
Hostname: localhost.

Setting the System Clock using the Hardware Clock as reference...
System Clock set. Local time: Fri May 11 09:31:55 GMT 2007

Cleaning: /tmp /var/lock /var/run.
Initializing random number generator... done.
Initializing Debug Account Authentication Seed (DAAS)... done.
INIT: Entering runlevel: 3
Starting zylog daemon: zylogd zylog starts.
Starting syslog-ng.
Starting uam daemon.
Starting app patrol daemon.
Starting periodic command scheduler: cron.
Start ZyWALL system daemon....
Got LINK_CHANGE
Port [1] is up --> Group [1] is up
% Anti-Virus signatures misssing, refer to your user documentation to recover th
e default database file.
% Loading AV signature database has failed.
Applying system configuration file, please wait...
ZyWALL system is configured successfully with startup-config.conf

Welcome to ZyWALL USG 300

Username:
```

Figure 64 Default System Database Console Session Warning When Reloading IDP

```
Router(config)# idp reload
IDP signatures misssing, please refer to your user documentation to recover the
default database file.
retval = -32056
ERROR: Enable IDP engine failed.
Router(config)#
```

Figure 65 Default System Database Missing Log: Anti-Virus



This procedure requires the Zyxel Device's default system database file. Download the firmware package from www.zyxel.com and unzip it. The default system database file uses a .db extension, for example, "1.01(XL.0)C0.db". Do the following after you have obtained the default system database file.

65.13.1 Using the atkz -u Debug Command

Note: You only need to use the `atkz -u` command if the default system database is damaged.

1 Restart the Zyxel Device.

2 When "Press any key to enter debug mode within 3 seconds." displays, press a key to enter debug mode.

Figure 66 Enter Debug Mode

```
BootModule Version: V1.011 | 2007-03-30 12:22:57
DRAM: Size = 510 Mbytes
DRAM POST: Testing:  522240K OK
DRAM Test SUCCESS !

Kernel Version: V2.4.27-kernel-2006-08-21 | 2006-08-21 19:54:00
ZLD Version: V1.01(XL.0) | 2006-09-11 17:41:56

Press any key to enter debug mode within 3 seconds.
.............................
Enter Debug Mode

>
```

3 Enter `atkz -u` to start the recovery process.

Figure 67 atkz -u Command for Restoring the Default System Database

```
> atkz -u
-u
OK

> atgo
Booting...
```

4 "Connect a computer to port 1 and FTP to 192.168.1.1 to upload the new file" displays on the screen. Connect your computer to the Zyxel Device's port 1 (only port 1 can be used).

Figure 68 Use FTP with Port 1 and IP 192.168.1.1 to Upload File

```
Checking CODE ... Done

Updating ...

Connect a computer to port 1 and FTP to 192.168.1.1 to upload the new file.
```

5 The Zyxel Device's FTP server IP address for firmware recovery is 192.168.1.1, so set your computer to use a static IP address from 192.168.1.2 ~192.168.1.254.

6 Use an FTP client on your computer to connect to the Zyxel Device. For example, in the Windows command prompt, type `ftp 192.168.1.1`. Keep the console session connected in order to see when the default system database recovery finishes.

7 Hit enter to log in anonymously.

8 Set the transfer mode to binary (type `bin`).

9 Transfer the firmware file from your computer to the Zyxel Device. Type `put` followed by the path and name of the firmware file. This examples uses `put e:\ftproot\ZLD FW \1.01(XL.0)C0.db`.

Figure 69 FTP Default System Database Transfer Command

```
C:\>ftp 192.168.1.1
Connected to 192.168.1.1.
220-=(<*>)=-.:. (( Welcome to PureFTPd 1.0.11 )) .:.-=(<*>)=-
220-You are user number 1 of 50 allowed
220-Local time is now 03:56 and the load is 0.00. Server port: 21.
220-Only anonymous FTP is allowed here
220 You will be disconnected after 15 minutes of inactivity.
User (192.168.1.1:(none)):
230 Anonymous user logged in
ftp> bin
200 TYPE is now 8-bit binary
ftp> put E:\ftproot\ZLD_FW\101XL\101XL0C0\1.01(XL.0)C0.db
```

10 Wait for the file transfer to complete.

Figure 70 FTP Default System Database Transfer Complete

```
200 PORT command successful
150 Connecting to port 3709
226-248.5 Mbytes free disk space
226-File successfully transferred
226 0.008 seconds (measured here), 13.31 Mbytes per second
ftp: 112398 bytes sent in 0.02Seconds 7024.88Kbytes/sec.
ftp> _
```

11 The console session displays “done” after the default system database is recovered.

Figure 71 Default System Database Received and Recovery Complete

```
Default System Database received ...

[Update Filesystem]
        Updating Database
        .
        done
```

12 The username prompt displays after the Zyxel Device starts up successfully. The default system database recovery process is now complete and the Zyxel Device IDP and anti-virus features are ready to use again.

Figure 72 Startup Complete

```
nothing was mounted
Hostname: localhost.

Setting the System Clock using the Hardware Clock as reference...
System Clock set. Local time: Wed May  9 03:26:53 UTC 2007

Cleaning: /tmp /var/lock /var/run.
Initializing random number generator... done.
Initializing Debug Account Authentication Seed (DAAS)... done.
Lionic device init successfully
cavium nitrox device CN505 init complete
INIT: Entering runlevel: 3
Starting zylog daemon: zylogd zylog starts.
Starting syslog-ng.
Starting uam daemon.
Starting app patrol daemon.
Starting periodic command scheduler: cron.
Start ZyWALL system daemon....
Got LINK_CHANGE
Port [1] is up --> Group [1] is up
Got LINK_CHANGE
Port [0] is up --> Group [0] is up
Applying system configuration file, please wait...
ZyWALL system is configured successfully with startup-config.conf

Welcome to ZyWALL 1050

Username:
```

CHAPTER 66
Logs

66.1 Log Commands Summary

This chapter provides information about the Zyxel Device's logs.

Note: When the system log reaches the maximum number of log messages, new log messages automatically overwrite existing log messages, starting with the oldest existing log message first.

See the User's Guide for the maximum number of system log messages in the Zyxel Device.

The following table describes the values required for many log commands. Other values are discussed with the corresponding commands.

Table 323 Input Values for Log Commands

LABEL	DESCRIPTION
interface_name	The name of the interface. Ethernet interface: For some Zyxel Device models, use ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your Zyxel Device model. For othere Zyxel Device models, use a name such as wan1, wan2, opt, lan1, or dmz. Virtual interface on top of Ethernet interface: add a colon (:) and the number of the virtual interface. For example: ge*x*:*y*, *x* = 1 - N, *y* = 1 - 4 VLAN interface: vlan*x*, *x* = 0 - 4094 Virtual interface on top of VLAN interface: vlan*x*:*y*, *x* = 0 - 4094, *y* = 1 - 12 Bridge interface: br*x*, *x* = 0 - N, where N depends on the number of bridge interfaces your Zyxel Device model supports. Virtual interface on top of bridge interface: br*x*:*y*, *x* = the number of the bridge interface, *y* = 1 - 4 PPPoE/PPTP interface: ppp*x*, *x* = 0 - N, where N depends on the number of PPPoE/PPTP interfaces your Zyxel Device model supports.
module_name	The name of the category; `kernel`, `syslog`, ... The `default` category includes debugging messages generated by open source software. The `all` category includes all messages in all categories. To view a list of categories, run command show logging status system-log.
protocol	The name of a protocol such as TCP, UDP, ICMP.

The following sections list the logging commands.

66.1.1 Log Entries Commands

This table lists the commands to look at log entries.

Table 324 logging Commands: Log Entries

COMMAND	DESCRIPTION
`show logging entries [priority pri] [category module_name] [srcip ip] [srcip6 ipv6_addr] [dstip ip] [dstip6 ipv6_addr] [service service_name] [begin <1..512> end <1..512>] [keyword keyword] [srciface interface_name] [dstiface interface_name] [protocol protocol]`	Displays the specified entries in the system log. *pri*: alert | crit | debug | emerg | error | info | notice | warn *keyword*: You can use alphanumeric and ( )+/:=?!*#@$_%- characters, and it can be up to 63 characters long. This searches the message, source, destination, and notes fields.
`show logging entries field field [begin <1..512> end <1..512>]`	Displays the specified fields in the system log. *field*: time | msg | src | dst | note | pri | cat | all

66.1.2 System Log Commands

This table lists the commands for the system log settings.

Table 325 logging Commands: System Log Settings

COMMAND	DESCRIPTION
`show logging status system-log`	Displays the current settings for the system log.
`logging system-log category module_name {disable | level normal | level all}`	Specifies what kind of information, if any, is logged in the system log and debugging log for the specified category.
`[no] logging system-log suppression interval <10..600>`	Sets the log consolidation interval for the system log. The no command sets the interval to ten.
`[no] logging system-log suppression`	Enables log consolidation in the system log. The no command disables log consolidation in the system log.
`[no] logging cef-format include year`	Includes the year in the `cef` (Common Event Format) syslog-compatible format.
`[no] connectivity-check continuous-log activate`	Has the Zyxel Device generate a log for each connectivity check. The no command has the Zyxel Device only log the first connectivity check.
`show connectivity-check continuous-log status`	Displays whether or not the Zyxel Device generates a log for each connectivity check.
`clear logging system-log buffer`	Clears the system log.
`[no] logging usb-storage`	Saves the sytem logs to a USB storage device, if one is connected. The `[no]` command disables this feature.
`logging usb-storage category module_name level {all | normal}`	Specifies what kind of information, if any, is logged to the USB storage device for the specified category.
`logging usb-storage delete over-keep-duration`	Deletes all log messages stored on the USB that are older than `keep-duration`.
`logging usb-storage flushThreshold <1..100>`	Sets how many new log messages must be created on the Zyxel Device before the new messages are written to the USB storage device.

Table 325 logging Commands: System Log Settings (continued)

COMMAND	DESCRIPTION
`[no] logging usb-storage keep-duration`	Sets a limit on how long log files are stored on the USB storage device, before being automatically deleted. This helps prevent the storage device from running out of space. The `[no]` command removes the limit, meaning log files are stored forever.
`logging usb-storage keep-duration day <1..365>`	Sets how long, in days, that log files are kept on the USB storage device before being automatically deleted.

66.1.2.1 System Log Command Examples

The following command displays the current status of the system log.

```
Router# configure terminal
Router(config)# show logging status system-log
512 events logged
suppression active  : yes
suppression interval: 10
category settings   :
    content-filter    : normal , forward-web-sites : no     ,
    blocked-web-sites : normal , user              : normal ,
    myZyxel.com       : normal , zysh              : normal ,
    idp               : normal , app-patrol        : normal ,
    ike               : normal , ipsec             : normal ,
    firewall          : normal , sessions-limit    : normal ,
    policy-route      : normal , built-in-service  : normal ,
    system            : normal , connectivity-check: normal ,
    device-ha         : normal , routing-protocol  : normal ,
    nat               : normal , pki               : normal ,
    interface         : normal , interface-statistics: no     ,
    account           : normal , port-grouping     : normal ,
    force-auth        : normal , l2tp-over-ipsec   : normal ,
    anti-virus        : normal , white-list        : normal ,
    black-list        : normal , ssl-vpn           : normal ,
    cnm               : normal , traffic-log       : no     ,
    file-manage       : normal , dial-in           : normal ,
    adp               : normal , default           : all    ,
```

66.1.3 Debug Log Commands

This table lists the commands for the debug log settings.

Table 326 logging Commands: Debug Log Settings

COMMAND	DESCRIPTION
`show logging debug status`	Displays the current settings for the debug log.
`show logging debug entries [priority pri] [category module_name] [srcip ip] [srcip6 ipv6_addr] [dstip ip] [dstip6 ipv6_addr] [service service_name] [srciface interface_name] [dstiface interface_name] [protocol protocol] [begin <1..512> end <1..512>] [keyword keyword]`	Displays the specified entries in the system log. *pri*: alert | crit | debug | emerg | error | info | notice | warn *keyword*: You can use alphanumeric and `()+/:=?!*#@$_%-` characters, and it can be up to 63 characters long. This searches the message, source, destination, and notes fields.

Table 326 logging Commands: Debug Log Settings (continued)

COMMAND	DESCRIPTION
`show logging debug entries field *field* [begin <1..1024> end <1..1024>]`	Displays the specified field in the debug log. *field*: time | msg | src | dst | note | pri | cat | all
`[no] logging debug suppression`	Enables log consolidation in the debug log. The no command disables log consolidation in the debug log.
`[no] logging debug suppression interval <10..600>`	Sets the log consolidation interval for the debug log. The no command sets the interval to ten.
`clear logging debug buffer`	Clears the debug log.

This table lists the commands for the remote syslog server settings. For the purposes of this device's CLI, Access Points are referred to as WTPs.

Table 327 logging Commands: Remote Syslog Server Settings

COMMAND	DESCRIPTION
`show logging status syslog`	Displays the current settings for the remote servers.
`[no] logging syslog <1..4>`	Enables the specified remote server. The no command disables the specified remote server.
`[no] logging syslog <1..4> address {*ip* | *hostname*}`	Sets the URL or IP address of the specified remote server. The no command clears this field. *hostname*: You may up to 63 alphanumeric characters, dashes (-), or periods (.), but the first character cannot be a period.
`[no] logging syslog <1..4> {disable | level normal | level all}`	Specifies what kind of information, if any, is logged for the specified category.
`[no] logging syslog <1..4> facility {local_1 | local_2 | local_3 | local_4 | local_5 | local_6 | local_7}`	Sets the log facility for the specified remote server. The no command sets the facility to local_1.
`[no] logging syslog <1..4> format {cef | vrpt}`	Sets the format of the log information. `cef`: Common Event Format, syslog-compatible format. `vrpt`: Zyxel's Vantage Report, syslog-compatible format.

This table lists the commands for setting how often to send information to the VRPT (Zyxel's Vantage Report) server.

Table 328 logging Commands: VRPT Settings

COMMAND	DESCRIPTION
`vrpt send device information interval <15..3600>`	Sets the interval (in seconds) for how often the Zyxel Device sends a device information log to the VRPT server.
`vrpt send interface statistics interval <15..3600>`	Sets the interval (in seconds) for how often the Zyxel Device sends an interface statistics log to the VRPT server.
`vrpt send system status interval <15..3600>`	Sets the interval (in seconds) for how often the Zyxel Device sends a system status log to the VRPT server.
`show vrpt send device information interval`	Displays the interval (in seconds) for how often the Zyxel Device sends a device information log to the VRPT server.
`show vrpt send interface statistics interval`	Displays the interval (in seconds) for how often the Zyxel Device sends an interface statistics log to the VRPT server.
`show vrpt send system status interval`	Displays the interval (in seconds) for how often the Zyxel Device sends a system status log to the VRPT server.

Table 328 logging Commands: VRPT Settings (continued)

COMMAND	DESCRIPTION
MODULE_NAME_WTP	{user| zysh| built-in-service| system| system-monitoring| routing-protocol| pki| interface| interface-statistics| account| force-auth| traffic-log| file-manage| wlan| daily-report| dhcp| default| capwap| wlan-station-info| all}
FACILITY	{local_1|local_2|local_3|local_4|local_5|local_6|local_7}
HOSTNAME	"(([a-z0-9\-])+\.)+([a-z]{2}\.[a-z]{2}|[a-z]{2,4})"
USER_NAME_	"([0-9]|[a-z]|[A-Z]|[-_]|\.|\@|[0-9]|[a-z]|[A-Z]|[-_])+"
ZYLOG_SUBJECT	"[a-zA-Z0-9 '()+,./:=?;!*#@$_%-]{1,61}""<subject>";
MODULE_NAME_WTP_	{user| zysh| built-in-service| system| routing-protocol| pki| interface| account| force-auth| file-manage| wlan| daily-report| dhcp| default| capwap| wlan-station-info| all}
WEEKDAYS	{sun|mon|tue|wed|thu|fri|sat}

66.1.4 E-mail Profile Commands

This table lists the commands for the e-mail profile settings.

Table 329 logging Commands: E-mail Profile Settings

COMMAND	DESCRIPTION
`show logging status mail`	Displays the current settings for the e-mail profiles.
`[no] logging mail <1..2>`	Enables the specified e-mail profile. The no command disables the specified e-mail profile.
`[no] logging mail <1..2> address {ip | hostname}`	Sets the URL or IP address of the mail server for the specified e-mail profile. The no command clears the mail server field. *hostname*: You may up to 63 alphanumeric characters, dashes (-), or periods (.), but the first character cannot be a period.
`logging mail <1..2> sending_now`	Sends mail for the specified e-mail profile immediately, according to the current settings.
`[no] logging mail <1..2> tls activate`	Select Transport Layer Security (TLS) if you want encrypted communications between the mail server and the Zyxel Device.
`[no ]logging mail <1..2> tls authenticate-server`	If you choose TLS Security, you may also select this to have the Zyxel Device authenticate the mail server in the TLS handshake.
`[no] logging mail <1..2> authentication`	Enables SMTP authentication. The no command disables SMTP authentication.
`[no] logging mail <1..2> authentication username username password password`	Sets the username and password required by the SMTP mail server. The no command clears the username and password fields. *username*: You can use alphanumeric characters, underscores (_), and dashes (-), and it can be up to 31 characters long. *password*: You can use most printable ASCII characters. You cannot use square brackets [ ], double quotation marks (“), question marks (?), tabs or spaces. It can be up to 63 characters long.
`[no] logging mail <1..2> port <1..65535>`	Sets the port number of the mail server for the specified e-mail profile.
`[no] logging mail <1..2> {send-log-to | send-alerts-to} e_mail`	Sets the e-mail address for logs or alerts. The no command clears the specified field. *e_mail*: You can use up to 63 alphanumeric characters, underscores (_), or dashes (-), and you must use the @ character.

Table 329 logging Commands: E-mail Profile Settings (continued)

COMMAND	DESCRIPTION
`[no] logging mail <1..2> subject subject`	Sets the subject line when the Zyxel Device mails to the specified e-mail profile. The no command clears this field. *subject*: You can use up to 60 alphanumeric characters, underscores (_), dashes (-), or !@#$%*()+=;:',./ characters.
`[no] logging mail <1..2> category module_name level {alert | all}`	Specifies what kind of information is logged for the specified category. The no command disables logging for the specified category.
`[no] logging mail <1..2> schedule {full | hourly}`	Sets the e-mail schedule for the specified e-mail profile. The no command clears the schedule field.
`logging mail <1..2> schedule daily hour <0..23> minute <0..59>`	Sets a daily e-mail schedule for the specified e-mail profile.
`logging mail <1..2> schedule weekly day day hour <0..23> minute <0..59>`	Sets a weekly e-mail schedule for the specified e-mail profile. *day*: sun | mon | tue | wed | thu | fri | sat
`[no] logging mail <1..2> tls starttls-off`	Turns off STARTTLS and uses the TLS protocol for SMTP mail encryption over TLS logging. The no command enables the default STARTTLS protocol.

66.1.4.1 E-mail Profile Command Examples

The following commands set up e-mail log 1.

```
Router# configure terminal
Router(config)# logging mail 1 address mail.zyxel.com.tw
Router(config)# logging mail 1 subject AAA
Router(config)# logging mail 1 authentication username lachang.li password
XXXXXX
Router(config)# logging mail 1 send-log-to lachang.li@zyxel.com.tw
Router(config)# logging mail 1 send-alerts-to lachang.li@zyxel.com.tw
Router(config)# logging mail 1 from lachang.li@zyxel.com.tw
Router(config)# logging mail 1 schedule weekly day mon hour 3 minute 3
Router(config)# logging mail 1
```

66.1.5 Console Port Logging Commands

This table lists the commands for the console port settings.

Table 330 logging Commands: Console Port Settings

COMMAND	DESCRIPTION
`show logging status console`	Displays the current settings for the console log. (This log is not discussed above.)
`[no] logging console`	Enables the console log. The no command disables the console log.
`logging console category module_name level {alert | crit | debug | emerg | error | info | notice | warn}`	Controls whether or not debugging information for the specified priority is displayed in the console log, if logging for this category is enabled.
`[no] logging console category module_name`	Enables logging for the specified category in the console log. The no command disables logging.

CHAPTER 67
Reports and Reboot

67.1 Report Commands Summary

The following sections list the report, session, and packet size statistics commands.

67.1.1 Report Commands

This table lists the commands for reports.

Table 331 report Commands

COMMAND	DESCRIPTION
`[no] report`	Begins data collection. The `no` command stops data collection.
`show report status`	Displays whether or not the Zyxel Device is collecting data and how long it has collected data.
`clear report [`*`interface_name`*`]`	Clears the report for the specified interface or for all interfaces.
`show report [`*`interface_name`* `{ip | service | url}]`	Displays the traffic report for the specified interface and controls the format of the report. Formats are: `ip` - traffic by IP address and direction `service` - traffic by service and direction `url` - hits by URL

67.1.2 Report Command Examples

The following commands start collecting data, display the traffic reports, and stop collecting data.

```
Router# configure terminal
Router(config)# show report ge1 ip
No. IP Address      User                  Amount          Direction
=================================================================
1   192.168.1.4     admin                 1273(bytes)     Outgoing
2   192.168.1.4     admin                 711(bytes)      Incoming
Router(config)# show report ge1 service
No. Port  Service          Amount          Direction
=================================================================
1   21    ftp              1273(bytes)     Outgoing
2   21    ftp              711(bytes)      Incoming
Router(config)# show report ge1 url
No. Hit        URL
=================================================================
1   1          140.114.79.60
Router(config)# show report status
Report status: on
Collection period: 0 days 0 hours 0 minutes 18 seconds
```

67.1.3 Session Commands

This table lists the commands to display the current sessions for debugging or statistical analysis.

Table 332 Session Commands

COMMAND	DESCRIPTION
show conn [user {*username*|any|unknown}] [service {*service-name*|any|unknown}] [source {*ip*|any}] [destination {*ip*|any}] [begin <1..128000>] [end <1..128000>] [dstcc {*country-code*|any}] [srtcc {*country-code*|any}] fastpath	Displays information about the selected sessions, a number of sessions (begin, end) or about all sessions. You can look at all the active sessions or filter the information by user name, service object, source IP, destination IP, country or session number(s). any means all users, services, countries and IP addresses respectively. unknown means unknown users and services respectively. dstcc and srtcc mean source and destination country code. *country_code*: 2-letter country-codes, such as TW, DE, or FR. Use show country-code list to see the codes that represent countries. fastpath Packets that pass through the Zyxel Device are inspected and either allowed through or dropped based on the security policy. IPv4 Packets that match the current connections in the fast path can pass through the Zyxel Device without unnecessary security policy checks. This feature maximizes performance.
show report [*interface_name*] https-url	Displays the most-visited Web sites accessed via SSL through the specified interface and how many times each site has been visited.
show conn ip-traffic destination	Displays information about traffic session sorted by the destination.
show conn ip-traffic source	Displays information about traffic session sorted by the source.
show conn status	Displays the number of active sessions.

67.1.4 Packet Size Statistics Commands

Using the packet size statistics to view packet size distribution may aid you in troubleshooting network performance. In particular, a large number of small packets can drastically reduce throughput. This table lists the commands to enable and disable packet size statistics data collection and display the setting status and statistics.

Table 333 Packet Size Statistics Commands

COMMAND	DESCRIPTION
`[no] report packet size statistics`	Enables or disables packet size statistics data collection.
`show report packet size statistics status`	Shows whether packet size statistics data collection is enabled or disabled.
`show report packet size statistics {interface_name} [interval interval]`	Displays the specified interface's packet size distribution statistics. You can also specify the packet size interval into which to group the statistics. *interval*: 128, 256, or 512 (bytes)
`report packet size statistics clear`	Clears the packet size statistics data for all interface.

67.2 Email Daily Report Commands

The following table identifies the values used in some of these commands. Other input values are discussed with the corresponding commands.

Table 334 Input Values for Email Daily Report Commands

LABEL	DESCRIPTION
e_mail	An e-mail address. You can use up to 80 alphanumeric characters, underscores (_), periods (.), or dashes (-), and you must use the @ character.

Use these commands to have the Zyxel Device e-mail you system statistics every day. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 335 Email Daily Report Commands

COMMAND	DESCRIPTION
`show daily-report status`	Displays the e-mail daily report settings.
`daily-report`	Enters the sub-command mode for configuring daily e-mail reports settings.
`[no] activate`	Turns daily e-mail reports on or off.
`draw-usage-graphics`	Has the report e-mail include usage graphs.
`mail-subject set subject`	Configures the subject of the report e-mails. Spaces are allowed.
`no mail-subject set`	Clears the configured subject for the report e-mails.
`[no] mail-subject append system-name`	Determines whether the system name will be appended to the subject of the report e-mails.
`[no] mail-subject append date-time`	Determines whether the sending date-time will be appended at subject of the report e-mails.
`[no] mail-from e_mail`	Sets the sender e-mail address of the report e-mails.

Table 335 Email Daily Report Commands (continued)

COMMAND	DESCRIPTION
`[no] mail-to-1 e_mail`	Sets to whom the Zyxel Device sends the report e-mails (up to five recipients).
`[no] mail-to-2 e_mail`	See above.
`[no] mail-to-3 e_mail`	See above.
`[no] mail-to-4 e_mail`	See above.
`[no] mail-to-5 e_mail`	See above.
`[no] item as-report`	Determines whether or not anti-spam statistics are included in the report e-mails.
`[no] item av-report`	Determines whether or not anti-virus statistics are included in the report e-mails.
`[no] item cf-report`	Determines whether or not content filtering statistics are included in the report e-mails.
`[no] item cpu-usage`	Determines whether or not CPU usage statistics are included in the report e-mails.
`[no] item idp-report`	Determines whether or not IDP statistics are included in the report e-mails.
`[no] item mem-usage`	Determines whether or not memory usage statistics are included in the report e-mails.
`[no] item port-usage`	Determines whether or not port usage statistics are included in the report e-mails.
`[no] item session-usage`	Determines whether or not session usage statistics are included in the report e-mails.
`[no] item traffic-report`	Determines whether or not network traffic statistics are included in the report e-mails.
`schedule hour <0..23> minute <00..59>`	Sets the time for sending out the report e-mails.
`[no] reset-counter`	Determines whether or not to discard all report data and starts all of the report statistics data counters over at zero after successfully sending out a report e-mail.
`send-now`	Sends the daily e-mail report immediately.
`reset-counter-now`	Discards all report data and starts all of the report statistics data counters over at zero.
`exit`	Leaves the sub-command mode.

67.2.1 Email Daily Report Example

This example sets the following about sending a daily report e-mail:

- Disables the reporting.
- Sets the subject of the report e-mails to test.
- Stops the system name from being appended to the mail subject.
- Appends the date and time to the mail subject.
- Sets the sender as my-email@example.com.
- Sets example-administrator@example.com as the first account to which to send the mail.
- Has the Zyxel Device not use the second and third mail-to options.

- Sets my-email@example.com as the fourth mail-to option.
- Has the Zyxel Device not use the fifth mail-to option.
- Sets the Zyxel Device to send the report at 1:57 PM.
- Has the Zyxel Device not reset the counters after sending the report.
- Has the report include CPU, memory, port, and session usage along with traffic statistics.
- Turns on the daily e-mail reporting.

```
Router(config)# daily-report
Router(config-daily-report)# no activate
Router(config-daily-report)# mail-subject set test
Router(config-daily-report)# no mail-subject append system-name
Router(config-daily-report)# mail-subject append date-time
Router(config-daily-report)# mail-from my-email@example.com
Router(config-daily-report)# mail-to-1 example-administrator@example.com
Router(config-daily-report)# no mail-to-2
Router(config-daily-report)# no mail-to-3
Router(config-daily-report)# mail-to-4 my-email@example.com
Router(config-daily-report)# no mail-to-5
Router(config-daily-report)# schedule hour 13 minutes 57
Router(config-daily-report)# no reset-counter
Router(config-daily-report)# item cpu-usage
Router(config-daily-report)# item mem-usage
Router(config-daily-report)# item port-usage
Router(config-daily-report)# item session-usage
Router(config-daily-report)# item traffic-report
Router(config-daily-report)# activate
Router(config-daily-report)# exit
```

This displays the email daily report settings and has the Zyxel Device send the report.

```
Router(config)# show daily-report status
email daily report status
=========================
activate: yes
scheduled time: 13:57
reset counter: no
mail subject:  test subject
append system name: no
append date time: yes
mail from: my-email@example.com
mail-to-1: example-administrator@example.com
mail-to-2:
mail-to-3:
mail-to-4: my-email@example.com
mail-to-5:
cpu-usage: yes
mem-usage: yes
session-usage: yes
port-usage: yes
traffic-report: yes

Router(config)# daily-report send-now
```

67.3 Reboot

Use this to restart the device (for example, if the device begins behaving erratically).

If you made changes in the CLI, you have to use the `write` command to save the configuration before you reboot. Otherwise, the changes are lost when you reboot.

Use the `reboot` command to restart the device.

CHAPTER 68
Diagnostics and Remote Assistance

68.1 Diagnostics

This chapter covers how to use the diagnostics feature. See also Chapter 71 on page 586 for information on other maintenance tools.

The diagnostics feature provides an easy way for you to generate a file containing the Zyxel Device's configuration and diagnostic information. You may need to generate this file and send it to customer support during troubleshooting.

68.2 Diagnosis Commands

The following table lists the commands that you can use to have the Zyxel Device collect diagnostics information. Use the `configure terminal` command to enter the configuration mode to be able to use these commands.

Table 336 diagnosis Commands

COMMAND	DESCRIPTION
`diag-info collect`	Has the Zyxel Device create a new diagnostic file.
`show diag-info`	Displays the name, size, and creation date (in yyyy-mm-dd hh:mm:ss format) of the diagnostic file.
`show cpu average`	Displays the current percentage usage of each CPU in the Zyxel Device as a percentage of total processing power and the current CPU utilization percentage for each application used on the Zyxel Device.
`show mem status all`	Displays the current DRAM memory utilization percentage for each application used on the Zyxel Device and each application's running time in hours - minutes - seconds.
`diaginfo collect ac`	Collects information on the AP controller (the Zyxel Device).
`diaginfo collect wtp`	Collects information on Access Points managed by the AP controller (the Zyxel Device).
`diaginfo delete / ac`	Deletes information collected on the AP controller (the Zyxel Device).
`diaginfo delete / wtp`	Deletes information collected on Access Points managed by the AP controller (the Zyxel Device).

Table 336 diagnosis Commands (continued)

COMMAND	DESCRIPTION
`nslookup {ipv4 | hostname} [server ipv4] [extension filter-extension]`	Performs name server lookup for querying a Domain Name System (DNS) server to get the domain name or IPv4 address mapping. The `server` and `extension` fields are optional. *filter_extension*: You can use 1-256 alphanumeric characters, spaces, or '()+,/ :=?;!*#@$_%.- characters.
`nslookup6 {ipv6 | hostname} [server ipv6] [extension filter-extension]`	Performs name server lookup for querying a Domain Name System (DNS) server to get the domain name or IPv6 address mapping. The `server` and `extension` fields are optional. *filter_extension*: You can use 1-256 alphanumeric characters, spaces, or '()+,/ :=?;!*#@$_%.- characters.

68.3 Diagnosis Commands Example

The following example creates a diagnostic file and displays its name, size, and creation date.

```
Router# configure terminal
Router(config)# diag-info collect
Please wait, collecting information
Router(config)# show diag-info
Filename  : diaginfo-20070423.tar.bz2
File size : 1259 KB
Date      : 2014-04-23 09:55:09
```

The following is an example of the `nslookup` command.

```
Router# nslookup www.zyxel.com.tw
Trying "www.zyxel.com.tw"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42419
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.zyxel.com.tw.              IN      ANY

;; ANSWER SECTION:
www.zyxel.com.tw.       38400   IN      CNAME   origin-tw.zyxel.com.

Received 67 bytes from 127.0.0.1#53 in 1 ms
Router#
```

68.4 Remote Assistance

Use Remote Assistance commands to configure and schedule external access to the Zyxel Device for troubleshooting. You can also specify the port numbers the services must use to connect to the Zyxel Device.

Note: Remote Assistance is not available in firmware version 4.50 or later.

68.5 Remote Assistance Commands

The following table lists the commands that you can use to configure Remote Assistance on the Zyxel Device. Use the `configure terminal` command to enter the configuration mode to be able to use these commands.

Table 337 remote-assistance Commands

COMMAND	DESCRIPTION
`(no) remote-assistance activate`	Enables an external person, such as customer support to access the Zyxel Device from a network outside the Zyxel Device local network for troubleshooting. The `no` command disables remote assistance.
`remote-assistance [https|ssh] port` *`port`*	Sets the service port number for external access. It should be the same port number as the one configured on the Zyxel Device.
`remote-assistance [address1|address2]` *`ipv4`*	Sets the public IPv4 addresses of external users that are allowed to access the Zyxel Device remotely.
`remote-assistance remove {address1|address2}`	Removes the public IPv4 addresses of external users that are allowed to access the Zyxel Device remotely.
`remote-assistance settings [random|manual]`	`random` allows access to the Zyxel Device remotely by using a randomly generated user name and password pair. `manual` allows access to the Zyxel Device remotely by using a previously configured specific user account.
`remote-assistance user-object` *`user`*	Specifies a previously created user/group object that can have external access to the Zyxel Device for troubleshooting.
`remote-assistance generate user-password`	Randomly generates a user name and password pair for remote access to the Zyxel Device.
`remote-assistance schedule DATE TIME` *`date time`*	Specifies a date (yyyy-mm-dd) and time (hh-mm) that external access is allowed.
`show remote-assistance`	Displays configured remote assistance settings including randomly generated user name / password, addresses, access ports and schedule.
`show remote-assistance generate`	Displays randomly generated user name / password for remote assistance.

CHAPTER 69
Session Timeout

Use these commands to modify and display the session timeout values. You must use the `configure terminal` command before you can use these commands.

Table 338 Session Timeout Commands

COMMAND	DESCRIPTION
`session timeout {udp-connect <1..300> | udp-deliver <1..300> | icmp <1..300>}`	Sets the timeout for UDP sessions to connect or deliver and for ICMP sessions.
`session timeout session {tcp-established | tcp-synrecv | tcp-close | tcp-finwait | tcp-synsent | tcp-closewait | tcp-lastack | tcp-timewait} <1..300>`	Sets the timeout for TCP sessions in the ESTABLISHED, SYN_RECV, FIN_WAIT, SYN_SENT, CLOSE_WAIT, LAST_ACK, or TIME_WAIT state.
`show session timeout {icmp | tcp-timewait | udp}`	Displays ICMP, TCP, and UDP session timeouts.

The following example sets the UDP session connect timeout to 10 seconds, the UDP deliver session timeout to 15 seconds, and the ICMP timeout to 15 seconds.

```
Router(config)# session timeout udp-connect 10
Router(config)# session timeout udp-deliver 15
Router(config)# session timeout icmp 15
Router(config)# show session timeout udp
UDP session connect timeout: 10 seconds
UDP session deliver timeout: 15 seconds
Router(config)# show session timeout icmp
ICMP session timeout: 15 seconds
```

CHAPTER 70
Packet Flow Explore

70.1 Packet Flow Explore

Use this to get a clear picture on how the Zyxel Device determines where to forward a packet and how to change the source IP address of the packet according to your current settings. This function provides you a summary of all your routing and SNAT settings and helps troubleshoot the related problems.

70.2 Packet Flow Explore Commands

The following table lists the commands that you can use to have the Zyxel Device display routing and SNAT related settings.

Table 339 Packet Flow Explore Commands

COMMAND	DESCRIPTION
`show route order`	Displays the order of routing related functions the Zyxel Device checks for packets. Once a packet matches the criteria of a routing rule, the Zyxel Device takes the corresponding action and does not perform any further flow checking.
`show system snat order`	Displays the order of SNAT related functions the Zyxel Device checks for packets. Once a packet matches the criteria of an SNAT rule, the Zyxel Device uses the corresponding source IP address and does not perform any further flow checking.
`show system route policy-route`	Displays activated policy routes.
`show system route nat-1-1`	Displays activated 1-to-1 NAT rules.
`show system route site-to-site-vpn`	Displays activated site-to-site VPN rules.
`show system route dynamic-vpn`	Displays activated dynamic VPN rules.
`show system route default-wan-trunk`	Displays the default WAN trunk settings.
`show ip route static-dynamic`	Displays activated static-dynamic routes.
`show system snat policy-route`	Displays activated policy routes which use SNAT.
`show system snat nat-1-1`	Displays activated NAT rules which use SNAT.
`show system snat nat-loopback`	Displays activated activated NAT rules which use SNAT with NAT loopback enabled.
`show system snat default-snat`	Displays the default WAN trunk settings.

70.3 Packet Flow Explore Commands Example

The following example shows all routing related functions and their order.

```
Router> show route order
route order: Policy Route, Direct Route, 1-1 SNAT, SiteToSite VPN, Dynamic
VPN, Static-Dynamic Route, Default WAN Trunk, Main Route
```

The following example shows all SNAT related functions and their order.

```
Router> show system snat order
snat order: Policy Route SNAT, 1-1 SNAT, Loopback SNAT, Default SNAT
```

The following example shows all SNAT related functions and their order.

```
Router> show system route policy-route
No.  PR NO. Source   Destination      Incoming     DSCP   Service   Nexthop
Type        Nexthop Info
================================================================================

```

The following example shows all activated 1-to-1 SNAT rules.

```
Router> show system route nat-1-1
No.  VS Name         Source     Destination   Outgoing        Gateway
================================================================================
```

The following example shows all activated site-to-site VPN rules.

```
Router> show system route site-to-site-vpn
No.  Source         Destination          VPN Tunnel
================================================================================

```

The following example shows all activated dynamic VPN rules.

```
Router> show system route dynamic-vpn
No.  Source         Destination             VPN Tunnel
================================================================================

```

The following example shows the default WAN trunk's settings.

```
Router> show system route default-wan-trunk
No.  Source          Destination     Trunk
================================================================================
1    any             any             trunk_ex
```

The following example shows all activated dynamic VPN rules.

```
Router> show system route dynamic-vpn
No.  Source         Destination             VPN Tunnel
================================================================================
```

The following example shows all activated static-dynamic VPN rules.

```
Router> show ip route static-dynamic
Flags: A - Activated route, S - Static route, C - directly Connected
       O - OSPF derived, R - RIP derived, G - selected Gateway
       ! - reject, B - Black hole, L - Loop

IP Address/Netmask    Gateway          IFace           Metric    Flags
Persis
t
================================================================================
0.0.0.0/0             10.1.1.254       wan1            0         ASG      -
```

The following example shows all activated policy routes which use SNAT.

```
Router> show system snat policy-route
No.  PR NO. Outgoing        SNAT
================================================================================
```

The following example shows all activated 1-to-1 NAT rules.

```
Router> show system snat nat-1-1
No.  VS Name     Source        Destination   Outgoing        SNAT
================================================================================
```

The following example shows all activated policy routes which use SNAT and enable NAT loopback..

```
Router> show system snat nat-loopback
Note: Loopback SNAT will be only applied only when the initiator is located
at the network which the server locates at

No.  VS Name        Source        Destination     SNAT
================================================================================
```

The following example shows all activated 1-to-1 NAT rules.

```
Router> show system snat nat-1-1
No.  VS Name     Source        Destination   Outgoing        SNAT
================================================================================
```

The following example shows the default WAN trunk settings.

```
Router> show system snat default-snat
Incoming                Outgoing                SNAT
================================================================================
Internal Interface      External Interface      Outgoing Interface IP


Internal Interfaces: lan1, hidden, lan2, dmz
External Interfaces: wan1, wan2, wan1_ppp, wan2_ppp
Router>
```

CHAPTER 71
Maintenance Tools

Use the maintenance tool commands to optimize the health of the Zyxel Device, check the status of other devices connected to the Zyxel Device, and troubleshoot network problems.

Table 340 Maintenance Tools Commands in Privilege Mode

COMMAND	DESCRIPTION
`packet-trace [interface` *`interface_name`*`] [[ip-proto|ipv6-proto] |` *`protocol_name`* `| any}] [src-host {`*`ip`* `|` *`hostname`* `| any}] [dst-host {`*`ip`* `|` *`hostname`* `| any}] [host {`*`ip`*`|` *`hostname`*`|` *`any`*`}] [port {<1..65535> | any}] [file] [duration <1..3600>] [extension-filter arp| link-header| data-header| match-port` *`port port`*`| match-host` *`host host`*`]`	Sniffs traffic going through the specified interface with the specified protocol, source address, destination address, and/or port number. If you specify `file`, the Zyxel Device dumps the traffic to `/packet_trace/packet_trace_interface`. Use FTP to retrieve the files (see Section 65.7 on page 548). If you do not assign the duration, the Zyxel Device keeps dumping traffic until you use Ctrl-C. *`protocol_name`*: You can use the name, instead of the number, for some IP protocols, such as `tcp`, `udp`, `icmp`, and so on. The names consist of 1-16 alphanumeric characters or dashes (-). The first character cannot be a number. *`hostname`*: You can use up to 252 alphanumeric characters, dashes (-), or periods (.). The first character cannot be a period. Use `extension-filter` if you want to use an extended packet trace command.
`traceroute {`*`ip`* `|` *`hostname`*`}`	Displays the route taken by packets to the specified destination. Use `Ctrl+c` to return to the prompt.
`traceroute6 {`*`ipv6`* `|` *`hostname`*`}`	Displays the route taken by packets to the specified destination. Use `Ctrl+c` to return to the prompt.
`[no] packet-capture activate`	Performs a packet capture that captures network traffic going through the set interface(s). Studying these packet captures may help you identify network problems. The no command stops the running packet capture on the Zyxel Device. Note: Use the `packet-capture configure` command to configure the packet-capture settings before using this command.
`packet-capture configure`	Enters the sub-command mode.
`duration <0..300>`	Sets a time limit in seconds for the capture. The Zyxel Device stops the capture and generates the capture file when either this period of time has passed or the file reaches the size specified using the `files-size` command below. 0 means there is no time limit.

Table 340 Maintenance Tools Commands in Privilege Mode (continued)

COMMAND	DESCRIPTION
file-suffix <*profile_name*>	Specifies text to add to the end of the file name (before the dot and filename extension) to help you identify the packet capture files. Modifying the file suffix also avoids making new capture files that overwrite existing files of the same name. The file name format is "interface name-file suffix.cap", for example "vlan2-packet-capture.cap".
files-size <1..10000>	Specify a maximum size limit in megabytes for the total combined size of all the capture files on the ZyWALL, including any existing capture files and any new capture files you generate. The Zyxel Device stops the capture and generates the capture file when either the file reaches this size or the time period specified (using the duration command above) expires.
host-ip {*ip-address* | *profile_name* | any>	Sets a host IP address or a host IP address object for which to capture packets. any means to capture packets for all hosts.
host-port <0..65535>	If you set the IP Type to any, tcp, or udp using the proto-type command below, you can specify the port number of traffic to capture.
iface {add | del} {*interface_name* | *virtual_interface_name*}	Adds or deletes an interface or a virtual interface for which to capture packets to the capture interfaces list.
ip-version {ip|ip6|any}	Sets whether to capture IPv4 or IPv6 traffic. Any means to capture packets for all types of traffic.
proto-type {icmp | icmp6 | igmp | igrp | pim | ah | esp | vrrp | udp | tcp | any}	Sets the protocol of traffic for which to capture packets. any means to capture packets for all types of traffic.
snaplen <68..1512>	Specifies the maximum number of bytes to capture per packet. The Zyxel Device automatically truncates packets that exceed this size. As a result, when you view the packet capture files in a packet analyzer, the actual size of the packets may be larger than the size of captured packets.
storage <internal|usbstorage>	Sets to have the Zyxel Device only store packet capture entries on the Zyxel Device (internal) or on a USB storage connected to the Zyxel Device.
ring-buffer <enable|disable>	Enables or disables the ring buffer used as a temporary storage.
split-size <1..2048>	Specify a maximum size limit in megabytes for individual packet capture files. After a packet capture file reaches this size, the Zyxel Device starts another packet capture file.
Ping {*ipv4* | *hostname*} [source *ipv4*] [size <0..65507>] [forever| count <1..4096>]	Sends an ICMP ECHO_REQUEST to test the reachability of a host on an IPv4 network and to measure the round-trip time for a message sent from the originating host to the destination computer. size: specifies the number of data bytes to be sent count: Stop after sending this number of ECHO_REQUEST packets. forever: keep sending ECHO_REQUEST packets until you use Ctrl+c to stop.

Table 340 Maintenance Tools Commands in Privilege Mode (continued)

COMMAND	DESCRIPTION
ping {ipv4_addr | *hostname*} [source *ipv4*] [size <0..65507>] [forever | count <1..4096>] [interface *interface_name*] [extension *filter-extension*]	Sends an ICMP ECHO_REQUEST to test the reachability of a host on an IPv4 network and to measure the round-trip time for a message sent from the originating host to the destination computer. Use the extension filter to extend the use of this command. source: Set source address to specified interface IPv4 address. size: specifies the number of data bytes to be sent. count: Stop after sending this number of ECHO_REQUEST packets. forever: keep sending ECHO_REQUEST packets until you use Ctrl+c to stop. *interface_name*: specifies interface through which to send the ECHO_REQUEST packets. *filter_extension*: You can use 1-256 alphanumeric characters, spaces, or '()+,/:=?;!*#@$_%.- characters.
ping6{*ipv6* | *hostname*} [source *ipv6*] [size <0..65527>] [forever| count <1..4096>] [interface {*interface_name* | *virtual_interface_name*}][extension *filter_extension*]	Sends an ICMP ECHO_REQUEST to test the reachability of a host on an IPv6 network and to measure the round-trip time for a message sent from the originating host to the destination computer. Use the extension filter to extend the use of this command. source: Set source address to specified interface IPv6 address. When pinging IPv6 link-local address this option is required. size: specifies the number of data bytes to be sent count: Stop after sending this number of ECHO_REQUEST packets. forever: keep sending ECHO_REQUEST packets until you use Ctrl+c to stop. *interface_name*: specifies interface through which to send the ECHO_REQUEST packets. *filter_extension*: You can use 1-256 alphanumeric characters, spaces, or '()+,/:=?;!*#@$_%.- characters.
traceroute {*ipv4* | *hostname*} [source *ipv4*] [interface *interface_name*] [extension *filter-extension*]	Displays the route packets take to an IPv4 network host. Use the extension filter to extend the use of this command. source: Set source address to specified interface IPv4 address. *interface_name*: specifies a network interface to obtain the source IP address for outgoing probe packets. *filter_extension*: You can use 1-256 alphanumeric characters, spaces, or '()+,/:=?;!*#@$_%.- characters.

Table 340 Maintenance Tools Commands in Privilege Mode (continued)

COMMAND	DESCRIPTION
`traceroute6 {ipv6 | hostname} [source ipv6] [interface interface_name] [extension filter-extension]`	Displays the route packets take to an IPv6 network host. Use the extension filter to extend the use of this command. `source`: Set source address to specified interface IPv6 address. *`interface_name`*: specifies a network interface to obtain the source IP address for outgoing probe packets. *`filter_extension`*: You can use 1-256 alphanumeric characters, spaces, or '()+,/:=?;!*#@$_%.- characters.
`tracepath6 {ipv6 | hostname}`	Displays the path MTU for the target address.
`show packet-capture status`	Displays whether a packet capture is ongoing.
`show ipv6 neighbor-list`	Displays the Zyxel Device's IPv6 neighbors.
`show packet-capture config`	Displays current packet capture settings.

Here are maintenance tool commands that you can use in configuration mode.

Table 341 Maintenance Tools Commands in Configuration Mode

COMMAND	DESCRIPTION
`ipv6 neighbor flush {ipv6 | all}`	Clears the specified IPv6 address or all IPv6 addresses from the IPv6 neighbor cache.

71.1 Maintenance Command Examples

Some packet-trace command examples are shown below.

```
Router# packet-trace duration 3
tcpdump: listening on eth0
19:24:43.239798 192.168.1.10 > 192.168.1.1: icmp: echo request
19:24:43.240199 192.168.1.1 > 192.168.1.10: icmp: echo reply
19:24:44.258823 192.168.1.10 > 192.168.1.1: icmp: echo request
19:24:44.259219 192.168.1.1 > 192.168.1.10: icmp: echo reply
19:24:45.268839 192.168.1.10 > 192.168.1.1: icmp: echo request
19:24:45.269238 192.168.1.1 > 192.168.1.10: icmp: echo reply

6 packets received by filter
0 packets dropped by kernel
```

```
Router# packet-trace interface ge2 ip-proto icmp file extension-filter -s
-> 500 -n
tcpdump: listening on eth1
07:24:07.898639 192.168.105.133 > 192.168.105.40: icmp: echo request (DF)
07:24:07.900450 192.168.105.40 > 192.168.105.133: icmp: echo reply
07:24:08.908749 192.168.105.133 > 192.168.105.40: icmp: echo request (DF)
07:24:08.910606 192.168.105.40 > 192.168.105.133: icmp: echo reply

8 packets received by filter
0 packets dropped by kernel
```

```
Router# packet-trace interface ge2 ip-proto icmp file extension-filter
-> and src host 192.168.105.133 and dst host 192.168.105.40 -s 500 -n
tcpdump: listening on eth1
07:26:51.731558 192.168.105.133 > 192.168.105.40: icmp: echo request (DF)
07:26:52.742666 192.168.105.133 > 192.168.105.40: icmp: echo request (DF)
07:26:53.752774 192.168.105.133 > 192.168.105.40: icmp: echo request (DF)
07:26:54.762887 192.168.105.133 > 192.168.105.40: icmp: echo request (DF)

8 packets received by filter
0 packets dropped by kernel
```

```
Router# traceroute www.zyxel.com
traceroute to www.zyxel.com (203.160.232.7), 30 hops max, 38 byte packets
 1  172.23.37.254  3.049 ms  1.947 ms  1.979 ms
 2  172.23.6.253  2.983 ms  2.961 ms  2.980 ms
 3  172.23.6.1  5.991 ms  5.968 ms  6.984 ms
 4  * * *
```

Here are maintenance tool commands that you can use in configure mode.

Table 342 Maintenance Tools Commands in Configuration Mode

COMMAND	DESCRIPTION
`show arp-table`	Displays the current Address Resolution Protocol table.
`arp IP` *`mac_address`*	Edits or creates an ARP table entry.
`no arp` *`ip`*	Removes an ARP table entry.

The following example creates an ARP table entry for IP address 192.168.1.10 and MAC address 01:02:03:04:05:06. Then it shows the ARP table and finally removes the new entry.

```
Router# arp 192.168.1.10 01:02:03:04:05:06
Router# show arp-table
Address                HWtype  HWaddress          Flags Mask           Iface
192.168.1.10            ether   01:02:03:04:05:06   CM                    ge1
172.23.19.254           ether   00:04:80:9B:78:00   C                     ge2
Router# no arp 192.168.1.10
Router# show arp-table
Address                HWtype  HWaddress          Flags Mask           Iface
192.168.1.10                    (incomplete)                             ge1
172.23.19.254           ether   00:04:80:9B:78:00   C                     ge2
```

71.1.1 Packet Capture Command Example

The following examples show how to configure packet capture settings to capture packets going through the Zyxel Device WAN1 interface only.

Use Split Size to specify a maximum size for individual packet capture files. After a packet capture file reaches this size, the Zyxel Device starts another packet capture file.

Use File Size to specify a maximum size limit for the total combined size of all the capture files on the Zyxel Device, including any existing capture files and any new capture files you generate.

Use Duration to set a limit in seconds for the capture. The Zyxel Device stops the capture and generates the capture file when either this period of time has passed or when the file reaches the File Size limit you specify.

Enable Ring Buffer to continuously capture and overwrite old files until you stop capturing packets manually. The Zyxel Device will not stop even if the File Size limit you specify is reached.You should specify the File Size limit to a larger number or delete existing captured files if you disable this feature.

This example follows the parameters in the list below.

- IP address: any
- Host IP: any
- Host Port: any (then you do not need to configure this setting)
- File Suffix: Example
- Split Size: 10 megabytes
- File Size: 100 megabytes
- Duration: 150 seconds
- Save the captured packets to: USB storage device
- Ring Buffer: Enable

1 Check if there's any packet capture running on the Zyxel Device.

```
Router(config)# show packet-capture status
```

2 Check the current packet capture settings.

```
Router(config)# show packet-capture config
iface: None
ip-version: any
proto-type: any
host-port: 0
host-ip: any
file-suffix: -packet-capture
snaplen: 1500
duration: 0
file-size: 10
split-size: 2
ring-buffer: 0
storage: 0
```

3 Enter packet capture sub-command mode to configure settings to capture traffic that goes through the specific interface.

```
Router(config)# packet-capture configure
Router(packet-capture)#
```

4 Configure the packet capture settings according to the list above.

```
Router(packet-capture)# iface add wan1
Router(packet-capture)# ip-type any
Router(packet-capture)# host-ip any
Router(packet-capture)# file-suffix Example
Router(packet-capture)# files-size 10o
Router(packet-capture)# duration 150
Router(packet-capture)# storage usbstorage
Router(packet-capture)# ring-buffer enable
Router(packet-capture)# split-size 10
Router(packet-capture)#
```

5 Exit the sub-command mode. Activate packet capture to have the Zyxel Device capture packets according to the settings you just configured.

```
Router(packet-capture)# exit
Router(config)# packet-capture activate
Router(config)#
```

6 Manually stop the running packet capturing when you get the information you need. Otherwise, with Ring Buffer enabled, the Zyxel Device will keep capturing and overwriting old captured files.

```
Router(config)# no packet-capture activate
Router(config)#
```

7 Check current packet capture status and list all stored packet captures.

```
Router(config)# show packet-capture status
capture status: off
Router(config)# dir /packet_trace
File Name                                         Size     Modified Time
==============================================================================
wan1-Example.cap                                575160   2009-11-24 09:06:59
Router(config)#
```

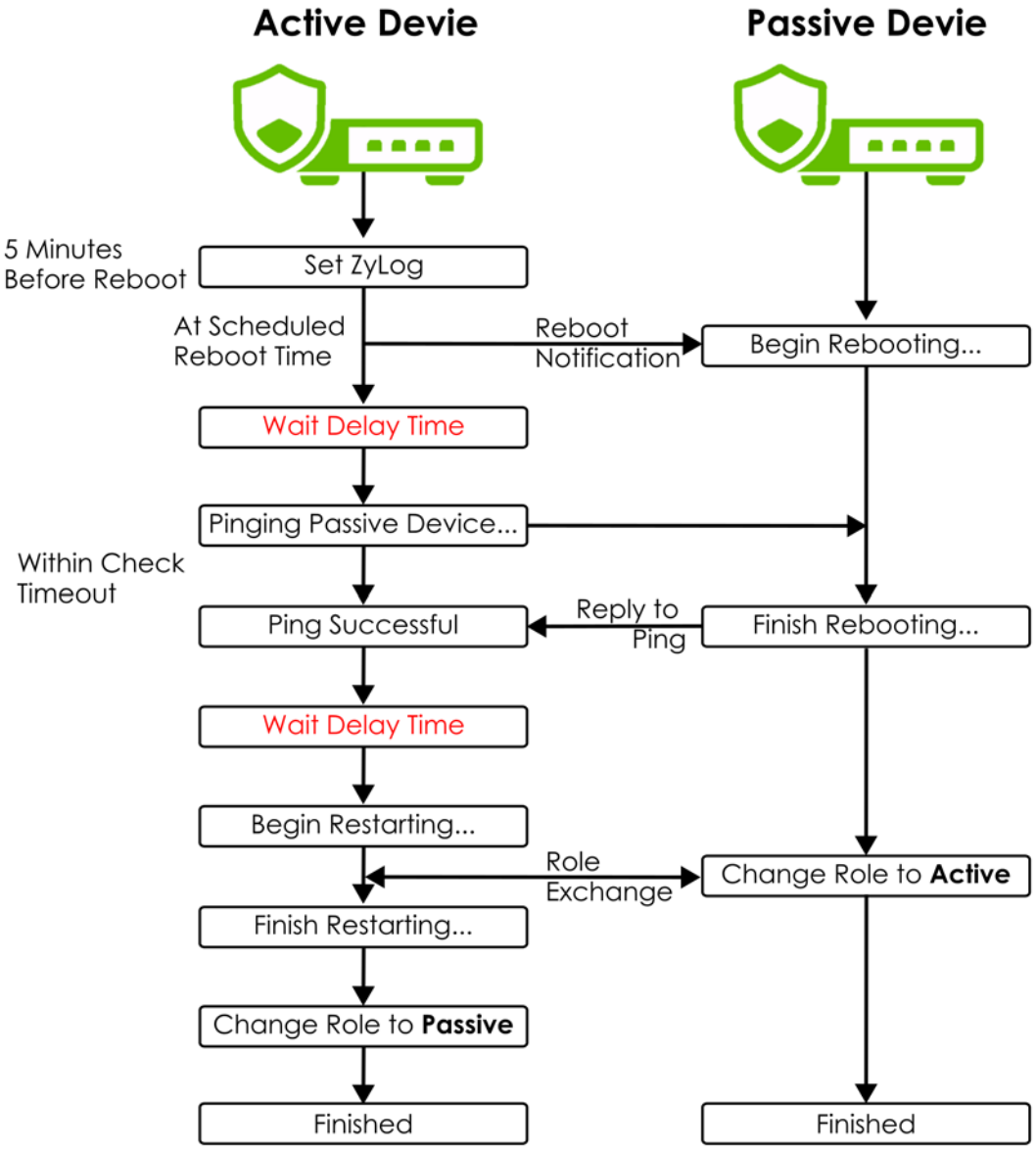
8 Download the captured files in the web configurator at Maintenance > Diagnostics > Packet Capture > Files. Open and study it using a packet analyzer tool (for example, Ethereal or Wireshark).

71.2 Scheduled Reboot

For stability, you can restart the Zyxel Device periodically according to a user-defined schedule.

71.2.1 High Availability Reboot Process

Figure 73 High Availability Reboot Process Flow



The following table describes the schedule reboot commands.

Table 343 Scheduled Reboot Commands

COMMAND	DESCRIPTION
`[no] schedule reboot activate`	Enables or disables the reboot schedule. When enabled, the Zyxel Device will restart according to the schedule.
`schedule reboot daily <time,hh:mm>`	Sets the device to restart once a day at the specified hour and minute. *hh:mm* is in 24-hour format, for example 23:30.
`schedule reboot weekly <time,hh:mm> {sun|mon|tue|wed|thu|fri|sat}`	Sets the device to restart once a week on the specified day, at the specified hour and minute. *hh:mm* is in 24-hour format, for example 23:30.

Table 343 Scheduled Reboot Commands (continued)

COMMAND	DESCRIPTION
`schedule reboot monthly <time,hh:mm> <day,dd>`	Sets the device to restart once a month on the specified day, at the specified hour and minute. *dd* must be written as two digits. The valid range is 01–28.
`device-ha2 schedule-reboot check-timeout <1..3600>`	Sets how long the active device pings the passive device for, in seconds, after the passive device has restarted. If the passive device does not respond within the specified time, the activate device cancels the scheduled reboot. The default time is 1800 seconds.
`device-ha2 schedule-reboot delay <1..300>`	Sets a delay time to ensure the passive device has sufficient time to shut down and start up. The delay time is measured in seconds, and the default is 10. After the passive device shuts down, the active device waits for the specified delay time before starting to ping the passive device. Then after the ping is successful, the activate device waits for the specified delay time before rebooting.
`show schedule reboot status`	Displays the status of the reboot schedule, including whether it is active and at what time and date the device is scheduled to reboot.
`show device-ha2 schedule-reboot check-timeout`	Displays the ping timeout time, in seconds.
`show device-ha2 schedule-reboot delay`	Displays the HA reboot delay time, in seconds.

71.3 Configuration File Backup

You can back up the Zyxel Device's configuration file, by downloading it to your local computer or by sending it to an email address.

Table 344 Configuration File Backup Commands

COMMAND	DESCRIPTION
`The conf-mail commands send a user-specified configuration file immediately to an email address.`	
`conf-mail mail-subject <subject>`	Sets the backup email subject text. The text must be 1–60 characters, and may consist of letters, numbers, and the following special characters: '()+,./ :=?;!*#@$_%-
`conf-mail mail-content <mail-content>`	Sets the backup email body text. The text must consist of 1–250 ASCII characters.
`conf-mail no mail-content`	Clears the backup email body text.
`conf-mail {mail-to-1|mail-to-2|mail-to-3|mail-to-4|mail-to-5} <user@domainname>`	Sets the receiving email address. You can send the configuration file to a maximum of five email addresses.
`conf-mail no {mail-to-1|mail-to-2|mail-to-3|mail-to-4|mail-to-5}`	Clears the receiving email address.

Table 344 Configuration File Backup Commands (continued)

COMMAND	DESCRIPTION
conf-mail attach password <*attachment password*>	Adds an encryption password to the configuration file in the email. The password must consist of 1–31 ASCII characters.
conf-mail send-now <*configfile*>	Sends the specified configuration file to the configured email addresses. <CONFIGFILE> must contain a full file path, for example: /conf/system-default.conf
show config-backup status	Shows the backup mail settings.
The conf-backup commands automatically backup the current Zyxel Device configuration file according to a schedule, and then send it to an email address.	
config-backup setting	Enters the configuration file scheduled backup subcommand mode.
mail-attach password <*attachment password*>	Adds an encryption password to the configuration file in the email. The password must consist of 1–31 ASCII characters.
no mail-attach password	Removes the encryption password from the email.
mail-info content <*mail-content*>	Sets the backup email body text. The text must consist of 1–250 ASCII characters.
no mail-info content	Clears the backup email body text.
mail-info *{mail-to-1|mail-to-2|mail-to-3|mail-to-4|mail-to-5}* <user@domainname>	Sets the receiving email address. You can send the configuration file to a maximum of five email addresses.
no *{mail-to-1|mail-to-2|mail-to-3|mail-to-4|mail-to-5}*	Clears the receiving email address.
[no] mail-send	The Zyxel Device backs up the current configuration file, and then sends it to the configured email addresses. With the [no] option, the Zyxel Device only backs up the current configuration file.
scheduler daily <*time,hh:mm*>	Sets the device to backup its config file once a day at the specified hour and minute. *hh:mm* is in 24-hour format, for example 23:30.
scheduler weekly <*time,hh:mm*> *{sun|mon|tue|wed|thu|fri|sat}*	Sets the device to backup its config file once a week on the specified day, at the specified hour and minute. *hh:mm* is in 24-hour format, for example 23:30.
scheduler monthly <*time,hh:mm*> <*day,dd*>	Sets the device to backup its config file once a month on the specified day, at the specified hour and minute. *dd* must be written as two digits. The valid range is 01–31. If the day is greater than the number of days in the month, then the job will run on the last day of the month.
exit	Exits subcommand mode.
[no] config-backup scheduler activate	Enables or disables the automatic configuration file backup.
config-backup run	Backups up the configuration file now.
show config-backup status	Shows the schedules configuration file backup settings.

CHAPTER 72
Miscellaneous

72.1 SDWan OnCloud

From firmware version 5.0 and later, certain models of Zyxel Device can be managed by Nebula Control Center (NCC).

Table 345 SDWAn Commands

COMMAND	DESCRIPTION
`show sdwan oncloudst`	Displays whether NCC is managing the Zyxel Device.

72.2 Watchdog Timer

This section provides information about the Zyxel Device's watchdog timers.

72.2.1 Hardware Watchdog Timer

The hardware watchdog has the system restart if the hardware fails.

> The **`hardware-watchdog-timer`** commands are for support engineers. It is recommended that you not modify the hardware watchdog timer settings.

Table 346 hardware-watchdog-timer Commands

COMMAND	DESCRIPTION
`[no] hardware-watchdog-timer <4..37>`	Sets how long the system's hardware can be unresponsive before resetting. The no command turns the timer off.
`show hardware-watchdog-timer status`	Displays the settings of the hardware watchdog timer.

72.2.2 Software Watchdog Timer

The software watchdog has the system restart if the core firmware fails.

The **software-watchdog-timer** commands are for support engineers. It is recommended that you not modify the software watchdog timer settings.

Table 347 software-watchdog-timer Commands

COMMAND	DESCRIPTION
[no] software-watchdog-timer <10..600>	Sets how long the system's core firmware can be unresponsive before resetting. The no command turns the timer off.
show software-watchdog-timer status	Displays the settings of the software watchdog timer.
show software-watchdog-timer log	Displays a log of when the software watchdog timer took effect.

72.2.3 Application Watchdog

The application watchdog has the system restart a process that fails. These are the app-watchdog commands. Use the configure terminal command to enter the configuration mode to be able to use these commands.

Table 348 app-watchdog Commands

COMMAND	DESCRIPTION
[no] app-watch-dog activate	Turns the application watchdog timer on or off.
[no] app-watch-dog auto-recover	If app-watch-dog detects a dead process, app-watch-dog will try to auto recover. The no command turns off auto-recover
[no] app-watch-dog console-print {always|once}	Display debug messages on the console (every time they occur or once). The no command changes the setting back to the default.
[no] app-watch-dog cpu-threshold min <1..100> max <1..100>	Sets the percentage thresholds for sending a CPU usage alert. The Zyxel Device starts sending alerts when CPU usage exceeds the maximum (the second threshold you enter). The Zyxel Device stops sending alerts when the CPU usage drops back below the minimum threshold (the first threshold you enter). The no command changes the setting back to the default.
[no] app-watch-dog interval <6..300>	Sets how frequently (in seconds) the Zyxel Device checks the system processes. The no command changes the setting back to the default.
[no] app-watch-dog retry-count <1..5>	Set how many times the Zyxel Device is to re-check a process before considering it failed. The no command changes the setting back to the default.
[no] app-watch-dog alert	Has the Zyxel Device send an alert the user when the system is out of memory or disk space.
[no] app-watch-dog disk-threshold min <1..100> max <1..100>	Sets the percentage thresholds for sending a disk usage alert. The Zyxel Device starts sending alerts when disk usage exceeds the maximum (the second threshold you enter). The Zyxel Device stops sending alerts when the disk usage drops back below the minimum threshold (the first threshold you enter). The no command changes the setting back to the default.
[no] app-watch-dog mem-threshold min <1..100> max <1..100>	Sets the percentage thresholds for sending a memory usage alert. The Zyxel Device starts sending alerts when memory usage exceeds the maximum (the second threshold you enter). The Zyxel Device stops sending alerts when the memory usage drops back below the minimum threshold (the first threshold you enter). The no command changes the setting back to the default.
app-watch-dog reboot-log flush	Flushes the reboot log record.

Table 348 app-watchdog Commands

COMMAND	DESCRIPTION
`[no] app-watch-dog sys-reboot`	If auto recover fail reaches the maximum retry count, app-watch-dog reboots the device. The no command turns off system auto reboot.
`show app-watch-dog config`	Displays the application watchdog timer settings.
`show app-watch-dog monitor-list`	Display the list of applications that the application watchdog is monitoring.
`show app-watch-dog reboot-log`	Displays the application watchdog reboot log.

72.2.3.1 Application Watchdog Commands Example

The following example displays the application watchdog configuration and lists the processes that the application watchdog is monitoring.

```
Application Watch Dog Setting:
  activate: yes
  alert: yes
  console print: always
  retry count: 3
  auto recover: yes
  system reboot: yes
  interval: 60 seconds
  mem threshold: 80% ~ 90%
  cpu threshold: 80% ~ 90%
  disk threshold: 80% ~ 90%
Router(config)# show app-watch-dog monitor-list
#app_name       min_process_count       max_process_count(-1 unlimited) recover_enable  recover_reboot  recover_always  recover_max_try_count   recover_max_fail_count
uamd                    1                               -1                      1               2               1               1                       3
firewalld               1                               -1                      0               1               1               1                       3
policyd                 1                               -1                      1               1               1               1                       3
contfltd                1                               -1                      1               1               1               1                       3
classify                1                               -1                      0               1               1               1                       3
ospfd                   1                               -1                      0               1               1               1                       3
ripd                    1                               -1                      0               1               1               1                       3
resd                    1                               -1                      0               1               1               1                       3
zyshd_wd                1                               -1                      0               1               1               1                       3
zyshd                   1                               -1                      0               0               1               1                       3
httpd                   1                               -1                      1               1               1               1                       3
dhcpd                   1                               -1                      1               1               1               1                       3
sshipsecpm              1                               -1                      1               1               1               1                       3
zylogd                  1                               -1                      0               1               1               1                       3
syslog-ng               1                               -1                      0               1               1               1                       3
zylogger                1                               -1                      0               1               1               1                       3
ddns_had                1                               -1                      0               1               1               1                       3
tpd                     1                               -1                      0               1               1               1                       3
wdtd                    1                               -1                      0               1               1               1                       3
zebra                   1                               -1                      0               1               1               1                       3
link_updown             1                               -1                      0               1               1               1                       3
fauthd                  1                               -1                      0               1               1               1                       3
pro                     1                               -1                      0               1               1               1                       3
signal_wrapper          1                               -1                      0               1               1               1                       3
asd                     1                               -1                      0               1               1               1                       3
ctipd.bin               1                               -1                      1               1               1               1                       3
ipmonitord              1                               -1                      0               1               1               1                       3
```

72.3 Conserve Memory

The Zyxel Device throughput may be slow if dynamic memory usage is reaching a maximum. Conserve Memory allows Zyxel Device to free up memory by omitting certain security scans.

Note: Enabling this feature is not recommended, as it might reduce the security of your network.

Conserve Memory is supported on ZyWALL USG (Unified Security Gateway) models only. This does not include USG FLEX models. For a full list of USG models, see Section 1.1 on page 26.

72.3.1 Converse Memory Settings

To converse dynamic memory, enable one or both of the following settings:

- AV Cloud Query Bypass: Traffic passing through the Zyxel Device is not scanned by Anti-Virus (express mode).
- UTM Features Bypass: Traffic passing through the Zyxel Device is not scanned by the following services: IDP, ADP, App Patrol, Anti-Virus (stream mode).

72.3.2 Conserve Memory Commands

The following table lists the Conserve Memory commands.

Table 349 Conserve Memory Commands

COMMAND	DESCRIPTION
`show mem-conserve status`	Displays all Conserve Memory settings.
`[no] mem-conserve activate`	Enables or disables the Conserve Memory feature.
`[no] mem-conserve av-bypass falling-threshold <1..4000>`	Sets the on threshold for AV Cloud Query Bypass, in Megabytes (MB). When the available memory of the Zyxel Device is equal to this value, the Zyxel Device enables AV Cloud Query Bypass mode.
`[no] mem-conserve av-bypass rising-threshold <1..4000>`	Sets the off threshold for AV Cloud Query Bypass, in Megabytes (MB). When the available memory of the Zyxel Device is equal to this value, the Zyxel Device disables AV Cloud Query Bypass mode.
`[no] mem-conserve av-bypass sustained-time <1..60>`	Sets the minimum amount of time, in minutes, that AV Cloud Query Bypass stays enabled after reaching the falling threshold. If available memory reaches the rising threshold during this time period, AV Cloud Query Bypass is not disabled.
`[no] mem-conserve utm-bypass falling-threshold <1..4000>`	Sets the on threshold for UTM Features Bypass, in Megabytes (MB). When the available memory of the Zyxel Device is equal to this value, the Zyxel Device enables UTM Features Bypass mode.

Table 349 Conserve Memory Commands

COMMAND	DESCRIPTION
`[no] mem-conserve utm-bypass rising-threshold <1..4000>`	Sets the off threshold for UTM Features Bypass, in Megabytes (MB). When the available memory of the Zyxel Device is equal to this value, the Zyxel Device disables UTM Features Bypass mode.
`[no] mem-conserve utm-bypass sustained-time <1..60>`	Sets the minimum amount of time, in minutes, that UTM Features Bypass stays enabled after reaching the falling threshold. If available memory reaches the rising threshold during this time period, UTM Features Bypass is not disabled.

72.3.3 Conserve Memory Example

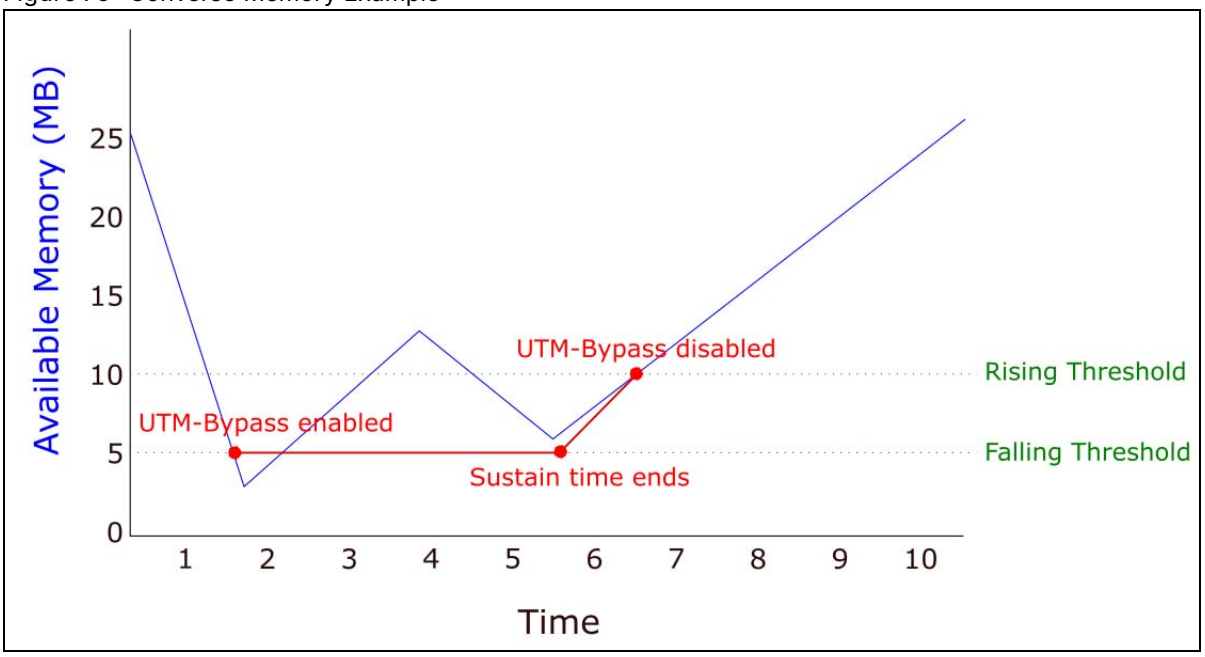
In this example, the Zyxel Device is set to bypass UTM security services if available memory drops to 5 MB, for a minimum of 4 seconds. The UTM security services bypass will be disabled if available memory increases to 10 MB.

Figure 74 Conserve Memory: Example

```
Router# configure terminal
Router(config)# mem-conserve utm-bypass falling-threshold 5
Router(config)# mem-conserve utm-bypass rising-threshold 10
Router(config)# mem-conserve utm-bypass sustained-time 4
```

The following figure shows the result of these commands:

Figure 75 Converse Memory Example



72.4 GUI Visibility

The GUI visibility commands show or hide advanced features in the web configurator.

Table 350 gui-visibility Commands

COMMAND	DESCRIPTION
`[no] gui-visibility gui-visibility policy-route-fromlocal-snat`	Allows you to configure Source Network Address Translation (SNAT) when Incoming interface is set to "ZyWALL" in the Web Configurator at Configuration > Network > Routing > Policy Route > Add/Edit Policy Route. The no command prevents this setting from being configured. Note: This command is available in ZLD firmware 5.0 and later.
`[no] gui-visibility show-advanced`	Expands all the advanced features in the web configurator, so you don't need to click each one open individually.
`show gui-visability status`	Displays the current GUI visibility settings.

72.5 Google Analytics

Enable the Google Analytics command to allow Google Analytics to track an administrator's use of the web configurator, such as clicking on a specific field or button, or enabling/disabling specific features. Use the `configure terminal` command to enter the configuration mode to be able to use these commands.

Table 351 Google Analytics Commands

COMMAND	DESCRIPTION
`[no] web-google-analytics activate`	Allows the Zyxel Device to collect and send the web configurator usage data to Google Analytics. By default this is enabled. The no command disables this setting.
`show web-google-analytics status`	Displays if the Zyxel Device is allowed to collect and send the web configurator usage data to Google Analytics.

CHAPTER 73
Managed AP Commands

73.1 Managed Series AP Commands Overview

Connect directly to a managed AP's CLI (Command Line Interface) to configure the managed AP's CAPWAP (Control And Provisioning of Wireless Access Points) client and DNS server settings.

Log into an AP's CLI and use the commands in this chapter if the AP does not automatically connect to the Zyxel Device or you need to configure the AP's DNS server. Use the CAPWAP client commands to configure settings to let the AP connect to the Zyxel Device. Use the DNS server commands to configure the DNS server address to which the AP connects. When the AP reboots, it only keeps the configuration from commands covered in this chapter.

73.2 Accessing the AP CLI

Connect to the AP's console port and use a terminal emulation program or connect through the network using Telnet or SSH. The settings and steps for logging in are similar to connecting to the Zyxel Device. See Section 1.2 on page 28 for details.

Note: The AP's default login username is admin and password is 1234. The username and password are case-sensitive. If the AP has connected to the Zyxel Device, the AP uses the same admin password as the Zyxel Device.

Use the `write` command to save the current configuration to the Zyxel Device.

Note: Always save the changes before you log out after each management session. All unsaved changes will be lost after the system restarts.

73.3 CAPWAP Client Commands

Use the CAPWAP client commands to configure the AP's IP address and other related management interface settings. Do not use the original interface commands to configure the IP address and related settings on the AP, because the AP does not save interface command settings after rebooting.

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 352 Input Values for CAPWAP Client Commands

LABEL	DESCRIPTION
ip	IPv4 address.
netmask	The network subnet mask. For example, 255.255.255.0.

Table 352 Input Values for CAPWAP Client Commands (continued)

LABEL	DESCRIPTION
gateway	The default gateway IP address of the interface. Enter a standard IPv4 IP address (for example, 127.0.0.1).
primary_ac_ap	The primary IPv4 address of the Zyxel Device.
secondary_ac_ap	Optional IPv4 address of the Zyxel Device.
vid	The VLAN ID (1~4094) of the managed AP.
primary_ac_dns	The primary fully qualified domain name (FQDN) of the Zyxel Device.
secondary_ac_dns	The secondary fully qualified domain name (FQDN) of the Zyxel Device.

The following table describes commands for configuring the AP's CAPWAP client parameters, which include the management interface. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 353 Command Summary: CAPWAP Client

COMMAND	DESCRIPTION
`capwap ap vlan ip address` *`ip netmask`*	Sets the IP address and network mask of the AP's management interface.
`capwap ap vlan ip gateway` *`gateway`*	Sets the default gateway IP address for the AP's management interface.
`capwap ap vlan no ip gateway`	Clears the default gateway IP address setting for the AP's management interface.
`capwap ap vlan vlan-id` *`vid`* `{ tag | untag }`	Sets the AP's management VLAN ID as well as whether the AP sends tagged or untagged packets. The management VLAN on the Zyxel Device and AP must match for the Zyxel Device to manage the AP. The Zyxel Device's force vlan command (see Table 14 on page 57) takes priority over this command.
`capwap ap ac-ip` *`{primary_ac_ip|primary_ac_dns} {secondary_ac_ip|secondary_ac_dns}`*	Specifies the primary and secondary IP address or domain name of the AP controller (the Zyxel Device) to which the AP connects.
`capwap ap ac-ip auto`	Sets the AP to use DHCP to get the address of the AP controller (the Zyxel Device).
`show capwap ap info`	Displays the IP address of the Zyxel Device managing the AP and CAPWAP settings and status.
`show capwap ap discovery-type`	Displays how the AP finds the Zyxel Device.
`show capwap ap ac-ip`	Displays the address of the Zyxel Device or `auto` if the AP finds the Zyxel Device through broadcast packets.

73.3.1 CAPWAP Client Commands Example

This example shows how to configure the AP's management interface and how it connects to the AP controller (the Zyxel Device), and check the connecting status. The following commands:

- Display how the AP finds the Zyxel Device
- Set the AP's management IP address to 192.168.1.37 and netmask 255.255.255.0
- Set the AP's default gateway IP address to 192.168.1.32
- Sets the AP's management interface to use VLAN ID 2 and send tagged packets

- Specifies the primary and secondary IP addresses of the Zyxel Device (192.168.1.1 and 192.168.1.2) to which the AP connects.
- Displays the settings it configured

```
Router# configure terminal
Router(config)# show capwap ap discovery-type
Discovery type : Broadcast
Router(config)# capwap ap vlan ip address 192.168.1.37 255.255.255.0
Router(config)# capwap ap vlan ip gateway 192.168.1.32
Router(config)# capwap ap vlan vlan-id 2 tag
Router(config)# capwap ap ac-ip 192.168.1.1 192.168.1.2
Router(config)# show capwap ap discovery-type
Discovery type : Static AC IP
Router(config)# show capwap ap ac-ip
AC IP: 192.168.1.1 192.168.1.2
Router(config)# exit
Router# show capwap ap info
                AC-IP                   192.168.1.1
       Discovery type                   Static AC IP
             SM-State                   RUN(8)
        msg-buf-usage                   0/10 (Usage/Max)
       capwap-version                   10118
         Radio Number                   1/4 (Usage/Max)
           BSS Number                   8/8 (Usage/Max)
              IANA ID                   037a
          Description                   AP-0013499999FF
```

73.4 DNS Server Commands

The following table describes commands for configuring the AP's DNS server. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 354 Command Summary: DNS Server

COMMAND	DESCRIPTION
`ip dns server zone-forwarder {<1..32>|append|insert <1..32>} {`*`domain_zone_name`*`|*} {interface `*`interface_name`*` | user-defined `*`ipv4_address`*` [interface {`*`interface_name`*` | auto}]}`	Sets a domain zone forwarder record that specifies a fully qualified domain name. You can also use a asterisk (*) if all domain zones are served by the specified DNS server(s). *`domain_zone_name`*: This is a domain zone, not a host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name. So whenever the Zyxel Device receives needs to resolve a zyxel.com.tw domain name, it can send a query to the recorded name server IP address. *`interface_name`*: This is the interface through which the ISP provides a DNS server. The interface should be activated and set to be a DHCP client. `auto`: any interface that the Zyxel Device uses to send DNS queries to a DNS server according to the routing rule.
`ip dns server zone-forwarder move <1..32> to <1..32>`	Changes the index number of a zone forwarder record.
`no ip dns server zone-forwarder <1..4>`	Removes the specified zone forwarder record.

73.4.1 DNS Server Commands Example

This example configures the AP to connect to the AP controller (the Zyxel Device) by DNS. The following commands:

- Set the AP's management IP address to 192.168.1.100 and netmask 255.255.255.0
- Sets the AP's management interface to use VLAN ID 3
- Set the AP's default gateway IP address to 192.168.1.1
- Add a domain zone forwarder record that specifies a DNS server's IP address of 10.1.1.1 and uses the bridge 0 interface to send queries to that DNS server
- Set the AP controller's primary domain name as capwap-server.zyxel.com and secondary domain name as capwap.test.com

```
Router(config)# capwap ap vlan ip address 192.168.1.100 255.255.255.0
Router(config)# capwap ap vlan vlan-id 3
Router(config)# capwap ap vlan ip gateway 192.168.1.1
Router(config)# ip dns server zone-forwarder append * user-defined 10.1.1.1
interface br0
Router(config)# capwap ap ac-ip capwap-server.zyxel.com capwap.test.com
```

73.4.2 DNS Server Commands and DHCP

The AP in the example in Section 73.4.1 on page 607 uses a static IP address. If the AP uses DHCP instead, you do not need to configure the DNS server's IP address on the AP when you configure DHCP option 6 on the DHCP server. For the example in Section 73.4.1 on page 607, you would just need to configure the management interface's VLAN ID (`capwap ap vlan vlan-id 3`).

List of Commands (Alphabetical)

This section lists the commands and sub-commands in alphabetical order. Commands and subcommands appear at the same level.

ap internal-auth shared-secret *key* 60
geo-ip [no] geography <*country_code*> all address {*ipv4* | *ip6*} 465
(no) bootfile-name <*filename*> 130
(no) bootp-server <*w.x.y.z*> 130
(no) cnm-agent enable-cnm-id 241
(no) remote-assistance activate 580
[isakmp_algo]] 289
[isakmp_algo]] 291
[no]logging mail <1..2> tls authenticate-server 569
[no] {*ipv4* | *ipv4_cidr* | *ipv4_range* | *wildcard_domainname* | *tld* |*ipv6* | *ipv6_range* | *ipv6_prefix* } 370
[no] {*ipv4* | *ipv4_cidr* | *ipv4_range* | *wildcard_domainname* | *top_level_domain*} 333
[no] 2g-scan-channel *wireless_channel_2g* 84
[no] 5g-scan-channel *wireless_channel_5g* 84
[no] 8021x-sso 257
[no] aaa authentication *profile-name* 479
[no] aaa group server ad *group-name* 474
[no] aaa group server ldap *group-name* 476
[no] aaa group server radius *group-name* 477
[no] access-page color-window-background 511
[no] access-page message-text *message* 511
[no] account {pppoe | pptp} *profile_name* 498
[no] account cellular *profile_name* 499
[no] account l2tp *profile_name* 303
[no] account *profile_name* 140
[no] activate 100
[no] activate 197
[no] activate 203
[no] activate 215
[no] activate 215
[no] activate 221
[no] activate 230
[no] activate 231
[no] activate 231
[no] activate 234
[no] activate 256
[no] activate 264
[no] activate 274
[no] activate 275
[no] activate 286
[no] activate 296
[no] activate 308
[no] activate 490
[no] activate 518
[no] activate 574
[no] activate 78
[no] activate 84
[no] activate 97
[no] additional-ddns-options 188
[no] address *address_object* 231

[no] address6 *address6_object* 231
[no] address6-object *object_name* {*ipv6_address* | *ipv6_range* | *ipv6_subnet*} 460
[no] address6-object OBJECT_NAME interface-ip interface {dhcpv6 | link-local | slaac | static} {addr_index} 460
[no] address6-object *object_name* interface-subnet *interface* {dhcpv6 | slaac | static} {*addr_index*} 460
[no] address-object *object_name* 463
[no] ad-server basedn *basedn* 472
[no] ad-server binddn *binddn* 473
[no] ad-server cn-identifier *uid* 473
[no] ad-server host *ad_server* 473
[no] ad-server password *password* 473
[no] ad-server password-encrypted *password* 473
[no] ad-server port *port_no* 473
[no] ad-server search-time-limit *time* 473
[no] ad-server ssl 473
[no] advertisement activate 276
[no] advertisement name *description* url *url* 276
[no] ampdu 78
[no] amsdu 78
[no] anti-botnet log [alert] 331
[no] anti-botnet statistics collect 338
[no] anti-botnet update auto 337
[no] anti-spam black-list [*rule_number*] e-mail *email* {activate|deactivate} 405
[no] anti-spam black-list [rule_number] ip6-address ipv6_subnet {activate|deactivate} 405
[no] anti-spam black-list [*rule_number*] ip-address *ip subnet_mask* {activate|deactivate} 405
[no] anti-spam black-list [*rule_number*] mail-header *mail-header mail-header-value* {activate|deactivate} 405
[no] anti-spam black-list [*rule_number*] subject *subject* {activate|deactivate} ... 405
[no] anti-spam black-list activate 404
[no] anti-spam dnsbl activate 407
[no] anti-spam ip-reputation activate 400
[no] anti-spam ip-reputation private-check activate 400
[no] anti-spam mail-content activate 400
[no] anti-spam mail-phishing activate 400
[no] anti-spam statistics collect 409
[no] anti-spam virus-outbreak activate 401
[no] anti-spam white-list [*rule_number*] e-mail *email* {activate|deactivate} 404
[no] anti-spam white-list [rule_number] ip6-address ipv6_subnet {activate|deactivate} 404
[no] anti-spam white-list [*rule_number*] ip-address *ip subnet_mask* {activate|deactivate} 404
[no] anti-spam white-list [*rule_number*] mail-header *mail-header mail-header-value* {activate|deactivate} 404
[no] anti-spam white-list [*rule_number*] subject *subject* {activate|deactivate} ... 404
[no] anti-spam white-list activate 404
[no] anti-spam xheader {white-list | black-list} *mail-header mail-header-value* .. 405
[no] anti-spam xheader dnsbl *mail-header mail-header-value* 408
[no] anti-spam xheader query-timeout *xheader-name xheader-value* 401
[no] anti-virus activate 317
[no] anti-virus black-list activate 319
[no] anti-virus cloud-query activate 317
[no] anti-virus cloud-query ftype-identify *file_type* 317
[no] anti-virus eicar activate 317
[no] anti-virus skip-unknown-file-type activate 317
[no] anti-virus statistics collect 323
[no] anti-virus update auto 322
[no] anti-virus white-list activate 320
[no] ap-group-profile *ap_group_profile_name* 70
[no] ap-mode detection activate 67
[no] apn *access_point_name* 499

[no] app <profile-name> 313
[no] app log_sid 314
[no] app statistics collect 314
[no] app update auto 314
[no] application <sid> 455
[no] application application_object 296
[no] application-object <object> 456
[no] app-profile <profile name> {[no log]|[log by-profile]} {activate | deactivate} 223
[no] app-watch-dog activate 598
[no] app-watch-dog alert 598
[no] app-watch-dog auto-recover 598
[no] app-watch-dog console-print {always|once} 598
[no] app-watch-dog cpu-threshold min <1..100> max <1..100> 598
[no] app-watch-dog disk-threshold min <1..100> max <1..100> 598
[no] app-watch-dog interval <6..300> 598
[no] app-watch-dog mem-threshold min <1..100> max <1..100> 598
[no] app-watch-dog retry-count <1..5> 598
[no] app-watch-dog sys-reboot 599
[no] area IP [{stub | nssa}] 178
[no] area IP authentication 178
[no] area IP authentication authentication-key *authkey* 178
[no] area IP authentication message-digest 178
[no] area IP authentication message-digest-key <1..255> md5 *authkey* 178
[no] area IP virtual-link IP 178
[no] area IP virtual-link IP authentication 178
[no] area IP virtual-link IP authentication authentication-key *authkey* 178
[no] area IP virtual-link IP authentication message-digest 178
[no] area IP virtual-link IP authentication message-digest-key <1..255> md5 *authkey* 178
[no] area IP virtual-link IP authentication same-as-area 178
[no] area IP virtual-link IP authentication-key *authkey* 178
[no] area IP virtual-link IP encrypted-authentication-key *<ciphertext>* 178
[no] as-number <1..4294967295> 181
[no] as-profile <profile name> {[no log]|[log by-profile]} {activate | deactivate} 223
[no] authentication {chap-pap | chap | pap | mschap | mschap-v2} 498
[no] authentication {force | required} 256
[no] authentication {none | pap | chap} 500
[no] authentication mode {md5 | text} 177
[no] authentication string *authkey* 177
[no] auth-server activate 490
[no] auth-server activate 518
[no] auth-server cert *certificate_name* 490
[no] auth-server cert *certificate_name* 518
[no] auth-server trusted-client *profile_name* 490
[no] auth-server trusted-client *profile_name* 518
[no] auto-destination 168
[no] auto-disable 168
[no] auto-healing activate 110
[no] av-profile <profile name>{[no log]|[log by-profile]} {activate | deactivate} 223
[no] backmx 187
[no] backup-custom *ip* 187
[no] backup-iface *interface_name* 187
[no] band {auto|wcdma|gsm|lte} 142
[no] bandwidth activate 264
[no] bandwidth activate 508
[no] billing discount activate 263
[no] billing discount unit <2..10> price *price* 263
[no] billing profile *profile_name* 263
[no] billing replenish activate 263
[no] billing tax-rate activate 263

[no] billing wlan-ssid-profile *profile_name* 263
[no] bind *interface_name* 140
[no] block-ack 79
[no] broadcast 83
[no] broadcast 84
[no] budget active 142
[no] budget data active {download-upload|download|upload} <1..100000> 143
[no] budget time active <1..672> 142
[no] bwm activate 168
[no] bwm activate 307
[no] bwm highest sip bandwidth priority 308
[no] bypass {ip-reputation | mail-content | virus-outbreak} 400
[no] bypass {white-list | black-list | dnsbl} 400
[no] bypass {white-list | black-list} 318
[no] bypass mail-phishing 400
[no] bypass-firewall activate 209
[no] capwap activate 57
[no] case-sensitive 475
[no] case-sensitive 476
[no] case-sensitive 477
[no] category <category_name> 421
[no] cdr activate 413
[no] cdr block block-wireless-client 413
[no] cdr counter-reset activate 413
[no] cdr update auto 416
[no] cdr white-list ipv4 *ip_address* 415
[no] cdr white-list mac *mac_address* 415
[no] certificate *cert_name* 422
[no] cf-profile <profile name> {[no log]|[log by-profile]} {activate | deactivate} 223
[no] client-identifier *mac_address* 128
[no] client-name *host_name* 128
[no] clock auto-sync-daylight-saving 513
[no] clock auto-sync-timezone 513
[no] clock daylight-saving 513
[no] clock saving-interval begin {apr|aug|dec|feb|jan|jul|jun|mar|may|nov|oct|sep}
{1|2|3|4|last} {fri|mon|sat|sun|thu|tue|wed} *hh:mm* end
{apr|aug|dec|feb|jan|jul|jun|mar|may|nov|oct|sep} {1|2|3|4|last}
{fri|mon|sat|sun|thu|tue|wed} *hh:mm* offset 513
[no] clock time-zone {-|+*hh:mm*} [+|-]HH:MM. 513
[no] cloud-helper firmware update auto 551
[no] cloud-helper-notify activate 552
[no] cnm-agent acs password *tr069_acs_password* 242
[no] cnm-agent acs username *tr069_acs_username* 242
[no] cnm-agent activate 241
[no] cnm-agent authentication enable 242
[no] cnm-agent auto-get-acs activate 241
[no] cnm-agent auto-get-acs activate 242
[no] cnm-agent cnm-id <ID> 241
[no] cnm-agent encrypted-xmpp-password 243
[no] cnm-agent manager {https_url|http_url} 242
[no] cnm-agent password 242
[no] cnm-agent periodic-inform activate 242
[no] cnm-agent periodic-inform interval *<10…86400>* 242
[no] cnm-agent trigger-inform *<0..8640>* 242
[no] cnm-agent username 243
[no] cnm-agent vantage certificate *tr069_cert_file_name* 242
[no] cnm-agent xmpp-domain *xmpp_domain* 243
[no] cnm-agent xmpp-host *xmpp_host* 243
[no] cnm-agent xmpp-password *xmpp_password* 243

[no] cnm-agent xmpp-resource *xmpp_resource* 243
[no] cnm-agent xmpp-username *xmpp_username* 243
[no] compression {yes | no} 498
[no] config-backup scheduler activate 596
[no] configuration-payload-provide {first-dns IPv6|second-dns IPv6} 283
[no] configuration-payload-provide {first-dns IPv6|second-dns IPv6} 293
[no] configuration-payload-provide activate 283
[no] configuration-payload-provide activate 293
[no] connection-id *connection_id* 499
[no] connectivity {nail-up | dial-on-demand} 140
[no] connectivity-check continuous-log activate 135
[no] connectivity-check continuous-log activate 566
[no] console baud *baud_rate* 514
[no] contain *ap_mac* 100
[no] content-filter block message *message* 369
[no] content-filter block redirect *redirect_url* 369
[no] content-filter https-domain-filter activate 370
[no] content-filter https-domain-filter block-page activate 374
[no] content-filter profile *<filtering_profile>* safesearch 374
[no] content-filter profile *filtering_profile* 371
[no] content-filter profile *filtering_profile* category {category_name} 372
[no] content-filter profile *filtering_profile* commtouch-url category {category_name} 372
[no] content-filter profile *filtering_profile* custom 371
[no] content-filter profile *filtering_profile* custom activex 371
[no] content-filter profile *filtering_profile* custom cookie 371
[no] content-filter profile *filtering_profile* custom java 372
[no] content-filter profile *filtering_profile* custom proxy 372
[no] content-filter profile *filtering_profile* custom trust-allow-features 372
[no] content-filter profile *filtering_profile* custom trust-only 372
[no] content-filter profile *filtering_profile* log-level-info 371
[no] content-filter profile *filtering_profile* url-server 371
[no] content-filter safesearch *<name>* 375
[no] content-filter service-timeout *service_timeout* 372
[no] content-filter sslv3 action block 371
[no] content-filter sslv3 action block 374
[no] content-filter statistics collect 376
[no] corefile copy usb-storage 149
[no] cpu-temperature-monitor activate 52
[no] crypto boost-tcp 278
[no] crypto ignore-df-bit 281
[no] crypto map *map_name* 281
[no] crypto map *map_name* 292
[no] crypto *map_name* 286
[no] crypto *map_name* 294
[no] crypto *profile_name* 184
[no] ctmatch {dnat | snat} 222
[no] ctsrts <0..2347> 80
[no] custom *ip* 187
[no] dcs activate 80
[no] ddns-server {FQDN DNS} 188
[no] deactivate 168
[no] deactivate 170
[no] default-router *ip* 129
[no] description *<description>* 230
[no] description <description> 455
[no] description <description> 456
[no] description *description* 119
[no] description *description* 129
[no] description *description* 168

[no] description *description* 170
[no] description *description* 216
[no] description *description* 222
[no] description *description* 231
[no] description *description* 232
[no] description *description* 257
[no] description description 296
[no] description *description* 308
[no] description DESCRIPTION 313
[no] description *description* 422
[no] description *description* 446
[no] description *description* 464
[no] description *description* 469
[no] description *description* 491
[no] description *description* 518
[no] destination {*address6_object*|any} 170
[no] destination {*address_object* | *group_name*} 257
[no] destination {*address_object*|any} 168
[no] destination *address_object* 308
[no] destinationip <profile name> 230
[no] destinationip *address_object* 222
[no] destinationip6 *address_object* 222
[no] device block mac <mac address> 439
[no] device identify activate 439
[no] device mac <mac address> description <description> 439
[no] device profile <profile name> 439
[no] device profile <profile name> category <category> 440
[no] device profile <profile name> description <description> 440
[no] device profile <profile name> os <os> 440
[no] device-ha activate 430
[no] device-ha ap-mode authentication {string *key* | ah-md5 *key*} 431
[no] device-ha ap-mode backup sync authentication password *password* 432
[no] device-ha ap-mode backup sync auto 432
[no] device-ha ap-mode backup sync from *master_address* port *port* 432
[no] device-ha ap-mode backup sync interval <5..1440> 432
[no] device-ha ap-mode *interface_name* activate 431
[no] device-ha ap-mode *interface_name* manage-ip *ip subnet_mask* 431
[no] device-ha ap-mode master sync authentication password *password* 432
[no] device-ha ap-mode preempt 431
[no] device-ha2 activate 434
[no] device-ha2 connchk-monitor 435
[no] device-ha2 disable-session-sync 434
[no] device-ha2 *interface_name* activate 434
[no] device-ha2 manage-ip *ip1 ip2 subnet_mask* 434
[no] device-ha2 srv-monitor 435
[no] device-ha2 sync password 434
[no] diag-info copy usb-storage 149
[no] dial-string *isp_dial_string* 499
[no] disable-bss-color 79
[no] disable-dfs-switch 81
[no] dns-content-filter black-list activate 377
[no] dns-content-filter statistics collect 379
[no] dns-content-filter white-list activate 377
[no] dns-filter black-list activate 341
[no] dns-filter drop-malform-packet activate 341
[no] dns-filter drop-malform-packet log 341
[no] dns-filter statistics collect 342
[no] dns-filter white-list activate 342
[no] domain-name *domain_name* 129

[no] domainname *domain_name* 512
[no] domain-name *walled_garden_fqdn* 275
[no] dot11n-disable-coexistence 81
[no] downstream <0..1048576> 119
[no] downstream <0..1048576> 148
[no] downstream <0..1048576> 159
[no] dpd 279
[no] dscp {<0..63> | any | class {af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs0 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | default | wmm_be0 | wmm_be24 | wmm_bk16 | wmm_bk8 | wmm_vi32 | wmm_vi40 | wmm_vo48 | wmm_vo56}} 308
[no] dscp {any | <0..63>} 168
[no] dscp {any | <0..63>} 170
[no] dscp class {default | *dscp_class*} 168
[no] dscp class {default | *dscp_class*} 170
[no] duplex <full | half> 138
[no] dynamic-guest *user_name* 508
[no] eap type {server AAA_method user-id {name|any}| client name username {password PASSWORD| encrypted-password PASSWORD} 290
[no] eap type {server auth_method user-id {name|any}| client name username {password PASSWORD| encrypted-password *password*} 291
[no] encryption {nomppe | mppe-40 | mppe-128} 499
[no] entry {IPv4 | IPv4_CIDR | IPv4_RANGE | IPv6 | IPv6_PREFIX | IPv6_RANGE | SSL_INSPECTION_WILDCARD_CNAME} 421
[no] error-url *url* 255
[no] fall-back 279
[no] fall-back 289
[no] fall-back 291
[no] fbwifi activate 258
[no] fbwifi idle-detection 258
[no] file-decompression [unsupported destroy] 318
[no] firewall-output activate 229
[no] firewall-output default-rule establish enable 229
[no] first-dns-server {*ip* | *interface_name* {1st-dns | 2nd-dns | 3rd-dns} | ZyWALL} 129
[no] first-wins-server *ip* 129
[no] flood-detection {tcp-flood | udp-flood | icmp-flood | igmp-flood} {activate | log [alert] | block} 235
[no] *forbid_hosts* 371
[no] force 257
[no] force vlan 70
[no] force-mu-mimo 81
[no] frag <256..2346> 81
[no] frame-capture activate 107
[no] free-time activate 271
[no] free-time auto-login 271
[no] free-time deliver-method onscreen 271
[no] free-time deliver-method sms 271
[no] free-time maximum-allowed-account <1..2000> 271
[no] free-time maximum-register-number <1..5> 271
[no] free-time reset-register *hh:mm* 271
[no] free-time time-period *time_period* 271
[no] from *zone_object* 222
[no] geo-ip database update auto 465
[no] google-auth 257
[no] groupname *groupname* 446
[no] groupname *groupname* 446
[no] gui-visibility gui-visibility policy-route-fromlocal-snat 603
[no] gui-visibility show-advanced 603
[no] ha-iface *interface_name* 187
[no] hardware-address *mac_address* 128
[no] hardware-watchdog-timer <4..37> 597

[no] hash-auto 199
[no] health-check activate 198
[no] hidden 274
[no] host *hostname* 187
[no] host *ip* 128
[no] hostname *hostname* 512
[no] htprotect 81
[no] https enable-sni 199
[no] icmp-decoder {bad-icmp-l4-size | icmp-fragment | icmp-smurf} activate 235
[no] idle <0..360> 498
[no] idle <0..360> 500
[no] idp 349
[no] idp anomaly white-list activate 237
[no] idp signature update auto 359
[no] idp statistics collect 360
[no] idp-profile <profile name> {[no log]|[log by-profile]} {activate | deactivate} 223
[no] igmp activate 160
[no] igmp direction {upstream | downstream} 160
[no] ignore-country-ie 81
[no] ikev2 policy policy_name 289
[no] ikev2 policy6 policy_name 290
[no] inbound ceiling {<0..1048576> | maximize-bandwidth-usage} 309
[no] inbound guarantee-bandwidth <0..1048576> priority <1..7> 309
[no] inbound-dscp-mark {<0..63> | class {af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs0 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | default | wmm_be0 | wmm_be24 | wmm_bk16 | wmm_bk8 | wmm_vi32 | wmm_vi40 | wmm_vo48 | wmm_vo56}} 309
[no] incoming-interface {interface *interface_name* | trunk *group_name*} 309
[no] in-dnat activate 283
[no] infected-action {destroy | send-win-msg} 318
[no] in-snat activate 283
[no] interface {*num*|*interface-name*} 164
[no] interface *interface_name* 119
[no] interface *interface_name* 142
[no] interface *interface_name* 169
[no] interface *interface_name* 170
[no] interface *interface_name* 184
[no] interface *interface_name* 203
[no] interface *interface_name* 215
[no] interface *interface_name* 272
[no] interface *tunnel_iface* 147
[no] interface-group *group-name* 163
[no] internal-welcome-url *url* 255
[no] ip <w.x.y.z> 259
[no] ip address dhcp 119
[no] ip address *ip subnet_mask* 119
[no] ip address *ip subnet_mask* 159
[no] ip address *ip subnet_mask* 490
[no] ip address *ip subnet_mask* 518
[no] ip ddns profile *profile_name* 187
[no] ip dhcp pool *profile_name* 128
[no] ip dhcp-pool *profile_name* 130
[no] ip dns server a-record *fqdn w.x.y.z* 515
[no] ip dns server mx-record *domain_name {w.x.y.z|fqdn}* 515
[no] ip dns server zone-forwarder {<1..32>|append|insert <1..32>} {*domain_zone_name*|*} interface *interface_name* 516
[no] ip ftp server 534
[no] ip ftp server cert *certificate_name* 534
[no] ip ftp server cipher-suite {3des| des| rc4| dhe} 534
[no] ip ftp server port <1..65535> 534

[no] ip ftp server tls-required 534
[no] ip gateway *ip* 119
[no] ip helper-address *ip* 130
[no] ip http authentication *auth_method* 527
[no] ip http content-security-policy 527
[no] ip http port <1..65535> 527
[no] ip http secure-port <1..65535> 527
[no] ip http secure-server 527
[no] ip http secure-server auth-client 527
[no] ip http secure-server cert *certificate_name* 528
[no] ip http secure-server force-redirect 528
[no] ip http secure-server sslv3 528
[no] ip http server 528
[no] ip http x-frame-options 529
[no] ip ipnp activate 272
[no] ip ospf {authentication-key *key8* | encrypted-authentication-key *encrypted_str*} 160
[no] ip ospf authentication [message-digest | same-as-area] 160
[no] ip ospf authentication-key *password* 134
[no] ip ospf cost <1..65535> 134
[no] ip ospf dead-interval <1..65535> 134
[no] ip ospf hello-interval <1..65535> 134
[no] ip ospf message-digest-key <1..255> {md5 *dr_authkey_16* | encrypted-md5 *encrypted_str*} 160
[no] ip ospf priority <0..255> 134
[no] ip ospf priority *priority* 159
[no] ip ospf retransmit-interval <1..65535> 134
[no] ip proxy-arp {*ipv4* | *ipv4_range* | *ipv4_cidr*} 126
[no] ip proxy-arp activate 126
[no] ip rip {send | receive} version <1..2> 133
[no] ip rip {send | receive} version <1..2> [1.2] 160
[no] ip v2-broadcast 133
[no] ip route {*w.x.y.z*} {*w.x.y.z*} {*interface*|*w.x.y.z*} <0..127> 174
[no] ip route control-virtual-server-rules activate 174
[no] ip ssh server 531
[no] ip ssh server cert *certificate_name* 531
[no] ip ssh server kexalg dhe 532
[no] ip ssh server port <1..65535> 531
[no] ip ssh server v1 532
[no] ip telnet server 532
[no] ip telnet server port <1..65535> 532
[no] ip v2-broadcast 160
[no] ip-address <*w.x.y.z*>/<*1..32*> 275
[no] ip-address *ip* 216
[no] ip-decoder {ip-spoof | ip-teardrop} action {drop | reject-sender | reject-receiver | reject-both} 236
[no] ip-decoder {ip-spoof | ip-teardrop} activate 236
[no] ip-decoder {ip-spoof | ip-teardrop} log 236
[no] ip-reputation black-list activate 328
[no] ip-reputation ebl activate 330
[no] ip-reputation ebl update auto 330
[no] ip-reputation log [alert] 327
[no] ip-reputation log-all 327
[no] ip-reputation statistics collect 329
[no] ip-reputation system-protect activate 327
[no] ip-reputation update auto 329
[no] ip-reputation webroot incoming-category {botnets | denial-of-service | exploits | phishing | proxy | reputation | scanners | spam-sources | tor-proxy | web-attacks} . 328
[no] ip-reputation webroot outgoing-category {botnets | phishing} 328
[no] ip-reputation white-list activate 328
[no] ip-select {iface | auto | custom} 187
[no] ip-select-backup {iface | auto | custom} 187

[no] ipv6 activate 523
[no] ipv6 address *dhcp6_profile dhcp6_suffix_128* 140
[no] ipv6 dhcp6 address-request 140
[no] ipv6 dhcp6 rapid-commit 140
[no] ipv6 dhcp6-request-object *dhcp6_profile* 141
[no] ipv6 enable 140
[no] ipv6 metric <0..15> 140
[no] ipv6 nd ra accept 140
[no] isakmp policy *policy_name* 279
[no] item as-report 575
[no] item av-report 575
[no] item cf-report 575
[no] item cpu-usage 575
[no] item idp-report 575
[no] item mem-usage 575
[no] item port-usage 575
[no] item session-usage 575
[no] item traffic-report 575
[no] join *interface_name* 154
[no] *keyword* 372
[no] l2tp-over-ipsec activate; 301
[no] l2tp-over-ipsec first-dns-server {*ip* | *interface_name*} {1st-dns|2nd-dns|3rd-dns}| {*ppp_interface*}{1st-dns|2nd-dns}} 302
[no] l2tp-over-ipsec first-wins-server *ip* 302
[no] l2tp-over-ipsec keepalive-timer <1..180> 302
[no] l2tp-over-ipsec second-dns-server {*ip* | *interface_name*} {1st-dns|2nd-dns|3rd-dns}| {*ppp_interface*}{1st-dns|2nd-dns}} 302
[no] l2tp-over-ipsec second-wins-server *ip* 302
[no] l2tp-over-ipsec user user_name 302
[no] language update auto 523
[no] lan-provision model {nwa5301-nj | wac6502d-e | wac6502d-s | wac6503d-s | 70
[no] lan-provision model {nwa5301-nj | wac6502d-e | wac6502d-s | wac6503d-s | 71
[no] lan-provision model {nwa5301-nj | wac6502d-e | wac6502d-s | wac6503d-s | 71
[no] lan-provision model {nwa5301-nj | wac6502d-e | wac6502d-s | wac6503d-s | 71
[no] ldap-server basedn *basedn* 473
[no] ldap-server binddn *binddn* 473
[no] ldap-server cn-identifier *uid* 473
[no] ldap-server host *ldap_server* 473
[no] ldap-server password *password* 473
[no] ldap-server password-encrypted *password* 473
[no] ldap-server port *port_no* 473
[no] ldap-server search-time-limit *time* 473
[no] ldap-server ssl 473
[no] lease {<0..365> [<0..23> [<0..59>]] | infinite} 130
[no] limit <0...40000> 231
[no] limit <0...40000> 232
[no] listen-interface *interface_name* 209
[no] load-balancing [slot1 | slot2] activate 71
[no] load-balancing [slot1 | slot2] kickout 71
[no] load-balancing <group1 | group2> group_name 59
[no] local-address <*ip*> 144
[no] local-address *ip* 140
[no] log 421
[no] log [alert] 222
[no] log [alert] 230
[no] log [alert] 309
[no] log [alert] 318
[no] log [alert] 399
[no] logging cef-format include year 566

[no] logging console 570
[no] logging console category *module_name* 570
[no] logging debug suppression 568
[no] logging debug suppression interval <10..600> 568
[no] logging mail <1..2> 569
[no] logging mail <1..2> {send-log-to | send-alerts-to} *e_mail* 569
[no] logging mail <1..2> address {*ip* | *hostname*} 569
[no] logging mail <1..2> authentication 569
[no] logging mail <1..2> authentication username *username* password *password* 569
[no] logging mail <1..2> category *module_name* level {alert | all} 570
[no] logging mail <1..2> port <1..65535> 569
[no] logging mail <1..2> schedule {full | hourly} 570
[no] logging mail <1..2> subject *subject* 570
[no] logging mail <1..2> tls activate 569
[no] logging mail <1..2> tls starttls-off 570
[no] logging syslog <1..4> 568
[no] logging syslog <1..4> {disable | level normal | level all} 568
[no] logging syslog <1..4> address {*ip* | *hostname*} 568
[no] logging syslog <1..4> facility {local_1 | local_2 | local_3 | local_4 | local_5 | local_6 | local_7} 568
[no] logging syslog <1..4> format {cef | vrpt} 568
[no] logging system-log suppression 566
[no] logging system-log suppression interval <10..600> 566
[no] logging usb-storage 149
[no] logging usb-storage 566
[no] logging usb-storage keep-duration 567
[no] login-page color-background 511
[no] login-page color-window-background 511
[no] login-page message-text % *message* 511
[no] login-url *url* 255
[no] logout-ip *ipv4_address* 255
[no] logout-url *url* 256
[no] mac-auth database mac *mac_address* type ext-mac-address mac-role mac-users description *description* 449
[no] mac-auth database mac *mac_address* type int-mac-address mac-role mac-users description *description* 449
[no] mac-auth database mac *oui* type ext-oui mac-role mac-users description *description* 450
[no] mac-auth database mac *oui* type int-oui mac-role mac-users description *description* 450
[no] mail-from *e_mail* 574
[no] mail-from *email_address* 519
[no] mail-send 596
[no] mail-subject append date-time 519
[no] mail-subject append date-time 574
[no] mail-subject append system-name 519
[no] mail-subject append system-name 574
[no] mail-to-1 *e_mail* 575
[no] mail-to-2 *e_mail* 575
[no] mail-to-3 *e_mail* 575
[no] mail-to-4 *e_mail* 575
[no] mail-to-5 *e_mail* 575
[no] match-action pop3 {forward | forward-with-tag} 400
[no] match-action smtp {drop | forward | forward-with-tag} 400
[no] maximum-paths <1..255> 181
[no] mem-conserve activate 601
[no] mem-conserve av-bypass falling-threshold <1..4000> 601
[no] mem-conserve av-bypass rising-threshold <1..4000> 601
[no] mem-conserve av-bypass sustained-time <1..60> 601
[no] mem-conserve utm-bypass falling-threshold <1..4000> 601
[no] mem-conserve utm-bypass rising-threshold <1..4000> 602

[no] mem-conserve utm-bypass sustained-time <1..60> 602
[no] metric <0..15> 119
[no] metric <0..15> 159
[no] mode-config {first-dns | second-dns} 283
[no] mode-config {first-wins | second-wins} 284
[no] monitor-mode 249
[no] mss <536..1452> 140
[no] mss <536..1460> 119
[no] mtu <576..1480> 147
[no] mtu <576..1500> 119
[no] multicast 83
[no] multicast 84
[no] multicast-to-unicast 82
[no] mx {*ip* | *domain_name*} 187
[no] nail-up 282
[no] nail-up 293
[no] name *description* 274
[no] name *description* 275
[no] name *profile_name* 203
[no] narrowed 283
[no] narrowed 293
[no] nat-pmp activate 210
[no] natt 279
[no] negotiation auto 138
[no] neighbor *ipv4* 181
[no] neighbor *ipv4* connect-retry 182
[no] neighbor *ipv4* default-originate 182
[no] neighbor *ipv4* description *description* 181
[no] neighbor *ipv4* ebgp-multihop hops <1..255> 181
[no] neighbor *ipv4* maximum-prefix < 1..4294967295 > 182
[no] neighbor *ipv4* password *password* 182
[no] neighbor *ipv4* remote-as <1..4294967295> 181
[no] neighbor *ipv4* timers < 0..65535> < 0..65535> 182
[no] neighbor *ipv4* ttl-security [hops] <1..254> 182
[no] neighbor *ipv4* update-source [*ipv4*|*interface_name*] 182
[no] neighbor *ipv4* weight <1..65535> 181
[no] netbios-broadcast 282
[no] network *interface* area IP 178
[no] network *interface_name* 133
[no] network *interface_name* 177
[no] network *interface_name* area *ip* 134
[no] network *ipv4_cidr* 181
[no] network-extension {activate | ip- *address_object* | 1st-dns {*address_object* | *ip* } | 2nd-dns {*address_object* | *ip* } | 1st-wins {*address_object* | *ip* } | 2nd-wins {*address_object* | *ip* } | network *address_object*} 296
[no] network-extension netbios-broadcast 296
[no] network-extension traffic-enforcement 296
[no] network-selection {auto|home} 142
[no] next-hop {auto|gateway *address object* |interface *interface_name* |trunk *trunk_name*|tunnel *tunnel_name*} 169
[no] next-hop {auto|gateway *address_object* |interface *interface_name* |trunk *trunk_name*|tunnel *tunnel_name*} 170
[no] nol-channel-block 82
[no] ntp 513
[no] ntp server {*fqdn*|*w.x.y.z*} 513
[no] object-group <object> 456
[no] object-group address *group_name* 463
[no] object-group *group_name* 464
[no] object-group *group_name* 469

[no] object-group service *group_name* 469
[no] outbound ceiling {<0..1048576> | maximize-bandwidth-usage} 309
[no] outbound guarantee-bandwidth <0..1048576> priority <1..7> 309
[no] outbound-dscp-mark {<0..63> | class {af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs0 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | default | wmm_be0 | wmm_be24 | wmm_bk16 | wmm_bk8 | wmm_vi32 | wmm_vi40 | wmm_vo48 | wmm_vo56}} 310
[no] outgoing-interface {interface *interface_name* | trunk *group_name*} 310
[no] outonly-interface *interface_name* 133
[no] outonly-interface *interface_name* 177
[no] out-snat activate 282
[no] override-full-power activate 59
[no] packet-capture activate 586
[no] passive-interface *interface_name* 133
[no] passive-interface *interface_name* 134
[no] passive-interface *interface_name* 177
[no] passive-interface *interface_name* 177
[no] password complexity-verify 446
[no] password *password* 498
[no] password *password* 499
[no] password *password* 520
[no] payment-service activate 266
[no] payment-service mobile-page-customization 266
[no] payment-service page-customization 266
[no] pin <*pin code*> 144
[no] ping-check activate 135
[no] ping-check activate 159
[no] policy controll-ipsec-dynamic-rules activate 171
[no] policy controll-virtual-server-rules activate 171
[no] policy override-direct-route activate 171
[no] policy6 override-direct-route activate 171
[no] policy-enforcement 282
[no] policy-enforcement 293
[no] port <*1..65535*> 203
[no] port *interface_name* 153
[no] printer-manager activate 269
[no] printer-manager encrypt activate 269
[no] printer-manager printer <1..10> 269
[no] priority-code <0..7. 153
[no] private-encryption-key <encryption-key> 545
[no] protocol gre 283
[no] pwd-expiry expiration days <1..365> 445
[no] pwd-expiry force-to-change-pwd activate 445
[no] radius-server host *radius_server* auth-port *auth_port* 474
[no] radius-server key *secret* 474
[no] radius-server timeout *time* 474
[no] redistribute {static | ospf} 177
[no] redistribute {static | rip} 177
[no] redistribute {static | rip} metric-type <1..2> metric <0..16777214> 177
[no] redistribute connected 181
[no] reject-legacy-station 82
[no] remote-address <*ip*> 144
[no] remote-address *ip* 140
[no] replay-detection 282
[no] replay-detection 293
[no] report 572
[no] report packet size statistics 574
[no] reset-counter 575
[no] respmsg url-filter block-page customized activate 522
[no] router-id IP 177

[no] router-id *router-id* 181
[no] rssi-retry 82
[no] rssi-thres 82
[no] rtls ekahau activate 325
[no] sandbox file-type {archives | chm | eicar | executables | macromedia-flash-data | ms-office-document | pdf | rtf | unknow-type} 345
[no] sandbox queue-packet 346
[no] sandbox statistics collect 346
[no] scan {http | ftp | imap4 | smtp | pop3} 318
[no] scan {smtp | pop3} 399
[no] scan-detection {tcp-xxx} {activate | log [alert] | block} 235
[no] scan-detection {udp-portscan} {activate | log [alert] | block} 235
[no] schedule reboot activate 594
[no] schedule *schedule_name* 257
[no] schedule *schedule_object* 169
[no] schedule *schedule_object* 170
[no] schedule *schedule_object* 222
[no] schedule *schedule_object* 310
[no] second-dns-server {*ip* | *interface_name* {1st-dns | 2nd-dns | 3rd-dns} | ZyWALL} 129
[no] second-wins-server *ip* 130
[no] secret *secret* 490
[no] secret *secret* 518
[no] secumanager activate 243
[no] secure-policy activate 219
[no] secure-policy asymmetrical-route activate 219
[no] secure-policy6 activate 220
[no] secure-policy6 asymmetrical-route activate 221
[no] security-service anti-botnet-IP activate 331
[no] security-service anti-spam activate 403
[no] security-service anti-virus activate 317
[no] security-service app-patrol activate 314
[no] security-service dns-filter activate 343
[no] security-service ip-reputation activate 327
[no] security-service ips activate 349
[no] security-service sandbox activate 346
[no] security-service update-server activate 55
[no] server <*fqdn*> <*w.x.y.z*> 203
[no] server alternative-cn-identifier *uid* 475
[no] server alternative-cn-identifier *uid* 476
[no] server basedn *basedn* 475
[no] server basedn *basedn* 476
[no] server binddn *binddn* 475
[no] server binddn *binddn* 476
[no] server cn-identifier *uid* 475
[no] server cn-identifier *uid* 476
[no] server description *description* 475
[no] server description *description* 476
[no] server description *description* 477
[no] server group-attribute <1-255> 477
[no] server group-attribute *group-attribute* 475
[no] server group-attribute *group-attribute* 476
[no] server host *ad_server* 475
[no] server host *ldap_server* 476
[no] server host *radius_server* 477
[no] server *ip* 499
[no] server key *secret* 477
[no] server password *password* 475
[no] server password *password* 476
[no] server port *port_no* 475

[no] server port *port_no* 476
[no] server search-time-limit *time* 475
[no] server search-time-limit *time* 476
[no] server ssl 475
[no] server ssl 476
[no] server timeout *time* 477
[no] service {http-redirect | smtp-redirect} 203
[no] service {*service_name*|any} 169
[no] service {*service_name*|any} 170
[no] service <profile name> 230
[no] service application-group *app_name* 310
[no] service *service_name* 222
[no] service service-object {*service_name* | any} 310
[no] service-name {*ip* | *hostname* | *service_name*} 499
[no] service-object *object_name* 469
[no] service-type {dyndns | dyndns_static | dyndns_custom | dynu-basic | dynu-premium | no-ip | peanut-hull | 3322-dyn | 3322-static | Selfhost | User custom} 187
[no] session-limit activate 231
[no] session-limit6 activate 231
[no] session-url *url* 256
[no] shutdown 120
[no] shutdown 147
[no] shutdown 159
[no] sid {1-4294967295} 363
[no] signature *sid* activate 351
[no] slave *interface_name* 155
[no] *slot_name* ap-profile *radio_profile_name* 67
[no] *slot_name* ap-profile *radio_profile_name* 70
[no] *slot_name* monitor-profile *monitor_profile_name* 67
[no] *slot_name* monitor-profile *monitor_profile_name*lilnterval 70
[no] *slot_name* output-power *wlan_power* 67
[no] *slot_name* output-power *wlan_power* 70
[no] *slot_name* repeater-ap *radio_profile_name* 70
[no] *slot_name* root-ap *radio_profile_name* 70
[no] *slot_name* ssid-profile <1..8> *ssid_profile_name* 67
[no] *slot_name* ssid-profile <1..8> *ssid_profile_name* 70
[no] *slot_name* zymesh-profile *zymesh_profile_name* 67
[no] *slot_name* zymesh-profile *zymesh_profile_name* 70
[no] sms-service activate 520
[no] smtp-address {*ip* | *hostname*} 520
[no] smtp-auth activate 520
[no] smtp-auth username *username* password *password* 520
[no] smtp-port <1..65535> 520
[no] smtp-tls activate 520
[no] smtp-tls authenticate-server 520
[no] smtp-tls starttls-off 520
[no] snat {outgoing-interface| {*address_object*}} 169
[no] snmp-server 536
[no] snmp-server community *community_string* {ro|rw} 536
[no] snmp-server contact *description* 536
[no] snmp-server enable {informs|traps} 536
[no] snmp-server host {*w.x.y.z*|*fqdn*|*ipv6 address*} [*community_string*] 536
[no] snmp-server location *description* 536
[no] snmp-server port <1..65535> 536
[no] software-watchdog-timer <10..600> 598
[no] source {*address6_object*|any} 170
[no] source {*address_object* | *group_name*} 257
[no] source {*address_object*|any} 169
[no] source *address_object* 310

[no] source *profile_name* 203
[no] sourceip *address_object* 222
[no] sourceip6 *address_object* 222
[no] sourceport {tcp|udp} {eq <1..65535>|range <1..65535> <1..65535>} 222
[no] speed <100,10> 138
[no] srcport {*profile_name*|any} 169
[no] srcport {*profile_name*|any} 170
[no] ssid-profile *wlan_interface_index ssid_profile* 82
[no] ssl-inspection cert-update auto 423
[no] ssl-inspection statistics collect 424
[no] ssl-profile <profile name> {[no log]|[log by-profile]} {activate | deactivate} 223
[no] sslvpn application *application_object* 501
[no] sslvpn *profile_name* 184
[no] sslvpn *tunnel_name* 169
[no] sso 257
[no] starting-address *ip* -size <1..65535> 129
[no] suppress-retry-rts 83
[no] system default-snat 164
[no] tcp-decoder {tcp-xxx} action {drop | reject- sender | reject-receiver | reject-both}} 235
[no] tcp-decoder {tcp-xxx} activate 235
[no] terms-of-service 256
[no] third-dns-server {*ip* | *interface_name* {1st-dns | 2nd-dns | 3rd-dns} | ZyWALL} 129
[no] threat-website action {block | log | pass | warn} 332
[no] threat-website block message *message* 332
[no] threat-website block redirect *url* 332
[no] threat-website category {anonymizers | browser-exploits | botnets | compromised | malicious-downloads | malicious-sites | malware | phishing | phishing-fraud | spam-sites | spam-urls | spyware-adware-keyloggers} 332
[no] threat-website ebl activate 335
[no] threat-website ebl update auto 336
[no] threat-website forbid-list activate 331
[no] threat-website profile <*profile name*> category {*anonymizers* | *malware* | *botnets* | *phishing* 335
[no] threat-website profile <*profile name*> description <*description*> 335
[no] threat-website profile <*profile name*> log 335
[no] threat-website statistics collect 338
[no] threat-website trust-list activate 331
[no] to {*zone_object*|ZyWALL} 222
[no] tointerface <interface name> 230
[no] transition-mode 91
[no] *trust_hosts* 372
[no] tunnel *tunnel_name* 169
[no] tunnel *tunnel_name* 170
[no] twofa-auth 280
[no] twofa-auth 290
[no] twofa-auth 291
[no] two-factor-auth activate 484
[no] two-factor-auth admin-access activate 487
[no] two-factor-auth admin-access deliver-method {sms|email} 487
[no] two-factor-auth admin-access service {ssh|telnet|web} 487
[no] two-factor-auth admin-access user username 487
[no] two-factor-auth admin-access valid-time <1..5> 487
[no] two-factor-auth deliver-method {sms | email | google-auth} 485
[no] two-factor-auth http activate 486
[no] two-factor-auth service {sslvpn|ipsec|l2tp} 485
[no] two-factor-auth user *username* 485
[no] two-factor-auth valid-time <1..15> 484
[no] type {domain|ip} 275
[no] type {per-user | shared | per-ip-source} 310

[no] udp-decoder {bad-udp-l4-size | udp-land | udp-smurf} activate 235
[no] ul-bandwidth-limit <1...1048576> 286
[no] upnp-igd activate 210
[no] upstream <0..1048576> 120
[no] upstream <0..1048576> 159
[no] url {URL TEXT} 188
[no] url *url* 274
[no] usb-storage activate 149
[no] usb-storage log_rotate_activate 150
[no] usb-storage update-firmware enable 151
[no] user *user_name* 169
[no] user *user_name* 171
[no] user user_name 204
[no] user *user_name* 222
[no] user *user_name* 231
[no] user *user_name* 232
[no] user *user_name* 296
[no] user *user_name* 310
[no] user *username* 446
[no] user *username* 498
[no] user *username* 499
[no] username *e-mail* 520
[no] username *username* password *password* 187
[no] users idle-detection 447
[no] users idle-detection timeout <1..60> 447
[no] users lockout-period <1..65535> 447
[no] users retry-count <1..99> 447
[no] users retry-limit 447
[no] users simultaneous-logon {administration | access} enforce 447
[no] users simultaneous-logon {administration | access} limit <1..1024> 447
[no] users update-lease automation 447
[no] utm-manager {doh| dot| system-protect} defaultport port number 344
[no] version <1..2> 177
[no] vlan-id <1..4094> 153
[no] *vlan_interface* 60
[no] vpn-concentrator *profile_name* 286
[no] vpn-concentrator6 *profile_name* 294
[no] vpn-configuration-provision activate 286
[no] vpn-configuration-provision iosfilter 287
[no] vpn-service auto-disable 278
[no] vpn-service enable 278
[no] walled-garden activate 273
[no] walled-garden rule <1..50> 273
[no] wan-iface *interface_name* 187
[no] web-auth activate 253
[no] web-auth redirect-fqdn *host_str* 253
[no] web-google-analytics activate 603
[no] webpage-encrypt 502
[no] welcome-url *url* 256
[no] wildcard 187
[no] wireless-health {activate | radio | sta} 102
[no] wlan-macfilter-profile *macfilter_profile_name* 94
[no] wlan-monitor-profile *monitor_profile_name* 84
[no] wlan-radio-profile radio profile name 102
[no] wlan-radio-profile *radio_profile_name* 77
[no] wlan-security-profile *security_profile_name* 89
[no] wlan-ssid-profile *ssid_profile_name* 86
[no] zero-wait-dfs 83
[no] zone *profile_name* 184

[no] zymesh-profile *zymesh_profile_name* 96
[no]address6-object *object_name* interface-gateway *interface* {slaac | static} {*addr_index*} 460
[no]https activate 187
[no]igmp activate 125
{anomaly | signature | system-protect} activation 349
{anomaly | signature} activate 349
{bg | bgn | a | ac | an | bgnax | anacax| ax} 79
<1..32> | insert <1..32>} 234
<1..32> | move <1..32> to <1..32>} 234
<1..4094> 414
<profile name> 230
<profile1> <profile2> 233
| *browser-exploits* | *phishing-fraud* | *compromised* | *spam-sites* | *malicious-downloads* | *spam-urls* | *malicious-sites* | *spyware-adware-keyloggers}* 335
| uint32 <0..4294967295> | ip *ipv4* [*ipv4* [*ipv4*]] | fqdn *fqdn* [*fqdn* [*fqdn*]] | text *text* | hex *hex* | vivc *enterprise_id hex_s* [*enterprise_id hex_s*] | vivs *enterprise_id hex_s* [*enterprise_id hex_s*] 129
2g-basic-speed *speed* 77
2g-channel *wireless_channel_2g* 77
2g-multicast-speed *wlan_2g_support_speed* 77
2g-wlan-rate-control *rate_2g* 77
5g-basic-speed *speed* 77
5g-channel *wireless_channel_5g* 77
5g-multicast-speed *wlan_5g_basic_speed* 78
5g-wlan-rate-control rate_5g 78
6g-channel wireless_channel_6g 78
6g-multicast-speed wlan_6g_basic_speed 78
6g-wlan-rate-control rate_6g 78
aaa authentication [no] match-default-group 480
aaa authentication default *member1* [*member2*] [*member3*] [*member4*] 479
aaa authentication *profile-name member1* [*member2*] [*member3*] [*member4*] 480
aaa authentication rename *profile-name-old profile-name-new* 479
aaa group server ad *group-name* 475
aaa group server ad rename *group-name group-name* 474
aaa group server ldap *group-name* 476
aaa group server ldap rename *group-name group-name* 476
aaa group server radius *group-name* 477
aaa group server radius rename {*group-name-old*} *group-name-new* 477
access-page message-color {*color-rgb* | *color-name* | *color-number*} 511
access-page title *title* 511
access-page window-color {*color-rgb* | *color-name* | *color-number*} 511
account *profile_name* 142
account *profile_name* 303
action {allow|deny|reject} 221
action {allow|deny|reject} 230
activate 237
activate 270
activate 279
activate 281
activate 289
activate 290
activate 292
address *ipv6_addr_prefix* 120
address *ipv6_addr_prefix* 122
address6-object *object_name* {*ip* | *ip_range* | *ip_subnet* | fqdn *fqdn*| geography *country code* | interface-ip | interface-subnet | interface-gateway} {*interface_name* | *virtual interface name*} 460
address6-object *object_name* geography <country code> all 460
address-object *object_name* {*ip* | *ip_range* | *ip_subnet* | fqdn *fqdn*| geography *country code* | interface-ip | interface-subnet | interface-gateway} {*interface_name* | *virtual interface*

name} 459
address-object *object_name* geography <country code> all 459
address-object rename *object_name object_name* 460
adjust-mss {auto | <200..1500>} 281
adjust-mss {auto | <200..1500>} 292
advertisement flush 276
advertisement rename *description_old description_new* 276
aggressiveness: low 105
algorithm {wrr|llf|spill-over} 163
anti-botnet action {forward | reject-both | reject-receiver | reject-sender} 331
anti-botnet statistics flush 338
anti-botnet update daily <0..23> 337
anti-botnet update hourly 337
anti-botnet update signatures 337
anti-botnet update weekly {sun | mon | tue | wed | thu | fri | sat} <0..23> 337
anti-spam dnsbl [1..5] domain *dnsbl_domain* {activate|deactivate} 407
anti-spam dnsbl ip-check-order {forward | backward} 407
anti-spam dnsbl max-query-ip [1..5] 407
anti-spam dnsbl query-timeout pop3 {forward | forward-with-tag} 407
anti-spam dnsbl query-timeout smtp {drop | forward | forward-with-tag} 407
anti-spam dnsbl query-timeout time [1..10] 408
anti-spam dnsbl statistics flush 407
anti-spam ip-reputation query-timeout time [*timeout*] 400
anti-spam ip-reputation statistics flush 400
anti-spam mail-phishing query-timeout pop3 {forward | forward-with-tag} 401
anti-spam mail-phishing query-timeout smtp {drop | forward | forward-with-tag} 401
anti-spam mail-phishing query-timeout time [*timeout*] 401
anti-spam mail-scan query-timeout pop3 {forward | forward-with-tag} 401
anti-spam mail-scan query-timeout smtp {drop | forward | forward-with-tag} 401
anti-spam mail-scan query-timeout time [*timeout*] 401
anti-spam profile append 399
anti-spam profile delete *rule_number* 400
anti-spam profile insert *rule_number* 399
anti-spam profile move *rule_number* to *rule_number* 400
anti-spam profile *rule_number* 399
anti-spam statistics flush 409
anti-spam tag {dnsbl | dnsbl-timeout} [*tag*] 407
anti-spam tag {mail-content | mail-phishing | virus-outbreak} [*tag*] 400
anti-spam tag black-list [*tag*] 405
anti-spam tag mail-phishing [*tag*] 400
anti-spam tag query-timeout [*tag*] 401
anti-spam xheader {mail-content | virus-outbreak} *xheader-name xheader-value* 401
anti-spam xheader mail-phishing *xheader-name xheader-value* 401
anti-virus black-list {md5-hash md5-pattern | sha256-hash sha256-pattern | file-pattern file-pattern} {activate|deactivate} 319
anti-virus black-list {replace <1..256> | file-pattern file-pattern md5-hash md5-pattern | sha256-hash sha256-pattern} 320
anti-virus mail-infect-ext activate 317
anti-virus *profile_name* 318
anti-virus reload signatures 317
anti-virus rename *old_profile_name new_profile_name* 318
anti-virus scan mode {express | hybrid | stream} 317
anti-virus statistics flush 323
anti-virus update ctdb 322
anti-virus update daily <0..23> 322
anti-virus update hourly 322
anti-virus update signatures 322
anti-virus update weekly {sun | mon | tue | wed | thu | fri | sat} <0..23> 322
anti-virus white-list {md5-hash md5-pattern | sha256-hash sha256-pattern | file-pattern file-

pattern} {activate|deactivate} 320
anti-virus white-list {replace <1..256> | file-pattern file-pattern md5-hash md5-pattern |
sha256-hash sha256-pattern} 320
ap internal-auth no shared-secret 60
ap-group first-priority *ap_group_profile_name* 69
ap-group flush wtp-setting *ap_group_profile_name* 69
ap-group-member *ap_group_profile_name* [no] member *mac_address* 70
ap-group-member *ap_group_wlan_name*[no] member local-ap 69
ap-group-profile *ap-group-profile_name* 67
ap-group-profile rename *ap_group_profile_name1 ap_group_profile_name2* 73
ap_mac 100
ap_mac 97
app reload signatures 314
app rename <profile-name> <profile-name> 314
app statistics flush 314
app update 314
app update daily <0..23> 314
app update hourly 314
app update weekly {sun | mon | tue | wed | thu | fri | sat} <0..23> 314
application <profile-name> action {forward|drop|reject} {no log|log [alert]} 314
application-object <object> 455
application-object rename <object> <object> 455
apply 42
apply /conf/*file_name.conf* [ignore-error] [rollback] 545
app-watch-dog reboot-log flush 598
area IP virtual-link IP message-digest-key <1..255> encrypted-authentication-key 179
area IP virtual-link IP message-digest-key <1..255> md5 *authkey* 179
arp {arp-interval <1..1000> | arp-ip-target <W.X.Y.Z>} 156
arp IP *mac_address* 590
atse 42
authentication {chap | chap-pap | mschap | mschap-v2 | pap} 303
authentication {pre-share | rsa-sig | user-base-psk} 279
authentication {pre-share | rsa-sig} 289
authentication {pre-share | rsa-sig} 290
authentication key <1..255> key-string *authkey* 177
authentication-type {<*profile name*> | default-user-agreement | default-web-portal | facebook-wifi} . 256
auth_method 490
auth_method 518
auth-server authentication 490
auth-server authentication 518
auto-healing activate: yes 111
auto-healing healing threshold: -85 dBm 111
auto-healing healing-interval *interval* 110
auto-healing healing-threshold 110
auto-healing interval: 10 111
auto-healing margin 111
auto-healing margin: 0 111
auto-healing power threshold: -70 dBm 111
auto-healing power-threshold <-50~-80> 110
auto-healing update 111
band {2.4G |5G| 6G} band-mode 79
bandwidth {upload | download} <0..1048576> priority <1..7> 264
bandwidth {upload | download} <0..1048576> priority <1..7> 508
base {all | everything | none} 234
beacon-interval <*40..1000*> 79
billing accounting-method {accumulation | time-to-finish } 262
billing accumulation idle-detection timeout <1..60> 262
billing accumulation-expire {day <1..360> | hour <1..24>} 262
billing currency {eur | gbp | usd | user-define *currency_code* } 262

billing decimal-places <2> 262
billing decimal-symbol {comma | dot} 262
billing discount button {a | b | c} [charge-by-level] 263
billing profile rename *profile_name profile_name* 263
billing tax-rate <0..100> 263
billing unused-expire {minute <30..60> | hour <1..24> | day <1..365>} 263
billing username-password-length <4..6> 263
bind profile 234
binding interface *interface_name* crypto-map *map_name* 160
bind-ipv4-addr *ipv4* 422
bind-ipv6-addr *ipv6* 422
broadcast pps <1~10000> 83
broadcast pps <1~10000> 84
bss-color <0~63> 79
budget {log|log-alert}[recursive <1..65535>] 143
budget {log-percentage|log-percentage-alert} [recursive <1..65535>] 143
budget current-connection {keep|drop} 143
budget new-connection {allow|disallow} 143
budget percentage {ptime|pdata} <0..99> 143
budget reset-counters 143
budget reset-day <0..31> 143
bwm <1..127> 307
bwm <1..127> 308
bwm append 307
bwm default inbound priority <1..7> 307
bwm default outbound priority <1..7> 307
bwm delete <1..127> 307
bwm insert <1..127> 308
bwm modify <1..127> 308
bwm move <1..127> to <1..127> 308
ca generate pkcs10 name *certificate_name* cn-type {ip cn *cn_ipv4_address* | ipv6 cn *cn_ipv6_address* |fqdn cn *cn_domain_name* | mail cn *cn_email*} [ou *organizational_unit*] [o *organization*] [l *town*] [s *state*] [c *country*] [usr-def user_definition] key-type {dsa | dsa-sha256 | ecdsa | ecdsa-sha256 | ecdsa-sha384 | rsa | rsa-sha256 | rsa-sha512} key-len *key_length* [extend-key extend_key] year lifetimes 494
ca generate pkcs12 name *name* password *password* 494
ca generate x509 name *certificate_name* cn-type {ip cn *ipv4* | ipv6 cn *cn_ipv6_address* | fqdn cn *cn_domain_name* | mail cn *cn_email*} [ou *organizational_unit*] [o *organization*] [l *town*] [s *state*] [c *country*] [usr-def user_definition] key-type {dsa | dsa-sha256 | ecdsa | ecdsa-sha256 | ecdsa-sha384 | rsa | rsa-sha256 | rsa-sha512} key-len *key_length* . 494
ca rename category {local|remote} *old_name new_name* 494
ca validation *remote_certificate* 495
capwap ap <mac address> [no] airtime-fairness activate 57
capwap ap ac-ip *{primary_ac_ip} {secondary_ac_ip}* 59
capwap ap ac-ip *{primary_ac_ip|primary_ac_dns} {secondary_ac_ip|secondary_ac_dns}* 605
capwap ap ac-ip auto 59
capwap ap ac-ip auto 605
capwap ap add *ap_mac* [*ap_model*] 59
capwap ap *ap_mac* 57
capwap ap *ap_mac* 66
capwap ap factory default *ap_mac* 59
capwap ap fallback disable 59
capwap ap fallback enable 59
capwap ap fallback interval <30..86400> 59
capwap ap idle timeout {25–100} 59
capwap ap kick {all | *ap_mac*} 60
capwap ap led-off *ap_mac* 60
capwap ap led-on *ap_mac* 60
capwap ap local-ap 67

capwap ap reboot *ap_mac* 60
capwap ap vlan ip address *ip netmask* 605
capwap ap vlan ip gateway *gateway* 605
capwap ap vlan no ip gateway 605
capwap ap vlan vlan-id *vid* { tag | untag } 605
capwap manual-add {enable | disable} 60
capwap station kick *sta_mac* 60
cdp {activate|deactivate} 495
cdr block http-service-port *<1..65535>* 414
cdr block https-service-port *<1..65535>* 414
cdr block message *denied_message* 414
cdr block period *<0..1440>* 414
cdr block redirect *<url>* 414
cdr block url {*message*|*redirect*} 414
cdr blocked-by {*ip*|*mac*} 414
cdr quarantine period *<0..1440>* 414
cdr quarantine vlan-id 414
cdr rule *rule_id* threshold *occurence* duration *duration* action {*alert*| *block*| *quarantine*| *block-alert*| *quarantine-alert*} 415
cdr send-alerts-to *email_address* 415
cdr signature reload 416
cdr signature update 416
cdr unblock ipv4 *ip_address* 415
cdr unblock mac *mac_address* 415
cdr update daily <0..23> 416
cdr update hourly 416
cdr update weekly {sun | mon | tue | wed | thu | fri | sat} <0..23> 416
cdr white-list replace <1..512> ipv4 *ip_address* 415
cdr white-list replace <1..512> mac *mac_address* 415
certificate *certificate-name* 279
certificate certificate-name 289
certificate certificate-name 290
certificate *cert_name* 302
charge *price* 508
check-period *1-86400* 198
ch-width *wlan_htcw* 79
clear 42
clear aaa authentication *profile-name* 479
clear aaa group server ad [*group-name*] 474
clear aaa group server ldap [*group-name*] 475
clear aaa group server radius *group-name* 477
clear ip dhcp binding {*ip* | *} 130
clear logging debug buffer 568
clear logging system-log buffer 566
clear report [*interface_name*] 572
clock date *yyyy-mm-dd* time *hh:mm:ss* 513
clock time *hh:mm:ss* 513
cloud-helper check all 550
cloud-helper check app 550
cloud-helper check app_incr 550
cloud-helper check av 551
cloud-helper check botnet 551
cloud-helper check ctdb 551
cloud-helper check firmware 551
cloud-helper check geoip 551
cloud-helper check idp 551
cloud-helper check rf 551
cloud-helper check sslca 551
cloud-helper check-notify new_features_rap 551

cloud-helper check-notify new_features_cdr 551
cloud-helper check-notify new_features_dns_cf 551
cloud-helper check-notify now 551
cloud-helper check-notify service_expired 551
cloud-helper check-notify whats_new 551
cloud-helper clean-download firmware 551
cloud-helper firmware update daily <*0..23*> reboot {no | yes} 551
cloud-helper firmware update weekly {fri | mon | sat | sun | thu | tue | wed} <*0..23*> reboot {no | yes} 551
cloud-helper get app 551
cloud-helper get av 552
cloud-helper get botnet 552
cloud-helper get firmware <1..2> 552
cloud-helper get idp 552
cloud-helper get sslca 552
cloud-helper pause-download firmware <1..2> 552
cloud-helper set {[retry_times <1..10>]} {[retry_period <2..60>]} {[retry_fail_period <180..720>]} 552
cloud-helper set remind {every-time | never} 552
cloud-helper set-read new_features_cdr 552
cloud-helper set-read new_features_dns_cf 552
cloud-helper set-read service_expired 552
cloud-helper set-read whats_new 552
cloud-helper update firmware <1..2> 552
cnm-agent server-type [vantage | tr069] 242
Command 197
config-backup run 596
config-backup setting 596
configuration-payload-provide address- {} 283
configuration-payload-provide address- {} 293
configure 42
conf-mail *{mail-to-1|mail-to-2|mail-to-3|mail-to-4|mail-to-5}* <user@domainname> 595
conf-mail attach password <*attachment password*> 596
conf-mail mail-content <*mail-content*> 595
conf-mail mail-subject <*subject*> 595
conf-mail no *{mail-to-1|mail-to-2|mail-to-3|mail-to-4|mail-to-5}* 595
conf-mail no mail-content 595
conf-mail send-now <*configfile*> 596
conn-check {FQDN | addr | activate} 168
conn-check {*ip address ip address* | first-and-last} method {icmp | tcp} period <5...3600> timeout <1...10> fail-tolerance <1...10> action {log | no-log} probe-condition {all | any} 284
connectivity {nail-up | dial-on-demand} 144
connect-timeout *1-300* 198
content-filter cf-queue flush 370
content-filter common-list {trust|forbid} 370
content-filter dashboard statistics flush 51
content-filter https-domain-filter block-cache-ttl <1~60> 374
content-filter https-domain-filter block-page port <*port*> 374
content-filter https-domain-filter forward-cache-ttl <1~1440> 374
content-filter passed warning flush 369
content-filter passed warning timeout <1..1440> 369
content-filter profile *filtering_profile* [commtouch-url] log-all 373
content-filter profile *filtering_profile* [commtouch-url] match {block | log | pass} 373
content-filter profile *filtering_profile* [commtouch-url] offline {block | log | warn | pass} 373
content-filter profile *filtering_profile* [commtouch-url] unrate {block | log | warn | pass} 373
content-filter profile filtering_profile commtouch-url log-all 373
content-filter profile *filtering_profile* commtouch-url match {block | log | pass} 372

content-filter profile *filtering_profile* commtouch-url match-unsafe {block | log | warn |pass} 372
content-filter profile *filtering_profile* commtouch-url offline {block | log | warn | pass} 373
content-filter profile *filtering_profile* commtouch-url unrate {block | log | warn | pass} 373
content-filter profile *filtering_profile* custom-list forbid 371
content-filter profile *filtering_profile* custom-list keyword 372
content-filter profile *filtering_profile* custom-list trust 372
content-filter report deactivate 366
content-filter report server {ip_address | hostname} 366
content-filter statistics flush 376
content-filter url-cache clear 369
content-filter url-cache clear *url* 369
content-filter url-server test 370
content-filter url-server test commtouch 369
cookie match <*string*> 375
cookie parameter <*string*> 375
cookie value <*string*> 375
copy 42
copy {/conf | /idp | /packet_trace | /script | /tmp}*file_name-a.conf* {/conf | /idp | /packet_trace | /script | /tmp}*/file_name-b.conf* 545
copy running-config /conf/*file_name.conf* 545
copy running-config startup-config 545
country-code *country_code* 60
country-code *country_code* 79
country-code *country_code* 84
cpu-temperature-monitor period *minutes* 52
cpu-temperature-monitor unit {celsius| fahrenheit} 52
create-time *yyyy-mm-dd hh:mm* 508
crypto map dial *map_name* 281
crypto map *map_name* 285
crypto map *map_name* 292
crypto map rename *map_name map_name* 281
crypto map rename *map_name map_name* 292
crypto map6 dial *map_name* 292
crypto *map_name* 286
currency {eur |gbp |usd | user-define *curreny_code*} 508
daily-report 574
dcs 2g-selected-channel *2.4g_channels* 80
dcs 5g-selected-channel *5g_channels* 80
dcs 6g-selected-channel *6g_channels* 80
dcs channel-deployment {3-channel|4-channel} 80
dcs client-aware {enable|disable} 80
dcs dcs-2g-method {auto|manual} 80
dcs dcs-5g-method {auto|manual} 80
dcs dcs-6g-method {auto|manual} 80
dcs dfs-aware {enable|disable} 77
dcs dfs-aware {enable|disable} 80
dcs mode {interval|schedule} 81
dcs now {ap_mac | profile_name} 109
dcs schedule <hh:mm> {mon|tue|wed|thu|fri|sat|sun} 81
dcs sensitivity-level {high|medium |low} 81
dcs time-interval *interval* 81
deactivate 237
deactivate 270
deactivate 279
deactivate 281
deactivate 289
deactivate 290

deactivate 292
debug (*) 42
debug conntrack flush 284
delete 42
delete {/conf | /idp | /packet_trace | /script | /tmp}/*file_name* 545
description *description* 234
description *description* 270
description *description* 70
description *description* 81
description description2 352
description *profile_description* 318
description2 97
details 42
device feedback mac <mac address> category <category> os <os> type <type> 440
device profile rename <profile name> <profile name> 439
device remove mac <mac address> 439
device remove mac <mac address> 439
device-ha ap-mode backup sync now 432
device-ha ap-mode cluster-id <1..32> 431
device-ha ap-mode priority <1..254> 431
device-ha ap-mode role {master|backup} 431
device-ha mode active-passive 430
device-ha2 ap-firmware-sync 435
device-ha2 failover connchk-hold-time <60..86400> 435
device-ha2 failover reset-interval <1..30> 435
device-ha2 failover-count <5 ..50> 435
device-ha2 firmware-update check-timeout 435
device-ha2 firmware-update delay 435
device-ha2 heartbeat period <1..10> fail-tolerance <1..10> 435
device-ha2 license-sync *serial_number* 435
device-ha2 schedule-reboot check-timeout <1..3600> 595
device-ha2 schedule-reboot delay <1..300> 595
device-ha2 sync password *password* 434
device-ha2 sync_from_active 434
device-ha2 sync_to_passive 434
device-ha2 virtual-mac *zynos_style_mac_address* 435
dhcp6 122
dhcp6 { server | client | relay upper { *config_interface* | *ipv6_addr* } } 121
dhcp6 address-request 121
dhcp6 address-request 122
dhcp6 duid { *duid* | mac } 121
dhcp6 rapid-commit 121
dhcp6 rapid-commit 122
dhcp6 refresh-time { <600..4294967294> | infinity } 121
dhcp6-lease-object *dhcp6_profile* 121
dhcp6-lease-object *dhcp6_profile* 122
dhcp6-lease-object *dhcp6_profile* { sip-server | ntp-server | dns-server } { *ipv6_addr* | *dhcp6_profile* } 505
dhcp6-lease-object *dhcp6_profile* address *ipv6_addr* duid *duid* 504
dhcp6-lease-object *dhcp6_profile* address- *ipv6_addr ipv6_addr* 505
dhcp6-lease-object *dhcp6_profile* prefix-delegation *ipv6_addr_prefix* duid *duid* ... 504
dhcp6-lease-object rename *dhcp6_profile dhcp6_profile* 505
dhcp6-request-object *dhcp6_profile* 121
dhcp6-request-object *dhcp6_profile* 123
dhcp6-request-object *dhcp6_profile* { dns-server | ntp-server | prefix-delegation | sip-server } 505
dhcp6-request-object rename *dhcp6_profile dhcp6_profile* 505
dhcp-option <1..254> *option_name* {boolean <0..1>| uint8 <0..255> | uint16 <0..65535> 129
diag 42

diag-info 42
diag-info collect 578
diaginfo collect ac 578
diaginfo collect wtp 578
diaginfo delete /ac 578
diaginfo delete /wtp 578
dir 42
dir {/conf | /idp | /packet_trace | /script | /tmp} 545
disable 43
dns query *fqdn* 199
dns-content-filter black-list FQDN {activate | deactivate} 377
dns-content-filter black-list replace <1..256> FQDN {activate | deactivate} 377
dns-content-filter fake-dns-response-ttl <300...86400> 378
dns-content-filter profile <*profilename*> 378
dns-content-filter redirect-ip custom IPv4 377
dns-content-filter redirect-ip default 377
dns-content-filter statistics flush 379
dns-content-filter white-list FQDN {activate | deactivate} 377
dns-content-filter white-list replace <1..256> FQDN {activate | deactivate} 377
dns-filter black-list FQDN {activate|deactivate} 341
dns-filter black-list replace <1..256> FQDN {activate|deactivate} 341
dns-filter fake-dns-response-ttl <300...86400> 343
dns-filter profile *profilename* 341
dns-filter redirect-ip custom IPv4 342
dns-filter redirect-ip default 342
dns-filter rename *old_profile_name new_profile_name* 342
dns-filter secure-dns {log | no log} 343
dns-filter secure-dns action {drop | pass} 343
dns-filter statistics flush 342
dns-filter white-list FQDN {activate|deactivate} 342
dns-filter white-list replace <1..256> FQDN {activate|deactivate} 342
domain match <*string*> 375
domain not-match <*string*> 375
dot11-preamble {long|short} 81
downdelay <0..1000> 156
dpd-interval <15..60> 279
draw-usage-graphics 574
dscp-marking <0..63> 168
dscp-marking <0..63> 170
dscp-marking class {default | *dscp_class*} 168
dscp-marking class {default | *dscp_class*} 170
dtim-period <1..255> 81
duration <0..300> 586
dynamic-guest freeuser *user_name* 507
dynamic-guest generate 507
dynamic-guest generate-freeuser 507
dynamic-guest keep-user-logged-in 507
eap auth_method AUTH_METHOD 290
eap auth_method *auth_method* 291
e-mail *email_address* 508
enable 120
enable 122
enable 43
encapsulation {tunnel | transport} 281
encapsulation {tunnel | transport} 292
encrypted-password *ciphertext* 303
encrypted-password *ciphertext* 498
encrypted-password *password* 508
encrypted-string ciphertext 177

exit 100
exit 107
exit 119
exit 138
exit 148
exit 163
exit 169
exit 170
exit 181
exit 203
exit 231
exit 232
exit 236
exit 255
exit 286
exit 318
exit 333
exit 363
exit 370
exit 370
exit 372
exit 372
exit 372
exit 421
exit 421
exit 422
exit 43
exit 575
exit 596
exit 68
exit 70
exit 83
exit 83
exit 84
exit 85
exit 88
exit 92
exit 94
exit 96
exit 98
expire-time *yyyy-mm-dd hh:mm* 508
FACILITY 569
fall-back-check-interval <60..86400> 279
fall-back-check-interval <60..86400> 289
fall-back-check-interval <60..86400> 291
fast forwarding {*activate* | *deactivate*} 525
fbwifi idle-detection timeout <1..60> 258
fbwifi reset-fbpage 258
fbwifi security {high |low} 258
file_name 106
file-prefix file_name 107
files-size <1..10000> 587
files-size *mon_dir_size* 107
file-suffix <*profile_name*> 587
firewall icsa {icmp-destroy-session} {enable | disable} 219
firewall-output append 229
firewall-output delete *rule_number* 229
firewall-output insert *rule_number* 229
firewall-output move *rule_number* to *rule_number* 229

firewall-output *rule_number* 229
flood-detection block-period <1..3600> 235
flush 163
follow-real-client-routing {yes | no} 422
fqdn-object query-period *<1..1440>* 460
fqdn-object sync-period *<1..5>* 460
fqdn-object test *fqdn* 461
frame-capture configure 107
friendly-ap *ap_mac description2* 98
from-zone zone_rule 234
gateway 122
gateway *ipv6_addr* metric <0..15> 120
geo-ip database update country 465
geo-ip database update weekly {fri | mon | sat | sun | thu | tue | wed} *<0..23>* 465
group1 279
group1 289
group1 291
group14 279
group14 289
group15 289
group16 289
group17 289
group18 289
group2 279
group2 289
group2 291
group5 279
group5 289
group5 291
groupname rename *groupname groupname* 446
guard-interval *wlan_htgi* 81
health-check type {*http* | *https* | *tcp* | *smtp* | *dns* | *ping*} 198
high low standard 105
host *sni* 199
host-ip {*ip-address* | *profile_name* | any> 587
HOSTNAME 569
host-port <0..65535> 587
http path *url* 199
icmp-decoder {bad-icmp-l4-size | icmp-fragment | icmp-smurf} action {drop | reject-sender | reject-receiver | reject-both} 236
icmp-decoder {bad-icmp-l4-size | icmp-fragment | icmp-smurf} log [alert] 236
idle <0..360> 303
idp anomaly rule {delete 234
idp anomaly *adp-profile* [base {all | everything | none}] 234
idp anomaly rule {append | 234
idp anomaly white-list rename *rule-name new-rule-name* 238
idp anomaly white-list *rule-name* 237
idp customize signature edit *quoted_string* 356
idp customize signature *quoted_string* 356
idp customize_import name sig_name 356
idp packet-capture {enable | disable} 363
idp packet-capture default setting 363
idp packet-capture select {add-id *sid* | del-id *sid*} 363
idp packet-capture select {enable | disable} 363
idp packet-capture show status 363
idp reload 349
idp rename anomaly 233
idp rename signature *profile1 profile2* 350
idp search signature *my_profile* name *quoted_string* sid SID severity *severity_mask* platform *plat-*

form_mask classtype *classtype_mask* service *service_mask* activate {any | yes | no} log {any | no | log | log-alert} action *action_mask* 353
idp session-block {activate | deactivate} 350
idp session-block period {1-3600} 350
idp signature default_profile 352
idp signature mode {detection | prevention} 350
idp signature *newpro* [base {all | lan | wan | dmz | none}] 351
idp signature profile signature sid {activate | log [alert] | action {drop | reject-sender | reject-receiver | reject-both}} 350
idp signature update daily <0..23> 359
idp signature update hourly 359
idp signature update signatures 359
idp signature update weekly {sun | mon | tue | wed | thu | fri | sat} <0..23> ... 359
idp statistics flush 360
idp system-protect {activate| deactivate} 349
idp white-list 363
iface {add | del} {*interface_name* | *virtual_interface_name*} 587
igmp {activate | direction {downstream | upstream} | version <1..3>} 156
igmp direction 125
igmp version *<1..3>* 125
ikev2 policy rename policy_name policy_name 290
ikev2 policy rename policy_name policy_name 291
in-dnat <1..10> protocol {all | tcp | udp} original-ip *address_name* <0..65535> <0..65535> *mapped-ip address_name* <0..65535> <0..65535> 283
in-dnat append protocol {all | tcp | udp} original-ip *address_name* <0..65535> <0..65535> mapped-ip *address_name* <0..65535> <0..65535> 283
in-dnat delete <1..10> 283
in-dnat insert <1..10> protocol {all | tcp | udp} original-ip *address_name* <0..65535> <0..65535> mapped-ip *address_name* <0..65535> <0..65535> 283
in-dnat move <1..10> to <1..10> 283
in-snat source *address_name* destination *address_name* snat *address_name* 283
interface 43
interface {*num*|append|insert *num*} *interface-name* [weight <1..10>|limit <1..2097152>|passive] 163
interface cellular budget-auto-save <5..1440> 144
interface dial *interface_name* 140
Interface dial wan1_ppp 303
Interface disconnect 303
interface disconnect *interface_name* 140
interface *interface_name* 130
interface *interface_name* 133
interface *interface_name* 134
interface *interface_name* 135
interface *interface_name* 137
interface *interface_name* 140
interface *interface_name* 153
interface *interface_name* 154
interface *interface_name* 155
interface *interface_name* 159
interface *interface_name* 257
Interface *interface_name* 303
interface *interface_name* ipv6 120
interface *interface_name* no ipv6 122
interface reset {*interface_name*|*virtual_interface_name*|all} 123
interface send statistics interval <15..3600> 123
interface-name {*ppp_interface* | *ethernet_interface*} *user_defined_name* 123
interface-rename *old_user_defined_name new_user_defined_name* 123
interval 110
ip address dhcp option-60 <text> 119
ip address *ipv4 ipv4* 147

ip dhcp pool rename *profile_name profile_name* 128
ip dhcp static _import_static_file *import file name* interface *interface name* 128
ip dns security-options {default | 1}] 516
ip dns server aaaa-record {FQDN_DNS | FQDN_WILDCARD_DNS} IPv6 516
ip dns server cache-flush 515
ip dns server cname-record {FQDN_DNS | FQDN_WILDCARD_DNS} {FQDN_DNS} 516
ip dns server rule {<1..32>|append|insert <1..32>} access-group {ALL|*address_object*} zone {ALL|*address_object*} action {accept|deny} 515
ip dns server rule move <1..32> to <1..32> 515
ip dns server zone-forwarder {<1..32>|append|insert <1..32>} {*domain_zone_name*|*} {interface *interface_name* | user-defined *ipv4_address* [interface {*interface_name* | auto}]} 606
ip dns server zone-forwarder {<1..32>|append|insert <1..32>} {*domain_zone_name*|*} user-defined *w.x.y.z {ip_type}* [private | interface {*interface_name* | auto}] 516
ip dns server zone-forwarder move <1..32> to <1..32> 516
ip dns server zone-forwarder move <1..32> to <1..32> 606
ip ftp server rule {*rule_number*|append|insert *rule_number*} access-group {ALL|*address_object*} zone {ALL|*zone_object*} action {accept|deny} 534
ip ftp server rule move *rule_number* to *rule_number* 534
ip gateway *ip* metric <0..15> 119
ip http secure-server cipher-suite {aes| rc4| des| 3des| dhe} 528
ip http secure-server table {admin|user} rule {*rule_number*|append|insert *rule_number*} access-group {ALL|*address_object*} zone {ALL|*zone_object*} action {accept|deny} 528
ip http secure-server table {admin|user} rule move *rule_number* to *rule_number* ... 528
ip http server table {admin|user} rule {*rule_number*|append|insert *rule_number*} access-group {ALL|*address_object*} zone {ALL|*zone_object*} action {accept|deny} 528
ip http server table {admin|user} rule move *rule_number* to *rule_number* 528
ip http skip-csrf-check 529
ip http-redirect activate *description* 201
ip http-redirect deactivate *description* 201
ip http-redirect *description* interface *interface_name* redirect-to *w.x.y.z* <1..65535> 201
ip http-redirect *description* interface *interface_name* redirect-to *w.x.y.z* <1..65535> deactivate 201
ip http-redirect flush 201
ip ipnp config 272
ip ospf authentication 134
ip ospf authentication message-digest 134
ip ospf authentication same-as-area 134
ip ospf cost <1..65535> 159
ip ospf dead-interval <1..65535> 160
ip ospf hello-interval <1..65535> 160
ip ospf message-digest-key <1..255> md5 *password* 134
ip ospf retransmit-interval <1..65535> 160
ip route replace {*w.x.y.z*} {*w.x.y.z*} {*interface*|*w.x.y.z*} <0..127> with {*w.x.y.z*} {*w.x.y.z*} {*interface*|*w.x.y.z*} <0..127> 174
ip ssh server rule {*rule_number*|append|insert *rule_number*} access-group {ALL|*address_object*} zone {ALL|*zone_object*} action {accept|deny} 531
ip ssh server rule move *rule_number* to *rule_number* 532
ip telnet server rule {*rule_number*|append|insert *rule_number*} access-group {ALL|*address_object*} zone {ALL|*zone_object*} action {accept|deny} 533
ip telnet server rule move *rule_number* to *rule_number* 533
ip virtual-server {activate | deactivate} *profile_name* 191
ip virtual-server delete *profile_name* 191
ip virtual-server flush 191
ip virtual-server load-balancer name 197
ip virtual-server load-balancer rename *old_name new_name* 199
ip virtual-server *profile_name* interface *interface_name* original-ip {any | IP | *address_object*} map-to {*address_object* | *ip*} map-type original-service *service_object* mapped-service *service_object* [nat-loopback [nat-1-1-map] [deactivate] | nat-1-1-map [deactivate] | deactivate] 191

ip virtual-server *profile_name* interface *interface_name* original-ip {any | IP | *address_object*} map-to {*address_object* | *ip*} map-type port protocol {any | tcp | udp} original-port <1..65535> mapped-port <1..65535> [nat-loopback [nat-1-1-map] [deactivate] | nat-1-1-map [deactivate] | deactivate] 190
ip virtual-server *profile_name* interface *interface_name* original-ip {any | IP | *address_object*} map-to {*address_object* | *ip*} map-type ports protocol {any | tcp | udp} original-port-begin <1..65535> original-port-end <1..65535> mapped-port-begin <1..65535> [nat-loopback [nat-1-1-map] [deactivate] | nat-1-1-map [deactivate] | deactivate] 190
ip virtual-server *profile_name* interface *interface_name* source-ip {any | IPv4 | address-object} original-ip {any | *ip* | *address_object*} map-to {*address_object* | *ip*} map-type any [nat-loopback [nat-1-1-map] [deactivate] | nat-1-1-map [deactivate] | deactivate] 190
ip virtual-server rename *profile_name profile_name* 191
ip6 route *destv6/prefix* { *ipv6_global_address* | *ipv6_link_local* | *interface*} [<0..127>] 174
ip6 route *destv6/prefix* { *ipv6_link_local interface*} [<0..127>] 174
ip6 route replace *destv6/prefix* { *gatewayv6* | *interface*} [<0..127>] with *destv6/prefix* { *gatewayv6* | *interface*} [<0..127>] 174
ip_address 106
ip-reputation action {block | pass} 327
ip-reputation action-level {high | medium | low} 327
ip-reputation black-list {IPv4|IPv4CIDR} {activate|deactivate} 328
ip-reputation black-list replace <1..256> IPv4 {activate|deactivate} 328
ip-reputation ebl *<profile name>* 330
ip-reputation ebl rename *old_profile_name new_profile_name* 330
ip-reputation ebl update 331
ip-reputation ebl update daily *<0..23>* 331
ip-reputation ebl update hourly 330
ip-reputation ebl update weekly *{sun |mon|tue|wed|thu|fri|sat} <0..23>* 331
ip-reputation statistics flush 329
ip-reputation update daily <0..23> 329
ip-reputation update hourly 329
ip-reputation update signatures 329
ip-reputation update weekly {sun | mon | tue | wed | thu | fri | sat} <0..23> ... 329
ip-reputation white-list {IPv4|IPv4CIDR} {activate|deactivate} 328
ip-reputation white-list replace <1..256> IPv4 {activate|deactivate} 328
ipsec-isakmp *policy_name* 281
ipsec-isakmp *policy_name* 292
ipv6 6to4 [prefix *ipv6_addr_prefix* | destination-prefix *ipv4_cidr* | relay *ipv4*] 148
ipv6 address *dhcp6_profile dhcp6_suffix_128* 121
ipv6 address *dhcp6_profile dhcp6_suffix_128* 122
ipv6 address *ipv6_addr_prefix* 148
ipv6 dhcp6 [client] 140
ipv6 dhcp6 duid { *duid* | mac } 141
ipv6 neighbor flush {*ipv6* | all} 589
ip-version {ip|ip6|any} 587
isakmp policy rename *policy_name policy_name* 280
keystring *pre_shared_key* 280
keystring pre_shared_key 290
keystring pre_shared_key 291
l2-isolation 215
l2tp-over-ipsec *address-object* 301
l2tp-over-ipsec authentication *authentication profile_name* 302
l2tp-over-ipsec crypto *map_name* 301
l2tp-over-ipsec recover default-ipsec-policy 301
lacp-rate {fast | slow} 156
language *language_name* 523
language update daily <0..23> 523
language update hourly 523
language update package 523
language update weekly {sun | mon | tue | wed | thu | fri | sat} <0..23> 523

lan_port {activate | inactivate} pvid <1..4094> 60
lan-provision ap *ap_mac* 60
lan-provision *lan_port* {activate | inactivate} pvid <1..4094> 58
lan-provision *vlan_interface* {activate | inactivate} vid <1..4094> join *lan_port* {tag | untag} [*lan_port* {tag | untag}] [*lan_port* {tag | untag}] 59
ldap {activate|deactivate} 495
ldap ip {*ip*|*fqdn*} port <1..65535> [id *name* password *password*] [deactivate] 495
led_locator *ap_mac_address* blink-timer <1..60> 113
led_locator *ap_mac_address* off 113
led_locator *ap_mac_address* on 113
led_suppress *ap_mac_address* disable 112
led_suppress *ap_mac_address* enable 112
lifetime <180..3000000> 279
lifetime <180..3000000> 289
lifetime <180..3000000> 291
limit-ampdu < *100..65535*> 78
limit-amsdu <*2290..4096*> 78
link-monitoring {arp | mii | none} 155
link-sticking outgoing interface {*interface_name* | all} 209
load-balance-algorithm {*rr*|*wrr*|*lc*|*sh*} 197
load-balancing [slot1 | slot2] alpha <1..255> 71
load-balancing [slot1 | slot2] beta <1..255> 71
load-balancing [slot1 | slot2] kickInterval <1..255> 71
load-balancing [slot1 | slot2] liInterval <1..255> 72
load-balancing [slot1 | slot2] max sta <1..127> 72
load-balancing [slot1 | slot2] sigma <51..100> 72
load-balancing [slot1 | slot2] timeout <1..255> 72
load-balancing [slot1 | slot2] traffic level {high | low | medium} 72
load-balancing mode [slot1 | slot2] {station | traffic | smart-classroom} 72
loadbalancing-index <inbound|outbound|total> 164
local-address *w.x.y.z* 303
local-id type {ip *ip* | fqdn *domain_name* | mail *e_mail* | dn *distinguished_name*} .. 280
local-id type {ip ip | fqdn domain_name | mail e_mail | dn distinguished_name} 290
local-id type {ip IPv6 | fqdn domain_name | mail e_mail | dn distinguished_name} 291
local-ip {ip {*ip* | *domain_name*} | interface *interface_name*} 280
local-ip {ip {ip | domain_name} | interface interface_name} 289
local-ip {ip IPv6} 291
local-ip *ip* 285
local-policy *address_name* 282
local-policy *address_name* 293
location *location* 68
logging console category *module_name* level {alert | crit | debug | emerg | error | info | notice | warn} 570
logging mail <1..2> schedule daily hour <0..23> minute <0..59> 570
logging mail <1..2> schedule weekly day *day* hour <0..23> minute <0..59> 570
logging mail <1..2> sending_now 569
logging system-log category *module_name* {disable | level normal | level all} 566
logging usb-storage category *category* disable 149
logging usb-storage category *category* level <all|normal> 149
logging usb-storage category *module_name* level {all | normal} 566
logging usb-storage delete over-keep-duration 566
logging usb-storage flushThreshold <1..100> 149
logging usb-storage flushThreshold <1..100> 566
logging usb-storage keep-duration day <1..365> 567
login-mac *mac_address* 508
login-page background-color {*color-rgb* | *color-name* | *color-number*} 511
login-page message-color {*color-rgb* | *color-name* | *color-number*} 511
login-page title *title* 512
login-page title-color {*color-rgb* | *color-name* | *color-number*} 512

login-page window-color {*color-rgb* | *color-name* | *color-number*} 512
logo background-color {*color-rgb* | *color-name* | *color-number*} 512
mac *mac* 137
mail-attach password <*attachment password*> 596
mail-info {*mail-to-1*|*mail-to-2*|*mail-to-3*|*mail-to-4*|*mail-to-5*} <user@domainname> 596
mail-info content <*mail-content*> 596
mail-server 519
mail-subject set *subject* 574
marked-interface any 311
marked-interface interface vlan<1..4064> 311
marked-interface none 311
marked-interface trunk trunk_name 311
max-sw-retries <0..10> 81
miimon <1..1000> 156
mode {802_3ad | active-backup | balance-alb | mode 802_3ad} 155
mode {main | aggressive} 279
mode {normal|trunk} 164
mode-config activate 283
mode-config address- *profile_name* 283
MODULE_NAME_WTP 569
MODULE_NAME_WTP_ 569
mon_dir_size 106
monitoring flush 98
monitor-mode id <organization-id> 249
move <1..8> to <1..8> 164
mtu <576..1492> 140
mtu <576..1492> 144
multicast pps <1~10000> 83
multicast pps <1~10000> 84
myzyxel-service get-cloud-timezone 513
myzyxel-service set-timezone-according-cloud 513
name *description* 508
name DNS_OPTIONS_NAME 516
nd ra accept 120
nd ra accept 122
nd ra advertise 120
nd ra advertise 122
nd ra default-lifetime 122
nd ra default-lifetime <4..9000> 121
nd ra hop-limit 122
nd ra hop-limit <0..255> 120
nd ra managed-config-flag 120
nd ra managed-config-flag 122
nd ra max-rtr-interval 122
nd ra max-rtr-interval <4..1800> 120
nd ra min-rtr-interval 122
nd ra min-rtr-interval <3..1350> 120
nd ra mtu 122
nd ra mtu <1280..1500> | <0> 120
nd ra other-config-flag 120
nd ra other-config-flag 122
nd ra prefix-advertisement *dhcp6_profile dhcp6_suffix_64* 121
nd ra prefix-advertisement DHCP6_PROFILE DHCP6_SUFFIX_64 122
nd ra prefix-advertisement *ipv6_addr_prefix* [auto { on | off}] [link{ on | off }] [preferred-time { <0..4294967294> | infinity }] [valid-time{ <0..4294967294> | infinity }] 120
nd ra reachable-time 122
nd ra reachable-time <0..3600000> 120
nd ra retrans-timer 122
nd ra retrans-timer <0..4294967295> 121

nd ra router-preference {low | medium | high } 120
network *ip mask* 129
network IP/<1..32> 129
no *{mail-to-1|mail-to-2|mail-to-3|mail-to-4|mail-to-5}* 596
no additional-from-cache activate 517
no address-object *object_name* 459
no address-object-group {any | PROFILE} 517
no anti-spam dnsbl domain *dnsbl_domain* 407
no anti-spam xheader {mail-content | virus-outbreak} 401
no anti-spam xheader mail-phishing 401
no anti-virus black-list {md5-hash md5-pattern | sha256-hash sha256-pattern | file-pattern file-pattern} 320
no anti-virus mail-infect-ext activate 317
no anti-virus white-list {md5-hash md5-pattern | sha256-hash sha256-pattern | file-pattern file-pattern} 320
no application-object <object> 455
no application-object <profile-name> 314
no area IP virtual-link IP message-digest-key <1..255> 179
no arp *ip* 590
no authentication key 177
no auth-server authentication 490
no auth-server authentication 518
no bind 234
no budget log 143
no budget log-percentage 143
no ca category {local|remote} *certificate_name* 496
no ca validation *name* 496
no content-filter profile *filtering_profile* [commtouch-url] match {log} 374
no content-filter profile *filtering_profile* [commtouch-url] offline {log} 374
no content-filter profile *filtering_profile* [commtouch-url] unrate {log} 374
no content-filter profile *filtering_profile* commtouch-url match {log} 374
no content-filter profile *filtering_profile* commtouch-url match-unsafe {log} 373
no content-filter profile *filtering_profile* commtouch-url offline {log} 374
no content-filter profile *filtering_profile* commtouch-url unrate {log} 374
no description 234
no dhcp6-lease-object *dhcp6_profile* 505
no dhcp6-request-object *dhcp6_profile* 505
no dhcp-option <1..254> 129
no dns-content-filter black-list FQDN 377
no dns-content-filter white-list FQDN 377
no dns-filter black-list FQDN 341
no dns-filter white-list FQDN 342
no dscp-marking 169
no dscp-marking 170
no friendly-ap *ap_mac* 98
no icmp-decoder {bad-icmp-l4-size icmp-fragment | icmp-smurf} log 236
no icmp-decoder {bad-icmp-l4-size | icmp-fragment | icmp-smurf} action 236
no idp anomaly <profile3> 233
no idp anomaly rule <1..32> 234
no idp anomaly white-list *rule-name* 237
no idp customize signature *custom_sid* 356
no idp signature *profile3* 350
no ip dns server rule <1..32> 516
no ip dns server zone-forwarder <1..4> 606
no ip ftp server rule *rule_number* 534
no ip http secure-server table {admin|user} rule *rule_number* 528
no ip http server table {admin|user} rule *rule_number* 528
no ip http skip-csrf-check 529
no ip http-redirect *description* 201

no ip ospf authentication 134
no ip ospf message-digest-key 134
no ip ssh server rule *rule_number* 532
no ip telnet server rule *rule_number* 533
no ip virtual-server load-balancer name 199
no ip virtual-server *profile_name* 190
no ip6 route *destv6/prefix* { *gatewayv6* | *interface*} [<0..127>] 174
no ip-reputation black-list IPv4 328
no ip-reputation ebl <*profile name*> 330
no ip-reputation white-list IPv4 328
no l2-isolation activate 215
no l2-isolation white-list activate 215
no l2-isolation white-list *rule_number* 215
no l2tp-over-ipsec session tunnel-id <0..65535> 302
no mac 137
no mail-attach password 596
no mail-info content 596
no mail-subject set 574
no network 129
no object-group application <object> 456
no packet-trace 43
no *rap slot_name* ssid-profile <1..6> 66
no real-server *address* 198
no recursion activate 517
no rogue-ap *ap_mac* 97
no sa spi *spi* 288
no sa tunnel-name *map_name* 288
no scan-detection sensitivity 234
no schedule-object *object_name* 470
no security-service ip6-exception profile_name 427
no security-service ip-exception profile_name 427
no server-auth <1..2> 91
no server-type 502
no service-object *object_name* 467
no signature *sid* action 352
no signature *sid* action 352
no signature *sid* log 351
no snmp-server rule *rule_number* 536
no ssl-inspection profile SSI_profile_name 423
no sslvpn login-port 296
no sslvpn policy *profile_name* 297
no storm-control ethernet ap mac_address 83
no storm-control wireless ap mac_address 84
no tcp-decoder {tcp-xxx} log 235
no threat-website ebl <*profile name*> 336
no udp-decoder {bad-udp-l4-size | udp-land | udp-smurf} action 235
no udp-decoder {bad-udp-l4-size | udp-land | udp-smurf} log 235
no use-defined-mac 137
no user 286
no username *username* 444
no vpn-configuration-provision port 287
no web-auth redirect-parameter 254
nslookup 43
nslookup {*ipv4* | *hostname*} [server *ipv4*] [extension *filter-extension*] 579
nslookup6 {*ipv6* | *hostname*} [server *ipv6*] [extension *filter-extension*] 579
ntp sync 513
object-group address rename *group_name group_name* 464
object-group application <object> 456
object-group application rename <object> <object> 456

object-group service rename *group_name group_name* 469
ocsp {activate|deactivate} 495
ocsp url *url* [id *name* password *password*] [deactivate] 496
output-power *wlan_power* 82
out-snat source *address_name* destination *address_name* snat *address_name* 282
packet-capture configure 586
packet-trace 43
packet-trace [interface *interface_name*] [[ip-proto|ipv6-proto] | *protocol_name* | any}] [src-host {*ip* | *hostname* | any}] [dst-host {*ip* | *hostname* | any}] [host {ip| hostname| any}] [port {<1..65535> | any}] [file] [duration <1..3600>] [extension-filter arp| link-header| data-header| match-port port port| match-host host host] 586
password *isp_account_password* 303
password *password* 508
payment-info {cash | payment-service} 508
payment-service account-delivery *delivery_method* {deactivate | activate} 266
payment-service check paypal-currency 269
payment-service fail-page failed-message *message* 266
payment-service mobile-fail-page failed-message *message* 266
payment-service mobile-profile-page selection-message *message* 267
payment-service mobile-sms-page info-message *message* 267
payment-service mobile-success-page {*notification-message* | *successful-message* | notification-message-color {#00FF00 | *color_name* | rgb(0,0,255)} 267
payment-service profile-page selection-message *message* 267
payment-service provider paypal 266
payment-service provider paypal account *e-mail* 268
payment-service provider paypal currency *paypal_currency* 268
payment-service provider paypal exit 266
payment-service provider paypal gateway *payment_gw_url* 269
payment-service provider paypal identity-token *paypal_token* 268
payment-service provider paypal no account 268
payment-service provider paypal no identity-token 268
payment-service provider select *provider* 266
payment-service success-page {account-message *message* | format-date {dd-mm-yyyy | mm-dd-yyyy | yyyy-mm-dd} | notification-message *message* | notification-message-color {#00FF00 | *color_name* | rgb(0,0,255)} | successful-message *message}* 267
peer-id type {any | ip *ip* | fqdn *domain_name* | mail *e_mail* | dn *distinguished_name*} 280
peer-id type {any | ip ip | fqdn domain_name | mail e_mail | dn distinguished_name} 290
peer-id type {any | ip IPv6 | fqdn domain_name | mail e_mail | dn distinguished_name} 291
peer-ip {*ip* | *domain_name*} [*ip* | *domain_name*] 280
peer-ip {ip | domain_name} [ip | domain_name] 289
peer-ip {ip IPv6] 291
peer-ip *ip* 285
persistence granularity *netmask* 198
persistence timeout *1-86400* 197
phone *phone_number* 509
ping 43
Ping {*ipv4* | *hostname*} [source *ipv4*] [size <0..65507>] [forever| count <1..4096>] 587
ping {ipv4_addr | *hostname*} [source *ipv4*] [size <0..65507>] [forever | count <1..4096>] [interface *interface_name*] [extension *filter-extension*] 588
ping6 43
ping6{*ipv6* | *hostname*} [source *ipv6*] [size <0..65527>] [forever| count <1..4096>] [interface {*interface_name* | *virtual_interface_name*}][extension *filter_extension*] 588
ping-check 156
ping-check {*domain_name* | *ip*} 159
ping-check {*domain_name* | *ip*} fail-tolerance <1..10> 159
ping-check {*domain_name* | *ip*} method {icmp | tcp} 159
ping-check {*domain_name* | *ip*} period <5..30> 159
ping-check {*domain_name* | *ip*} port <1..65535> 159
ping-check {*domain_name* | *ip*} timeout <1..10> 159

ping-check {FQDN | IPv4 | default-gateway} [period <5..3600>] [timeout <1..10>] [fail-tolerance <1..10>] [method {icmp | tcp}] [port <1..65535>] [probe-condition {any | all}] 135
pn-check-thres <0..100> 82
policy {*policy_number* | append | insert *policy_number*} 168
policy default-route 171
policy delete *policy_number* 171
policy flush 171
policy list table 171
policy move *policy_number* to *policy_number* 171
policy6 {*policy_number* | append | insert *policy_number*} 169
port <1..65535> ending-port <1..65535>] 502
port <1..65535> ending-port <1..65535>] [program-path *program-path*] 502
port status Port<1..*x*> 137
price *price* 264
printer-ip *ip_address* 509
printer-ip *ipv4_address* 270
printer-manager button {a | b | c} *profile_name* 269
printer-manager discover 269
printer-manager encrypt secret-key *secret_key* 269
printer-manager multi-printout <1..3> 269
printer-manager port <1..65535> 269
printer-manager printer append 269
printer-manager printout-type {customized | default} 270
priority-code <0..7> 311
proto-type {icmp | icmp6 | igmp | igrp | pim | ah | esp | vrrp | udp | tcp | any} 587
psk *psk* 96
psm 43
pwd-expiry expiration send-now 445
pwd-expiry link-to-device custom {myrouter | <FQDN> | <IPv6 Address> | <W.X.Y.X>} 445
quit 181
quota {total | upload | download} gigabytes <0..100> 264
quota {total | upload | download} gigabytes <0..100> 509
quota {total | upload | download} megabytes <0..1023> 264
quota {total | upload | download} megabytes <0..1023> 509
quota type {total | upload-download} 264
quota type {total | upload-download} 509
radio-24g: none 105
radio-5g: none 105
rap *slot_name* output-power *wlan_power* 66
rap slot_name ssid-profile <1..6> *ssid_profile_name* [tunlif *interface*] vid *vlan_id* 66
real-server *address* mapped-port *port* weight *weight* [hash *hash*] 198
reboot 43
redirect-service *<1..20>* 203
redirect-service append *<1..20>* 203
redirect-service flush 204
redirect-service insert *<1..20>* 204
redirect-service move *<1..20>* to *<1..20>* 204
redistribute {static | ospf} metric <0..16> 177
release 43
release dhcp *interface-name* 130
remaining-time <1..25920000> 509
remote-assistance [address1|address2] *ipv4* 580
remote-assistance [https|ssh] port *port* 580
remote-assistance generate user-password 580
remote-assistance remove {address1|address2} 580
remote-assistance schedule DATE TIME *date time* 580
remote-assistance settings [random|manual] 580
remote-assistance user-object *user* 580
remote-policy *address_name* 282

remote-policy *address_name* 293
rename 43
rename {/conf | /idp | /packet_trace | /script | /tmp}/*old-file_name* {/conf | /idp | /packet_trace | /script | /tmp}/*new-file_name* 546
rename /script/*old-file_name* /script/*new-file_name* 546
renew 43
renew dhcp *interface-name* 130
replenish enable 509
report packet size statistics clear 574
reset-counter-now 575
respmsg url-filter block-page background-color {<rgb(0,0,255)> | <color name> | <#00FF00>} 522
respmsg url-filter block-page banner-color {<rgb(0,0,255)> | <color name> | <#00FF00>} 522
respmsg url-filter block-page banner-message-color {<rgb(0,0,255)> | <color name> | <#00FF00>} 522
respmsg url-filter block-page message-color {<rgb(0,0,255)> | <color name> | <#00FF00>} 522
retry *1-99* 198
ring-buffer <enable|disable> 587
rogue-ap *ap_mac description2* 97
rogue-ap containment 100
rogue-ap detection 97
role *wlan_role* 82
router bgp 181
router ospf 134
router ospf 177
router ospf 178
router ospf 178
router rip 133
router rip 177
Router(config)# 111
Router(config)# 524
Router(config)# auto-healing activate 111
Router(config)# auto-healing power-threshold -70 111
Router(config)# exit 105
Router(config)# show auto-healing config 111
Router(config)# wireless-health-action aggressiveness 105
Router(config)# wireless-health-action aggressiveness low 105
Router(config)# zon lldp server 524
Router(config)# zon lldp server status 524
router(config-sso-primary)# 259
router(config-sso-primary)# 259
router(config-sso-secondary)# 259
router(config-sso-secondary)# [no] port <1025..65535> 259
Router(SIP Signaling Port)# [no] port <1025..65535> 207
Router# show wireless-health-action 105
Router> configure terminal 105
rssi-dbm <-20~-76> 82
rssi-interval (1..86400> 82
rssi-kickout <-20~-105> 82
rssi-optype <0-3> 82
rssi-privilegetime 82
rssi-retrycount <1~100> 82
rssi-verifytime 82
rtls ekahau ip address *<ip>* 325
rtls ekahau ip port <1..65535> 325
run 43
run /script/*file_name.zysh* 546
rx-mask *chain_mask* 82
sandbox dashboard statistics flush 345

sandbox dashboard statistics flush 346
sandbox file-scanning-log {log | log-alert | no} 345
sandbox file-send-log {log | log-alert | no} 345
sandbox malicious-action malicious {allow | destroy} {log | log-alert | no} 345
sandbox malicious-action suspicious {allow | destroy} {log | log-alert | no} 345
sandbox mdb flush 345
sandbox response-clean-log {log | log-alert | no} 346
sandbox server-file {delete | keep} 346
sandbox statistics flush 346
scan-detection block-period <1..3600> 234
scan-detection sensitivity {low | medium | high} 234
scan-dwell <*100..1000*> 85
scan-method *scan_method* 84
scenario {site-to-site-static|site-to-site-dynamic|remote-access-server|remote-access-client} 282
scenario {site-to-site-static|site-to-site-dynamic|remote-access-server|remote-access-client} 293
schedule hour <0..23> minute <00..59> 519
schedule hour <0..23> minute <00..59> 575
schedule reboot daily <*time,hh:mm*> 594
schedule reboot monthly <*time,hh:mm*> <*day,dd*> 595
schedule reboot weekly <*time,hh:mm*> {*sun|mon|tue|wed|thu|fri|sat*} 594
schedule *schedule_object* 82
schedule-object *object_name date time date time* 471
schedule-object *object_name time time* [*day*] [*day*] [*day*] [*day*] [*day*] [*day*] [*day*] 471
scheduler daily <*time,hh:mm*> 596
scheduler monthly <*time,hh:mm*> <*day,dd*> 596
scheduler weekly <*time,hh:mm*> {*sun|mon|tue|wed|thu|fri|sat*} 596
schedule-run 1 *file_name.zysh* {daily | monthly | weekly} time {*date* | sun | mon | tue | wed | thu | fri | sat} 546
secumanager server {IPv4| FQDN} port <1...65535> 244
secumanager server-ca {default| CERT_NAME} 244
secure policy <1...500> device <profile name> 440
secure-policy <profile name> 222
secure-policy activate 218
secure-policy append 219
secure-policy backup activate 218
secure-policy default-rule action {allow | deny | reject} { no log | log [alert] } 219
secure-policy delete *rule_number* 219
secure-policy flush 219
secure-policy insert *rule_number* 219
secure-policy move *rule_number* to *rule_number* 219
secure-policy *rule_number* 219
secure-policy *zone_object* {*zone_object*|ZyWALL} append 219
secure-policy *zone_object* {*zone_object*|ZyWALL} delete <1..5000> 219
secure-policy *zone_object* {*zone_object*|ZyWALL} flush 219
secure-policy *zone_object* {*zone_object*|ZyWALL} insert *rule_number* 219
secure-policy *zone_object* {*zone_object*|ZyWALL} move *rule_number* to *rule_number* 219
secure-policy *zone_object* {*zone_object*|ZyWALL} *rule_number* 219
secure-policy6 append 220
secure-policy6 default-rule action {allow | deny | reject} { no log | log [alert] } 221
secure-policy6 delete *rule_number* 221
secure-policy6 flush 221
secure-policy6 insert *rule_number* 221
secure-policy6 move *rule_number* to *rule_number* 221
secure-policy6 *rule_number* 220
secure-policy6 *zone_object* {*zone_object*|ZyWALL} append 220
secure-policy6 *zone_object* {*zone_object*|ZyWALL} delete <1..5000> 220
secure-policy6 *zone_object* {*zone_object*|ZyWALL} flush 220
secure-policy6 *zone_object* {*zone_object*|ZyWALL} insert *rule_number* 220
secure-policy6 *zone_object* {*zone_object*|ZyWALL} move *rule_number* to *rule_number* 220

secure-policy6 *zone_object* {*zone_object*|ZyWALL} *rule_number* 220
secure-policy-style {*general* | *advance*} 224
secure-policy-style advance all-inspect-by-policy 224
secu-reporter activate {no | yes} 245
secu-reporter adp {activate|deactivate} 245
secu-reporter anti-botnet {activate|deactivate} 246
secu-reporter anti-spam {activate|deactivate} 245
secu-reporter anti-virus {activate|deactivate} 245
secu-reporter ap-managed {activate|deactivate} 245
secu-reporter app-patrol {activate|deactivate} 245
secu-reporter content-filter {activate|deactivate} 245
secu-reporter idp {activate|deactivate} 246
secu-reporter interface-statistics {activate|deactivate} 246
secu-reporter on-cloud-config {dns-threat-filter| ip-reputation| url-threat-filter} update 246
secu-reporter reputation-filter {activate|deactivate} 246
secu-reporter sandbox {activate|deactivate} 246
secu-reporter traffic-log {activate | deactivate} 245
secu-reporter traffic-log {activate|deactivate} 246
secu-reporter upload-filesize *<1..10>* 245
secu-reporter upload-interval *<60..600>* 245
secu-reporter vpn {activate|deactivate} 246
security-service anti-spam inspect *{all-traffic | by-policy}* 403
security-service anti-virus inspect *{all-traffic | by-policy}* 318
security-service dns-filter inspect *{all-traffic | by-policy}* 343
security-service ip6-exception {profile_name} 427
security-service ip-exception {*profile_name*} 426
security-service ips inspect *{all-traffic | by-policy}* 349
security-service threat-website inspect *{all-traffic | by-policy}* 333
security-service update-server server-url <url> 55
send-now 575
serial-number *number* 509
server {*domain_name* | *w.x.y.z*} 303
server-type {file-sharing | owa | web-server} url URL [entry-point *entry_point*] . 501
server-type file-sharing share-path *share-path* 502
server-type rdp server-address *server-address* [starting- 502
server-type vnc server-address *server-address* [starting- 502
server-type weblink url *url* 502
service-object *object_name* {tcp | udp} {eq <1..65535> | range <1..65535> <1..65535>} 467
service-object *object_name* icmp *icmp_value* 468
service-object *object_name* icmpv6 {<0..255> | neighbor-solicitation | router-advertisement | echo | packet-toobig | router-solicitation | echo-reply | parameter-problem | time-exceeded | neighbor-advertisement | redirect | unreachable} 468
service-object *object_name* protocol <1..255> 468
service-object rename *object_name object_name* 468
service-register checkexpire 54
service-register _setremind {after-10-days | after-180-days | after-30-days | every-time | never} 54
session timeout {udp-connect <1..300> | udp-deliver <1..300> | icmp <1..300>} ... 581
session timeout session {tcp-established | tcp-synrecv | tcp-close | tcp-finwait | tcp-synsent | tcp-closewait | tcp-lastack | tcp-timewait} <1..300> 581
session-limit append 231
session-limit delete *rule_number* 231
session-limit flush 231
session-limit insert *rule_number* 231
session-limit limit <0...20000> 231
session-limit move *rule_number* to *rule_number* 231
session-limit *rule_number* 231
session-limit6 append 232

session-limit6 delete *rule_number* 232
session-limit6 flush 232
session-limit6 insert *rule_number* 232
session-limit6 limit <0...20000> 231
session-limit6 move *rule_number* to *rule_number* 232
session-limit6 *rule_number* 231
session-page {activate | deactivate} 254
session-status-update alg {active|inactive} 221
session-status-update reply-time <5..300> 221
set firmware boot number <1..2> 546
set firmware boot option <0..1> 546
set pfs {group1 | group2 | group5 | none} 282
set pfs {group1 | group2 | group5 | none} 293
set security-association lifetime seconds <180..3000000> 282
set security-association lifetime seconds <180..3000000> 293
set session-key {ah <256..4095> *auth_key* | esp <256..4095> [cipher *enc_key*] authenticator *auth_key*} 285
setenv 43
setenv-startup stop-on-error off 546
show 128
show 310
show 400
show 43
show 519
show [all] 318
show {address-object | address6-object | service-object | schedule-object} [*object_name*] 459
show {ip-reputation| dns-filter| threat-website} sr-allow-list 246
show aaa authentication {*group-name*|default} 479
show aaa group server ad *group-name* 474
show aaa group server ldap *group-name* 475
show aaa group server radius *group-name* 477
show access-page settings 512
show account [pppoe *profile_name* | pptp *profile_name*] 498
show account cellular *profile_name* 499
show account l2tp [*profile_name*] 303
show ad-server 472
show advertisement 276
show advertisement activation 276
show anti-botnet dashboard statistics summary 51
show anti-botnet signature update 337
show anti-botnet signatures date 332
show anti-botnet signatures number 332
show anti-botnet signatures version 332
show anti-botnet statistics collect status 339
show anti-botnet statistics recent-activities 339
show anti-botnet statistics summary 339
show anti-botnet status 332
show anti-botnet update status 337
show anti-spam black-list [status] 405
show anti-spam dashboard statistics summary 51
show anti-spam dnsbl domain 407
show anti-spam dnsbl ip-check-order 407
show anti-spam dnsbl max-query-ip 407
show anti-spam dnsbl query-timeout {smtp | pop3} 407
show anti-spam dnsbl query-timeout time 408
show anti-spam dnsbl statistics 407
show anti-spam dnsbl status 407
show anti-spam ip-reputation high-sensitivity 402
show anti-spam ip-reputation private-check 402
show anti-spam ip-reputation query-timeout time 401

show anti-spam ip-reputation statistics 410
show anti-spam mail-phishing query-timeout pop3 402
show anti-spam mail-phishing query-timeout smtp 402
show anti-spam mail-phishing query-timeout time 402
show anti-spam mail-phishing status 402
show anti-spam mail-scan query-timeout pop3 402
show anti-spam mail-scan query-timeout smtp 402
show anti-spam mail-scan query-timeout time 402
show anti-spam mail-scan statistics 410
show anti-spam mail-scan status 402
show anti-spam profile [*rule_number*] 400
show anti-spam statistics collect 409
show anti-spam statistics ranking {source | mail-address} 410
show anti-spam statistics summary 409
show anti-spam tag {dnsbl | dnsbl-timeout} 407
show anti-spam tag {mail-content | mail-phishing | virus-outbreak} 402
show anti-spam tag black-list 405
show anti-spam tag mail-phishing 402
show anti-spam tag query-timeout 402
show anti-spam white-list [status] 405
show anti-spam xheader {mail-content | mail-phishing | virus-outbreak} 402
show anti-spam xheader {white-list | black-list} 405
show anti-spam xheader dnsbl 408
show anti-spam xheader mail-phishing 402
show anti-spam xheader query-timeout 403
show anti-virus black-list 319
show anti-virus black-list status 319
show anti-virus cloud-query ftype-identify status 317
show anti-virus cloud-query status 317
show anti-virus eicar activation 317
show anti-virus profile 319
show anti-virus profile [profile_name] 319
show anti-virus scan mode status 317
show anti-virus search signature {all | name virus_name} [{from id to id}] 321
show anti-virus signatures status 322
show anti-virus skip-unknown-file-type activation 317
show anti-virus statistics collect 323
show anti-virus statistics ranking {destination | destination6 | source | source6 | virus-name} 323
show anti-virus statistics summary 323
show anti-virus statistics summary 51
show anti-virus update 322
show anti-virus update status 322
show anti-virus white-list 320
show anti-virus white-list status 320
show ap-group first-priority 72
show ap-group-profile {all | *ap_group_profile_name*} 72
show ap-group-profile *ap_group_profile_name* lan-provision interface {all | vlan | ethernet | *ap_lan_port* | *vlan_interface*} model {nwa5301-nj | wac6502d-e | wac6502d-s | wac6503d-s | wac6553d-e} 72
show ap-group-profile ap_group_profile_name lan-provision model 73
show ap-group-profile *ap_group_profile_name* load-balancing config 72
show ap-group-profile rule_count 73
show ap-info {*mac_address* | all} {sta | usage} {24G | 5G | 6G| all} *timer* 47
show ap-info top 10 alert {2.4G | 5G | 6G| all} 101
show ap-info top *number* {sta | usage} *timer* 47
show ap-info total {sta | usage} {24G | 5G | 6G| all} *timer* 47
show app category <*category_id*> 314
show app profiles 314

show app profiles <profile-name> 314
show app profiles <profile-name> application 314
show app profiles <profile-name> application category {*category_id* | all} 314
show app search-name <*application_keyword*> 314
show app signature update 314
show app signatures date 314
show app signatures status 314
show app signatures version 314
show app statistics collect 314
show app statistics summary 314
show app tag info 315
show app update status 315
show application-object <object> 455
show app-watch-dog config 599
show app-watch-dog monitor-list 599
show app-watch-dog reboot-log 599
show arp-table 590
show auth-server status 491
show auth-server status 518
show auth-server trusted-client 491
show auth-server trusted-client 518
show auth-server trusted-client *profile_name* 491
show auth-server trusted-client *profile_name* 518
show auto-healing config 111
show bgp [global |neighbor] 182
show bgp [summary | route | mem] 182
show billing discount default rule 263
show billing discount rule 263
show billing discount status 263
show billing profile [*profile_name*] 263
show billing status 263
show boot status 47
show bridge available member 154
show bwm activation 171
show bwm activation 308
show bwm all 308
show bwm applications list 308
show bwm default 308
show bwm highest sip bandwidth priority 308
show bwm-usage < [policy-route *policy_number*] | [interface *interface_name*] 171
show ca category {local|remote} 496
show ca category {local|remote} name *certificate_name* certpath 496
show ca category {local|remote} name *certificate_name* format {text|pem} 496
show ca hierarchy name *certificate_name* [format all | cn | file] 496
show ca spaceusage 496
show ca validation name *name* 496
show capwap ap {all | *ap_mac*} 60
show capwap ap {all | *ap_mac*} 60
show capwap ap {all | ap_mac} config 60
show capwap ap {all | *ap_mac*} config status 61
show capwap ap ac-ip 605
show capwap ap ac-ip 61
show capwap ap all lite2 108
show capwap ap all statistics 61
show capwap ap *ap_mac slot_name* detail 60
show capwap ap discovery-type 605
show capwap ap fallback 61
show capwap ap fallback interval 61
show capwap ap idle timeout 61

show capwap ap info 605
show capwap ap wait-list 61
show capwap manual-add 61
show capwap station all 61
show cdr block-list 416
show cdr event-list 416
show cdr rules 416
show cdr signature 416
show cdr status 416
show cdr update 416
show cdr white-list 416
show clock date 513
show clock status 514
show clock time 514
show cloud-helper autoupdate firmware 550
show cloud-helper firmware 550
show cloud-helper highlight 550
show cloud-helper notify_all 550
show cloud-helper remind 550
show cloud-helper retry 550
show cnm-agent configuration 241
show comport status 47
show config-backup status 596
show config-backup status 596
show conn [user {*username*|any|unknown}] [service {*service-name*|any|unknown}] [source {*ip*|any}] [destination {*ip*|any}] [begin <1..128000>] [end <1..128000>] [dstcc {*country-code*|any}] [srtcc {*country-code*|any}] fastpath 573
show conn ip-traffic destination 573
show conn ip-traffic source 573
show conn status 573
show connectivity-check continuous-log status 135
show connectivity-check continuous-log status 566
show console 514
show content-filter common-list {trust|forbid} 371
show content-filter dashboard statistics summary 51
show content-filter https-domain-filter status 371
show content-filter passed warning 371
show content-filter profile 375
show content-filter profile [*filtering_profile]* 375
show content-filter profile [*filtering_profile]* commtouch 375
show content-filter profile commtouch 375
show content-filter safesearch 375
show content-filter settings 371
show content-filter statistics collect 376
show content-filter statistics summary 376
show content-filter statistics summary 376
show corefile copy usb-storage 150
show country-code list 61
show cpu all 47
show cpu average 578
show cpu status 47
show cpu-temperature-monitor status 52
show crypto boost-tcp 279
show crypto map [*map_name*] 281
show crypto map6 [*map_name*] 292
show daily-report status 574
show ddns [*profile_name*] 187
show ddns-status 187
show default country-code 61

show device identify status 439
show device info all 439
show device info ip <ip address> 439
show device info mac <mac address> 439
show device profile <profile name> 439
show device profile all 439
show device-ha ap-mode backup sync 432
show device-ha ap-mode backup sync status 432
show device-ha ap-mode backup sync summary 432
show device-ha ap-mode forwarding-port *interface_name* 432
show device-ha ap-mode interfaces 432
show device-ha ap-mode master sync 432
show device-ha ap-mode next-sync-time 432
show device-ha ap-mode status 432
show device-ha mode 432
show device-ha status 430
show device-ha2 activation 435
show device-ha2 device-status 435
show device-ha2 firmware-update check-timeout 436
show device-ha2 firmware-update delay 436
show device-ha2 firmware-update status 436
show device-ha2 interfaces 436
show device-ha2 log 436
show device-ha2 mgnt-iface 436
show device-ha2 mode 435
show device-ha2 passive device-status 435
show device-ha2 passive log 436
show device-ha2 passive trace-log 436
show device-ha2 schedule-reboot check-timeout 595
show device-ha2 schedule-reboot delay 595
show device-ha2 status 436
show device-ha2 sync status 436
show device-ha2 sync summary 436
show device-ha2 trace-log 436
show device-ha2 virtual-mac 436
show device-register status 54
show dhcp6 interface 504
show dhcp6 lease-object [*dhcp6_profile*] 504
show dhcp6 object-binding *interface_name* 504
show dhcp6 request-object [*dhcp6_profile*] 504
show diag-info 578
show diag-info copy usb-storage 149
show disk 47
show dns-content-filter {white-list | black-list} 377
show dns-content-filter dashboard statistics summary 377
show dns-content-filter fake-dns-response-ttl 378
show dns-content-filter profile {all | profileName} 377
show dns-content-filter search FQDN 378
show dns-content-filter statistics collect 379
show dns-content-filter statistics list 379
show dns-content-filter statistics summary 379
show dns-content-filter status 378
show dns-filter {white-list|black-list} 342
show dns-filter dashboard statistics summary 343
show dns-filter fake-dns-response-ttl 343
show dns-filter profile {*all* | *profilename*} 343
show dns-filter search FQDN 343
show dns-filter statistics collect 343
show dns-filter statistics list 343

show dns-filter statistics summary 343
show dns-filter status 343
show dynamic-guest log 508
show dynamic-guest log create-time begin *yyyy-mm-dd hh:mm* end *yyyy-mm-dd hh:mm* .. 508
show dynamic-guest users 508
show extension-slot 47
show fast forwarding status 525
show fbwifi activate 258
show fbwifi service-register status 258
show fbwifi status 258
show firewall icsa status 220
show firewall-output 229
show firewall-output status 229
show firmware image boot option 546
show fqdn 461
show fqdn 512
show fqdn-object all 461
show fqdn-object query-period 461
show fqdn-object sync-period 461
show fqdn-object6 all 461
show frame-capture config 107
show frame-capture status 107
show free-time status 271
show geo-ip *country-code* 465
show geo-ip country-list *region code* 465
show geo-ip database update 465
show geo-ip database version 465
show geo-ip database version country 465
show geo-ip geography 465
show geo-ip geography6 465
show geo-ip region-code 465
show groupname [*groupname*] 446
show gui-visability status 603
show hardware-watchdog-timer status 597
show idp 349
show idp {signature | anomaly} base profile 350
show idp anomaly *adp-profile* ip-decoder {ip-spoof | ip-teardrop} details 237
show idp anomaly *adp-profile* ip-decoder all details 237
show idp anomaly base profile 233
show idp anomaly profile flood-detection [all details] 236
show idp anomaly profile flood-detection {tcp-flood | udp-flood | icmp-flood | icmp-flood} details 236
show idp anomaly profile icmp-decoder {bad-icmp-l4-size | icmp-smurf} details ... 237
show idp anomaly profile icmp-decoder all details 237
show idp anomaly profile scan-detection [all details] 236
show idp anomaly profile scan-detection {tcp-portscan | tcp-portscan-syn | tcp-portsweep | tcp-portscan-fin} details 236
show idp anomaly profile scan-detection {udp-portscan} details 236
show idp anomaly profile tcp-decoder {bad-tcp-flag | bad-tcp-l4-size | tcp-land} details 237
show idp anomaly profile tcp-decoder all details 236
show idp anomaly profile udp-decoder {bad-udp-l4-size | udp-land | udp-smurf} details 237
show idp anomaly profile udp-decoder all details 237
show idp anomaly profiles 234
show idp anomaly rules 234
show idp anomaly rules 234
show idp anomaly white-list {all | rule-name} 238
show idp dashboard statistics summary 51
show idp engine version 351
show idp rate_based_sig <*profile name*> 349

show idp search signature *my_profile* name *quoted_string* sid SID severity *severity_mask* platform *platform_mask* classtype *classtype_mask* service *service_mask* activate {any | yes | no} log {any | no | log | log-alert} action *action_mask* 353
show idp signature all details 350
show idp signature base profile {all|none|wan|lan|dmz} settings 351
show idp signature mode 351
show idp signature *profile* signature all details 350
show idp signature profile signature sid details 351
show idp signature profiles 351
show idp signature signatures {version | date | number} 359
show idp signature update 359
show idp signature update status 359
show idp signatures custom-signature all details 356
show idp signatures custom-signature *custom_sid* {details | contents | non-contents} 356
show idp signatures custom-signature number 356
show idp signatures date 360
show idp signatures number 360
show idp signatures version 360
show idp statistics collect 361
show idp statistics collect status 361
show idp statistics ranking {signature-name | source | source6 | destination |destination6 | rate-based} 361
show idp statistics summary 360
show idp white-list 363
show ikev2 policy [policy_name] 289
show ikev2 policy6 [policy_name] 290
show interface {ethernet | vlan | bridge | ppp} status 118
show interface {*interface_name* | ethernet | vlan | bridge | ppp | virtual ethernet | virtual vlan | virtual bridge | all} 118
show interface cellular [corresponding-slot|device-status|support-device] 144
show interface cellular budget-auto-save 144
show interface cellular corresponding-slot 144
show interface cellular device-status 144
show interface cellular status 144
show interface cellular support-device 144
show interface *interface_name* [budget] 144
show interface *interface_name* device profile 144
show interface *interface_name* device status 144
show interface *interface_name* proxy-arp address 127
show interface *interface_name* proxy-arp status 127
show interface lag 156
show interface lagx 156
show interface ppp 303
show interface ppp system-default 141
show interface ppp user-define 141
show interface send statistics interval 119
show interface summary all 119
show interface summary all status 119
show interface tunnel status 148
show interface *tunnel_iface* 148
show interface vti 161
show interface vtix 161
show interface-group {system-default|user-define|*group-name*} 163
show interface-name 123
show ip bgp neighbor *ipv4* [advertised-routes | prefix-counts | routes] 182
show ip dhcp binding [*ip*] 130
show ip dhcp dhcp-options 127
show ip dhcp list interface {all | *interface name*} keyword *keyword* 127
show ip dhcp pool [*profile_name*] 127

show ip dhcp pool *profile_name* dhcp-options 128
show ip dhcp static interface {all | *interface name*} 127
show ip dns security-options all 516
show ip dns server 516
show ip dns server database 516
show ip dns server status 516
show ip ftp server status 534
show ip http server secure status 529
show ip http server status 529
show ip http skip-csrf-check 529
show ip http-redirect [*description*] 201
show ip ipnp activation 273
show ip ipnp interface 273
show ip route [kernel | connected | static | ospf | rip | bgp] 179
show ip route bgp 182
show ip route control-virtual-server-rules 174
show ip route static-dynamic 582
show ip route-settings 174
show ip ssh server status 532
show ip telnet server status 533
show ip virtual-server [*profile_name*] 190
show ip virtual-server load-balance statistics rate name 199
show ip virtual-server load-balancer *name* 199
show ip virtual-server load-balancer *name* real-server 199
show ip virtual-server load-balancer statistics *name* 199
show ip-reputation {white-list|black-list} 328
show ip-reputation {white-list|black-list} status 328
show ip-reputation dashboard statistics summary 51
show ip-reputation ebl 331
show ip-reputation ebl *<1..4> {date | number}* 331
show ip-reputation ebl *<profile name>* 331
show ip-reputation ebl signature update 331
show ip-reputation search {Ipv6Address | Ipv4Address} 329
show ip-reputation signature update 329
show ip-reputation signatures date 328
show ip-reputation signatures number 328
show ip-reputation signatures version 328
show ip-reputation statistics collect status 329
show ip-reputation statistics recent-activities 329
show ip-reputation statistics summary 329
show ip-reputation status 327
show ip-reputation update status 329
show ip-reputation webroot {incoming-category | outgoing-category} 328
show ipv6 dhcp6 binding 504
show ipv6 interface {*interface_name* | all} 118
show ipv6 nd ra status *config_interface* 118
show ipv6 neighbor-list 589
show ipv6 static address *interface* 118
show ipv6 status 523
show isakmp keepalive 279
show isakmp policy [*policy_name*] 279
show isakmp sa 288
show l2-isolation 215
show l2-isolation activation 215
show l2-isolation white-list [*rule_number*] 215
show l2-isolation white-list activation 215
show l2tp-over-ipsec 302
show l2tp-over-ipsec session 302
show lag available slaves 156

show language {setting | all} 523
show lan-provision ap *ap_mac* interface {*lan_port* | *vlan_interface* | all| ethernet | uplink | vlan} 61
show ldap-server 473
show led status 47
show led_locator *ap_mac_address* status 113
show led_suppress *ap_mac_address* status 112
show lockout-users 451
show logging debug entries [priority *pri*] [category *module_name*] [srcip *ip*] [srcip6 *ipv6_addr*] [dstip *ip*] [dstip6 *ipv6_addr*] [service *service_name]* [srciface *interface_name*] [dstiface *interface_name*] [protocol *protocol*] [begin <1..512> end <1..512>] [keyword *keyword*] 567
show logging debug entries field *field* [begin <1..1024> end <1..1024>] 568
show logging debug status 567
show logging entries [priority *pri*] [category *module_name*] [srcip *ip*] [srcip6 *ipv6_addr*] [dstip *ip*] [dstip6 *ipv6_addr*] [service *service_name]* [begin <1..512> end <1..512>] [keyword *keyword*] [srciface *interface_name*] [dstiface *interface_name*] [protocol *protocol*] 566
show logging entries field *field* [begin <1..512> end <1..512>] 566
show logging status console 570
show logging status mail 569
show logging status syslog 568
show logging status system-log 566
show logging status usb-storage 149
show login-page default-title 512
show login-page settings 512
show logo settings 512
show mac 47
show mem status 47
show mem status all 578
show mem-conserve status 601
show monitor-mode 249
show myzyxel-service get-cloud-timezone 513
show ntp server 514
show object-group {address | address6} [*group_name*] 463
show object-group application <object> 456
show object-group service *group_name* 469
show ospf area IP virtual-link 178
show packet-capture config 589
show packet-capture status 589
show page-customization 512
show password complexity-verify status 446
show payment-service account-delivery 267
show payment-service activation 268
show payment-service check payment-all-currency 268
show payment-service fail-page settings 268
show payment-service mobile-fail-page settings 268
show payment-service mobile-page-customization 268
show payment-service mobile-profile-page settings 268
show payment-service mobile-sms-page settings 268
show payment-service mobile-success-page settings 268
show payment-service page-customization 268
show payment-service profile-page settings 268
show payment-service provider paypal 268
show payment-service provider select 268
show payment-service sms-page settings 268
show payment-service success-page settings 268
show ping-check [*interface_name* | status] 135
show policy-route [*policy_number*] 171
show policy-route begin <1..200> end <1..200> 171

show policy-route conn-check 171
show policy-route conn-check [*policy_number*] 171
show policy-route conn-check status [*policy_number*] 171
show policy-route controll-ipsec-dynamic-rules 171
show policy-route controll-virtual-server-rules 171
show policy-route override-direct-route 171
show policy-route rule_count 172
show policy-route underlayer-rules 172
show policy-route6 [*policy_number*] 172
show policy-route6 begin <1..200> end <1..200> 172
show policy-route6 controll-ipsec-dynamic-rules 172
show policy-route6 override-direct-route 171
show policy-route6 rule_count 172
show port setting 138
show port statistic portx interval <5..3600> 138
show port status 138
show port type physical 138
show port vlan-id 153
show port-grouping 137
show printer-manager button 270
show printer-manager discover-printer-status 270
show printer-manager printer [<1..10>] 270
show printer-manager printerfw version 270
show printer-manager printer-status 270
show printer-manager printout-type 270
show printer-manager settings 270
show printer-manager workableIP 270
show private-encryption-key status 545
show pwd-expiry {all | expiration | force-to-change-pwd | link-to-device} 446
show radius-server 474
show ram-size 47
show redirect-service *<1..20>* 204
show reference object aaa authentication [default | *auth_method*] 45
show reference object account pppoe [*object_name*] 45
show reference object account pptp [*object_name*] 45
show reference object address [*object_name*] 45
show reference object address6 [*object_name*] 45
show reference object app-patrol [profile-name] 45
show reference object ca category {local|remote} [*cert_name*] 45
show reference object crypto map [*crypto_name*] 45
show reference object device <profile name> 439
show reference object dhcp6-lease-object [*object_name*] 46
show reference object dhcp6-request-object [*object_name*] 46
show reference object interface [*interface_name* | *virtual_interface_name*] 45
show reference object isakmp policy [*isakmp_name*] 45
show reference object schedule [*object_name*] 45
show reference object service [*object_name*] 45
show reference object sslvpn application [*object_name*] 45
show reference object sslvpn policy [*object_name*] 45
show reference object username [*username*] 45
show reference object zone [*object_name*] 46
show reference object-group aaa ad [*group_name*] 46
show reference object-group aaa ldap [*group_name*] 46
show reference object-group aaa radius [*group_name*] 46
show reference object-group address [*object_name*] 46
show reference object-group address6 [*object_name*] 46
show reference object-group interface [*object_name*] 46
show reference object-group service [*object_name*] 46
show reference object-group username [*username*] 46

show remote-assistance 580
show remote-assistance generate 580
show report [*interface_name* {ip | service | url}] 572
show report [*interface_name*] https-url 573
show report packet size statistics {*interface_name*} [interval *interval*] 574
show report packet size statistics status 574
show report status 572
show respmsg url-filter block-page 522
show rip {global | interface {all | *interface_name*}} 133
show rogue-ap containment config 100
show rogue-ap containment list 100
show rogue-ap detection info 98
show rogue-ap detection list {rogue | friendly| all} 98
show rogue-ap detection monitoring 98
show rogue-ap detection status 98
show route order 582
show rtls ekahau cli 325
show rtls ekahau config 325
show running-config 546
show sa counter 288
show sa monitor [{begin <1..1000>} | {end <1..1000>} | {crypto-map *regexp*} | {policy *regexp*} |{rsort *sort_order*} | {sort *sort_order*}] 288
show sa monitor [ap-description *desc*] rap 66
show sandbox dashboard statistics summary 51
show sandbox file-type all 346
show sandbox file-type status 346
show sandbox statistics collect 346
show sandbox statistics dashboard summary 346
show sandbox statistics ranking file-name 346
show sandbox statistics summary 346
show sandbox status 346
show schedule reboot status 595
show schedule-object 470
show sdwan oncloudst 597
show secumanager status 243
show secure-dns search {FQDN|IP Address} 344
show secure-policy 220
show secure-policy any ZyWALL 220
show secure-policy backup status 218
show secure-policy block_rules 220
show secure-policy _check-exposed-srv 218
show secure-policy filter from *zone_object* to *zone_object* srcip <ip-address> dstip <ip> service {any | tcp | udp | icmp | gre | esp | user-defined} port-number user *user_name* sch *schedule_object* 219
show secure-policy *rule_number* 220
show secure-policy status 220
show secure-policy *zone_object* {*zone_object*|ZyWALL} 220
show secure-policy *zone_object* {*zone_object*|ZyWALL} *rule_number* 220
show secure-policy6 221
show secure-policy6 any ZyWALL 221
show secure-policy6 block_rules 221
show secure-policy6 filter from *zone_object* to *zone_object* srcip6 <ip-address> dstip6 <ip> service {any | tcp | udp | icmp | gre | esp | user-defined} port-number user *user_name* sch *schedule_object* 220
show secure-policy6 *rule_number* 221
show secure-policy6 status 221
show secure-policy6 *zone_object* {*zone_object*|ZyWALL} 221
show secure-policy6 *zone_object* {*zone_object*|ZyWALL} *rule_number* 221
show secure-policy-style status 224

show secu-reporter category status 246
show secu-reporter status 245
show security-service inspect status 224
show security-service ip6-exception 427
show security-service ip-exception 427
show security-service signature status 315
show security-service signature status 322
show security-service signature status 337
show security-service status 315
show security-service status 318
show security-service status 327
show security-service status 332
show security-service status 343
show security-service status 346
show security-service status 349
show security-service status 403
show security-service status 51
show security-service update-server 55
show serial-number 47
show service-object [*object_name*] 467
show service-register content-filter-engine 54
show service-register status {all | application-security | as | av | cdr | concurrent-device-upgrade | content-filter | firmware-upgrade | geo-ip | idp | malware-blocker | ctdb | managed-ap-service | pkg | reputation-filter | sandbox | secu-reporter | secure-wifi | sslvpn | sslvpn-status | web-security | zymesh| network-premium} 54
show service-register status content-filter {commtouch} 54
show service-register status secu-reporter 245
show service-register status sslvpn-status 54
show session timeout {icmp | tcp-timewait | udp} 581
show session-limit 231
show session-limit begin *rule_number* end *rule_number* 231
show session-limit *rule_number* 231
show session-limit status 231
show session-limit6 232
show session-limit6 begin *rule_number* end *rule_number* 232
show session-limit6 *rule_number* 232
show session-limit6 status 232
show session-status-update reply-time 221
show setenv-startup 546
show sms-service 521
show sms-service activation 521
show sms-service default-country-code 521
show sms-service provider email-to-sms 521
show sms-service provider vianett 521
show snmp status 537
show snmp-server v3user status 537
show socket listen 47
show socket open 47
show software-watchdog-timer log 598
show software-watchdog-timer status 598
show ssl-inspection cert-list 423
show ssl-inspection cert-update status 424
show ssl-inspection default-cert update 424
show ssl-inspection default-cert version 424
show ssl-inspection exclude-list 421
show ssl-inspection exclude-list address 421
show ssl-inspection exclude-list settings 421
show ssl-inspection exclude-list web-category 421
show ssl-inspection profile [SSI_profile_name] 423

show ssl-inspection statistics collect 424
show ssl-inspection statistics summary 424
show ssl-inspection status 419
show sslvpn application [*application_object*] 501
show sslvpn login-port 296
show sslvpn monitor 296
show ssl-vpn network-extension local-ip 296
show sslvpn policy [*profile_name*] 296
show sso { agent | port | presharekey} 257
show sso agent 259
show sso agent primary 259
show sso agent secondary 259
show sso agent status 259
show sso port 259
show sso presharekey 259
show sta-info {*mac_address* | all} usage *timer* 48
show sta-info top 10 alert {2.4G | 5G | 6G| all} 101
show sta-info top *number* usage *timer* 48
show sta-info total usage *timer* 48
show storm-control ethernet ap mac_address 84
show system default-interface-group 164
show system default-snat 164
show system protection signature update status 52
show system protection signatures version 52
show system route default-wan-trunk 582
show system route dynamic-vpn 582
show system route nat-1-1 582
show system route policy-route 582
show system route site-to-site-vpn 582
show system snat default-snat 582
show system snat nat-1-1 582
show system snat nat-loopback 582
show system snat order 582
show system snat policy-route 582
show system uptime 47
show threat-website {trust|forbid} 332
show threat-website ebl 336
show threat-website ebl <*1..4*> {*date* | *number*} 336
show threat-website ebl <*profile name*> 336
show threat-website ebl signature update 336
show threat-website search {*ipv6address* | *ipv4address*} 336
show threat-website statistics collect 339
show threat-website statistics list 339
show threat-website statistics summary 339
show threat-website status 332
show two-factor-auth 486
show two-factor-auth admin-access 488
show two-factor-auth admin-access 488
show usb-storage 149
show usb-storage space 151
show usb-storage space ftp 151
show usb-storage space tmp 151
show usb-storage space usb 151
show usb-storage update-firmware status 151
show username [*username*] 444
show username username google-auth backup-code 488
show username username google-auth qrcode 488
show users {*username* | all | current} 451
show users default-setting {all | user-type {admin|user|guest|limited-admin|ext-user| ext-

group-user}} 446
show users idle-detection-settings 447
show users retry-settings 447
show users simultaneous-logon-settings 447
show users update-lease-settings 447
show utm-manager {doh| dot| system-protect} defaultport 344
show version 47
show vpn-concentrator [*profile_name*] 286
show vpn-concentrator6 [*profile_name*] 294
show vpn-configuration-provision activation 287
show vpn-configuration-provision authentication 287
show vpn-configuration-provision iosfilter 288
show vpn-configuration-provision port 287
show vpn-configuration-provision rules 287
show vpn-counters 288
show vpn-interface-restriction status 161
show vpn-policy-pool 66
show vpn-service status 278
show vrpt send device information interval 568
show vrpt send interface statistics interval 568
show vrpt send system status interval 568
show walled-garden activation 274
show walled-garden rule <1..50> 274
show web-auth activation 254
show web-auth default-rule 254
show web-auth exceptional-service 254
show web-auth method 254
show web-auth policy {<1..1024> | all} 254
show web-auth portal status 255
show web-auth redirect-fqdn 254
show web-auth redirect-parameter 254
show web-auth status 255
show web-google-analytics status 603
show wireless-health-action 101
show wlan-macfilter-profile {all | *macfilter_profile_name*} 94
show wlan-monitor-profile {all | *monitor_profile_name*} 84
show wlan-radio-profile {all | *radio_profile_name*} 77
show wlan-security-profile {all | *security_profile_name*} 89
show wlan-ssid-profile *{all | ssid_profile_name}* 86
show workspace application 297
show workspace cifs 297
show zon lldp neighbors 524
show zon lldp server config 524
show zon lldp server statistics 524
show zon lldp server status 524
show zon zdp server status 524
show zone [*profile_name*] 184
show zone binding-iface 184
show zone default-binding 184
show zone none-binding 184
show zone system-default 184
show zone user-define 184
show zymesh ap info 95
show zymesh link info {repeater-ap | root-ap} 95
show zymesh provision-group 96
show zymesh-profile {all | *zymesh_profile_name*} 96
show vcp allowed crypto map 287
show vcp allowed crypto map6 287
show vcp allowed users 287

shutdown 43
signature *sid* action {drop | reject-sender | reject-receiver | reject-both} 351
signature *sid* action {drop | reject-sender | reject-receiver | reject-both} 352
signature *sid* block_period 352
signature *sid* counts 352
signature *sid* log [alert] 351
signature *sid* seconds 352
sms-service account-send phone *phone_number* account *user_name* password *password* . 520
sms-service default-country-code *country_code* 520
sms-service provider email-to-sms 521
sms-service provider vianett 520
sms-service provider-select vianett {vianett|email-to-sms} 520
sms-service test-send phone *phone_number* msg *message* 521
sms-service _two-factor-auth-admin-send phone phone user *username* verification-code verification_code 445
smtp helo-name *name* 199
snaplen <68..1512> 587
snmp-server rule {*rule_number*|append|insert *rule_number*} access-group {ALL|*address_object*} zone {ALL|*zone_object*} action {accept|deny} 536
snmp-server rule move *rule_number* to *rule_number* 536
snmp-server v3user username *description* authentication {md5 | sha} privacy {none | des | aes} privilege {ro | rw} 537
snmp-server version {v2c | v3} 537
source {src-ipv4-obj | any} destination {dst-ipv4-obj | any} service {service_obj | any} 237
source <*url*> 330
source <*url*> 336
split-size <1..2048> 587
src-ip {add|del} {*ipv4_address* | local} 107
ssh {user@W.X.Y.Z | or W.X.Y.Z) 531
ssid *ssid* 96
ssl-inspection cache flush 423
ssl-inspection cert-update now 423
ssl-inspection exclude-list 421
ssl-inspection exclude-list-settings 421
ssl-inspection pkt-enc-mss <536..1460> 419
ssl-inspection profile rename SSI_profile_name1 SSI_profile_name2 423
ssl-inspection profile *ssi_profile_name* 422
ssl-inspection server-sign-cert mode {default | rsa-1024 | rsa-2048} 419
ssl-inspection server-sign-cert mode {ecdsa-rsa-1024|ecdsa-rsa-2048} 419
ssl-inspection statistics flush 424
ssl-inspection tls1-2 aesgcm {activate | deactivate} 423
ssl-inspection tls1-3 {activate | deactivate} 423
sslv2 action {pass | block} {no log | log [alert]} 422
sslvpn login message <description> 296
sslvpn login-port <1..65535> 296
sslvpn logout message <description> 296
sslvpn network-extension local-ip *ip* 296
sslvpn no connection username *user_name* 297
sslvpn policy {*profile_name* | *profile_name* append | *profile_name* insert <1..16>} 296
sslvpn policy move <1..16> to <1..16> 297
sslvpn policy rename *profile_name profile_name* 297
sso agent primary 259
sso agent secondary 259
sso encrypted-presharekey <ciphertext> 259
sso presharekey <preshared key> 259
sso_port <1025..65535> 259
station: none 105
status 60
status: active 524

status-code {*int*|*range*} 199
storage <internal|usbstorage> 587
storm-control ethernet ap mac_address 83
storm-control wireless ap mac_address 84
subframe-ampdu *<2..64>* 78
subframe-ampdu <2..64> 82
support-version-max {ssl3 | tls1_0 | tls1_1 | tls1_2 | tls1_3} 422
support-version-min {ssl3 | tls1_0 | tls1_1 | tls1_2 | tls1_3} 422
sysname *system_name* 68
system default-interface-group *group-name* 164
system protection signature update signature 52
tcp-decoder {tcp-xxx} log [alert] 235
telnet 43
test aaa 43
test aaa {server|secure-server} {ad|ldap} host {*hostname*|*ipv4-address*} [host {*hostname*|*ipv4-address*}] port <1..65535> base-dn *base-dn-string* [bind-dn *bind-dn-string* password *password*] login-name-attribute *attribute* [alternative-login-name-attribute *attribute*] account *account-name* 480
The conf-backup commands automatically backup the current Zyxel Device configuration file according to a schedule, and then send it to an email address. 596
The conf-mail commands send a user-specified configuration file immediately to an email address. 595
threat-website {trust | forbid} 332
threat-website dashboard statistics flush 51
threat-website ebl *<profile name>* 335
threat-website ebl rename *old_profile_name new_profile_name* 336
threat-website ebl update 336
threat-website ebl update daily *<0..23>* 336
threat-website ebl update hourly 336
threat-website ebl update weekly *{sun |mon|tue|wed|thu|fri|sat} <0..23>* 336
threat-website profile *<profile name>* action *{block | pass | warn}* 334
threat-website profile *profile_name* 334
threat-website rename *old_profile_name new_profile_name* 334
threat-website statistics flush 338
time-period {day <1..365> | hour <1..24> | minute <30..60>} 264
time-period <1..432000> 509
tracepath6 {*ipv6* | *hostname*} 589
traceroute 43
traceroute {*ip* | *hostname*} 586
traceroute {*ipv4* | *hostname*} [source *ipv4*] [interface *interface_name*] [extension *filter-extension*] 588
traceroute6 43
traceroute6 {*ipv6* | *hostname*} 586
traceroute6 {*ipv6* | *hostname*} [source *ipv6*] [interface *interface_name*] [extension *filter-extension*] 589
traffic-prioritize {tcp-ack|content-filter|dns} bandwidth <0..1048576> priority <1..7> [maximize-bandwidth-usage]; 148
traffic-prioritize {tcp-ack|content-filter|dns} bandwidth <0..1048576>]; 155
traffic-prioritize {tcp-ack|content-filter|dns} priority-code <0..7> deactivate . 148
traffic-prioritize {tcp-ack|content-filter|dns} priority-code <0..7> deactivate . 155
traffic-prioritize {tcp-ack|content-filter|dns|ipsec-vpn|ssl-vpn} bandwidth <0..1048576> priority <1..7> [maximize-bandwidth-usage]; 120
traffic-prioritize {tcp-ack|content-filter|dns|ipsec-vpn|ssl-vpn} deactivate 120
transform-set *crypto_algo_ah* [*crypto_algo_ah* [*crypto_algo_ah*]] 281
transform-set *crypto_algo_ah* [*crypto_algo_ah* [*crypto_algo_ah*]] 292
transform-set *crypto_algo_esp* [*crypto_algo_esp* [*crypto_algo_esp*]] 281
transform-set *crypto_algo_esp* [*crypto_algo_esp* [*crypto_algo_esp*]] 292
transform-set isakmp-algo [isakmp_algo 289
transform-set isakmp-algo [isakmp_algo 291

transform-set isakmp-algo [isakmp_algo [*isakmp_algo*]] 279
tunnel destination *ipv4* 147
tunnel mode [ipv6ip [manual | 6to4]]] 148
tunnel mode ip gre 147
tunnel source [*ipv4*|*tunnel_bind_interface*|_any] 147
two-factor-auth admin-access auth-method {google-auth|pin-code} 487
two-factor-auth allow-access-url-thru-tunnel [activate | deactivate] 486
two-factor-auth http port <1...65535> 486
two-factor-auth message {*message_quoted* | *message*} 485
two-factor-auth message-type {default | file} 485
two-factor-auth server interface *interface_name* 485
two-factor-auth server user-defined {*ipv4*|*domain_name*} 485
two-factor-auth sms message {*message_quoted* | *message*} 485
_two-factor-auth-send email email user *username* verification-code verification_code 445
tx-mask *chain_mask* 83
type {external | general | internal} 156
type {external | internal} 255
type {internal | external | general} 137
udp-decoder {bad-udp-l4-size | udp-land | udp-smurf} action {drop | reject-sender | reject-receiver | reject-both} 235
udp-decoder {bad-udp-l4-size | udp-land | udp-smurf} log [alert] 235
unlock lockout-users {*ip* | console| *ipv6_addr*} 451
unsupported-suite action {pass | block} {no log | log [alert]} 422
untrusted-cert-chain action {block | inspect | pass} {no log | log [alert]} 423
updelay <0..1000> 156
url [timeout *query_timeout*] 370
url match <*string*> 375
url not-match <*string*> 375
url parameter <*string*> 375
url value <*string*> 375
usb-storage mount 149
usb-storage umount 149
usb-storage warn <*10..99*> percentage 151
usb-storage warn <*100..9999*> megabyte 151
usb-storage warn *number* <*percentage*|megabyte> 149
use-defined-mac 137
user *isp_account_username* 303
user *username* 286
USER_NAME_ 569
username rename *username username* 444
username *username* [no] {email1-verify|email2-verify} 445
username username [no] {email1-verify|email2-verify} 488
username *username* [no] description *description* 444
username *username* [no] email <1..2> *email-address* 445
username username [no] google-auth 487
username *username* [no] logon-lease-time <0..1440> 445
username *username* [no] logon-re-auth-time <0..1440> 445
username *username* [no] phone *phone_number* 445
username *username* [no] phone-verify 445
username username [no] phone-verify 488
username username 2fa-auth-method {default|google-auth|pin-code} 487
username username encrypted-password <*password*> 444
username username google-auth backup-code create 488
username username google-auth verify-code <verification code> 487
username *username* logon-time-setting <default | manual> 445
username *username* nopassword user-type {admin | guest | limited-admin | user} ... 444
username *username* password *password* user-type {admin | guest | limited-admin | user} 444
username *username* user-type ext-group-user associated-aaa-server *server_profile* group-id *id* 444

username *username* user-type ext-user 444
username *username* user-type mac-address 444
username *username* vlan activate 445
username *username* vlan id <1..4094> 445
users default-setting [no] logon-lease-time <0..1440> 446
users default-setting [no] logon-re-auth-time <0..1440> 447
users default-setting [no] user-type <admin |ext-user|guest|limited-admin|user|ext-group-user> 447
users default-setting [no] user-type <admin |ext-user|guest|limited-admin|user|ext-group-user> logon-lease-time <0..1440> 447
users default-setting [no] user-type <admin |ext-user|guest|limited-admin|user|ext-group-user> logon-re-auth-time <0..1440> 447
users force-logout {*username* | *ip* | *ipv6_addr*} 451
virtual-service interface *interface_name* external-ip {*address*|*object*} external-port *port* protocol {*tcp*|*udp*}] 197
virtual-service interface *interface_name* external-ip {*address*|*object*} external-service *service* .. 197
vlan <1..4094> {tag | untag} 72
vlan_interface {activate | inactivate} vid <1..4094> join *lan_port* {tag | untag} [*lan_port* {tag | untag}] [*lan_port* {tag | untag}] 60
vlan-priority-code <0..7> 311
vpn-concentrator rename *profile_name profile_name* 286
vpn-concentrator6 rename *profile_name profile_name* 294
vpn-configuration-provision authentication *auth_method* 287
vpn-configuration-provision generate {ios | windows | android} ikev2-wizard profile <profile name> 288
vpn-configuration-provision port <1...65535> 287
vpn-configuration-provision rule { append | *conf_index* | insert *conf_index* } 286
vpn-configuration-provision rule { delete *conf_index* | move *conf_index* to *conf_index* } 286
vpn-interface-restriction activate 160
vpn-interface-restriction deactivate 161
vpn-policy-pool start *start_ip* end *end_ip* 66
vrpt send device information interval <15..3600> 568
vrpt send interface statistics interval <15..3600> 568
vrpt send system status interval <15..3600> 568
wac6553d-e} *ap_lan_port* activate pvid <1..4094> 70
wac6553d-e} *ap_lan_port* inactivate pvid <1..4094> 71
wac6553d-e} *vlan_interface* activate vid <1..4094> join *ap_lan_port* {tag | untag} [*ap_lan_port* {tag | untag}] [*ap_lan_port* {tag | untag}] 71
wac6553d-e} *vlan_interface* inactivate vid <1..4094> join *ap_lan_port* {tag | untag} [*ap_lan_port* {tag | untag}] [*ap_lan_port* {tag | untag}] 71
walled-garden domain-ip rule <1..50> 274
walled-garden domain-ip rule append 274
walled-garden domain-ip rule flush 274
walled-garden rule append 273
walled-garden rule flush 274
walled-garden rule insert <1..50> 274
walled-garden rule move <1..50> to <1..50> 274
web-auth [no] exceptional-service *service_name* 253
web-auth default-rule authentication {required | unnecessary} {no log | log [alert]} 253
web-auth google-auth valid-time *<1..5>* 253
web-auth login setting 253
web-auth method portal 253
web-auth policy <1..1024> 253
web-auth policy append 253
web-auth policy delete <1..1024> 253
web-auth policy flush 253
web-auth policy insert <1..1024> 253
web-auth policy move <1..1024> to <1..1024> 253
web-auth redirect-parameter 254
web-auth web-portal 254

WEEKDAYS 569
white-list activate 215
white-list append 215
white-list flush 215
white-list no activate 215
white-list *rule_number* 215
wireless-health radio {action | act-lock-time <1...1440> | recovery-threshold <10...1000>| act-threshold <10...1000>| data-collect-interval <0...120>} 103
wireless-health radio action {dcs_now | downgrade_cw | none} 104
wireless-health sta {action | act-lock-time <1...1440>| act-threshold <10...1000>| data-collect-interval <0...120>} 103
wireless-health sta action {kick_sta | none} 104
wireless-health-action aggressiveness {high | standard | low} 102
wlan-macfilter-profile rename *macfilter_profile_name1 macfilter_profile_name2* 94
wlan-monitor-profile rename *monitor_profile_name1 monitor_profile_name2* 84
wlan-radio-profile rename *radio_profile_name1 radio_profile_name2* 77
wlan-security-profile rename *security_profile_name1 security_profile_name2* 89
wlan-ssid-profile rename *ssid_profile_name1 ssid_profile_name2* 86
write 43
write 546
xauth type {server *auth_method* [user-id {*username* | any}] | client name *username* password *password*} [deactivate] 280
xmit-hash-policy {layer2 | layer2_3} 156
zon lldp server 524
zon lldp server tx-hold <1..10> 524
zon lldp server tx-interval <1..600> 524
zon zdp server 524
zone *profile_name* 184
ZYLOG_SUBJECT 569
zymesh provision-group *ac_mac* 96
zymesh-profile rename *zymesh_profile_name1 zymesh_profile_name2* 96