

NXC Series

NXC 2500/ 5500

NXC Controllers

Firmware Version 5.40

Edition 11, 06/2019

Handbook

Default Login Details

LAN Port IP Address	https://192.168.1.1
User Name	admin
Password	1234

Contents

Manage APs through NXC Controller	8
1.1 How to Manage APs through NXC Controller	8
1.1.1 Configuration in the AP.....	9
1.1.2 Test the Result	10
1.1.3 What Could Go Wrong?	11
1.2 How to Enlarge Managed AP Number with License	12
1.2.1 Device Registration	13
1.2.2 Service Registration	14
1.2.3 License Refresh.....	14
1.2.4 Test the Result	15
Set up a Wireless Connection Environment	16
2.1 How to configure with the Wizard Setting.....	16
2.1.1 How to configure the Wizard Setting with First login?	17
2.1.2 Test the Result	26
2.1.3 What Could Go Wrong?	28
2.2 How to Set WiFi Multiple SSID for Office Environment?	29
2.2.1 When USG is DHCP Server for VLAN10 and VLAN20	29
2.2.1.1 Configure NXC's Interface to Go to Internet	30
2.2.1.2 Configure VLAN	31
2.2.1.3 Configure Security and SSID.....	33
2.2.1.4 Configure AP Profile to Broadcast SSID	36
2.2.2 When NXC is DHCP Server for VLAN10 and VLAN20	37
2.2.2.2 Configure Interface ge1 to Go to Internet	38
2.2.2.2 Configure VLAN	39
2.2.2.3 Set Policy Route	43
2.2.2.4 Configure Security and SSID.....	45
2.2.2.5 Configure AP Profile to Broadcast SSID	48
2.2.3 Test the Result	49
2.2.4 What Could Go Wrong?	50
2.3 How to Set up Fail Over/Fall Back?.....	51
2.3.1 Configure Fail Over and Fall Back	52
2.3.2 Test the Result	53
2.3.3 What Could Go Wrong?	54
2.4 How to Set up Mesh to Extend Wireless Coverage?.....	55

2.4.1 Configure ZyMesh Profile	56
2.4.2 Configure Root AP and Repeater AP	57
2.4.3 Test the Result	58
2.4.4 What Could Go Wrong?	59
2.5 How to Set up Seamless Wireless Roaming?	61
2.5.1 Configure APs via AP Group	62
2.5.2 Test the Result	65
2.5.3 What Could Go Wrong?	66
2.6 How to implement Wireless VoIP Best Practice (VoWiFi)?	68
2.6.1 Configure Interface	69
2.6.2 Configure AP profile with Security, SSID and radio	71
2.6.3 Configure AP Group	74
2.6.4 Test the Result	75
2.6.5 What Could Go Wrong?	76
Optimize the Wireless Environment.....	79
3.1 How to Set up User Ratio of 2.4GHz and 5GHz to Avoid WiFi Congestion?	79
3.1.1 Configure Band Select	80
3.1.2 Test the Result	83
3.1.3 What Could Go Wrong?	84
3.2 How to Set up RSSI Threshold to Avoid Low Rate User Connection Affected Wireless Performance?	85
3.2.1 Configure Radio Setting for RSSI Threshold	86
3.2.2 Apply Radio with RSSI Threshold	87
3.2.3 Test the Result	88
3.3 How to Set up Rate Limiting for Bandwidth Control?	89
3.3.1 Configure Rate Limiting	90
3.3.2 Apply Rate Limiting to Management AP	91
3.3.3 Test the Result	92
3.4 How to Share AP loading to Optimize Wireless Performance?	93
3.4.1 Configure Load Balance to “by Station Number”	94
3.4.2 Configure Load Balance to “by Traffic Level”	95
3.4.3 Configure Load Balance to “by Smart Classroom”	96
3.4.4 Test the Result	97
3.4.5 What Could Go Wrong?	99
Secure the Wireless Environment - 802.1x.....	100

4.1 How to Configure 802.1x to Secure the Wireless Environment with an External RADIUS Server?	100
4.1.1 Configure Radius Server Setting	101
4.1.2 Configure AP Profile	102
4.1.3 Test the Result	104
4.1.4 What Could Go Wrong	109
4.2 How to Configure 802.1x to Secure the Wireless Environment with an External AD Server?	110
4.2.1 Configure AD Server Setting.....	111
4.2.2 Configure AP Profile	114
4.2.3 Test the Result	116
4.2.4 What Could Go Wrong	121
4.3 How to Configure 802.1x to Secure the Wireless Environment with an External LDAP Server?	122
4.3.1 Configure LDAP Server Setting.....	123
4.3.2 Configure AP Profile	125
4.3.3 Test the Result	127
4.3.4 What Could Go Wrong	128
4.4 How to Configure 802.1x to Secure the Wireless Environment with an Internal RADIUS in NXC?	129
4.4.1 Configure Authentication Method Setting	130
4.4.2 Configure AP Profile	132
4.4.3 Test the Result	134
4.5 How to Configure 802.1x to secure the Wireless Environment with Dynamic VLAN by Using External AAA server?	137
4.5.1 Configure Interface	138
4.5.2 Configure AP Profile	143
4.5.3 Configure AAA Server Setting.....	145
Topic: Dynamic VLAN by radius attribute	152
4.5.4 Test the Result	162
4.5.4.2 Dynamic VLAN by External User Group.....	164
4.5.5 What Could Go Wrong	166
4.6 How to Configure 802.1x EAP-TLS to Secure the Wireless Environment with Self-Signed Certificate?	167
4.6.1 Configure Certificate	168
4.6.2 Configure AP profile	172

4.6.3 Test the Result	174
4.6.4 What Could Go Wrong?	177
4.7 How to Configure 802.1x EAP-TLS to Secure the Wireless Environment with Third-party CA Certificate?	179
4.7.1 Configure Certificate	180
4.7.2 Configure AP profile	185
4.7.3 Configure Auth. Server	187
4.7.4 Test the Result	188
4.7.5 What Could Go Wrong?	191
Secure the Wireless Environment – Captive portal.....	192
5.1 How to Configure Captive Portal Redirect on Controller?	192
5.1.1 Configure Authentication Method Setting	194
5.1.2 Configure Captive Portal	195
5.1.3 Configure AP Profile when USG is the Gateway	197
5.1.4 Configure AP Profile when NXC is the Gateway	199
5.1.5 Test the Result	203
5.1.6 What Could Go Wrong	205
5.2 How to Configure Captive Portal Redirect on AP?	206
5.2.1 Configure AP Profile and User	207
5.2.2 Configure Captive Portal	209
5.2.3 Broadcast SSID.....	211
5.2.4 Test the Result	212
5.2.5 What Could Go Wrong	213
5.3 How to Configure Captive Portal with QR Code?	214
5.3.1 Configure AP Profile	215
5.3.2 Configure VLAN	217
5.3.3 Create Assistance Account	219
5.3.4 Set Guest Address & Zone	220
5.3.5 Configure Captive Portal	221
5.3.6 Broadcast SSID.....	224
5.3.7 Test the Result	225
5.3.8 What Could Go Wrong	227
5.4 How to Configure Captive Portal with External Webserver?	229
5.4.1 Configure Interface	230
5.4.2 Configure Authentication Method Setting & Address.....	233
5.4.3 Configure Captive Portal	235

5.4.4 Configure AP Profile	237
5.4.5 Test the Result	238
5.4.6 What Could Go Wrong	239
5.5 How to Configure Multiple Captive Portals for different users?	240
5.5.1 Configure AP Profile and User.....	241
5.5.2 Configure Captive Portal	243
5.5.3 Broadcast SSID.....	246
5.5.4 Test the Result	248
5.5.5 What Could Go Wrong	250
Secure the Wireless Environment – Others	251
6.1 How to Configure MAC Authentication?	251
6.1.1 Configure AP Profile	252
6.1.2 Configure User/Group Profile	253
6.1.3 Configure Authentication Method Setting	254
6.1.4 Configure AP Group Profile	255
6.1.5 Test the Result	256
6.2 MAC Authentication fallback to Captive Portal?	258
6.2.1 Configure AP Profile	259
6.2.2 Configure User/Group Profile	260
6.2.3 Configure Authentication Method Setting	261
6.2.4 Configure Captive Portal Setting	262
6.2.5 Configure AP Group Profile	264
6.2.6 Test the Result	265
6.2.7 What Could Go Wrong	269
6.3 How to Detect the Rogue AP?	270
6.3.1 Configure AP to Monitor Mode	271
6.3.2 Detected Devices and Containment	272
6.3.3 Test the Result	273
6.4 How to monitor the traffic and stations on web GUI?	274
Maintain NXC Controller	276
7.1 How to Do Firmware upgrade	276
7.1.1 Firmware from GUI?	277
7.1.1.1 Firmware Upgrade on GUI.....	278
7.1.1.2 Test the Result	279
7.1.1.3 What Could Go Wrong	280
7.1.2 Firmware from FTP?	281

7.1.2.1 Firmware Upgrade on GUI.....	282
7.1.2.2 Test the Result	284
7.1.2.3 What Could Go Wrong	285
7.2 How to Reset the Controller/AP?	286
7.2.1 Reset to Default from GUI.....	287
7.2.2 Reset to Default from Hardware	288
7.2.3 Test the Result	289
7.3 How to upgrade the firmware for AP via NXC?	290
7.3.1 How to Change the Updating Method for the AP as Manual?.....	291
7.3.1.1 Change the Updating Method via GUI	291
7.3.1.2 Test the Result	292
7.3.2 How to upgrade the specific AP firmware manually?	293
7.3.2.1 Upgrade the AP firmware via GUI.....	293
7.3.2.2 Test the Result	294
7.3.2.3 What Could Go Wrong	295
7.3.3 How to upgrade the firmware for AP group?	296
7.3.3.1 Upgrade the firmware for AP group via GUI	296
7.3.3.2 Test the Result	297
7.3.3.3 What Could Go Wrong	297
7.4 How to Upgrade the AP firmware via cloud?	298
7.4.1 Upgrade the firmware for AP group via GUI	298
7.4.2 Test the Result	300
7.4.3 What Could Go Wrong	300
Trouble Shooting	301
8.1 How to Collect the Diagnostic Info?	301
8.1.1 Collect Diagnostic Info	302
8.1.2 Test the Result	304
8.2 How to Configure the E-mail Settings for Sending Logs?	305
8.2.1 Configure Log & Report	306
8.2.2 Test the Result	308

Manage APs through NXC Controller

1.1 How to Manage APs through NXC Controller

This example shows how to use the NXC controller to manage APs via manual setting, DHCP option 138 and broadcast. In this case shown as below, there are two subnets in the environment. The APs can find NXC controller in the same subnet via broadcasting without any settings. The APs in different subnet can find NXC controller by manually setting NXC controller's IP or DHCP option 138 in DHCP server.

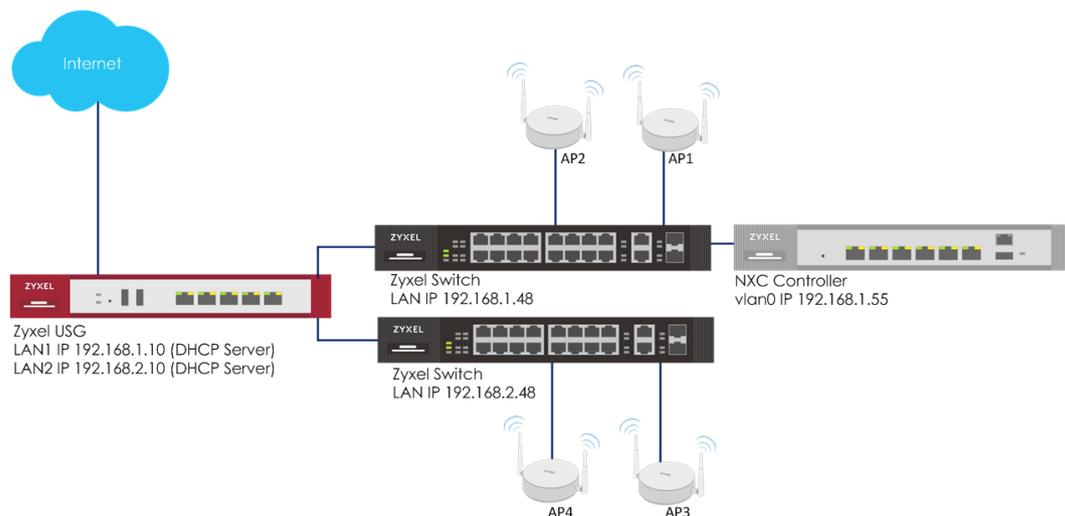


Figure 1.1 Manage APs through NXC Controller

 Note:

All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC5500 (Firmware Version: 5.40), GS2210-8HP (Firmware Version: V4.30).

1.1.1 Configuration in the AP

- 1 In the same subnet (for AP1 and AP2), the APs don't need to do any setting. The APs can find the NXC controller via broadcast and NXC controller always accepts APs to managed list by default. The NXC controller manages the APs without any setting.
- 2 In the different subnet (for AP3 and AP4), the APs need to set the NXC controller's IP manually. Go to **CONFIGURATION > Network > AC Discovery**, set **Discovery Setting** to **Manual** and set the NXC controller's IP **192.168.1.55** to **Primary static AC IP**. Click **Apply** to apply the setting.

Discovery Setting

Auto
 Manual
 Primary static AC IP:
 Secondary static AC IP: (Optional)
 Disable

- 3 Or, you can use DHCP option 138 in the DHCP server for the APs which are in the different subnet from NXC controller.

Option: CAPWAP AC (138) ▾
 Name: CAPWAP_AC
 Code: 138
 Type: IP
 First IP Address: 192.168.1.55

1.1.2 Test the Result

- 1 When the APs and the NXC controller are in the same subnet, the NXC controller manages the APs without any settings. The result is visible in **MONITOR > Wireless > AP Information > AP List**.

AP List									
#	Status	Registration	Description	CPU Usage	IP Address	Model	Version	Group	
1	✔	Mgmt AP	AP-A0E4C...	9 %	192.168.1.35	WAC6502D-S	5.10(AASE...	default	
2	✔	Mgmt AP	AP-B8ECA...	36 %	192.168.1.33	WAC5302D-S	5.10(ABFH...	default	

- 2 When the APs and the NXC controller are in the different subnets, the APs can find NXC controller through manually setting NXC controller's IP or DHCP option 138. After the APs find the NXC controller, the NXC controller can manage the APs. The result is visible in **MONITOR > Wireless > AP Information > AP List**.

AP List									
#	Status	Registration	Description	CPU Usage	IP Address	Model	Version	Group	
1	✔	Mgmt AP	AP-A0E4C...	10 %	192.168.2.36	WAC6502...	5.10(AASE...	default	
2	✔	Mgmt AP	AP-B8ECA...	15 %	192.168.2.35	WAC5302...	5.10(ABFH...	default	

1.1.3 What Could Go Wrong?

- 1 To make sure the NXC controller goes to correct traffic routing, please remember to set up the gateway in NXC controller.

IP Address Assignment

Get Automatically

Use Fixed IP Address

IP Address:

Subnet Mask:

Gateway: (Optional)

- 2 When you use the manual NXC controller IP or DHCP option 138, please make sure the NXC controller's IP is correct so that the APs can find the NXC controller.

1.2 How to Enlarge Managed AP Number with License

This example shows how to enlarge managed AP number with license. The default managed AP number for NXC2500 is 8 units and NXC5500 is 64 units. If you want to control more than default managed units, it's necessary to import the license to enlarge managed AP number.

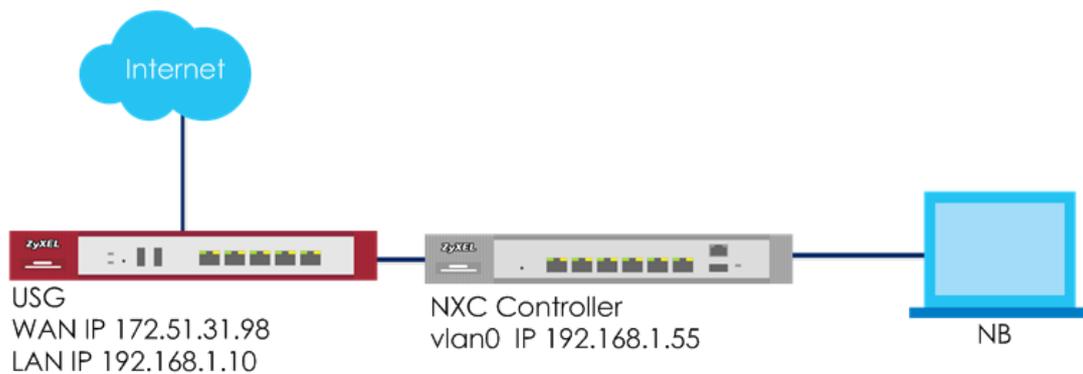


Figure 1.2 Enlarge Managed AP Number

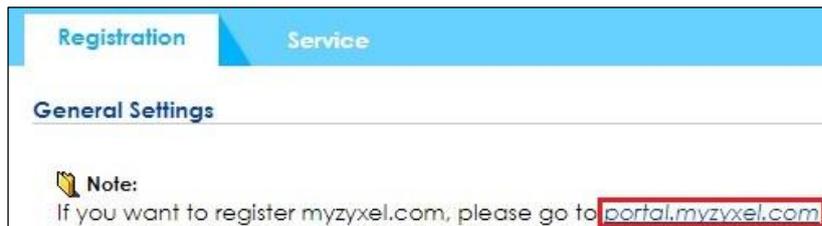


Note:

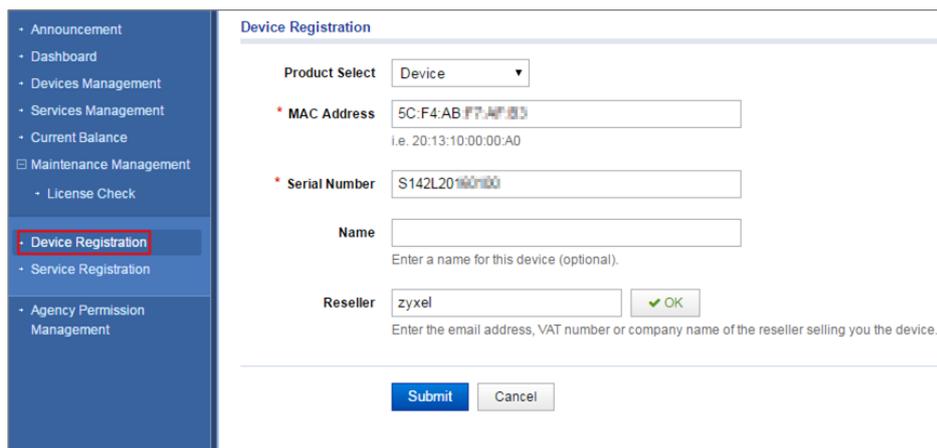
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC2500 (Firmware Version: 5.40), GS2210-8HP (Firmware Version: V4.30).

1.2.1 Device Registration

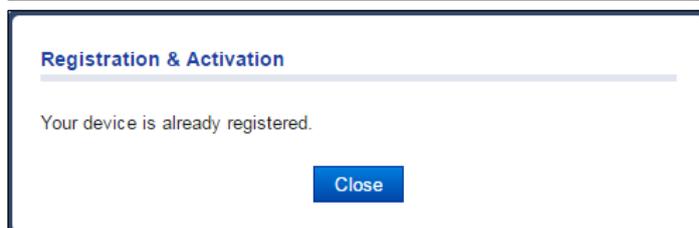
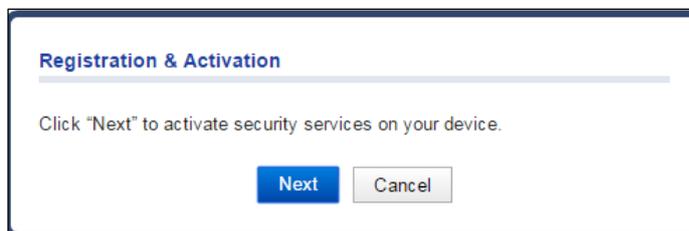
- 1 Click the hyperlink on NXC controller's GUI to connect portal.myzyxel.com in **CONFIGURATION > Licensing > Registration**.



- 2 After log in the registration portal, click the **Device Registration** to register a device by filling in the **MAC Address** and **Serial Number**. Click **Submit**.



- 3 Click **Next** to activate security services on the device, and click **Close** in next step.



1.2.2 Service Registration

- 1 Click **Service Registration** and fill in the **License Key**. Click **Submit** to register the license key.

The screenshot shows the 'Service Registration' page. On the left, a navigation menu includes 'Announcement', 'Dashboard', 'Devices Management', 'Services Management', 'Current Balance', 'Maintenance Management', and 'License Check'. The 'Service Registration' option is highlighted. The main content area features an 'Import' button, a 'License Key' input field with the value 'S-APC001-34F27B03771F', and 'Submit' and 'Cancel' buttons.

- 2 Click **Service Management**, and click the **Link**. Select a device, and then click **Submit** to activate the license key for the selected device.

The screenshot shows the 'Services Management' page. A green banner at the top states 'License is registered successfully'. Below it, there's a 'Product Select' dropdown set to 'Device' and a search bar. A table lists license keys with columns for 'License Key', 'Name', 'Type', 'Amount/Time', and 'Status'. One entry is visible: 'S-APC001-34F27B03771F' for 'Managed AP Service' with 'Standard' type and '8 Piece' amount. A 'Link' button is next to it. A 'Link Product' dialog box is open, showing a 'Products' dropdown with 'NXC2500(5C:F4:AB:F7:AF:83)' selected and 'Submit' and 'Cancel' buttons.

1.2.3 License Refresh

- 1 Click **Service License Refresh** in below path of NXC controller web GUI. Go to **CONFIGURATION > Licensing > Registration**.

The screenshot shows the 'License Refresh' page. A 'Service License Refresh' button is highlighted. Below it, a note states: 'Update device license information from myZyxel.com server. If you want to activate license, please go to portal.myzyxel.com'.

1.2.4 Test the Result

- 1 The Count of Managed AP number changes from 8 to 16 in **CONFIGURATION > Licensing > Registration**.

License Status					
#	Status	Registration Type	Expiration Date	Count	Service
1	Licensed	Standard		16	Managed AP Service

Set up a Wireless Connection Environment

2.1 How to configure with the Wizard Setting.

This example shows how to get start with Wizard. It will be easier to complete the deployment configuration of the AP and the NXC. The Wizard setting includes Uplink Connection, VLAN Setting and AP Profile. The NXC will be the DHCP server for the stations, and all the guest stations must pass the captive portal authentication. NXC5500 does not support Wizard Setting now.

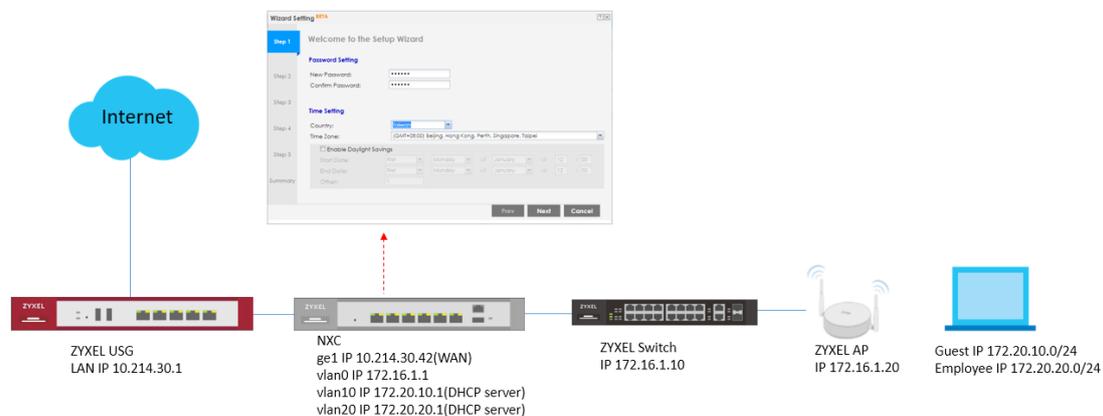


Figure 2.1 Add configuration via Wizard settings.

Note:

All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG210 (Firmware Version: V4.30), GS2210 (Firmware Version: V4.50), NXC2500 (Firmware Version: 5.40)

2.1.1 How to configure the Wizard Setting with First login?

- 1 Change the **Password Setting** to the private one. Configure the correct **Time Setting**. Enable **Daylight Saving** if needed. Click **Next**.

Wizard Setting **BETA**

Step 1 Welcome to the Setup Wizard

Password Setting

Step 2 New Password: [.....]
Confirm Password: [.....]

Time Setting

Step 3 Country: Taiwan

Step 4 Time Zone: [GMT+08:00] Beijing, Hong Kong, Perth, Singapore, Taipei

Enable Daylight Savings

Step 5 Start Date: First Monday of January at 12 : 00
End Date: First Monday of January at 12 : 00
Offset: 1

Summary

Prev Next Cancel

- 2 Configure the **Uplink Connection** which will be connected to the USG as 10.214.30.33/24, and the gateway is USG LAN IP address 10.214.30.1. Add the DNS server as 8.8.8.8. Configure the **Management VLAN** to manage AP. The default setting IP address is 172.16.1.1/24 and enable DHCP server. Click **Next**.

Wizard Setting **BETA**

Step 1 NXC2500 NAT mode

Step 2 Uplink Connection

Step 3 Static IP

IP Address: 10.214.30.33
Subnet Mask: 255.255.255.0
Gateway: 10.214.30.1
DNS Server: 8.8.8.8

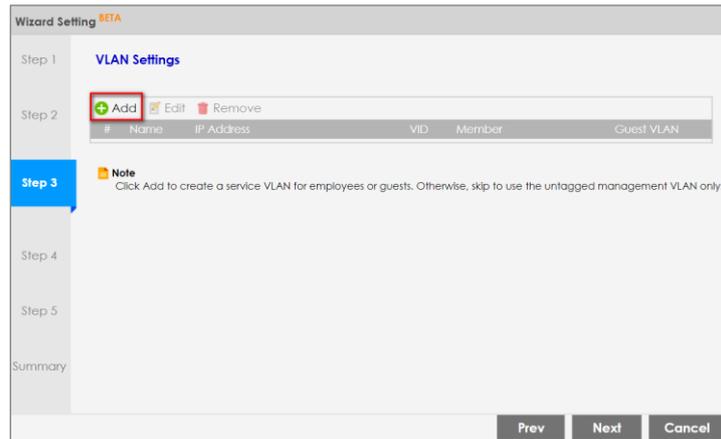
Management VLAN

Step 5 Untagged VLAN ID: 1
IP Address: 172.16.1.1
Subnet Mask: 255.255.255.0
DHCP: DHCP Server

Summary

Prev Next Cancel

- 3 Add VLAN interfaces for Employee and Guest.
 - a. Add Interface for Guest. Click **Add** to create a service VLAN for guests.



b. Set the configuration as below:

Tagged VLAN ID:10,

Guest VLAN is Enable. (Guest VLAN: This field displays if this is a guest VLAN and if the captive portal feature is enabled.)

Restrict Intranet Access: Enable

(Restrict Intranet Access: define the local networks to which wireless clients cannot have access)

Captive Portal: Enable.

Create Dynamic Guest Manager: fill in the guest manager information.

Fill in the **IP address, Subnet Mask, and DHCP setting.**

Click **OK.**

Edit Interfacevlan10

Interface Name: (2~4094)

Tagged VLAN ID: (2~4094)

Guest VLAN

Restrict Intranet Access

#	Network	Netmask
1	192.168.0.0	255.255.0.0
2	172.16.0.0	255.240.0.0
3	10.0.0.0	255.0.0.0

Captive Portal [Edit Portal Theme](#)

Internal Web Portal [Wiz_Customized_Portal](#)

External Web Portal

Walled Garden

Create Dynamic Guest Manager

User Name:

Password:

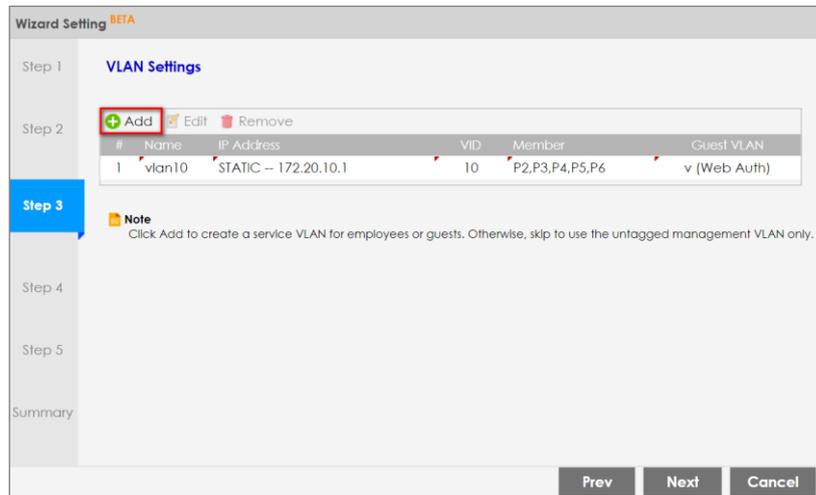
Retype:

IP Address:

Subnet Mask:

DHCP:

- c. Add Interface for Employee. Click **Add** to create a service VLAN for guests.

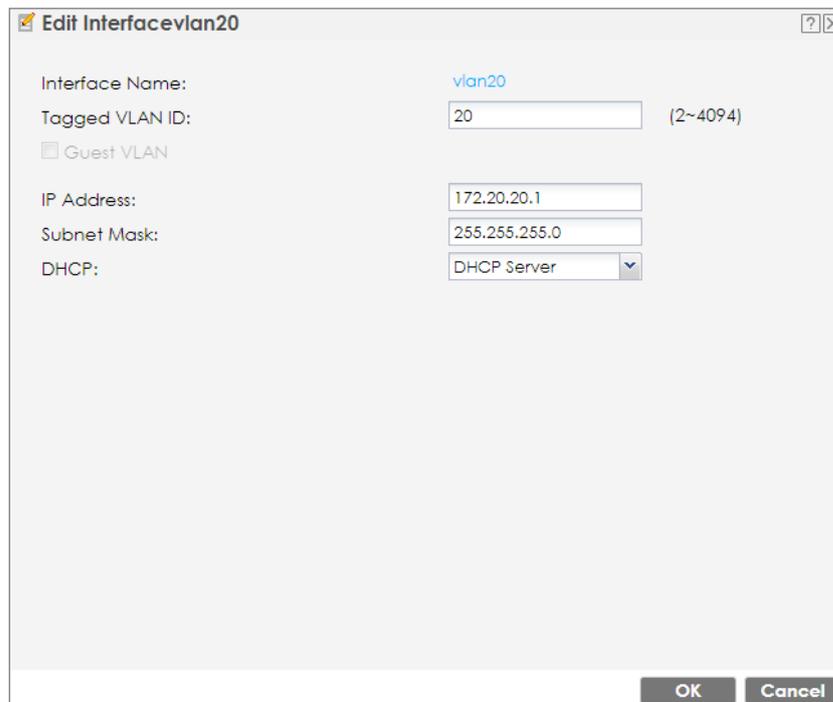


- d. Set the configuration as below:

Tagged VLAN ID: 20

Fill in the **IP address**, **Subnet Mask**, and **DHCP setting**.

Click **OK**.



e. Click **Next**.

Wizard Setting **BETA**

Step 1: VLAN Settings

Step 2:

#	Name	IP Address	VID	Member	Guest VLAN
1	vlan10	STATIC -- 172.20.10.1	10	P2,P3,P4,P5,P6	v (Web Auth)
2	vlan20	STATIC -- 172.16.20.1	20	P2,P3,P4,P5,P6	

Step 3: **Note**
Click Add to create a service VLAN for employees or guests. Otherwise, skip to use the untagged management VLAN only.

Step 4:

Step 5:

Summary:

Buttons: Prev, Next, Cancel

4 Configure the SSID profile.

a. Edit the SSID profile for Guest

Double click the SSID profile to modify the configuration.

Wizard Setting **BETA**

Step 1: SSID

Step 2:

#	Status	SSID	Security Mode	Band Mode	VLAN ID	Guest VLAN
1	ON	Zyxel	WPA2-PSK	Dual Band	1	
2	ON	Zyxel	WPA2-PSK	Dual Band	1	
3	OFF	Zyxel	WPA2-PSK	Dual Band	1	
4	OFF	Zyxel	WPA2-PSK	Dual Band	1	
5	OFF	Zyxel	WPA2-PSK	Dual Band	1	
6	OFF	Zyxel	WPA2-PSK	Dual Band	1	
7	OFF	Zyxel	WPA2-PSK	Dual Band	1	
8	OFF	Zyxel	WPA2-PSK	Dual Band	1	

Step 3:

Step 4: **Step 4**

Step 5:

Summary:

Buttons: Prev, Next, Cancel

b. Edit the first **SSID Profile** for Guest VLAN.

Wireless Name (SSID): Guest

Guest VLAN: Enable (it will fill in the Guest VLAN setting automatically.)

Security Mode: WPA2

Pre-Shared Key: 12345678

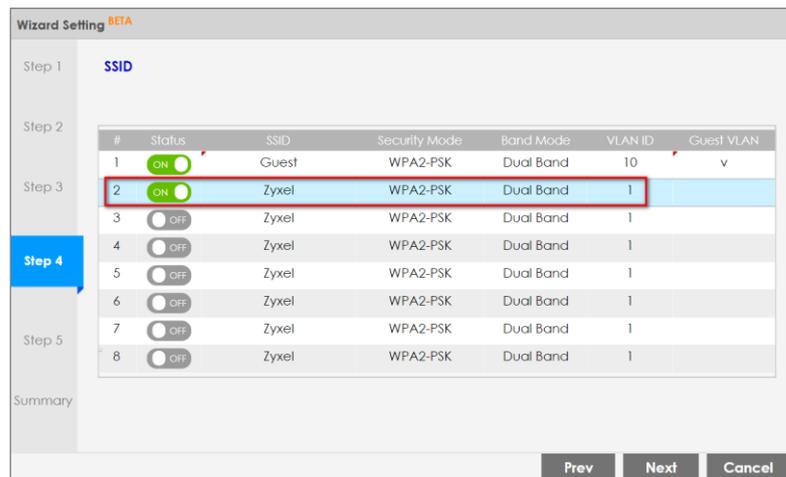
Click **OK**.

Edit SSID Profile

Wireless Name (SSID):	Guest
Status:	Activate
<input checked="" type="checkbox"/> Guest VLAN	
<input checked="" type="checkbox"/> Tagged VLAN ID	10
Band Mode:	Dual Band
Security Mode:	WPA2
Pre-Shared Key:	12345678

OK Cancel

- c. Edit the second **SSID Profile** for Employee.
Double click the SSID profile to modify the configuration.



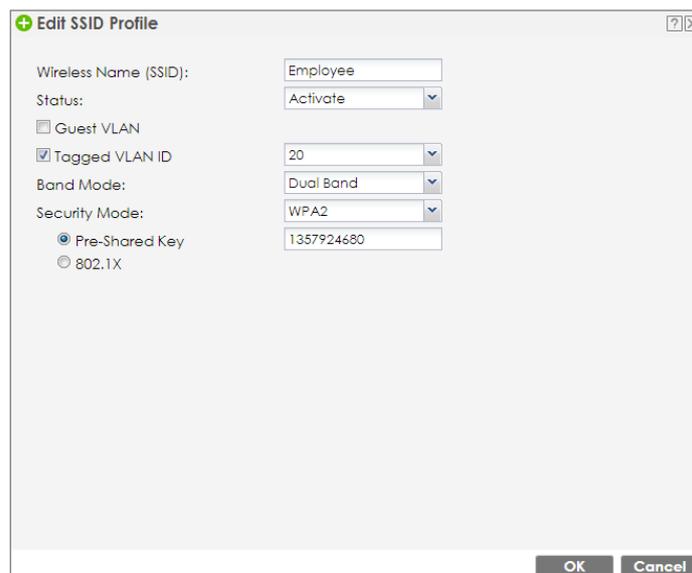
- d. Set the configuration as below:

Tagged VLAN ID: 20

Security Mode: WPA2

Pre-Shared Key: 1357924680

Click **OK**.



e. Click **Next**.

Wizard Setting **BETA**

Step 1: **SSID**

Step 2:

#	Status	SSID	Security Mode	Band Mode	VLAN ID	Guest VLAN
1	<input checked="" type="radio"/>	Guest	WPA2-PSK	Dual Band	10	v
2	<input checked="" type="radio"/>	Employee	WPA2-PSK	Dual Band	20	
3	<input type="radio"/>	Zyxel	WPA2-PSK	Dual Band	1	
4	<input type="radio"/>	Zyxel	WPA2-PSK	Dual Band	1	
5	<input type="radio"/>	Zyxel	WPA2-PSK	Dual Band	1	
6	<input type="radio"/>	Zyxel	WPA2-PSK	Dual Band	1	
7	<input type="radio"/>	Zyxel	WPA2-PSK	Dual Band	1	
8	<input type="radio"/>	Zyxel	WPA2-PSK	Dual Band	1	

Step 3:

Step 4

Step 5:

Summary:

Prev Next Cancel

5 Modify the Radio setting for the AP. Adjust the **Output Power** for both of the channels, and **Channel Width** for 5GHz.

Wizard Setting **BETA**

Step 1: **Radio**

Step 2:

Band: 2.4GHz

Channel Width: 20 MHz

Step 3:

Channel Selection: Auto

Max Output Power: 30 dBm(0-30)

Step 4:

Step 5

Band: 5GHz

Channel Width: 20/40/80MHz

Channel Selection: Auto

Max Output Power: 30 dBm(0-30)

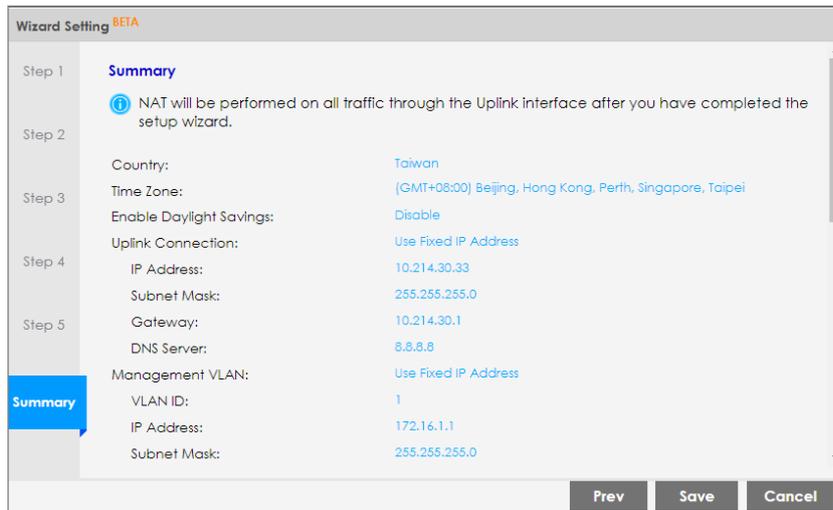
Summary:

Prev Next Cancel

- 6 Get the Summary page and confirm if all of the configurations can match to the environment.

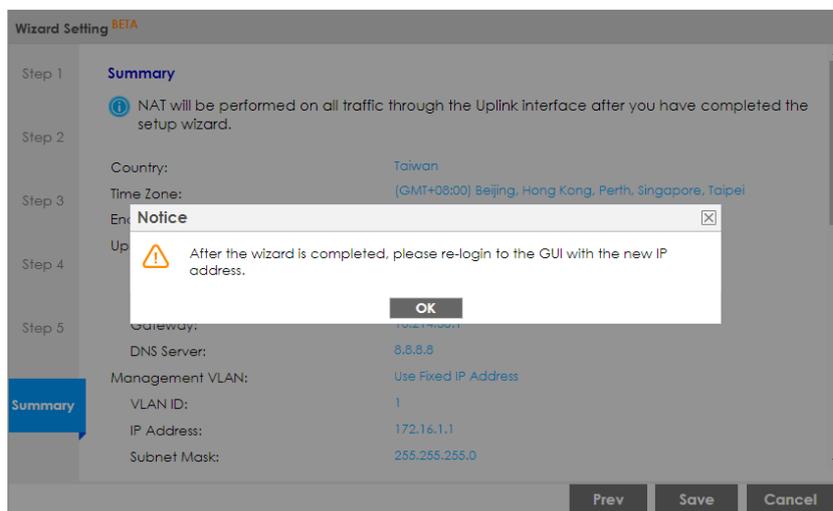
If yes, click **Save**.

If not, click **Prev** to modify the setting.



- 7 Here is the page after click **Save** from item 6.

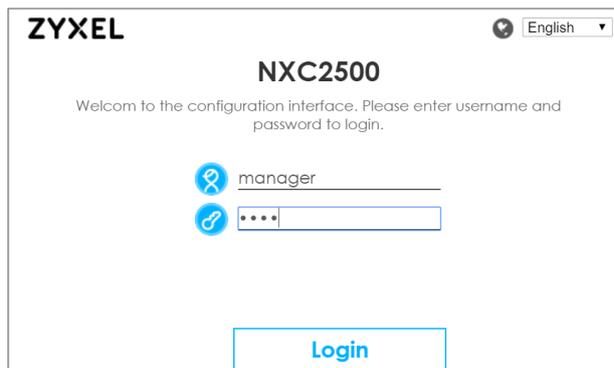
Click **OK**. And **refresh** the browser to re-login.



2.1.2 Test the Result

Connect NXC P1 to USG LAN, and NXC P2 to Switch. And connect AP to the Switch.

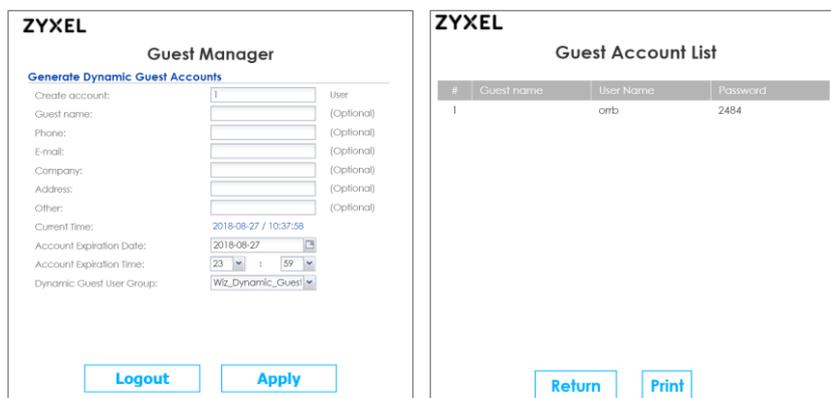
- 1 Login with guest-manager account.



The image shows the login page for the ZYXEL NXC2500 configuration interface. The page title is "ZYXEL" and "NXC2500". Below the title, it says "Welcome to the configuration interface. Please enter username and password to login." There are two input fields: one for the username "manager" and one for the password, which is masked with dots. A "Login" button is located at the bottom center. A language dropdown menu is set to "English" in the top right corner.

- 2 **Dynamic Guest User Group: Wiz_Dynamic_Guest**

Click **Apply**.

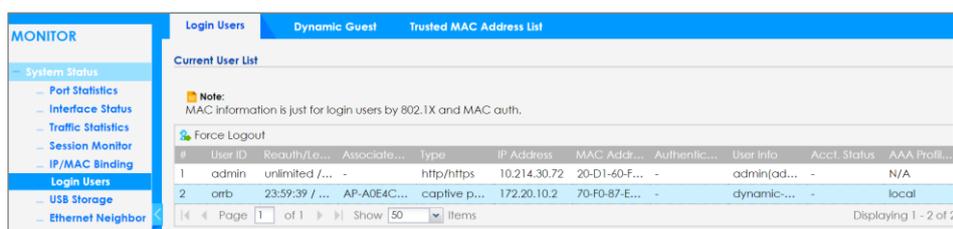


The image shows two screenshots from the ZYXEL configuration interface. The left screenshot is the "Guest Manager" page, specifically the "Generate Dynamic Guest Accounts" section. It contains several input fields for account details: "Create account:" (set to 1), "Guest name:", "Phone:", "E-mail:", "Company:", "Address:", and "Other:". It also shows the "Current Time" as 2018-09-27 / 10:37:58, "Account Expiration Date" as 2018-09-27, "Account Expiration Time" as 23:59, and "Dynamic Guest User Group" set to "Wiz_Dynamic_Guest". There are "Logout" and "Apply" buttons at the bottom. The right screenshot is the "Guest Account List" page, showing a table with one entry:

#	Guest name	User Name	Password
1		orb	2484

There are "Return" and "Print" buttons at the bottom of the table.

- 3 Use a station connect to the SSID "Guest" and login with the Guest account. Monitor the account via the Monitor > System Status > Login Users > Login Users.

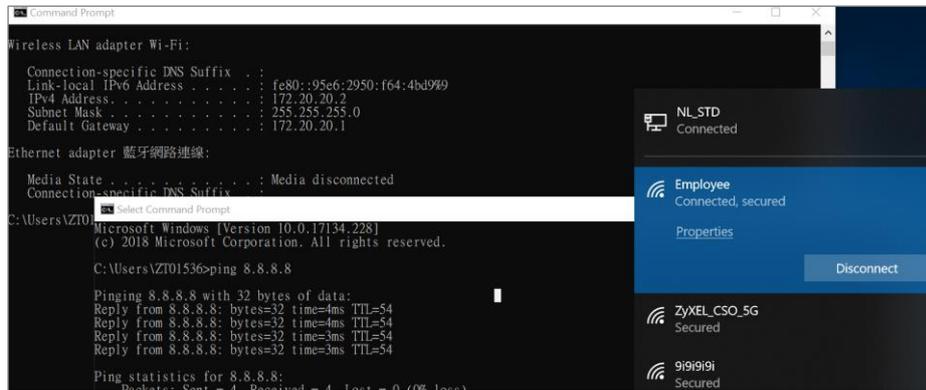


The image shows the "MONITOR" page in the ZYXEL configuration interface, specifically the "Login Users" section. The page has a sidebar with navigation options like "System Status", "Port Statistics", "Interface Status", "Traffic Statistics", "Session Monitor", "IP/MAC Binding", "Login Users", "USB Storage", and "Ethernet Neighbor". The main content area shows a "Current User List" table with the following data:

#	User ID	Reauth/Le...	Associate...	Type	IP Address	MAC Addr...	Authentic...	User Info	Acct. Status	AAA Profil...
1	admin	unlimited / ...	-	http/https	10.214.30.72	20-D1-60-F...	-	admin(ad...	-	N/A
2	orb	23:59:39 / ...	AP-A0E4C...	captive p...	172.20.10.2	70-F0-87-E...	-	dynamic...	-	local

At the bottom of the table, there is a pagination control showing "Page 1 of 1" and "Show 50 Items". The status "Displaying 1 - 2 of 2" is also visible.

4 Use a station to connect to the SSID "Employee".



2.1.3 What Could Go Wrong?

- 1 The object which is created by the Wizard cannot be deleted via the web GUI. It must be modified via the Wizard setting again.
- 2 If there is VLAN ID for the management VLAN, remember to add VLAN on the switch.

2.2 How to Set WiFi Multiple SSID for Office Environment?

2.2.1 When USG is DHCP Server for VLAN10 and VLAN20

The example instructs how to configure VLANs and set different VLANs for different SSIDs in NXC. In this example, USG is the only DHCP server in the environment, and NXC only needs to set VLAN for passing traffic. In this example, we configure interfaces, set VLANs, create security and SSID profiles, and then configure AP profiles for managed APs.

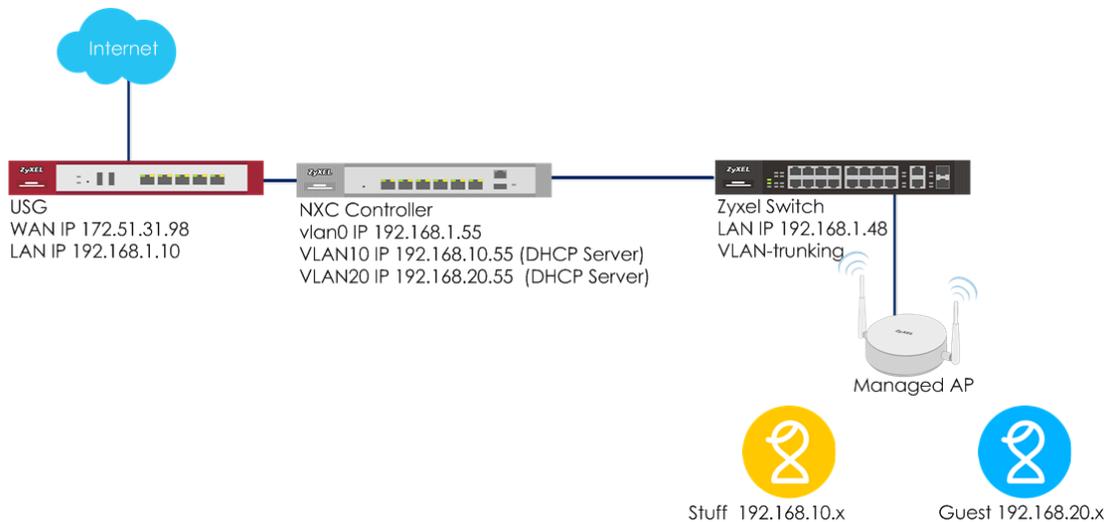


Figure 2.2.1 Set Different VLANs for Different SSIDs When USG is DHCP Server



Note:

All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC5500 (Firmware Version: 5.40), GS2210-8HP (Firmware Version: V4.30).

2.2.1.1 Configure NXC's Interface to Go to Internet

- 1 Connect NXC controller to USG LAN port. In the USG, all LAN ports are DHCP server for interface LAN, VLAN10, VLAN20, and all the stations connected to APs get an IP from the USG.
- 2 In the NXC, go to **CONFIGURATION > Network > Interface > VLAN** to set the NXC's IP address to be in the same subnet as the USG's LAN IP and have the USG act as the gateway. Double click **vlan0** to edit **IP Address Assignment** section. Click **OK**.

IP Address Assignment	
<input type="radio"/> Get Automatically	
<input checked="" type="radio"/> Use Fixed IP Address	
IP Address:	<input type="text" value="192.168.1.55"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>
Gateway:	<input type="text" value="192.168.1.10"/> (Optional)

2.2.1.2 Configure VLAN

- 1 Connect Switch to NXC ge2 (P2), and connect all APs to the switch.
- 2 In the NXC, go to **CONFIGURATION > Network > Interface > VLAN**, Click **Add** to create a new VLAN (VLAN10).



- 3 In General Settings, check **Enable**.
In Interface Properties, key in Interface Name: **vlan10**; set VID: **10**
In Member Configuration, set ge2 to be a **Member** and **Tx Tagging** to **yes**.
In IP Address Assignment, **Use Fixed IP Address** and key in **IP Address, Subnet Mask**. Click **OK**.

General Settings

Enable

Interface Properties

Interface Name:

VID: (1~4094)

Zone:

Description: (Optional)

Member Configuration

#	Port Name	Member	Tx Tagging
1	ge1	yes	yes
2	ge2	yes	yes
3	ge3	no	no
4	ge4	no	no
5	ge5	no	no
6	ge6	no	no

IP Address Assignment

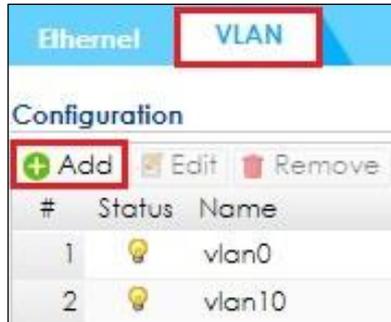
Get Automatically

Use Fixed IP Address

IP Address:

Subnet Mask:

- Click **Add** to create VLAN20 configuration in **CONFIGURATION > Network > Interface > VLAN**.



- In General Settings, check **Enable**.

In Interface Properties, key in Interface Name: **vlan20**; set VID: **20**

In Member Configuration, set ge2 to be a **Member** and **Tx Tagging** to **yes**.

In IP Address Assignment, **Use Fixed IP Address** and key in **IP Address, Subnet Mask**. Click **OK**.

General Settings

Enable

Interface Properties

Interface Name:

VID: (1~4094)

Zone:

Description: (Optional)

Member Configuration

#	Port Name	Member	Tx Tagging
1	ge1	yes	yes
2	ge2	yes	yes
3	ge3	no	no
4	ge4	no	no
5	ge5	no	no
6	ge6	no	no

IP Address Assignment

Get Automatically

Use Fixed IP Address

IP Address:

Subnet Mask:

2.2.1.3 Configure Security and SSID

- 1 Go to **CONFIGURATION > Object > AP Profile > SSID > Security List**, Click **Add** to create a new security profile for staff. In **General Settings**, key in **Staff** as profile name, and set security mode to **wpa2**. In **Authentication Settings**, select to **PSK** and key in **Pre-shared Key**. Click **OK**.

General Settings	
Profile Name:	Staff
Security Mode:	wpa2
Fast Roaming Settings	
<input type="checkbox"/> 802.11r	
Radius Settings	
Radius Server Type:	Internal
MAC Authentication Setting	
<input type="checkbox"/> MAC Authentication	
Auth. Method:	default
Delimiter (Account):	colon (:)
Case (Account):	upper
Delimiter (Calling Station ID):	colon (:)
Case (Calling Station ID):	upper
<input type="checkbox"/> Fallback to Captive Portal after MAC authentication	
Authentication Settings	
<input type="radio"/> 802.1X	
Auth. Method:	default
ReAuthentication Timer:	0
<input checked="" type="radio"/> PSK	
Pre-Shared Key:	1qaz2wsx

- Click **Add** to create a new security profile for guest.
In **General Settings**, key in **guest** as profile name, and set security mode to **none**. Click **OK**.

General Settings	
Profile Name:	guest
Security Mode:	none

- Go to **CONFIGURATION > Object > AP Profile > SSID > SSID List** and click **Add** to create a SSID for staff.
In **Profile Name** and **SSID**, key in **Staff**.
In **Security Profile**, select **Staff**.
In **VLAN ID**, key in **10**. Click **OK**.

+ Add SSID Profile	
Create new Object +	
Profile Name:	Staff
SSID:	Staff
Security Profile:	Staff
MAC Filtering Profile:	disable
Layer-2 Isolation Profile:	disable
QoS:	WMM
Rate Limiting (Per Station Traffic Rate)	
Downlink:	0 mbp (0~160, 0 is unlimited)
Uplink:	0 mbp (0~160, 0 is unlimited)
Band Select:	disable
Forwarding Mode:	Local bridge
VLAN ID:	10 (1~4094)
<input type="checkbox"/> Hidden SSID <input type="checkbox"/> Enable Intra-BSS Traffic blocking <input type="checkbox"/> Enable U-APSD <input type="checkbox"/> Schedule SSID	

4 Click **Add** to create a SSID for guest in vlan20.

In **Profile Name** and **SSID**, key in **guest**.

In **Security Profile**, select **guest**.

In **VLAN ID**, key in **20**. Click **OK**.

Add SSID Profile

Create new Object

Profile Name:

SSID:

Security Profile:

MAC Filtering Profile:

Layer-2 Isolation Profile:

QoS:

Rate Limiting (Per Station Traffic Rate)

Downlink: (0~160, 0 is unlimited)

Uplink: (0~160, 0 is unlimited)

Band Select:

Forwarding Mode:

VLAN ID: (1~4094)

Hidden SSID

Enable Intra-BSS Traffic blocking

Enable U-APSD

Schedule SSID

2.2.1.4 Configure AP Profile to Broadcast SSID

- 1 Go to **CONFIGURATION > Wireless > AP Management > AP Group**, click **Edit** for **default** group.

In Radio 1 and Radio 2, set the SSID profile, **Staff** and **guest**. Click **OK** to apply the configuration.

Radio 1 Setting

OP Mode AP Mode MON Mode Root AP Repeater AP i

Radio 1 AP Profile: v

Max Output Power: dBm (0~30)

Edit

#	SSID Profile
1	Staff
2	guest
3	disable
4	disable
5	disable
6	disable
7	disable
8	disable

Radio 2 Setting

OP Mode AP Mode MON Mode Root AP Repeater AP i

Radio 2 AP Profile: v

Max Output Power: dBm (0~30)

Edit

#	SSID Profile
1	Staff
2	guest

2.2.2 When NXC is DHCP Server for VLAN10 and VLAN20

The example instructs how to configure VLANs and set different VLANs for different SSIDs in NXC when NXC is DHCP server for VLANs. The USG does not need to do any other settings when there are different VLANs add to the environment since NXC is a DHCP server for VLANs. In this example, we configure interfaces, set VLANs, create security and SSID profiles, and then configure AP profiles for managed APs.

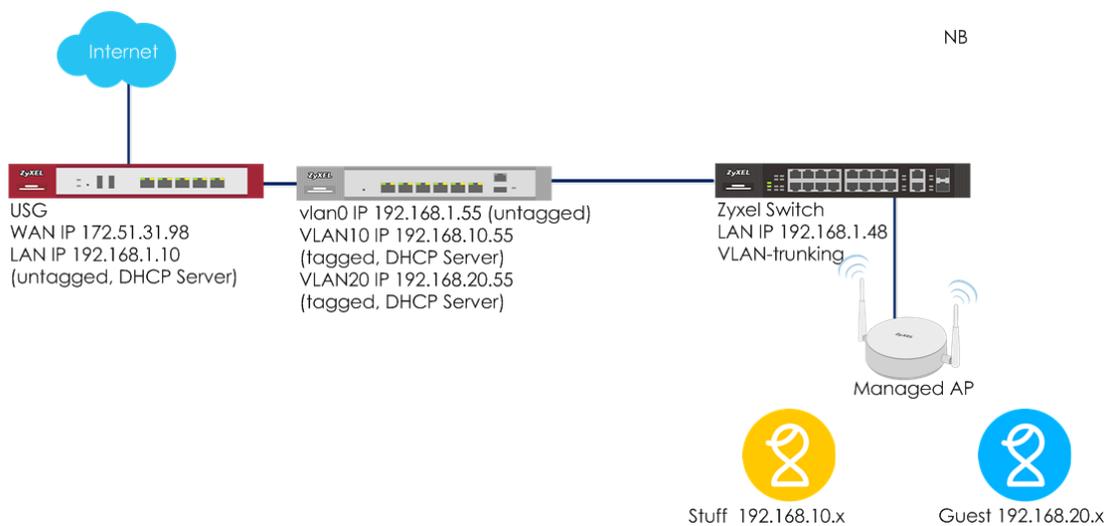


Figure 2.2.2 Set different VLANs for different SSIDs when NXC is DHCP server

Note:

All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC5500 (Firmware Version: 5.40), GS2210-8HP (Firmware Version: V4.30).

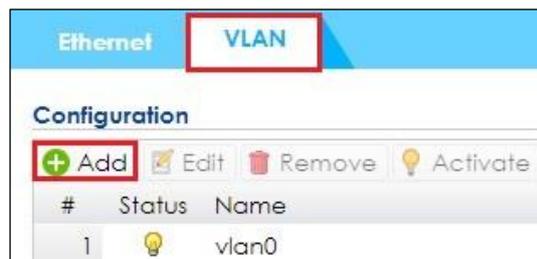
2.2.2.2 Configure Interface ge1 to Go to Internet

- 1 Connect ge1 (P1) to USG LAN port. In USG, LAN ports are DHCP server and all APs get IP from LAN.
- 2 In the NXC, go to **CONFIGURATION > Network > Interface > VLAN** to set USG's LAN IP as the gateway. Double click **vlan0** to edit **IP Address Assignment** section. Click **OK**.

IP Address Assignment	
<input type="radio"/> Get Automatically	
<input checked="" type="radio"/> Use Fixed IP Address	
IP Address:	<input type="text" value="192.168.1.55"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>
Gateway:	<input type="text" value="192.168.1.10"/> (Optional)

2.2.2.2 Configure VLAN

- 1 Connect Switch to NXC ge2, and connect all APs to the switch.
- 2 In the NXC, go to **CONFIGURATION > Network > Interface > VLAN**, Click **Add** to create a new VLAN.



3 In General Settings, check **Enable**.

In Interface Properties, key in Interface Name: **vlan10**; VID: **10**

In Member Configuration, set ge2 to be a **Member** and **Tx Tagging**.

In IP Address Assignment, **Use Fixed IP Address** and key in **IP Address, Subnet Mask, and Gateway**.

In DHCP Setting, select **DHCP server** and key in **IP Pool Start Address** and **Pool Size**. **First DNS server** select to **Customer Defined 8.8.8.8**. The users on VLAN 10 get IP from this DHCP server. Click **OK**.

General Settings

Enable

Interface Properties

Interface Name:

VID: (1~4094)

Zone: +

Description: (Optional)

Member Configuration

#	Port Name	Member	Tx Tagging
1	ge1	no	no
2	ge2	yes	yes
3	ge3	no	no
4	ge4	no	no
5	ge5	no	no
6	ge6	no	no

IP Address Assignment

Get Automatically

Use Fixed IP Address

IP Address:

Subnet Mask:

Gateway: (Optional)

Metric: (0-15)

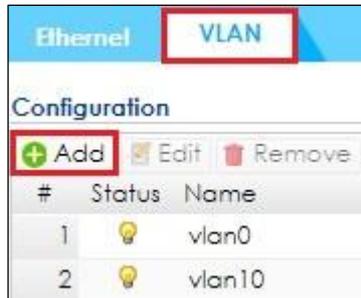
DHCP Setting

DHCP:

IP Pool Start Address (Optional): Pool Size:

First DNS Server (Optional):

- 4 Click **Add** to create VLAN20 in **CONFIGURATION > Network > Interface > VLAN**.



5 In General Settings, check **Enable**.

In Interface Properties, key in Interface Name: **vlan20**; VID: **20**

In Member Configuration, set ge2 are **Member** and **Tx Tagging**.

In IP Address Assignment, **Use Fixed IP Address** and key in **IP Address, Subnet Mask, and Gateway**.

In DHCP Setting, select **DHCP server** and key in **IP Pool Start Address and Pool Size. First DNS server** select to **Customer Defined 8.8.8.8**. The users on VLAN 20 get IP from this DHCP server. Click **OK**.

General Settings

Enable

Interface Properties

Interface Name:

VID: (1~4094)

Zone:

Description: (Optional)

Member Configuration

#	Port Name	Member	Tx Tagging
1	ge1	no	no
2	ge2	yes	yes
3	ge3	no	no
4	ge4	no	no
5	ge5	no	no
6	ge6	no	no

IP Address Assignment

Get Automatically

Use Fixed IP Address

IP Address:

Subnet Mask:

Gateway: (Optional)

Metric: (0-15)

DHCP Setting

DHCP:

IP Pool Start Address (Optional): Pool Size:

First DNS Server (Optional):

2.2.2.3 Set Policy Route

- 1 Set Policy Route in **CONFIGURATION > Network > Routing > Policy Route** to create new routing rule. Click **Show Advanced Settings**.

In **Configuration**, check **Enable**.

In **Criteria**, select **Incoming** as **Interface** and **Please select one member** is **vlan10**.

In **Next-Hop**, select **Type** as **Interface** and **Interface** is **vlan0**

In **Address Translation**, select **Source Network Address Translation** to **outgoing-interface** to use the IP address of the outgoing interface as the source IP address of the packet that matches this route. Click **OK**.

Configuration	
<input checked="" type="checkbox"/> Enable	
Description:	<input type="text"/>
Criteria	
User:	any
Incoming:	Interface
Please select one member:	vlan10
Source Address:	any
Destination Address:	any
DSCP Code:	any
Schedule:	none
Service:	any
Source Port:	any
Next-Hop	
Type:	Interface
Interface:	vlan0
<input type="checkbox"/> Auto-Disable	
DSCP Marking	
DSCP Marking:	preserve
Address Translation	
Source Network Address Translation:	outgoing-interfac

- 2 Set Policy Route in **CONFIGURATION > Network > Routing > Policy Route** to create new routing rule. Click **Show Advanced Settings**.

In **Configuration**, check **Enable**.

In **Criteria**, select **Incoming** as **Interface** and **Please select one member** is **vlan20**.

In **Next-Hop**, select **Type** as **Interface** and **Interface** is **vlan0**

In **Address Translation**, select **Source Network Address Translation** to **outgoing-interface** to use the IP address of the outgoing interface as the source IP address of the packet that matches this route. Click **OK**.

Configuration	
<input checked="" type="checkbox"/> Enable	
Description:	<input type="text"/>
Criteria	
User:	any
Incoming:	Interface
Please select one member:	vlan20
Source Address:	any
Destination Address:	any
DSCP Code:	any
Schedule:	none
Service:	any
Source Port:	any
Next-Hop	
Type:	Interface
Interface:	vlan0
<input type="checkbox"/> Auto-Disable	
DSCP Marking	
DSCP Marking:	preserve
Address Translation	
Source Network Address Translation:	outgoing-interfac

2.2.2.4 Configure Security and SSID

- 1 Go to **CONFIGURATION > Object > AP Profile > SSID > Security List**, Click **Add** to create a new security profile for staff. In **General Settings**, key in **Staff** as profile name, and set security mode to **wpa2**. In **Authentication Settings**, select to **PSK** and key in **Pre-shared Key**. Click **OK**.

General Settings	
Profile Name:	Staff
Security Mode:	wpa2
Fast Roaming Settings	
<input type="checkbox"/> 802.11r	
Radius Settings	
Radius Server Type:	Internal
MAC Authentication Setting	
<input type="checkbox"/> MAC Authentication	
Auth. Method:	default
Delimiter (Account):	colon (:)
Case (Account):	upper
Delimiter (Calling Station ID):	colon (:)
Case (Calling Station ID):	upper
<input type="checkbox"/> Fallback to Captive Portal after MAC authentication	
Authentication Settings	
<input type="radio"/> 802.1X	
Auth. Method:	default
ReAuthentication Timer:	0
<input checked="" type="radio"/> PSK	
Pre-Shared Key:	1qaz2wsx

- 2 Click **Add** to create a new security profile for guest. In **General Settings**, key in **guest** as profile name, and set security mode to **none**. Click **OK**.

General Settings	
Profile Name:	guest
Security Mode:	none

3 Go to **CONFIGURATION > Object > AP Profile > SSID > SSID List** and click Add to create a SSID for staff.

In **Profile Name** and **SSID**, key in Staff.

In **Security Profile**, select Staff.

In **VLAN ID**, key in 10. Click **OK**.

Add SSID Profile
 Create new Object ▾

Profile Name:

SSID:

Security Profile:

MAC Filtering Profile:

Layer-2 Isolation Profile:

QoS:

Rate Limiting (Per Station Traffic Rate)

Downlink: (0~160, 0 is unlimited)

Uplink: (0~160, 0 is unlimited)

Band Select:

Forwarding Mode:

VLAN ID: (1~4094)

Hidden SSID

Enable Intra-BSS Traffic blocking

Enable U-APSD

Schedule SSID

4 Click **Add** to create a SSID for guest in vlan20.

In **Profile Name** and **SSID**, key in **guest**.

In **Security Profile**, select **guest**.

In **VLAN ID**, key in **20**. Click **OK**.

Add SSID Profile
 Create new Object ▾

Profile Name:

SSID:

Security Profile:

MAC Filtering Profile:

Layer-2 Isolation Profile:

QoS:

Rate Limiting (Per Station Traffic Rate)

Downlink: (0~160, 0 is unlimited)

Uplink: (0~160, 0 is unlimited)

Band Select:

Forwarding Mode:

VLAN ID: (1~4094)

Hidden SSID

Enable Intra-BSS Traffic blocking

Enable U-APSD

Schedule SSID

2.2.2.5 Configure AP Profile to Broadcast SSID

- 1 Go to **CONFIGURATION > Wireless > AP Management > AP Group**, click **Edit** for **default** group.

In Radio 1 and Radio 2, set the SSID profile, **Staff** and **guest**.

Click **OK** to apply the configuration.

The screenshot displays the configuration interface for two radio units, Radio 1 and Radio 2. Both are set to AP Mode with a maximum output power of 30 dBm. Radio 1 is configured with the 'default' AP profile, and Radio 2 with 'default2'. Both have their SSID profiles set to 'Staff' and 'guest'.

Radio 1 Setting

OP Mode: AP Mode MON Mode Root AP Repeater AP

Radio 1 AP Profile: default

Max Output Power: 30 dBm (0~30)

#	SSID Profile
1	Staff
2	guest
3	disable
4	disable
5	disable
6	disable
7	disable
8	disable

Radio 2 Setting

OP Mode: AP Mode MON Mode Root AP Repeater AP

Radio 2 AP Profile: default2

Max Output Power: 30 dBm (0~30)

#	SSID Profile
1	Staff
2	guest

2.2.3 Test the Result

- 1 Use a laptop to select SSID Staff and key in the security setting for connection. After connection successful, laptop can get an IP in VLAN10.

DHCP Enabled	Yes
IPv4 Address	192.168.10.100
IPv4 Subnet Mask	255.255.255.0

- 2 Use a mobile phone to select SSID guest and connect to it. After connection is successful, mobile phone can get an IP in VLAN20.

IP ADDRESS		
DHCP	BootP	Static
IP Address	192.168.20.100	
Subnet Mask	255.255.255.0	

- 3 The connected stations are visible in NXC controller **MONITOR > Station Info > Station List**.

#	IP Address	Associated AP	SSID Name	Signal Stre...	Channel	Tx Rate	Rx Rate
1	192.168.10.100	AP-A0E4CB7...	Staff	-50dBm 	36	216M	270M
2	192.168.20.100	AP-B8ECA31...	Guest	-50dBm 	1	65M	24M

2.2.4 What Could Go Wrong?

- 1 When USG is a DHCP server, users may not get IP if USG and switch do not set VLAN10 and VLAN20.
- 2 When NXC is a DHCP server, user may not go to Internet if the policy route does not set to outgoing-interface.
- 3 For the broadcasting the radio, the example only sets radio1 for 2.4GHz. If 5GHz also needs to broadcast the same setting, you can set in radio2 with the same operation steps.

2.3 How to Set up Fail Over/Fall Back?

The example instructs how to set up fail over and fall back. All management APs connect to NXC controller 1 in this example. When the NXC controller 1 fails to connect, all managed APs are controlled by NXC controller 2 by fail over setting. Once NXC controller 1 works again, the APs are back to NXC controller 1 via fall back setting.

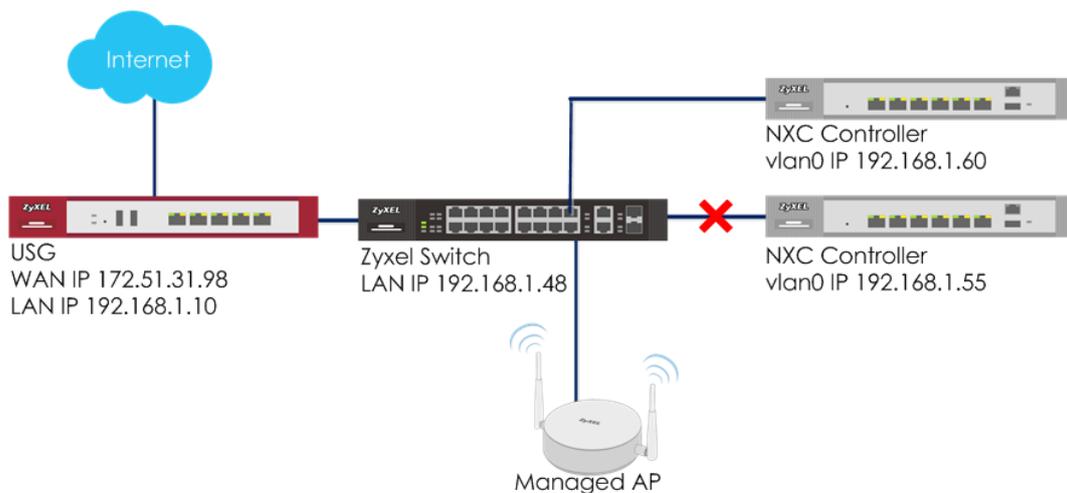


Figure 2.3 Fail Over and Fall Back

 Note:

All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC2500 (Firmware Version: 5.40), GS2210-8HP (Firmware Version: V4.30).

2.3.1 Configure Fail Over and Fall Back

- 1 To set the fail over in **CONFIGURATION > Wireless > AP Management > AP Policy**, enable **Force Override Controller IP Config on AP**. Select **Manual** and set the **Primary Controller:** 192.168.1.55 and **Secondary Controller:** 192.168.1.60

Force Override Controller IP Config on AP

Override Type: Auto Manual

Primary Controller:

Secondary Controller:

- 2 To set the fall back in **CONFIGURATION > Wireless > AP Management > AP Policy**, enable **Fall back to Primary Controller when possible**. When the **Fall Back Check Interval** is set to 30 seconds and the APs have transferred to the secondary controller because of the primary one fails to connect, the APs check whether the primary controller works every 30 seconds and change back to associate with the primary one as soon as it's available.

Fall back to Primary Controller when possible

Fall Back Check Interval: (30-86400 seconds)

2.3.2 Test the Result

- 1 In **MONITOR > Log**, check whether the NXC controller 1 sets the configuration for the AP(s). Logs show the messages after the configuration is applied to in the AP.

#	Time	Priority	Category	Message
1	2017-09-...	Info	CAPWAP	Success Send Updating Configuration to AP. MAC:04:BF:6D:16:1A:CC,Name:AP-04BF6D161ACC,Model:WAC6103D-I
2	2017-09-...	Info	CAPWAP	Start Send Updating Configuration to AP. MAC:04:BF:6D:16:1A:CC,Name:AP-04BF6D161ACC,Model:WAC6103D-I

- 2 Disconnect the NXC controller 1 from switch, and the managed APs go to find NXC controller 2 and get controlled by it. In NXC controller 2, when the AP is controlled by the 2nd NXC, the 2nd NXC also sends configuration to the AP and shows in log.

#	Time	Priority	Category	Message
1	2017-09-...	Info	CAPWAP	Success Send Updating Configuration to AP. MAC:04:BF:6D:16:1A:CC,Name:AP-04BF6D161ACC,Model:WAC6103D-I
2	2017-09-...	Info	CAPWAP	Start Send Updating Configuration to AP. MAC:04:BF:6D:16:1A:CC,Name:AP-04BF6D161ACC,Model:WAC6103D-I

- 3 In NXC controller 2, the AP also shows in **MONITOR > Wireless > AP Information > AP List**.

#	Status	Registration	Description	CPU Usage	IP Address	Model	Version	Group	Station	LED status	Power Mo...
1	✓	Mgmt AP	AP-04BF6D...	6 %	192.168.1.190	WAC6103D-I	5.10(AAXH...	default	0	🟢	Full

- 4 When NXC controller 1 links up again, the AP is controlled by NXC controller 1 again after 30 seconds.

#	Time	Priority	Category	Message
1	2017-09-...	Info	CAPWAP	Success Send Updating Configuration to AP. MAC:04:BF:6D:16:1A:CC,Name:AP-04BF6D161ACC,Model:WAC6103D-I
2	2017-09-...	Info	CAPWAP	Start Send Updating Configuration to AP. MAC:04:BF:6D:16:1A:CC,Name:AP-04BF6D161ACC,Model:WAC6103D-I

2.3.3 What Could Go Wrong?

- 1 The controllers need to have the same configurations/profiles and firmware, or the AP changes the setting/firmware after doing fail over.
- 2 If NXC controllers 1 and 2 control different APs, after the APs policy settings are applied, clear the Force Override option on controller 2 via unchecking the **Force Override Controller IP Config on AP** to avoid overriding the setting of APs from NXC controller 1.



General Settings

Force Override Controller IP Config on AP

Override Type: Auto Manual

Primary Controller:

Secondary Controller:

2.4 How to Set up Mesh to Extend Wireless Coverage?

The example instructs how to set up ZyMesh. When AP's signal needs to extend, use ZyMesh to set up connection between root AP and repeater AP. Because ZyMesh profile makes the WDS connection, the root AP and repeater AP don't need to use the same SSID for users connecting.

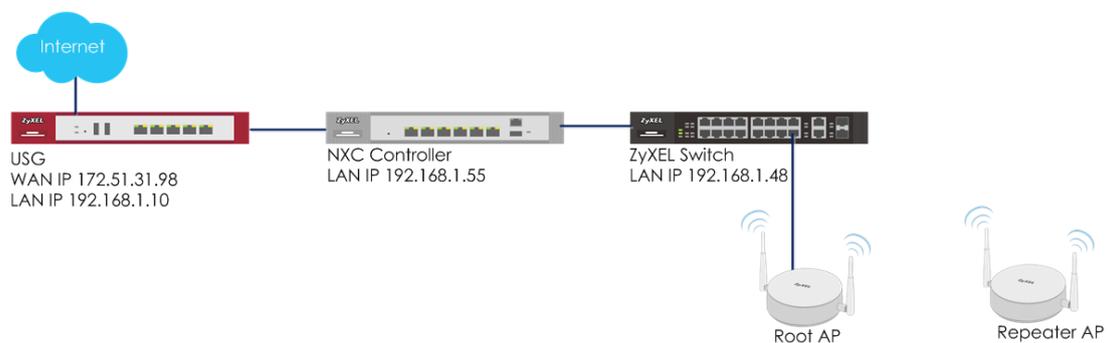


Figure 2.4 Setup ZyMesh for Root AP and Repeater AP



Note:

All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC5500 (Firmware Version: 5.40), GS2210-8HP (Firmware Version: V4.30).

2.4.1 Configure ZyMesh Profile

- 1 Both root AP and repeater AP need to use the same ZyMesh profile to set up connection.

Go to **CONFIGURATION > Object > ZyMesh Profile**, Click **Add** to create a ZyMesh SSID and pre-shared key. The ZyMesh SSID hides and it is not visible.

In **General Settings**, set **Profile Name**, **ZyMesh SSID**, and **Pre-Shared Key**. Click **OK**.

+ Add ZyMesh Profile	
General Settings	
Profile Name:	ZyMesh_Setup
ZyMesh SSID:	ZyMesh_Setup i
Pre-Shared Key:	12345678

2.4.2 Configure Root AP and Repeater AP

- 1 In the same AP, radio 2 is not able to work as the repeater when radio 1 is root AP. Select an AP in **CONFIGURATION > Wireless > AP Management > Mngt. AP List** to edit the selected AP as root AP.

In Radio 1 Setting, check **Override Group Radio Setting**. Select **Root AP** and **ZyMesh_AP** as the Radio 1 ZyMesh Profile. Click **OK**.

The screenshot shows the 'Radio 1 Setting' form. The 'Override Group Radio Setting' checkbox is checked and highlighted with a red box. Under 'OP Mode', the 'Root AP' radio button is selected and highlighted with a red box. The 'Radio 1 AP Profile' dropdown is set to 'default'. The 'Radio 1 ZyMesh Profile' dropdown is set to 'ZyMesh_AP' and highlighted with a red box.

- 2 Select an AP in the Mngt. AP List and configure the AP as repeater in **CONFIGURATION > Wireless > AP Management > Mngt. AP List**.

In Radio 1 Setting, check **Override Group Radio Setting**. Select **Repeater AP** and **ZyMesh_AP** as the Radio 1 ZyMesh Profile. Click **OK**.

The screenshot shows the 'Radio 1 Setting' form. The 'Override Group Radio Setting' checkbox is checked and highlighted with a red box. Under 'OP Mode', the 'Repeater AP' radio button is selected and highlighted with a red box. The 'Radio 1 AP Profile' dropdown is set to 'default'. The 'Radio 1 ZyMesh Profile' dropdown is set to 'ZyMesh_AP' and highlighted with a red box.

2.4.3 Test the Result

- 1 Check ZyMesh Link Info in **MONITOR > Wireless > ZyMesh > ZyMesh Link Info**. When the ZyMesh sets up successfully, root AP and repeater AP information shows in the ZyMesh link info.

ZyMesh Link Info										
#	Description	IP Address	Channel ID	Hop	Uplink AP Info	SSID Name	Signal Stre...	Link Up Time	MAC Addr...	Tx Power
1	AP-A0E4CB7E...	192.168.1.191	6	1	Root / AP-04...	ZyMesh_cap	-50dBm / -...	2017/09/1...	A2:23:CB:7...	28 dBm

2.4.4 What Could Go Wrong?

- 1 If the ZyMesh profiles are not the same on root AP and repeater AP, it's not able to connect using ZyMesh successfully. Go to **CONFIGURATION > Wireless > AP Management > Mgnt. AP List** to make sure root AP and repeater AP's ZyMesh profile are the same.

Radio 1 Setting

Override Group Radio Setting

OP Mode AP Mode MON Mode **Root AP** Repeater AP i

Radio 1 AP Profile: default

Radio 1 ZyMesh Profile: **ZyMesh_AP**

Radio 1 Setting

Override Group Radio Setting

OP Mode AP Mode MON Mode Root AP **Repeater AP** i

Radio 1 AP Profile: default

Radio 1 ZyMesh Profile: **ZyMesh_AP**

- 2 When ZyMesh set up, the repeater AP's throughput is lower due to path loss.
- 3 When ZyMesh set up, the repeater AP's uplink port is down to avoid loop. It is able to bridge via uplink port by checking **Enable Wireless Bridging** in repeater AP's setting. The repeater AP can still transmit data through its Ethernet port.

Override Group Radio Setting

OP Mode AP Mode MON Mode Root AP Repeater AP i

Radio 1 AP Profile: default

Radio 1 ZyMesh Profile: ZyMesh_AP

Enable Wireless Bridging

- 4 The APs' country code must be the same for setting up ZyMesh connection. You can check the country code in

CONFIGURATION > Wireless > Controller

Controller Setting	
Country Code:	Taiwan <input type="button" value="v"/>

- 5 DCS on root and repeater AP will cause the ZyMesh disconnected when the AP change to the other change. So, please disable DCS or set longer time for doing DCS when building up a ZyMesh deployment.

2.5 How to Set up Seamless Wireless Roaming?

The example instructs how to configure two APs profile and topology for roaming. These two APs need to use the same SSID, security, DHCP server, and signal overlap. The two APs have the same DHCP server from USG, and this example shows how to configure APs in the same SSID and security.

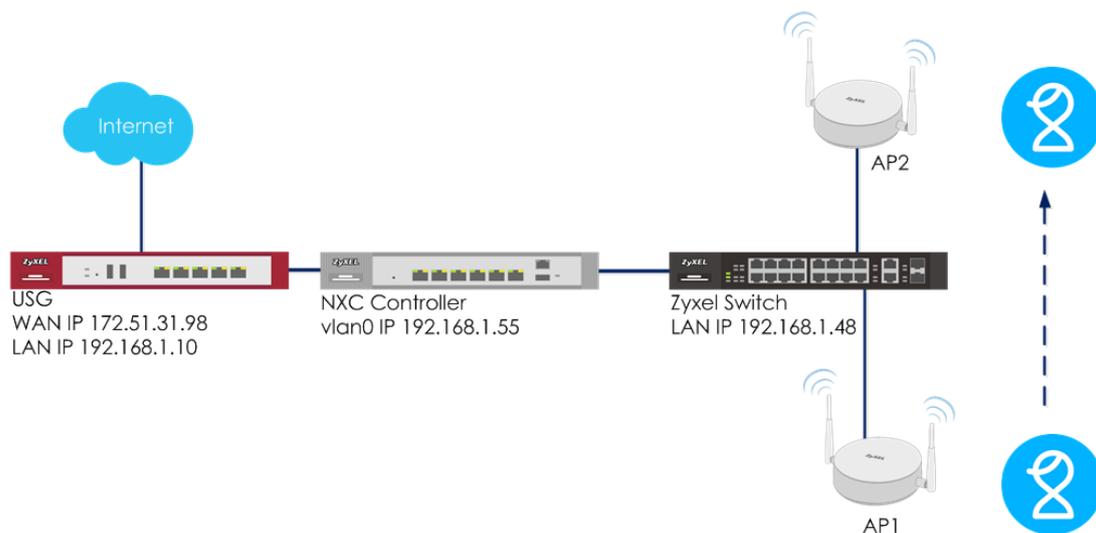


Figure 2.5 Roaming from AP1 to AP2

 **Note:**

All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC5500 (Firmware Version: 5.40), GS2210-8HP (Firmware Version: V4.30).

2.5.1 Configure APs via AP Group

- 1 Roaming needs to use the same SSID and security. AP group can assign APs' configuration, so that APs have the same SSID and security.

Create a new security profile for roaming.

Go to **CONFIGURATION > Object > AP Profile > SSID > Security List**, Click **Add**.

In **General Settings**, key in **Roaming** as profile name, and set security mode to **wpa2**.

In **Authentication Settings**, select to **PSK** and key in **Pre-shared Key**. Click **OK**

General Settings	
Profile Name:	Roaming
Security Mode:	wpa2
Fast Roaming Settings	
<input type="checkbox"/> 802.11r	
Radius Settings	
Radius Server Type:	Internal
MAC Authentication Setting	
<input type="checkbox"/> MAC Authentication	
Auth. Method:	default
Delimiter (Account):	colon (:)
Case (Account):	upper
Delimiter (Calling Station ID):	colon (:)
Case (Calling Station ID):	upper
<input type="checkbox"/> Fallback to Captive Portal after MAC authentication fail	
Authentication Settings	
<input type="radio"/> 802.1X	
Auth. Method:	default
ReAuthentication Timer:	0
<input checked="" type="radio"/> PSK	
Pre-Shared Key:	1qaz2wsx

2 Create a new SSID for roaming.

In **Profile Name** and **SSID**, key in **Roaming**.

In **Security Profile**, select **Roaming**. Click **OK**



+ Add SSID Profile	
Create new Object ▾	
Profile Name:	Roaming
SSID:	Roaming
Security Profile:	Roaming ▾
MAC Filtering Profile:	disable ▾
Layer-2 Isolation Profile:	disable ▾
QoS:	WMM ▾

- 3 Create a new AP group for roaming, and select AP1 and AP2 as member of the AP group.

In **Profile Name**, key in **Roaming**.

In **Radio1 Setting and Radio 2 Setting**, change SSID profile to **Roaming**.

In **AP List**, move two APs from **Available** to **Member**. Click **OK**.

+ Add AP Group Profile

General Settings

Group Name: (Optional)

Description: (Optional)

Radio 1 Setting

OP Mode AP Mode MON Mode Root AP Repeater AP

Radio 1 AP Profile:

Max Output Power: dBm (0~30)

Edit

#	SSID Profile
1	Roaming
2	disable

Radio 2 Setting

OP Mode AP Mode MON Mode Root AP Repeater AP

Radio 2 AP Profile:

Max Output Power: dBm (0~30)

Edit

#	SSID Profile
1	Roaming
2	disable

AP List

Available

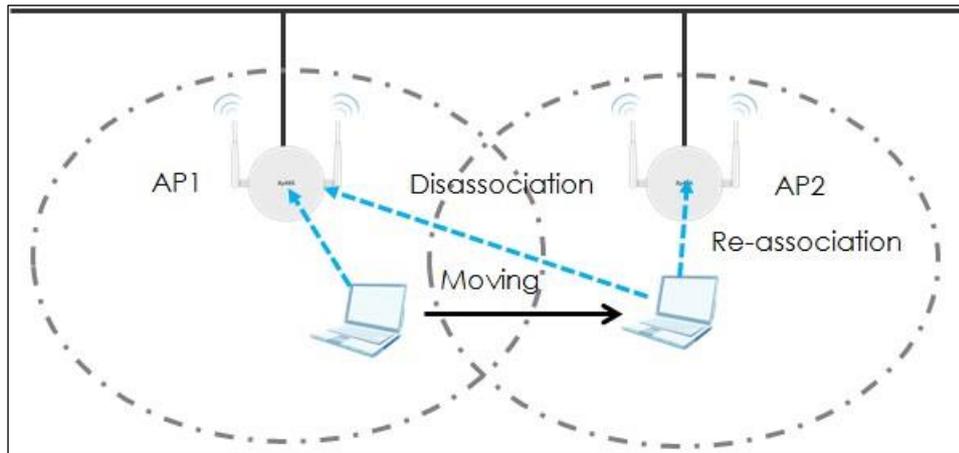
Member

=== default ===

- AP-04BF6D161ACC(04:BF:6D:16:1A:CC)
- AP-A0E4CB7EEC22(A0:E4:CB:7E:EC:22)

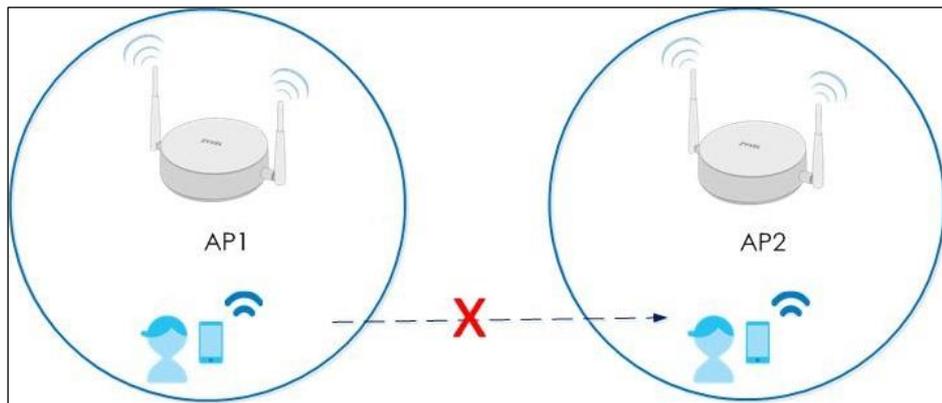
2.5.2 Test the Result

- 1 User connects to the SSID and make sure the user can access the Internet without any problem.
- 2 When user is roaming from AP1 to AP2, the connection is not interrupted because of reconnection from AP1 to AP2.

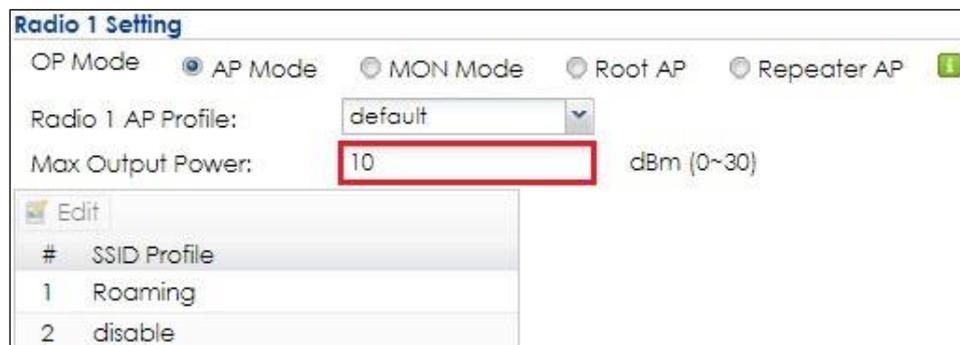


2.5.3 What Could Go Wrong?

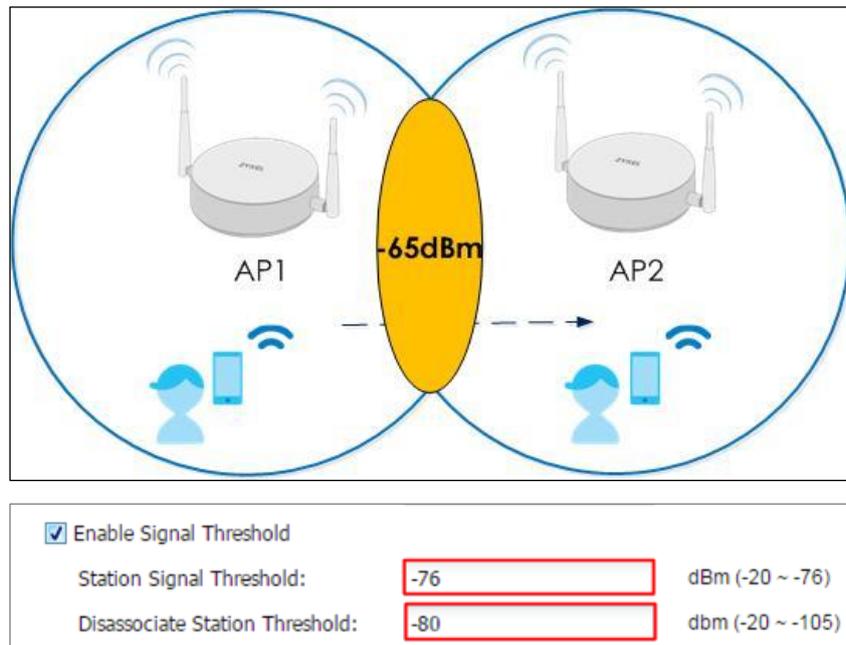
- 1 User may disconnect when AP1 and AP2's signal is not overlapping. If the Max out power is 30 and two APs still don't overlap, please move these two APs closer to make signal overlap.



- 2 When AP1 and AP2 overlapping is too large, the AP1 and AP2's signal are interference to each other. Here are two ways for solving this issue. One is to make these two APs more far away from each other; the other is to decrease Max output power.



- 3 Enable threshold in radio might cause disconnection between AP and station. When the overlap area RSSI is lower than threshold value, station is not able to connect to AP. The **Station Signal Threshold** and **Disassociation Station Threshold** should be lower than the overlapping area's RSSI.



- 4 "Band Select" may potentially cause interruptions for time-sensitive applications because of roaming delays. So, it's suggested disabling band select.
- 5 The connection might not be stable if the "Load Balance" is enabled and the maximum station number is reached. The roaming station may connect to the AP and disconnect soon.
- 6 It's up to station to roam or not. The roaming tendency is able to modify in computer's setting.

2.6 How to implement Wireless VoIP Best Practice (VoWiFi)?

This guide provides several recommendations to optimize the quality of VoIP and mitigate the latency when mobile devices roaming between APs. For the roaming, the two APs have the same DHCP server from USG, and this example shows how to configure APs in the same SSID, security and enable important features.

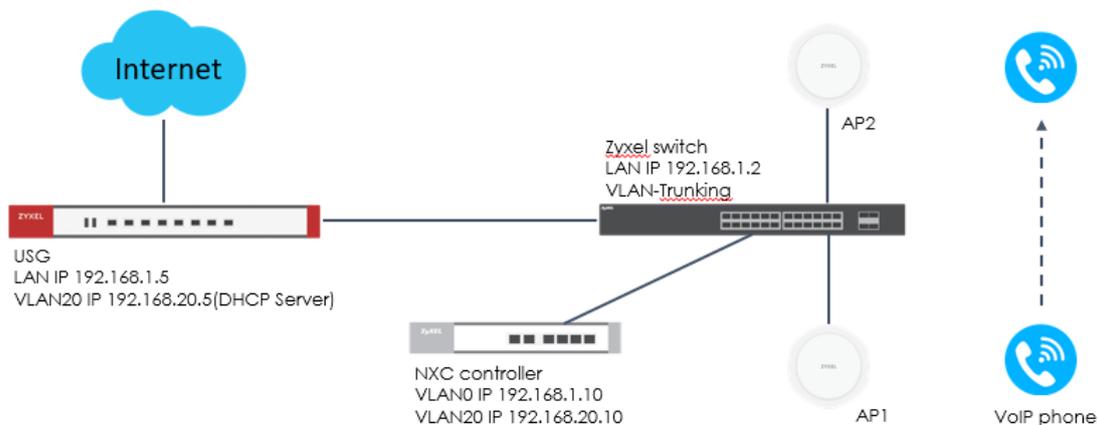


Figure 2.6 VoIP phone roaming from AP1 to AP2



Note:

All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.33), NXC5500 (Firmware Version: 5.40), GS2210-8HP (Firmware Version: V4.50).

2.6.1 Configure Interface

- 1 The USG have a VLAN20 DHCP pool only for Voice phones.
Connect Switch to NXC ge1 (P1), and connect all APs to the switch. The switch ports connect all the devices must have in the VLAN 20 with Tx Tagging.
- 2 In the NXC, go to **CONFIGURATION > Network > Interface > VLAN**, Click **Add** to create a new VLAN (VLAN20).

- In **General Settings**, check **Enable**. In Interface Properties, key in **Interface Name**, key in **vlan20**; set **VID** with **20**. In **Member Configuration**, set ge1 to be a **Member** and **Tx Tagging** to **yes**. In **IP Address Assignment-Use Fixed IP Address** and key in **IP Address**, **Subnet Mask**. Click **OK**.

General Settings

Enable

Interface Properties

Interface Name:

VID: (1~4094)

Zone: ⓘ

Description: (Optional)

Member Configuration

Edit

#	Port Name	Member	Tx Tagging
1	ge1	yes	yes
2	ge2	no	no
3	ge3	no	no
4	ge4	no	no
5	gc5	no	no
6	ge6	no	no

IP Address Assignment

Get Automatically

Use Fixed IP Address

IP Address:

Subnet Mask:

Gateway: (Optional)

Metric: (0-15)

DHCP Setting

DHCP:

Enable IP/MAC Binding

Enable Logs for IP/MAC Binding Violation

2.6.2 Configure AP profile with Security, SSID and radio

- 1 Create a new security profile for VoIP phone roaming and must enable 802.11r for fast roaming.

Go to **CONFIGURATION > Object > AP Profile > SSID > Security List**, Click **Add**.

In **General Settings**, key in **VoIP** as profile name, and set security mode to **wpa2**.

In **Fast Roaming Settings**, enable **802.11r**.

In **Authentication Settings**, select to **PSK** and key in **Pre-shared Key**. Click **OK**

General Settings	
Profile Name:	VoIP
Security Mode:	wpa2
Fast Roaming Settings	
<input checked="" type="checkbox"/> 802.11r	
Radius Settings	
Radius Server Type:	Internal
MAC Authentication Setting	
<input type="checkbox"/> MAC Authentication	
Auth. Method:	default
Delimiter (Calling Station ID):	colon (:)
Case (Calling Station ID):	upper
<input type="checkbox"/> Fallback to Captive Portal after MAC authentication failu	
Authentication Settings	
<input type="radio"/> 802.1X	
Auth. Method:	default
ReAuthentication Timer:	0
<input checked="" type="radio"/> PSK	
Pre-Shared Key:	12345678
Cipher Type:	aes
Idle timeout:	300
Group Key Update Timer:	30000
<input type="checkbox"/> Management Frame Protection	<input checked="" type="radio"/> Optional <input type="radio"/> Requi

2 Create a new SSID for VoIP phone roaming.

In **Profile Name** and **SSID**, key in **VoIP**.

In **Security Profile**, select **VoIP**. Click **OK**.

In **Layer-2 Isolation Profile**, select **disable**.

In **Forwarding Mode** select **Local bridge**.

In **VLAN ID**, key in **20**.

Check the box of **Enable U-APSD** and **802.11k/v Assisted Roaming**.

+ Add SSID Profile
📄 Create new Object ▾

Profile Name:	<input type="text" value="VoIP"/>
SSID:	<input type="text" value="VoIP"/>
Security Profile:	<input type="text" value="VoIP"/>
MAC Filtering Profile:	<input type="text" value="disable"/>
Layer-2 Isolation Profile:	<input type="text" value="disable"/>
QoS:	<input type="text" value="WMM"/>
Rate Limiting (Per Station Traffic Rate)	
Downlink:	<input type="text" value="0"/> <input type="text" value="mbps"/> (0~160, 0 is unlimited)
Uplink:	<input type="text" value="0"/> <input type="text" value="mbps"/> (0~160, 0 is unlimited)
<input type="checkbox"/> Band Select	
Forwarding Mode:	<input type="text" value="Local bridge"/>
VLAN ID:	<input type="text" value="20"/> (1~4094)
<input type="checkbox"/> Controller offline policy <small>BETA</small>	
<input type="checkbox"/> Hidden SSID	
<input type="checkbox"/> Enable Intra-BSS Traffic blocking	
<input checked="" type="checkbox"/> Enable U-APSD	
<input type="checkbox"/> Enable ARP Proxy	
<input checked="" type="checkbox"/> 802.11k/v Assisted Roaming <small>BETA</small>	
<input type="checkbox"/> Schedule SSID	

- Use dedicated SSID for VoWiFi and 5 GHz for the Voice SSID is the best strategy to improve voice quality. Use 20 Mhz channel width for the voice SSID.

Edit the **default2 profile** for 5G radio.

In **channel Width**, select **20MHz**.

Check the box of **Enable Signal Threshold**, key in **-76dBm** for **Station signal Threshold** and key in **-80dBm** for **Disassociate Station Threshold**.

Check the box of **Allow Station Connection after Multiple Retries**.

Edit Radio Profile default2

Hide Advanced Settings

General Settings

Activate

Profile Name: default2

802.11 Band: 11a/n

Channel Width: 20MHz

Channel Selection: DCS Manual 36

Enable DCS Client Aware

Enable 5 GHz DFS Aware

5 GHz Channel Selection Method: auto

Time Interval

DCS Time Interval: 720 (10~1440 minutes)

Schedule

Advanced Settings

Country Code: Switzerland

Guard Interval: Short Long

Enable A-MPDU Aggregation

A-MPDU Limit: 50000 (100~65535)

A-MPDU Subframe: 32 (2~64)

Enable A-MSDU Aggregation

A-MSDU Limit: 4096 (2290~4096)

RTS/CTS Threshold: 2347 (0~2347)

Beacon Interval: 100 (40ms~1000ms)

DTIM: 2 (1~255)

Enable Signal Threshold

Station Signal Threshold: -76 dBm (-20 ~ -76)

Disassociate Station Threshold: -80 dbm (-20 ~ -105)

Allow Station Connection after Multiple Retries

Station Retry Count: 1 (1 ~ 100)

Allow 802.11n/ac stations only

2.6.3 Configure AP Group

- 1 Create a new AP group for VoIP Phone roaming, and select AP1 and AP2 as member of the AP group. The maximum 5 GHz power should <18dBm to avoid mismatch capability with client output power.

In **Profile Name**, key in **VOIP-5G_roaming**.

In **Radio 2 Setting**, select **default2** for **Radio 2 AP Profile** and change SSID profile to **VoIP**.

In **Max Output Power**, key in **18dBm**.

In **AP List**, move two APs from Available to Member. Click **OK**.

General Settings

Group Name: VoIP-5G_roaming

Description: (Optional)

Location: (Optional)

Radio 2 Setting

OP Mode AP Mode MON Mode Root AP Repeater AP

Radio 2 AP Profile: default2

Max Output Power: 18 dBm (0~30)

Edit

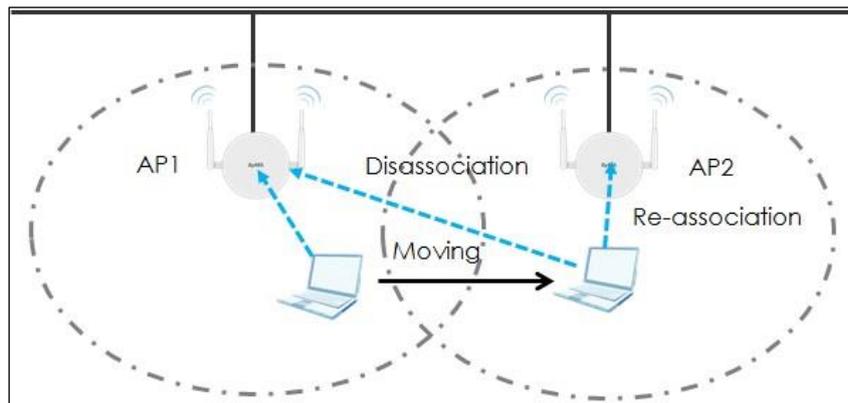
#	SSID Profile
1	VoIP
2	disable
3	disable

AP List

Available	Member
	<p>=== VoIP-5G roaming ===</p> <p>A6103- A0E4CB84B8CE(A0:E4:CB:84:B8:CE)</p> <p>A6303- 5C6A80EC04C3(5C:6A:80:EC:04:C3)</p>

2.6.4 Test the Result

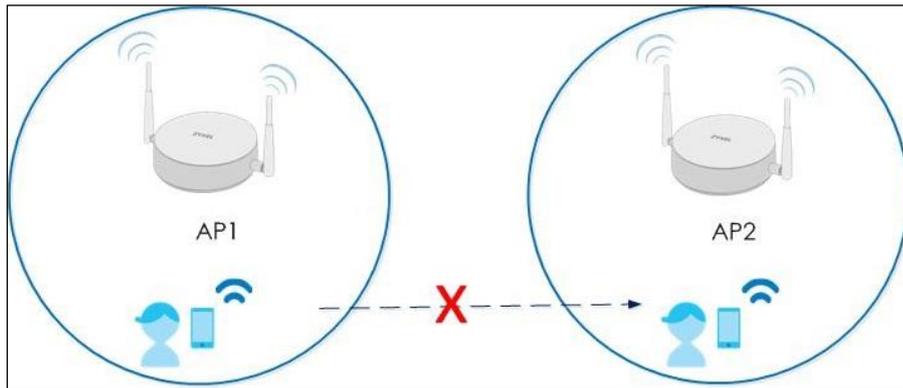
- 1 User connects to the SSID and make sure the user can access the Internet without any problem.
- 2 When user is roaming from AP1 to AP2, the connection is not interrupted because of reconnection from AP1 to AP2.



- 3 The Voice quality is good has not any delay or lose during 1-2 seconds when VoIP phone roaming between AP1 and AP2.

2.6.5 What Could Go Wrong?

- 1 User may disconnect when AP1 and AP2's signal is not overlapping. Please move these two APs closer or add some APs between two AP to make signal overlap.



- 2 When AP1 and AP2 overlapping is too large, the AP1 and AP2's signal are interference to each other. Here are two ways for solving this issue. One is to make these two APs more far away from each other; the other is to decrease Max output power.

Radio 2 Setting

OP Mode AP Mode MON Mode Root AP Repeater AP i

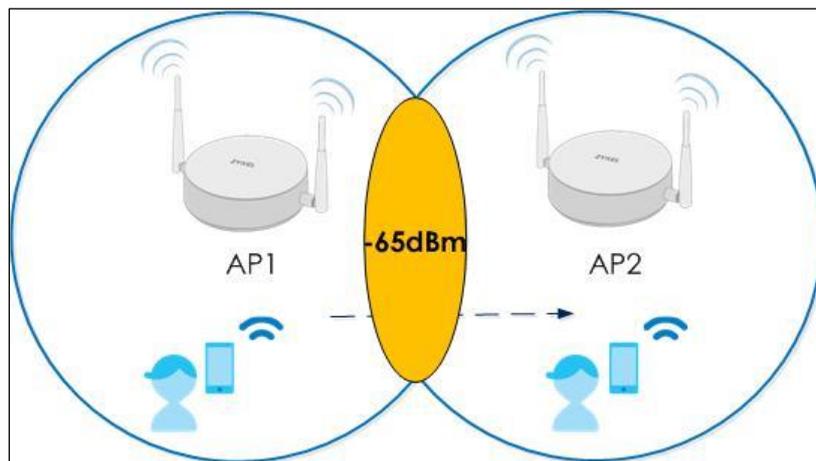
Radio 2 AP Profile: i

Max Output Power: dBm (0~30)

Edit

#	SSID Profile
1	VoIP
2	disable
3	disable

- 3 Enable threshold in radio might cause disconnection between AP and station. When the overlap area RSSI is lower than threshold value, station is not able to connect to AP. The **Station Signal Threshold** and **Disassociation Station Threshold** should be lower than the overlapping area's RSSI and check the box of **Allow Station Connection after Multiple Retries**.
- 4 Do not suggest aggressive Disassociate Station Threshold (-80 or lower is suggested) as the steering client behavior may cause call-drop.



<input checked="" type="checkbox"/> Enable Signal Threshold		
Station Signal Threshold:	<input type="text" value="-76"/>	dBm (-20 ~ -76)
Disassociate Station Threshold:	<input type="text" value="-80"/>	dbm (-20 ~ -105)
<input checked="" type="checkbox"/> Allow Station Connection after Multiple Retries		
Station Retry Count:	<input type="text" value="1"/>	(1 ~ 100)

- 5 The connection might not be stable if the "Load Balance" is enabled and the maximum station number is reached. The roaming station may connect to the AP and disconnect soon.
- 6 It's up to station to roam or not. The roaming tendency is able to modify in computer's setting.
- 7 For RF channel selection, use scheduled DCS channel in off-hours – Voice call is very sensitive to latency and jitter. When AP performs channel scanning, it will cause latency and jitter changes.

- 8** For all location desired VoWiFi clients, suggest better than -67 dBm signal coverage for 5 GHz. This usually means in one location, there will be at least one good signal AP (>-67dBm) and other 2~3 AP in fair signal (-72~-78dBm).
- 9** In the case that 2.4 GHz must be enabled for the voice SSID, always set 2.4 GHz power 6~8 dBm lower than 5 GHz. And don't use different SSID for 2.4 GHz and 5 GHz for voice application. It will sometimes confuse the roaming behavior of the phone device.
- 10** Don't use Band-steering: it could cause interoperability issues with WiFi phone. In the worst case scenario, the WiFi phone determined to use 2.4 GHz only and AP keep trying to steer it to 5 GHz. For data only, that is usually not an issue but could lead to Voice quality issue.
- 11** No more than 3 SSIDs should be enabled on any single AP.

Optimize the Wireless Environment

3.1 How to Set up User Ratio of 2.4GHz and 5GHz to Avoid WiFi Congestion?

The example instructs how to configure AP profile with band select. When 2.4GHz and 5G capable users connect to the AP, user is easy to connect to 5GHz when enabling band select. This example uses band select to balance wireless band, 2.4GHz and 5GHz.

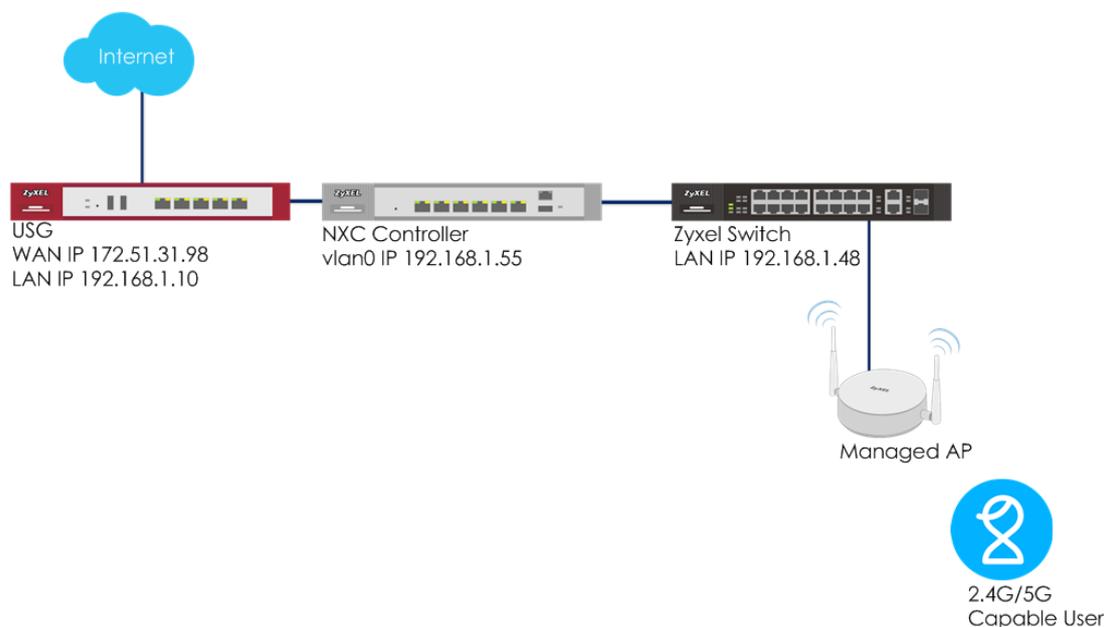


Figure 3.1 Configure AP profile with Band Select



Note:

All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC5500 (Firmware Version: 5.40), GS2210-8HP (Firmware Version: V4.30).

3.1.1 Configure Band Select

- Band select setting is in SSID. Before creating a new SSID, security is necessary to create first. Go to **CONFIGURATION > Object > AP Profile > SSID > Security List**, click Add to create a new security rule for band select.

In **General Settings**, use **BandSelect** as the **Profile Name**, and **wpa2** as the **Security Mode**.

In **Authentication Settings**, select **PSK** and make a **Pre-Shared Key**. Click **OK**.

General Settings	
Profile Name:	BandSelect
Security Mode:	wpa2
Fast Roaming Settings	
<input type="checkbox"/> 802.11r	
Radius Settings	
Radius Server Type:	Internal
MAC Authentication Setting	
<input type="checkbox"/> MAC Authentication	
Auth. Method:	default
Delimiter (Account):	colon (:)
Case (Account):	upper
Delimiter (Calling Station ID):	colon (:)
Case (Calling Station ID):	upper
<input type="checkbox"/> Fallback to Captive Portal after MAC authentication failure	
Authentication Settings	
<input type="radio"/> 802.1X	
Auth. Method:	default
ReAuthentication Timer:	0
<input checked="" type="radio"/> PSK	
Pre-Shared Key:	135797531

2 Go to **CONFIGURATION > Object > AP Profile > SSID > SSID List**, click Add to create a new SSID for band select.

Use **Band_Select** as the **Profile Name** and **SSID**. Select **BandSelect** as the **Security Profile**.

In **Band Select**, select **standard** to let user easy access to AP via band 5GHz. Check **Stop Threshold** and set station number to **10**. Check **Balance Ratio** and select **4:1**. Click **OK**.

+ Add SSID Profile
 Create new Object ▾

Profile Name: Band_Select

SSID: Band_Select

Security Profile: BandSelect ▾

MAC Filtering Profile: disable ▾

Layer-2 Isolation Profile: disable ▾

QoS: WMM ▾

Rate Limiting (Per Station Traffic Rate)

Downlink: 0 mbps (0~160, 0 is unlimited)

Uplink: 0 mbps (0~160, 0 is unlimited)

Band Select: standard ▾

Stop Threshold 10 Station (10~20)

Balance Ratio 4:1 (5GHz : 2.4GHz)

3 Go to **CONFIGURATION > AP Management > AP Group**, click Add to create a new group for band select.

In **General Setting**, set Group Name as **Band_Select**.

In **Radio 1 Setting** and **Radio 2 Setting**, select SSID profile **Band_Select**.

In **AP List**, select APs to **Member**. Click **Override Member AP Setting**. Click **Yes** when window pop up.

+ Add AP Group Profile

General Settings

Group Name:

Description: (Optional)

Radio 1 Setting

OP Mode AP Mode MON Mode Root AP Repeater AP !

Radio 1 AP Profile:

Max Output Power: dBm (0~30)

Edit

#	SSID Profile
1	Band_Select
2	disable

Radio 2 Setting

OP Mode AP Mode MON Mode Root AP Repeater AP !

Radio 2 AP Profile:

Max Output Power: dBm (0~30)

Edit

#	SSID Profile
1	Band_Select
2	disable

AP List

Available	Member
	=== default ===
	AP-04BF6D161ACC(04:BF:6D:16:1A:CC)
	AP-A0E4CB7EEC22(A0:E4:CB:7E:EC:22)

3.1.2 Test the Result

- 1 Use a 2.4GHz and 5GHz supported device (ex. Mobile phone or laptop) to connect with SSID Band_Select. The device connects to 5GHz first when it connects to the SSID.

3.1.3 What Could Go Wrong?

- 1 If the AP does not support dual band, band select does not work.
- 2 When the connected station number is greater than stop threshold station number, the band select stops working.
- 3 Band Select may potentially cause interruptions for time-sensitive applications if the client only has 2.4G ability, like roaming delays.
- 4 The station connected ratio is approximately the ratio you select in the SSID profile setting.

3.2 How to Set up RSSI Threshold to Avoid Low Rate User Connection Affected Wireless Performance?

The example instructs how to set up RSSI threshold. RSSI threshold ensure wireless clients receive good signal to prevent them from being impacted by the others with poor signal. There are two RSSI value to set. One is station signal threshold which sets a minimum client signal strength to connect with AP; the other is disassociation station threshold to sets a minimum kick-off signal strength.

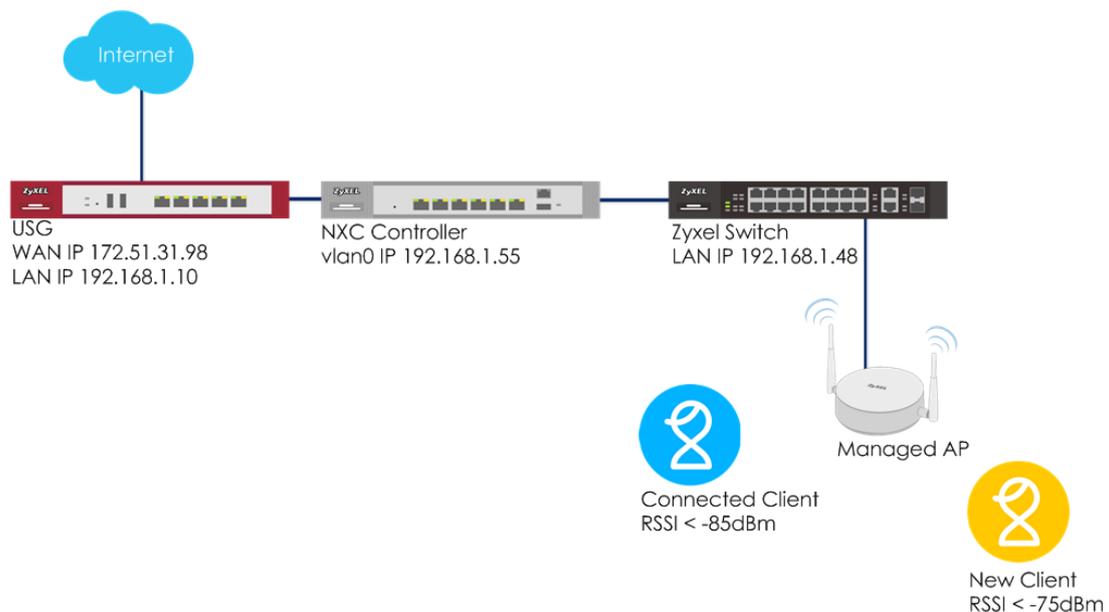


Figure 3.2 RSSI Threshold



Note:

All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC5500 (Firmware Version: 5.40), GS2210-8HP (Firmware Version: V4.30).

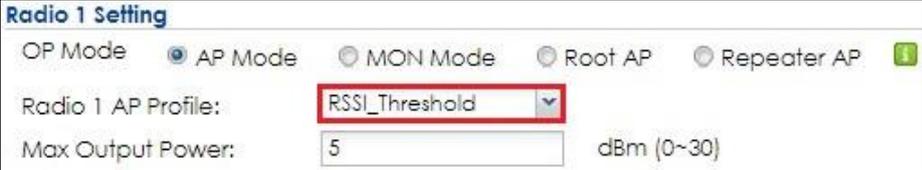
3.2.1 Configure Radio Setting for RSSI Threshold

- 1 Go to **CONFIGURATION > Object > AP Profile > Radio**, click **Add** to add a new 2.4GHz radio, **RSSI_Threshold**, for setting RSSI threshold. Click **Show Advanced Settings** to check **Enable Signal Threshold**, and edit the value for **Station Signal Threshold** and **Disassociation Station Threshold**. Click **OK**. The station needs signal strength at least -76dBm to make connection with AP, and when the signal is less than -80dBm, the AP disconnects with client.

<input checked="" type="checkbox"/> Enable Signal Threshold		
Station Signal Threshold:	<input type="text" value="-76"/>	dBm (-20 ~ -76)
Disassociate Station Threshold:	<input type="text" value="-80"/>	dbm (-20 ~ -105)

3.2.2 Apply Radio with RSSI Threshold

- 1 Go to **CONFIGURATION > Wireless > AP Management > AP Group**, click default and **Edit** it. In **Radio 1 Setting**, change **radio 1 AP Profile** to **RSSI_Threshold**. Click **Override Member AP Setting**, and then click **Yes** to apply setting to member APs.



Radio 1 Setting

OP Mode AP Mode MON Mode Root AP Repeater AP !

Radio 1 AP Profile: RSSI_Threshold ▼

Max Output Power: dBm (0~30)

3.2.3 Test the Result

- 1 In **MONITOR > Station Info > Station List**, check the new connected client's signal strength is stronger than -76dBm.

Station List							
#	IP Address	Associated AP	SSID Name	Signal Stre...	Channel	Tx Rate	Rx Rate
1	192.168.10.100	AP-A0E4CB7...	Staff	-50dBm 	36	216M	270M

- 2 In **MONITOR > Log >View AP Log**, select the AP to which the station is connected and query its log. When the connected client's RSSI is less than -80dBm, the AP kick-out the station because of the RSSI threshold.

2	2017-0...	info	Wlan Station Info	STA Association. MAC:00:19:CB:32:BE:AC, AP:AP04, Interface:...
3	2017-0...	info	Wlan Station Info	STA: 00:19:cb:32:be:ac has blocked by Lower STA Signal on C...

- 3 After modifying the RSSI threshold, it's necessary to check the station's connection status to fine tune the setting value. For example, if the stations don't connect to the nearer AP but the far one, you can adjust the disassociation station threshold to bigger value.

3.3 How to Set up Rate Limiting for Bandwidth Control?

The example instructs how to set up rate limiting for each station traffic rate. In this example, downlink is to set the maximum incoming transmission data rate, and uplinks is to set the maximum outgoing transmission data rate for each client connected to specific SSID.

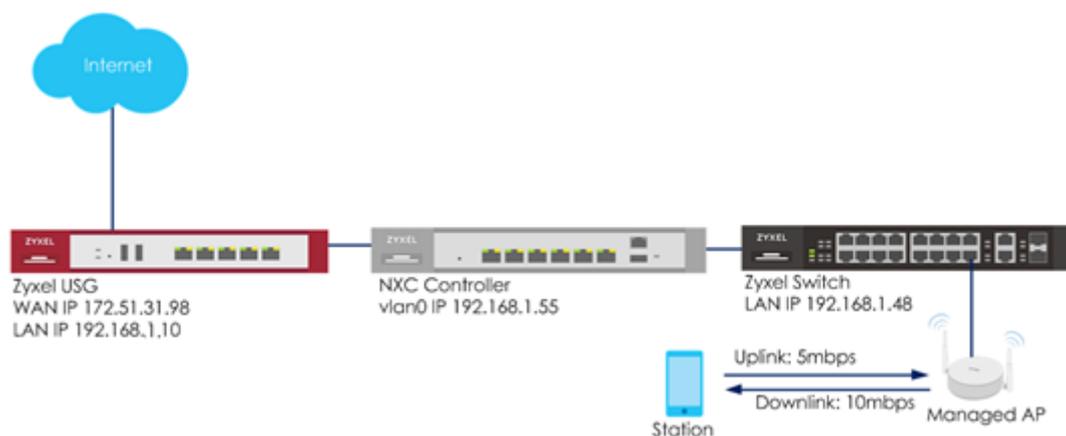


Figure 3.3 Uplink and Downlink Rate Limiting per Station



Note:

All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC5500 (Firmware Version: 5.40), GS2210-8HP (Firmware Version: V4.30).

3.3.1 Configure Rate Limiting

- 1 Go to **CONFIGURATION > Object > AP Profile > SSID**, click **Add** to add a new SSID, **RateLimiting**. Set the **Downlink** and **Uplink** maximum transmission data rate per station traffic. Click **OK**.

+ Add SSID Profile

Create new Object +

Profile Name:	<input type="text" value="RateLimiting"/>
SSID:	<input type="text" value="RateLimiting"/>
Security Profile:	<input type="text" value="default"/> ▼
MAC Filtering Profile:	<input type="text" value="disable"/> ▼
Layer-2 Isolation Profile:	<input type="text" value="disable"/> ▼
QoS:	<input type="text" value="WMM"/> ▼
Rate Limiting (Per Station Traffic Rate)	
Downlink:	<input style="width: 50px;" type="text" value="10"/> <input style="width: 50px;" type="text" value="mbps"/> ▼ (0~160, 0 is unlimited)
Uplink:	<input style="width: 50px;" type="text" value="5"/> <input style="width: 50px;" type="text" value="mbps"/> ▼ (0~160, 0 is unlimited)

3.3.2 Apply Rate Limiting to Management AP

- 1 Go to **CONFIGURATION > Wireless > AP Management > AP Group**, click default and **Edit** it. In **Radio 1 Setting/Radio 2 Setting**, change **SSID Profile** to **RateLimiting**. Click **Override Member AP Setting**, and then click **Yes** to apply setting to member APs.

Radio 1 Setting

OP Mode AP Mode MON Mode Root AP Repeater AP ?

Radio 1 AP Profile: ▼

Max Output Power: dBm (0~30)

✎ Edit

#	SSID Profile
1	RateLimiting
2	disable

Radio 2 Setting

OP Mode AP Mode MON Mode Root AP Repeater AP ?

Radio 2 AP Profile: ▼

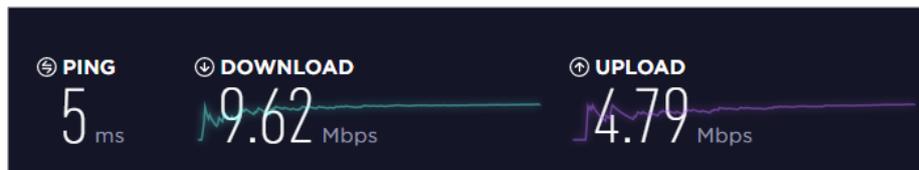
Max Output Power: dBm (0~30)

✎ Edit

#	SSID Profile
1	RateLimiting
2	disable

3.3.3 Test the Result

- 1 When the station connected to AP via SSID **RateLimiting**, the maximum incoming transmission data rate is not over 10mbps, and maximum outgoing transmission data rate is not over 5mbps.



3.4 How to Share AP loading to Optimize Wireless Performance?

The example instructs how to set up AP group with load balance. There are three types for load balance, by station number, by traffic level, and by smart classroom. This example shows the configuration of these three kinds of load balance for different scenarios and the load balance is set per radio.

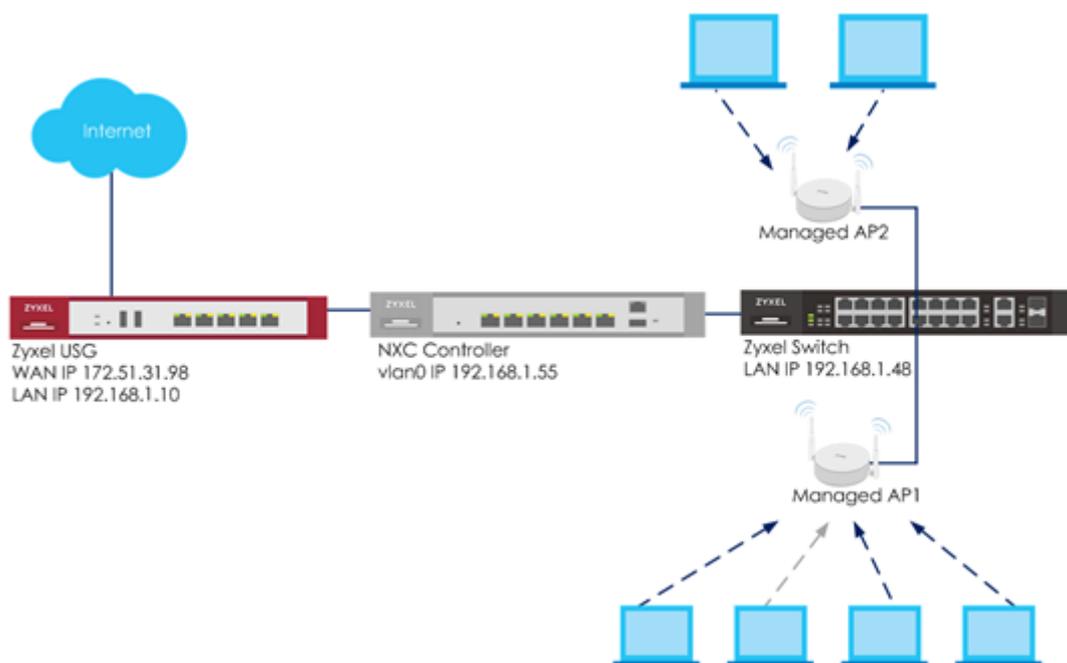


Figure 11 Load Balance



Note:

All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC5500 (Firmware Version: 5.40), GS2210-8HP (Firmware Version: V4.30).

3.4.1 Configure Load Balance to “by Station Number”

- 1 Go to **CONFIGURATION > Wireless > AP Management > AP Group**, click default for editing.

In **Load Balancing Setting**, check **Enable Load Balancing** and **Disassociate station when overloaded**. Change **Mode** to **by Station Number** and set the **Max Station Number**. Click **Override Member AP setting**. Click **Yes**. When the station number is greater than the max station number, AP disconnects clients by the longest idle time first, and then by the poorest signal strength.

Load Balancing Setting

Enable Load Balancing

Mode: By Station Number

Max Station Number: (1~127)

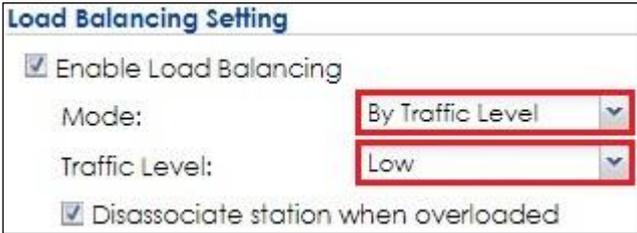
Disassociate station when overloaded

3.4.2 Configure Load Balance to “by Traffic Level”

- 1 Go to **CONFIGURATION > Wireless > AP Management > AP Group**, click default for editing.

In **Load Balancing Setting**, check **Enable Load Balancing** and **Disassociate station when overloaded**. Select **Mode** to **by Traffic Level** and set the **Traffic Level**. Click **Override Member AP setting**. Click **Yes**.

For load balancing by traffic level, the total throughput is defined as High: 35Mbps; Medium: 23Mbps; Low: 11Mbps. When total throughput of connected stations exceed the selected traffic level, AP disconnects clients with the longest idle time first, and then with the poorest signal strength.



Load Balancing Setting	
<input checked="" type="checkbox"/> Enable Load Balancing	
Mode:	By Traffic Level
Traffic Level:	Low
<input checked="" type="checkbox"/> Disassociate station when overloaded	

3.4.3 Configure Load Balance to “by Smart Classroom”

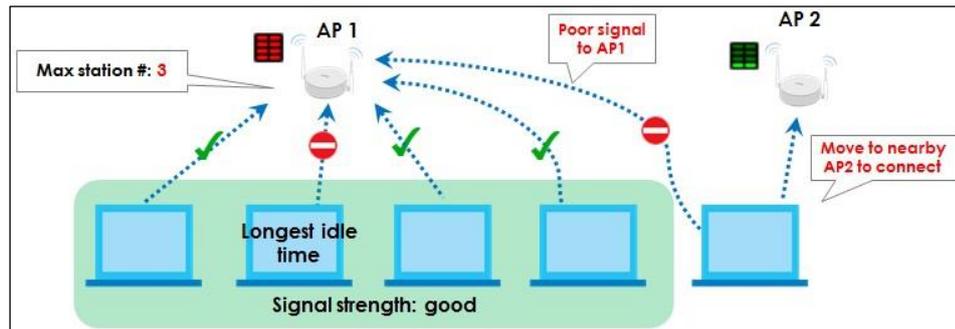
- 1 Go to **CONFIGURATION > Wireless > AP Management > AP Group**, click default for editing.

In **Load Balancing Setting**, check **Enable Load Balancing**. Select **Mode** to **by Smart Classroom** and set the **Max Station Number**. Click **Override Member AP setting**. Click **Yes**. When the station number is greater than the max station number, AP disconnects clients with the poorest signal strength.

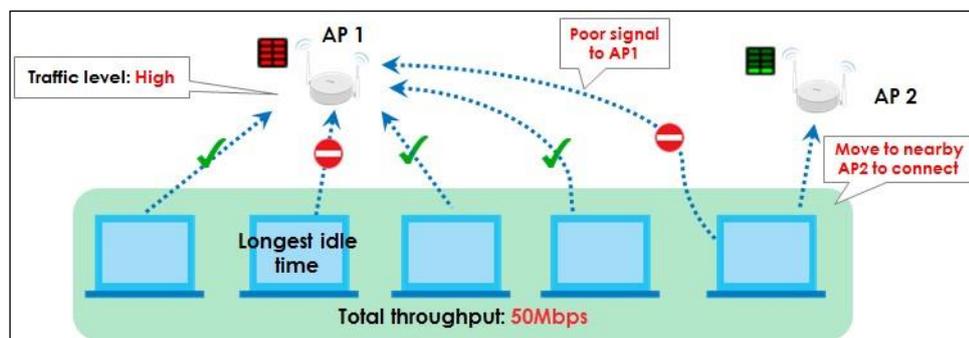
Load Balancing Setting	
<input checked="" type="checkbox"/> Enable Load Balancing	
Mode:	By Smart Classroom ▼
Max Station Number:	10 (1~127)

3.4.4 Test the Result

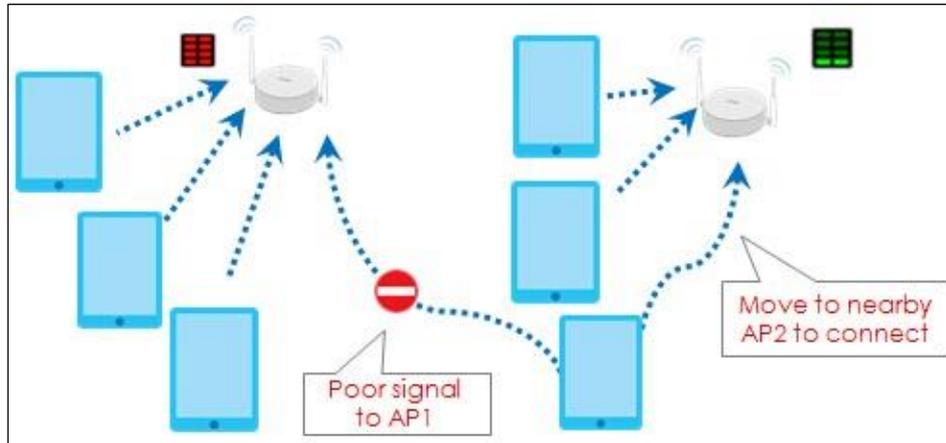
- 1 When load balancing by station number, the AP disconnects client with the longest idle time first, and then with the poorest signal strength if the client number is greater than setting number.



- 2 The traffic level is set to low and the maximum bandwidth allowed is 11 Mbps. When total throughput of connected stations exceed the selected traffic level, AP disconnects clients with the longest idle time first, and then with the poorest signal strength.



- 3 When the station number is greater than the max station number, AP disconnects clients with the poorest signal strength.



3.4.5 What Could Go Wrong?

- 1 It needs two APs to do the load Balance, or the function is not workable.
- 2 Load balance's purpose is sharing loading instead of limiting the station numbers.
- 3 If all APs are over max station number setting/traffic level, the stations still can connect to APs.

Secure the Wireless Environment - 802.1x

4.1 How to Configure 802.1x to Secure the Wireless Environment with an External RADIUS Server?

The example instructs how to set up NXC controller with an external radius server. When station wants to connect with AP, you can use an AAA server to provide access control to your network. In this example, the radius server is external but not embedded in NXC controller, and the Radius server is set ready for authentication.

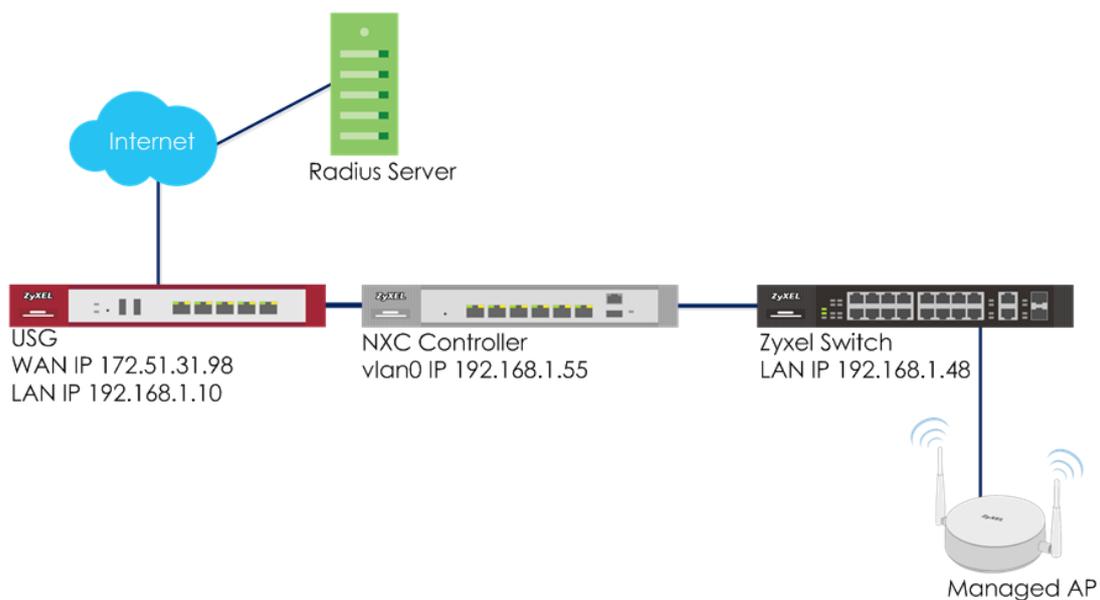


Figure 4.1 Set up AP/NXC with an External Radius Server



Note:

All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC5500 (Firmware Version: 5.40), GS2210-8HP (Firmware Version: V4.30).

4.1.1 Configure Radius Server Setting

- 1 Go to **CONFIGURATION > Object > AAA Server > RADIUS**, click **#1 radius**, and then click **Edit**. Set the **Server Address**, and **Authentication Port** is **1812**. Enter the **Key** for Radius server and click **OK**.

General Settings		
Name:	radius	
Description:	<input type="text"/>	(Optional)
Authentication Server Settings		
Server Address:	<input type="text" value="172.51.31.111"/>	(IP or FQDN)
Authentication Port:	<input type="text" value="1812"/>	(1-65535)
Backup Server Address:	<input type="text"/>	(IP or FQDN) (Optional)
Backup Authentication Port:	<input type="text"/>	(1-65535) (Optional)
Key:	<input type="password" value="*****"/>	

- 2 Go to **CONFIGURATION > Object > Auth. Method**, click **#1 default**, and then click **Edit**. Change the Method to **group radius**. Click **OK** to save.

Edit Authentication Method default	
General Settings	
Name:	default
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Remove"/> <input type="button" value="Move"/>	
#	Method List
1	group radius

4.1.2 Configure AP Profile

- 1 Configure AP profile to use 802.1x authentication and user needs to log in with their ID and Password when connecting to AP's SSID. Go to **CONFIGURATION > Object > AP Profile > SSID > Security List**, click **Add** to add security for 802.1x.

In **General Settings**, enter the **Profile Name** and select **Security Mode** to **wpa2**.

In **Radius Settings**, select **Internal** that means the authentication needs NXC to communicate with external radius server.

In **Authentication Settings**, select **802.1x** and **Auth. Method** is **default**. Click **OK**.

+ Add Security Profile

General Settings

Profile Name: Radius

Security Mode: wpa2

Fast Roaming Settings

802.11r

Radius Settings

Radius Server Type: Internal

MAC Authentication Setting

MAC Authentication

Auth. Method: default

Delimiter (Account): colon (:)

Case (Account): upper

Delimiter (Calling Station ID): colon (:)

Case (Calling Station ID): upper

Fallback to Captive Portal after MAC authentication failure

Authentication Settings

802.1X

Auth. Method: default

ReAuthentication Timer: 0 (30~30000 seconds, 0 is unlimited)

- Go to **CONFIGURATION > Object > AP Profile > SSID > SSID List**, click **add** to add a SSID for connection with 802.1x security. Key-in the **Profile Name** and **SSID**, and change **Security Profile** to **RadiusTest** which sets in step1. Click **OK** to save.

+ Add SSID Profile

Create new Object ▾

Profile Name: RadiusTest

SSID: RadiusTest

Security Profile: Radius ▾

- Go to **CONFIGURATION > Wireless > AP Management > AP Group**, click **default** to **Edit**. Change SSID to **RadiusTest** in the SSID Profile. Click **Override Member AP Setting** to apply the SSID to AP and click **Yes** in the pop-up window. Click **OK**.

Edit AP Group Profile default

General Settings

Group Name: default

Description: (Optional)

Radio 1 Setting

OP Mode: AP Mode MON Mode Root AP Repeater AP

Radio 1 AP Profile: default ▾

Max Output Power: 30 dBm (0~30)

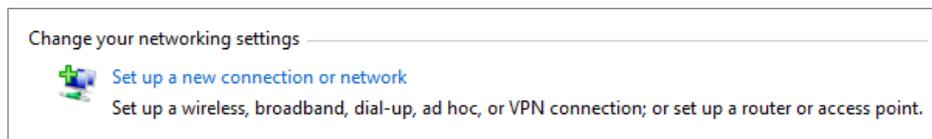
Edit

#	SSID Profile
1	RadiusTest

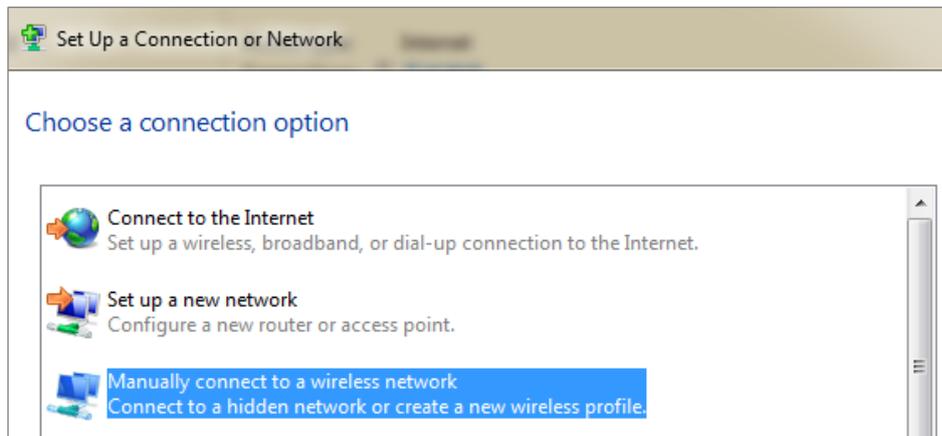
4.1.3 Test the Result

- 1 Before connecting the SSID, the computer needs to do some settings to make connection successfully.

Opening **Network and Sharing Center** in computer, click **Set up a new connection or network** for building up a new network.



- 2 Select **Manually connect to a wireless network**. Click **Next**.



- 3 Key-in the SSID **Network name** and change the **Security type** to **WPA2-Enterprise**, and the **Encryption type** is **AES**. Click **Next**.

Enter information for the wireless network you want to add

Network name:

Security type:

Encryption type:

- 4 Select **Change connection settings**.

Successfully added RadiusTest

[→ Change connection settings](#)
Open the connection properties so that I can change the settings.

- 5 Change **Security type** to **WPA2-Enterprise**, and **Encryption type** is **AES**. Click **Settings**.

Connection Security

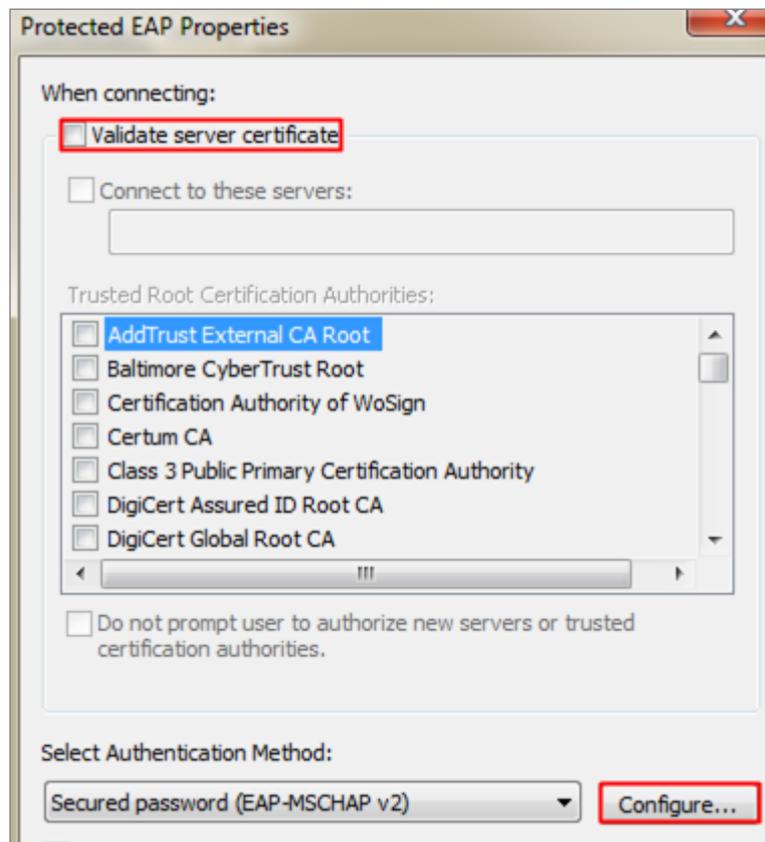
Security type:

Encryption type:

Choose a network authentication method:

Remember my credentials for this connection each time I'm logged on

- 6 Uncheck **Validate server certificate** and click **Configure**.



- 7 Uncheck the checkbox in the pop-up window. Click **OK**.



- 8 Back to the security setting page and click **Advanced settings**.

Connection Security

Security type: WPA2-Enterprise

Encryption type: AES

Choose a network authentication method:
Microsoft: Protected EAP (PEAP) Settings

Remember my credentials for this connection each time I'm logged on

Advanced settings

- 9 Check **Specify authentication mode**. Click **OK** to save.

802.1X settings 802.11 settings

Specify authentication mode

User or computer authentication Save credentials

Delete credentials for all users

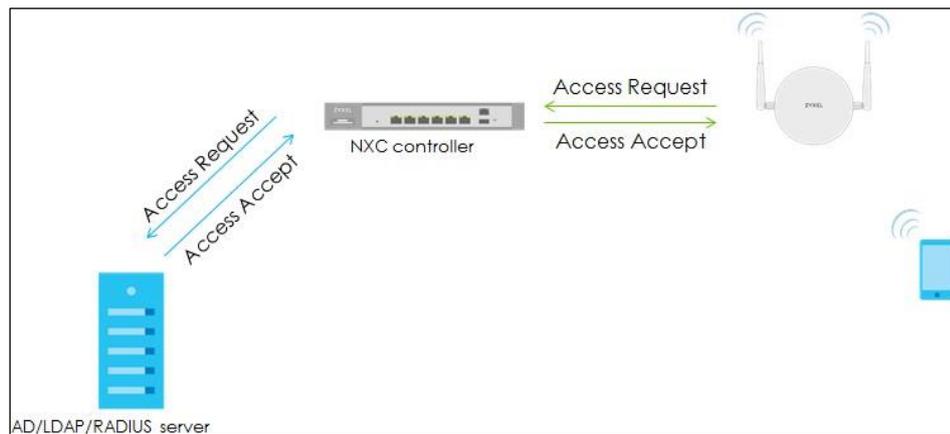
- 10 Select to the SSID, RadiusTest, for wireless connection. Enter user credentials for authentication. After entering the correct ID and password, the wireless connection is setup successfully.

Network Authentication
Please enter user credentials

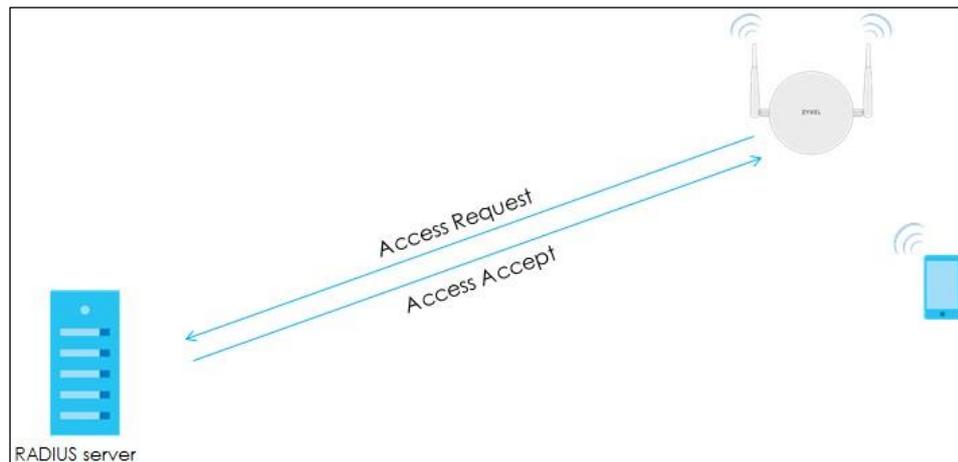


4.1.4 What Could Go Wrong

- 1 There are two kinds of **Radius Server Types** in security profile setting. **Internal** means the authentication is doing between NXC controller and Radius server. The Radius server needs to add NXC controller as trusted client.



- 2 **External** means the authentication is doing between Managed AP and Radius server. The Radius server needs to add the managed AP as trusted client.



4.2 How to Configure 802.1x to Secure the Wireless Environment with an External AD Server?

The example instructs how to set up the NXC controller with an external AD server. When the station wants to connect with the AP, you can use an AAA server to provide access control to your network. In this example, the AD server is external but not embedded in the NXC controller, and the controller is already set to use the AD server for authentication.

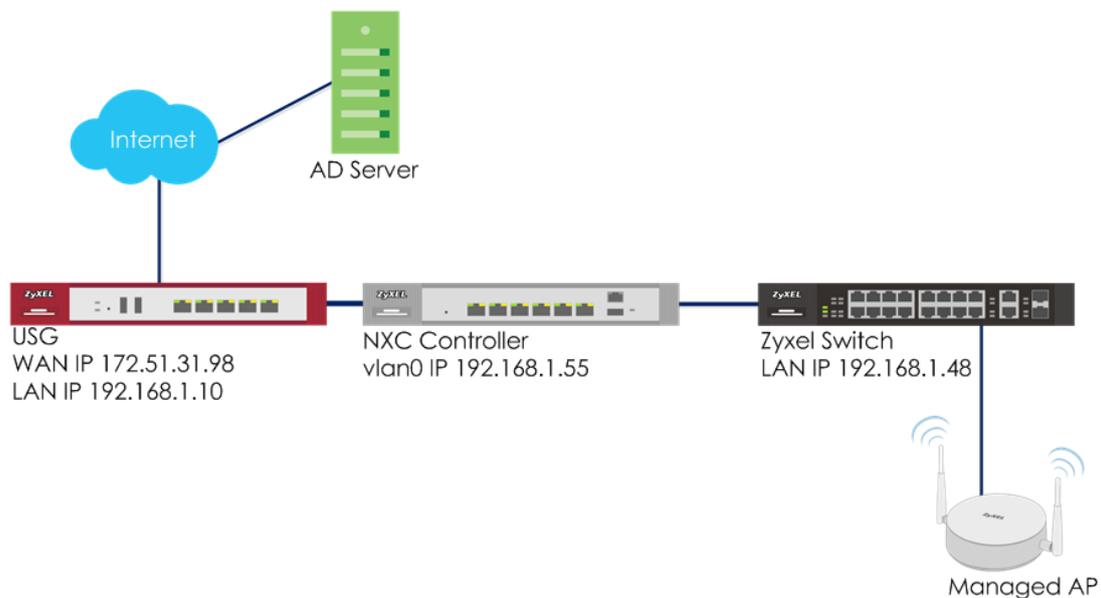


Figure 4.2 Set up AP/NXC with an External AD Server



Note:

All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC5500 (Firmware Version: 5.40), GS2210-8HP (Firmware Version: V4.30).

4.2.1 Configure AD Server Setting

- 1 Go to **CONFIGURATION > Object > AAA Server > Active Directory**, click **#1 ad**, and then click **Edit** to configure AD server's information.
- 2 In **Server Settings**, enter **Server Address**. Here use **172.51.31.112** as the example. Go to AD server to check Base DN. Here is an example for checking the Base DN on Windows server, and it can be copied from clicking right on the domain name > properties > Attribute Editor > distinguished Name > View.

Edit Active Directory ad

General Settings

Name: ad

Description: (Optional)

Server Settings

Server Address: (IP or FQDN)

Backup Server Address: (IP or FQDN) (Optional)

Port: (1-65535)

Base DN:

- 3 In **Server Authentication**, enter **Bind DN** and **Password**. You can check Bind DN in the AD server. In the AD server, clicking right on the Administrator > properties > Attribute Editor > distinguished Name > View. The Password is Administrator's password in the AD server.

Server Authentication

Bind DN:

Password:

Retype to Confirm:

- In **Domain Authentication for MSChap**, check **Enable** and enter the **User Name**, **User Password**, **Realm**, and **NetBIOS Name**.
The Realm is the domain name of the AD server.

Domain Authentication for MSChap

Enable

User Name:

User Password:

Retype to Confirm:

Realm:

NetBIOS Name:

- After finishing the configuration, enter **administrator** as the **Username** and click **Test** in **Configuration Validation**.

Test Result

Test Status:
OK

Returned User Attributes:

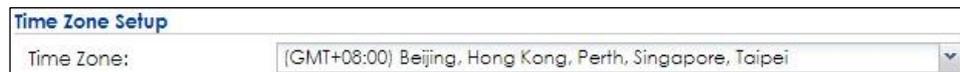
```
dn: CN=test01,CN=Users,DC=zyxel,DC=com,DC=tw
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: test01
sn: test01
userCertificate::
MIIGpTCCBY2gAwIBAgIKGeKVMAABAAADLzANBgkqhkiG9w0BAQ0
FADBUMRIwEAYKCZImiZPyLQGByCdBcxEzARBgoJkiaJk/IsZAEZFg
Njb20xFTATBgoJkiaJk/IsZAEZFgV6eXhldDESMBAGA1UEAxMJU1ZEcm
```

OK

- Go to **CONFIGURATION > Object > Auth. Method**. Select to the default method, and click **Edit**. Select the AD server you create. Click **OK**.



- Go to **CONFIGURATION > System > Date/Time** and check **Current Time and Date**. The date and time must be the same as the date and time of the AD server. If it's different, you can select the correct time zone in **Time Zone Setting**.



- Go to **CONFIGURATION > System > DNS** for setting domain zone information. In **Domain Zone Forwarder**, click Add to add a new domain zone. Enter the **Domain Zone** and **Public DNS Server** which is the AD server's IP.



4.2.2 Configure AP Profile

- 1 Configure AP profile to use 802.1x authentication that the user needs to log in with their ID and Password when connecting to AP's SSID. Go to **CONFIGURATION > Object > AP Profile > SSID > Security List**, click **Add** to add security for 802.1x.

In **General Settings**, enter the **Profile Name** and change **Security Mode** to **wpa2**.

In **Radius Settings**, select to **Internal** and it means the authentication needs NXC to communicate with an external AD server.

In **Authentication Settings**, select to **802.1x** and **Auth. Method** is **default**. Click **OK**.

General Settings	
Profile Name:	ADtest
Security Mode:	wpa2
Fast Roaming Settings	
<input type="checkbox"/> 802.11r	
Radius Settings	
Radius Server Type:	Internal
MAC Authentication Setting	
<input type="checkbox"/> MAC Authentication	
Auth. Method:	default
Delimiter (Account):	colon (:)
Case (Account):	upper
Delimiter (Calling Station ID):	colon (:)
Case (Calling Station ID):	upper
<input type="checkbox"/> Fallback to Captive Portal after MAC authentication failure	
Authentication Settings	
<input checked="" type="radio"/> 802.1x	
Auth. Method:	default
ReAuthentication Timer:	0 (30~30000 seconds, 0 is unlimited)

- Go to **CONFIGURATION > Object > AP Profile > SSID > SSID List**, click **add** to add a SSID for the connection with 802.1x security. Key in the **Profile Name** and **SSID**, and change **Security Profile** to **ADtest** which you configured in step1. Click **OK** to save.

+ Add SSID Profile

Create new Object ▾

Profile Name:

SSID:

Security Profile:

- Go to **CONFIGURATION > Wireless > AP Management > AP Group**, select the **default** AP profile and edit. Select **ADtest** in the SSID Profile. Click **OK** to apply the SSID to AP.

Radio 1 Setting

OP Mode AP Mode MON Mode Root AP Repeater AP 1

Radio 1 AP Profile:

Max Output Power: dBm (0~30)

Edit

#	SSID Profile
1	ADtest
2	disable
3	disable
4	disable
5	disable
6	disable
7	disable
8	disable

Radio 2 Setting

OP Mode AP Mode MON Mode Root AP Repeater AP 1

Radio 2 AP Profile:

Max Output Power: dBm (0~30)

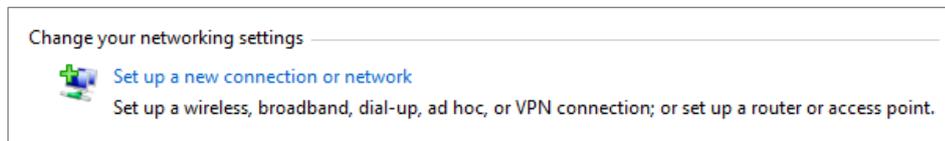
Edit

#	SSID Profile
1	ADtest

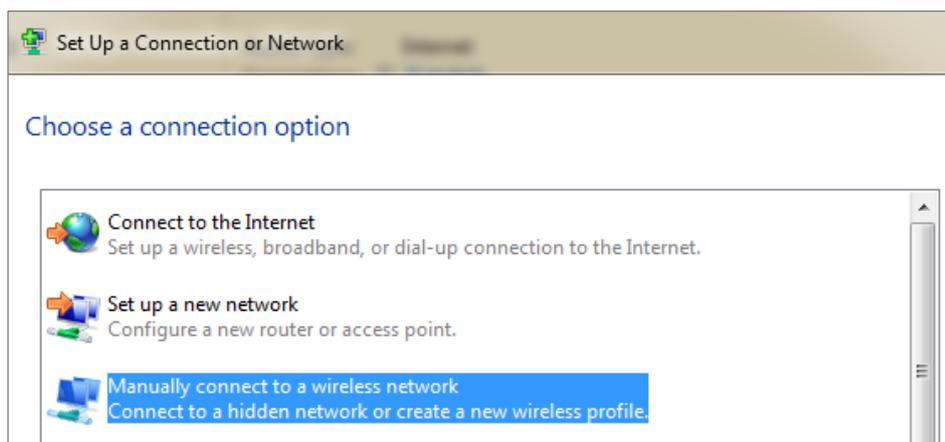
4.2.3 Test the Result

- 1 Before connecting the SSID, the computer needs to do some settings to make a connection successfully. Here is an example for Windows 7.

Open **Network and Sharing Center** in the computer, click **Set up a new connection or network** to build up a new network.



- 2 Select **Manually connect to a wireless network**. Click **Next**.



- 3 Key in the SSID in **Network name**, set the **Security type** to **WPA2-Enterprise**, and the **Encryption type** is **AES**. Click **Next**.

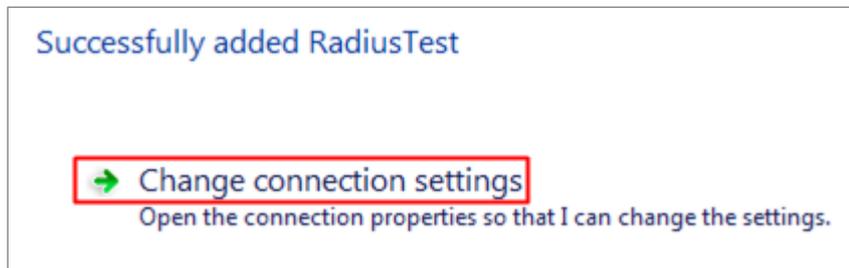
Enter information for the wireless network you want to add

Network name:

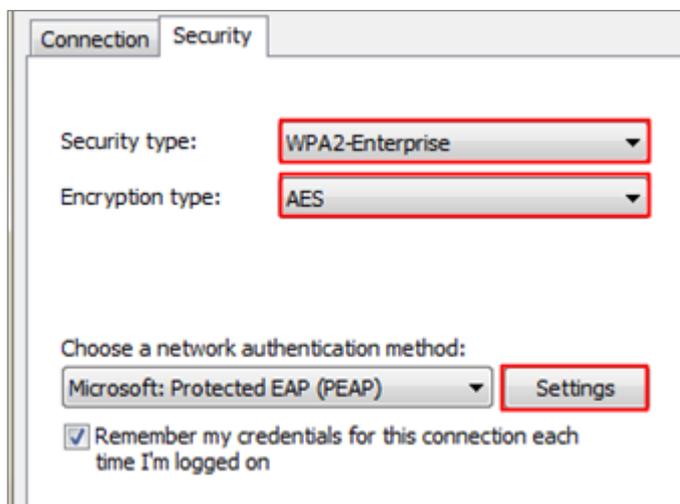
Security type:

Encryption type:

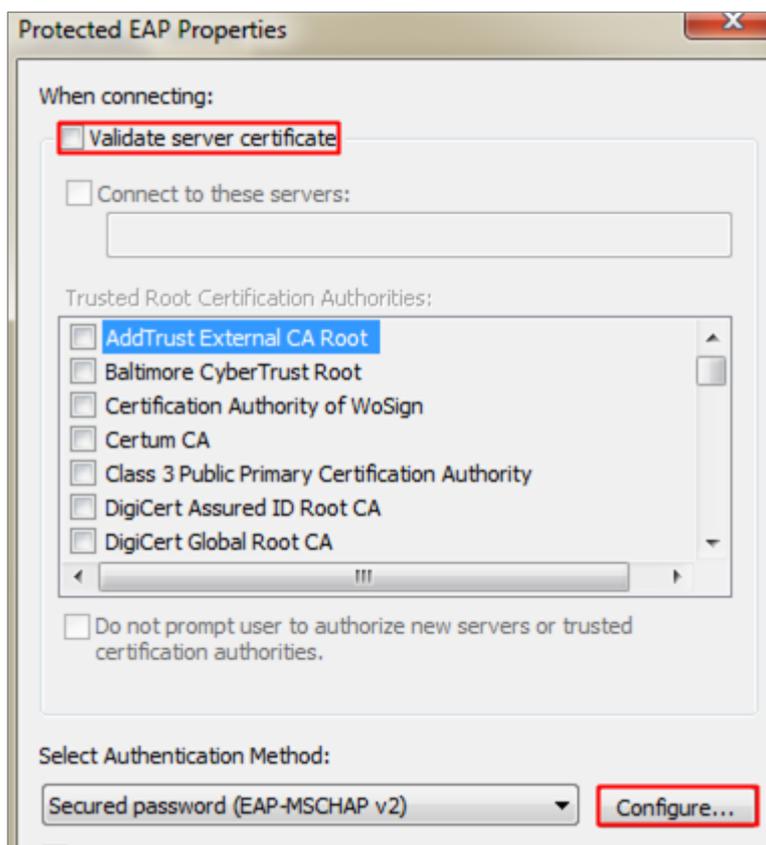
4 Select **Change connection settings**.



5 Change **Security type** to **WPA2-Enterprise**, and **Encryption type** is **AES**. Click **Settings**.



6 Uncheck **Validate server certificate** and click **Configure**.



7 Uncheck the selection of the pop-up window. Click **OK**.



- Go back to the security setting page and click **Advanced settings**.

Connection Security

Security type: WPA2-Enterprise

Encryption type: AES

Choose a network authentication method:

Microsoft: Protected EAP (PEAP) Settings

Remember my credentials for this connection each time I'm logged on

Advanced settings

- Check **Specify authentication mode**. Click **OK** to save.

802.1X settings 802.11 settings

Specify authentication mode

User or computer authentication Save credentials

Delete credentials for all users

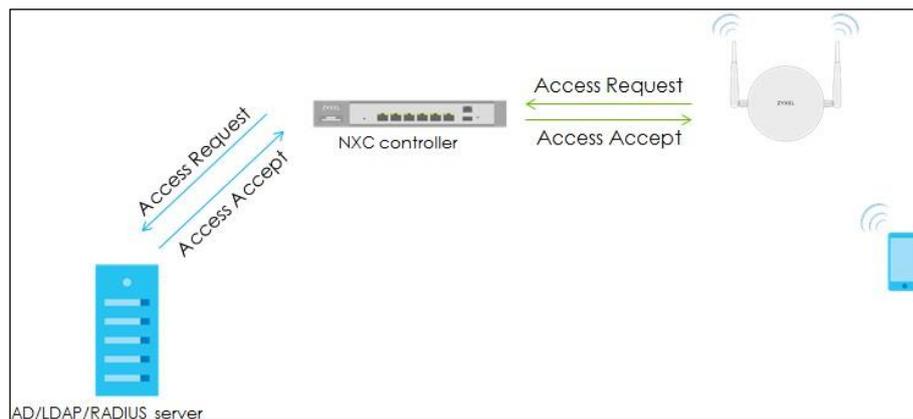
- 10 Select and connect to the pre-defined SSID "ADTest". Enter user credentials for authentication. After entering the correct ID and password, the wireless connection is set up successfully.

Network Authentication
Please enter user credentials



4.2.4 What Could Go Wrong

- 1 There are two kinds of **Radius Server Types** in security profile setting. **Internal** means the authentication is doing between the NXC controller and the AD server.



- 2 When the **Radius Server Types** change to **External**, it means the authentication is doing between the Managed AP and the Radius server. However, the AD server does not support EAP protocol, so it's necessary to install IAS or NPS on the AD server for EAP protocol.

4.3 How to Configure 802.1x to Secure the Wireless Environment with an External LDAP Server?

The example instructs how to set up the NXC controller with an external LDAP server. When the station wants to connect with the AP, you can use an AAA server to provide access control to your network. In this example, the LDAP server is external but not embedded in NXC controller, and the controller is already set to use the LDAP server for authentication.

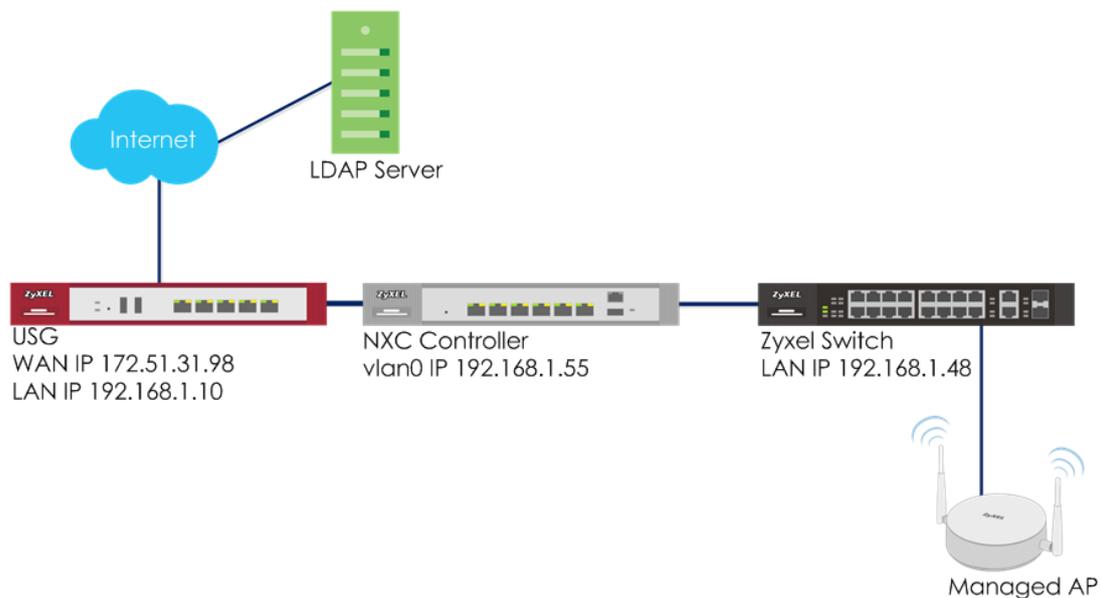


Figure 4.3 Set up AP/NXC with an External LDAP Server



Note:

All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC5500 (Firmware Version: 5.40), GS2210-8HP (Firmware Version: V4.30).

4.3.1 Configure LDAP Server Setting

- 1 Go to **CONFIGURATION > Object > AAA Server > LDAP**, click **#1 Idap**, and then click **Edit** to edit the LDAP server's information.
- 2 In **Server Settings**, enter **Server Address**. Here use **10.253.31.239** as the example. Go to LDAP server to check Base DN and Bind DN.

Edit LDAP Idap

General Settings

Name: (Optional)

Description: (Optional)

Server Settings

Server Address: (IP or FQDN)

Backup Server Address: (IP or FQDN) (Optional)

Port: (1-65535)

Base DN:

Use SSL

Search time limit: (1-300 seconds)

Case-sensitive User Names i

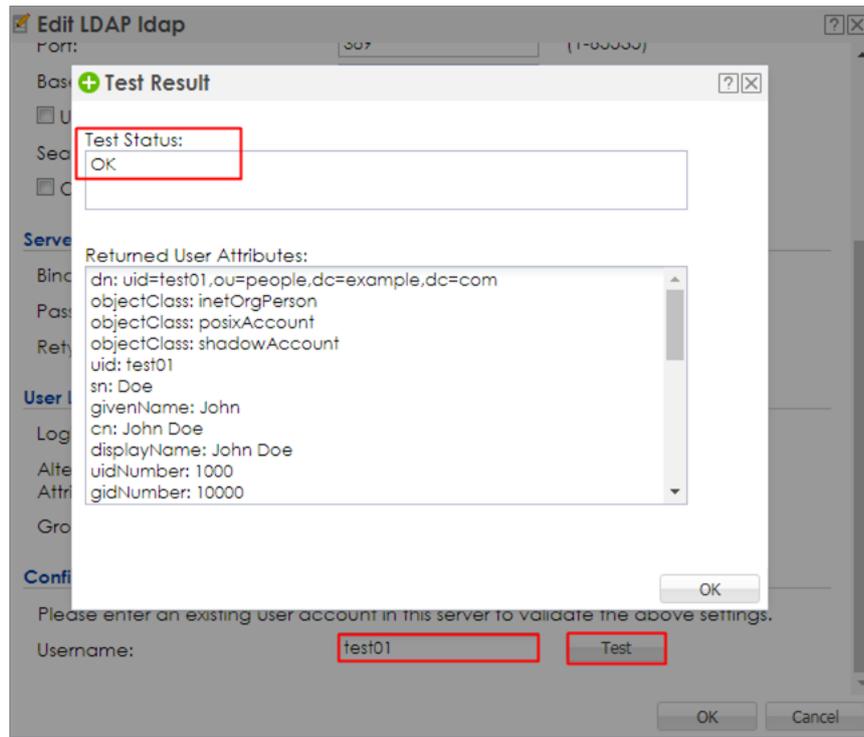
Server Authentication

Bind DN:

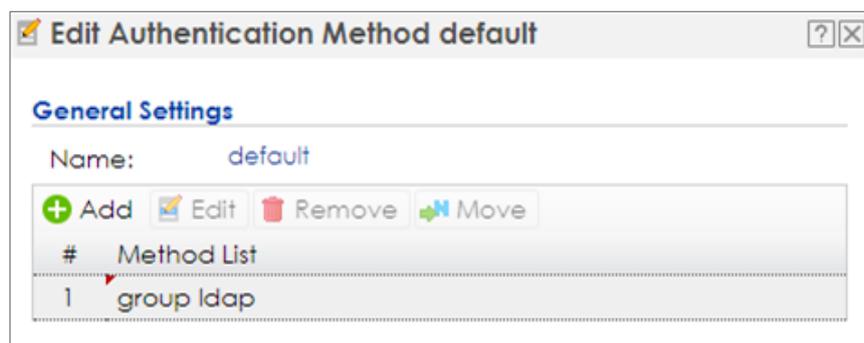
Password:

Retype to Confirm:

- 3 After finishing the configuration, enter **administrator** as the **Username** and click **Test** in **Configuration Validation**.



- 4 Go to **CONFIGURATION > Object > Auth. Method**. Select default method, and click **Edit**. Select the LDAP server you create. Click **OK**.



4.3.2 Configure AP Profile

- 1 Configure AP profile to use 802.1x authentication that user needs to log in with their ID and Password when connecting to AP's SSID. Go to **CONFIGURATION > Object > AP Profile > SSID > Security List**, click **Add** to add security for 802.1x.

In **General Settings**, enter the **Profile Name** and change **Security Mode** to **wpa2**.

In **Radius Settings**, select **Internal** and it means the authentication needs NXC to communicate with external LDAP server.

In **Authentication Settings**, select **802.1x** and **Auth. Method** is **default**. Click **OK**.

The screenshot shows the 'Add Security Profile' configuration window. The 'General Settings' section has 'Profile Name' set to 'LDAPtest' and 'Security Mode' set to 'wpa2'. The 'Fast Roaming Settings' section has '802.11r' checked. The 'Radius Settings' section has 'Radius Server Type' set to 'Internal'. The 'MAC Authentication Setting' section has 'MAC Authentication' checked, with 'Auth. Method' set to 'default', 'Delimiter (Account)' set to 'colon (:)', 'Case (Account)' set to 'upper', 'Delimiter (Calling Station ID)' set to 'colon (:)', and 'Case (Calling Station ID)' set to 'upper'. The 'Authentication Settings' section has '802.1X' selected, with 'Auth. Method' set to 'default' and 'ReAuthentication Timer' set to '0'. There are 'OK' and 'Cancel' buttons at the bottom right.

- 2 Go to **CONFIGURATION > Object > AP Profile > SSID > SSID List**, click **add** to add a SSID for the connection with 802.1x security. Key in the **Profile Name** and **SSID**, and change **Security Profile**

to **LDAP** which you configured in step 1. Click **OK** to save.

+ Add SSID Profile

Create new Object ▾

Profile Name:

SSID:

Security Profile: ▾

- Go to **CONFIGURATION > Wireless > AP Management > AP Group**, select the **default** AP profile and edit. Select **LDAPtest** in the SSID Profile. Click **Override Member AP Setting** to apply the SSID to the AP and click **Yes** in the pop-up window. Click **OK**.

Edit AP Group Profile default

Radio 1 Setting

OP Mode AP Mode MON Mode Root AP Repeater AP **i**

Radio 1 AP Profile: ▾

Max Output Power: dBm (0~30)

Edit

#	SSID Profile
1	LDAPtest
2	disable
3	disable
4	disable
5	disable
6	disable
7	disable
8	disable

Radio 2 Setting

OP Mode AP Mode MON Mode Root AP Repeater AP **i**

Radio 2 AP Profile: ▾

Max Output Power: dBm (0~30)

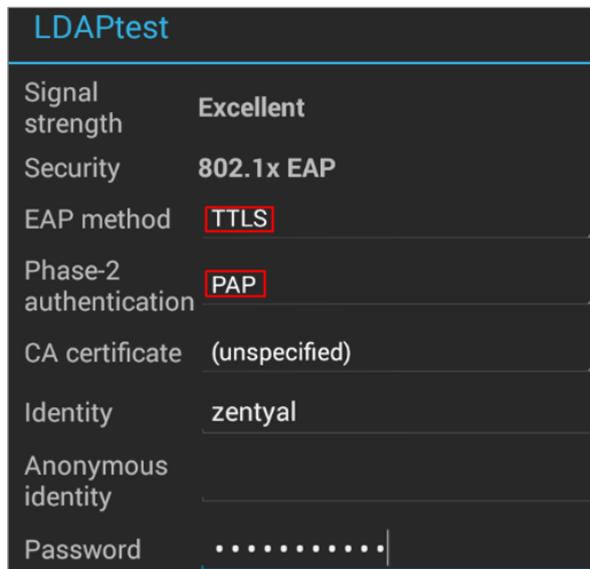
Edit

#	SSID Profile
1	LDAPtest
2	disable
3	disable
4	disable

OK Cancel Override Member AP setting

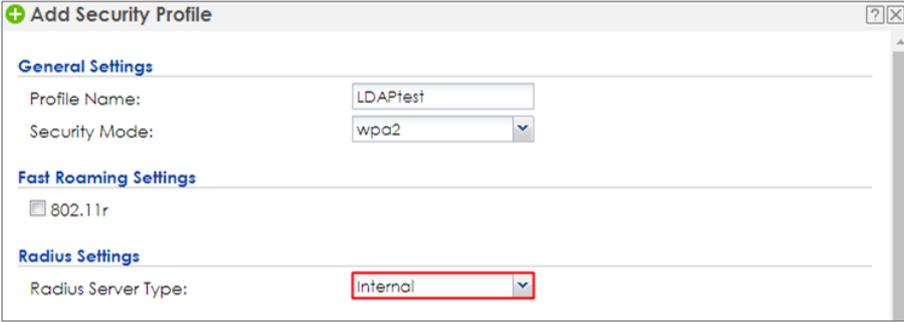
4.3.3 Test the Result

- 1 The LDAP can be use in Android phone for authentication. When connecting to the SSID, the **EAP method** is set to **TTLS**, and **Phase-2 authentication** is **PAP**. Enter the user ID and password to connect. The station and AP connected with correct ID and password.



4.3.4 What Could Go Wrong

- 1 The Radius server type is always **internal** in **CONFIGURATION > Object > AP Profile > SSID > Security List** because LDAP is not able to be used as the authentication server. It does not support **external** for LDAP server.



The screenshot shows a web-based configuration window titled "Add Security Profile". It is divided into three sections: "General Settings", "Fast Roaming Settings", and "Radius Settings".

- General Settings:** Profile Name is "LDAPtest" and Security Mode is "wpa2".
- Fast Roaming Settings:** The "802.11r" checkbox is unchecked.
- Radius Settings:** The Radius Server Type is set to "Internal", which is highlighted with a red rectangular box.

4.4 How to Configure 802.1x to Secure the Wireless Environment with an Internal RADIUS in NXC?

The example instructs how to set up NXC controller and let users do local authentication without external radius server. The user data base is set up in the NXC controller and the client can enter the username and password to do authentication via 802.1x.

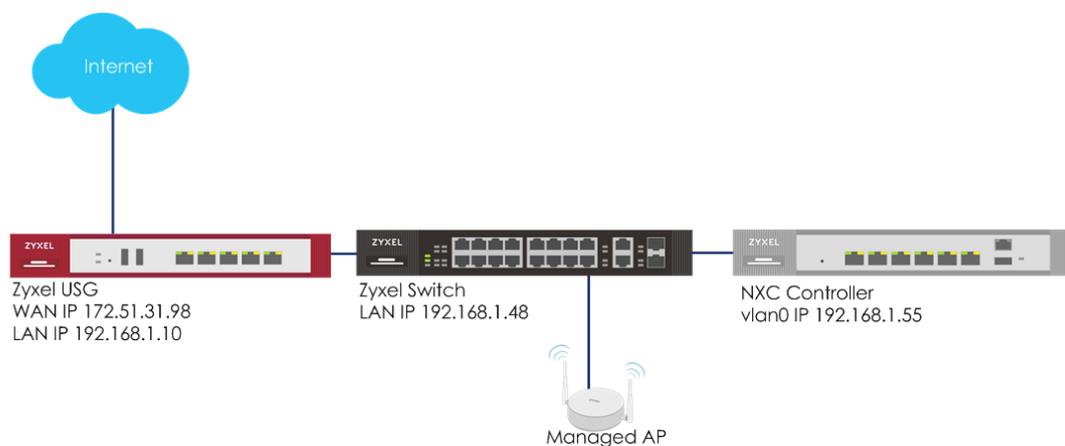


Figure 4.4 Local Authentication



Note:

All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC2500 (Firmware Version: 5.30), GS2210-8HP (Firmware Version: V4.30).

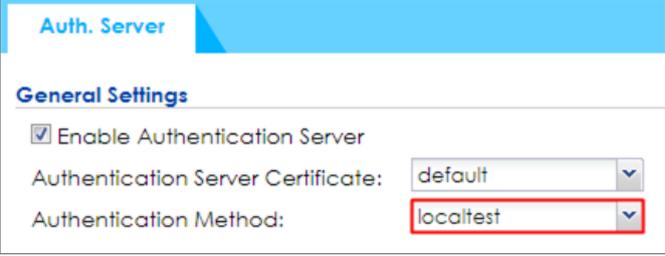
4.4.1 Configure Authentication Method Setting

- 1 Go to **CONFIGURATION > Object > User/Group**, and click **add** to create a new user ID and password. Stations can log in to connect with the AP to access the Internet via this account.

- 2 Go to **CONFIGURATION > Object > Auth. Method**, and click **add** to create an authentication method. Enter the **Name** of this authentication method and select to local in the **Method List**.

#	Method List
1	local

- 3 Go to **CONFIGURATION > System > Auth. Server**, and set **Authentication Method** to **localtest** which is created in step 2.



The screenshot shows the 'Auth. Server' configuration page. Under the 'General Settings' section, the 'Enable Authentication Server' checkbox is checked. The 'Authentication Server Certificate' dropdown is set to 'default'. The 'Authentication Method' dropdown is set to 'localtest', which is highlighted with a red rectangular box.

4.4.2 Configure AP Profile

- 1 Configure the AP profile to use 802.1x authentication that user needs to log in with their ID and Password when connecting to the AP's SSID. Go to **CONFIGURATION > Object > AP Profile > SSID > Security List**, and click **Add** to add security for 802.1x.

In **General Settings**, enter the **Profile Name** and change **Security Mode** to **wpa2**.

In **Radius Settings**, select to **Internal** and it means the authentication needs NXC to communicate with external LDAP server.

In **Authentication Settings**, select **802.1x** and **Auth. Method** is **localtest**. Click **OK**.

Add Security Profile

General Settings

Profile Name: local802

Security Mode: wpa2

Fast Roaming Settings

802.11r

Radius Settings

Radius Server Type: Internal

MAC Authentication Setting

MAC Authentication

Auth. Method: default

Delimiter (Account): colon (:)

Case (Account): upper

Delimiter (Calling Station ID): colon (:)

Case (Calling Station ID): upper

Fallback to Captive Portal after MAC authentication failure

Authentication Settings

802.1X

Auth. Method: localtest

ReAuthentication Timer: 0 (30~30000 seconds, 0 is unlimited)

OK Cancel

- Go to **CONFIGURATION > Object > AP Profile > SSID > SSID List**, click **add** to add a SSID for the connection with 802.1x security. Key in the **Profile Name** and **SSID**, and change **Security Profile** to **local802** which is created in step1. Click **OK** to save.

+ Add SSID Profile

Create new Object ▾

Profile Name:

SSID:

Security Profile:

- Go to **CONFIGURATION > Wireless > AP Management > AP Group**, select the **default** AP profile and edit. Select **local802** in the SSID Profile. Click **Override Member AP Setting** to apply the SSID to the AP and click **Yes** in the pop-up window. Click **OK**.

Edit AP Group Profile default

Radio 1 Setting

OP Mode AP Mode MON Mode Root AP Repeater AP ⓘ

Radio 1 AP Profile:

Max Output Power: dBm (0~30)

Edit

#	SSID Profile
1	local802
2	disable
3	disable
4	disable
5	disable
6	disable
7	disable
8	disable

Radio 2 Setting

OP Mode AP Mode MON Mode Root AP Repeater AP ⓘ

Radio 2 AP Profile:

Max Output Power: dBm (0~30)

Edit

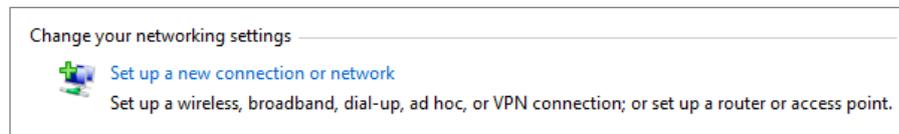
#	SSID Profile
1	local802
2	disable

OK Cancel **Override Member AP setting**

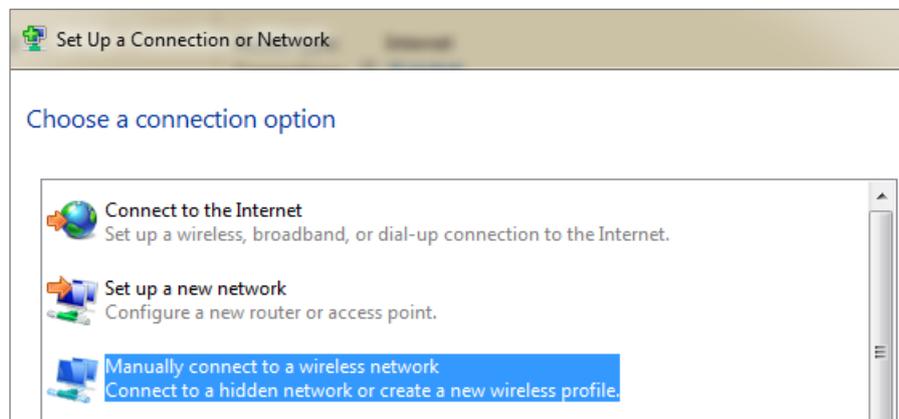
4.4.3 Test the Result

- 1 Before connecting the SSID, the computer needs to do some settings to make the connection successfully. Here is an example for Windows 7.

Opening **Network and Sharing Center** in computer, click **Set up a new connection or network** to build up a new network.



- 2 Select **Manually connect to a wireless network**. Click **Next**.



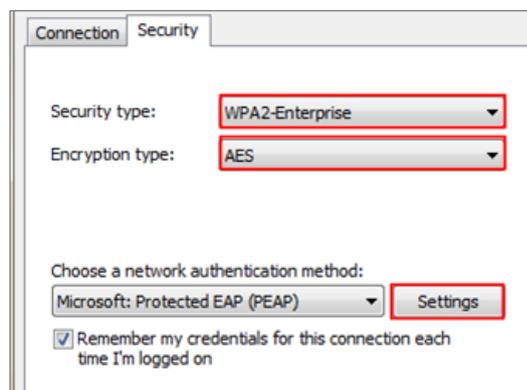
- 3 Key in the SSID to **Network name** and change the **Security type** to **WPA2-Enterprise**, and the **Encryption type** is **AES**. Click **Next**.

A screenshot of the 'Enter information for the wireless network you want to add' dialog box. It contains three fields: 'Network name:' with the value 'local802', 'Security type:' with a dropdown menu showing 'WPA2-Enterprise', and 'Encryption type:' with a dropdown menu showing 'AES'.

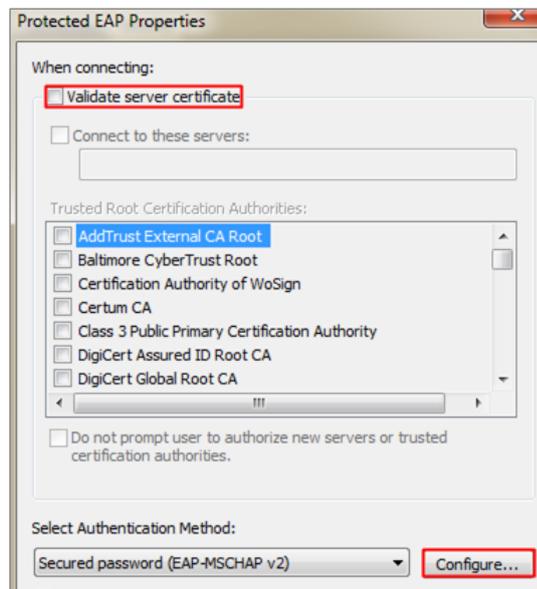
4 Select **Change connection settings**.



5 Select **Security type** to **WPA2-Enterprise**, and **Encryption type** is **AES**. Click **Settings**.



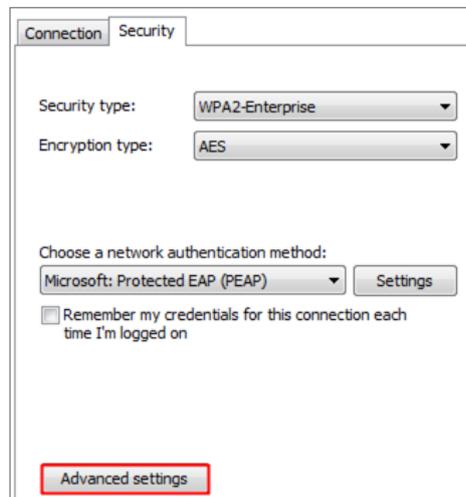
6 Uncheck **Validate server certificate** and click **Configure**.



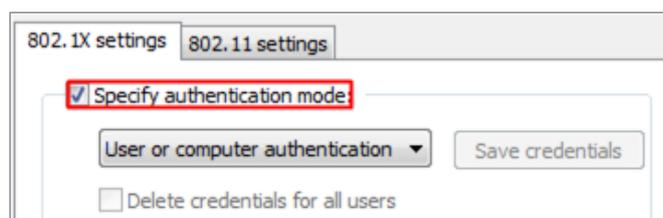
- 7 Uncheck the selection of pop-up window. Click **OK**.



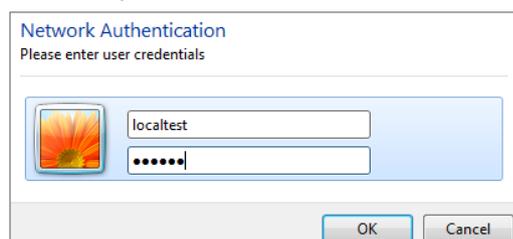
- 8 Go back to the security setting page and click **Advanced settings**.



- 9 Check **Specify authentication mode**. Click **OK** to save.



- 10 Select and connect to the pre-defined SSID "ADTest". Enter user credentials for authentication. After entering the correct ID and password, the wireless connection is set up successfully.



4.5 How to Configure 802.1x to secure the Wireless Environment with Dynamic VLAN by Using External AAA server?

When the station wants to connect with the AP, you can use an AAA server to provide access control to your network. In this example, assuming there are two stations in different groups and they can connect to the same SSID for accessing the Internet, but get IPs in different subnets because of the dynamic VLAN settings.

There are two ways for dynamic VLAN settings. One is to use the radius server attribute, and the other is to use the NXC controller external user group with radius or AD server. The example instructs how to set up dynamic VLAN by using external AAA servers with these two ways.

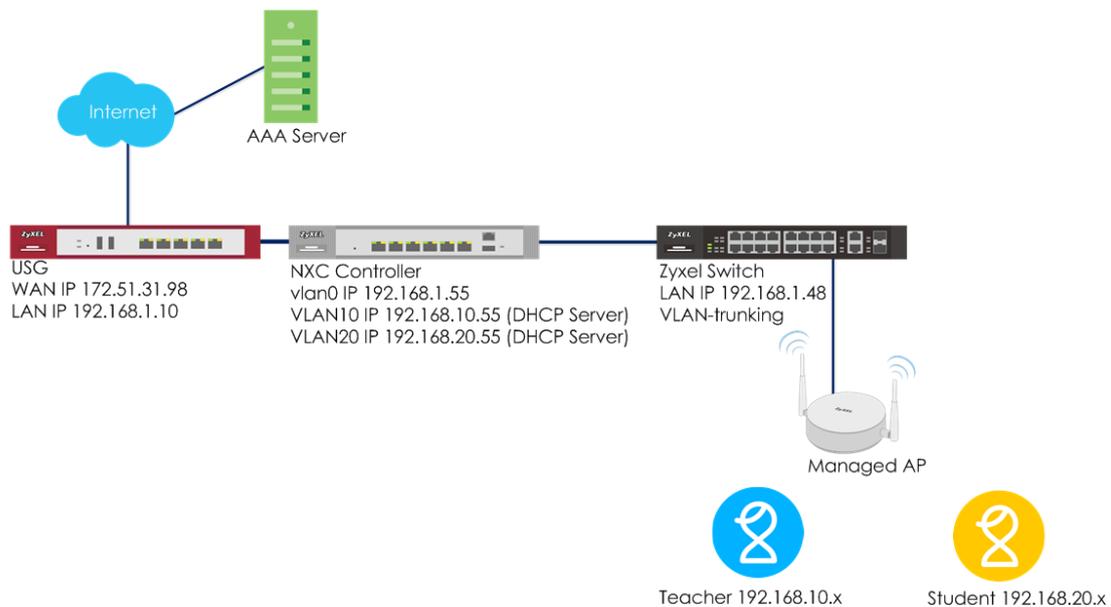


Figure 4.5 Dynamic VLAN with NXC controller using external Radius Server

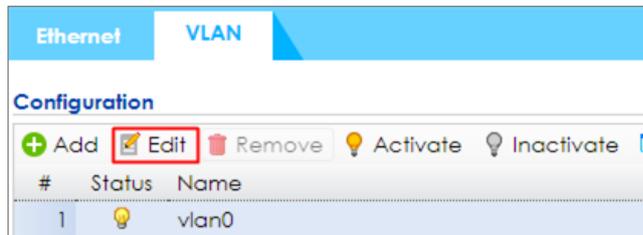


Note:

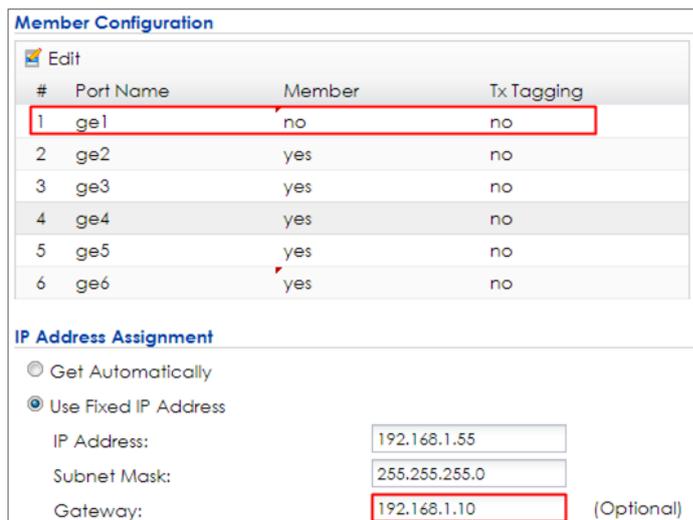
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC2500 (Firmware Version: 5.30), GS2210-8HP (Firmware Version: V4.30).

4.5.1 Configure Interface

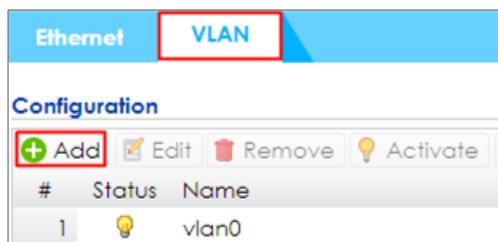
- 1 Go to **CONFIGURATION > Network > Interface > VLAN**, click **vlan0** and **Edit** it.



- 2 Set **ge1** (P1) to not be vlan0's member by selecting no in **Member Configuration**. Set the gateway IP in **IP Address Assignment**. Click **OK** to save. Connect ge1 (P1) to the USG's LAN port.



- 3 Connect Switch to NXC ge2 (P2), and APs all connect to the switch.
- 4 In the NXC, go to **CONFIGURATION > Network > Interface > VLAN**. Click **Add** to create a new VLAN configuration.



5 In General Settings, check **Enable**.

In Interface Properties, key in Interface Name: **vlan10**; VID: **10**

In Member Configuration, set ge2 to be **Member** and **Tx Tagging**.

In IP Address Assignment, **Use Fixed IP Address** and key in **IP Address, Subnet Mask, and Gateway**.

In DHCP Setting, select **DHCP server** and key in **IP Pool Start Address** and **Pool Size**. **First DNS server** change to **Customer Defined 8.8.8.8**. The users in VLAN 10 get an IP from this DHCP server. Click **OK**.

Interface Properties

Interface Name:

VID: (1~4094)

Zone:

Description: (Optional)

Member Configuration

#	Port Name	Member	Tx Tagging
1	ge1	no	no
2	ge2	yes	yes
3	ge3	no	no
4	ge4	no	no
5	ge5	no	no
6	ge6	no	no

IP Address Assignment

Get Automatically

Use Fixed IP Address

IP Address:

Subnet Mask:

Gateway: (Optional)

Metric: (0-15)

DHCP Setting

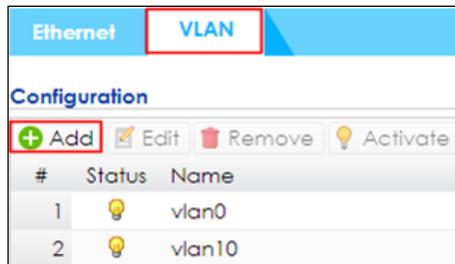
DHCP:

IP Pool Start Address (Optional): Pool Size:

First DNS Server (Optional):

OK Cancel

- Click **Add** to create vlan20 in **CONFIGURATION > Network > Interface > VLAN**.



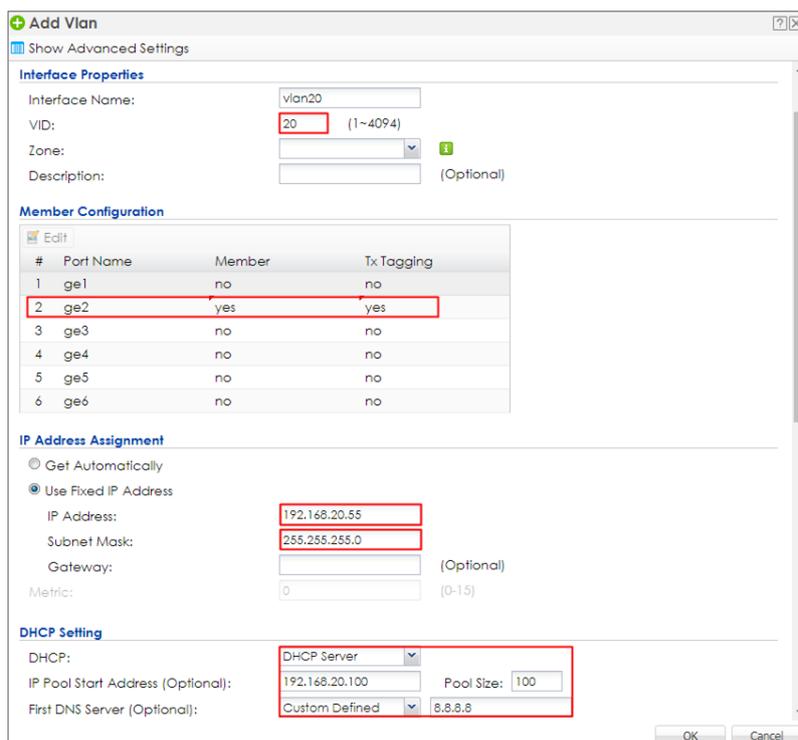
- In General Settings, check **Enable**.

In Interface Properties, key in Interface Name: **vlan20**; VID: **20**

In Member Configuration, set ge2 to be **Member** and **Tx Tagging**.

In IP Address Assignment, **Use Fixed IP Address** and key in **IP Address, Subnet Mask, and Gateway**.

In DHCP Setting, select **DHCP server** and key in **IP Pool Start Address** and **Pool Size**. **First DNS server** change to **Customer Defined 8.8.8.8**. The users in VLAN 20 get an IP from this DHCP server. Click **OK**.



- Go to **CONFIGURATION > Network > Interface > Ethernet**, select **ge1** and **Edit** it. Change the **Interface Type** to **external** and **Get Automatically** in **IP Address Assignment**.

Edit Ethernet

Show Advanced Settings

General Settings

Enable Interface

Interface Properties

Interface Type:	external	
Interface Name:	ge1	
Port:	P1	
PVID:	1 (1~4094)	
Zone:	none	
MAC Address:	4C:9E:FF	
Description:		(Optional)

IP Address Assignment

Get Automatically

Use Fixed IP Address

- 9 Go to **CONFIGURATION > Network > Routing > Policy Route** and click **Add** to add a policy route. Select **Interface ge1** in **Next-Hop**, and **outgoing-interface** in **Address Translation** after clicking **Show Advanced Settings**.

+ Add Policy Route [?] [X]

Hide Advanced Settings Create new Object ▾

Configuration

Enable

Description: (Optional)

Criteria

User: any ▾

Incoming: any (Excluding Ente ▾

Source Address: any ▾

Destination Address: any ▾

DSCP Code: any ▾

Schedule: none ▾

Service: any ▾

Source Port: any ▾

Next-Hop

Type: interface ▾

Interface: ge1 ▾

Auto-Disable

DSCP Marking

DSCP Marking: preserve ▾

Address Translation

Source Network Address Translation: outgoing-interface ▾

OK Cancel

4.5.2 Configure AP Profile

- 1 Configure the AP profile to use 802.1x authentication that the user needs to log in with their ID and Password when connecting to the AP's SSID. Go to **CONFIGURATION > Object > AP Profile > SSID > Security List**, select the **default** AP profile and edit.

In **General Settings**, enter the **Profile Name** and change **Security Mode** to **wpa2**.

In **Radius Settings**, change to **Internal** and it means the authentication needs NXC to communicate with external radius server.

In **Authentication Settings**, change to **802.1x** and **Auth. Method** is **default**. Click **OK**.

Edit Security Profile default

General Settings

Profile Name: default

Security Mode: wpa2

Fast Roaming Settings

802.11r

Radius Settings

Radius Server Type: internal

MAC Authentication Setting

MAC Authentication

Auth. Method: default

Delimiter (Account): dash (-)

Case (Account): upper

Delimiter (Calling Station ID): dash (-)

Case (Calling Station ID): upper

Fallback to Captive Portal after MAC authentication failure

Authentication Settings

802.1X

Auth. Method: default

ReAuthentication Timer: 0 (30~30000 seconds, 0 is unlimited)

OK Cancel

- Go to **CONFIGURATION > Object > AP Profile > SSID > SSID List**, and select the **default** AP profile and edit. Key in the **Profile Name** and **SSID**, and change **Security Profile** to **default** which is created in step1. Click **OK** to save.

Edit SSID Profile default

Create new Object ▾

Profile Name: default

SSID: DyVlan

Security Profile: default

MAC Filtering Profile: disable

Layer-2 Isolation Profile: disable

QoS: WMM

- Go to **CONFIGURATION > Wireless > AP Management > AP Group**, select the **default** AP profile and edit. Select **default** in the SSID Profile #1 in both radio1 and radio2. Click **OK** to apply the settings.

Edit AP Group Profile default

Radio 1 Setting

OP Mode AP Mode MON Mode Root AP Repeater AP ⓘ

Radio 1 AP Profile: default

Max Output Power: 30 dBm (0~30)

Radio 2 Setting

OP Mode AP Mode MON Mode Root AP Repeater AP ⓘ

Radio 2 AP Profile: default2

Max Output Power: 30 dBm (0~30)

Radio 1 SSID Profile List:

#	SSID Profile
1	default
2	disable
3	disable
4	disable
5	disable
6	disable
7	disable
8	disable

Radio 2 SSID Profile List:

#	SSID Profile
1	default
2	disable

OK Cancel Override Member AP setting

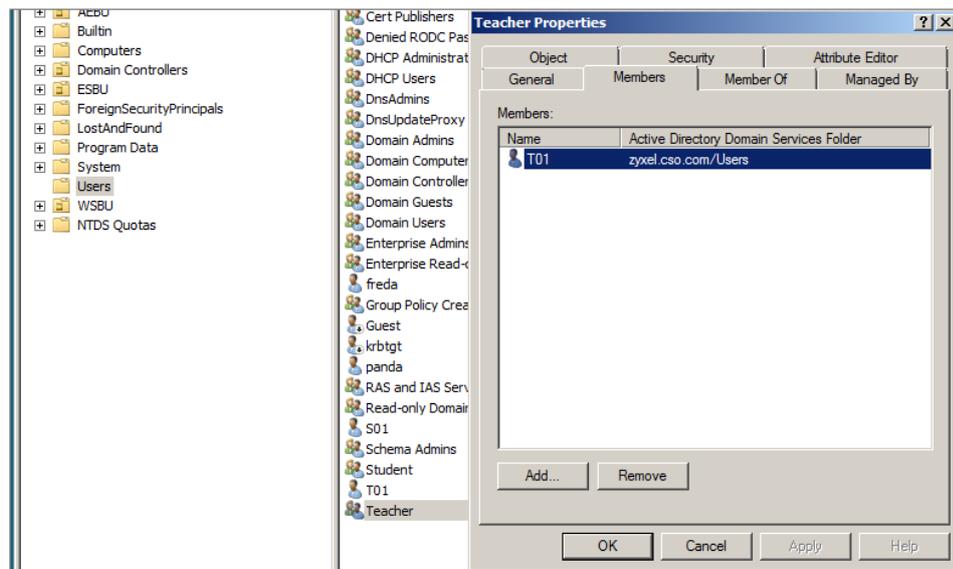
4.5.3 Configure AAA Server Setting

4.5.3.1 Dynamic VLAN by radius server attribute

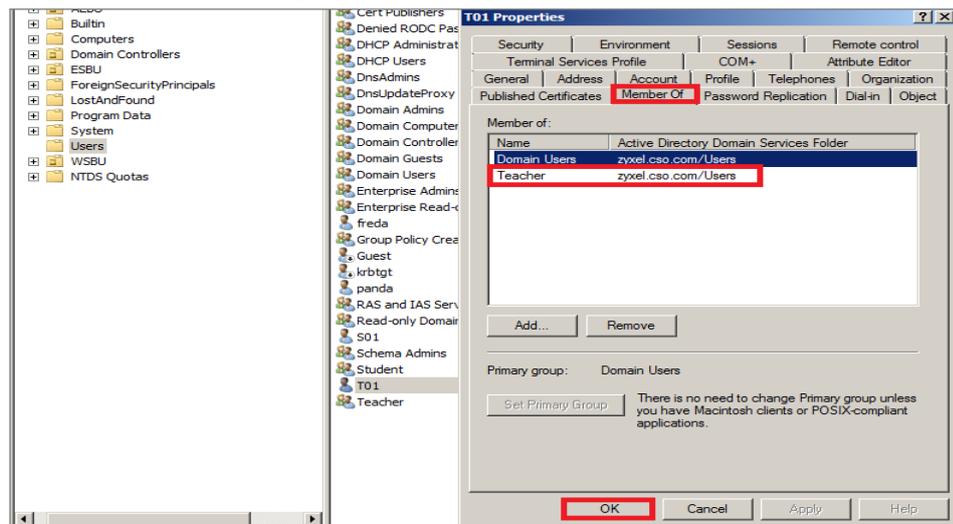
A. Settings on Radius Server

Here is an example by using Windows 2008 server with NPS and AD server.

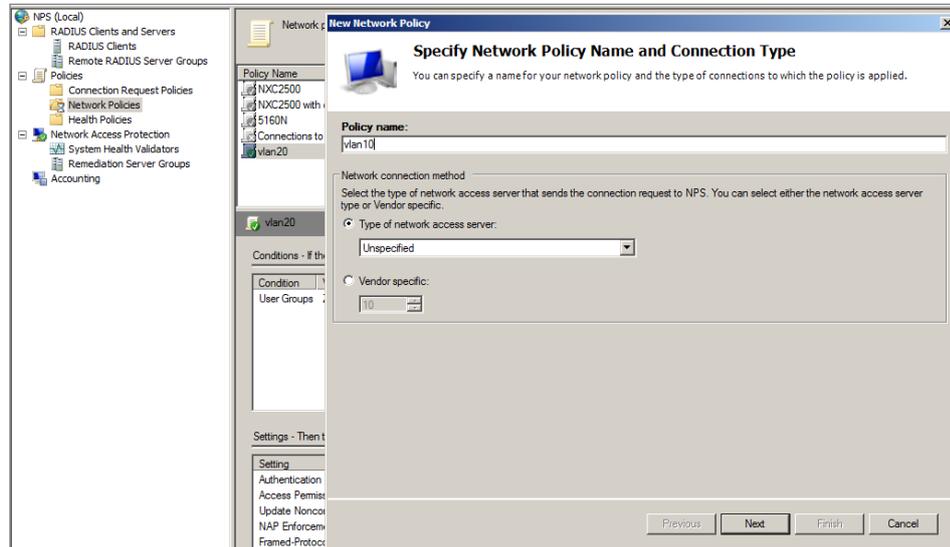
- 1 Add the user to a group in AD server.



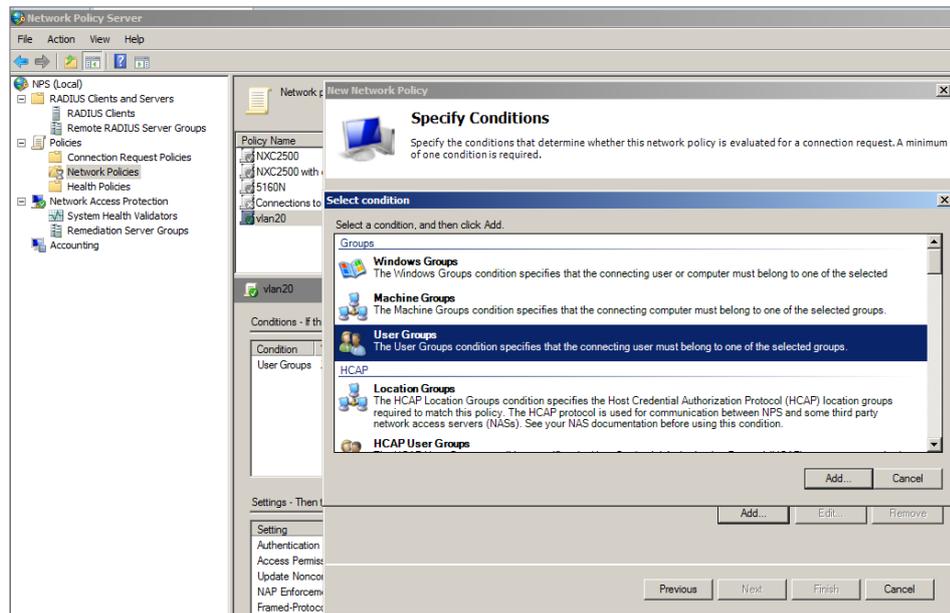
- 2 Go to **Member Of** to check if the member, **Teacher**, is added successfully in the group.



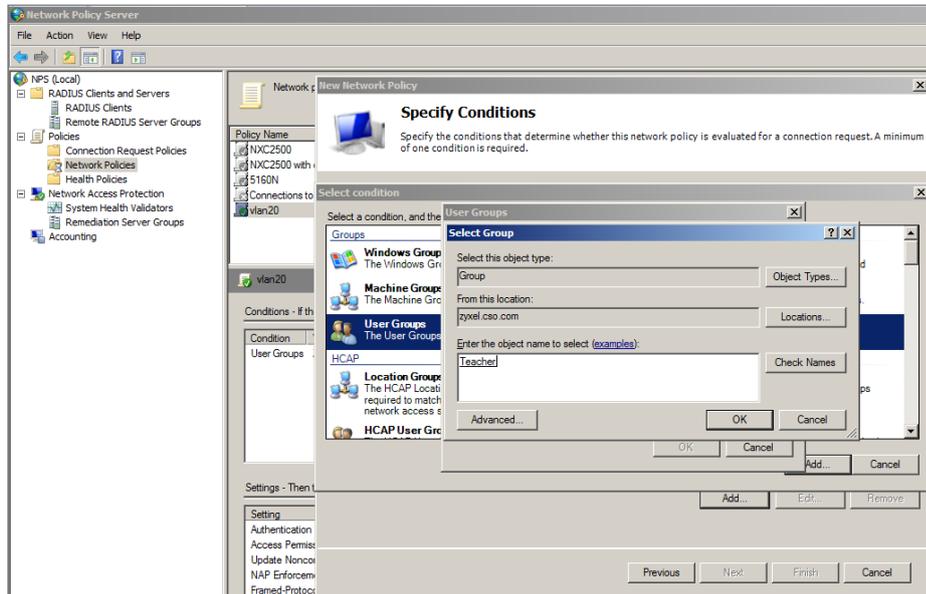
- 3 Add a new Network Policy of NPS server for a group and then click **'Next'**.



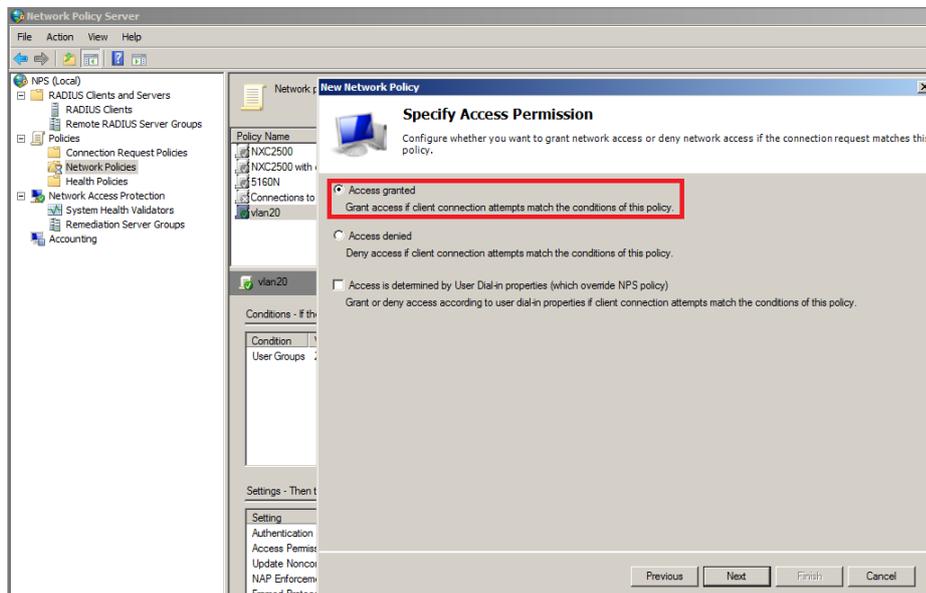
- 4 Add 'User Group' condition.



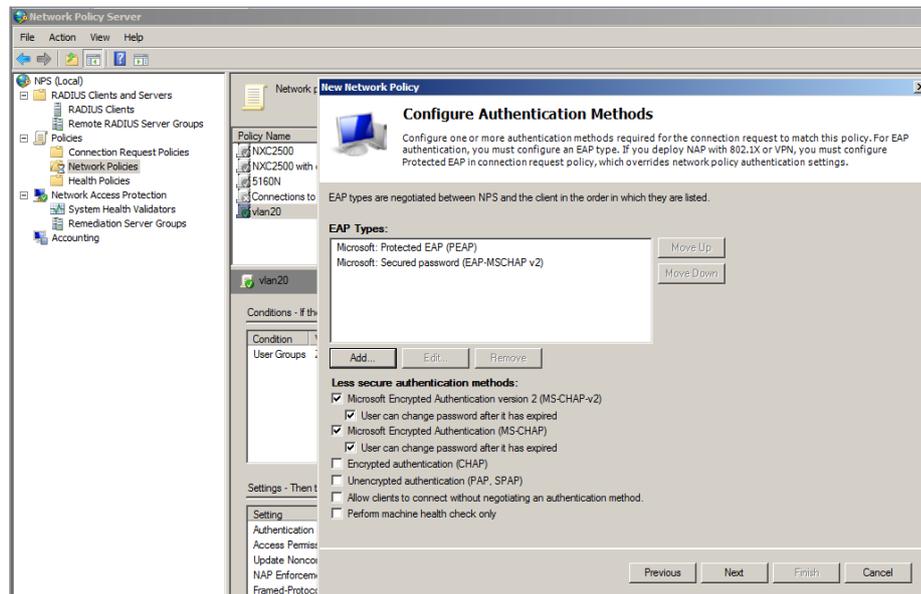
5 Select the group which is set in AD server.



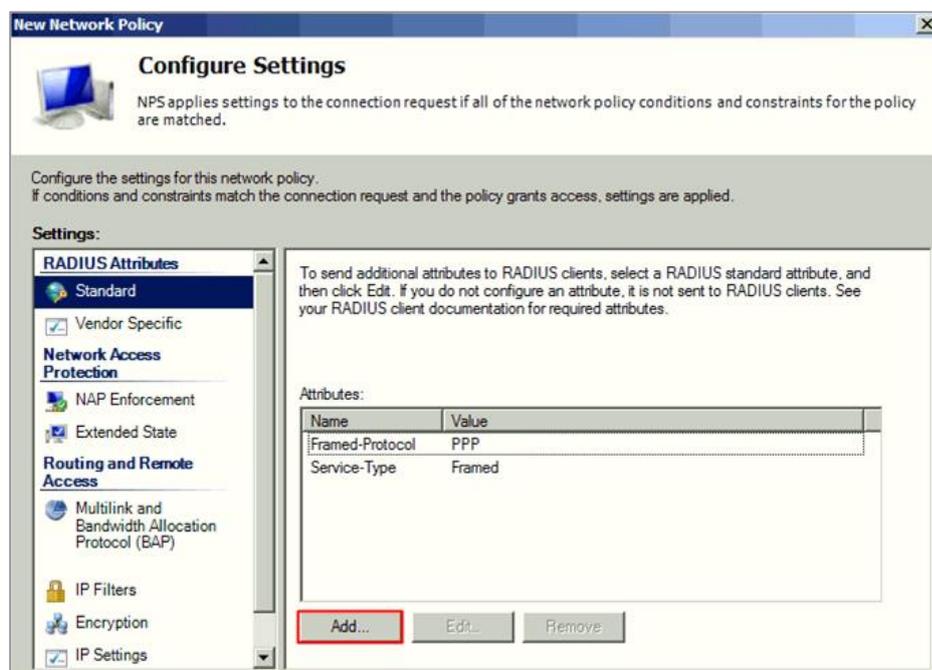
6 Set the access permission and click 'Next'.

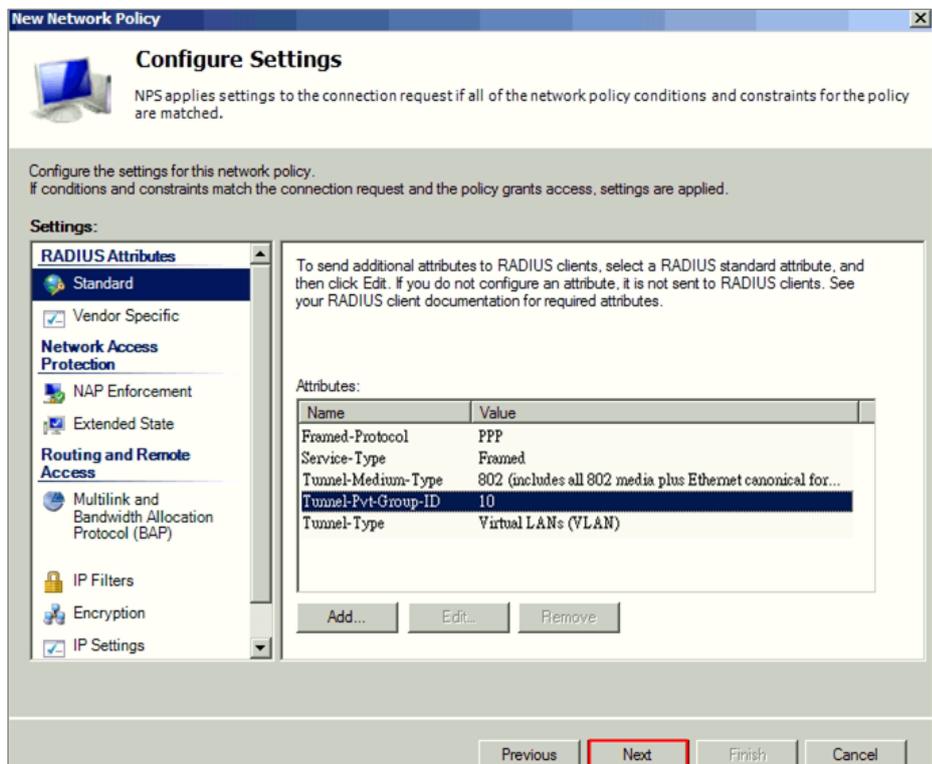
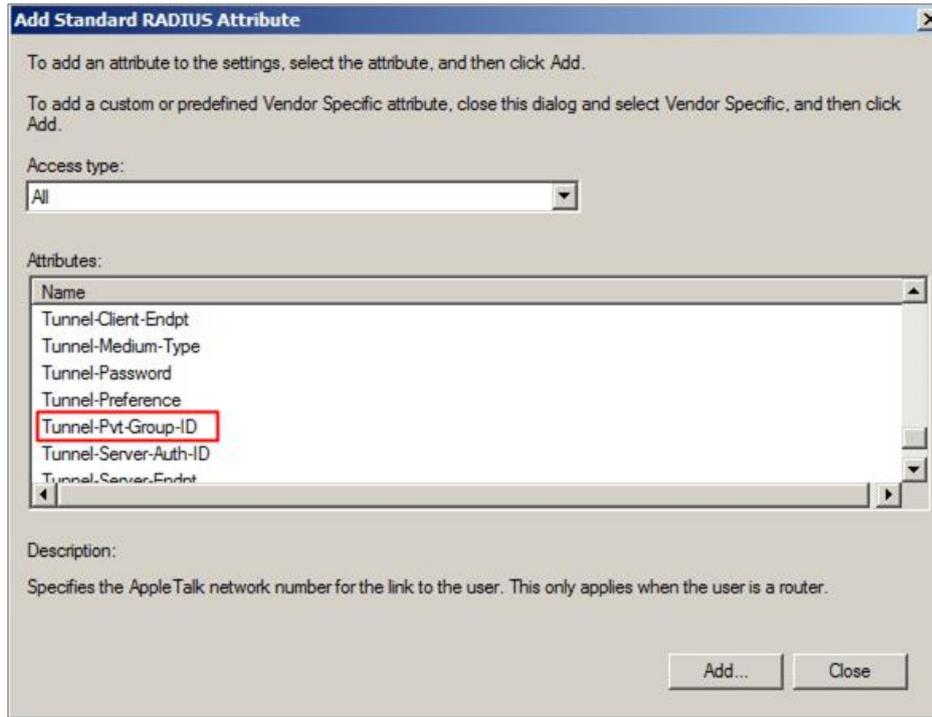


7 Configuration Authentication Methods and click 'Next'.

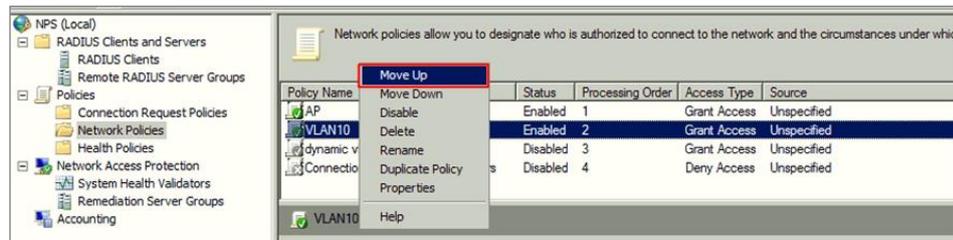


8 There are three attribute needed to add, Tunnel-Medium-Type, Tunnel-Pvt-Group-ID, Tunnel Type. Set the attribute configuration and click 'Next'.





- 9 Do the same steps to create the other group for other users.
- 10 Move up the policies to top in Network Policies of NPS to make sure it's the first one to hit when the traffic is come.



B. Settings on NXC Controller

- 1 Go to **CONFIGURATION > Object > AAA Server > RADIUS**, click **#1 radius**, and then click **Edit**. Set the **Server Address**, and **Authentication Port** is **1812**. Enter the **Key** for Radius server and click **OK**.

Edit RADIUS radius

General Settings

Name: radius

Description: (Optional)

Authentication Server Settings

Server Address: 172.51.31.111 (IP or FQDN)

Authentication Port: 1812 (1-65535)

Backup Server Address: (IP or FQDN) (Optional)

Backup Authentication Port: (1-65535) (Optional)

Key:

- 2 Go to **CONFIGURATION > Object > Auth. Method**, click **#1 default**, and then click **Edit**. Change the Method to **group radius**. Click **OK** to save.

Edit Authentication Method default

General Settings

Name: default

+ Add Edit Remove Move

#	Method List
1	group radius

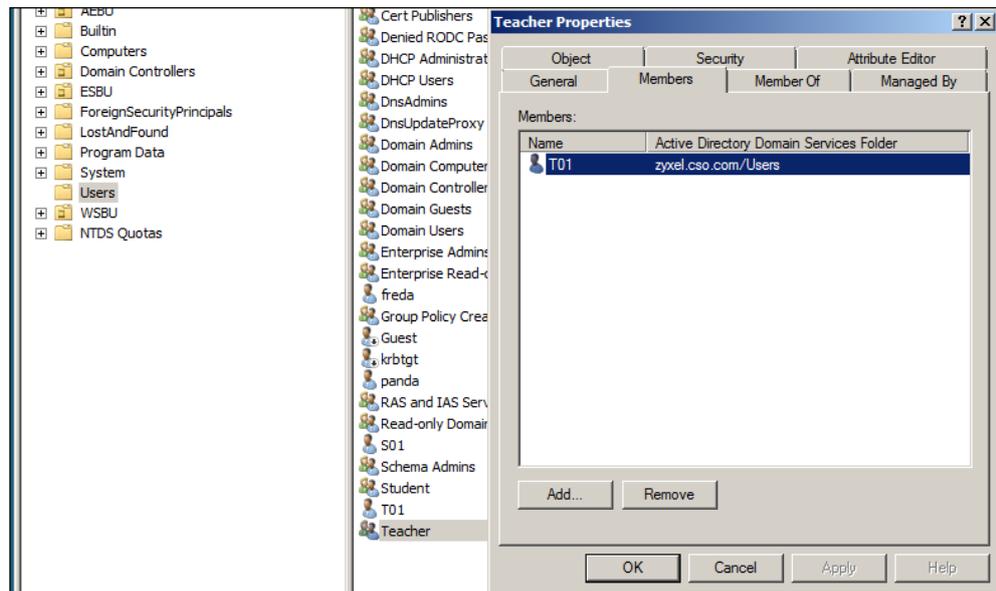
Topic: Dynamic VLAN by radius attribute

4.5.3.2 Dynamic VLAN by External User Group

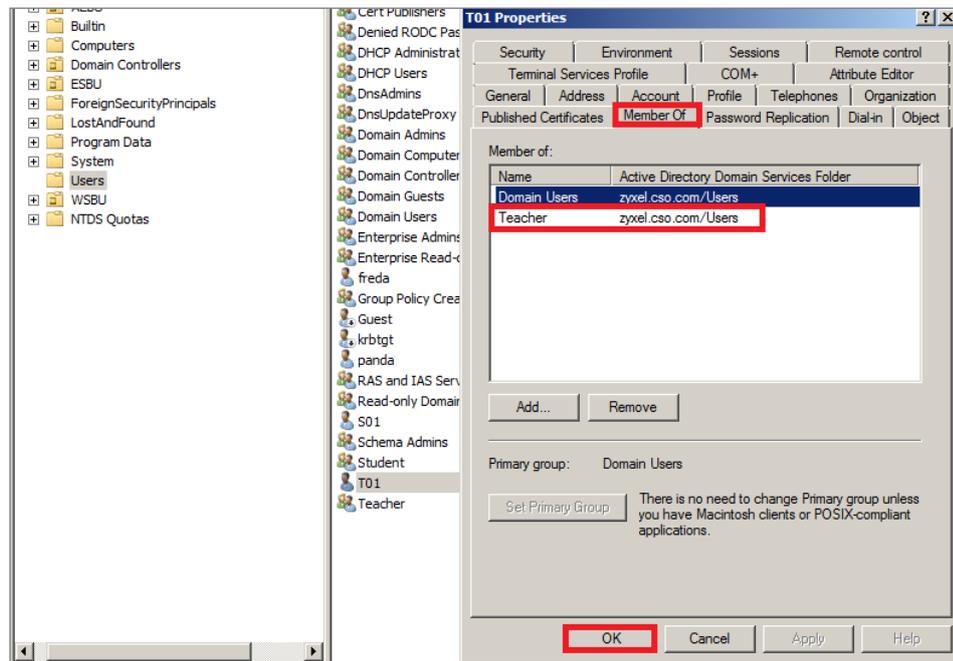
When users use dynamic VLAN by external user group, the radius and AD server are supported. Here are two examples for settings these two servers and NXC controller.

A. Settings on Radius/AD Server

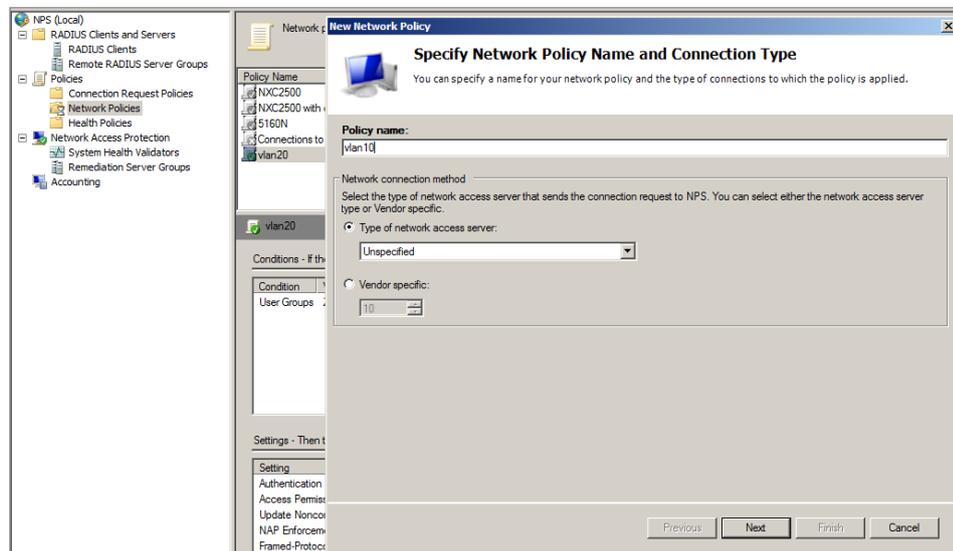
- 1 Add the user to a group in AD server.



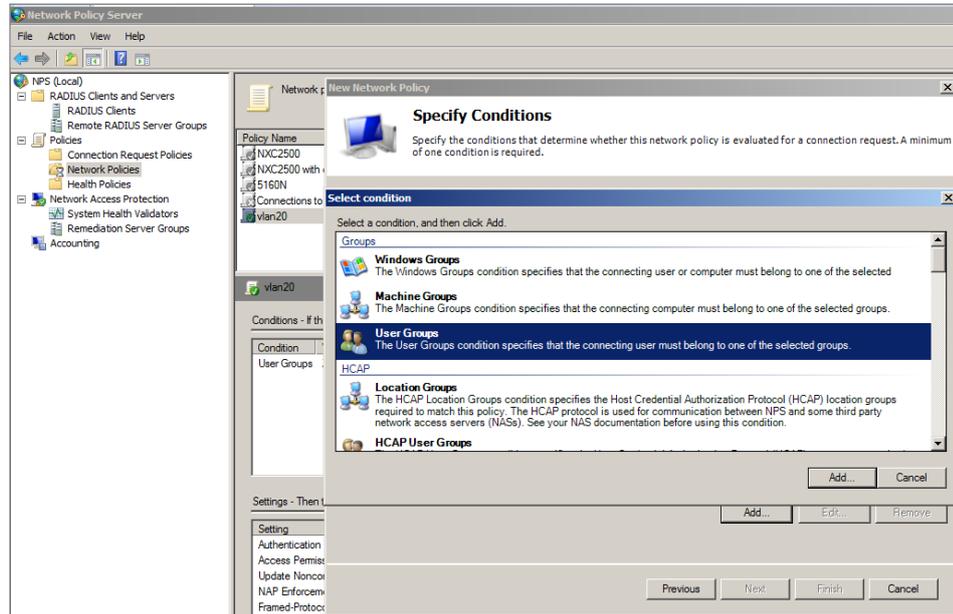
2 Check the user's properties about its group in Member Of.



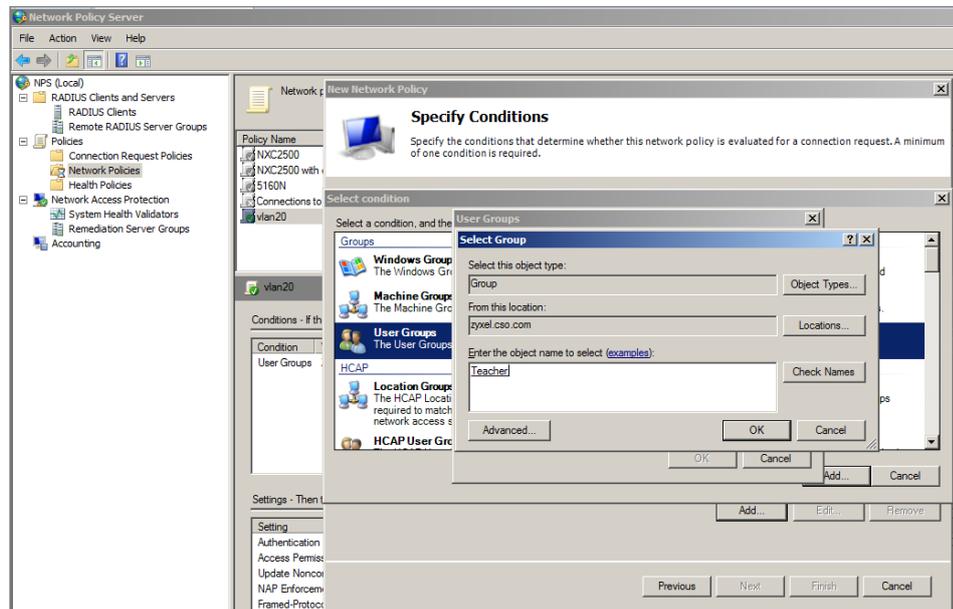
3 Add a new Network Policy of NPS server for a group and then click 'Next'.



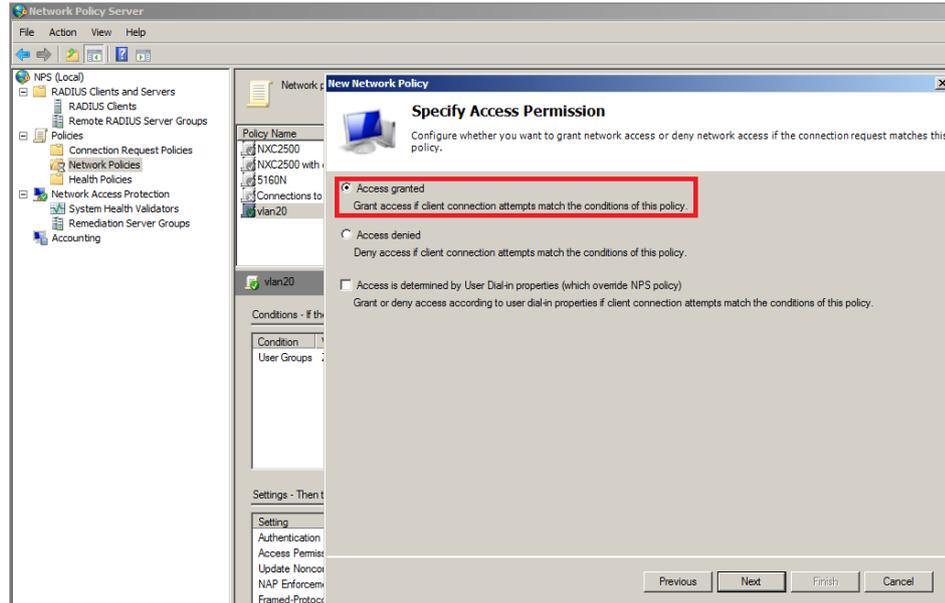
4 Add 'User Group' condition.



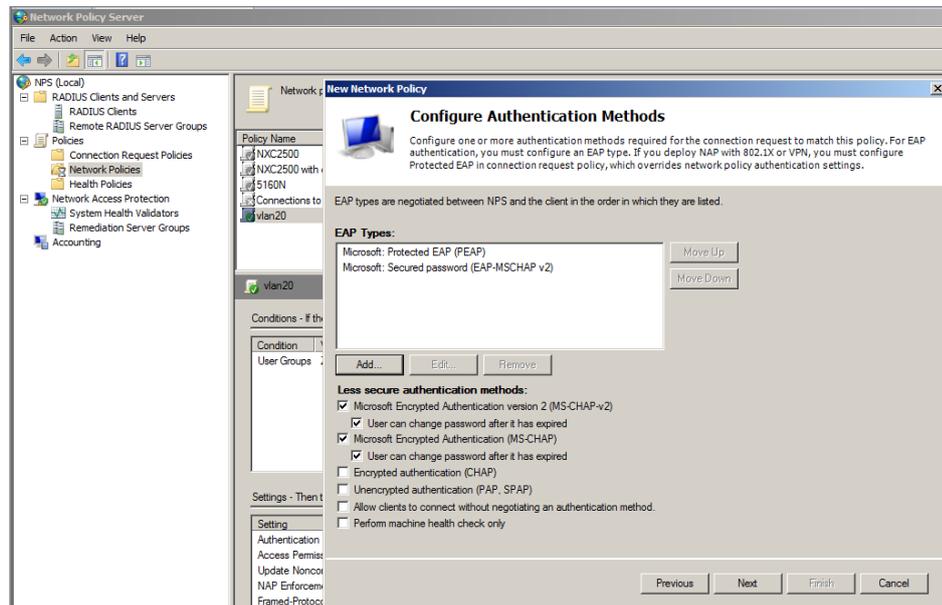
5 Select the group which is set in AD server.



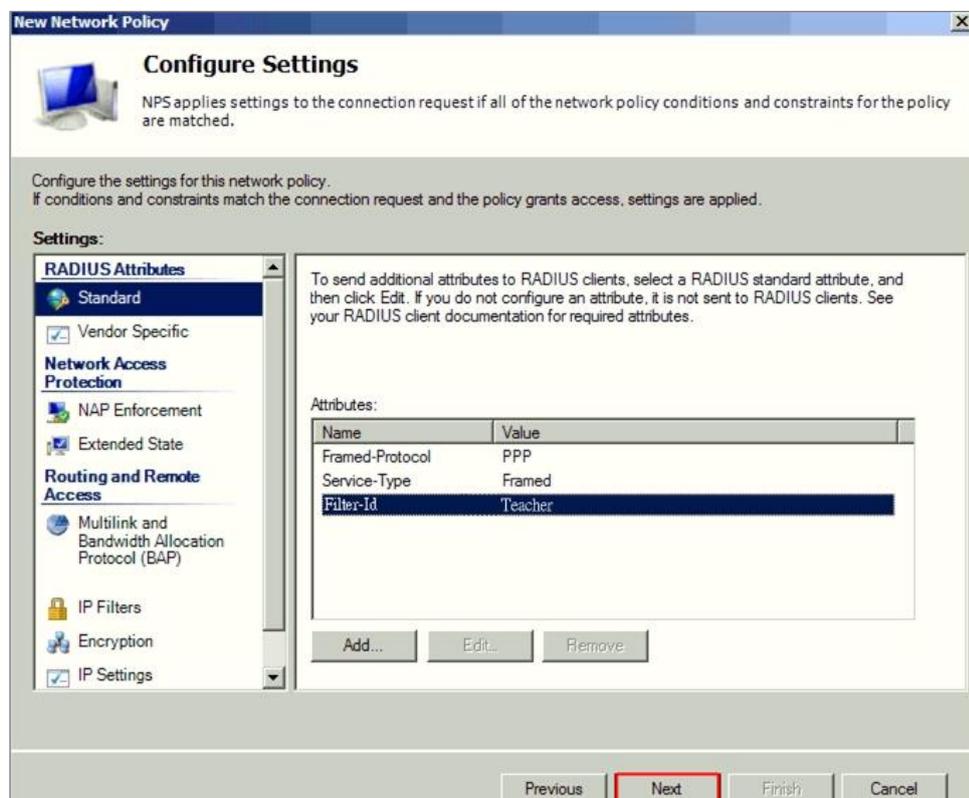
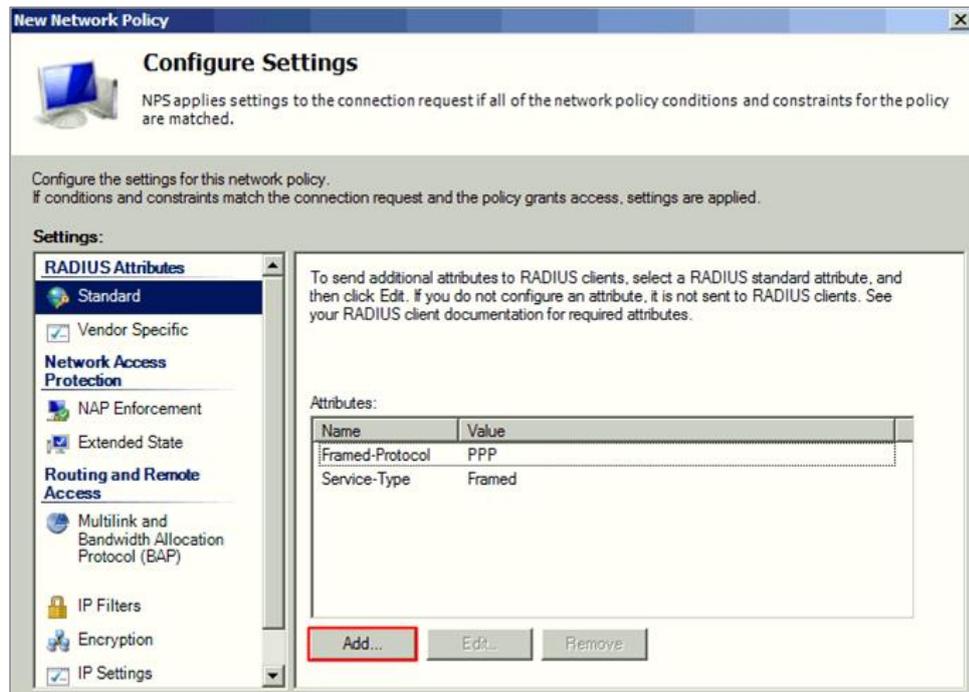
6 Set the access permission and click 'Next'.



7 Configuration Authentication Methods and click 'Next'.



- 8 There are three attribute needed to add Filter-ID as Teacher.



- 9 Do the same steps to create the other group for other users.

B. Settings on NXC Controller

b1. Using Radius Server

- 1 Go to **CONFIGURATION > Object > AAA Server > RADIUS**, click **#1 radius**, and then click **Edit**. Set the **Server Address**, and **Authentication Port** is **1812**. Enter the **Key** for Radius server and click **OK**.

Edit RADIUS radius

General Settings

Name: radius

Description: (Optional)

Authentication Server Settings

Server Address: 172.51.31.111 (IP or FQDN)

Authentication Port: 1812 (1-65535)

Backup Server Address: (IP or FQDN) (Optional)

Backup Authentication Port: (1-65535) (Optional)

Key: [redacted]

- 2 Go to **CONFIGURATION > Object > Auth. Method**, click **#1 default**, and then click **Edit**. Change the Method to **group radius**. Click **OK** to save.

Edit Authentication Method default

General Settings

Name: default

+ Add Edit Remove Move

#	Method List
1	group radius

3 Go to **Configuration > Object > User/Group > User > Add/Edit**

When user type is 'ext-group-user', set the corresponded value in 'Group Identifier' field, then enable and set the 'User VLAN ID' option.

User Configuration		
User Name :	Teacher	
User Type:	ext-group-user	
Group Identifier:	Teacher	
Associated AAA Server Object:	radius	
Description:	Local User	
Authentication Timeout Settings	<input checked="" type="radio"/> Use Default Settings <input type="radio"/> Use Manual Settings	
Lease Time:	1440	minutes
Reauthentication Time:	1440	minutes
<input checked="" type="checkbox"/> User VLAN ID:	10	(1~4094)

User Configuration		
User Name :	Student	
User Type:	ext-group-user	
Group Identifier:	Student	
Associated AAA Server Object:	radius	
Description:	Local User	
Authentication Timeout Settings	<input checked="" type="radio"/> Use Default Settings <input type="radio"/> Use Manual Settings	
Lease Time:	1440	minutes
Reauthentication Time:	1440	minutes
<input checked="" type="checkbox"/> User VLAN ID:	20	(1~4094)

b2. Using AD Server

- 1 Go to **CONFIGURATION > Object > AAA Server > Active Directory**, click **#1 ad**, and then click **Edit** to configure AD server's information.
- 2 In **Server Settings**, enter **Server Address**. Here use **172.51.31.112** as the example. Go to AD server to check Base DN. Here is an example for checking the Base DN on Windows server, and it can be copied from clicking right on the **domain name > properties > Attribute Editor > distinguished Name > View**.

Edit Active Directory ad		
General Settings		
Name:	ad	
Description:	<input type="text"/>	(Optional)
Server Settings		
Server Address:	<input type="text" value="172.51.31.112"/>	(IP or FQDN)
Backup Server Address:	<input type="text"/>	(IP or FQDN) (Optional)
Port:	<input type="text" value="389"/>	(1-65535)
Base DN:	<input "="" type="text" value="dc=zyxel,dc=com,dc="/>	

- 3 In **Server Authentication**, enter **Bind DN** and **Password**. You can check Bind DN in the AD server. In the AD server, clicking right on the Administrator > properties > Attribute Editor > distinguished Name > View. The Password is Administrator's password in the AD server.

Server Authentication	
Bind DN:	<input type="text" value="cn=test,cn=Users,dc=z"/>
Password:	<input type="password" value="••••"/>
Retype to Confirm:	<input type="password" value="••••"/>

- In **Domain Authentication for MSChap**, check **Enable** and enter the **User Name**, **User Password**, **Realm**, and **NetBIOS Name**.

The Realm is the domain name of the AD server.

- After finishing the configuration, enter **administrator** as the **Username** and click **Test** in **Configuration Validation**.

- Go to **CONFIGURATION > Object > Auth. Method**. Select to the default method, and click **Edit**. Select the AD server you create. Click **OK**.

7 Go to **Configuration > Object > User/Group > User > Add/Edit**.

When user type is 'ext-group-user', set the corresponded value in 'Group Identifier' field, then enable and set the 'User VLAN ID' option. There are two Filter-ID in radius server and the 'Group Identifier' of each ext-group-user is the same as the radius server's setting.

The **Group Identifier** is the distinguishedName of the group in AD server.

+ Add A User

User Configuration

User Name :

User Type:

Group Identifier:

Associated AAA Server Object:

Description:

Authentication Timeout Settings Use Default Settings Use Manual Settings

Lease Time: 1440 minutes

Reauthentication Time: 1440 minutes

User VLAN ID: (1~4094)

8 Setting the other ext-group-user for student group as the step 4.

4.5.4 Test the Result

4.5.4.1 Dynamic VLAN by radius server attribute

- 1 Use mobile phone to connect with SSID **DyVlan**. Enter the Username and Password which are in VLAN 10 group, and then click Join to connect with the AP.

Enter the password for "DyVlan"

Cancel Enter Password Join

Username T01

Password ●●●●●●●●

- 2 The logged-in client gets an IP in VLAN10.

< Wi-Fi DyVlan

Forget This Network

IP ADDRESS

DHCP BootP Static

IP Address 192.168.10.100

Subnet Mask 255.255.255.0

- 3 Use the mobile phone to connect with SSID **DyVlan**. Enter the Username and Password which is in VLAN 20 group, and then click Join to connect with the AP.

Cancel Enter Password Join

Username S01

Password ●●●●●●●●

- 4 The logged-in client gets an IP in VLAN20.

The screenshot shows the Wi-Fi settings for a network named "DyVlan". At the top, there is a back arrow and the text "Wi-Fi" and "DyVlan". Below this is a "Forget This Network" link. Under the heading "IP ADDRESS", there are three tabs: "DHCP" (which is selected and highlighted in blue), "BootP", and "Static". Below the tabs, the IP Address is displayed as 192.168.20.100 and the Subnet Mask is displayed as 255.255.255.0.

IP ADDRESS		
DHCP	BootP	Static
IP Address	192.168.20.100	
Subnet Mask	255.255.255.0	

4.5.4.2 Dynamic VLAN by External User Group

- 1 Use mobile phone to connect with SSID **DyVlan**. Enter the Username and Password which are in VLAN 10 group, and then click Join to connect with the AP.

Enter the password for "DyVlan"

Cancel **Enter Password** Join

Username T01

Password ●●●●●●●●

- 2 The logged-in client gets an IP in VLAN10.

< Wi-Fi **DyVlan**

Forget This Network

IP ADDRESS

DHCP
BootP
Static

IP Address 192.168.10.100

Subnet Mask 255.255.255.0

- 3 Use the mobile phone to connect with SSID **DyVlan**. Enter the Username and Password which is in VLAN 20 group, and then click Join to connect with the AP.

Cancel **Enter Password** Join

Username S01

Password ●●●●●●●●

- 4 The logged-in client gets an IP in VLAN20.

The screenshot shows the Wi-Fi settings for a network named "DyVlan". At the top, there is a back arrow and the text "Wi-Fi" and "DyVlan". Below this is a "Forget This Network" link. Under the heading "IP ADDRESS", there are three tabs: "DHCP" (which is selected and highlighted in blue), "BootP", and "Static". Below the tabs, the IP Address is listed as 192.168.20.100 and the Subnet Mask is listed as 255.255.255.0.

IP ADDRESS		
DHCP	BootP	Static
IP Address	192.168.20.100	
Subnet Mask	255.255.255.0	

4.5.5 What Could Go Wrong

- 1 When you set the dynamic VLAN in the NXC controller, the radius server needs to set the corresponding VLAN groups for authentication.
- 2 Because the dynamic VLAN setting is in the NXC controller, it only supports radius server type "**Internal**" in **CONFIGURATION > Object > AP Profile > SSID > Security List**.

4.6 How to Configure 802.1x EAP-TLS to Secure the Wireless Environment with Self-Signed Certificate?

This example shows how to use Android/iOS phone import the self-sign certificate from NXC to get the wireless connection with 802.1x EAP-TLS protected. We need a certificate which is generated by the NXC.

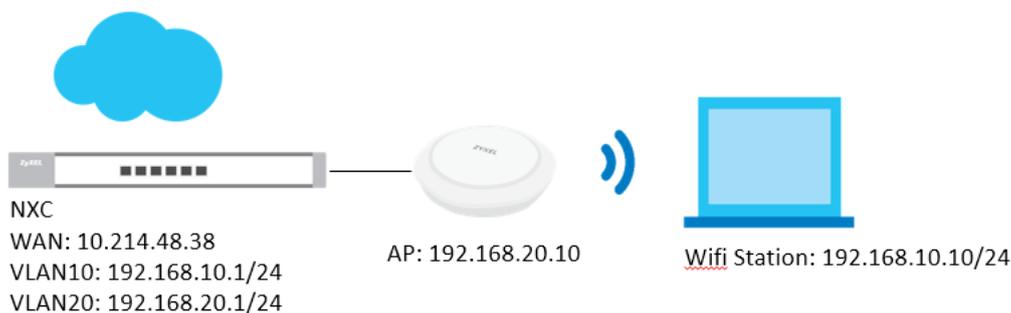


Figure 4.6 Use 802.1x with EAP-TLS



Note:

All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using NXC2500 (Firmware Version: 5.40)

4.6.1 Configure Certificate

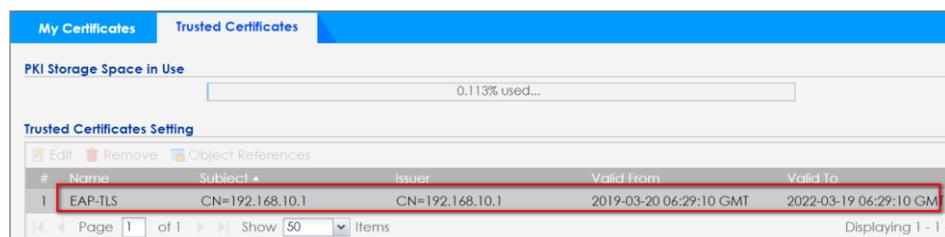
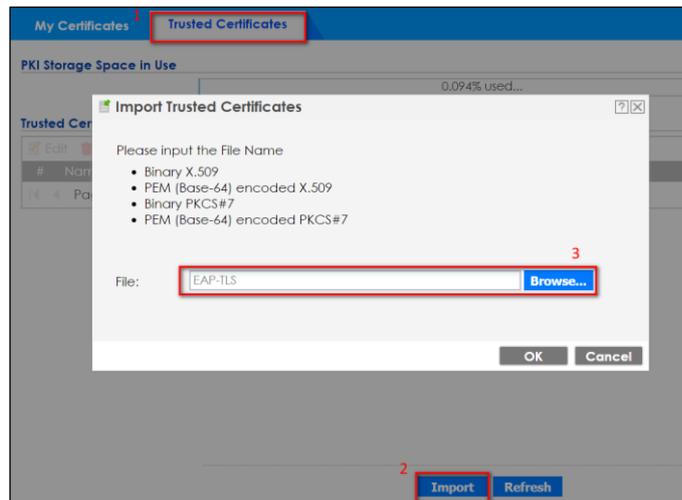
- 1 Go to **CONFIGURATION > Object > Certificate > My certificates**, and **add** a self-signed certificate. In **Subject Information**, Set the **NXC's IP** in the **Host IP Address**.

In **Enrollment Options**, select **Create a self-signed certificate**

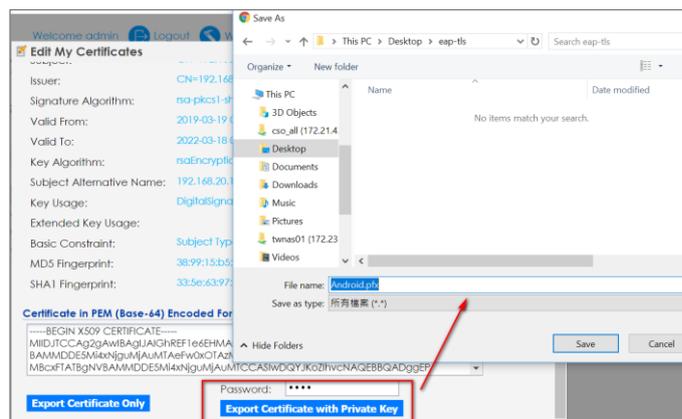
- 2 Export the self-signed certificate from My certificates. **Double click** the self-signed certificate and scroll down the page to press **Export Certificate Only**. **Save** the certificate.

#	Name	Type	Subject	Issuer	Valid from	Valid To
1	EAP-TLS	SELF	CN=192.168.10.1	CN=192.168.10.1	2019-06-06 08:00:38 G...	2022-06-05 08:00:38 G...

3 Go to **Trusted Certificate** and **import** the self-signed certificate.

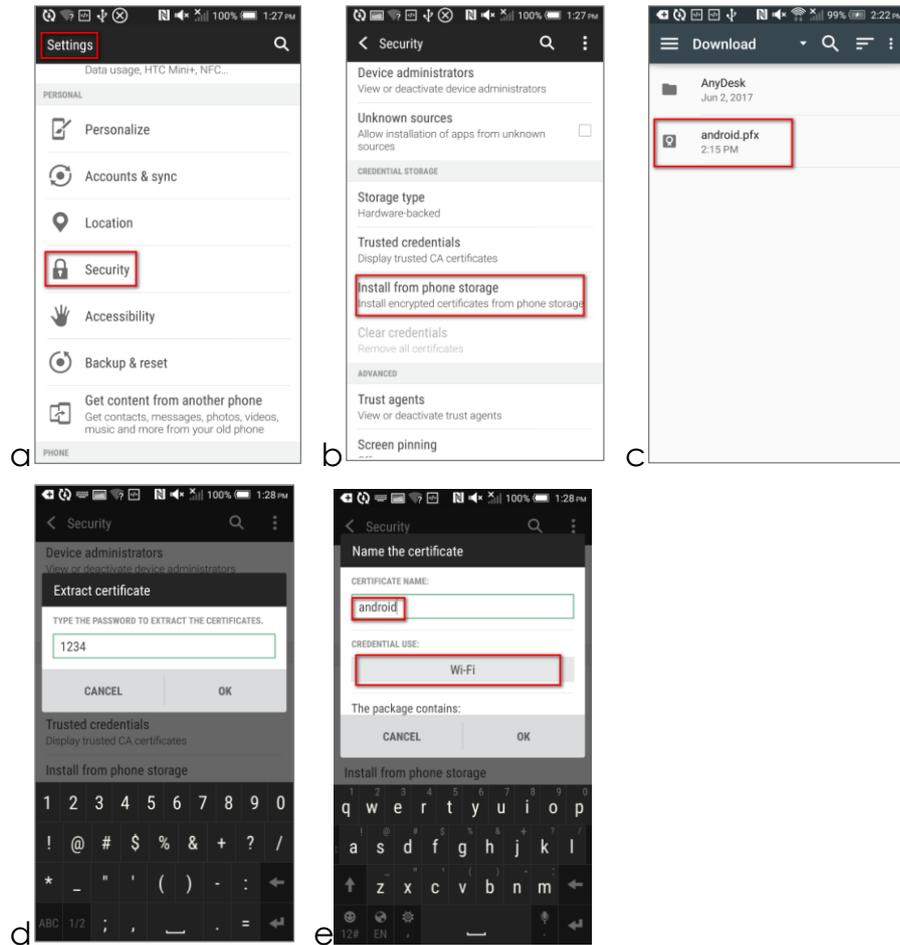


4 Go to **My certificate** and Export the “Self-signed certificate with Private Key”. **Double click** the self-signed certificate and scroll down the page to press **Export Certificate with Private Key**. **Save** the certificate and add file extension (*.pfx, *.p12 or *.crt).

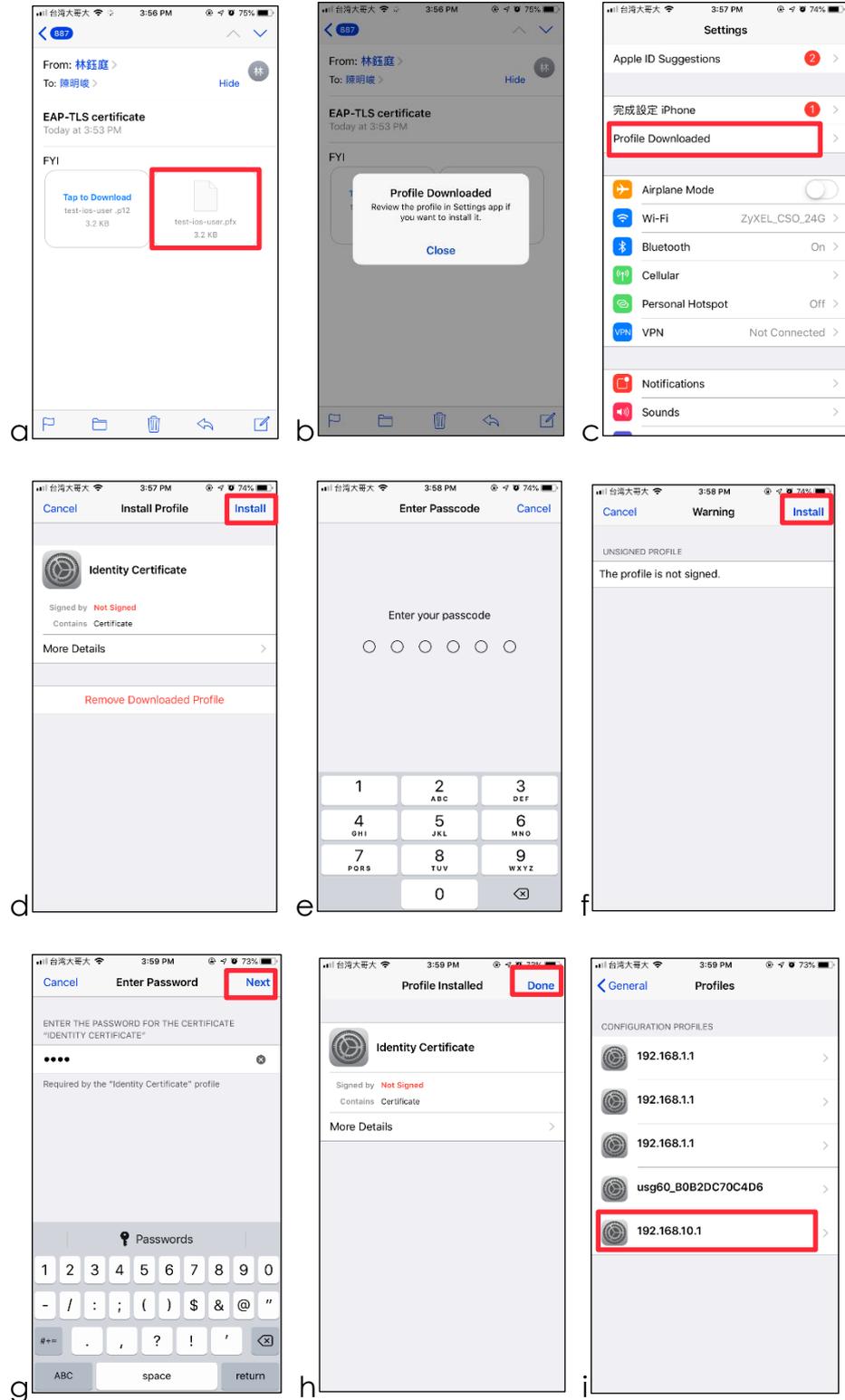


- Import the self-signed certificate into Android phone. (Here I copied the certificate to the Android phone storage then import them. I send the mail with certificate to iPhone and install it.)

Android: In step “e”, the “CREDENTIAL USE” must select as “Wi-Fi”



iOS:



4.6.2 Configure AP profile

- 1 Go to **CONFIGURATION > Object > AP Profile > SSID > Security List**, and **add** a Security profile

Edit Security Profile test

General Settings

Profile Name: EAP-TLS
 Security Mode: wpa2

Fast Roaming Settings

802.11r

Radius Settings

Radius Server Type: Internal

MAC Authentication Setting

MAC Authentication

Auth. Method: default
 Delimiter (Account): dash (-)
 Case (Account): upper
 Delimiter (Calling Station ID): dash (-)
 Case (Calling Station ID): upper
 Fallback to Captive Portal after MAC authentication failure

Authentication Settings

802.1X
 Auth. Method: default
 ReAuthentication Timer: 0 (30~30000 seconds, 0 is unlimited)

PSK

Pre-Shared Key:
 Cipher Type: aes
 Idle timeout: 300 (30~30000 seconds)
 Group Key Update Timer: 30000 (30~30000 seconds)
 Pre-Authentication: Enable
 Management Frame Protection Optional Required

OK Cancel

- 2 Go to **CONFIGURATION > Object > AP Profile > SSID > SSID List**, and **add** an SSID profile.

Edit SSID Profiletest

Create new Object +

Profile Name: EAP-TLS
 SSID: Zyxel-EAPTLS
 Security Profile: EAP-TLS

MAC Filtering Profile: disable
 Layer-2 Isolation Profile: disable
 QoS: WMM

Rate Limiting (Per Station Traffic Rate)

Downlink: 0 mbps (0~160, 0 is unlimited)
 Uplink: 0 mbps (0~160, 0 is unlimited)

Band Select

Forwarding Mode: Local bridge

VLAN ID: 10 (1~4094)

Controller offline policy ^{BETA}
 Hidden SSID
 Enable Intra-BSS Traffic blocking
 Enable U-APSD
 Enable ARP Proxy

OK Cancel

- 3 Go to **CONFIGURATION > Wireless > AP Management > AP Group**, and **add** this SSID into the default group.

Edit AP Group Profile default

General Settings

Group Name: default
Description: (Optional)
Location: (Optional)

Radio 1 Setting

OP Mode: AP Mode MON Mode Root AP Repeater AP

Radio 1 AP Profile: default
Max Output Power: 30 dBm (0~30)

#	SSID Profile
1	default
2	EAP-TLS
3	disable
4	disable
5	disable
6	disable
7	disable
8	disable

Radio 2 Setting

OP Mode: AP Mode MON Mode Root AP Repeater AP

Radio 2 AP Profile: default2
Max Output Power: 30 dBm (0~30)

#	SSID Profile
1	default
2	EAP-TLS
3	disable
4	disable
5	disable
6	disable
7	disable
8	disable

VLAN Settings

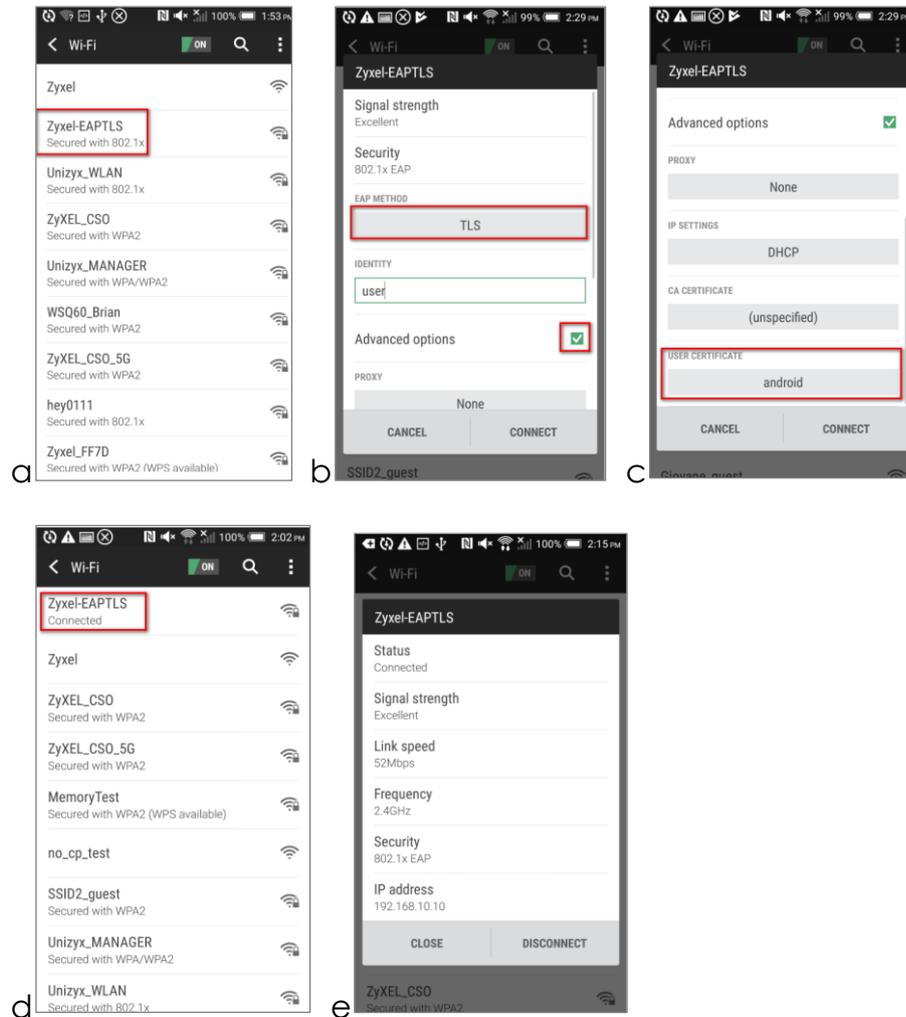
Force Overwrite VLAN Config
Management VLAN ID: 1 (1~4094)

OK Cancel Override Member AP setting

4.6.3 Test the Result

- 1 Use Android/iOS phone and connect to the SSID Zyxel-EAPTLS.

Android:



iOS:



- 2 Check the station information On NXC station info. Go to **Configuration > Wireless > Station info.**

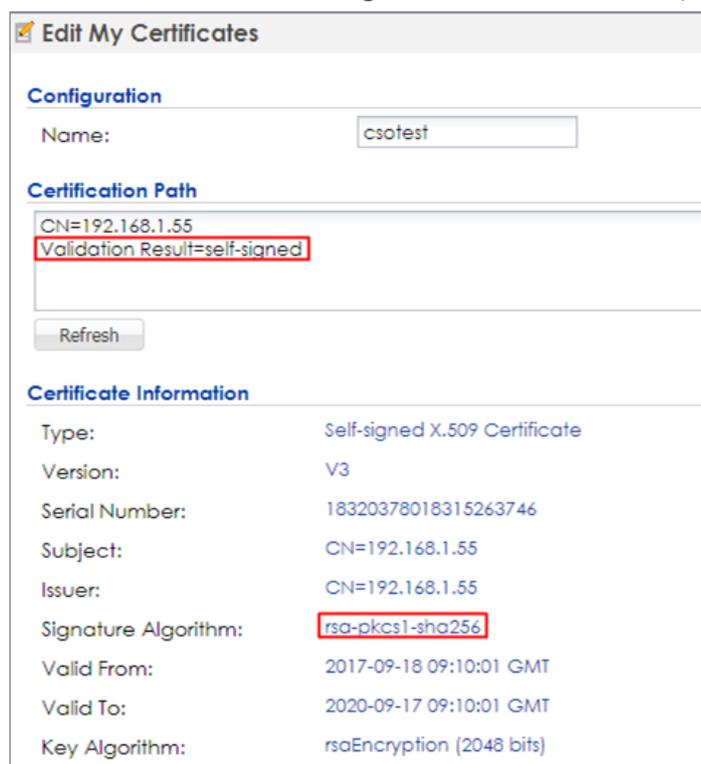


The screenshot shows the ZyXEL NXC web interface. On the left is a navigation menu with options: Ethernet Neighbor, Wireless, AP Information, ZyMesh, SSID Info, Station Info (highlighted), and Detected Device. The main content area shows a table of wireless stations with a 'Disconnect' button at the top left. The table has columns for #, IP Address, Associated AP, SSID Name, 802.1X, Captive Portal, MAC Auth, MAC Address, and Signal Strength. One station is listed with IP 192.168.10.10, AP-A0E4, SSID Zyxel-EAPTLS, and a signal strength of -48dBm.

#	IP Address	Associated AP	SSID Name	802.1X	Captive Portal	MAC Auth	MAC Address	Signal Strength
1	192.168.10.10	AP-A0E4	Zyxel-EAPTLS	N/A	N/A		2C:8A:3	-48dBm

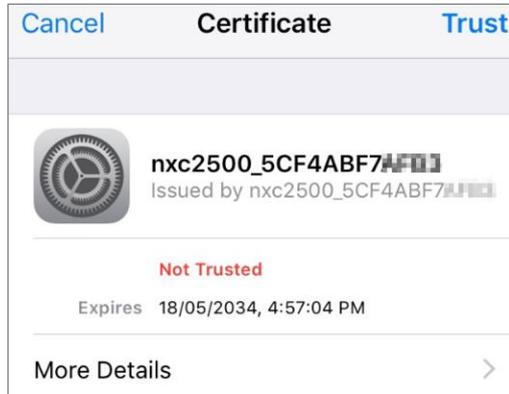
4.6.4 What Could Go Wrong?

- 1 Users must import the certificate which is signed by NXC, and credential use must select Wi-Fi.
- 2 When pressing disconnecting on the Android phone, we might need to import the certificates again.
- 3 Different Android/iOS firmware versions may have different certificate importing behavior. Please ensure the certificates are imported successfully.
- 4 The Windows PC doesn't support self-signed certificate.
- 5 Go to **CONFIGURATION > Object > Certificate > My Certificates**, click the self-signed certificate and click edit. It shows **validation result=self-signed** in certification path.



- 6 When the customer connects to a SSID with 802.1x security, there is a certificate trust request pop-up screen with the

detailed information of the certificate in iOS.



4.7 How to Configure 802.1x EAP-TLS to Secure the Wireless Environment with Third-party CA Certificate?

This example shows how to use Android/iOS phone import the third-party certificate to get the wireless connection with 802.1x EAP-TLS protected. We need a certificate which is purchasing by the third-party CA.

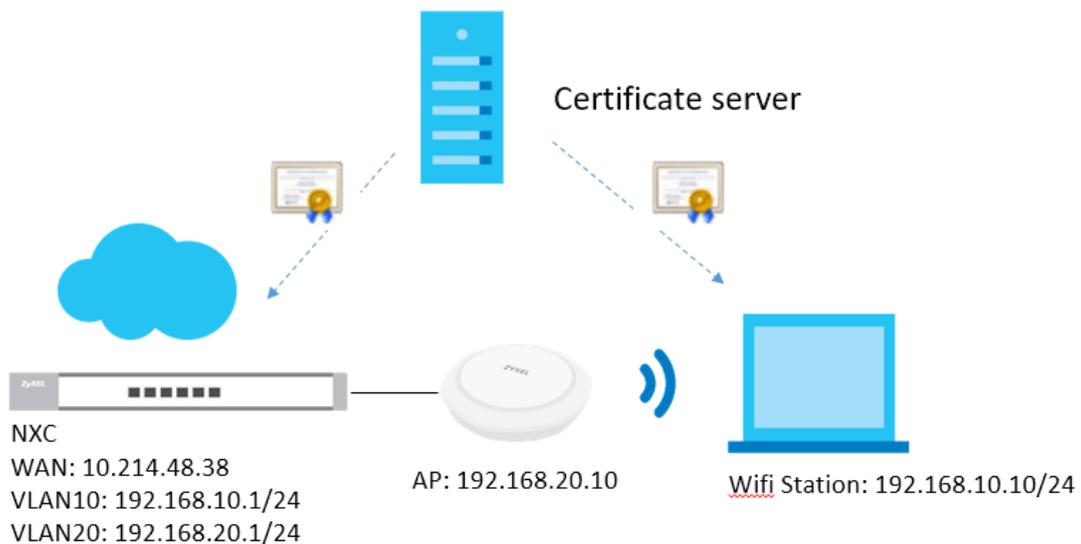


Figure 4.7 Use 802.1x with EAP-TLS

Note:

All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using NX2500 (Firmware Version: 5.40)

4.7.1 Configure Certificate

- 1 Generate certificate request on the NXC. Go to **CONFIGURATION > Object > Certificate > My certificates**, and **add** a request certificate. In **Subject Information**, Set the **NXC's IP** in the **Host IP Address**.

In **Enrollment Options**, select **Create a certification request and save it locally for later manual enrollment**.

Add My Certificates

Configuration

Name: NXC

Subject Information

Host IP Address: 192.168.10.1

Host Domain Name

E-mail

Organizational Unit: (Optional)

Organization: (Optional)

Town (City): (Optional)

State (Province): (Optional)

Country: (Optional)

Key Type: RSA-SHA256

Key Length: 2048 bits

Extended Key Usage

Server Authentication

Client Authentication

Enrollment Options

Create a self-signed certificate

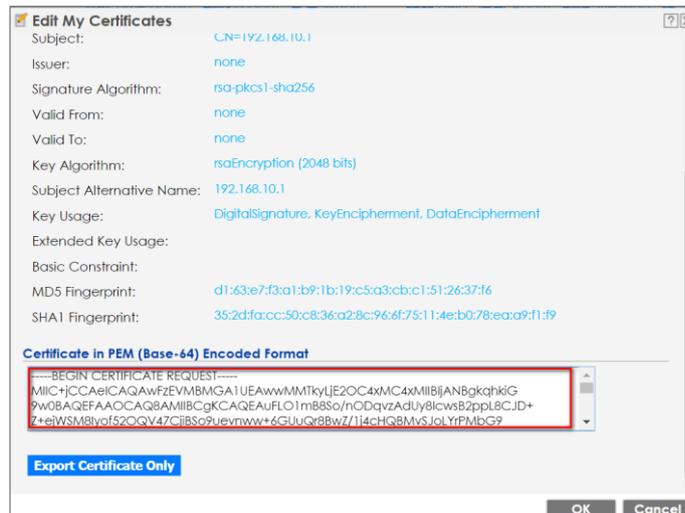
Create a certification request and save it locally for later manual enrollment

OK Cancel

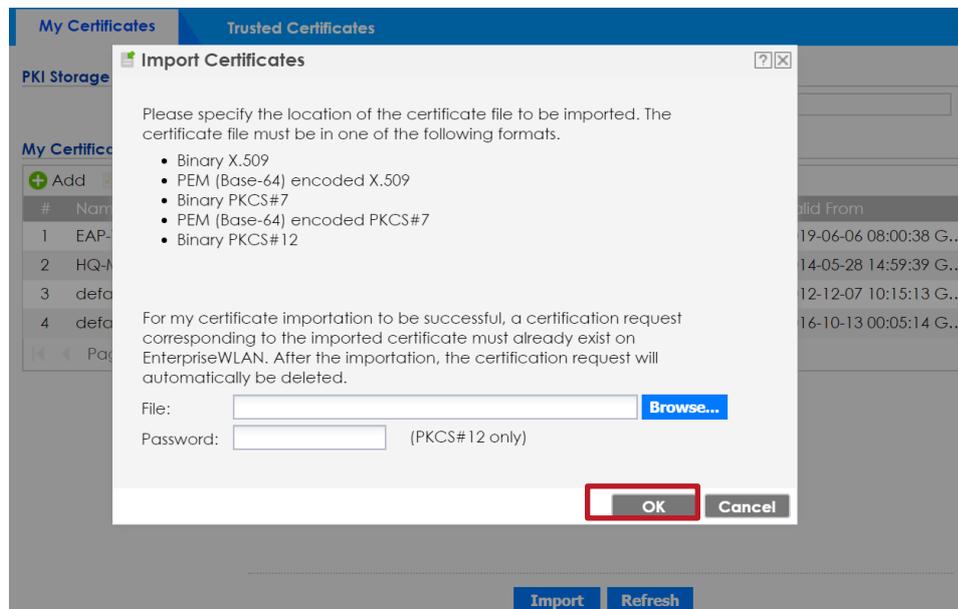
My Certificates Setting

#	Name	Type	Subject	Issuer	Valid From	Valid To
1	NXC	REQ	CN=192.168.10.1	none	none	none

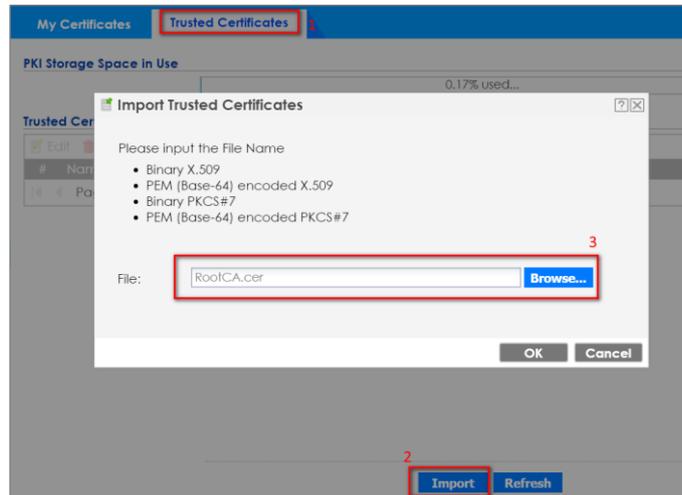
- 2 **Double click** the certificate and scroll down the page to **copy** the **Base-64 code**, then provide it to the third-party certificate company.



- 3 After receiving the certificate, import the NXC identity certificate into "My Certificates", and the REQ certificate will be changed to CERT automatically. Go to **CONFIGURATION > Object > Certificate > My Certificates > Import**.



- 4 Import the root CA and Intermediate CA's certificate (if exists) into "Trusted Certificate". Go to **CONFIGURATION > Object > Certificate > Trusted Certificates > Import**.

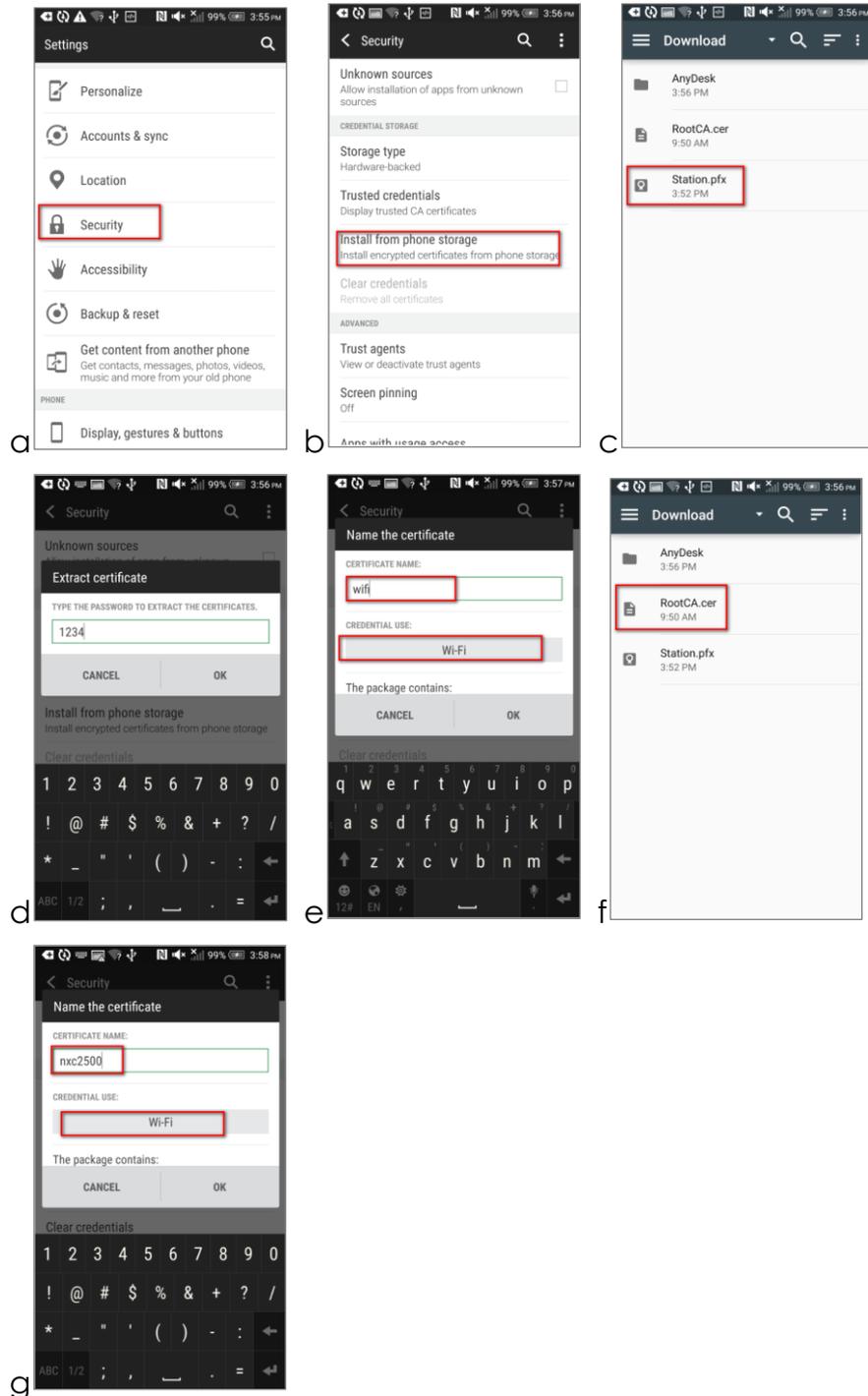


Trusted Certificates Setting					
#	Name	Subject	Issuer	Valid From	Valid To
1	RootCA.cer	CN=SVDradius, DC=zyxel, ...	CN=SVDradius, DC=zyxel, ...	2016-03-04 04:31:22 GMT	2036-03-04 04:41:21 GMT

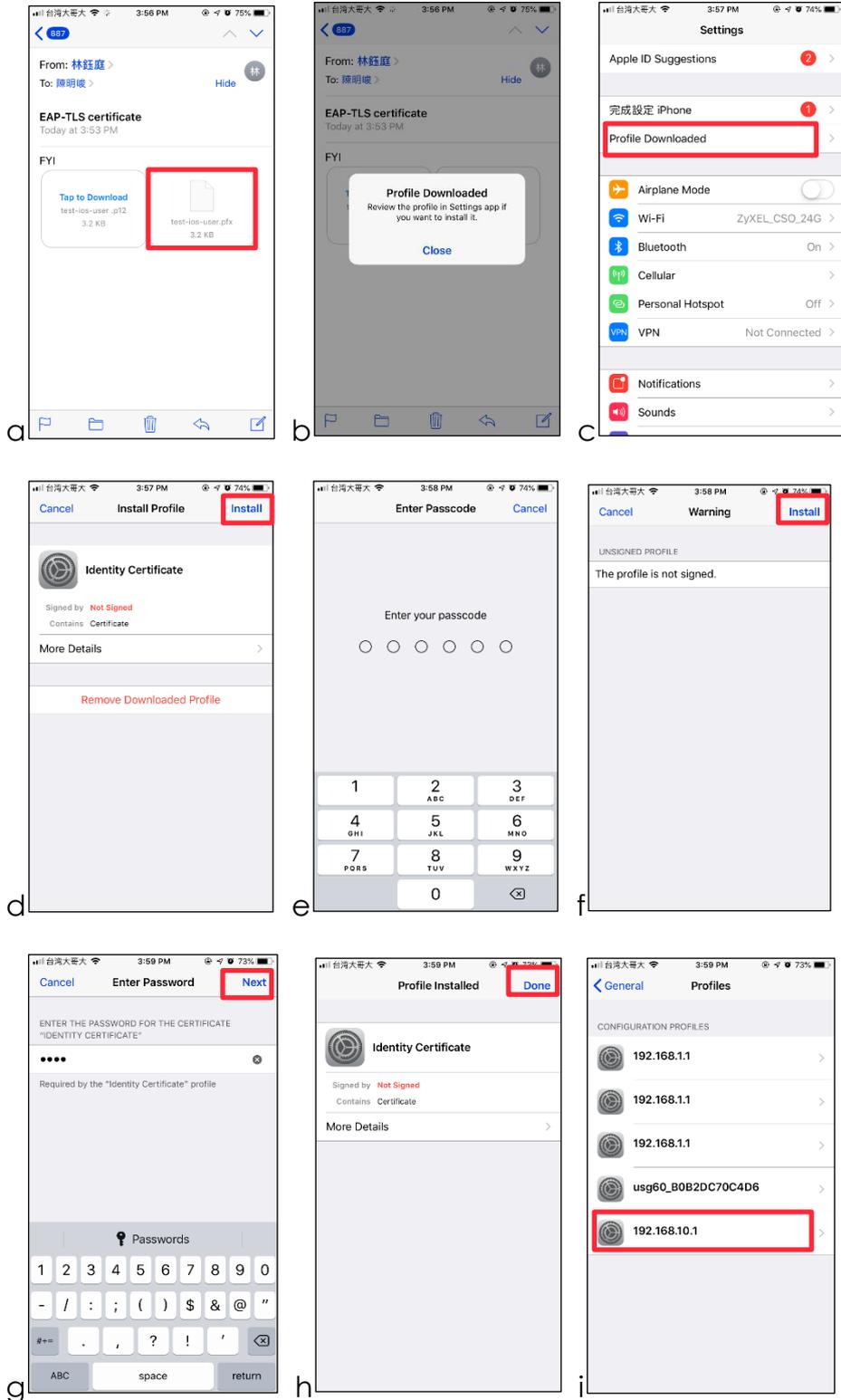
Page 1 of 1 Show 50 Items Displaying 1 - 1 of 1

- 5 Import the station identity certificate, root CA and Intermediate CA's certificate (if exists) into the Android/iOS phone. (The station could download the certificates from email, dropbox or a cloud storage space).

Android: In step "e", the Credential use must select Wi-Fi.



ios: The way is same as import self-signed certificate.



4.7.2 Configure AP profile

- 1 Go to **CONFIGURATION > Object > AP Profile > SSID > Security List**, and **add** a Security profile.

Edit Security Profile test

General Settings

Profile Name: EAP-TLS
 Security Mode: wpa2

Fast Roaming Settings

802.11r

Radius Settings

Radius Server Type: Internal

MAC Authentication Setting

MAC Authentication

Auth. Method: default
 Delimiter (Account): dash (-)
 Case (Account): upper
 Delimiter (Calling Station ID): dash (-)
 Case (Calling Station ID): upper
 Fallback to Captive Portal after MAC authentication failure

Authentication Settings

802.1X

Auth. Method: default
 ReAuthentication Timer: 0 (30-30000 seconds, 0 is unlimited)

PSK

Pre-Shared Key:
 Cipher Type: aes
 Idle timeout: 300 (30-30000 seconds)
 Group Key Update Timer: 30000 (30-30000 seconds)
 Pre-Authentication: Enable
 Management Frame Protection Optional Required

OK Cancel

- 2 Go to **CONFIGURATION > Object > AP Profile > SSID > SSID List**, and **add** an SSID profile.

Edit SSID Profiletest

Create new Object +

Profile Name: EAP-TLS
 SSID: Zyxel-EAPTLS
 Security Profile: EAP-TLS

MAC Filtering Profile: disable
 Layer-2 Isolation Profile: disable
 QoS: WMM

Rate Limiting (Per Station Traffic Rate)

Downlink: 0 mbps (0~160, 0 is unlimited)
 Uplink: 0 mbps (0~160, 0 is unlimited)

Band Select

Forwarding Mode: Local bridge

VLAN ID: 10 (1~4094)

Controller offline policy ^{BETA}
 Hidden SSID
 Enable Intra-BSS Traffic blocking
 Enable U-APSD
 Enable ARP Proxy

OK Cancel

- 3 Go to **CONFIGURATION > Wireless > AP Management > AP Group**, and **add** this SSID into the default group.

The screenshot shows the 'Edit AP Group Profile default' configuration window. It is divided into several sections:

- General Settings:** Group Name: default; Description: (Optional); Location: (Optional).
- Radio 1 Setting:** OP Mode: AP Mode; Radio 1 AP Profile: default; Max Output Power: 30 dBm (0~30). Below this is a table of SSID profiles:

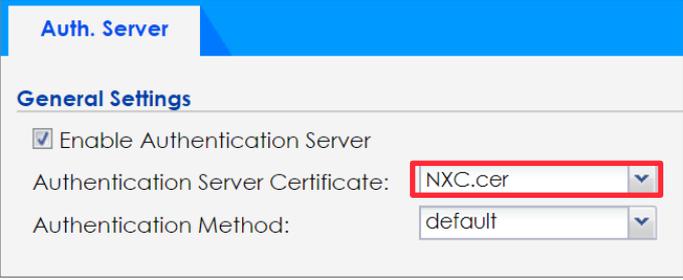
#	SSID Profile
1	default
2	EAP-TLS
3	disable
4	disable
5	disable
6	disable
7	disable
8	disable
- Radio 2 Setting:** OP Mode: AP Mode; Radio 2 AP Profile: default2; Max Output Power: 30 dBm (0~30). Below this is a table of SSID profiles:

#	SSID Profile
1	default
2	EAP-TLS
3	disable
4	disable
5	disable
6	disable
7	disable
8	disable
- VLAN Settings:** Force Overwrite VLAN Config: ; Management VLAN ID: 1 (1~4094).

Buttons at the bottom: OK, Cancel, Override Member AP setting.

4.7.3 Configure Auth. Server

- 1 Change the certificate to NXC identity certificate from third-party CA. Go to **CONFIGURATION > System > Auth. Server > Auth. Server**, and the **Authentication Server Certificate** select **NXC.cer**.



Auth. Server

General Settings

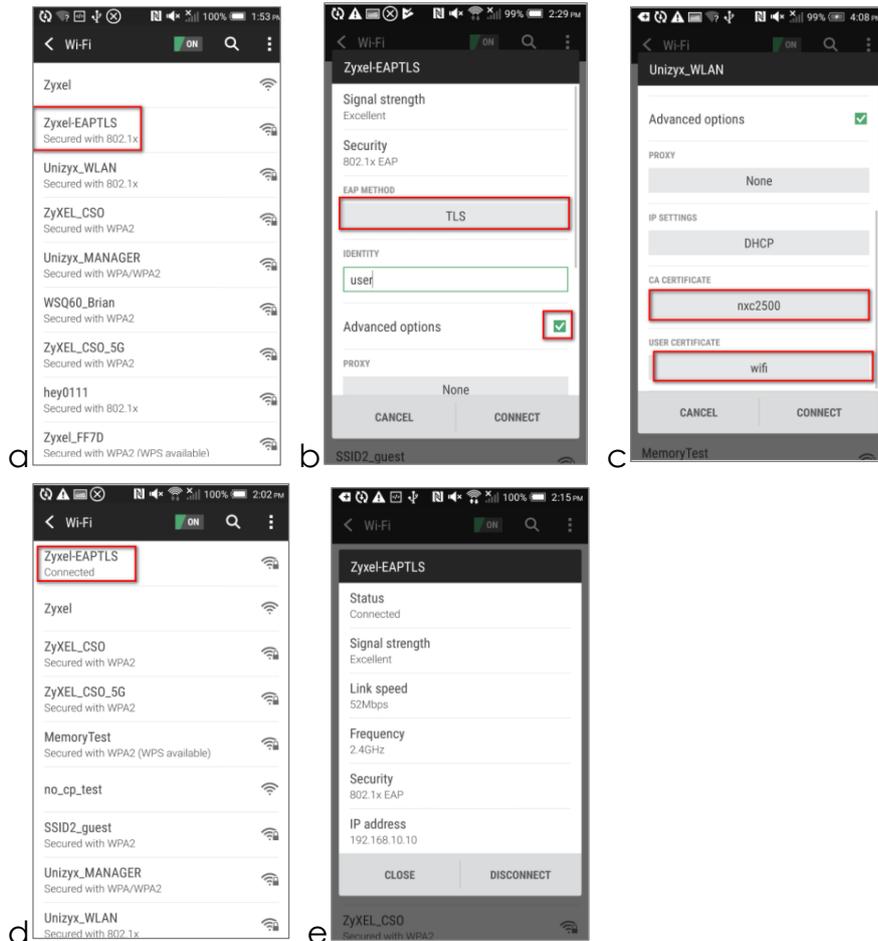
Enable Authentication Server

Authentication Server Certificate: **NXC.cer**

Authentication Method: default

4.7.4 Test the Result

- 1 Use Android/iOS phone and connect to the SSID Zyxel-EAPTLS.
Android: In step "c", please select root CA's certificate in "CA CERTIFICATE" Column and select station identity certificate in "USER CERTIFICATE"



iOS: In step “e”, please select the station personal certificate from CA.



- 2 Check the station information On NXC station info. Go to **Configuration > Wireless > Station info.**



The screenshot shows the 'Station Info' page in the ZyXEL NXC web interface. The left sidebar contains a navigation menu with the following items: Ethernet Neighbor, Wireless, AP Information, ZyMesh, SSID Info, Station Info (highlighted), and Detected Device. The main content area displays a table with the following columns: #, IP Address, Associated AP, SSID Name, 802.1X, Captive Portal, MAC Auth, MAC Address, and Signal Strength. A single entry is shown in the table with the following values: # 1, IP Address 192.168.10.10, Associated AP AP-A0E4 [redacted], SSID Name Zyxel-EAPTLS, 802.1X N/A, Captive Portal N/A, MAC Auth [redacted], MAC Address 2C:8A:7 [redacted], and Signal Strength -48dBm [signal strength icon].

#	IP Address	Associated AP	SSID Name	802.1X	Captive Portal	MAC Auth	MAC Address	Signal Strength
1	192.168.10.10	AP-A0E4 [redacted]	Zyxel-EAPTLS	N/A	N/A	[redacted]	2C:8A:7 [redacted]	-48dBm [signal strength icon]

4.7.5 What Could Go Wrong?

- 1 User must import the certificate correctly on each device.
NXC: Root/Intermediate CA's certificate > Trust Certificate; NXC's certificate > My Certificate;
Station: Root/Intermediate CA's Certificate > Trusted CA list; Stations' personal certificate > Personal Certificate.
- 2 When pressing disconnecting on the Android phone, we might need to import the certificates again.
- 3 Different Android firmware versions may have different certificate importing behavior. Please ensure the certificates are imported successfully.

Secure the Wireless Environment – Captive portal

5.1 How to Configure Captive Portal Redirect on Controller?

The example instructs how to set up captive portal redirect on the controller. A captive portal can intercepts network traffic, according to the authentication policies, until the user authenticates his or her connection, usually through a specifically designated login web page. Typically, you often find captive portal pages in public hotspots. There are two kinds of the topologies for captive portal redirect on the controller: one is to set USG as the gateway; the other is to set NXC controller as the gateway. The configurations of these two kinds of topologies show in below procedures.

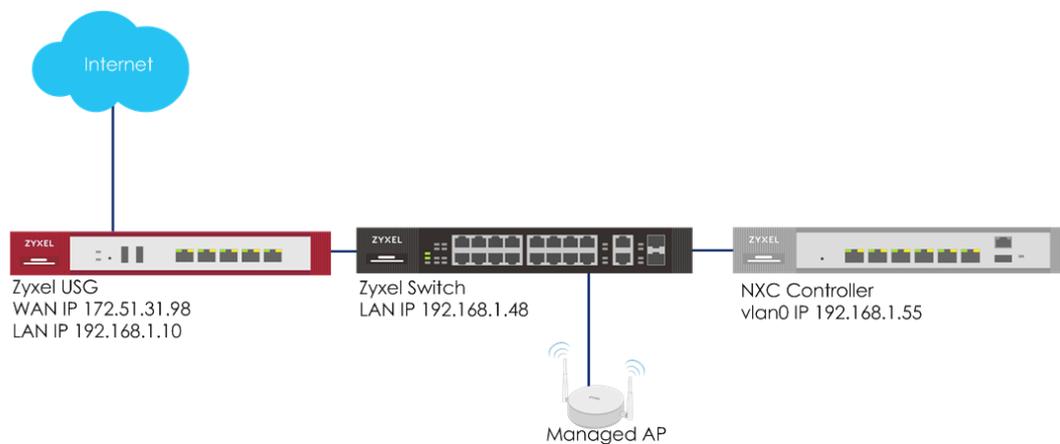


Figure 5.1.a Captive portal redirect on controller (USG is gateway)

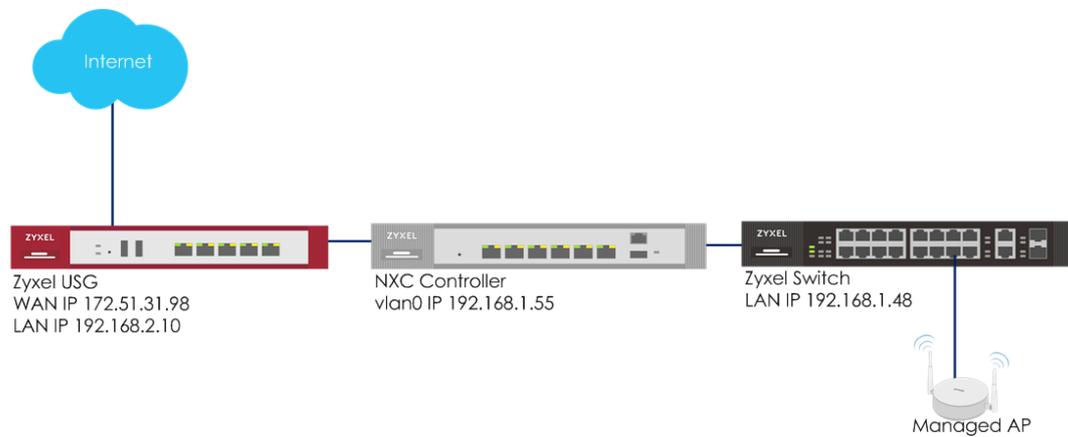


Figure 5.1.b Captive portal redirect on controller (NXC is gateway)

 Note:

All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC2500 (Firmware Version: 5.30), GS2210-8HP (Firmware Version: V4.30).

5.1.1 Configure Authentication Method Setting

- 1 Go to **CONFIGURATION > Object > User/Group**, click **add** to create a new user ID and password. Stations can log in captive portal to access the Internet via this account. Enter the **User Name** as login ID for captive portal and **User Type** is **guest**. Enter the **Password** as the login password. The default of **Authentication Timeout Setting** is 1440 minutes, and usually it's shorter for guests. Select to **Use Manual Settings** to set **Lease Time** and **Reauthentication Time**. Click **OK** to save.

+ Add A User

User Configuration

User Name :

User Type:

Password:

Retype:

Description:

Authentication Timeout Settings Use Default Settings Use Manual Settings

Lease Time: (0-1440 minutes, 0 is unlimited)

Reauthentication Time: (0-1440 minutes, 0 is unlimited)

- 2 Go to **CONFIGURATION > Object > Auth. Method**, click **add** to create an authentication method. Enter the **Name** of this authentication method and select to local in the **Method List**.

General Settings

Name:

#	Method List
1	local

5.1.2 Configure Captive Portal

- 1 Go to **CONFIGURATION > Object > Address > Address**, click **add** to create an address range which needs to do captive portal authentication before accessing to the Internet. Enter profile **Name** and change **Address Type** to **RANGE**. In this example, the IP range for guest is **192.168.1.100** to **192.168.1.200** on DHCP server (USG). Click **OK** to save.

+ Add Address Rule	
Name:	CPtest
Address Type:	RANGE
Starting IP Address:	192.168.1.100
End IP Address:	192.168.1.200

- 2 Go to **CONFIGURATION > Captive Portal > Redirect on Controller > Authentication Policy Rule**, click **add** to create a policy rule for stations which get an IP range from 192.168.1.100 to 192.168.1.200.

In **General Settings**, check **Enable Policy** and enter the **Description** of this policy.

In **User Auth Policy**, change **Source Address** to **CPtest** and **Authentication is required**. Check **Force User Authentication**, and change the **Authentication Method** to **localtest**. Click **OK** to save.

+ Auth. Policy Edit	
Create new Object	
General Settings	
<input checked="" type="checkbox"/> Enable Policy	
Description:	CPtest (Optional)
User Auth Policy	
Source Address:	CPtest RANGE, 192.168.1.100-192.168.1.200
Destination Address:	any
Schedule:	none
Authentication:	force
Authentication Method:	localtest

- 3 If you want to use the domain name instead of an IP address, you can set it in the Authentication Type. (If you don't have FQDN, please skip this step)

+ Auth. Policy Add
 Create new Object ▾

Authentication Type

Internal Web Portal

Enable Domain Name Redirect Link by FQDN: ⓘ

Portal Theme: ▾

- 4 Go to **CONFIGURATION > System > WWW** and enable **Redirect HTTP to HTTPS**. Click **Apply** to apply the settings.

HTTPS

Enable

Server Port:

Authenticate Client Certificates (See [Trusted CAs](#))

Server Certificate: ▾

Redirect HTTP to HTTPS

- 5 Go to **CONFIGURATION > Captive Portal > Captive Portal**, check **Enable Captive Portal**. Click **Apply** to apply the settings.

Captive Portal Custom Captive Portal

General Settings

Enable Captive Portal

5.1.3 Configure AP Profile when USG is the Gateway

- 1 To make sure the USG is the gateway for vlan0 interface which is for client accessing the Internet, go to **CONFIGURATION > Network > Interface > VLAN > vlan0 > Edit**, enter USG's IP in **Gateway**. Click **OK** to apply settings.

IP Address Assignment	
<input type="radio"/> Get Automatically	
<input checked="" type="radio"/> Use Fixed IP Address	
IP Address:	192.168.1.55
Subnet Mask:	255.255.255.0
Gateway:	192.168.1.10 (Optional)
Metric:	0 (0-15)

- 2 Go to **CONFIGURATION > Object > AP Profile > SSID > SSID List**, click **Add** to add a SSID for captive portal. Key in the **SSID** to **CP_guest**, and change **Security Profile** to **default** which sets none security. Change **Forwarding Mode** to **Tunnel** Mode and click **OK** to save.

+ Add SSID Profile	
Create new Object ▾	
Profile Name:	CP_test
SSID:	CP_guest
Security Profile:	default ▾
MAC Filtering Profile:	disable ▾
Layer-2 Isolation Profile:	disable ▾
QoS:	WMM ▾
Rate Limiting (Per Station Traffic Rate)	
Downlink:	0 mbps ▾ (0~160, 0 is unlimited)
Uplink:	0 mbps ▾ (0~160, 0 is unlimited)
Band Select:	disable ▾
Forwarding Mode:	Tunnel ▾
VLAN Interface:	vlan0 ▾ VID: 1

- Go to **CONFIGURATION > Wireless > AP Management > AP Group**, select the **default** AP profile and edit. Select **#1 to CP_test** which created in step2. Click **Override Member AP Setting** to apply the SSID to AP and click **Yes** in the pop-up window. Click **OK**.

Radio 1 Setting

OP Mode AP Mode MON Mode Root AP Repeater AP i

Radio 1 AP Profile: v

Max Output Power: dBm (0~30)

Edit

#	SSID Profile
1	CP_test
2	disable
3	disable
4	disable
5	disable
6	disable
7	disable
8	disable

Radio 2 Setting

OP Mode AP Mode MON Mode Root AP Repeater AP i

Radio 2 AP Profile: v

Max Output Power: dBm (0~30)

Edit

#	SSID Profile
1	CP_test

- Logout** from NXC controller.

5.1.4 Configure AP Profile when NXC is the Gateway

- 1 Make sure the NXC is the gateway for vlan0 interface which is the captive portal and stations need to connect to. Go to **CONFIGURATION > Network > Interface > VLAN > vlan0 > Edit**, select **no** in Member for ge1 and enter the NXC's IP in **Gateway**. Enable **DHCP server** and set the IP from **192.168.1.100 to 192.168.1.200** (IP pool 100). The **Default Router** is **vlan0**. Click **OK** to apply settings

Edit Vlan vlan0
 Show Advanced Settings

Member Configuration

Edit

#	Port Name	Member	Tx Tagging
1	ge1	no	no
2	ge2	yes	no
3	ge3	yes	no
4	ge4	yes	no
5	ge5	yes	no
6	ge6	yes	no

IP Address Assignment

Get Automatically
 Use Fixed IP Address

IP Address:
 Subnet Mask:
 Gateway: (Optional)
 Metric: (0-15)

DHCP Setting

DHCP:
 IP Pool Start Address (Optional): Pool Size:
 First DNS Server (Optional):

- Go to **CONFIGURATION > Network > Interface > Ethernet**, click **ge1** and then click **Edit** to make ge1 as the external interface for connecting with the Internet. Change **Interface Type** to **external** and **IP Address Assignment** is **Get Automatically**. Click **OK** to save.

Edit Ethernet
Show Advanced Settings

General Settings

Enable Interface

Interface Properties

Interface Type: external ⓘ

Interface Name: ge1

Port: P1

PVID: 1 (1~4094)

Zone: none ⓘ

MAC Address: 5C:00:00:00:00:00

Description: (Optional)

IP Address Assignment

Get Automatically

Use Fixed IP Address

- Go to **CONFIGURATION > Network > Routing > Policy Route**, and click **Add** to add a routing rule for outgoing traffic. Click **Show Advanced Settings**. Check **Enable** in **Configuration**. Select **Interface** in **Incoming** and select to **vlan0** in **Please select one member**. Change **Type** to **Interface** and select **Interface ge1**. Change **Source Network Address Translation** to **outgoing-interface**. Click **OK**.

+ **Add Policy Route**
Hide Advanced Settings
Create new Object ▾

Criteria

User:	any ▾
Incoming:	Interface ▾
Please select one member:	vlan0 ▾
Source Address:	any ▾
Destination Address:	any ▾
DSCP Code:	any ▾
Schedule:	none ▾
Service:	any ▾
Source Port:	any ▾

Next-Hop

Type:	Interface ▾
Interface:	ge1 ▾
<input type="checkbox"/> Auto-Disable	

DSCP Marking

DSCP Marking:	preserve ▾
---------------	------------

Address Translation

Source Network Address Translation:	outgoing-interface ▾
-------------------------------------	----------------------

- Go to **CONFIGURATION > Object > AP Profile > SSID > SSID List**, and click **Add** to add a SSID for captive portal. Key in the **SSID** to **CP_guest**, and change **Security Profile** to **default** which sets none security. Click **OK** to save.

Create new Object

Profile Name: CP_test

SSID: CP_guest

Security Profile: default

MAC Filtering Profile: disable

- Go to **CONFIGURATION > Wireless > AP Management > AP Group**, and click **default** to **Edit**. Change **#1** to **CP_test** which is created in step2. Click **Override Member AP Setting** to apply the SSID to AP and click **Yes** in the pop-up window. Click **OK**

Radio 1 Setting

OP Mode AP Mode MON Mode Root AP Repeater AP i

Radio 1 AP Profile: default

Max Output Power: 30 dBm (0~30)

Edit

#	SSID Profile
1	CP_test
2	disable
3	disable
4	disable
5	disable
6	disable
7	disable
8	disable

Radio 2 Setting

OP Mode AP Mode MON Mode Root AP Repeater AP i

Radio 2 AP Profile: default2

Max Output Power: 30 dBm (0~30)

Edit

#	SSID Profile
1	CP_test

5.1.5 Test the Result

- 1 Connect to SSID CP_guest from the computer. After the connection is successfully established, check if the IP is in the range from 192.168.1.100 to 192.168.1.200, and the gateway is NXC's IP.

Property	Value
Connection-specific DN...	
Description	Broadcom 802.11n Network Adapter
Physical Address	5C-AC-4C-05-14-1F
DHCP Enabled	Yes
IPv4 Address	192.168.1.102
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	Monday, September 19, 2016 5:36:32 PM
Lease Expires	Thursday, September 22, 2016 5:41:27 PM
IPv4 Default Gateway	192.168.1.55
IPv4 DHCP Server	192.168.1.55
IPv4 DNS Server	8.8.8.8

- 2 Open a browser and visit a website it after the computer connects to the AP successfully. The browser redirects to the captive portal page and needs to enter the username and password for authentication before accessing the Internet.

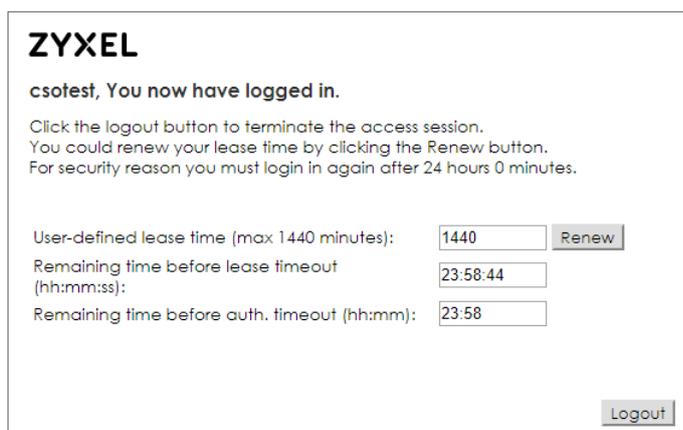
ZYXEL ⌵

Welcom to the configuration interface,
please enter username and password to login.

- 3 If you use redirect by FQDN, the website address shows the domain name you set in captive portal authentication Type.

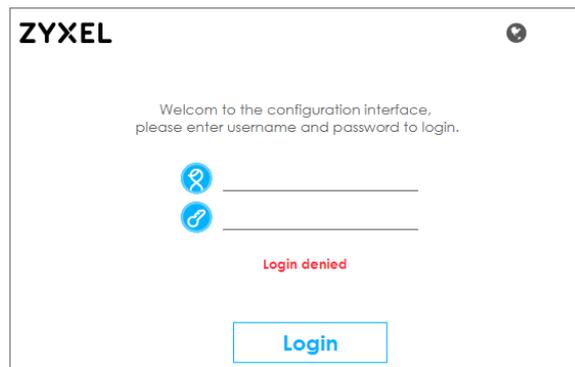


- 4 After entering the username and password correctly, the connected station is able to access the Internet now. There is also a pop-window to show the detail information of the renew time and re-authentication time after authentication succeed.

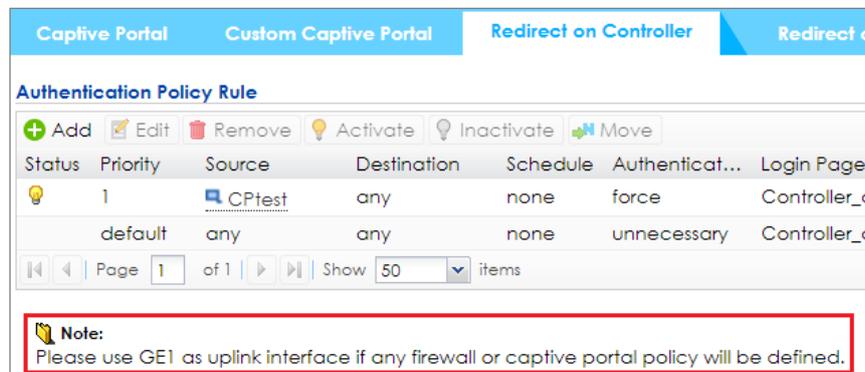


5.1.6 What Could Go Wrong

- 1 The DNS **MUST** be set in the DHCP setting, or the captive portal might fail to redirect because NXC controller is not able to know the correct IP address of the website which stations access to.
- 2 The captive portal fails to redirect the webpage if the station logs in to the NXC controller before and does not logout.
- 3 When USG is the gateway, the **Forwarding Mode** MUST be **Tunnel** mode to make sure the traffic from AP goes to NXC controller.
- 4 If the user enters an incorrect username or password, there is a login failure webpage. Please use the correct username and password to log in again.



- 5 When using the NXC2500 as the controller, the uplink port MUST be ge1.



5.2 How to Configure Captive Portal Redirect on AP?

The example instructs how to set up captive portal redirect on the AP. A captive portal can intercepts network traffic, according to the authentication policies, until the user authenticates his or her connection, usually through a specifically designated login web page. Typically, you often find captive portal pages in public hotspots.

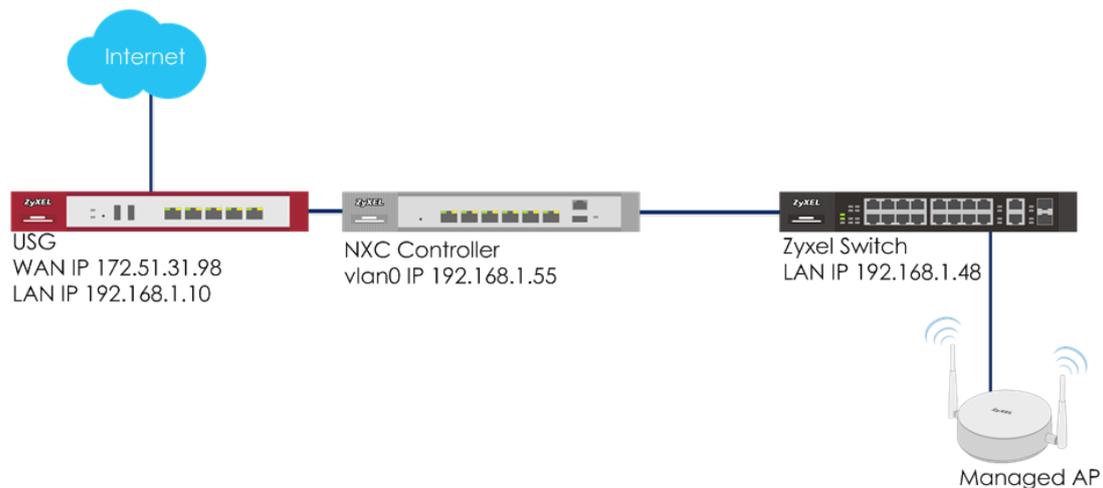


Figure 5.2 Captive portal redirect on AP



Note:

All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC5500 (Firmware Version: 5.40), GS2210-8HP (Firmware Version: V4.30).

5.2.1 Configure AP Profile and User

- 1 Go to **CONFIGURATION > Object > AP Profile > SSID > SSID List**, click **Add** to add a SSID for captive portal. Key-in the **Profile Name** is **CP_test** and **SSID** as **CP_guest**, and select **Security Profile** to **default** which sets none security. Click **OK** to save.

+ Add SSID Profile

Create new Object ▾

Profile Name: CP_test

SSID: CP_guest

Security Profile: default ▾

- 2 Go to **CONFIGURATION > Object > User/Group**, and click **add** to create a new user ID and password. Stations can log in captive portal to access Internet via this account. Enter the **User Name** as login ID for captive portal and **User Type** is **guest**. Enter the **Password** as the login password. The default of **Authentication Timeout Setting** is 1440 minutes, and usually it's shorter for guests. Select to **Use Manual Settings** to set **Lease Time** and **Reauthentication Time**. Click **OK** to save.

+ Add A User

User Configuration

User Name : cstest

User Type: guest ▾

Password:

Retype:

Description: Local User

Authentication Timeout Settings Use Default Settings Use Manual Settings

Lease Time: 720 (0-1440 minutes, 0 is unlimited)

Reauthentication Time: 720 (0-1440 minutes, 0 is unlimited)

- 3 Go to **CONFIGURATION > Object > Auth. Method**, and click **add** to create an authentication method. Enter the **Name** of this authentication method and select to local in the **Method List**.

+ Add Authentication Method

General Settings

Name:

+ Add **Edit** **Remove** **Move**

Method List ▾

1	local
---	-------

5.2.2 Configure Captive Portal

- 1 Go to **CONFIGURATION > Captive Portal > Redirect on AP > Authentication Policy Rule**, and click **add** to create a policy rule for stations which connect to SSID profile CP_test.
In **General Settings**, check **Enable Policy** and enter the **Profile Name** of this policy.
In **User Auth Policy**, change **SSID** to **CPtest** and **Authentication** is **required**. Check **Force User Authentication**, and change the **Authentication Method** to **localtest**. Click **OK** to save.

+ Auth. Policy Add
Create new Object ▾

General Settings

Enable Policy

Theme Name:

Description: (Optional)

User Auth Policy

SSID:

Source Address:

Destination Address:

Schedule:

Authentication:

Authentication Method:

- 2 Go to **CONFIGURATION > Captive Portal > Redirect on AP > Authentication Policy Group**, and click **default** to edit. In the setting, click **Add** to add the policy rule which is created in previous step.

+ Edit Authentication Policy Group default [?] [X]

General Settings

Profile Name: default

Description: (Optional)

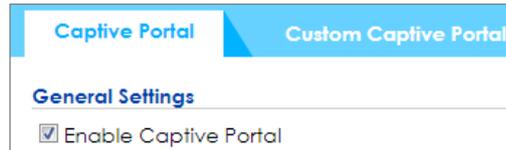
+ Add **Edit** **Remove** **Move**

#	Name
1	CP_test

Page 0 of 0 | Show 50 items | No data to display

Note:
The "default" policy rule will be the last one for each group profile.

- 3 Go to **CONFIGURATION > Captive Portal > Captive Portal**, check **Enable Captive Portal**. Click **Apply** to apply the settings



The screenshot shows a web interface for configuring the Captive Portal. At the top, there are two tabs: 'Captive Portal' (selected) and 'Custom Captive Portal'. Below the tabs, there is a section titled 'General Settings'. Under this section, the checkbox for 'Enable Captive Portal' is checked.

Captive Portal	Custom Captive Portal
General Settings	
<input checked="" type="checkbox"/> Enable Captive Portal	

5.2.3 Broadcast SSID

- 1 Go to **CONFIGURATION > Wireless > AP Management > AP Group**, click **default** to **Edit**. Change **#1** to **CP_test**.

Radio 1 Setting

OP Mode: AP Mode MON Mode Root AP Repeater AP

Radio 1 AP Profile: default

Max Output Power: 30 dBm (0~30)

#	SSID Profile
1	CP_test
2	disable
3	disable
4	disable
5	disable
6	disable
7	disable
8	disable

Radio 2 Setting

OP Mode: AP Mode MON Mode Root AP Repeater AP

Radio 2 AP Profile: default2

Max Output Power: 30 dBm (0~30)

#	SSID Profile
1	CP_test

- 2 In the same setting page as previous step, select **default** for **Auth. Policy Group** in **Portal Redirect on AP**. Click **OK** to save.

Portal Redirect on AP

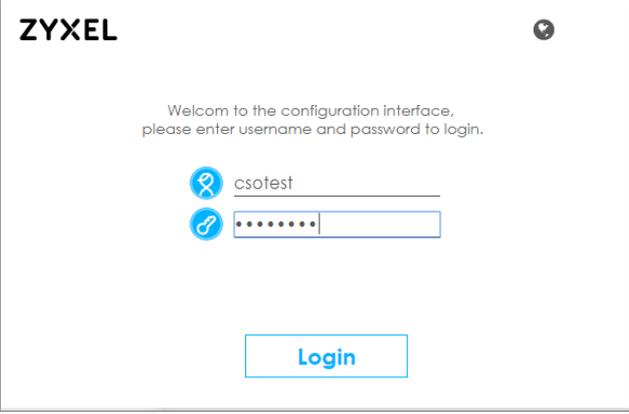
Auth. Policy Group: default

Skip authentication to provide contingency access while controller is unreachable.

- 3 **Logout** from NXC controller.

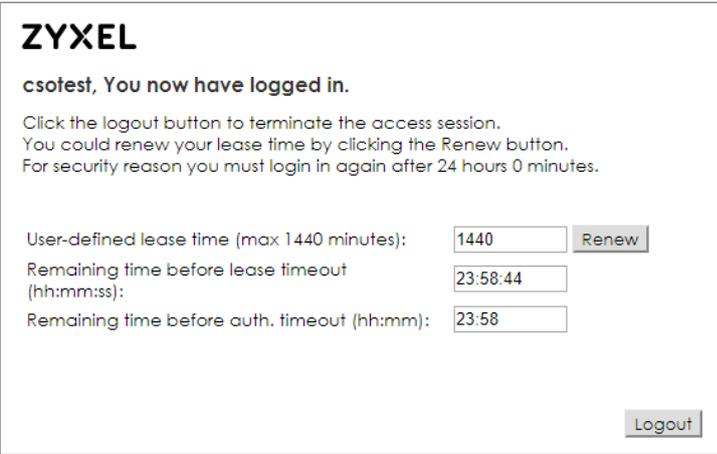
5.2.4 Test the Result

- 1 Connect the station to the SSID 'CP_guest'. Open a browser and visit a website after the computer and AP connect successfully. The browser redirects the webpage to captive portal page and the user needs to enter the username and password for authentication before accessing the Internet



The screenshot shows the ZYXEL captive portal login interface. At the top left is the ZYXEL logo, and at the top right is a small circular icon. The main text reads: "Welcom to the configuration interface, please enter username and password to login." Below this, there are two input fields: the first is for the username, containing "csotest", and the second is for the password, represented by a series of dots. A blue "Login" button is positioned at the bottom center of the form.

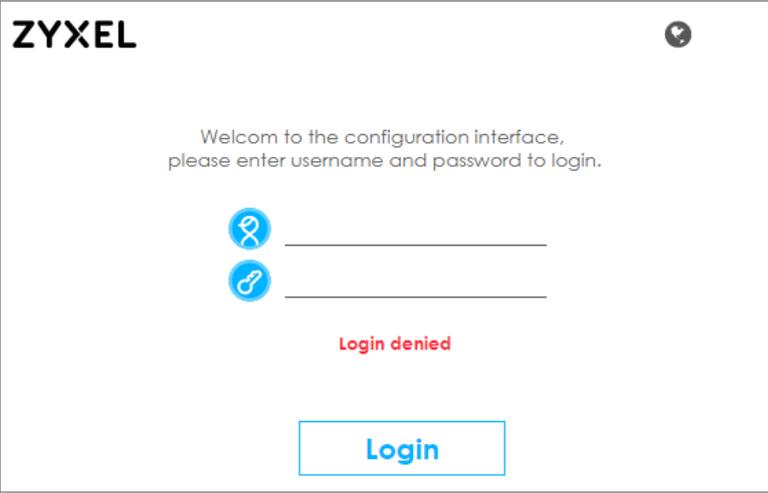
- 2 After entering the username and password correctly, the connected station is able to access the Internet now. There is also a pop-window to show the detail information of the renew time and re-authentication time after authentication succeed.



The screenshot shows the ZYXEL captive portal post-login interface. At the top left is the ZYXEL logo. The main text reads: "csotest, You now have logged in." Below this, there are three lines of text: "Click the logout button to terminate the access session.", "You could renew your lease time by clicking the Renew button.", and "For security reason you must login in again after 24 hours 0 minutes." Below the text, there are three input fields: "User-defined lease time (max 1440 minutes):" with the value "1440" and a "Renew" button; "Remaining time before lease timeout (hh:mm:ss):" with the value "23:58:44"; and "Remaining time before auth. timeout (hh:mm):" with the value "23:58". A "Logout" button is located at the bottom right of the form.

5.2.5 What Could Go Wrong

- 1 The DNS **MUST** be set in the DHCP setting, or the captive portal might fail to redirect because NXC controller is not able to know the correct IP address of the website which stations access to.
- 2 The captive portal fails to redirect the webpage if the station logs in to the NXC controller before and does not logout.
- 3 When you use redirect on AP, the **Forwarding Mode** MUST be **Local bridge** mode.
- 4 If the user enters an incorrect username or password, there is a login failure webpage. Please use the correct username and password to log in again.



The screenshot shows the ZYXEL login page. At the top left is the ZYXEL logo. Below it, the text reads: "Welcom to the configuration interface, please enter username and password to login." There are two input fields: the first is for the username, indicated by a blue icon of a person, and the second is for the password, indicated by a blue icon of a key. Below the input fields, the text "Login denied" is displayed in red. At the bottom, there is a blue "Login" button.

5.3 How to Configure Captive Portal with QR Code?

The example instructs how to set up captive portal authentication with QR code. This new feature offers two convenient and fast methods to access the Internet. The first method is authenticator assisted. This means that the employees are the authenticators, who can authenticate the guest to access the Internet. The second method is self-serviced. The guest can use a mobile device to scan the QR code to pass the authentication.

The Captive portal with QR code can be utilized for some applications including private enterprises, schools, seminars, meetings and guests to access the network through the duration of their visit.

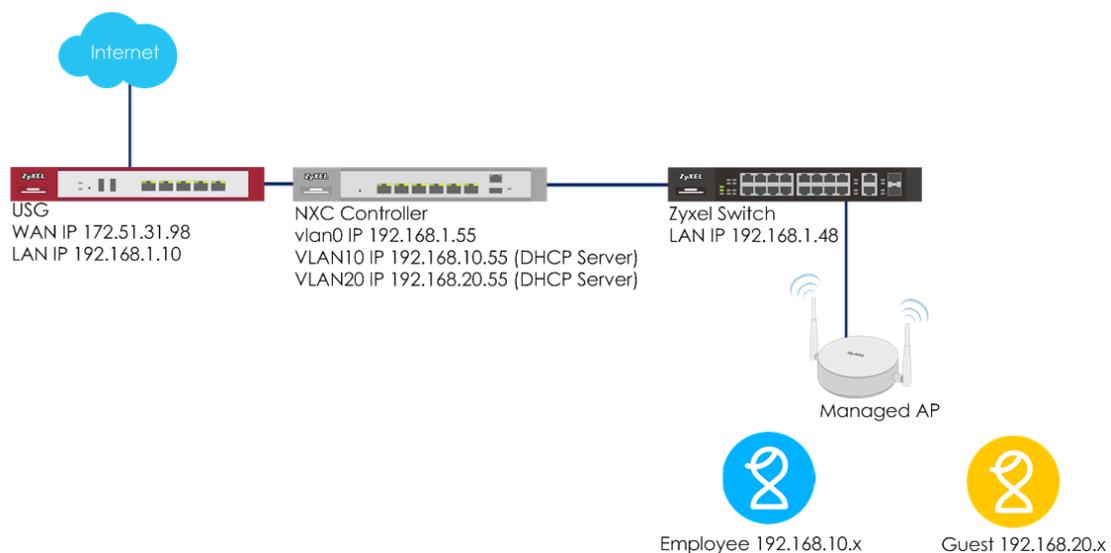


Figure 5.3 Captive portal redirect on AP



Note:

All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC2500 (Firmware Version: 5.30), GS2210-8HP (Firmware Version: V4.30).

5.3.1 Configure AP Profile

- 1 Go to **CONFIGURATION > Object > AP Profile > SSID > SSID List**, and double click **default** to modify the SSID for captive portal. Key in the **SSID** to **CP_QR**, and change **Security Profile** to **default** which sets none security. The VLAN ID is set to 20. Click **OK** to save.

+ Add SSID Profile
 Create new Object ▾

Profile Name:

SSID:

Security Profile:

MAC Filtering Profile:

Layer-2 Isolation Profile:

QoS:

Rate Limiting (Per Station Traffic Rate)

Downlink: (0~160, 0 is unlimited)

Uplink: (0~160, 0 is unlimited)

Band Select:

Forwarding Mode:

VLAN ID: (1~4094)

- 2 Go to **CONFIGURATION > Object > AP Profile > SSID > Security List**, Click **Add** to add the security profile for employees. Key in the **Profile Name** and **SSID** to **employee**. Click **OK** to save.

+ Add Security Profile

General Settings

Profile Name:

Security Mode:

Fast Roaming Settings

802.11r

Radius Settings

Radius Server Type:

MAC Authentication Setting

MAC Authentication

Auth. Method:

Delimiter (Account):

Case (Account):

Delimiter (Calling Station ID):

Case (Calling Station ID):

Fallback to Captive Portal after MAC authentication failure

Authentication Settings

802.1X

Auth. Method:

ReAuthentication Timer: (30~30000 seconds, 0 is unlimited)

- Go to **CONFIGURATION > Object > AP Profile > SSID > SSID List**, double click **Add** to add the SSID for employees. Key in the **Profile Name** and **SSID** to **CP_employee** with **VLAN ID 10**, and change **Security Profile** to **employee**. Click **OK** to save.

+ Add SSID Profile

Create new Object ▾

Profile Name:	CP_employee
SSID:	CP_employee
Security Profile:	employee ▾
MAC Filtering Profile:	disable ▾
Layer-2 Isolation Profile:	disable ▾
QoS:	WMM ▾
Rate Limiting (Per Station Traffic Rate)	
Downlink:	0 <input type="text"/> mbps ▾ (0~160, 0 is unlimited)
Uplink:	0 <input type="text"/> mbps ▾ (0~160, 0 is unlimited)
Band Select:	disable ▾
Forwarding Mode:	Local bridge ▾
VLAN ID:	10 (1~4094)

5.3.2 Configure VLAN

- 1 Go to **CONFIGURATION > Network > Interface > VLAN**, click **Add** to add VLAN 10 and set NXC2500 as the DHCP server of VLAN 10. Click **OK** to save.

+ Add Vlan
 Show Advanced Settings

Interface Properties

Interface Name:

VID: (1~4094)

Zone: i

Description: (Optional)

Member Configuration

✎ Edit

#	Port Name	Member	Tx Tagging
1	ge1	yes	yes
2	ge2	no	no
3	ge3	no	no
4	ge4	no	no
5	ge5	no	no
6	ge6	no	no

IP Address Assignment

Get Automatically

Use Fixed IP Address

IP Address:

Subnet Mask:

Gateway: (Optional)

Metric: (0-15)

DHCP Setting

DHCP:

IP Pool Start Address (Optional): Pool Size:

First DNS Server (Optional):

- Go to **CONFIGURATION > Network > Interface > VLAN**, click **Add** to add VLAN 20 and set NXC2500 as the DHCP server of VLAN 20. Click **OK** to save.

+ Add Vlan

Show Advanced Settings

Interface Properties

Interface Name:

VID: (1~4094)

Zone: i

Description: (Optional)

Member Configuration

Edit

#	Port Name	Member	Tx Tagging
1	ge1	yes	yes
2	ge2	no	no
3	ge3	no	no
4	ge4	no	no
5	ge5	no	no
6	ge6	no	no

IP Address Assignment

Get Automatically

Use Fixed IP Address

IP Address:

Subnet Mask:

Gateway: (Optional)

Metric: (0-15)

DHCP Setting

DHCP:

IP Pool Start Address (Optional): Pool Size:

First DNS Server (Optional):

5.3.3 Create Assistance Account

- 1 Go to **CONFIGURATION > Object > User/Group > User**, and click **Add** to add the user as the assistance account for employees to help the guest pass the authentication when the guest scan the QR code. Click **OK** to save.

- 2 Go to **CONFIGURATION > Object > User/Group > User**, and click **Add** to add the user as the assistance account to let guest self-authenticate. Click **OK** to save.

- 3 Go to **CONFIGURATION > Object > Auth. Method > Authentication Method**, and double click **default** to edit the method as **local**. Click **OK** to save.

#	Method List
1	local

5.3.4 Set Guest Address & Zone

- 1 Go to **CONFIGURATION > Object > Address > Address**, click **Add** to add the guest address. Change the **Address Type** to **RANGE** and enter the starting and end IP address. Click **OK** to save.

Edit Address Rule QR_Guest_addr

Name:

Address Type:

Starting IP Address:

End IP Address:

- 2 Go to **CONFIGURATION > Network > Zone**, click **LAN** to edit. Change **vlan0, vlan10, vlan20** to the same zone and then the employee's account can help to do captive portal authentication. Click **OK** to save.

Edit Zone

Group Members

Name:

Block Intra-zone Traffic i

Member List

Available		Member
=== Interface ===		
ge1		vlan0
ge2		vlan10
ge3		vlan20
ge4		
ge5		
ge6		

5.3.5 Configure Captive Portal

- 1 Go to **CONFIGURATION > Captive Portal > Redirect on Controller > Authentication Policy Rule**, click **add** to create a policy rule for guests whose IP addresses are in the setting range.

In **User Auth Policy**, change **Source Address** to **QR_Guest_addr** and **Authentication** is **required**. Check **Force User Authentication** to force every connected IP in the range to be redirected to captive portal. Change the **Authentication Method** to **default**.

In **Authentication Type**, use the **Internal Web Portal**.

The screenshot shows the 'Auth. Policy Add' configuration window. It is divided into three main sections: 'General Settings', 'User Auth Policy', and 'Authentication Type'. In the 'General Settings' section, the 'Enable Policy' checkbox is checked, and the 'Description' field is set to 'QR_Redirect'. The 'User Auth Policy' section includes 'Source Address' (QR_Guest_addr), 'Destination Address' (any), 'Schedule' (none), 'Authentication' (force), and 'Authentication Method' (default). The 'Authentication Type' section has 'Internal Web Portal' selected, with 'Enable Domain Name Redirect Link by FQDN' checked and 'Portal Theme' set to 'Controller_default'.

Section	Field	Value
General Settings	Enable Policy	<input checked="" type="checkbox"/>
	Description	QR_Redirect (Optional)
User Auth Policy	Source Address	QR_Guest_addr (RANGE: 192.168.20.100-192.168.20.110)
	Destination Address	any
	Schedule	none
	Authentication	force
	Authentication Method	default
Authentication Type	Internal Web Portal	<input checked="" type="radio"/>
	Enable Domain Name Redirect Link by FQDN	<input checked="" type="checkbox"/>
	Portal Theme	Controller_default
External Web Portal		<input type="radio"/>

- In the same page of step 1. Check the Authentication with QR code, and change the Guest Account to QR_Guest. Check **Authenticator-assisted** and the **QR Portal Address** is vlan10 interface IP. The **Authenticator** is the employee account or group. Click **Apply**.

QR Code

Authentication with QR code

Guest Account: i

Authenticator-assisted

QR Portal Address: i

Authenticator:

Self-serviced

QR Portal Address: i

Note Message:

QR Code

- Go to **CONFIGURATION > Captive Portal > Captive Portal**. Check **Enable Captive Portal**. Click **Apply**.

Captive Portal
Custom Captive Portal

General Settings

Enable Captive Portal

- 4 Go to **CONFIGURATION > Captive Portal > Redirect on Controller > QR Code Configuration**. Check **Print Out QR Code** and use the QR code for customer to do self-service.

QR Code

Authentication with QR code

Guest Account: 

Authenticator-assisted

QR Portal Address: 

Authenticator:

Self-serviced

QR Portal Address: 

Note Message:

QR Code



5.3.6 Broadcast SSID

- 1 Go to **CONFIGURATION > Wireless > AP Management > AP Group**, click **default** to **Edit**. Change **#1** to **CP_QR** and **#2** to **CP_employee**.

The screenshot displays the 'Edit AP Group Profile default' configuration page. It is divided into two sections: 'Radio 1 Setting' and 'Radio 2 Setting'. Each section includes radio mode selection (AP Mode is selected), AP Profile selection, and Max Output Power (30 dBm). Below these settings are 'Edit' buttons and tables of SSID profiles. In both tables, the first two rows are highlighted with red boxes: row 1 is 'CP_QR' and row 2 is 'CP_employee'. Rows 3 through 8 in both tables are labeled 'disable'.

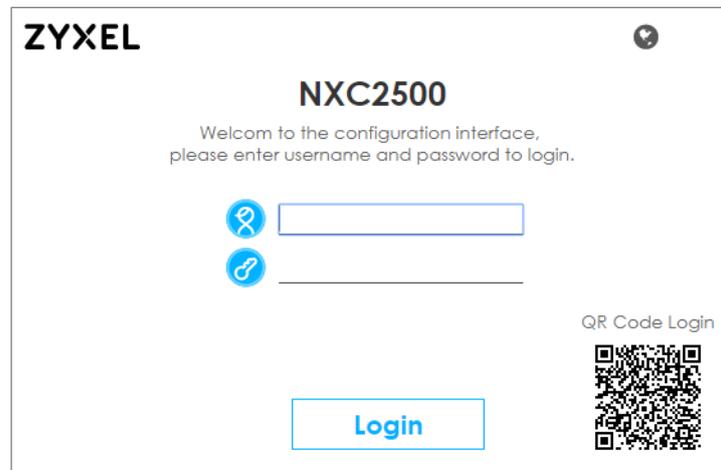
#	SSID Profile
1	CP_QR
2	CP_employee
3	disable
4	disable
5	disable
6	disable
7	disable
8	disable

#	SSID Profile
1	CP_QR
2	CP_employee

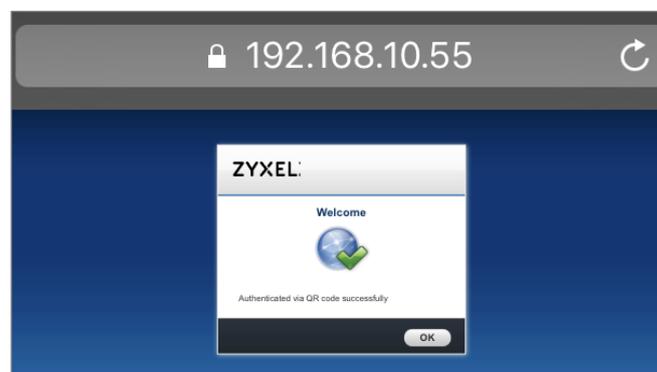
5.3.7 Test the Result

1 Authenticator-assisted

- i. When the guests connect to the SSID 'CP_QR', they get IP addresses between 192.168.20.100 to 192.168.20.110, and are redirected to captive portal with QR code as shown below.

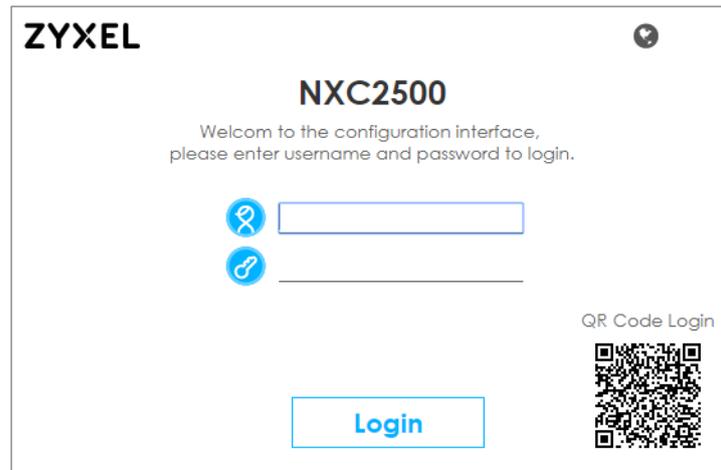


- ii. When the captive portal page is shown, the customer asks for an employee who has connected with SSID "CP_employee" and gets the employee's help to scan the QR code. After the employee scans the QR code, there's a welcome page. The customer is able to access the Internet after the welcome page display.

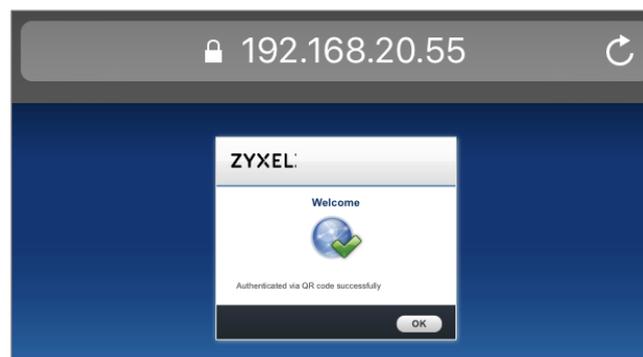


2 Self-serviced

- i. When the guests connect to the SSID 'CP_RQ', they get an IP addresses between 192.168.20.100 to 192.168.20.110, and is redirected to captive portal with QR code as shown below.

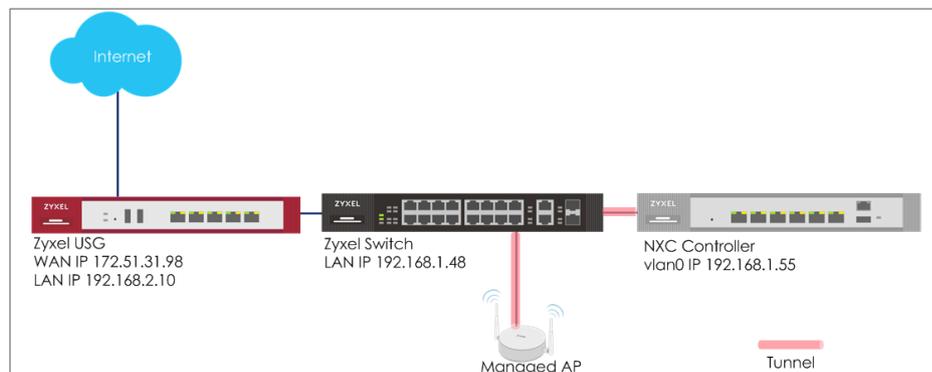


- ii. When the captive portal page is shown, the guest scans the printed QR code in the last step. After scanning the QR code, a welcome page display and the guest is able to access the Internet.

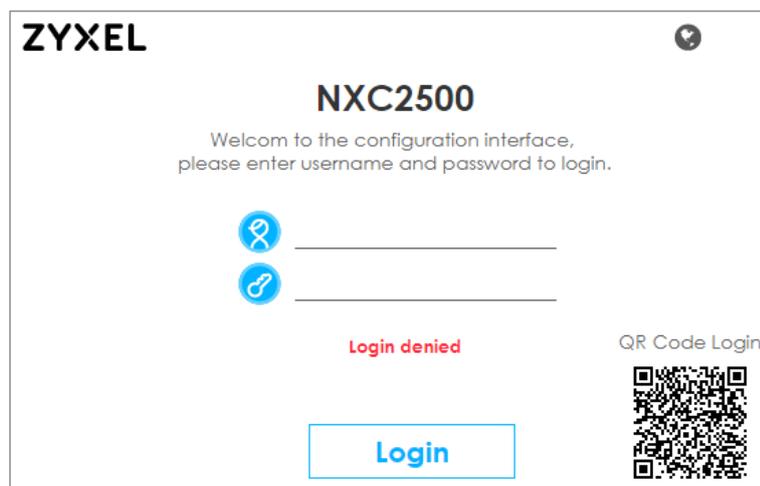


5.3.8 What Could Go Wrong

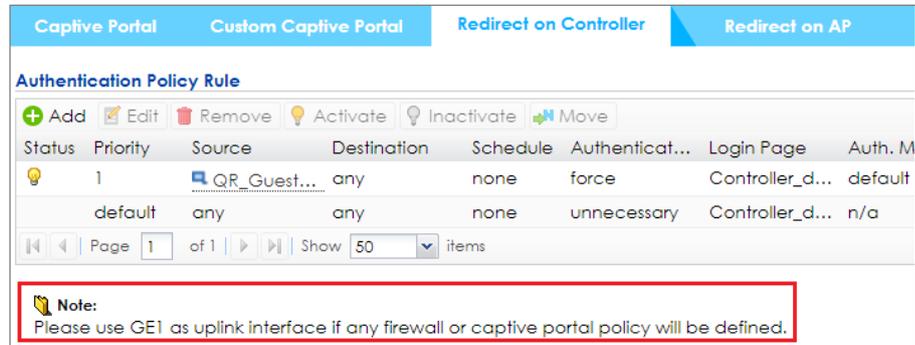
- 1 The DNS **MUST** be set in the DHCP server, or the captive portal might fail to redirect because NXC controller is not able to know the correct IP address of the website which stations want to access.
- 2 The captive portal fails to redirect the webpage if the station logs in to the NXC controller before and does not logout.
- 3 When USG is the gateway as shown in the topology below, the **Forwarding Mode** MUST be **Tunnel** mode to make sure the traffic from AP goes to NXC controller.



- 4 If the user enters an incorrect username or password, there is a login failure webpage. Please click **Retry** and use the correct username and password to log in.



- 5 When using the NXC2500 as the controller, the uplink port MUST be ge1.



The screenshot shows the ZyXel web interface for configuring an Authentication Policy Rule. The interface has four tabs: 'Captive Portal', 'Custom Captive Portal', 'Redirect on Controller', and 'Redirect on AP'. The 'Authentication Policy Rule' section is active, displaying a table with columns for Status, Priority, Source, Destination, Schedule, Authentication, Login Page, and Auth. M. There are two rows of data. A red box highlights a note at the bottom of the interface: 'Note: Please use GE1 as uplink interface if any firewall or captive portal policy will be defined.'

Status	Priority	Source	Destination	Schedule	Authenticat...	Login Page	Auth. M
🔦	1	QR_Guest...	any	none	force	Controller_d...	default
	default	any	any	none	unnecessary	Controller_d...	n/a

Note:
Please use GE1 as uplink interface if any firewall or captive portal policy will be defined.

5.4 How to Configure Captive Portal with External Webserver?

The example instructs how to set up captive portal redirect via the external web page. A captive portal can intercepts network traffic, according to the authentication policies, until the user authenticates his or her connection, usually through a specifically designated login web page. Typically, you often find captive portal pages in public hotspots. Here is an example when the customer wants to use an external captive portal for wireless client's authentication.

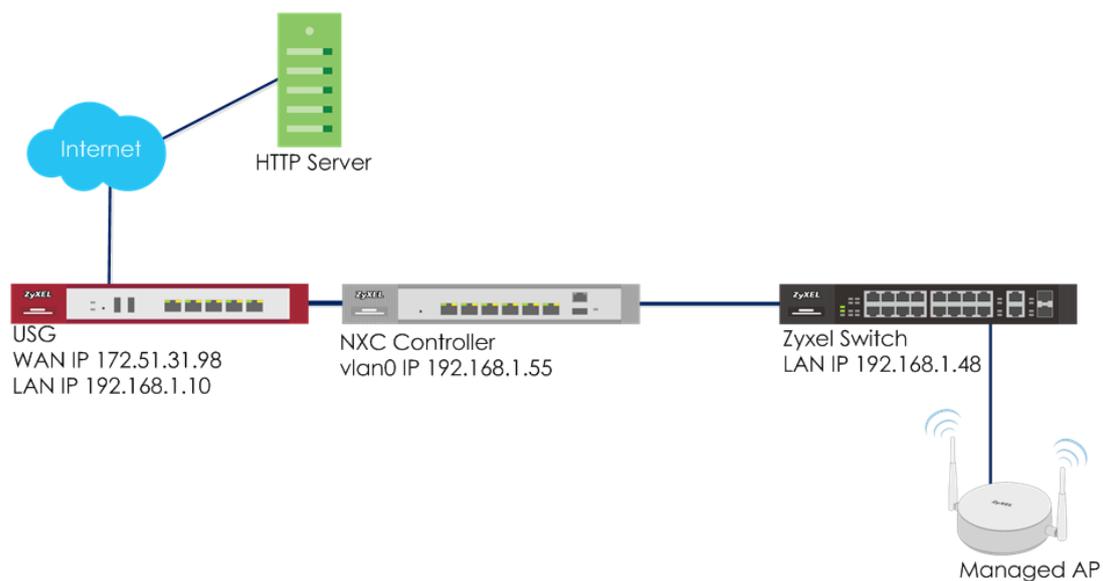


Figure 5.4 Captive Portal with External Webserver

 **Note:**

All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC2500 (Firmware Version: 5.30), GS2210-8HP (Firmware Version: V4.30).

5.4.1 Configure Interface

- 1 Go to **CONFIGURATION > Network > Interface > VLAN**, click **vlan0** and edit it. Remove ge6 by selecting “no” in the **Member Configuration**. Set a fixed IP for the interface, and use DHCP server with DNS. Click **OK** to save.

✎ **Edit Vlan vlan0**

📖 Show Advanced Settings

Interface Properties

Interface Name: vlan0

VID: 1

Zone: LAN ▼ i

Description: (Optional)

Member Configuration

✎ Edit

#	Port Name	Member	Tx Tagging
1	ge1	yes	no
2	ge2	yes	no
3	ge3	yes	no
4	ge4	yes	no
5	ge5	yes	no
6	ge6	no	no

IP Address Assignment

Get Automatically

Use Fixed IP Address

IP Address:

Subnet Mask:

Gateway: (Optional)

Metric: (0-15)

DHCP Setting

DHCP:

IP Pool Start Address (Optional): Pool Size:

First DNS Server (Optional):

- 2 Go to **CONFIGURATION > Network > Interface > Ethernet**, select **ge6** and **Edit** it. Change the **Interface Type** to **external**. Click **OK** to save.

Edit Ethernet

Show Advanced Settings

General Settings

Enable Interface

Interface Properties

Interface Type:	external	
Interface Name:	ge6	
Port:	P6	
PVID:	1 (1~4094)	
Zone:	none	
MAC Address:	B0:B2:DC:6E:AB:66	
Description:		(Optional)

IP Address Assignment

Get Automatically

Use Fixed IP Address

- Go to **CONFIGURATION > Network > Policy Route**, click **Add** to add a routing rule for outgoing traffic. Click **Show Advanced Settings**. Check **Enable** in **Configuration**. Select **Interface** in **Incoming** and select to **vlan0** in **Please select one member**. Change **Type** to **Interface** and select **Interface ge6**. Change **Source Network Address Translation** to **outgoing-interface**. Click **OK**.

+ Add Policy Route

Hide Advanced Settings Create new Object ▾

Configuration

Enable

Description: (Optional)

Criteria

User: ▾

Incoming: Interface ▾

Please select one member: vlan0 ▾

Source Address: ▾

Destination Address: ▾

DSCP Code: ▾

Schedule: ▾

Service: ▾

Source Port: ▾

Next-Hop

Type: Interface ▾

Interface: ge6 ▾

Auto-Disable

DSCP Marking

DSCP Marking: ▾

Address Translation

Source Network Address Translation: outgoing-interface ▾

5.4.2 Configure Authentication Method Setting & Address

- 1 Go to **CONFIGURATION > Object > User/Group**, click **add** to create a new user ID and password. Stations can log in to the captive portal to access the Internet via this account. Enter the **User Name** as login ID for captive portal and **User Type** is **guest**. Enter the **Password** as the login password. The default of **Authentication Timeout Setting** is 1440 minutes, and usually it's shorter for guests. Select **Use Manual Settings** to set **Lease Time** and **Reauthentication Time**. Click **OK** to save.

- 2 Go to **CONFIGURATION > Object > Auth. Method**, click **add** to create an authentication method. Enter the **Name** of this authentication method and select local in the **Method List**.

#	Method List
1	local

- 3 Go to CONFIGURATION > Object > Address > Address, click **add** to create an address range which needs to do captive portal authentication before accessing to the Internet. Enter profile **Name** and change **Address Type** to **RANGE**. In this example, the IP range for guest is **192.168.1.199** to **192.168.1.209**. Click **OK** to save.

+ Add Address Rule

Name:	<input type="text" value="CP_ex"/>
Address Type:	<input type="text" value="RANGE"/> ▼
Starting IP Address:	<input type="text" value="192.168.1.199"/>
End IP Address:	<input type="text" value="192.168.1.209"/>

5.4.3 Configure Captive Portal

- 1 Go to **CONFIGURATION > Captive Portal > Redirect on Controller > Authentication Policy Rule**, click **add** to create a policy rule.

In **User Auth Policy**, change **Source Address** to **CP_ex** and **Authentication** is **required**. Check **Force User Authentication**, and change the **Authentication Method** to **default**. Click **OK** to save.

Auth. Policy Add
 Create new Object ▾

General Settings

Enable Policy
 Description: (Optional)

User Auth Policy

Source Address: **CP_ex** RANGE, 192.168.1.199-192.168.1.209
 Destination Address: any
 Schedule: none
 Authentication: **force**
 Authentication Method: **default**

- 2 In the same setting page as previous step, click the “Download” hyperlink to download the external web portal example. You can use the downloaded example to add in the http server as the external webpage.

Authentication Type

Internal Web Portal
 Enable Domain Name Redirect Link by FQDN: ⓘ
 Portal Theme: Controller_default ▾

External Web Portal

Login URL: **http://192.168.2.134/lo**
 Logout URL: http://192.168.2.134/lo Optional
 Welcome URL: http://192.168.2.134/w Optional
 Session URL: http://192.168.2.134/se Optional
 Error URL: http://192.168.2.134/er Optional
 User-logout URL: http://192.168.2.134/us Optional

[Download](#) the external web portal example.

- 3 Go to **CONFIGURATION > Captive Portal > Captive Portal**, check **Enable Captive Portal**. Click **Apply** to apply the settings.

Captive Portal	Custom Captive Portal
General Settings	
<input checked="" type="checkbox"/> Enable Captive Portal	

5.4.4 Configure AP Profile

- 1 Go to **CONFIGURATION > Object > AP Profile > SSID > SSID List**, double click **add** to add a SSID for wireless connection with external captive portal. Key in the **SSID** to **CP_ex**, and change **Security Profile** to **default** which sets none security. Click **OK** to save.

- 2 Go to **CONFIGURATION > Wireless > AP Management > AP Group**, click **default** to **Edit**. change **#1** to **CP_ex**. Click **Override Member AP Setting** to apply the SSID to AP and click **Yes** in the pop-up window. Click **OK**.

- 3 **Logout** from NXC controller.

5.4.5 Test the Result

- 1 Connect the station to the SSID 'CP_ex'. Open a browser and visit a website after the computer and AP connect successfully. The browser redirects the webpage to external captive portal page and the user needs to enter the username and password for authentication before accessing the Internet.



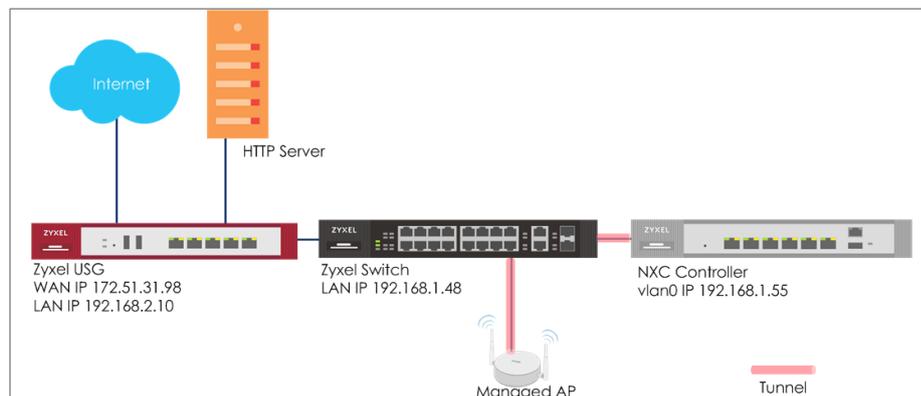
The screenshot shows a web browser window displaying the ZyXel captive portal login page. At the top, the ZyXel logo is visible. Below the logo, the text "Enter User Name / Password and click to login." is displayed. There are two input fields: one for the "User Name" containing the text "csotest" and one for the "Password" containing seven dots. A "Login" button is located at the bottom right of the form.

- 2 After entering the username and password correctly, there's a successful webpage. The connected station is able to access the Internet now.

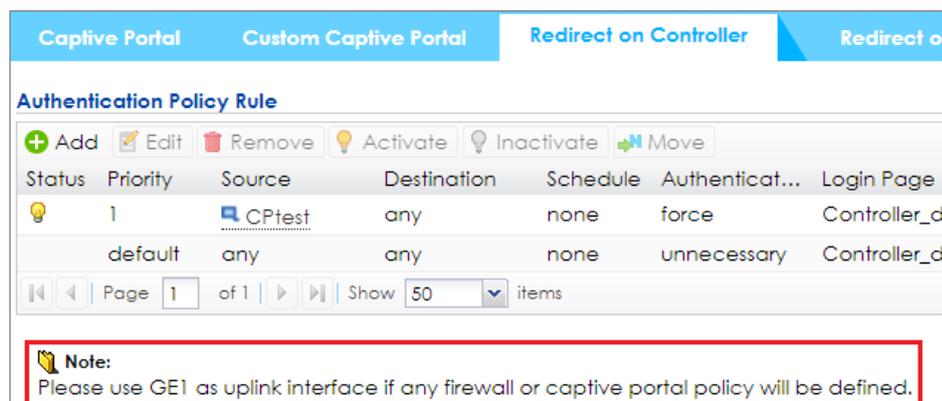


5.4.6 What Could Go Wrong

- 1 The DNS **MUST** be set in the DHCP server, or the captive portal might fail to redirect because NXC controller is not able to know the correct IP address of the website which stations want to access.
- 2 The captive portal fails to redirect the webpage if the station is log in to the NXC controller before and does not logout.
- 3 When USG is the gateway as shown in the topology below, the **Forwarding Mode** MUST be **Tunnel** mode to make sure the traffic from AP goes to NXC controller.



- 4 When using the NXC2500 as the controller, the uplink port MUST be ge1.



5.5 How to Configure Multiple Captive Portals for different users?

The example instructs how to set up different portal pages with different authentication policies and different authentication method. When there are different applications that all needs to use captive portal authentication, different portal pages and different authentication methods will be needed. Users are able to setup or upload multiple customized themes to the NXC controller. For each policy rule, users are able to select the login page and auth. method.

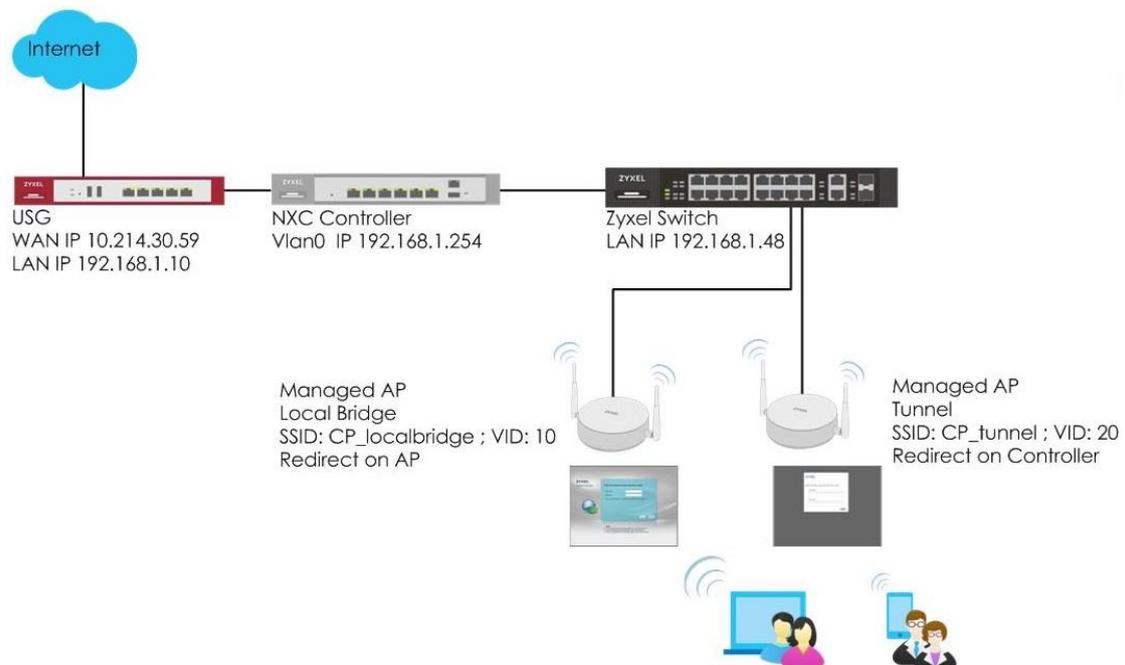


Figure 5.5 multiple captive portal for different users



Note:

All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC2500 (Firmware Version: 5.30), GS2210-8HP (Firmware Version: V4.30).



Note:

Some Zyxel APs are not supported tunnel mode, they only support localbridge mode.

- NWA5120 series (5121-NI / 5123-NI / 5121-N) / NWA5301-NJ / WAC5302D-S / NWA5123-AC-HD

5.5.1 Configure AP Profile and User

- 1 Go to **CONFIGURATION > Object > AP Profile > SSID > SSID List**, click **Add** to add two SSIDs for captive portal. Key-in the **SSID names** are **CP_localbridge** and **CP_tunnel**, and select **Security Profile** to **default** which sets none security. Click **OK** to save.

Profile Name:	<input type="text" value="CP_loadbridge"/>
SSID:	<input type="text" value="CP_loadbridge"/>
Security Profile:	default
MAC Filtering Profile:	disable
Layer-2 Isolation Profile:	disable
QoS:	WMM
Rate Limiting (Per Station Traffic Rate)	
Downlink:	<input type="text" value="0"/> <input type="text" value="mbps"/> (0~160, 0 is unlimited)
Uplink:	<input type="text" value="0"/> <input type="text" value="mbps"/> (0~160, 0 is unlimited)
<input type="checkbox"/> Band Select	
Forwarding Mode:	Local bridge
VLAN ID:	<input type="text" value="10"/> (1~4094)

Profile Name:	<input type="text" value="CP_tunnel"/>
SSID:	<input type="text" value="CP_tunnel"/>
Security Profile:	default
MAC Filtering Profile:	disable
Layer-2 Isolation Profile:	disable
QoS:	WMM
Rate Limiting (Per Station Traffic Rate)	
Downlink:	<input type="text" value="0"/> <input type="text" value="mbps"/> (0~160, 0 is unlimited)
Uplink:	<input type="text" value="0"/> <input type="text" value="mbps"/> (0~160, 0 is unlimited)
<input type="checkbox"/> Band Select	
Forwarding Mode:	Tunnel
VLAN Interface:	<input type="text" value="vlan20"/> VID: 20

- Go to **CONFIGURATION > Object > User/Group**, and click **add** to create a new user ID and password. Stations can log in captive portal to access Internet via this account. Enter the **User Name** as login ID for captive portal and **User Type** is **guest**. Enter the **Password** as the login password. The default of **Authentication Timeout Setting** is 1440 minutes, and usually it's shorter for guests. Select to **Use Manual Settings** to set **Lease Time** and **Reauthentication Time**. Click **OK** to save.

+ Add A User

User Configuration

User Name :

User Type:

Password:

Retype:

Description:

Authentication Timeout Settings: Use Default Settings Use Manual Settings

Lease Time: 1440 minutes

Reauthentication Time: 1440 minutes

- Go to **CONFIGURATION > Object > Auth. Method**, and click **add** to create an authentication method. Enter the **Name** of this authentication method and select to local in the **Method List**.

+ Add Authentication Method

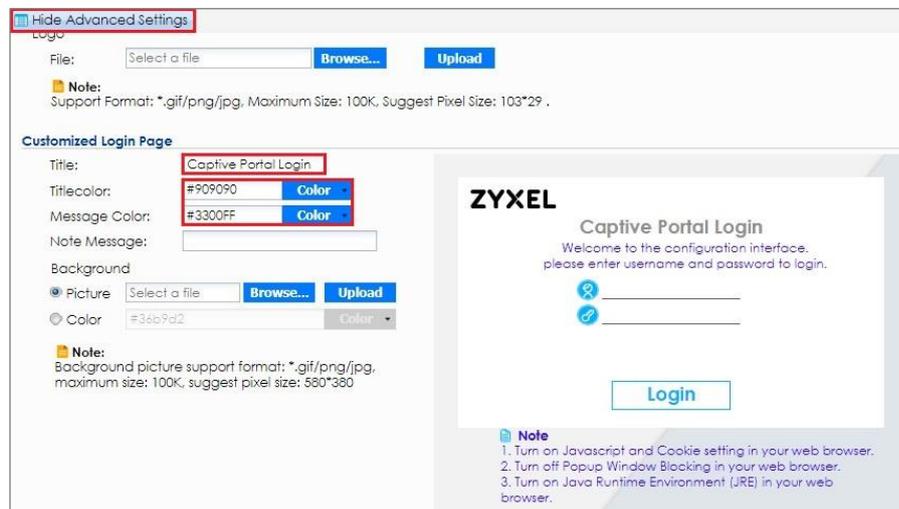
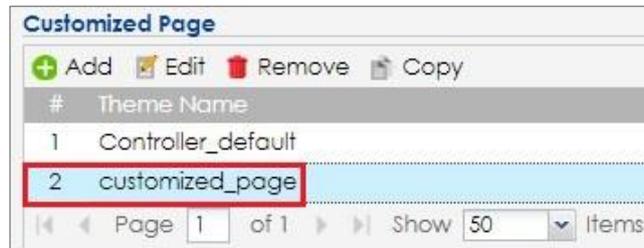
General Settings

Name:

#	Method List
1	local

5.5.2 Configure Captive Portal

- 1 Go to **CONFIGURATION > Custom Captive Portal > customized page.**



- Go to **CONFIGURATION > Captive Portal > Redirect on AP > Authentication Policy Rule**, and click **add** to create a policy rule for stations which connect to SSID profile **CP_localbridge**. In **General Settings**, check **Enable Policy** and enter the **Theme Name** of this policy.
In **User Auth Policy**, change **SSID** to **CP_localbridge** and **Authentication** is **Force**, and change the **Authentication Method** to **localtest**. Click **OK** to save.

General Settings

Enable Policy

Theme Name:

Description: (Optional)

User Auth Policy

SSID:

Source Address:

Destination Address:

Schedule:

Authentication:

Authentication Method:

Authentication Type

Internal Web Portal

Portal Theme:

- Go to **CONFIGURATION > Captive Portal > Redirect on AP > Authentication Policy Group**. In the setting, click **Add** to add the policy rule which is created in previous step.

General Settings

Profile Name:

Description: (Optional)

+ Add Edit Remove Move

#	Name
1	Redirect_on_AP

Page 1 of 1 Show 50 Items Displaying 1 - 1 of 1

- Go to **CONFIGURATION > Captive Portal > Redirect on Controller > Authentication Policy Rule**, click **add** to create a policy rule for stations which get an SUBNET from 192.168.20.x. In **General Settings**, check **Enable Policy** and enter the **Description** of this policy. In **User Auth Policy**, change **Source Address** to **vlan20** and **Authentication** is **Force**. Check **Force User Authentication**, and change the **Authentication Method** to **localtest**. Click **OK** to save.

General Settings

Enable Policy

Description: (Optional)

User Auth Policy

Source Address: **vlan20** SUBNET, 192.168.20.0/24

Destination Address: any

Schedule: none

Authentication: **force**

Authentication Method: **localtest**

Authentication Type

Internal Web Portal

Enable Domain Name Redirect Link by FQDN: ⓘ

Portal Theme: **Uploaded_default**

- Go to **CONFIGURATION > Captive Portal > Captive Portal**, check **Enable Captive Portal**. Click **Apply** to apply the settings.

Captive Portal Custom Captive Portal

General Settings

Enable Captive Portal

5.5.3 Broadcast SSID

- 1 Go to **CONFIGURATION > Wireless > AP Management > AP Group**, click Add two SSIDs: Localbridge and Tunnel.

Group Name: (Optional)

Description: (Optional)

Location: (Optional)

Radio 1 Setting

OP Mode AP Mode MON Mode Root AP Repeater AP

Radio 1 AP Profile: (Optional)

Max Output Power: dBm (0~30)

#	SSID Profile
1	CP_tunnel
2	disable
3	disable
4	disable
5	disable
6	disable
7	disable
8	disable

Radio 2 Setting

OP Mode AP Mode MON Mode Root AP Repeater AP

Radio 2 AP Profile: (Optional)

Max Output Power: dBm (0~30)

#	SSID Profile
1	CP_tunnel

General Settings

Group Name:

Description: (Optional)

Location: (Optional)

Radio 1 Setting

OP Mode AP Mode MON Mode Root AP Repeater AP

Radio 1 AP Profile:

Max Output Power: dBm (0~30)

Edit

#	SSID Profile
1	CP_loadbridge
2	disable
3	disable
4	disable
5	disable
6	disable
7	disable
8	disable

Radio 2 Setting

OP Mode AP Mode MON Mode Root AP Repeater AP

Radio 2 AP Profile:

Max Output Power: dBm (0~30)

Edit

#	SSID Profile
1	CP_loadbridge

- 2 In the same setting page as previous step, select **CP_LB** for **Auth. Policy Group** in **Portal Redirect on AP**. Click **OK** to save.

Portal Redirect on AP

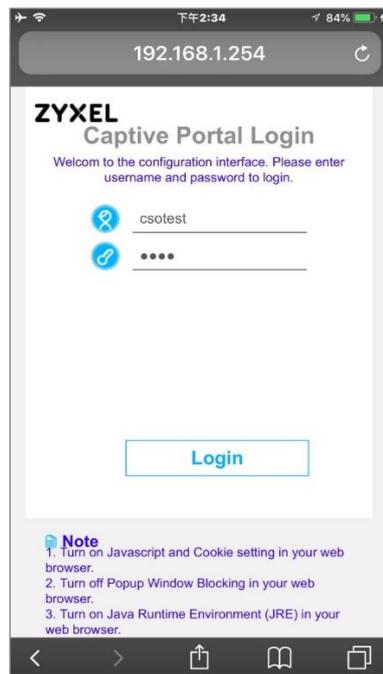
Auth. Policy Group:

Skip authentication to provide contingency access while controller is unreachable.

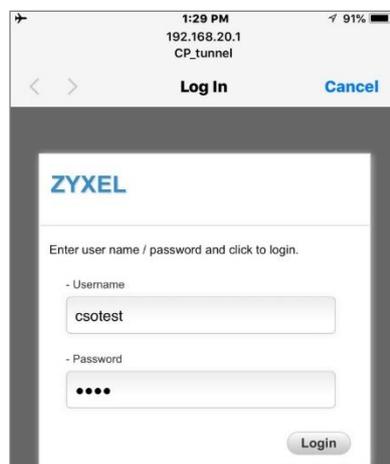
- 3 **Logout** from NXC controller.

5.5.4 Test the Result

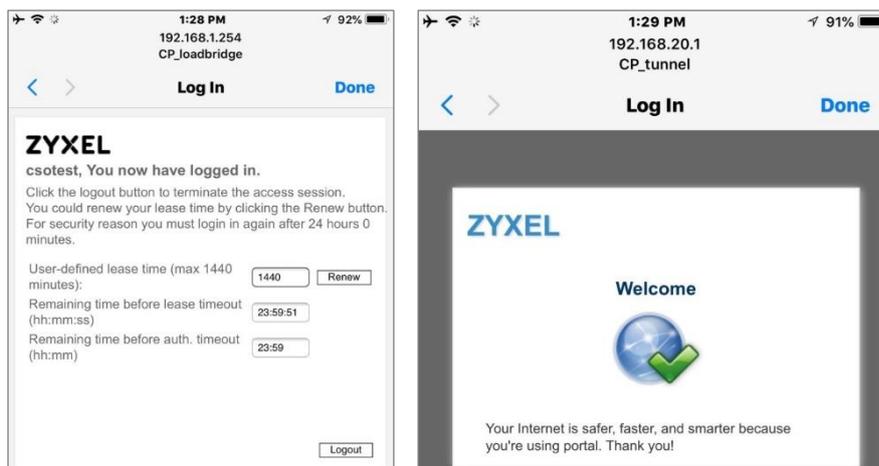
- 1 Connect the station to the SSID 'CP_localbridge'. The browser redirects the webpage to captive portal page and the user needs to enter the username and password for authentication before accessing the Internet.



- 2 Connect the station to the SSID 'CP_tunnel'. The browser redirects the webpage to captive portal page and the user needs to enter the username and password for authentication before accessing the Internet.



- 3 After entering the username and password correctly, the connected station is able to access the Internet now. There is also a pop-window to show the detail information of the renew time and re-authentication time after authentication succeed or a successful welcome page.



5.5.5 What Could Go Wrong

- 1 The DNS **MUST** be set in the DHCP setting, or the captive portal might fail to redirect because NXC controller is not able to know the correct IP address of the website which stations access to.
- 2 The captive portal fails to redirect the webpage if the station logs in to the NXC controller before and does not logout.
- 3 When you use redirect on AP, the **Forwarding Mode** MUST be **Local bridge** mode.
- 4 If the user enters an incorrect username or password, there is a login failure webpage. Please use the correct username and password to log in again.

Secure the Wireless Environment – Others

6.1 How to Configure MAC Authentication?

The example instructs how to set up MAC authentication. Authenticate the wireless client by its MAC address instead of using username and password to authenticate the wireless.

In the classroom, the teachers' devices are trusted on the controller; they can pass MAC authentication directly and are regarded as MAC user roles on controller.

In this topology, we set the NXC as an authenticated server to save the devices' MAC addresses. The gateway USG is a DHCP server.

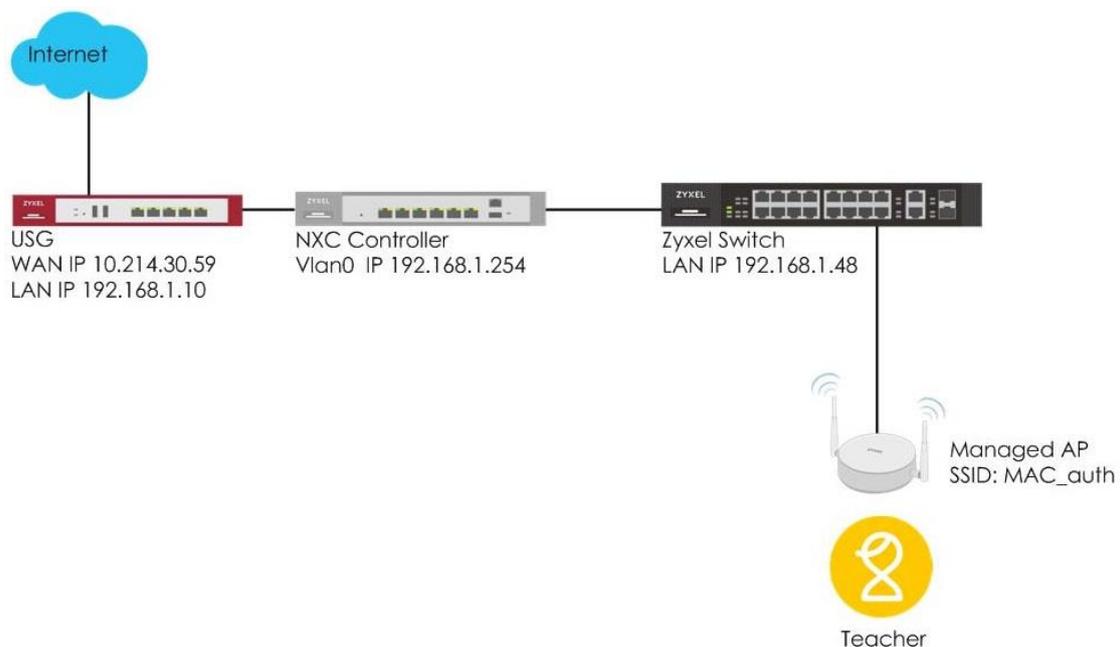


Figure 6.1 MAC Authentication



Note:

All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC2500 (Firmware Version: 5.30), GS2210-8HP (Firmware Version: V4.30).

6.1.1 Configure AP Profile

- 1 Go to **CONFIGURATION > Object > AP Profile > SSID > Security > Add**. Create a new security profile which sets none security and enables **MAC Authentication**.

+ Add Security Profile

General Settings

Profile Name: Zyxel_MAC

Security Mode: none

Radius Settings

Radius Server Type: Internal

MAC Authentication Setting

MAC Authentication

Auth. Method: default

Delimiter (Account): colon (:)

Case (Account): upper

Delimiter (Calling Station ID): colon (:)

Case (Calling Station ID): upper

- 2 Go to **CONFIGURATION > Object > AP Profile > SSID > SSID List**, Create the SSID profile with the security profile.

+ Add SSID Profile

Create new Object ▾

Profile Name: MAC_auth

SSID: MAC_auth

Security Profile: Zyxel_MAC

MAC Filtering Profile: disable

Layer-2 Isolation Profile: disable

QoS: WMM

6.1.2 Configure User/Group Profile

- 1 Go to **CONFIGURATION > Object > User/Group > MAC Address > MAC Authentication**. Add the teacher's MAC address for MAC authentication in the NXC local server.

Add MAC Auth Address

MAC Address/OUI: 7C:01:91:6C:01:10

MAC Role: mac-users

Save it into local DataBase

Description: Teacher's Mobile

OK Cancel

User	Group	Setting	MAC Address
MAC Authentication			
+ Add Edit Remove			
#	MAC Address / OUI	MAC Type	
1	7C:01:91:6C:01:10	int-mac-address	

6.1.3 Configure Authentication Method Setting

- 1 Go to **CONFIGURATION > Object > Auth. Method**, click **Add** to create an authentication method. Enter the **Name** of this authentication method and select to local in the **Method List**.

+ Add Authentication Method

General Settings

Name:

+ Add Edit Remove Move

#	Method List
1	local

OK Cancel

Authentication Method

Configuration

+ Add Edit Remove Object References

#	Method Name	Method List
1	default	local
2	localtest	local

6.1.4 Configure AP Group Profile

- 1 Go to **CONFIGURATION > Wireless > AP Management > AP Group > Group Summary > Radio setting**. Set the SSID profile to the AP radio.

Radio 1 Setting

OP Mode AP Mode MON Mode Root AP Repeater AP ?

Radio 1 AP Profile: default

Max Output Power: 30 dBm (0~30)

Edit

#	SSID Profile
1	MAC_auth
2	disable
3	disable
4	disable
5	disable
6	disable
7	disable
8	disable

Radio 2 Setting

OP Mode AP Mode MON Mode Root AP Repeater AP ?

Radio 2 AP Profile: default2

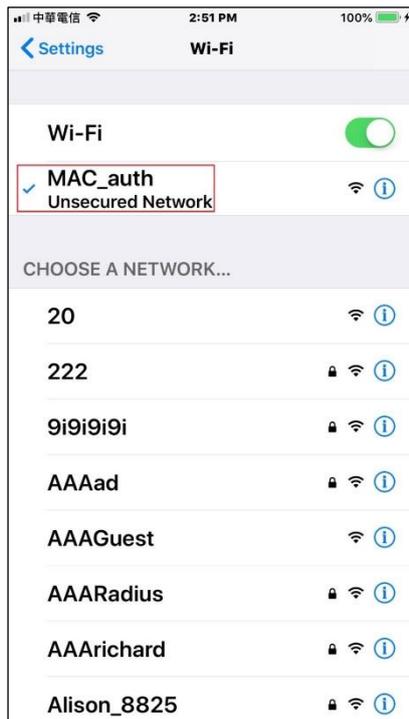
Max Output Power: 30 dBm (0~30)

Edit

#	SSID Profile
1	MAC_auth
2	disable
3	disable
4	disable

6.1.5 Test the Result

- 1 Use the teacher's trusted device and connect to the SSID: **MAC_auth**. The device successfully passes the MAC authentication and is allowed to access the Internet directly.



- 2 Go to **MONITOR > Wireless > Station Info**. Check the station information on the NXC.

Trusted MAC Address List						
#	User ID	SSID Profile Name	SSID	MAC Address	First Login Time	Validate Time
1	Student-1	MAC_CP	MAC_CP	EC:55:F9:4EB1:78	2018-08-08 09:19:16	2018-08-08 14:19:16

- Go to **MONITOR > System Status > Login Users > Login Users**.
Check the logged in users on the NXC and find the teacher's device information.

Station List						
Show Advanced Settings						
Station List						
#	IP Address	Associated AP	SSID Name	Tx Rate	Rx Rate	
1	192.168.1.102	AP-5C6A80EBA...	MAC_auth	270M	24M	

Login Users						
Dynamic Guest						
Trusted MAC Address List						
Current User List						
<p>Note: MAC information is just for login users by 802.1X and MAC auth.</p> <p>Force Logout</p>						
#	User ID	Reauth/Leas...	Associated AP	Type	IP Address	MAC Address
1	7C:01:91:6C:01:10	unlimited / u...	AP-5C6A80E...	mac-auth	192.168.1.102	7C-01-91-6C-01-10

6.2 MAC Authentication fallback to Captive Portal?

The example instructs how to set up MAC authentication fallback to captive portal. User can decide NXC whether cache the trusted client's mac address or not. If user decides NXC not to cache the trusted client's MAC address, it will work as captive portal. If user enters the trusted client's mac address on the authenticated server before, it will work as MAC authentication.

In the classroom, the teachers and students all use Wi-Fi service but have different privileges and restrictions. The teachers' devices are trusted on the controller; they can pass MAC authentication directly and are regarded as MAC user roles on controller. The students' devices need to pass captive portal authentication with their own IDs/passwords. They are regarded as portal user roles on controller.

In this topology, we set the NXC as an authenticated server to save the devices' MAC addresses and clients' names and passwords. The gateway USG is a DHCP server.

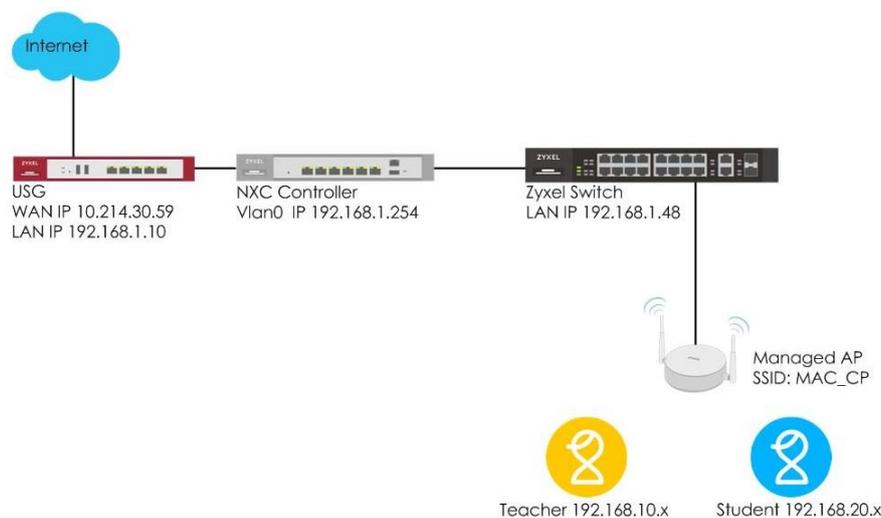


Figure 6.2 MAC Authentication fallback to captive portal



Note:

All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC2500 (Firmware Version: 5.30), GS2210-8HP (Firmware Version: V4.30).

6.2.1 Configure AP Profile

- 1 Go to **CONFIGURATION > Object > AP Profile > SSID > Security > Add**. Create a new security profile which sets none security and enables **MAC Authentication** and **Fallback to captive Portal after MAC authentication failure**.

- 2 Go to **CONFIGURATION > Object > AP Profile > SSID > SSID List**, Create the SSID profile with the security profile.

6.2.2 Configure User/Group Profile

- 1 Go to **CONFIGURATION > Object > User/Group > User > Add**. Click **Add** to create a new user ID and password. Stations can log in captive portal to access the Internet via this account. Add the student's name and password for captive portal authentication in the NXC local server. **User Type** is **guest**. Enter the **Password** as the login password. The default of **Authentication Timeout Setting** is 1440 minutes, and usually it's shorter for guests. Select to **Use Manual Settings** to set **Lease Time** and **Reauthentication Time**. Click **OK** to save.

Add A User

User Configuration

User Name : Student-1

User Type: guest

Password: ****

Retype: ****

Description: Local User

Authentication Timeout Settings

Lease Time: 1440 minutes

Reauthentication Time: 1440 minutes

Use Default Settings Use Manual Settings

OK Cancel

- 2 Go to **CONFIGURATION > Object > User/Group > MAC Address > MAC Authentication**. Add the teacher's MAC address for MAC authentication in the NXC local server.

Add MAC Auth Address

MAC Address/OUI: 7C:01:91:6C:01:10

MAC Role: mac-users

Save it into local DataBase

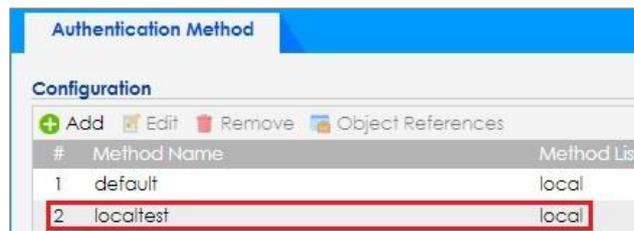
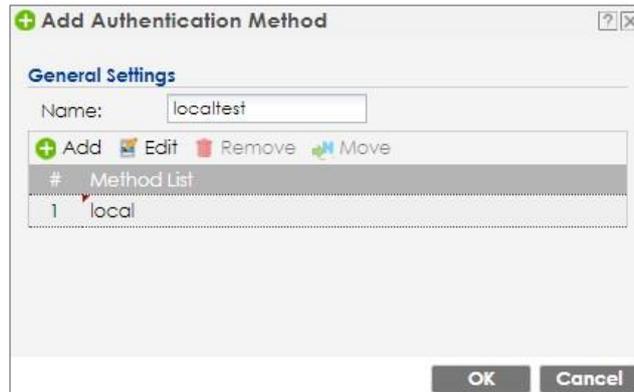
Description: Teacher's Mobile

OK Cancel

User	Group	Setting	MAC Address
MAC Authentication			
+ Add Edit Remove			
#	MAC Address / OUI	MAC Type	
1	7C:01:91:6C:01:10	int-mac-address	

6.2.3 Configure Authentication Method Setting

- 1 Go to **CONFIGURATION > Object > Auth. Method**, click **Add** to create an authentication method. Enter the **Name** of this authentication method and select to local in the **Method List**.



6.2.4 Configure Captive Portal Setting

- 1 Go to **CONFIGURATION > Network > Captive Portal > Redirect on AP > Authentication Policy Rule > Add**. Set the SSID for user authentication policy to redirect captive portal on the AP.

Auth. Policy Add
Create new Object ▾

General Settings

Enable Policy

Theme Name:

Description: (Optional)

User Auth Policy

SSID:

Source Address:

Destination Address:

Schedule:

Authentication:

Authentication Method:

- 2 Go to **CONFIGURATION > Network > Captive Portal > Redirect on AP > Authentication Policy Group > Add**. Set the authentication policy rule in the policy group.

Add Authentication Policy Group ? | X

General Settings

Profile Name:

Description: (Optional)

+ Add ✎ Edit ✖ Remove ↔ Move

#	Name
1	Zyxel_CP

Page 0 of 0 Show 50 Items No data to display

Note:
The "default" policy rule will be the last one for each group profile.

- Go to **CONFIGURATION > Network > Captive Portal > Captive Portal > General Settings**. Enable the captive portal function.



- Go to **CONFIGURATION > Network > Captive Portal > Captive Portal > SSID Profile with MAC Cache > Add**. Set the SSID profile with the MAC cache. The MAC address cache time can be set from 1-168 hours.

SSID Profile with MAC Cache		
#	SSID Profile	Caching Time (hour)
1	MAC_CP (MAC_CP)	5

6.2.5 Configure AP Group Profile

- 1 Go to **CONFIGURATION > Wireless > AP Management > AP Group > Group Summary > Radio setting**. Set the SSID profile to the AP radio.

Edit AP Group Profile default

Radio 1 Setting

OP Mode OP Mode AP Mode MON Mode Root AP Repeater AP ?

Radio 1 AP Profile:

Max Output Power: dBm (0~30)

#	SSID Profile
1	MAC_CP
2	disable
3	disable
4	disable
5	disable
6	disable
7	disable
8	disable

Radio 2 Setting

OP Mode OP Mode AP Mode MON Mode Root AP Repeater AP ?

Radio 2 AP Profile:

Max Output Power: dBm (0~30)

#	SSID Profile
1	MAC_CP
2	disable
3	disable
4	disable

- 2 Go to **CONFIGURATION > Wireless > AP Management > AP Group > Group Summary > Portal redirect on AP**. Set the authentication policy group.

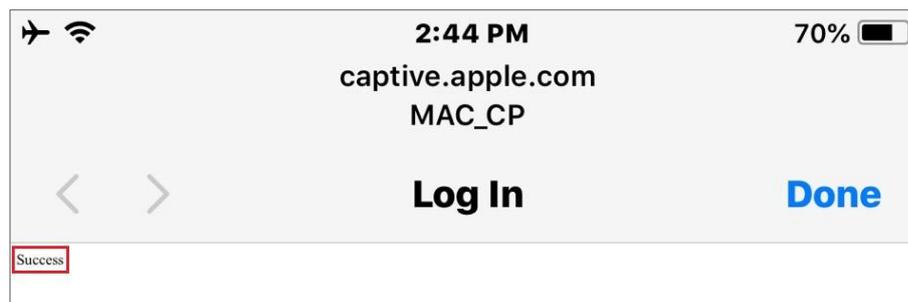
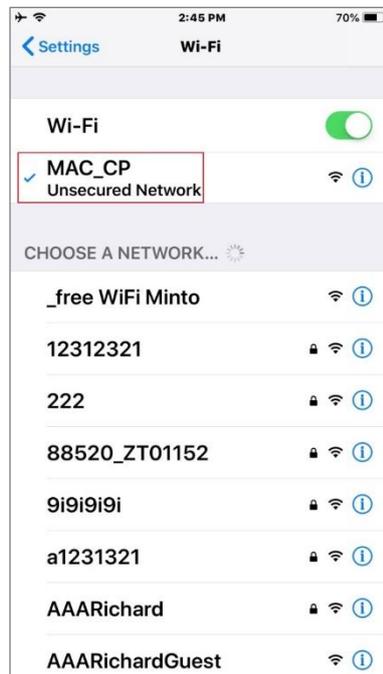
Portal Redirect on AP

Auth. Policy Group:

Skip authentication to provide contingency access while controller is unreachable.

6.2.6 Test the Result

- 1 Use the teacher's trusted device and connect to the SSID: **MAC_CP**. The captive portal doesn't pop up because the devices' MAC address is trusted by the NXC's local server. The device successfully passes the MAC authentication and is allowed to access the Internet directly.



- Go to **MONITOR > Wireless > Station Info**. Check the station information on the NXC.

#	IP Address	Associated AP	SSID Name	Tx Rate	Rx Rate
1	192.168.1.102	AP-5C6A80EBA...	MAC_CP	300M	24M

- Go to **MONITOR > System Status > Login Users > Login Users**. Check the logged in users on the NXC and find the teacher's device information.

#	User ID	Reauth/Leas...	Associated AP	Type	IP Address	MAC Address
1	7C:01:91:6C:01:10	unlimited / u...	AP-5C6A80E...	mac-auth	192.168.1.102	7C-01-91-6C-01-10

- Use the student's mobile device or PC to connect to the SSID: **MAC_CP**. Open the browser and it will redirect to the captive portal screen. Enter the student's username and password to pass the captive portal.

ZYXEL

NXC2500

Welcome to the configuration interface. Please enter username and password to login.

 Student-1 _____

 _____

Note

1. Turn on Javascript and Cookie setting in your web browser.
2. Turn off Popup Window Blocking in your web browser.
3. Turn on Java Runtime Environment (JRE) in your web browser.

ZYXEL

Student-1, You now have logged in.

Click the logout button to terminate the access session.
You could renew your lease time by clicking the Renew button.
For security reason you must login in again after 24 hours 0 minutes.

User-defined lease time (max 1440 minutes):

Remaining time before lease timeout (hh:mm:ss)

Remaining time before auth. timeout (hh:mm)

- Go to **MONITOR > Wireless > Station Info**. Check the station information on the NXC.

Station List							
Show Advanced Settings							
#	IP Address	Associated AP	SSID Name	Signal Strength	Channel	Tx Rate	Rx Rate
1	192.168.1.103	AP-5C6A80EB...	MAC_CP	-50dBm 	1	104M	130M
2	192.168.1.102	AP-5C6A80EB...	MAC_CP	-48dBm 	153	270M	24M

- Go to **MONITOR > System Status > Login Users > Login Users**.
Check the logged in users on the NXC and find the student's device information.

#	User ID	Reauth/Le...	Associated ...	Type	IP Address	MAC Address	Authentica...	User Info
1	7C:01:91:6C:01:10	unlimited / ...	AP-5C6A80...	mac-auth	192.168.1.102	7C-01-91-6C-01-10	-	mac-address[...]
2	Student-1	22:15:52 / 2...	AP-5C6A80...	captive portal	192.168.1.103	EC-55-F9-4E-81-7B	-	guest Student-1

- The student's device was cached in the NXC's trusted MAC address list with a 5 hour limitation

6.2.7 What Could Go Wrong

- 1 If captive portal page is not redirected for student role, please check whether the MAC address cache time is still cached during that time.
- 2 If captive portal is not enabled but the fallback option is selected, the users can always connect to the Wi-Fi regardless of whether the MAC authentication is successful or not.
- 3 This Feature does not support with legacy NWA3KN and NWA5KN series products.

6.3 How to Defect the Rogue AP?

A rogue AP works without being controlled by the administrator of the Network. It may cause the security issue for the network and we can use the AP in monitor mode to contain the rogue AP.

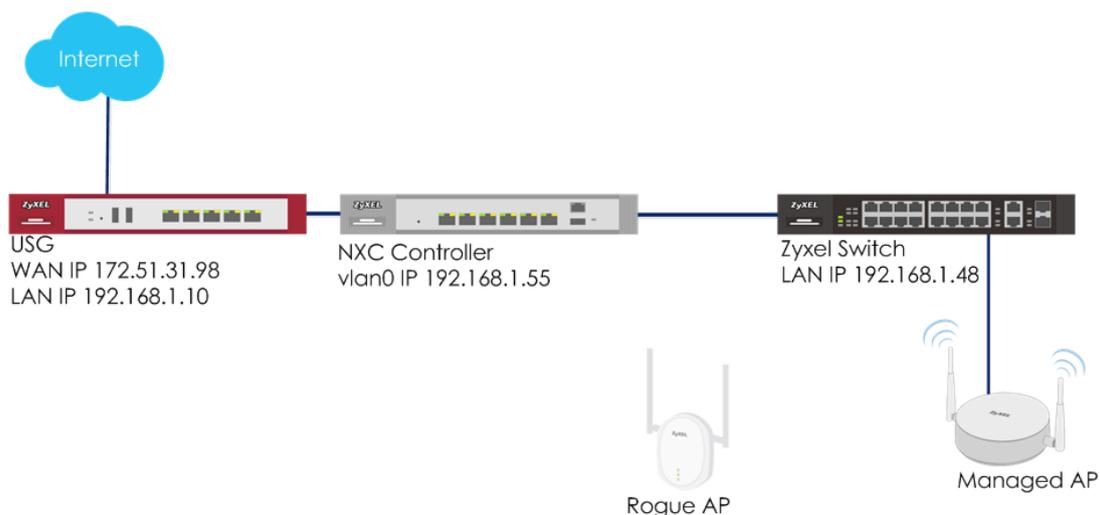


Figure 6.3 Monitor Rogue AP and Containment



Note:

All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC2500 (Firmware Version: 5.30), GS2210-8HP (Firmware Version: V4.30).

6.3.1 Configure AP to Monitor Mode

- 1 Configure a monitor profile in **CONFIGURATION > Object > MON Profile**. Select the **default** profile and click **Edit** to change. Check the **Scan Channel Mode** is **auto** and **Country Code** is correct and is the location where you use the AP. Click **OK** to save.

- 2 Configure AP to monitor mode in **CONFIGURATION > Wireless > AP Management**. Select the AP which is going to work in monitor mode and click **Edit** to change. Check **Override Group Radio Setting** and select **MON Mode** with **default radio 1 profile** which is set in step 1. Click **OK** to save.

6.3.2 Detected Devices and Containment

- 1 In **MONITOR > Wireless > Detected Device**, Click **Refresh** if there's no rogue AP in the list. Select the rogue AP and click **Mark as Rogue AP**.

Detected Device						
<input checked="" type="radio"/> Mark as Rogue AP <input type="radio"/> Mark as Friendly AP						
#	Role	Classified by	MAC Address	SSID Name	Chann...	802.11 Mode
1	Suspected ro...	Un-manage...	02:10:18:27:00:02	ZyXEL_0000	11	IEEE 802.11n 40MHz
2	Suspected ro...	Un-manage...	04:BF:6D:01:00:00	DELSA6F5D80	11	IEEE 802.11n 40MHz
3	Suspected ro...	Un-manage...	10:7B:EF:D8:D8:5D	testfwupgrade	11	IEEE 802.11n 20MHz
4	Suspected ro...	Un-manage...	1C:74:0D:C7:4B:AE	NBG-418Nv2_Multi...	2	IEEE 802.11n 40MHz
5	Suspected ro...	Un-manage...	1C:74:0D:F9:5E:3A	64 Network	6	IEEE 802.11n 20MHz
6	Suspected ro...	Un-manage...	1C:74:0D:FF:D1:00	Multy X 9453	8	IEEE 802.11ac 20MHz
7	Suspected ro...	Un-manage...	22:74:0D:FF:D1:00	Orz.guest	7	IEEE 802.11ac 20MHz
8	Suspected ro...	Un-manage...	22:74:0D:FF:D1:00	Orz.guest	8	IEEE 802.11ac 20MHz
9	Suspected ro...	Un-manage...	26:74:0D:FF:D1:00	<no ssid>	7	IEEE 802.11ac 20MHz
10	Suspected ro...	Weak Securit...	34:57:60:80:00:F8	CN-V100	11	IEEE 802.11n 20MHz

- 2 When the AP is marked as a rogue AP, it can be set in the containment list in **CONFIGURATION > Wireless > Rogue AP > Rogue/Friendly AP List** and the stations are difficult to connect with the containment AP.

Rogue/Friendly AP List			
<input checked="" type="checkbox"/> Add <input type="checkbox"/> Edit <input type="checkbox"/> Remove <input checked="" type="checkbox"/> Containment <input type="checkbox"/> Dis-Containment			
#	Containment	Role	MAC Address
1		rogue-ap	26:74:0D:FF:D1:00

6.3.3 Test the Result

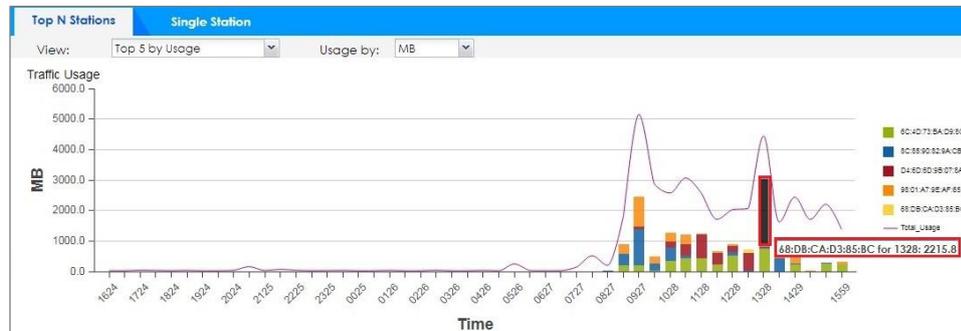
- 1 When the AP is marked as a rogue AP, it is shown in **MONITOR > Wireless > Detected Device**.

Detected Device						
		<input type="checkbox"/> Mark as Rogue AP	<input checked="" type="checkbox"/> Mark as Friendly AP			
#	Role ^	Classified by	MAC Address	SSID Name	Chann...	802.11 Mode
1	Rogue AP	User Config	26:74:0D:f7:28:70	<no ssid>	11	IEEE 802.11ac 40MHz
2	Suspected ro...	Un-manage...	02:10:18:01:00:02	ZyXEL_0000	11	IEEE 802.11n 40MHz
3	Suspected ro...	Un-manage...	04:BF:6D:67:57:50	DELSA6F5D80	11	IEEE 802.11n 40MHz
4	Suspected ro...	Un-manage...	10:7B:EF:D3:D3:0B	testfwupgrade	11	IEEE 802.11n 20MHz
5	Suspected ro...	Un-manage...	1C:74:0D:55:60:73	AndrewSSSS	1	IEEE 802.11n 20MHz

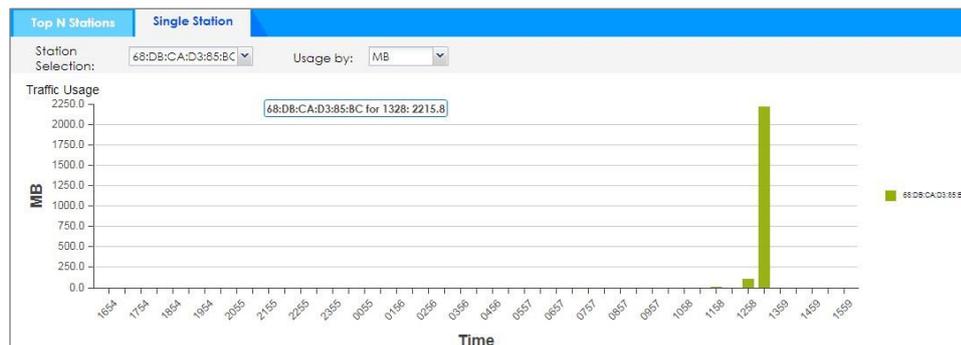
- 2 When the AP is set in the containment list, the stations are disconnected right away after they connect to the rogue AP.

6.4 How to monitor the traffic and stations on web GUI?

- 1 In **Dashboard > Station > Traffic**, Click the **Top N Stations** tab to view usage information for multiple stations at a time.



- 2 Or click the **Single Station** tab to view a specific wireless station's usage details.



The y-axis shows the amount of data (in MB or GB) consumed by the selected station(s).

The x-axis shows the time period over which the traffic flow occurred.

Move the cursor over a bar to see usage details over a specific time period.

The chart will record 24 hours of traffic usage.

For example, we can observe message of the station MAC: 68:DB:CA:D3:85:BC for 1328:2215.8 which means this MAC's traffic is 2215.8MB at 13:28.

- As well as we can check the broadcast number on the AP. In **MONITOR > Wireless > AP Information > AP List**, click **More Information** on the AP.

#	Status	Registration	Description	CPU Usage	IP Address	Model	Version	Group	Station	Rece
1	1	Limited AP	AP01	29%	10.214.70.201	NWA5123-AC...	5.30 ABIM.2 -DF-201...	ZyXEL_CS...	6	2018/
2	1	Limited AP	AP03	38%	10.214.70.203	WAC6303D-S	5.30 ABGL.2 -DF-20...	ZyXEL_CS...	9	2018/
3	1	Limited AP	AP05	56%	10.214.70.205	NWA5123-AC...	5.30 ABIM.2 -DF-201...	ZyXEL_CS...	16	2018/
4	1	Limited AP	AP06	19%	10.214.70.206	WAC5302D-S	5.30 ABFH.2 -DF-201...	ZyXEL_CS...	1	2018/

It displays the number of broadcast packets transmitted / received on the port.

AP Information

Configuration Status: Limited AP
 Conflict: n/a
 Non Support: BAND SELECT in Radio2, BAND SELECT in Radio1

Port Status

Port	Status	PVID	Up Time	Tx Bcast	Rx Bcast
UPLINK	1000M/Full	n/a	120:59:07	9401	1284380
lan1	Down	1	00:00:00	0	0

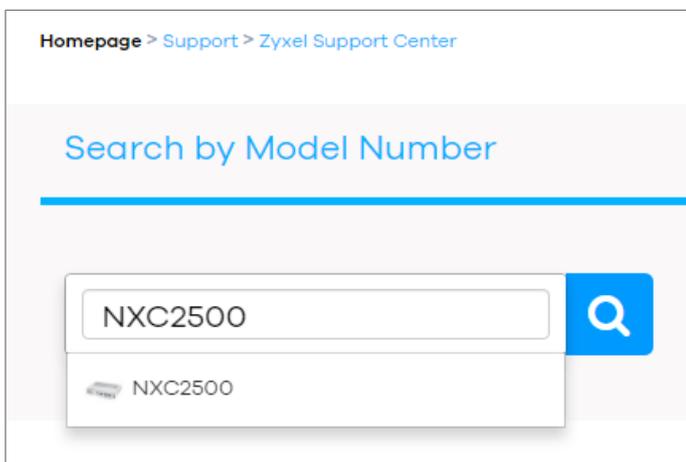
Maintain NXC Controller

7.1 How to Do Firmware upgrade

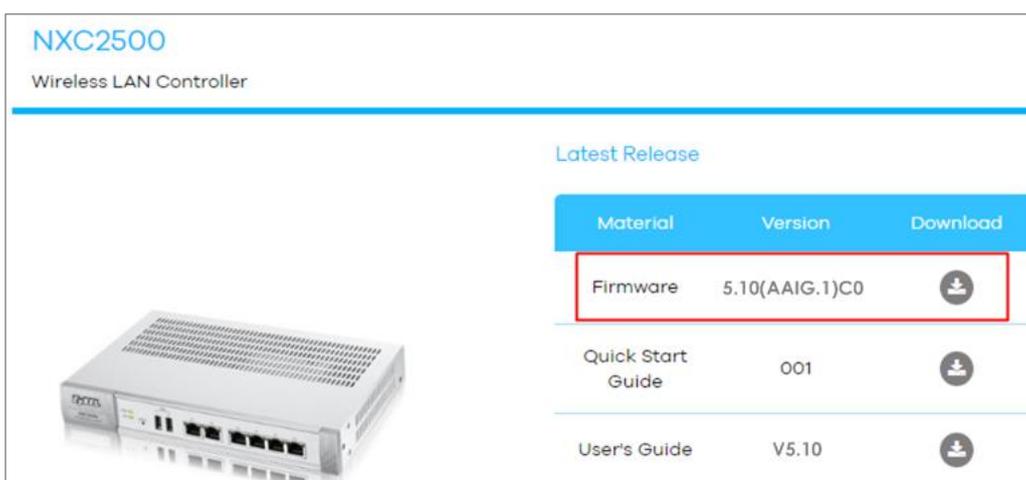
1. There are two ways to do firmware upgrade, GUI and FTP. The firmware can be downloaded from Zyxel support center. Please find below the website address of the support center.

http://www.zyxel.com/support/support_landing.shtml

2. Use "Search by Model Number" in the webpage.



3. Click the download icon in NXC2500 latest release as shown below.



7.1.1 Firmware from GUI?

The example instructs how to do FW upgrade from GUI. The Firmware version will be changed from v5.00 to v5.10.

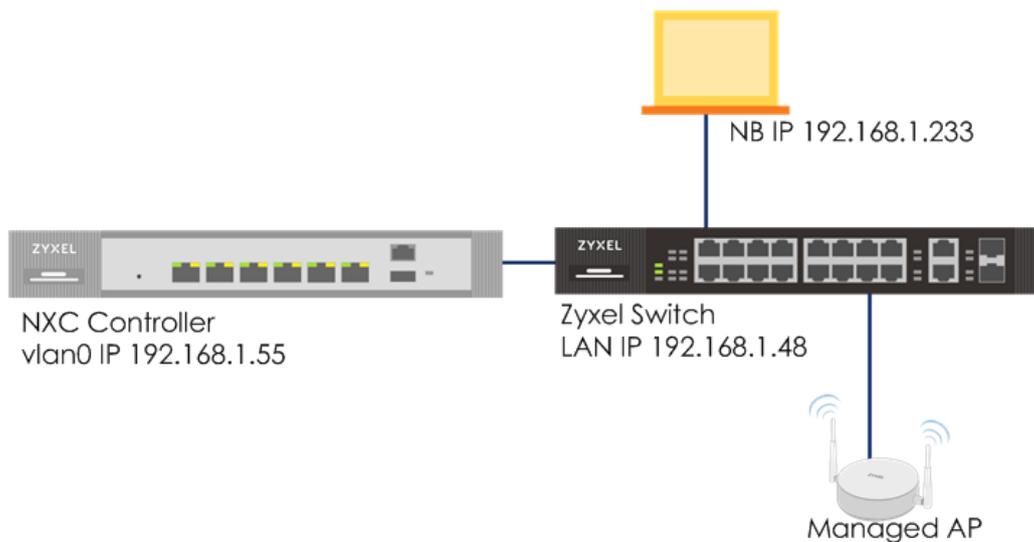


Figure 7.1.1 Firmware Upgrade from GUI



Note:

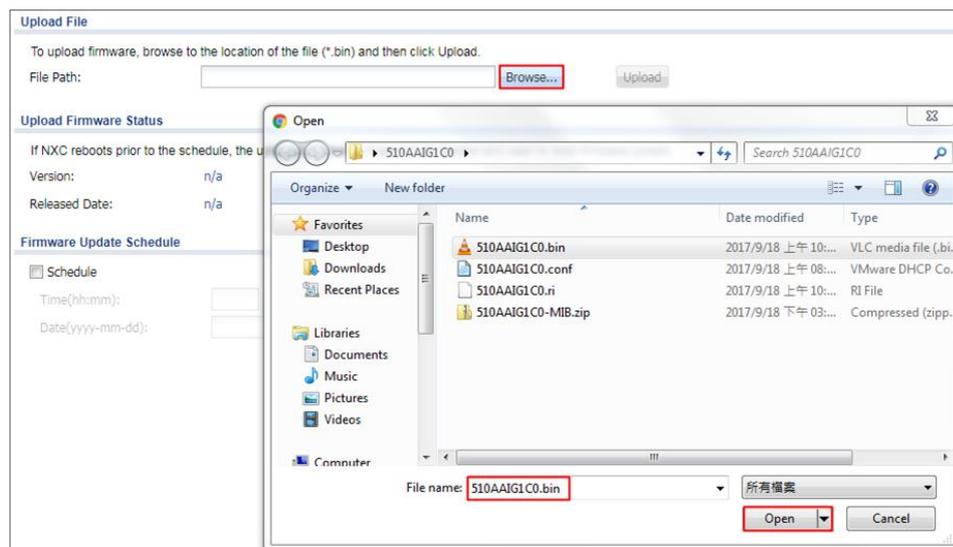
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC2500 (Firmware Version: 5.00), GS2210-8HP (Firmware Version: V4.30).

7.1.1.1 Firmware Upgrade on GUI

- 1 In **MAINTENANCE > File Manager > Firmware Package**, check if the NXC's current firmware version is the same as the one you are going to install.

Version	
Boot Module:	V1.00
Current Version:	V5.00(AAIG.3)
Released Date:	2017-02-03 07:02:31

- 2 In **MAINTENANCE > File Manager > Firmware Package**, click **Browse...** in Upload File and select the firmware you want to install.

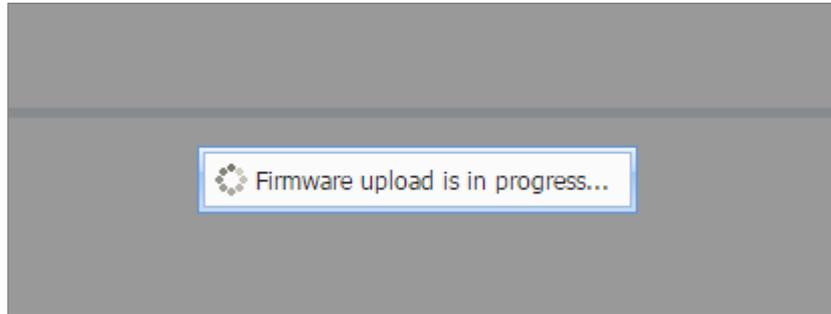


- 3 In **MAINTENANCE > File Manager > Firmware Package**, click **Upload...** to start to upload the firmware.



7.1.1.2 Test the Result

- 1 After starting firmware upgrade, there's a notification about firmware upload.



- 2 After finishing firmware upload, the system will start to firmware upgrade.



- 3 After the firmware upgrade is complete and successful, you can check it on GUI Dashboard.

Device Information	
System Name:	HQ2 CSO NXC2500
System Location:	HQ2 CSO Field Trial
Model Name:	NXC2500
Serial Number:	S132L05170057
MAC Address Range:	B0:B2:DC:6E:4A:3F ~ B0:B2:DC:6E:4A:34
Firmware Version:	V5.10(AAIG.1) / V1.03 / 2017-09-18 10:28:54

7.1.1.3 What Could Go Wrong

- 1 When the firmware is uploading and the traffic for transferring the firmware is disconnected, the firmware upgrade will not be successful.
- 2 When the firmware is upgrading, please do not reset or reboot the controller. Otherwise, it might cause system crashes or firmware upgrade failure.

7.1.2 Firmware from FTP?

The example instructs how to do FW upgrade from FTP. This is usually used when you failed to access the web GUI.

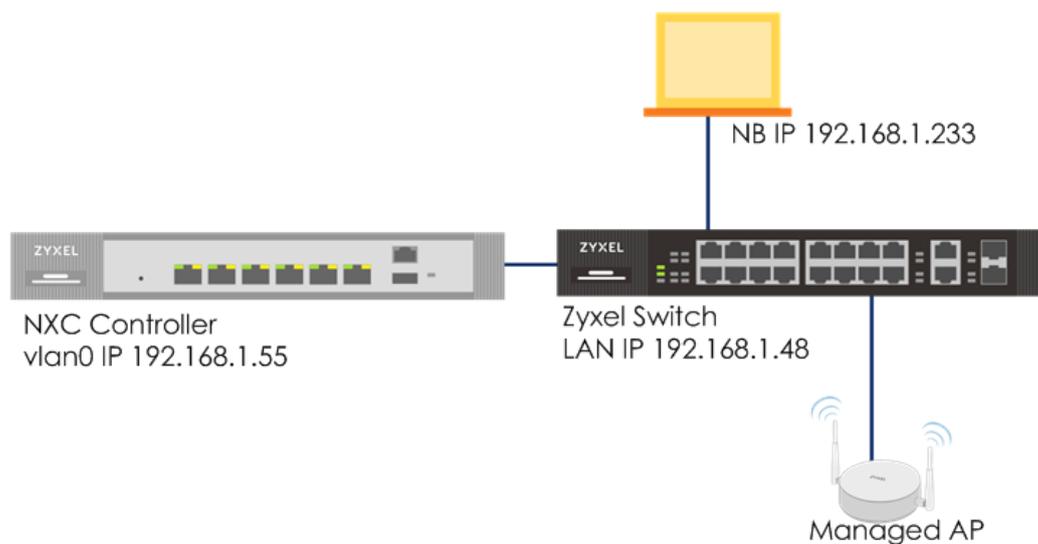


Figure 7.1.2 Firmware Upgrade from GUI



Note:

All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC2500 (Firmware Version: 5.30), GS2210-8HP (Firmware Version: V4.30).

7.1.2.1 Firmware Upgrade on GUI

- 1 Copy the firmware to the root directory of the C drive on your computer c:\ and do not change the file name of the firmware.
- 2 Use the following command to ping the controller for checking the connection.

```
ping 192.168.1.55
```

```
C:\>ping 192.168.1.55

Pinging 192.168.1.55 with 32 bytes of data:
Reply from 192.168.1.55: bytes=32 time=1ms TTL=64
Reply from 192.168.1.55: bytes=32 time<1ms TTL=64
Reply from 192.168.1.55: bytes=32 time<1ms TTL=64
Reply from 192.168.1.55: bytes=32 time<1ms TTL=64
```

- 3 In the Windows command prompt, type [ftp 192.168.1.55](ftp://192.168.1.55) to log in to the controller via username **admin** and password **1234** (by default).

```
C:\>ftp 192.168.1.55
Connected to 192.168.1.55.
220 FTP Server (NXC2500) [::ffff:192.168.1.55]
User (192.168.1.55:(none)): admin
331 Password required for admin
Password:
```

- 4 Enter bin for transfer mode to binary.

```
ftp> bin
200 Switching to Binary mode.
```

- 5 Enter **put c:\ 510AAIG1C0\510AAIG1C0.bin** and wait for the file transfer to complete. After the transmission is finished, the controller will start to upgrade.

```
ftp> put C:\510AAIG1C0\510AAIG1C0.bin
200 PORT command successful
150 Opening BINARY mode data connection for 510AAIG1C0.bin
226-firmware verifying...
226-firmware updating...
226-Please Wait about 5 minutes!!
226-Do not poweroff or reset,
226-system will reboot automatically after finished updating.
226 Transfer complete.
ftp: 254883548 bytes sent in 12.68Seconds 20102.81Kbytes/sec.
```

7.1.2.2 Test the Result

- 1 After starting firmware upgrade, the LED flashes and it takes about 5 minutes to finish.
- 2 After the firmware is upgraded successfully, you can check it on GUI Dashboard.

Device Information	
System Name:	HQ2 CSO NXC2500
System Location:	HQ2 CSO Field Trial
Model Name:	NXC2500
Serial Number:	S132L051700007
MAC Address Range:	B0:B2:DC:6E:4A:3F ~ B0:B2:DC:6E:4A:34
Firmware Version:	V5.10(AAIG.1) / V1.03 / 2017-09-18 10:28:54

7.1.2.3 What Could Go Wrong

- 1 When the firmware is uploading and the traffic for transferring the firmware is disconnected, the firmware upgrade will not be successful.
- 2 When the firmware is upgrading, please do not reset or reboot the controller. Otherwise, it might cause system crashes or firmware upgrade failure.

7.2 How to Reset the Controller/AP?

The example instructs how to reset the controller/AP. This is usually used when there's a new deployment or misconfiguration.

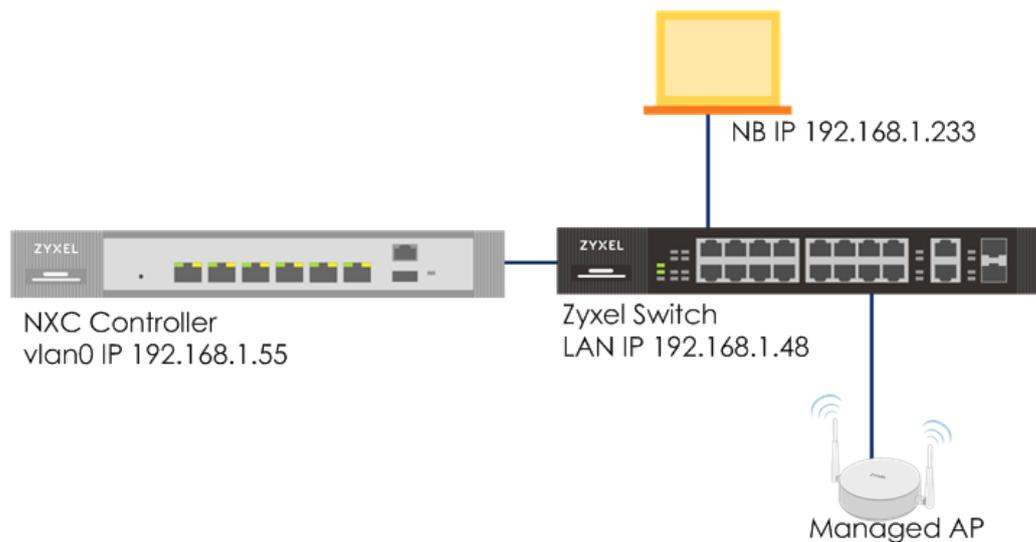


Figure 7.2 Firmware Upgrade from GUI

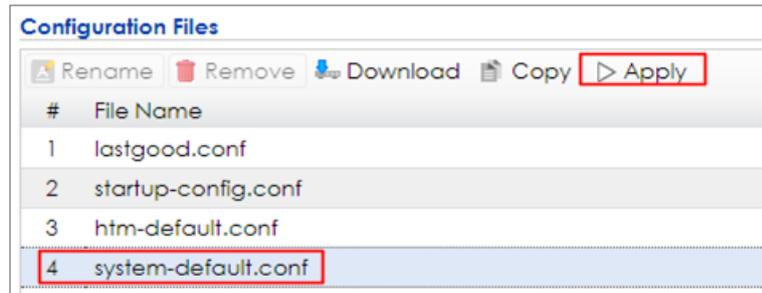


Note:

All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC2500 (Firmware Version: 5.30), GS2210-8HP (Firmware Version: V4.30).

7.2.1 Reset to Default from GUI

- 1 Log in to controller and go to **MANTENANCE > File Manager > Configuration File**. Click **“system-default conf”** in the list and **Apply**.



7.2.2 Reset to Default from Hardware

- 1 Push the RESET button over 15 seconds for resetting to defaults.

7.2.3 Test the Result

- 1 After resetting to default settings, the controller's IP is 192.168.1.1 and AP's IP is 192.168.1.2.
- 2 All the settings are changed back to default settings.

7.3 How to upgrade the firmware for AP via NXC?

The example instructs how to upgrade the firmware for partial APs. We can decide if the AP will be upgraded firmware automatically by NXC or upgraded firmware manually by ourselves. And choose the updating method as CAPWAP or FTP. In this chapter, there is also an example instructs how to upgrade firmware for partial AP. Not upgrade AP firmware at the same time.

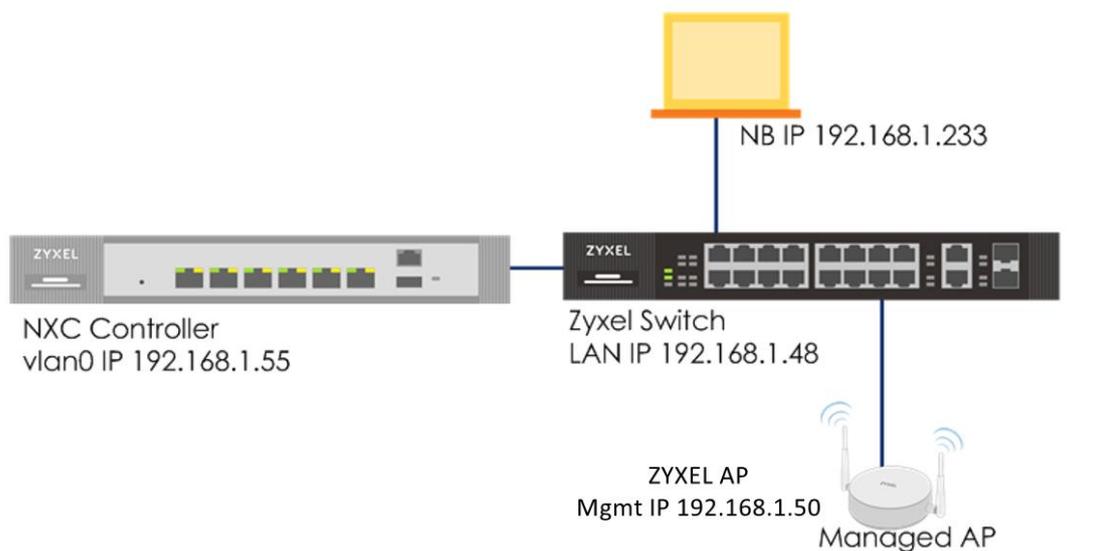


Figure 7.3 Upgrade AP firmware via GUI



Note:

All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using NXC2500 (Firmware Version: 5.30) and GS2210-8HP (Firmware Version: V4.30).

7.3.1 How to Change the Updating Method for the AP as Manual?

The example instructs how to change the updating mode for AP as Manual. The AP will not upgrade the firmware unless we click the "Upgrade Now". It can help to manage the upgrade time. We can choose when to upgrade the firmware to the AP.

7.3.1.1 Change the Updating Method via GUI

- 1 Log in to controller and go to **CONFIGURATION > Wireless > AP Management > AP Policy > Firmware Updating.**

Updating Method: **CAPWAP**

Updating Mode: **Manual**

Click **Apply**.

The screenshot shows the ZyXel configuration interface. The left sidebar contains a navigation menu with categories like Licensing, Wireless, AP Management, Network, Object, System, and Log & Report. The main content area is titled 'CONFIGURATION' and has tabs for 'Mgmt. AP List', 'AP Policy', 'AP Group', and 'Firmware'. Under 'AP Policy', there are 'General Settings' and 'Firmware Updating' sections. The 'Firmware Updating' section is highlighted with a red box and contains the following settings:

- Updating Method: CAPWAP FTP
- Updating Mode: Auto Manual

At the bottom right of the configuration area, there are 'Apply' and 'Reset' buttons.

7.3.2 How to upgrade the specific AP firmware manually?

The example instructs how to upgrade the firmware for specific AP. We do not have to upgrade all the AP firmware at the same time.

7.3.2.1 Upgrade the AP firmware via GUI

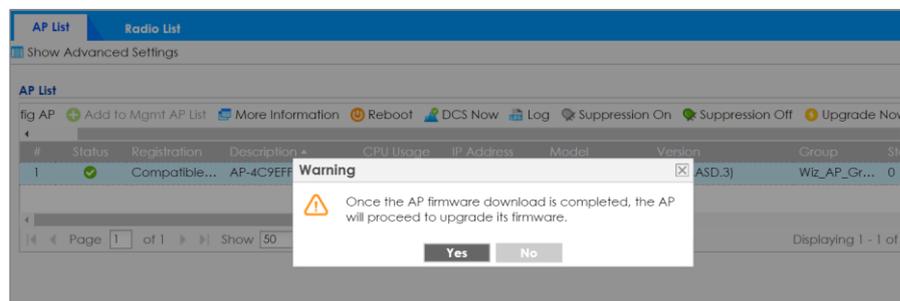
- 1 Log in to controller and go to **Monitor > Wireless > AP Information > AP List**.

Choose the AP which is needed to be upgraded firmware. Click **Upgrade Now**.



#	Status	Registration	Description	CPU Usage	IP Address	Model	Version	Group	Stat
1	✓	Compatible...	AP-4C9EFF...	0 %	192.168.1.50	WAC6502D-E	5.20(AASD.3)	Wiz_AP_Gr...	0

- 2 It will pop out a warning page. Click **Yes**.



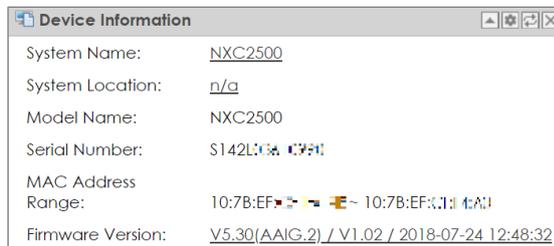
- 3 There is information about AP upgrading firmware in the Monitor log.



#	Time	Prior...	Cat...	Message
1	2018-08-...	alert	Poli...	Interface ge2 dead, related policy route rules will be disabled.
2	2018-08-...	alert	CA...	AP Disconnect. MAC:4C:9E:FF:5:1:5, Name:AP-4C9EFF5115, Reason:...
3	2018-08-...	info	CA...	AP Reboot. MAC:4C:9E:FF:5:1:5, Name:AP-4C9EFF5115, Model:WAC...
4	2018-08-...	info	CA...	AP Reboot by firmware updating. MAC:4C:9E:FF:5:1:5, Name:AP-4C9...

7.3.2.2 Test the Result

The AP firmware version should be the same with the NXC



Device Information window showing the following details:

- System Name: NXC2500
- System Location: n/a
- Model Name: NXC2500
- Serial Number: S142L103 0001
- MAC Address Range: 10:7B:EF:00:00:00 - 10:7B:EF:00:00:0F
- Firmware Version: V5.30(AAIG.2) / V1.02 / 2018-07-24 12:48:32



#	Status	Registration	Description	CPU Usage	IP Address	Model	Version	Group
1	✔	Mgmt AP	AP-4C9EFF90B058	8 %	192.168.1.50	WAC6502D-E	5.30(AASD.2)	Wiz_AP_Gr...

7.3.2.3 What Could Go Wrong

- 1 If the AP firmware is the latest, the “Upgrade Now” button will be gray.

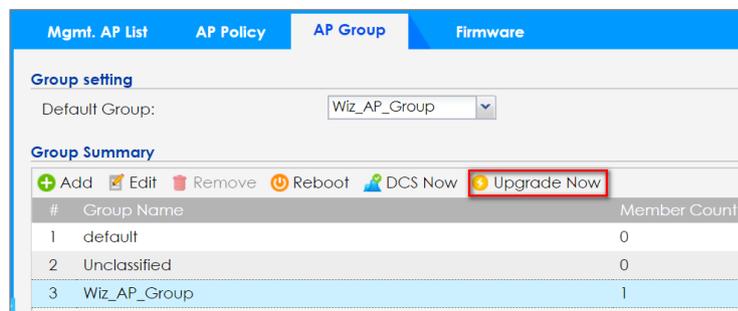
7.3.3 How to upgrade the firmware for AP group?

The example instructs how to upgrade the firmware for specific AP group.

7.3.3.1 Upgrade the firmware for AP group via GUI

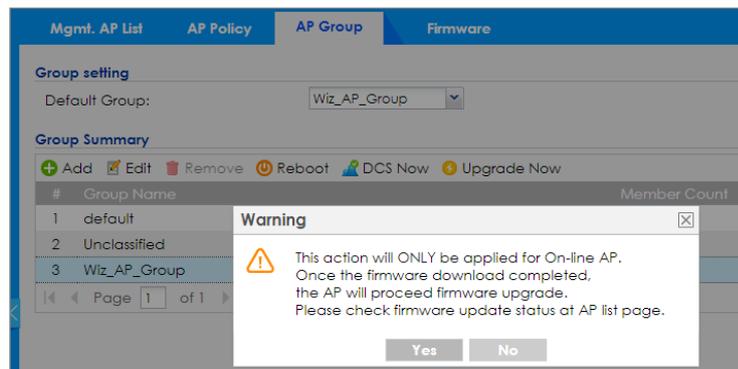
- 1 Log in to controller and go to **CONFIGURATION > Wireless > AP Management > AP Group**.

Choose the AP Group and click **“Upgrade Now”**.



- 2 It will pop out a warning message.

Click **Yes**.

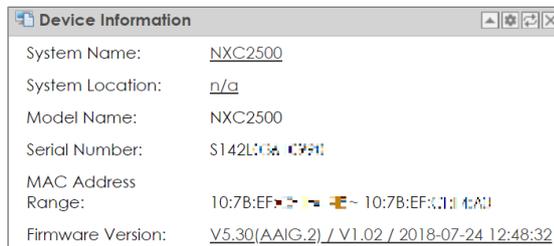


- 3 Check the log in Monitor. It will show the AP group Reboot by firmware updating.

#	Time	Prior...	Cat...	Message
1	2018-08-...	info	AP ...	AP firmware download has begun for firmware upgrade.
2	2018-08-...	info	CA...	AP Group Reboot by firmware updating. Name:Wiz_AP_Group

7.3.3.2 Test the Result

The AP firmware version should be the same with the NXC.



A screenshot of an 'AP List' table. The table has a toolbar with icons for 'Config AP', 'Add to Mgmt AP List', 'More Information', 'Reboot', 'DCS Now', 'Log', 'Suppression On', and 'Suppression Off'. The table contains one row of data:

#	Status	Registration	Description	CPU Usage	IP Address	Model	Version	Group
1	✔	Mgmt AP	AP-4C9EFF90B058	8 %	192.168.1.50	WAC6502D-E	5.30(AASD.2)	Wiz_AP_Gr...

7.3.3.3 What Could Go Wrong

- 1 If the AP firmware is the latest, there will no action for the firmware upgrade.
- 2 The firmware upgrade for the AP group will only be applied for O-line AP. If the AP is offline, it will not be upgraded.

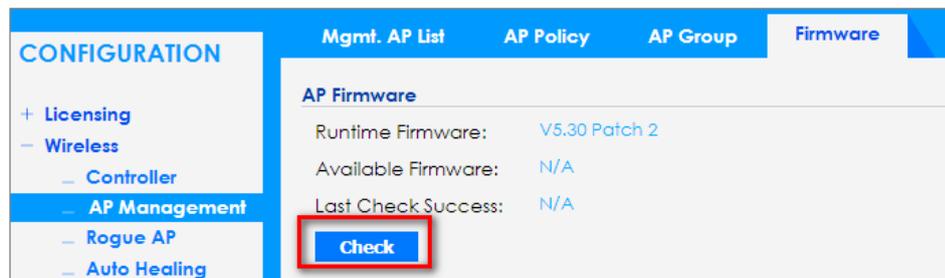
7.4 How to Upgrade the AP firmware via cloud?

The example instructs how to upgrade the AP firmware via cloud. We do not have to download the DF to our PC and upload it to the AP. Just check the firmware version via internet. If there is newer firmware version, we can download it to NXC then apply to AP.

7.4.1 Upgrade the firmware for AP group via GUI

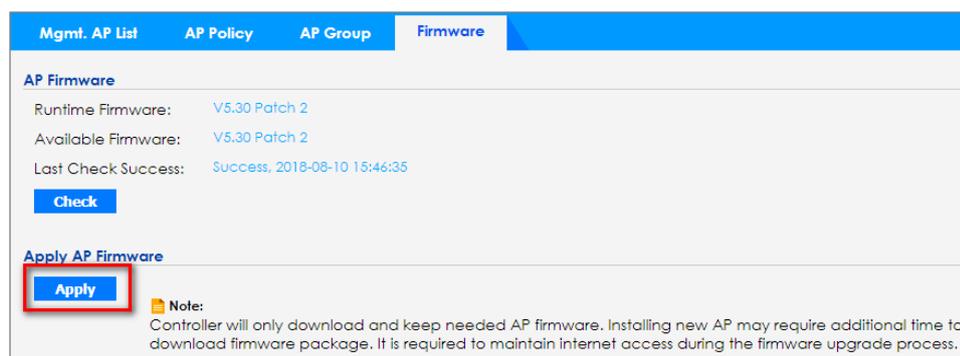
- 1 Log in to controller and go to **CONFIGURATION > Wireless > AP Management > Firmware**.

Click **Check**.

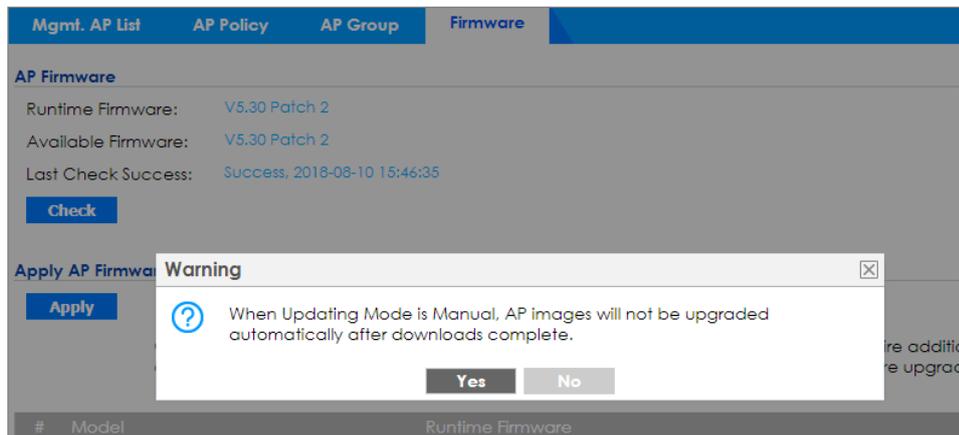


- 2 After getting the latest firmware version from the cloud, it will show the available firmware version and last check success time.

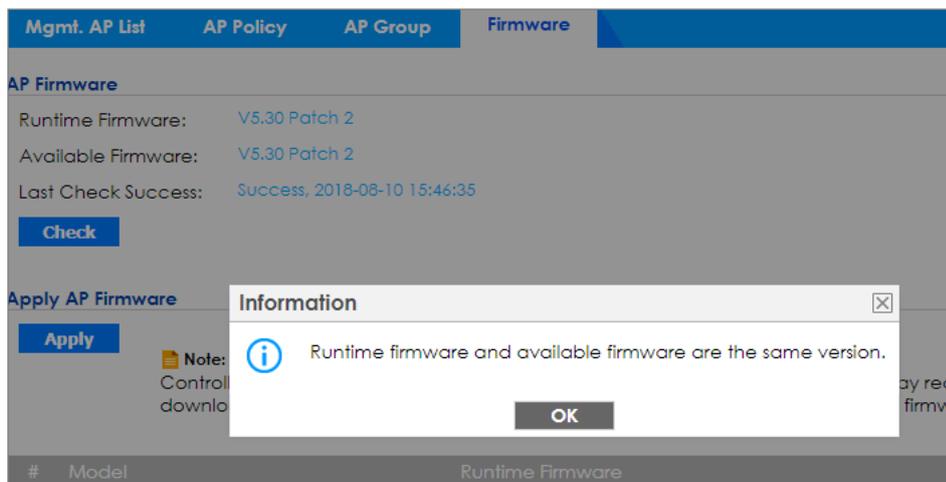
Click **Apply** to have the NXC download the latest AP firmware from the firmware server.



- It will pop out a warning message.
Click **Yes**.



- It will pop out information.
Click **OK**.

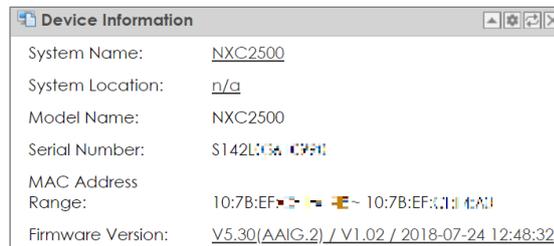


- Log in to controller and go to **Monitor > Wireless > AP Information > AP List**.
Choose the AP which is needed to be upgraded firmware.
Click **Upgrade Now**.



7.4.2 Test the Result

The AP firmware version should be the same with the NXC.



A screenshot of an 'AP List' table. The table has a toolbar with icons for 'Config AP', 'Add to Mgmt AP List', 'More Information', 'Reboot', 'DCS Now', 'Log', 'Suppression On', and 'Suppression Off'. The table contains one row of data:

#	Status	Registration	Description	CPU Usage	IP Address	Model	Version	Group
1	Online	Mgmt AP	AP-4C9EFF90B058	8 %	192.168.1.50	WAC6502D-E	5.30(AASD.2)	Wiz_AP_Gr...

7.4.3 What Could Go Wrong

- 1 If the AP firmware is the latest, there will no action for the firmware upgrade.

The firmware upgrade for the AP group will only be applied for O-line AP. If the AP is offline, it will not be upgraded.

Trouble Shooting

8.1 How to Collect the Diagnostic Info?

The diagnostic info needs to be collected when there's any problem happened on the controller or AP.

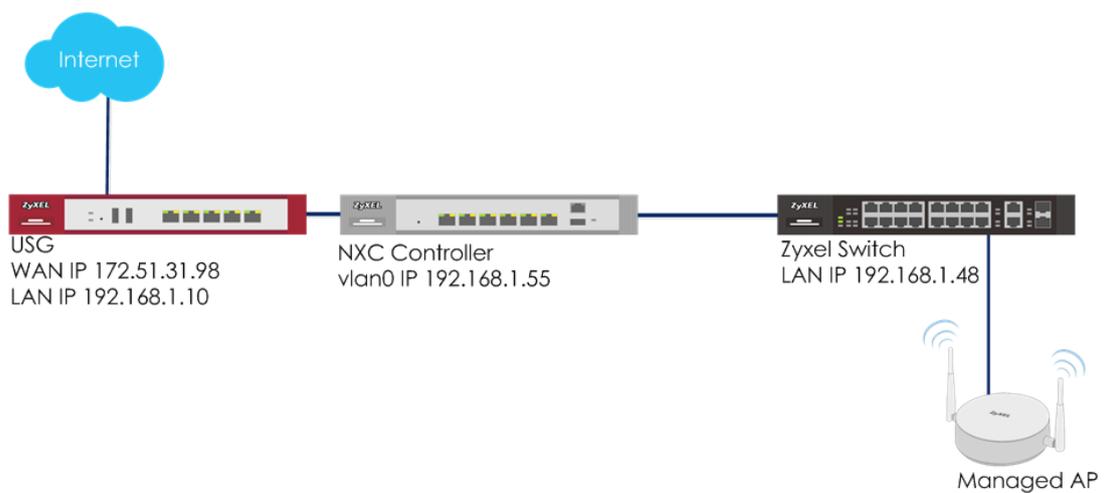


Figure 8.1 Collect the Diagnostic Info

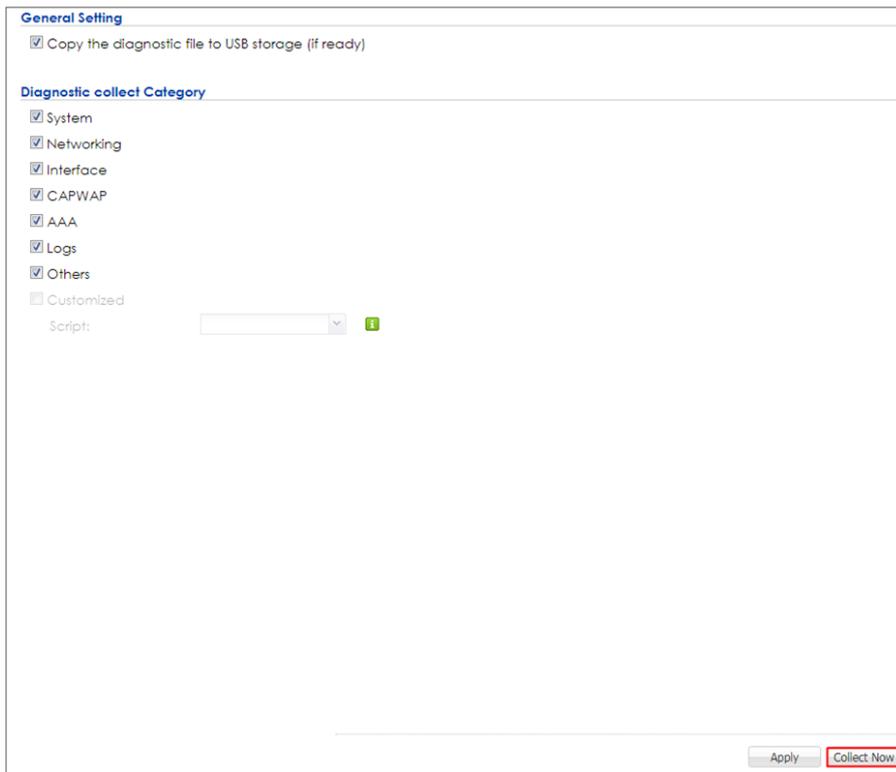


Note:

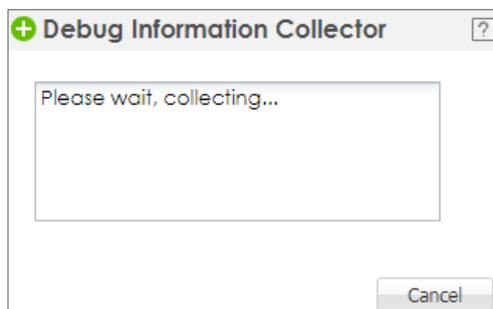
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC2500 (Firmware Version: 5.40), GS2210-8HP (Firmware Version: V4.30).

8.1.1 Collect Diagnostic Info

- 1 In **MAINTENANS > Diagnostic > Diagnostics**, select on **Collect on Controller** and click **Collect Now** when the controller has any problem.



- 2 A window pops up when the controller is collecting the diagnostic.



- In **MAINTENANS > Diagnostic > Diagnostics**, select on **Collect on AP** and move the AP's MAC to the **collected APs** list. Click **Collect Now** to start collection.

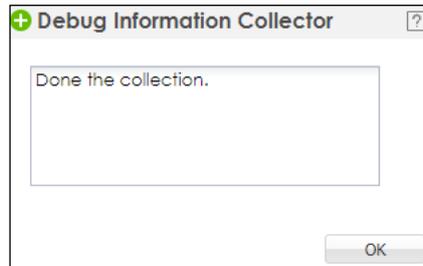
The screenshot shows the 'AP General Setting' window. It features two list boxes: 'Available Aps' on the left containing AP02, AP03, AP04, AP05, and AP06; and 'Collected APs' on the right containing AP01. A red box highlights AP01 in the 'Collected APs' list. Below these lists are navigation arrows and a checkbox labeled 'Copy the diagnostic file to USB storage (if ready)'. Under the 'Diagnostic collect Category' section, several categories are checked: System, Networking, Interface, CAPWAP, Wireless, AAA, Logs, and Others. The 'Customized' category is unchecked, with a 'Script:' dropdown menu below it. At the bottom right, there are 'Apply' and 'Collect Now' buttons, with 'Collect Now' highlighted by a red box.

- A window pops up when the controller is collecting the diagnostic.

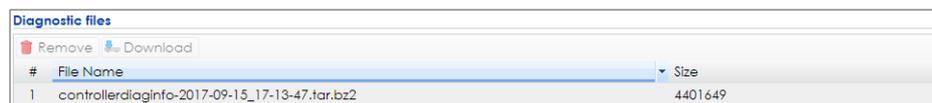
The screenshot shows a dialog box titled 'Debug Information Collector'. Inside the dialog, there is a text area containing the message 'Please wait, collecting...'. At the bottom right of the dialog, there is a 'Cancel' button.

8.1.2 Test the Result

- 1 When the collection finished, a pop-up window shows "**Done the collection.**"



- 2 After capturing the packet, there is a file in **MAINTENANCE > Diagnostics > Diagnostic > Files** for downloading.



Diagnostic files		
Remove Download		
#	File Name	Size
1	controllerdiaginfo-2017-09-15_17-13-47.tar.bz2	4401649

8.2 How to Configure the E-mail Settings for Sending Logs?

This configuration set email for sending logs and let the controller manager gets the daily report and the system logs.

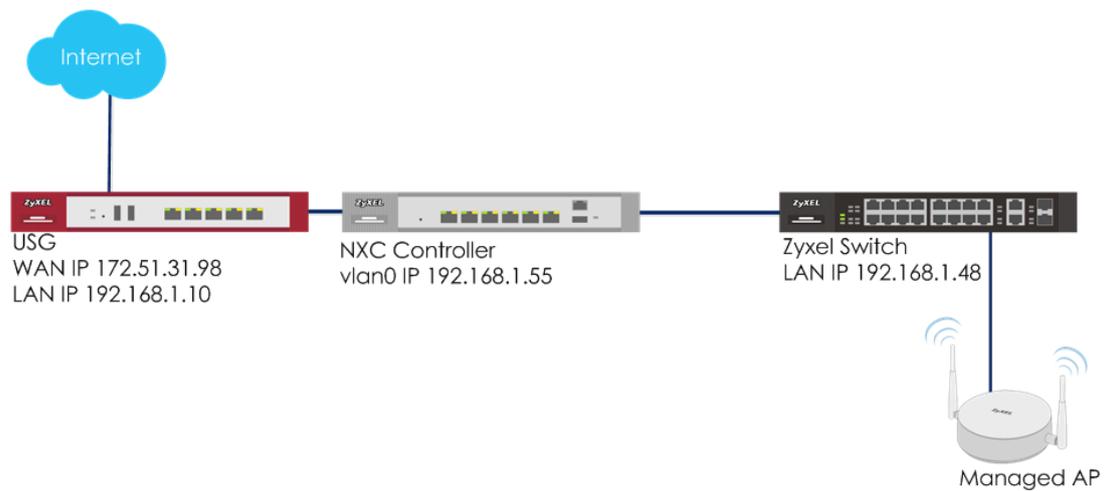


Figure 8.2 E-mail Settings for Sending Logs



Note:

All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG20v2 (Firmware Version: V4.15), NXC2500 (Firmware Version: 5.40), GS2210-8HP (Firmware Version: V4.30).

8.2.1 Configure Log & Report

- 1 Configure daily report in **CONFIGURATION > Log & Report > Email Daily Report**.

In **Email Settings**, enter the **Mail Server** which can send out the email. Check the **Append data time** for daily report, and set the email address in **Mail From** and **Mail To**. Click **Apply** to save the setting.

General Settings

Enable Email Daily Report

Email Settings

Mail Server: (Outgoing SMTP Server Name or IP Address)

SSL/TLS Encryption: (dropdown)

Mail Server Port: (1-65535) (Optional)

Mail Subject:

Append system name

Append date time

Mail From: (Email Address)

Mail To: (Email Address)

(Email Address)

(Email Address)

(Email Address)

SMTP Authentication

User Name:

Password:

Retype to Confirm:

Schedule

Time For Sending Report: (hours) (minutes)

Report Items

System Resource Usage

CPU Usage

Memory Usage

Session Usage

Port Usage

2 Configure daily report in **CONFIGURATION > Log & Report > Log Settings**.

In **Log Settings**, click the first setting and **Edit** it. Check **Active** to activate this setting. Enter the **Mail Server**, and set the email address in **Mail From** and **Mail To**. Set the sending condition to **Daily and When Full**, and the **Time for Sending Log**. Click **OK** to save.

Edit Log Setting

E-mail Server 1

Active

Mail Server: (Outgoing SMTP Server Name or IP Address)

SSL/TLS Encryption: (v)

Mail Server Port: (1-65535) (Optional)

Mail Subject:

Append system name

Append date time

Send From: (E-Mail Address)

Send Log to: (E-Mail Address)

Send Alerts to: (E-Mail Address)

Sending Log: (v)

Day for Sending Log: (v)

Time for Sending Log: (🕒)

8.2.2 Test the Result

- 1 The manager who has the email receives the system Daily report.

Top Host IP Address/User			
#	Direction	IP Address/User	Amount
1	Tx To	239.255.255.250	509.635 (MBytes)
2	Rx From	10.214.30.230	83.529 (MBytes)
3	Rx From	192.168.1.2	74.376 (MBytes)
4	Rx From	10.214.20.52	52.311 (MBytes)
5	Rx From	10.214.20.90	51.360 (MBytes)
6	Tx To	10.214.60.255	49.809 (MBytes)
7	Rx From	10.214.60.57	40.584 (MBytes)
8	Rx From	10.214.20.11	31.258 (MBytes)
9	Tx To	224.0.0.251	29.546 (MBytes)
10	Tx To	255.255.255.255	25.069 (MBytes)
11	Rx From	10.214.100.15	22.196 (MBytes)
12	Rx From	10.214.60.142	19.341 (MBytes)
13	Rx From	10.214.60.62	17.357 (MBytes)
14	Rx From	10.214.60.72	12.570 (MBytes)
15	Rx From	10.214.60.45	12.087 (MBytes)
16	Rx From	10.214.60.42	11.014 (MBytes)
17	Rx From	10.214.60.43	10.201 (MBytes)
18	Rx From	10.214.60.54	9.801 (MBytes)
19	Tx To	224.0.0.252	8.910 (MBytes)
20	Rx From	10.214.60.112	8.829 (MBytes)

- The manager who has the email receives the log daily or when it's full.

No.	Date/Time Priority Message	Source Category	Destination Note
1	2017-09-18 14:12:42 info	wlan-dcs	WLAN DCS
	Radio2 configure DCS as INTERVAL mode		
2	2017-09-18 14:12:45 info	capwap	
	Updated Configuration by a WLAN Controller Success. Partial Update [count=2]		
3	2017-09-18 14:12:50 info	wlan-dcs	WLAN DCS
	Radio1 configure DCS as INTERVAL mode		
4	2017-09-18 14:14:05 info	wlan-dcs	WLAN DCS
	Radio1 DCS start channel selection procedure		
5	2017-09-18 14:14:05 info	wlan-dcs	WLAN DCS
	Radio2 DCS start channel selection procedure		
6	2017-09-18 14:14:05 info	wlan-dcs	WLAN DCS
	Radio1 DCS change channel from 6 to 11. (At first time.)		
7	2017-09-18 14:14:05 info	wlan-dcs	WLAN DCS
	Radio2 DCS change channel from 36 to 40. (At first time.)		
8	2017-09-18 14:15:50 info	wlan-dcs	WLAN DCS
	Radio1 DCS start channel selection procedure		
9	2017-09-18 14:15:50		