

Switch Series

Edition 2023.1

Handbook

Default Login Details

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

Contents

Basic principles for network management	7
1.1 How to change the switch management IP address to avoid accessing the wrong device	7
1.1.1 Configuration in the Switch-2	8
1.1.2 Test the Result	10
1.2 How to configure the switch with a device name to avoid accessing the wrong device	11
1.2.1 Configuration in Switch-1	12
1.2.2 Test the Result	13
1.3 How to configure the switch to update the time from an NTP server	14
1.3.1 Configuration in Switch	15
1.3.2 Test the Result	16
1.3.3 What could go wrong?	18
1.4 How to configure the switch to backup events on a SYSLOG server	19
1.4.1 Configure the Switch-1	20
1.4.2 Test the Result	22
1.4.3 What could go wrong?	23
1.5 How to configure the switch with a port name to quickly identify directly connected devices	24
1.5.1 Configure Switch-1	25
1.5.2 Test the Result	26
1.6 How to collect the Diagnostic Info	27
1.6.1 Collect the Diagnostic Info from web GUI	28
1.6.2 Test the Result	29
1.7 How to change the default administrator password	30
1.7.1 Change the default administrator password	31
1.7.2 Test the Result	32
1.8 How to configure a whitelist for remote management to prevent unauthorized access	33
1.8.1 Configure the whitelist of the remote management	34
1.8.2 Test the Result	35
1.8.3 What could go wrong?	35
Designing the Local Area Network	37
2.1 How to configure the switch to separate traffic between departments using VLAN	37
2.1.1 Configure Switch-1	38
2.1.2 Configure Switch-2	40
2.1.3 Test the Result	42
2.2 How to configure the switch to route traffic across VLANs	43
2.2.1 Configure VLAN 10	44
2.2.2 Configure VLAN 20	46

2.2.3 Set the gateway on PC-1 and PC-2	48
2.2.4 Test the Result	50
2.2.5 What could go wrong	51
2.3 How to configure the switch to perform DHCP service in a VLAN	52
2.3.1 Configure VLAN 10	53
2.3.2 Configure VLAN 20	55
2.3.3 Configure the Switch and PC	57
2.3.4 Test the Result	60
2.3.5 What Could Go Wrong	61
2.4 How to Configure the Switch to Translate Customer VLAN to Service Provider VLAN	62
2.4.1 Configuration on the Core Switch	64
2.4.2 Configuration on the Edge Switch	66
2.4.3 Test the Results	69
Improving Network Reliability	72
3.1 How to configure a stacked switch to ensure high server availability	72
3.1.1 Configure Switch-1 and Switch-2 for Stacking	72
3.1.2 Configure Link Aggregation on Stacked switch	75
3.1.3 Configure Link Aggregation on Switch-3	75
3.1.4 Test the Result	77
3.1.5 What Could Go Wrong	78
3.2 How to configure RSTP in a ring topology	79
3.2.1 Configure Switch	80
3.2.2 Test the Result	82
3.2.3 What Could Go Wrong	84
3.3 How to configure VRRP to provide hosts with a redundant gateway	85
3.3.1 Configuration in the Gateway-A	86
3.3.2 Configuration in the Gateway-B	89
3.3.3 Test the Result	92
3.3.4 What Could Go Wrong?	93
3.4 How to configure bandwidth control to limit incoming or outgoing traffic rate	94
3.4.1 Configure Switch	95
3.4.2 Test the Result	96
3.5 How to configure ACL to rate limit IP traffic	97
3.5.1 Configure VLAN and Route Traffic	98
3.5.2 Configure the Classifier	99
3.5.3 Configure the ACL (Policy Rule)	101
3.5.4 Test the Result	103
3.5.5 What Could Go Wrong	105

3.6 How to Implement VRRP with Multiple Routing Interface Combine with HA-pro Using Zyxel Enterprise Switch	106
3.6.1 Configuration	108
3.6.2 Verification	123
3.6.3 What may go wrong?	125
3.7 How to Configure the Switch to Tunnel Layer 2 Protocol Packets Through Service Provider Network	126
3.7.1 Configuration on the Edge Switch	128
3.7.2 Configuration on the Customer Switch	131
3.7.3 Test the Results	134
3.7.4 What Could Go Wrong	136
Designing an IPTV Network	137
4.1 Introduction for IGMP	137
4.1.1 What are General Queries and Group Specific Queries?	137
4.1.2 What are IGMP Snooping Querier Modes?	137
4.1.3 What are the differences between IGMP Snooping fast/normal/immediate leave?	137
4.2 How to configure IGMP routing for multicast clients in a different LAN	139
4.2.1 Configure Switch-1	140
4.2.2 Configure Switch-2	141
4.2.3 Test the Result	142
4.2.4 What Could Go Wrong	143
4.3 How to configure IGMP Snooping for multicast clients in the same LAN	144
4.3.1 Configure Switch	145
4.3.2 Test the Result	146
Network Security	147
5.1 How to configure the port security to limit the number of connected devices	147
5.1.1 Configure Switch-1	148
5.1.2 Test the Result	149
5.1.3 What Could Go Wrong	150
5.2 How to configure MAC filter to block unwanted traffic	151
5.2.1 Configure Switch-1	152
5.2.2 Test the Result	153
5.2.3 What Could Go Wrong	154
5.3 How to configure the switch to prevent IP scanning	155
5.3.1 Configuration in the Switch	156
5.3.2 Test the Result	157
5.3.3 What Could Go Wrong?	160

- 5.4 How to Configure the Switch and RADIUS Server to Provide Network Access through 802.1x Port Authentication 161**
 - 5.4.1 Configuration in the Switch 162
 - 5.4.2 Configuration in the RADIUS-Server 162
 - 5.4.3 Test the Result 164
 - 5.4.4 What May Go Wrong? 167
- 5.5 How to configure the switch to send unauthorized users in a guest VLAN 168**
 - 5.5.1 Configure 802.1x Port Authentication on the Switch 169
 - 5.5.2 Configure VLAN for Guest VLAN 169
 - 5.5.3 Configure Guest VLAN for Failed Authentication..... 169
 - 5.5.4 Configure the RadiusServer..... 169
 - 5.5.5 Configure the setting on User-A, User-B and Guest..... 170
 - 5.5.6 Test the Result 172
 - 5.5.7 What Could Go Wrong? 173
- 5.6 How to Configure the Switch and RADIUS Server to Provide Network Access through Device MAC Address 175**
 - 5.6.1 Configuration in the Switch 176
 - 5.6.2 Configuration in the RADIUS-Server 178
 - 5.6.3 Test the Result 179
 - 5.6.4 What Could Go Wrong? 180
- 5.7 How to configure the switch to prevent ARP spoofing 181**
 - 5.7.1 Configuration in the Switch 182
 - 5.7.2 Test the Result 184
 - 5.7.3 What Could Go Wrong? 185
- 5.8 How to Configure the Switch to Protect Against Rogue DHCP Servers 186**
 - 5.8.1 Configuration in the Switch 187
 - 5.8.2 Test the Result 190
 - 5.8.3 What Could Go Wrong? 191
- 5.9 How to configure IPSG static binding for trusted network devices. 192**
 - 5.9.1 Configuration in the Switch 193
 - 5.9.2 Test the Result 194
- 5.10 How to configure ACL to block unwanted traffic 195**
 - 5.10.1 Configure VLAN and Route Traffic 196
 - 5.10.2 Configure the Classifier 197
 - 5.10.3 Configure the Policy Rule 198
 - 5.10.4 Test the Result 199
 - 5.10.5 What Could Go Wrong 200
- 5.11 How to use ACL to mirror traffic of a specific criteria 201**
 - 5.11.1 Configuration of ACL 203
 - 5.11.2 Test the Result 207

- 5.11.3 What May Go Wrong 208
- 5.12 How to Separate Traffic through L2 Port Isolation 209**
 - 5.12.1 Configuration in the Switch 212
 - 5.12.2 Test the Result 214
 - 5.12.3 What May Go Wrong 216
- Implementing VOIP 217**
- 6.1 How to configure an IP Phone's VLAN using LLDP-MED 217**
 - 6.1.1 Configure VLAN for IP Phone 218
 - 6.1.2 Configure Switch 219
 - 6.1.3 Test the Result 220
 - 6.1.4 What Could Go Wrong 221
- 6.2 How to configure the switch to separate VOIP traffic from data traffic 222**
 - 6.2.1 Configure VLAN 100 for IP Phone 223
 - 6.2.2 Configure Voice VLAN 224
 - 6.2.3 Test the Result 225
 - 6.2.4 What Could Go Wrong 226
- 6.3 How to configure the switch to improve Voice traffic quality 227**
 - 6.3.1 Configure VLAN for voice traffic 228
 - 6.3.2 Configure Voice VLAN 229
 - 6.3.3 Configure Mirroring (For "Test the Result") 230
 - 6.3.4 Test the Result 231
 - 6.3.5 What Could Go Wrong 232

Basic principles for network management

1.1 How to change the switch management IP address to avoid accessing the wrong device

This example shows administrators how to use the Web GUI to manage the IP addresses of the switches and avoid administrators from unintentionally accessing the wrong devices. As shown below, there are two switches in the environment. Both default IP addresses of the two switches are 192.168.1.1.

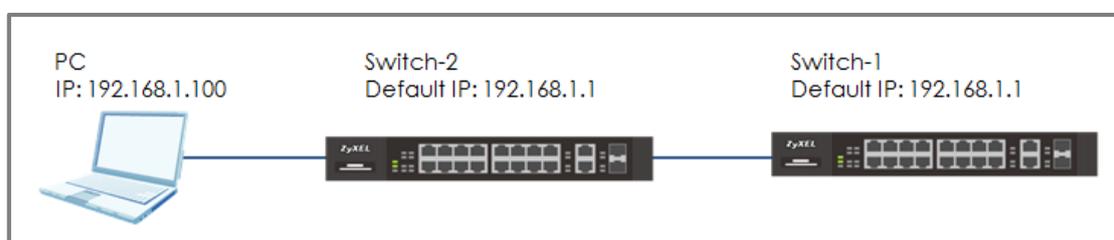


Figure 1 Two switches are using the same default IP address

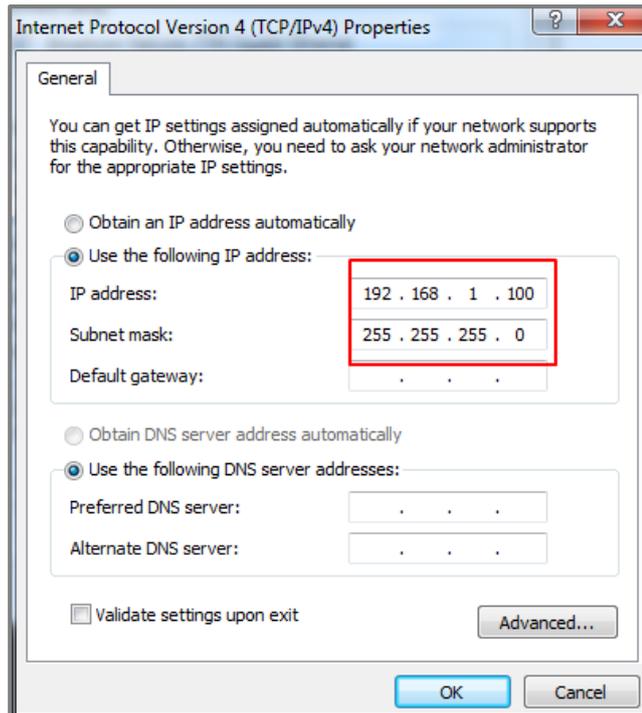


Note:

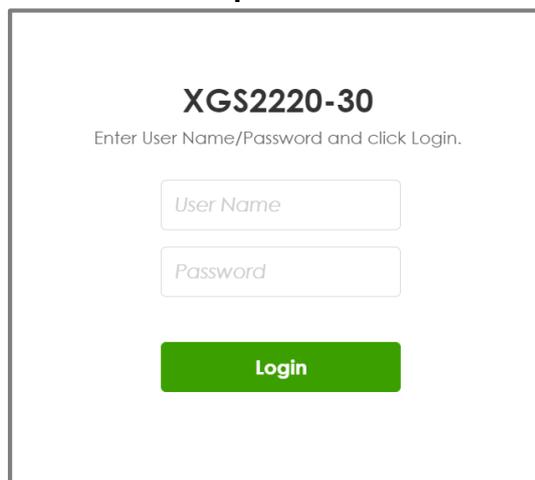
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using XGS2220-30 (Firmware Version: V4.80).

1.1.1 Configuration in the Switch-2

- 1 Disconnect the link between Switch-1 and Switch-2.
- 2 Set the PC's IP address on to the same subnet as the switches.
For example, set the PC IP address as **192.168.1.100**.



- 3 Open a browser (IE, Chrome, Safari, Firefox, etc...). Go to website **http://192.168.1.1** (default management IP address). Key in "**username: admin; password: 1234**" and log in.



- 4 Enter the webpage and go to **Menu > SYSTEM > IP Setup > IP Setup > IP Interface > Add/Edit**. Set the IP address you prefer, for example **192.168.1.2**. Then click **Apply**.

DHCP Client

Option-60

Class-ID

Static IP Address

IP Address

IP Subnet Mask

VID

- 5 Log back in using the new IP address **192.168.1.2**. After logging in again, remember to click the **Save** icon to save the new configurations.



1.1.2 Test the Result

- 1 Log in via the web GUI and go to **Menu > SYSTEM > IP Setup > IP Status**. Check if the IP address is already configured as **192.168.1.2**.

IP Interface						
Index	IP Address	IP Subnet Mask	VID	Type	Action	
1	192.168.1.2	255.255.255.0	1	Static		

1.2 How to configure the switch with a device name to avoid accessing the wrong device

This example shows administrators how to use the Web GUI to manage device name and avoid accessing the wrong devices. As shown below, the PC connects with Switch-1 in the environment. In the default setting, device name (System Name) will be the model name (XGS2220 in this example).

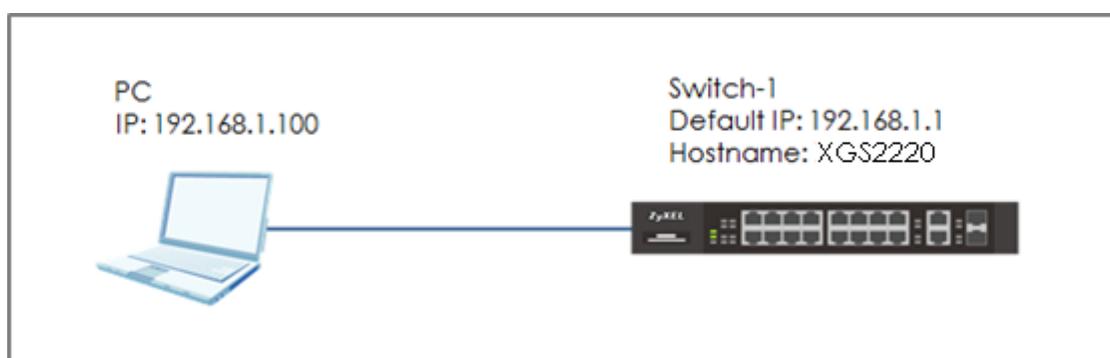


Figure 2 Change the device name of the switch



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 XGS2220-30 (Firmware Version: V4.80).

1.2.1 Configuration in Switch-1

- 1 Enter the web GUI and go to **Menu > SYSTEM > General Setup**. Change the System Name (Switch-1 in this example) and click **Apply**.

The screenshot shows a configuration page with the following fields and values:

- System Name: Switch-1 (highlighted with a red box)
- Location: (empty)
- Contact Person's Name: (empty)
- Use Time Server when Bootup: NTP(RFC-1305) (dropdown)
- Time Server IP Address: 216.239.35.12
- Time Server Sync Interval: 1440 minutes
- Current Time: 14 : 07 : 49 UTC+08:00
- New Time (hh:mm:ss): 14 : 07 : 49
- Current Date: 2022 - 11 - 24
- New Date (yyyy-mm-dd): 2022 - 11 - 24
- Time Zone: UTC+08:00 (dropdown)
- Daylight Saving Time: Off (radio button)
- Start Date: First Sunday of January at 0:00 (dropdowns)
- End Date: First Sunday of January at 0:00 (dropdowns)

Buttons: Apply (green), Cancel (grey)

- 2 Click **“Save”** to save the configuration.



1.2.2 Test the Result

Enter the web GUI and you will see the page of the switch information. Check if the **System Name** is the name you configured (**Switch-1** in this example) or not.

System Information	
System Name Switch-1	System Location
Boot Version V1.00 06/13/2022	ZyNOS F/W Version V4.80(ABXN.0) 08/03/2022
System Time 11/23/2022 15:10:52	System Uptime 007 days,09 hours,10 mins,16 secs

1.3 How to configure the switch to update the time from an NTP server

This example shows administrators how to use the NTP server to update the system time of the switch. As shown below, the PC connects with Switch and Switch connects with the USG in the environment.

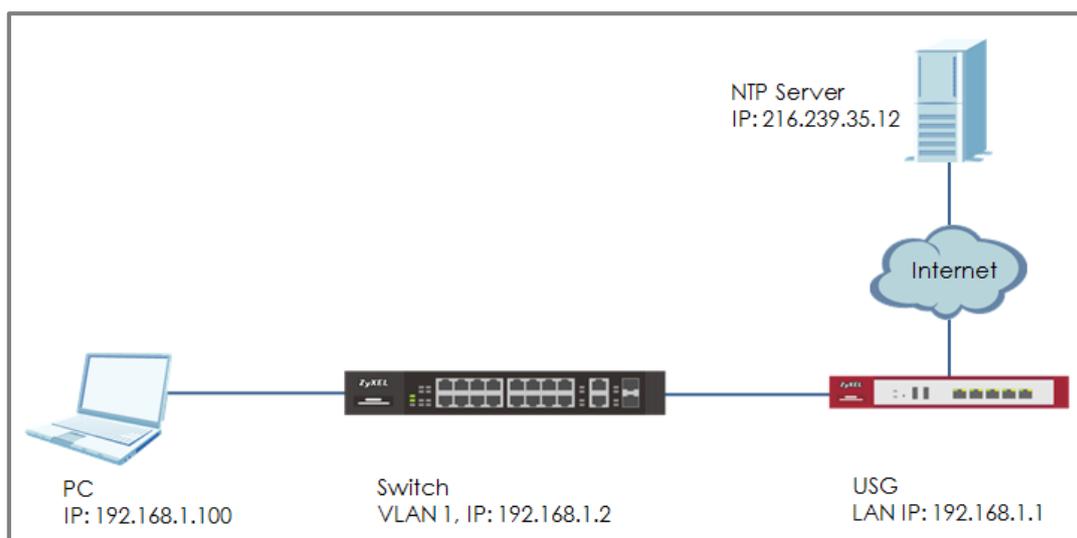


Figure 3 Set up Switch to get time from NTP Server



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 XGS2220-30 (Firmware Version: V4.80). We use google free public NTP server (216.239.35.12) to be our NTP server. You can also choose another available NTP server. Furthermore, due to there is routing set up in this configuration, the user interface might be some difference for other models.

1.3.1 Configuration in Switch

- 1 Enter the web GUI and go to **Menu > SYSTEM > IP Setup > IP Setup > IP Setup**. Set the default Gateway as USG IP: **192.168.1.1**. Then click **“Apply”**.

IP Setup

Default Gateway

Domain Name Server 1

Domain Name Server 2

- 2 Go to **Menu > SYSTEM > General Setup**. Select **“Use Time Server when Bootup”** to **NTP(RFC-1305)** and set the **“Time Server IP Address”**. In this scenario, we use the google free public NTP server (**216.239.35.12**) as an example. Also, select the **“Time Zone”** in your location. Finally, remember to click **“Apply”**.

Use Time Server when Bootup

Time Server IP Address

Time Server Sync Interval minutes

Current Time : : UTC+00:00

New Time (hh:mm:ss) : :

Current Date - -

New Date (yyyy-mm-dd) - -

Time Zone

Daylight Saving Time OFF

Start Date of at

End Date of at

- 3 Click **Save** to save the configuration.



1.3.2 Test the Result

- 1 Go to **Menu > SYSTEM > General Setup**. Both the Current Time and Current Date should be the current time in your location. If the current time is not updated as the correct time, click **“Refresh”**.

Use Time Server when Bootup: NTP(RFC-1305)
Time Server IP Address: 216.239.35.12
Time Server Sync Interval: 1440 minutes
Current Time: 14 : 07 : 49 UTC+08:00
New Time (hh:mm:ss): 14 : 07 : 49
Current Date: 2022 - 11 - 24
New Date (yyyy-mm-dd): 2022 - 11 - 24
Time Zone: UTC+08:00
Daylight Saving Time: OFF
Start Date: First Sunday of January at 0:00
End Date: First Sunday of January at 0:00



- 2 Try to select the “User Time Server when Bootup” as **None**. Few second later, change back to **NTP(RFC-1305)**. The time will still update to the current time.

Use Time Server when Bootup: None
Time Server IP Address: 216.239.35.12
Time Server Sync Interval: 1440 minutes
Current Time: 22 : 16 : 37 UTC+08:00
New Time (hh:mm:ss): 22 : 16 : 37
Current Date: 2022 - 11 - 24
New Date (yyyy-mm-dd): 2022 - 11 - 24
Time Zone: UTC+08:00
Daylight Saving Time: OFF
Start Date: First Sunday of January at 0:00
End Date: First Sunday of January at 0:00

Use Time Server when Bootup	NTP(RFC-1305) ▾
Time Server IP Address	216.239.35.12
Time Server Sync Interval	1440 minutes
Current Time	22 : 18 : 11 UTC+08:00
New Time (hh:mm:ss)	22 : 18 : 11
Current Date	2022 - 11 - 24
New Date (yyyy-mm-dd)	2022 - 11 - 24
Time Zone	UTC+08:00 ▾
Daylight Saving Time	<input type="radio"/> OFF
Start Date	First ▾ Sunday ▾ of January ▾ at 0:00 ▾
End Date	First ▾ Sunday ▾ of January ▾ at 0:00 ▾

1.3.3 What could go wrong?

- 1 Switch may not be able to access the NTP Server successfully. Follow the step to test if NTP Server is available. Go to **Menu > Maintenance > Diagnostic**. Select IPv4 and type the IP address of NTP Server (216.239.35.12) into the IP Address field. Click **“Ping”**.

The screenshot displays a diagnostic tool interface with two main sections: 'Ping Test' and 'Trace Route Test'. The 'Ping Test' section is active, showing a table of results for a ping to 216.239.35.12. The table has columns for 'sent', 'rcvd', 'rate', 'rtt', 'avg', 'mdev', 'max', and 'min reply from'. Three rows of data are shown, all with a 100% success rate. The 'Trace Route Test' section is inactive. The 'Ping Test' configuration shows 'IPv4' selected, 'IP Address/Host Name' set to '216.239.35.12', 'Source IP Address' empty, and 'Count' set to '3'. A 'Ping' button is visible at the bottom left.

sent	rcvd	rate	rtt	avg	mdev	max	min	reply from
1	1	100	9	9	0	9	9	216.239.35.12
2	2	100	7	9	1	9	7	216.239.35.12
3	3	100	7	9	1	9	7	216.239.35.12

Ping Test

IPv4
 IPv6

IP Address/Host Name: 216.239.35.12

Source IP Address: []

Count: 3

Trace Route Test

IPv4
 IPv6

IP Address/Host Name: []

TTL: 30

Wait Time: 2 Seconds

Queries: 3

Ping

1.4 How to configure the switch to backup events on a SYSLOG server

The example shows administrators how to set up the switch to send system log events to a remote syslog server.

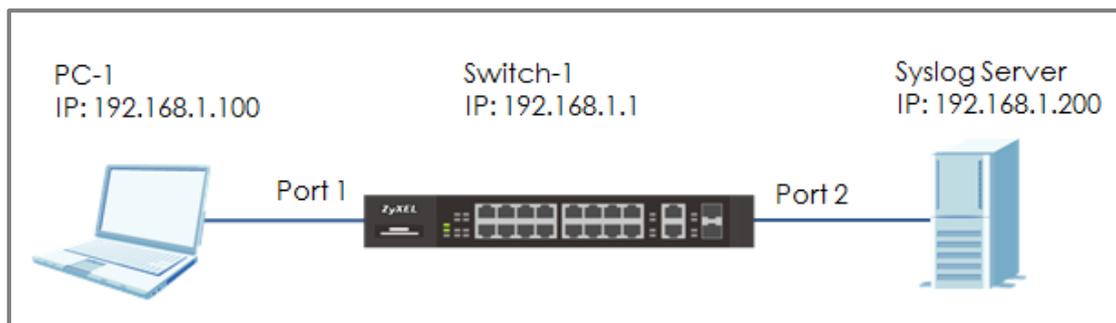


Figure 4 Upload the syslog automatically to the server



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 XGS2220-30 (Firmware Version: V4.80).

1.4.1 Configure the Switch-1

- 1 Enter the web GUI and go to **Menu > SYSTEM > Syslog Setup > Syslog Server Setup > Add/Edit**. Enable the **Activate** setting and set up the server IP address. In this example, it is **192.168.1.200**. Choose the Log Level you prefer (**Level 0-7** in this example). The wider the range, the more detailed log will be recorded. Remember to click **“Apply”**.

Active ON

Server Address

UDP Port

Log Level

Note:
Log Level refers to which events should be sent to the Syslog Server.
Severity: Emergency (0), Alert (1), Critical (2), Error (3), Warning (4), Notice (5), Informational (6), and Debug (7).

- 2 In the same page, activate the **Syslog** and activate the logging type you prefer. Also, remember to click **“Apply”**.

Syslog Setup

Active ON

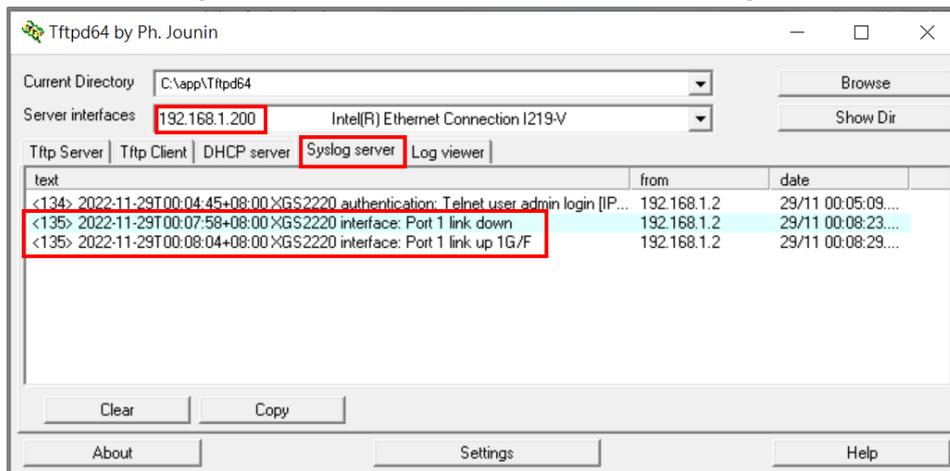
Logging Type	Active	Facility
System	<input checked="" type="checkbox"/>	local use 0
Interface	<input checked="" type="checkbox"/>	local use 0
Switch	<input checked="" type="checkbox"/>	local use 0
AAA	<input checked="" type="checkbox"/>	local use 0
IP	<input checked="" type="checkbox"/>	local use 0

3 Click **Save** to save the configuration.

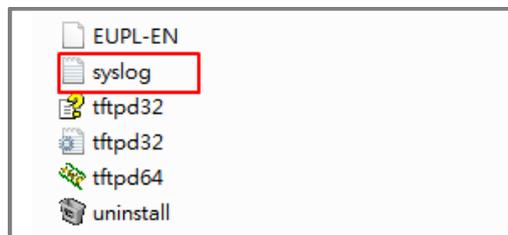


1.4.2 Test the Result

- 1 Unplug and re-plug PC-1 from the switch.
- 2 The Syslog Server should receive an event log from the switch.

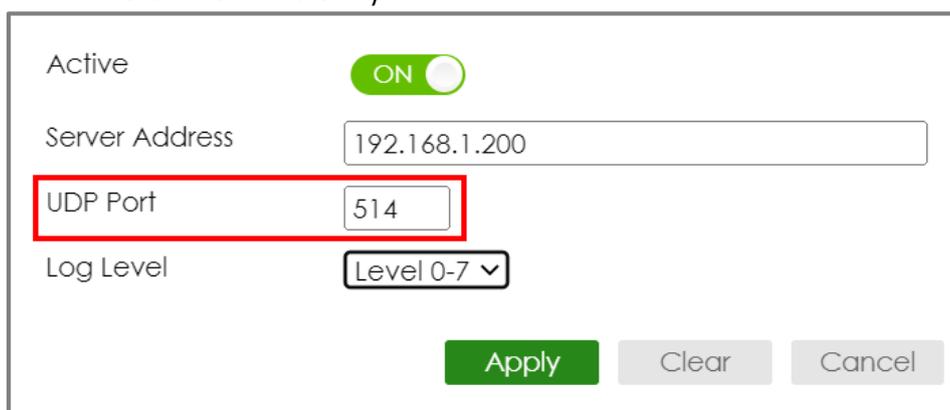


- 3 We can also check the **directory** ("C:\app\Tftpd64" in this example) to find out if a text file is created on the Syslog Server.



1.4.3 What could go wrong?

- 1 If Switch-1 and Syslog Server are in different subnets, remember to set **default gateway** so that Switch-1 and the Syslog Server can communicate with each other.
- 2 Confirm the service port number of the Switch-1 and the Syslog Server are the same. (Default service port for the Syslog Server in the Switch-1 is **514**).



The screenshot shows a configuration window for Syslog. It includes a toggle for 'Active' (set to ON), a text field for 'Server Address' (192.168.1.200), a text field for 'UDP Port' (514, highlighted with a red box), and a dropdown for 'Log Level' (Level 0-7). At the bottom are 'Apply', 'Clear', and 'Cancel' buttons.

1.5 How to configure the switch with a port name to quickly identify directly connected devices

The example shows administrators how to configure the switch with a port name to quickly identify directly connected devices. By doing this, administrators can quickly identify which port connects to which device, location, or section of the network.

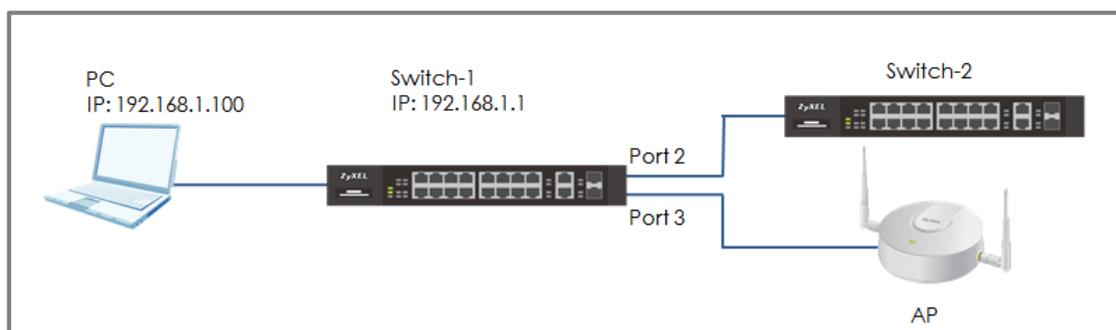


Figure 5 Configure the port name of the switch



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 XGS2220-30 (Firmware Version: V4.80).

1.5.1 Configure Switch-1

- 1 Enter the web GUI and go to **Menu > Port > Port Setup**. Type the name of each directly connected devices on the corresponding port name. For example, you can type Switch-2 in port 2 and AP in port 3. Then click **“Apply”**.

Port	Active	Name	Speed / Duplex	Flow Control
*	<input type="checkbox"/>	<input type="text"/>	Auto <input type="text"/>	Disable <input type="text"/>
1	<input checked="" type="checkbox"/>	<input type="text"/>	Auto <input type="text"/>	Disable <input type="text"/>
2	<input checked="" type="checkbox"/>	Switch-2	Auto <input type="text"/>	Disable <input type="text"/>
3	<input checked="" type="checkbox"/>	AP	Auto <input type="text"/>	Disable <input type="text"/>
4	<input checked="" type="checkbox"/>	<input type="text"/>	Auto <input type="text"/>	Disable <input type="text"/>

- 2 Click **Save** to save the configuration.



1.5.2 Test the Result

- 1 Go to **Menu > Monitor > Port Status**. You will see the name you type in the column of name.

Port	Name	Link	State	LACP
1		Down	STOP	Disabled
2	Switch-2	1G/F	FORWARDING	Disabled
3	AP	1G/F	FORWARDING	Disabled

1.6 How to collect the Diagnostic Info

The example shows local administrators how to collect the Diagnostic Info by web GUI. The Diagnostic Info is a set of logs that includes useful information such as System Information, CPU utilization history, system logs and debug reports for issue analysis.



Figure 6 Collect the Diagnostic Info from web GUI

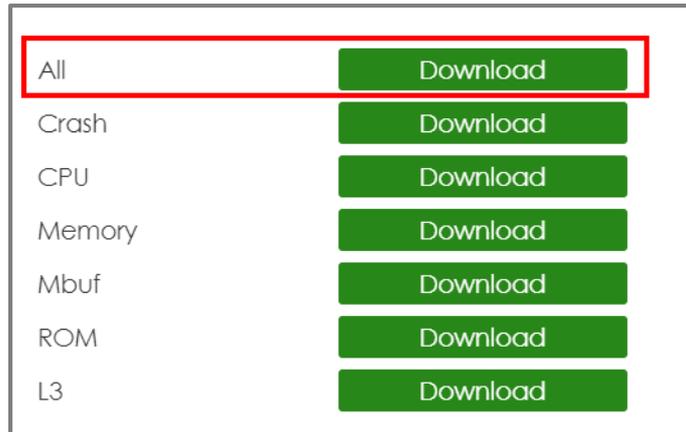


Note:

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 XGS2220-30 (Firmware Version: V4.80).

1.6.1 Collect the Diagnostic Info from web GUI

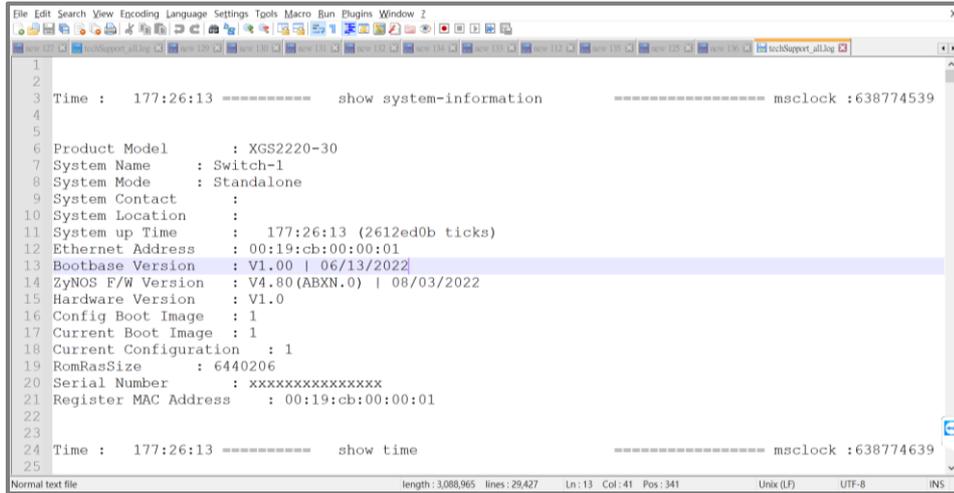
- 1 Enter the web GUI and go to **Menu > Maintenance > Tech-Support**. Click the Download button for **All**. You can also select the specific Diagnostic Info you need. (Ex: Crash, ROM,.....)



All	Download
Crash	Download
CPU	Download
Memory	Download
Mbuf	Download
ROM	Download
L3	Download

1.6.2 Test the Result

- 1 Open the file and you can view the Diagnostic Info. (In this example, we use the **Notepad++** to open the .txt file.)



```
1
2
3 Time : 177:26:13 ----- show system-information ----- mslock :638774539
4
5
6 Product Model      : XGS2220-30
7 System Name       : Switch-1
8 System Mode      : Standalone
9 System Contact    :
10 System Location   :
11 System up Time    : 177:26:13 (2612ed0b ticks)
12 Ethernet Address  : 00:19:cb:00:00:01
13 Bootbase Version  : V1.00 | 06/13/2022
14 ZyNOS F/W Version : V4.80 (ABXN.0) | 08/03/2022
15 Hardware Version  : V1.0
16 Config Boot Image : 1
17 Current Boot Image : 1
18 Current Configuration : 1
19 RomRasSize       : 6440206
20 Serial Number     : xxxxxxxxxxxxxxxxx
21 Register MAC Address : 00:19:cb:00:00:01
22
23 Time : 177:26:13 ----- show time ----- mslock :638774639
24
25
```

1.7 How to change the default administrator password

The example shows administrators how to change the default administrator password used for management access. Failure to change the default administrator password is a security risk that allows unauthorized user access to your device's management.

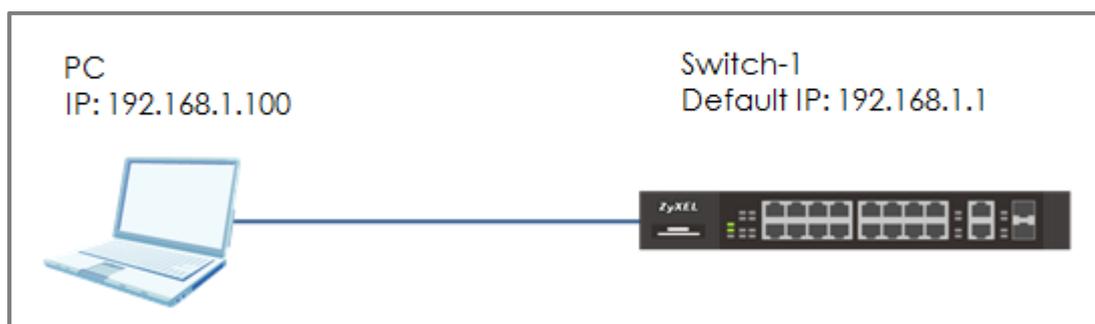


Figure 7 Change the default administrator password



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 XGS2220-30 (Firmware Version: V4.80).

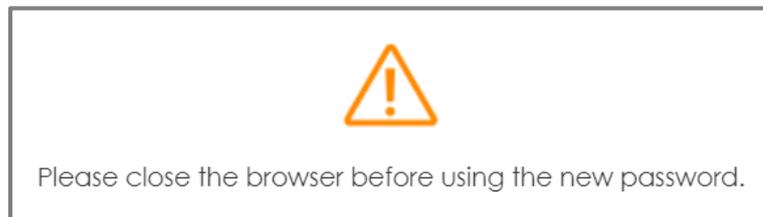
1.7.1 Change the default administrator password

- 1 Enter the web GUI and go to **Menu > System > Logins**. Enter the Old Password and New Password. Then click **“Apply”**.



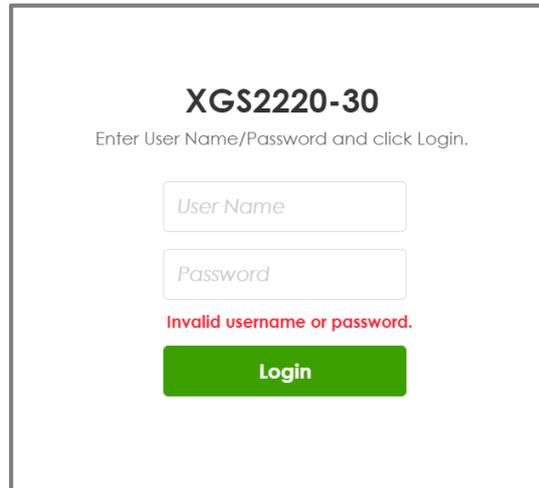
The screenshot shows a web form titled "Administrator" with three password input fields: "Old Password", "New Password", and "Retype to confirm". Each field contains four dots representing masked characters. Below the fields is a red warning icon and text: "Please record your new password whenever you change it. The system will lock you out if you have forgotten your password."

- 2 After clicking the **“Apply”**, the browser will show a message similar below.



1.7.2 Test the Result

- 1 Close the web GUI and login again with the **OLD** password. The login page will show "Invalid username or password".



The screenshot shows the login interface for a Zyxel device. At the top, the device model 'XGS2220-30' is displayed. Below it, the instruction 'Enter User Name/Password and click Login.' is shown. There are two input fields: 'User Name' and 'Password'. Below the password field, a red error message reads 'Invalid username or password.'. At the bottom of the form is a green 'Login' button.

- 2 Use the **new** password to login. Switch-1 web GUI should be accessible.

1.8 How to configure a whitelist for remote management to prevent unauthorized access

The example shows administrators how to configure a whitelist for host devices that prevents attempted access from unauthorized devices or subnets. The whitelist inspects the source IP addresses of hosts and the types of services accessing the switch (Ex: Telnet, FTP, HTTP.....).

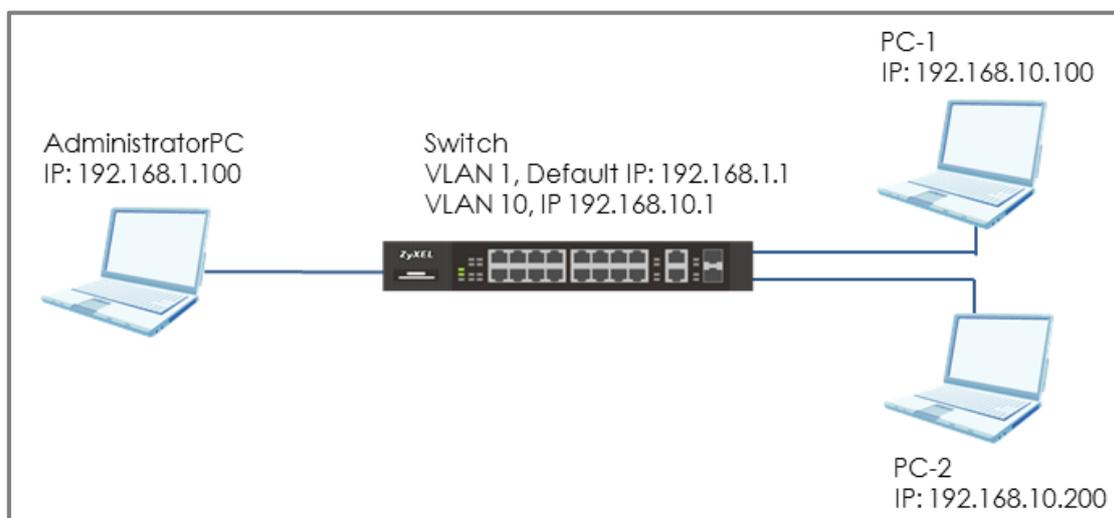


Figure 8 Configure the whitelist for remote management



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 XGS2220-30 (Firmware Version: V4.80).

1.8.1 Configure the whitelist of the remote management

- 1 Enter the web GUI and go to **Menu > Security > Access Control > Remote Management** using AdministratorPC. Enter the range of IP addresses and the corresponding types of services that are allowed to access the Switch. Then click **“Apply”**.

Entry	Active	Start Address	End Address	Telnet	FTP	HTTP	ICMP	SNMP	SSH	HTTPS
1	<input checked="" type="radio"/>	192.168.10.100	192.168.10.200	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	<input checked="" type="radio"/>	192.168.1.100	192.168.1.120	<input checked="" type="checkbox"/>						
3	<input type="radio"/>	0.0.0.0	0.0.0.0	<input type="checkbox"/>						
4	<input type="radio"/>	0.0.0.0	0.0.0.0	<input type="checkbox"/>						
5	<input type="radio"/>	0.0.0.0	0.0.0.0	<input type="checkbox"/>						
6	<input type="radio"/>	0.0.0.0	0.0.0.0	<input type="checkbox"/>						
7	<input type="radio"/>	0.0.0.0	0.0.0.0	<input type="checkbox"/>						
8	<input type="radio"/>	0.0.0.0	0.0.0.0	<input type="checkbox"/>						

1.8.2 Test the Result

- 1 In the setting, we set the IP range: **192.168.10.100-192.168.10.120**, which is allowed to access the Switch by all protocol types, EXCEPT **HTTP**. Therefore, if we use PC-1 (192.168.10.100) to access the Switch by **HTTP**, the Switch will refuse the connection. If we try to access the web GUI by **HTTPS** (Enter the **https://192.168.10.1**), PC-1 can connect to the Switch successfully.



- 2 The PC-2 (192.168.10.200) is not in the range which is allowed to access the Switch. PC-2 cannot access or ping the switch's management IP address.



- 3 AdministratorPC can access the Switch by **all** service types successfully.

1.8.3 What could go wrong?

- 1 The IP address is setting up repeatedly, but the setting is different. The logic rule of whitelist is **OR**.

For example, if we set the range of the IP addresses shown below. **192.168.10.120** is repeatedly set up accidentally. The result is that all types of services are **ALLOWED** for **192.168.10.120**.

Entry	Active	Start Address	End Address	Telnet	FTP	HTTP	ICMP	SNMP	SSH	HTTPS
1	<input checked="" type="checkbox"/>	192.168.10.100	192.168.10.120	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	<input checked="" type="checkbox"/>	192.168.10.120	192.168.1.120	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

- If the administrator has forgotten or lost track of the whitelisted IP addresses, the administrator will not be able to access the Switch. To solve this problem, use **Console** to verify the settings. Administrators can find out which IP addresses are allowed to access the Switch by reviewing the running configurations.

```
XGS2220#
XGS2220# show running-config
Building configuration...

Current configuration:

: Product Name = XGS2220-30
: Firmware Version = V4.80(ABXN.0) | 08/03/2022
no service-control snmp
no remote-management 1 service telnet ftp http
vlan 1
 name 1
 normal ""
 fixed 1-30
 forbidden ""
 untagged 1-30
 ip address 192.168.1.2 255.255.255.0
 ip address default-gateway 192.168.1.1
exit
interface route-domain 192.168.1.2/24
exit
interface vlan 1
 ipv6
 ipv6 address dhcp client ia-na
exit
time timezone 800
timesync server 216.239.35.12
timesync ntp
service-control http 80 180
remote-management 2
remote-management 1 start-addr 192.168.10.100 end-addr 192.168.10.200 service icmp snmp ssh https
```

Note:
If the Switch **does not support Console**, please check the manual of your Switch model to find out how to restore device to factory default settings.

Designing the Local Area Network

2.1 How to configure the switch to separate traffic between departments using VLAN

The example shows administrators how to set up the switch to make separate traffic between departments. Using **Static VLAN**, hosts accessing the same VLAN will only be able to communicate with hosts accessing the same VLAN.

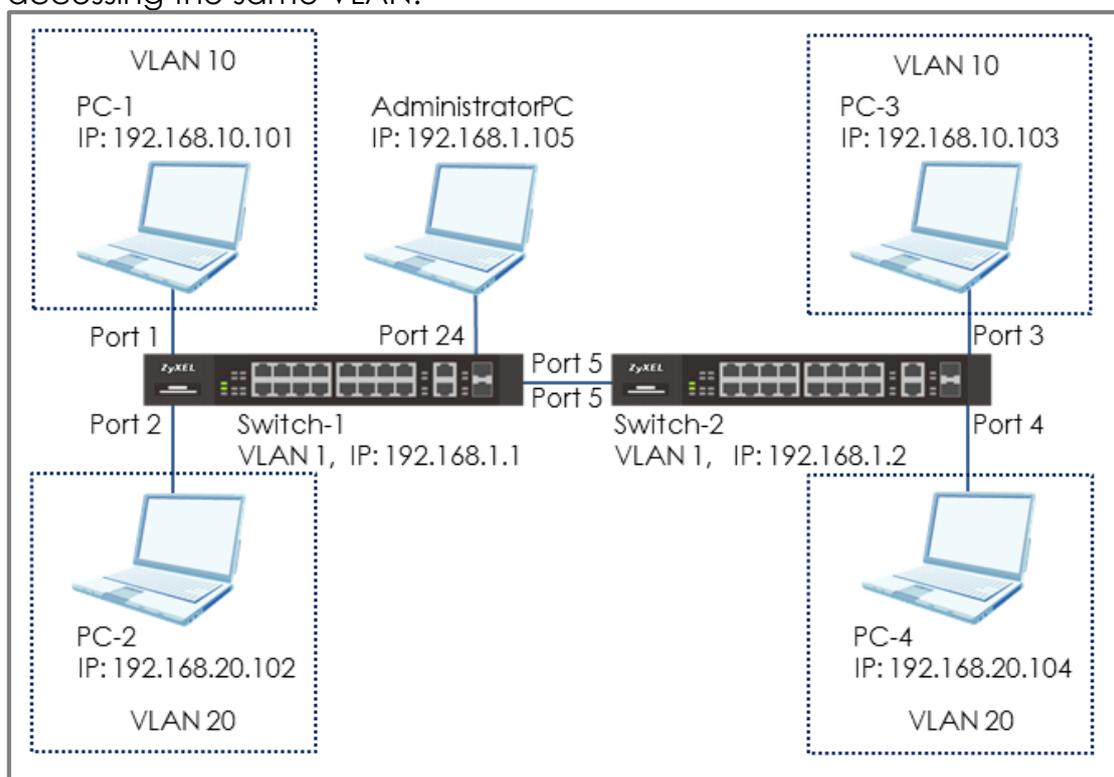


Figure 9 Set up VLAN to separate the traffic between departments



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 XGS2220-30 (Firmware Version: V4.80).

2.1.1 Configure Switch-1

- 1 Use AdministratorPC to set **VLAN 1** in **Switch-1**: Port 1, 2 as **Normal** port. (Prevent VLAN 1 broadcast packets to port 1, 2). Enter the web GUI and go to **Menu > Switching > VLAN > VLAN Setup > Static VLAN > Select VID 1 > Add/Edit**. Select port 1, 2 as **Normal**. Click **“Apply”**.

Port	Control	Tagging
*	Normal	<input checked="" type="checkbox"/> Tx Tagging
1	<input checked="" type="radio"/> Normal	<input type="checkbox"/> Tx Tagging
2	<input checked="" type="radio"/> Normal	<input type="checkbox"/> Tx Tagging
3	<input type="radio"/> Normal <input checked="" type="radio"/> Fixed	<input type="checkbox"/> Tx Tagging
4	<input type="radio"/> Normal <input checked="" type="radio"/> Fixed	<input type="checkbox"/> Tx Tagging
5	<input type="radio"/> Normal <input checked="" type="radio"/> Fixed	<input type="checkbox"/> Tx Tagging

- 2 Use AdministratorPC to create **VLAN 10** in **Switch-1**: Enter the web GUI and go to **Menu > Switching > VLAN > VLAN Setup > Static VLAN > Add/Edit**. Enable the **Active** setting. Type the Name and VLAN Group ID=**10**. Select port **1, 5** as **Fixed** and uncheck Tx Tagging (**Untagged**) on port 1 and check Tx Tagging (**Tagged**) on port 5. Click **“Apply”**.

Port	Control	Tagging
*	Normal	<input checked="" type="checkbox"/> Tx Tagging
1	<input type="radio"/> Normal <input checked="" type="radio"/> Fixed	<input type="checkbox"/> Tx Tagging
2	<input checked="" type="radio"/> Normal	<input checked="" type="checkbox"/> Tx Tagging
3	<input checked="" type="radio"/> Normal	<input checked="" type="checkbox"/> Tx Tagging
4	<input checked="" type="radio"/> Normal	<input checked="" type="checkbox"/> Tx Tagging
5	<input type="radio"/> Normal <input checked="" type="radio"/> Fixed	<input checked="" type="checkbox"/> Tx Tagging

- Use AdministratorPC to create **VLAN 20** in **Switch-1**: Enter the web GUI and go to **Menu > Switching > VLAN > VLAN Setup > Static VLAN > Add/Edit**. Enable the **Active** setting. Type the Name and VLAN Group ID=**20**. Select port 2, 5 as Fixed and uncheck Tx Tagging (**Untagged**) on port **2** and check Tx Tagging (**tagged**) on port **5**. Click "**Apply**".

Active ON

Name

VLAN Group ID

Port	Control			Tagging
*	Normal <input type="text" value="Normal"/>			<input checked="" type="checkbox"/> Tx Tagging
1	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
2	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
3	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
4	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
5	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging

- Set the PVID on **Switch-1**: Go to **Menu > Switching > VLAN > VLAN Setup > VLAN Port Setup**. Set port 1 as PVID=**10** (VLAN 10) and port 2 as PVID=**20** (VLAN 20).

Port	Ingress Check	PVID	Acceptable Frame Type	VLAN Trunking	Isolation
*	<input type="checkbox"/>	<input type="text"/>	All <input type="text" value="All"/>	<input type="checkbox"/>	<input type="checkbox"/>
1	<input type="checkbox"/>	<input type="text" value="10"/>	All <input type="text" value="All"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input type="text" value="20"/>	All <input type="text" value="All"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="text" value="1"/>	All <input type="text" value="All"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	<input type="text" value="1"/>	All <input type="text" value="All"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>	<input type="text" value="1"/>	All <input type="text" value="All"/>	<input type="checkbox"/>	<input type="checkbox"/>

2.1.2 Configure Switch-2

- 1 Use AdministratorPC to set **VLAN 1** in **Switch-2**: Port 3, 4 as **Normal** port (this prevents VLAN 1 from broadcasting packets to port 3, 4). Enter the web GUI and go to **Menu > Switching > VLAN > VLAN Setup > Static VLAN > Select VID 1 > Add/Edit**. Select port 3, 4 as **Normal**. Click **“Apply”**.

Port	Control			Tagging
*	Normal			<input checked="" type="checkbox"/> Tx Tagging
1	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
2	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
3	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
4	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
5	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging

- 2 Use AdministratorPC to create **VLAN 10** in **Switch-2**. Enter the web GUI and go to **Menu > Switching > VLAN > VLAN Setup > Static VLAN > Add/Edit**. Enable the **Active** setting. Type the Name and VLAN Group ID=**10**. Select port 3, 5 as **Fixed** and uncheck Tx Tagging (**Untagged**) on port 3 and check Tx Tagging (**tagged**) on port 5. Click **“Apply”**.

Port	Control			Tagging
*	Normal			<input checked="" type="checkbox"/> Tx Tagging
1	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
2	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
3	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
4	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
5	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging

- 3 Use AdministratorPC to create VLAN 20 in **Switch-2**. Enter the web GUI and go to **Menu > Switching > VLAN > VLAN Setup > Static VLAN > Add/Edit**. Enable the **Active** setting. Type the Name and VLAN Group ID=**20**. Select port 4, 5 as **Fixed** and uncheck Tx Tagging (**Untagged**) on port 4 and check Tx Tagging (**tagged**) on port 5. Click "**Apply**".

Active ON

Name

VLAN Group ID

Port	Control			Tagging
*	Normal <input type="text" value="Normal"/>			<input checked="" type="checkbox"/> Tx Tagging
1	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
2	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
3	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
4	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
5	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging

- 4 Set the PVID on **Switch-2**: Go to **Menu > Switching > VLAN > VLAN Setup > VLAN Port Setup**. Set port 3 as PVID=**10** (VLAN 10) and port 4 as PVID=**20**.

Port	Ingress Check	PVID	Acceptable Frame Type	VLAN Trunking	Isolation
*	<input type="checkbox"/>	<input type="text"/>	All <input type="text" value="All"/>	<input type="checkbox"/>	<input type="checkbox"/>
1	<input type="checkbox"/>	<input type="text" value="1"/>	All <input type="text" value="All"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input type="text" value="1"/>	All <input type="text" value="All"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="text" value="10"/>	All <input type="text" value="All"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	<input type="text" value="20"/>	All <input type="text" value="All"/>	<input type="checkbox"/>	<input type="checkbox"/>

2.1.3 Test the Result

- 1 The PC in the same VLAN can ping each other. PC-1 can ping PC-3 successfully, but PC-1 cannot ping PC-2.

```
C:\Users\User>ping 192.168.10.103 -t
Pinging 192.168.10.103 with 32 bytes of data:
Reply from 192.168.10.103: bytes=32 time<1ms TTL=128
Reply from 192.168.10.103: bytes=32 time<1ms TTL=128
Reply from 192.168.10.103: bytes=32 time<1ms TTL=128
```

```
C:\Users\User>ping 192.168.20.102
Pinging 192.168.20.102 with 32 bytes of data:
PING: transmit failed. General failure.
```

- 2 PC-2 can ping PC-4 successfully, but PC-2 cannot ping PC-3.

```
C:\Users\User>ping 192.168.20.104 -t
Pinging 192.168.20.104 with 32 bytes of data:
Reply from 192.168.20.104: bytes=32 time<1ms TTL=128
Reply from 192.168.20.104: bytes=32 time<1ms TTL=128
Reply from 192.168.20.104: bytes=32 time<1ms TTL=128
```

```
C:\Users\User>ping 192.168.10.103
Pinging 192.168.10.103 with 32 bytes of data:
PING: transmit failed. General failure.
```

2.2 How to configure the switch to route traffic across VLANs

The purpose of VLANs are to isolate one broadcast domain from another. If we would like hosts from different VLANs to communicate with each other, we have to set the switch to route traffic. The example shows how to configure the switch to route traffic across one VLAN to another.

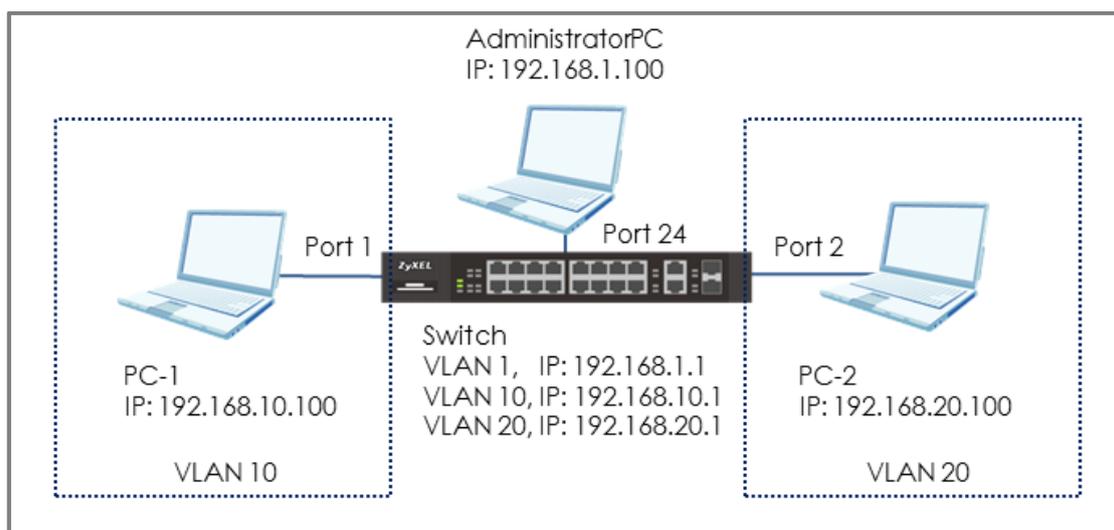


Figure 10 Set up switch to route traffic across VLANs



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 XS3800-28 (Firmware Version: V4.80).

2.2.1 Configure VLAN 10

- 1 Use AdministratorPC to create VLAN 10. Enter the web GUI and go to **Menu > Switching > VLAN > VLAN Setup > Static VLAN > Add/Edit**. Enable the **Active** setting. Type the Name and VLAN Group ID=10. Select port **1** as **Fixed** and uncheck Tx Tagging (Untagged). Click **“Apply”**.

Active ON

Name

VLAN Group ID

Port	Control			Tagging
*	Normal			<input checked="" type="checkbox"/> Tx Tagging
1	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
2	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
3	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
4	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
5	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging

- 2 Go to **Menu > Switching > VLAN > VLAN Setup > VLAN Port Setup**. Set the PVID. Set port **1** as PVID=10 (VLAN 10). Click **“Apply”**.

Port	Ingress Check	PVID	Acceptable Frame Type	VLAN Trunking	Isolation
*	<input type="checkbox"/>	<input type="text"/>	All	<input type="checkbox"/>	<input type="checkbox"/>
1	<input type="checkbox"/>	10	All	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	20	All	<input type="checkbox"/>	<input type="checkbox"/>

- 3 Create a Static IP Address for Switch in **VLAN 10** (To be the gateway in VLAN 10): Go to **Menu > SYSTEM > IP Setup > IP Setup > IP Interface > Add/Edit**. Set the Static IP Address: **192.168.10.1** for Switch in VLAN 10. Click "**Apply**".

The screenshot shows the configuration interface for a switch interface. It has two main sections: "DHCP Client" and "Static IP Address".

- DHCP Client:** This section is unselected. It includes a checked "Option-60" and a "Class-ID" field containing "Zyxel Corporator".
- Static IP Address:** This section is selected with a radio button. It includes:
 - IP Address:** A text box containing "192.168.10.1".
 - IP Subnet Mask:** A text box containing "255.255.255.0".
 - VID:** A text box containing "10".

At the bottom of the form are three buttons: "Apply" (green), "Clear" (grey), and "Cancel" (grey).

2.2.2 Configure VLAN 20

- 1 Create VLAN 20. Follow the same steps. Go to **Menu > Switching > VLAN > VLAN Setup > Static VLAN > Add/Edit**. Enable the **Active** setting. Type the Name and VLAN Group ID=20. Select port **2** as **Fixed** and uncheck Tx Tagging (Untagged). Click **“Apply”**.

Active ON

Name

VLAN Group ID

Port	Control			Tagging
*	Normal <input type="text" value="Normal"/>			<input checked="" type="checkbox"/> Tx Tagging
1	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
2	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
3	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
4	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
5	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging

- 2 Go to **Menu > Switching > VLAN > VLAN Setup > VLAN Port Setup**. Set the PVID. Set port **2** as PVID=20 (VLAN 20). Click **“Apply”**.

Port	Ingress Check	PVID	Acceptable Frame Type	VLAN Trunking	Isolation
*	<input type="checkbox"/>	<input type="text"/>	All <input type="text" value="All"/>	<input type="checkbox"/>	<input type="checkbox"/>
1	<input type="checkbox"/>	10 <input type="text" value="10"/>	All <input type="text" value="All"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	20 <input type="text" value="20"/>	All <input type="text" value="All"/>	<input type="checkbox"/>	<input type="checkbox"/>

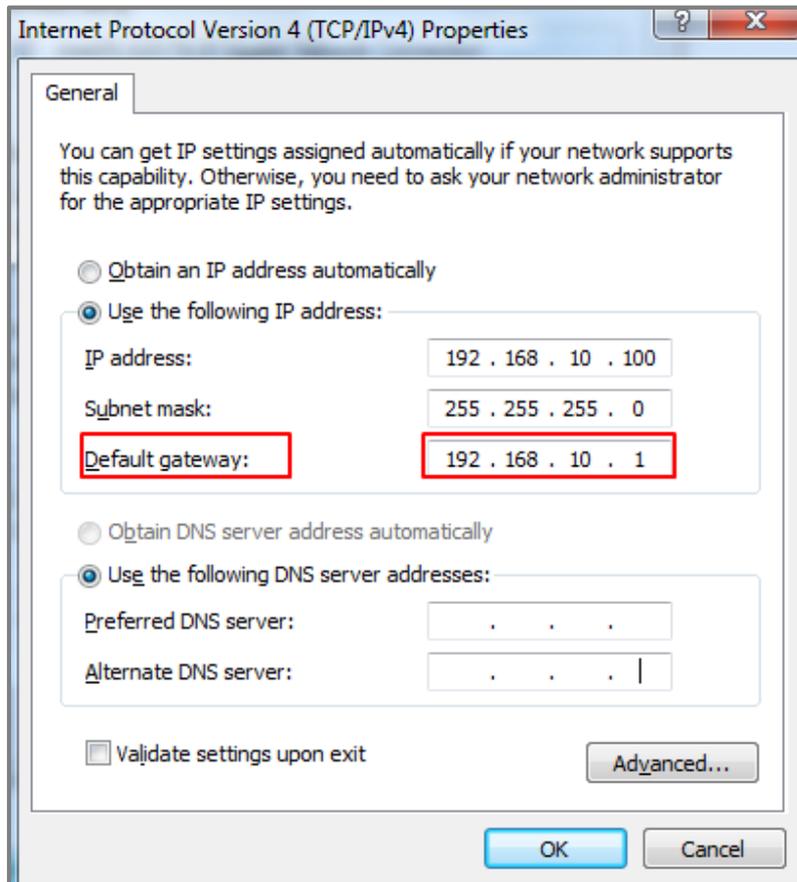
- 3 Create a Static IP Address for Switch in VLAN 20 (To be the gateway in VLAN 20). Go to **Menu > SYSTEM > IP Setup > IP Setup > IP Interface > Add/Edit**. Set a Static IP Address: **192.168.20.1** for Switch in **VLAN 20**. Click **“Apply”**.

The screenshot shows the 'Static IP Address' configuration page in the Zyxel web interface. The 'Static IP Address' radio button is selected. The 'Option-60' checkbox is checked, and the 'Class-ID' field contains 'Zyxel Corporation'. The 'IP Address' field is set to '192.168.20.1', the 'IP Subnet Mask' field is set to '255.255.255.0', and the 'VID' field is set to '20'. The 'Apply' button is highlighted in green, while 'Clear' and 'Cancel' are greyed out.

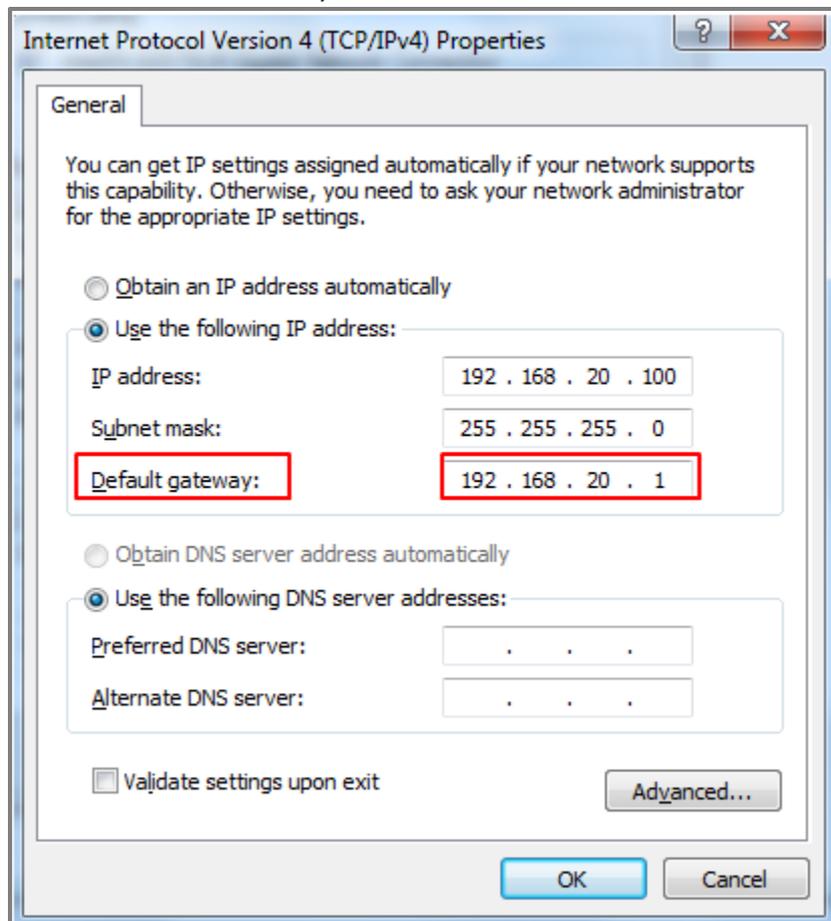
<input type="radio"/> DHCP Client	
Option-60	<input checked="" type="checkbox"/>
Class-ID	Zyxel Corporation
<input checked="" type="radio"/> Static IP Address	
IP Address	192.168.20.1
IP Subnet Mask	255.255.255.0
VID	20
Apply	Clear Cancel

2.2.3 Set the gateway on PC-1 and PC-2

- 1 Set the Gateway of **PC-1** as **192.168.10.1** (The Static IP Address of Switch in **VLAN 10**).



- 2 Set the Gateway of PC-2 as **192.168.20.1** (The Static IP Address of Switch in **VLAN 20**).



2.2.4 Test the Result

- 1 PC-1 can ping PC-2 successfully.

```
C:\Users\User>ping 192.168.20.100

Pinging 192.168.20.100 with 32 bytes of data:
Reply from 192.168.20.100: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.20.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

2.2.5 What could go wrong

- 1** If PC-1 cannot reach PC-2:
 - a. Verify that the subnet of PC-1 is not using the same subnet as that of PC-2.
 - b. Verify that the default gateways of PC-1 and PC-2 matches the Switch's IP interface on their respective VLANs.
 - c. Make sure that there are no policy routes using the subnet of PC-1 or PC-2 as a destination IP criteria.

2.3 How to configure the switch to perform DHCP service in a VLAN

The example shows administrators how to configure the switch to provide dynamic IP addresses to hosts in each VLANs.

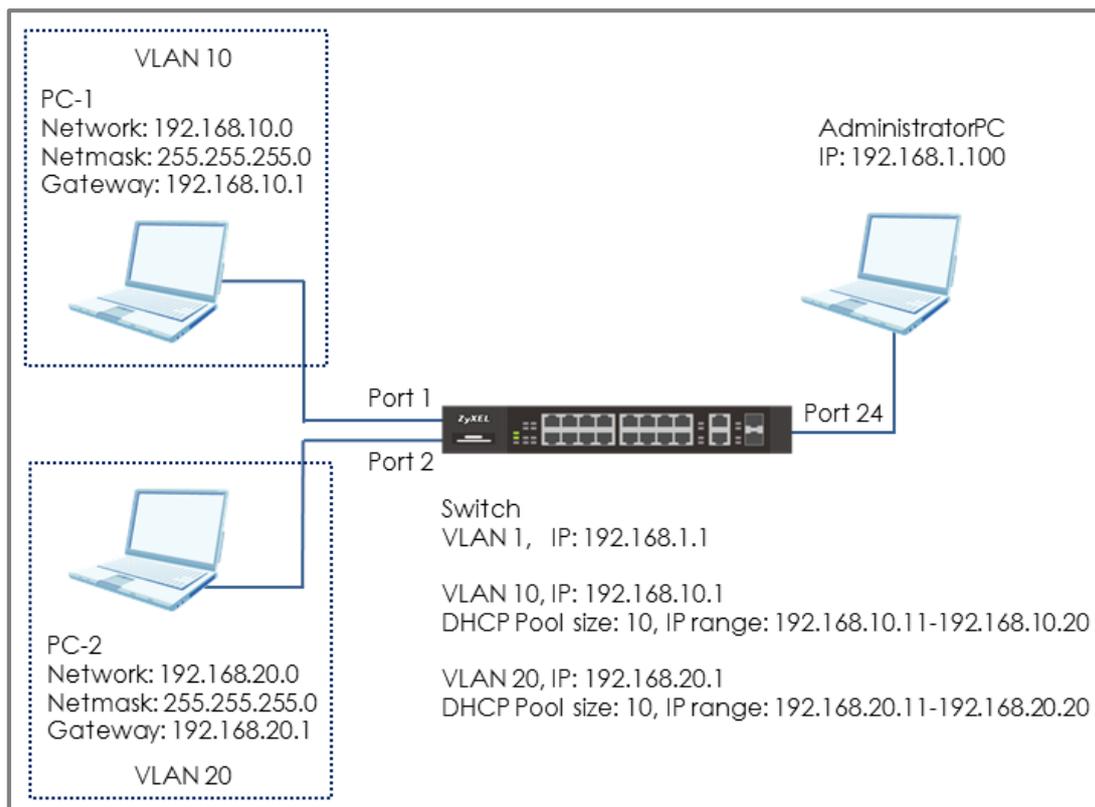


Figure 11 Perform DHCP service in different VLAN



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 XS3800-32 (Firmware Version: V4.80). Only L3 Switch supports the function of DHCP Server. (The models: 3700 series, 3800 series and 4600 series)

2.3.1 Configure VLAN 10

- 1 Use AdministratorPC to create VLAN 10. Enter the web GUI and go to **Menu > Switching > VLAN > VLAN Setup > Static VLAN > Add/Edit**. Enable the **Active** setting. Type the Name and VLAN Group ID=10. Select port **1** as **Fixed** and uncheck Tx Tagging (Untagged). Click **“Apply”**.

Port	Control	Tagging
*	Normal	<input checked="" type="checkbox"/> Tx Tagging
1	<input checked="" type="radio"/> Fixed	<input type="checkbox"/> Tx Tagging
2	<input checked="" type="radio"/> Normal	<input checked="" type="checkbox"/> Tx Tagging
3	<input checked="" type="radio"/> Normal	<input checked="" type="checkbox"/> Tx Tagging

- 2 Go to **Menu > Switching > VLAN > VLAN Setup > VLAN Port Setup**. Set the PVID. Set port **1** as PVID=10 (VLAN 10). Click **“Apply”**.

Port	Ingress Check	PVID	Acceptable Frame Type
*	<input type="checkbox"/>		All
1	<input type="checkbox"/>	10	All
2	<input type="checkbox"/>	20	All
3	<input type="checkbox"/>	1	All
4	<input type="checkbox"/>	1	All

- 3 Create a Static IP Address for Switch in **VLAN 10** (IP Address to be DHCP Server in VLAN 10): Go to **Menu > SYSTEM > IP Setup > IP Setup > IP Interface > Add/Edit**. Set the Static IP Address: **192.168.10.1** for Switch in VLAN 10. Click **“Add”**.

<input type="radio"/> DHCP Client	
Option-60	<input checked="" type="checkbox"/>
Class-ID	<input type="text" value="Zyxel Corporation"/>
<input checked="" type="radio"/> Static IP Address	
IP Address	<input type="text" value="192.168.10.1"/>
IP Subnet Mask	<input type="text" value="255.255.255.0"/>
VID	<input type="text" value="10"/>
<input type="button" value="Apply"/> <input type="button" value="Clear"/> <input type="button" value="Cancel"/>	

2.3.2 Configure VLAN 20

- 1 Create VLAN 20. Follow the same steps. Go to **Menu > Switching > VLAN > VLAN Setup > Static VLAN > Add/Edit**. Enable the **Active** setting. Type the Name and VLAN Group ID=20. Select port **2** as **Fixed** and uncheck Tx Tagging (Untagged). Click **“Apply”**.

Port	Control	Tagging
*	Normal	<input checked="" type="checkbox"/> Tx Tagging
1	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
2	<input type="radio"/> Normal <input checked="" type="radio"/> Fixed <input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
3	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging

- 2 Go to **Menu > Switching > VLAN > VLAN Setup > VLAN Port Setup**. Set the PVID. Set port **2** as PVID=20 (VLAN 20). Click **“Apply”**.

Port	Ingress Check	PVID	Acceptable Frame Type
*	<input type="checkbox"/>		All
1	<input type="checkbox"/>	10	All
2	<input type="checkbox"/>	20	All
3	<input type="checkbox"/>	1	All
4	<input type="checkbox"/>	1	All

- 3 Create Static IP Address for Switch in VLAN 20 (IP Address to be DHCP Server in VLAN 20): Go to **Menu > SYSTEM > IP Setup > IP Setup > IP Interface > Add/Edit**. Set the Static IP Address: **192.168.20.1** for Switch in **VLAN 20**. Click **“Add”**.

DHCP Client

Option-60

Class-ID

Static IP Address

IP Address

IP Subnet Mask

VID

2.3.3 Configure the Switch and PC

- 1 Set up DHCP Server in **VLAN 10**: Go to **Menu > Networking > DHCP > DHCPv4 Server > DHCP Server Setup > Add/Edit**. Set up the VID (VLAN of PC-1). The Client IP Pool Starting Address refers to the first IP Address the Switch will assign to DHCP clients. The Size of Client IP Pool refers to the maximum number of IP addresses the switch will provide. Set the gateway as the IP of the Switch in VLAN 10 (**192.168.10.1**). Click "Add".

VID	<input type="text" value="10"/>
Client IP Pool Starting Address	<input type="text" value="192.168.10.11"/>
Size of Client IP Pool	<input type="text" value="10"/>
IP Subnet Mask	<input type="text" value="255.255.255.0"/>
Default Gateway	<input type="text" value="192.168.10.1"/>
Primary DNS Server	<input type="text" value="0.0.0.0"/>
Secondary DNS Server	<input type="text" value="0.0.0.0"/>
Lease Time	<input checked="" type="radio"/> Infinite <input type="radio"/> Days <input type="text" value="3"/> Hours <input type="text" value="00"/> Minutes <input type="text" value="00"/>
Unavailable Lease Time	Days <input type="text" value="1"/> Hours <input type="text" value="00"/> Minutes <input type="text" value="00"/>
<input type="button" value="Apply"/> <input type="button" value="Clear"/> <input type="button" value="Cancel"/>	



Note:

In this example, the pool size is 10 and the starting IP address is 192.168.10.11. Therefore, the IP range that the DHCP Server will assign is between 192.168.10.11 and 192.168.10.20.

- 2 Set up DHCP Server in **VLAN 20**: Go to **Menu > Networking > DHCP > DHCPv4 Server > DHCP Server Setup > Add/Edit**. Set up the VID (VLAN of PC-2). The Client IP Pool Starting Address refers to the first IP Address the Switch will assign to DHCP clients. The Size of Client IP Pool refers to the maximum number of IP addresses the switch will provide. Set the gateway as the IP of the Switch in VLAN 20 (**192.168.20.1**). Click "Add". Click "Add".

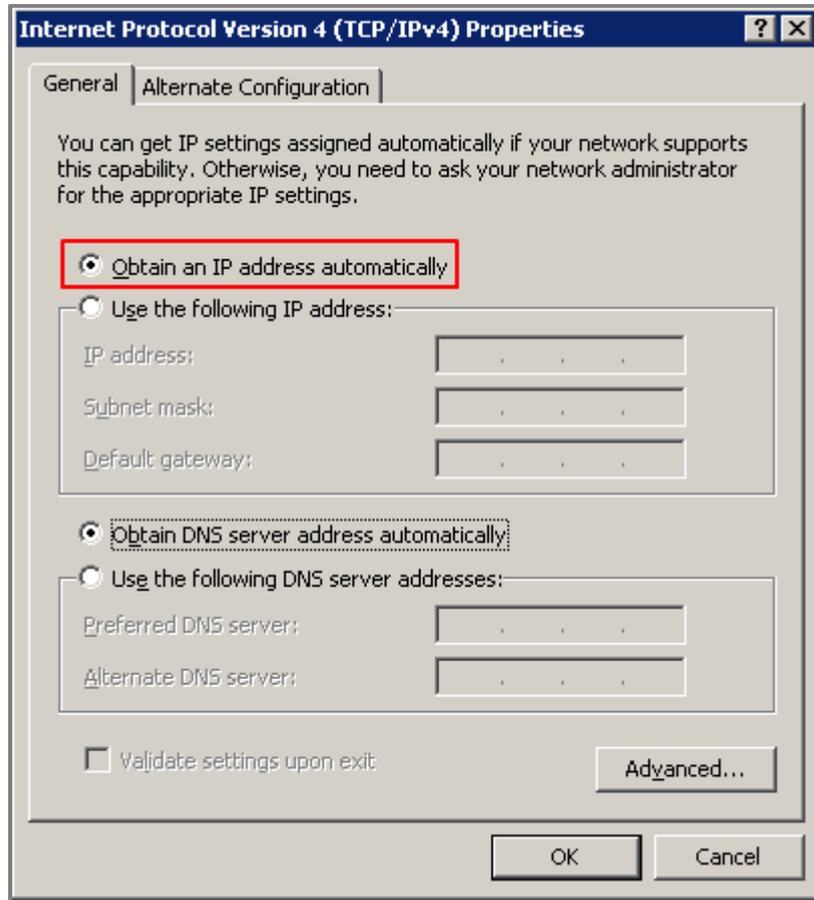
VID	<input type="text" value="20"/>
Client IP Pool Starting Address	<input type="text" value="192.168.20.11"/>
Size of Client IP Pool	<input type="text" value="10"/>
IP Subnet Mask	<input type="text" value="255.255.255.0"/>
Default Gateway	<input type="text" value="192.168.20.1"/>
Primary DNS Server	<input type="text" value="0.0.0.0"/>
Secondary DNS Server	<input type="text" value="0.0.0.0"/>
Lease Time	<input checked="" type="radio"/> Infinite <input type="radio"/> Days <input type="text" value="3"/> Hours <input type="text" value="00"/> Minutes <input type="text" value="00"/>
Unavailable Lease Time	Days <input type="text" value="1"/> Hours <input type="text" value="00"/> Minutes <input type="text" value="00"/>
<input type="button" value="Apply"/> <input type="button" value="Clear"/> <input type="button" value="Cancel"/>	



Note:

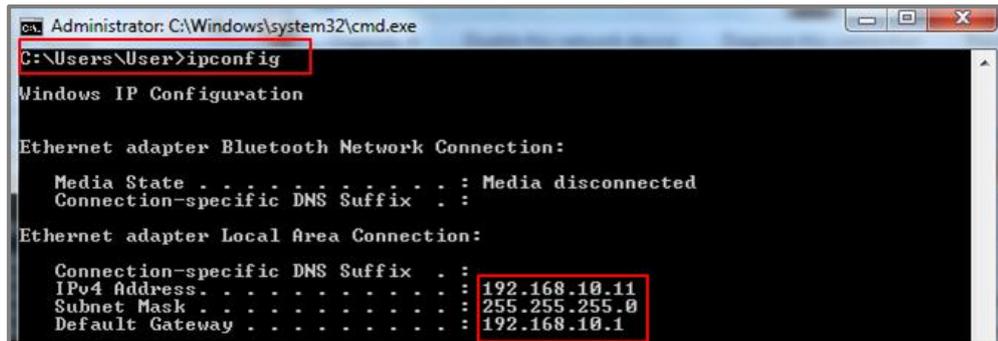
In this example, the pool size is 10 and the starting IP address is 192.168.20.11. Therefore, the IP range that the DHCP Server will assign is between 192.168.20.11 and 192.168.20.20.

- 3 Set PC-1 and PC-2 as DHCP clients by configuring IPv4 to **"Obtain an IP Address automatically"**.



2.3.4 Test the Result

- 1 PC-1 can get the IP Address assigned by Switch successfully. We can check this by using the command **"ipconfig"** in command prompt. PC-1 will get an IP address in the range of: **192.168.10.11-192.168.10.20** and the gateway is **192.168.10.1**.



```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\User>ipconfig

Windows IP Configuration

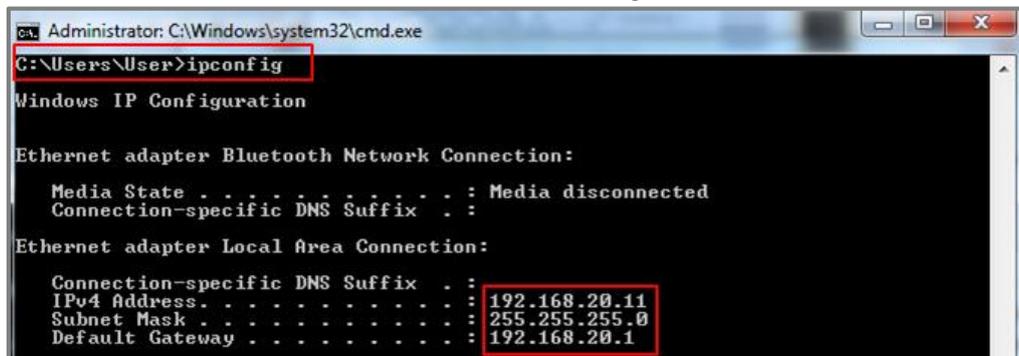
Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . :
    IPv4 Address. . . . . : 192.168.10.11
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.10.1
```

- 2 PC-2 can get the IP Address assigned by Switch successfully. We can check this by using the command **"ipconfig"** in command prompt. PC-2 will get an IP address in the range of: **192.168.20.11-192.168.20.20** and the gateway is **192.168.20.1**.



```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\User>ipconfig

Windows IP Configuration

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . :
    IPv4 Address. . . . . : 192.168.20.11
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.20.1
```

2.3.5 What Could Go Wrong

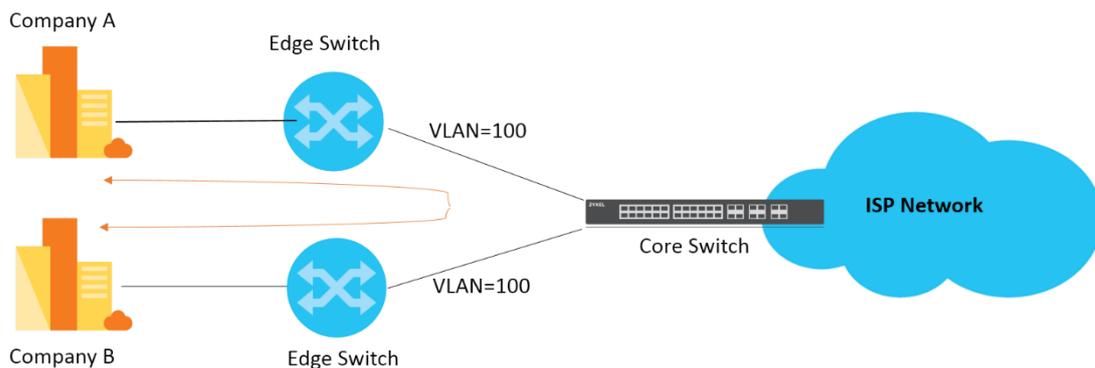
- 1 If some devices are no longer receiving any dynamic IP address from the DHCP server, consider increasing the Size of Client Pool.
- 2 If you want to surf the Internet using a URL or domain name, please remember to set up **DNS Server**.

VID	<input type="text" value="20"/>
Client IP Pool Starting Address	<input type="text" value="192.168.20.11"/>
Size of Client IP Pool	<input type="text" value="10"/>
IP Subnet Mask	<input type="text" value="255.255.255.0"/>
Default Gateway	<input type="text" value="192.168.20.1"/>
Primary DNS Server	<input type="text" value="0.0.0.0"/>
Secondary DNS Server	<input type="text" value="0.0.0.0"/>
Lease Time	<input checked="" type="radio"/> Infinite <input type="radio"/> Days <input type="text" value="3"/> Hours <input type="text" value="00"/> Minutes <input type="text" value="00"/>
Unavailable Lease Time	Days <input type="text" value="1"/> Hours <input type="text" value="00"/> Minutes <input type="text" value="00"/>
<input type="button" value="Apply"/> <input type="button" value="Clear"/> <input type="button" value="Cancel"/>	

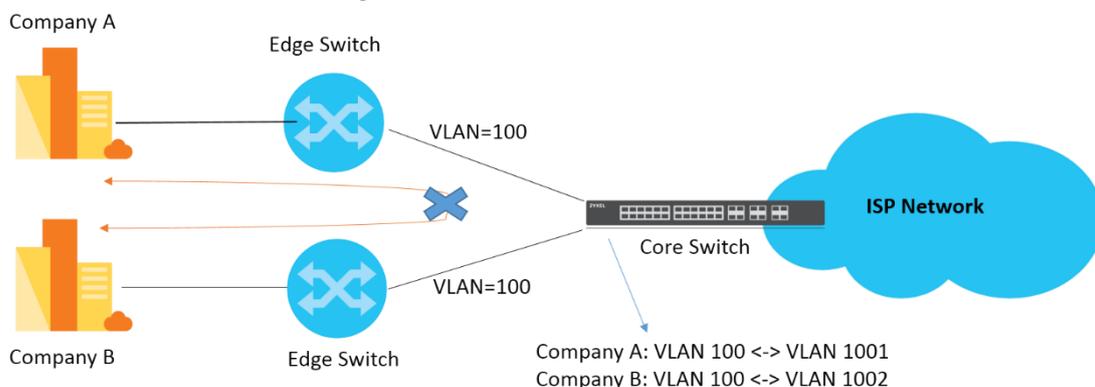
2.4 How to Configure the Switch to Translate Customer VLAN to Service Provider VLAN

VLAN Mapping provides a mechanism to map a Customer VLAN to a service provider's VLAN (Translated-VLAN). Packets received on a port will map to a Translated VLAN based on a port ID and customer VLAN ID from packets.

VLAN Mapping also can be used to prevent traffic from forwarding between different customers when they use the same VLAN in their own networks. In the following example, both of company A and company B use the same VLAN 10. When company A sends traffic to an ISP network, the traffic is possible to be forwarded to company B across a core switch because both of the companies are in the same VLAN 10.



Once VLAN Mapping is configured on edge switches, it can translate customer VLANs of company A and company B to different VLANs respectively. Thus, the traffic will not be forwarded between company A and company B since they are in the different VLANs after processing VLAN translation on edge switches.



The following example will instruct how an administrator configures a switch to achieve VLAN translation.

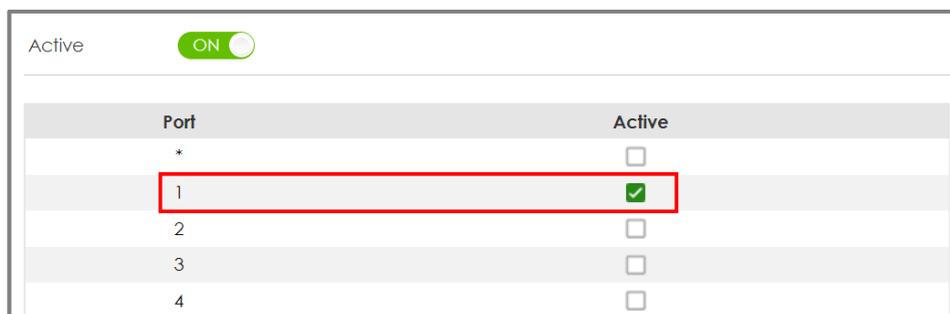


Note:

The example was tested using two GS2220 (Firmware Version: V4.80) as edge switches, and one XGS2220 (Firmware Version: V4.80) as a core switch.

2.4.1 Configuration on the Core Switch

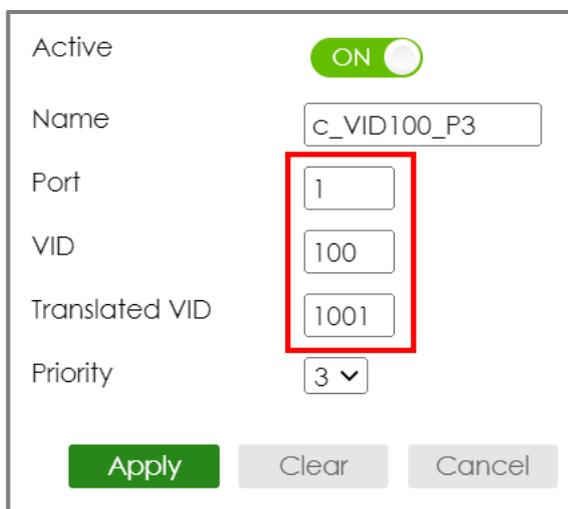
- 1 Access to the web GUI, Go to **Menu > Switching > VLAN Mapping**. Enable the **Active** setting and activate port **1**.



Active

Port	Active
*	<input type="checkbox"/>
1	<input checked="" type="checkbox"/>
2	<input type="checkbox"/>
3	<input type="checkbox"/>
4	<input type="checkbox"/>

- 2 Go to **Menu > Switching > VLAN Mapping > VLAN Mapping Setup > Add/Edit**. Enable the **Active** setting and type the **Name**. Set Port as **1**, VID as **100**, and Translated VID as **1001**. Select Priority value as 3 (Optional), and click "Apply".



Active

Name

Port

VID

Translated VID

Priority

- 3 Go to **Menu > Switching > VLAN > VLAN Setup > Static VLAN Setup**. Check the **Active** box, type the **Name** and VLAN Group ID= as **1001**. Select port **1, 26** as **Fixed**, and click "Apply".

Active

Name

VLAN Group ID

Port	Control			Tagging
*	Normal			<input checked="" type="checkbox"/> Tx Tagging
1	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
2	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
3	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
4	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
5	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
6	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
24	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
25	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
26	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
27	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
28	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging



Note:

Create a Static VLAN only for the Translated VLAN, and set both of ports as members for the Translated VLAN. Otherwise the packets from the Translated VLAN received on port 26 will NOT be forwarded to port 1.

2.4.2 Configuration on the Edge Switch

- 1 Setup **Customer Switch-1**: Access to the web GUI. Go to **Menu > Switching > VLAN > VLAN Setup > Static VLAN Setup**. (If you are using V4.70 firmware, please go to **Menu > Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup**.) Check the **Active** box, type the **Name** and VLAN Group ID= as **100**. Select port **1** as **Fixed** and uncheck Tx Tagging (Untagged). Select port **9** as **Fixed**, and click **“Apply”**.

Port	Control			Tagging
*	Normal			<input checked="" type="checkbox"/> Tx Tagging
1	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
2	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
3	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
4	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
5	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
6	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
7	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
8	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
9	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
10	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
11	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging

- 2 Setup **Customer Switch-1**: Go to **Menu > Switching > VLAN > VLAN Setup > VLAN Port Setup** (If you are using V4.70 firmware, please go to **Menu > Advanced Application > VLAN > VLAN Configuration > VLAN Port Setup**.) Set port **1** PVID= as **100** (VLAN 100), and click **“Apply”**.

Port	Ingress Check	PVID	Acceptable Frame Type
*	<input type="checkbox"/>	<input type="text"/>	All <input type="button" value="v"/>
1	<input type="checkbox"/>	100 <input type="button" value="v"/>	All <input type="button" value="v"/>
2	<input type="checkbox"/>	1 <input type="button" value="v"/>	All <input type="button" value="v"/>
3	<input type="checkbox"/>	1 <input type="button" value="v"/>	All <input type="button" value="v"/>
4	<input type="checkbox"/>	1 <input type="button" value="v"/>	All <input type="button" value="v"/>

- 3 Setup Customer Switch-2:** Go to **Menu > Switching > VLAN > VLAN Setup > Static VLAN Setup**. (If you are using V4.70 firmware, please go to **Menu > Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup**.) Check the **Active** box, type the **Name** and VLAN Group ID= as **1001**. Select port **1** as **Fixed** and uncheck Tx Tagging (Untagged). Select port **9** as **Fixed**, and click **“Apply”**.

Active

Name

VLAN Group ID

Port	Control	Tagging
*	Normal <input type="button" value="v"/>	<input checked="" type="checkbox"/> Tx Tagging
1	<input type="radio"/> Normal <input checked="" type="radio"/> Fixed <input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
2	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
3	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
4	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
5	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
6	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
7	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
8	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
9	<input type="radio"/> Normal <input checked="" type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
10	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
11	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging

- 4 Setup Customer Switch-2:** Go to **Menu > Switching > VLAN > VLAN Setup > VLAN Port Setup** (If you are using V4.70 firmware, please go to **Menu > Advanced Application > VLAN > VLAN**

Configuration > VLAN Port Setup.) Set port **1** PVID= as **1001** (VLAN 1001), and click **“Apply”**.

Port	Ingress Check	PVID	Acceptable Frame Type
-	<input type="checkbox"/>	<input type="text"/>	All <input type="button" value="v"/>
1	<input type="checkbox"/>	1001	All <input type="button" value="v"/>
2	<input type="checkbox"/>	1 <input type="text"/>	All <input type="button" value="v"/>
3	<input type="checkbox"/>	1 <input type="text"/>	All <input type="button" value="v"/>
4	<input type="checkbox"/>	1 <input type="text"/>	All <input type="button" value="v"/>

2.4.3 Test the Results

- 1 PC-1 can ping PC-2 successfully.

```
C:\>ping 192.168.1.200

Pinging 192.168.1.200 with 32 bytes of data:
Reply from 192.168.1.200: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.200:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

- 2 Configure Mirroring to verify the VLAN ID/Priority value in the packets which are received on **port 1** of the core switch, and ensure they are the original value **VLAN=100/Priority=0**). Access to the web GUI and go to **Menu > Switching > Mirroring > Mirroring**. Switch **on** the mirroring. Set the Monitor port as port **2**, which is used to monitor the traffic, and check the destination **port 1** in this example. Select the direction as “Both”, and click “Apply”.

Port	Mirrored	Direction
*	<input type="checkbox"/>	Ingress
1	<input checked="" type="checkbox"/>	Both
2	<input type="checkbox"/>	Ingress
3	<input type="checkbox"/>	Ingress
4	<input type="checkbox"/>	Ingress

- 3 Connect with another PC to port 2 of the core switch. Open **wireshark** to monitor the packets, and filter “**icmp**”.

No.	Time	Source	Destination	Protocol	Length	Se	Sy	Info
10	2019-11-29 14:22:42.868199	192.168.1.100	192.168.1.200	ICMP	78			Echo (ping) request
13	2019-11-29 14:22:42.868908	192.168.1.200	192.168.1.100	ICMP	78			Echo (ping) reply
18	2019-11-29 14:22:43.869101	192.168.1.100	192.168.1.200	ICMP	78			Echo (ping) request
19	2019-11-29 14:22:43.869397	192.168.1.200	192.168.1.100	ICMP	78			Echo (ping) reply
23	2019-11-29 14:22:44.871108	192.168.1.100	192.168.1.200	ICMP	78			Echo (ping) request
24	2019-11-29 14:22:44.871432	192.168.1.200	192.168.1.100	ICMP	78			Echo (ping) reply
28	2019-11-29 14:22:45.873120	192.168.1.100	192.168.1.200	ICMP	78			Echo (ping) request
29	2019-11-29 14:22:45.873521	192.168.1.200	192.168.1.100	ICMP	78			Echo (ping) reply

Frame 10: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
 Ethernet II, Src: WistronI_30:0e:b8 (3c:97:0e:30:0e:b8), Dst: Inventec_27:04:93 (00:1e:33:27:04:93)
 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 100
 Internet Protocol Version 4, Src: 192.168.1.100, Dst: 192.168.1.200
 Internet Control Message Protocol

- Configure Mirroring to verify the VLAN ID/Priority in the packets sent out from **port 26** of the core switch and ensure they should be the translated values (**VLAN=1001/Priority=3**). Go to **Menu > Advanced Application > Mirroring**. Uncheck port 1 and check **port 26**. Select the direction as "Both", and click "**Apply**".

Active

Monitor Port

Port	Mirrored	Direction
*	<input type="checkbox"/>	Ingress
1	<input type="checkbox"/>	Both
2	<input type="checkbox"/>	Ingress
3	<input type="checkbox"/>	Ingress
4	<input type="checkbox"/>	Ingress
24	<input type="checkbox"/>	Ingress
25	<input type="checkbox"/>	Ingress
26	<input checked="" type="checkbox"/>	Both

- Connect with another PC to port 2 of the core switch. Open **wireshark** to monitor the packets, and filter "**icmp**".

No.	Time	Source	Destination	Protocol	Length	Se	Sy	Info
11	2019-11-29 14:31:57.053356	192.168.1.100	192.168.1.200	ICMP	78			Echo (ping) request
14	2019-11-29 14:31:57.053673	192.168.1.200	192.168.1.100	ICMP	78			Echo (ping) reply
16	2019-11-29 14:31:58.054182	192.168.1.100	192.168.1.200	ICMP	78			Echo (ping) request
17	2019-11-29 14:31:58.054606	192.168.1.200	192.168.1.100	ICMP	78			Echo (ping) reply
19	2019-11-29 14:31:59.055558	192.168.1.100	192.168.1.200	ICMP	78			Echo (ping) request
20	2019-11-29 14:31:59.055908	192.168.1.200	192.168.1.100	ICMP	78			Echo (ping) reply
22	2019-11-29 14:32:00.058421	192.168.1.100	192.168.1.200	ICMP	78			Echo (ping) request
23	2019-11-29 14:32:00.058888	192.168.1.200	192.168.1.100	ICMP	78			Echo (ping) reply

Frame 16: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
Ethernet II, Src: WistronI_30:0e:b8 (3c:97:0e:30:0e:b8), Dst: Inventec_27:04:93 (00:1e:33:27:04:93)
802.1Q Virtual LAN, PRI: 3, DEI: 0, ID: 1001
Internet Protocol Version 4, Src: 192.168.1.100, Dst: 192.168.1.200
Internet Control Message Protocol

Improving Network Reliability

3.1 How to configure a stacked switch to ensure high server availability

The example shows administrators how to configure a stacked switch to ensure high server availability. In this example, we stack Switch-1 and Switch-2 into one logical switch. By stacking the switch together, even if one switch goes offline, clients can still reach the server. This ensures high availability for servers. This example instructs administrators to disconnect all links before configuring the switches to avoid any network outages caused by broadcast storms.

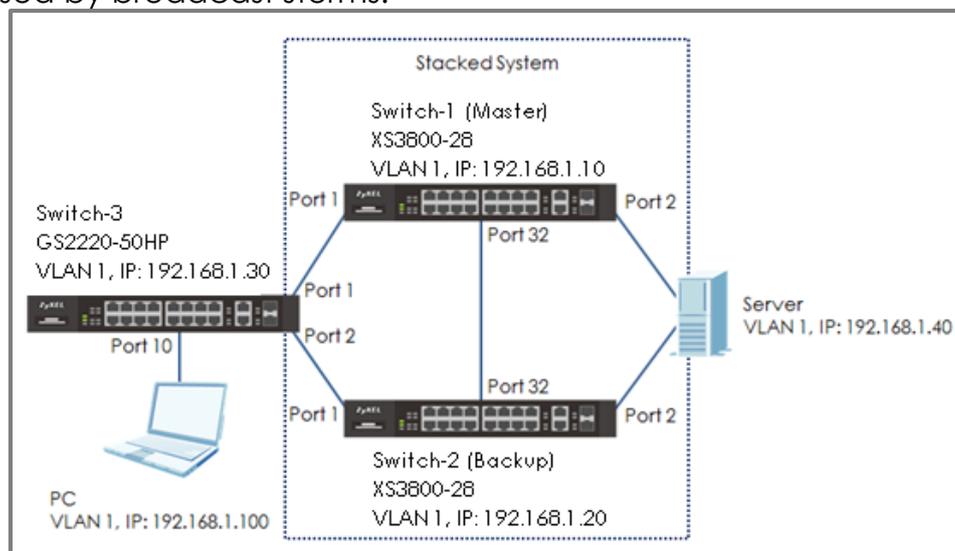


Figure 12 Configure the stacked switch



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 XGS3800-28 (Firmware Version: V4.80) and GS2220-50HP (Firmware Version: V4.80).

3.1.1 Configure Switch-1 and Switch-2 for Stacking

- 1 Set up **Switch-1**: Enter the web GUI and go to **Menu > System > Stacking > Stacking Setup**. Key in the system priority (The higher the number is, the higher priority it is to become a master) and

click "Apply". Enable the **Active** setting and click "Apply". Switch-1 will reboot.



Stacking Setup

Active ON OFF

Force Master Mode OFF ON

System Priority



Note:

In this example, we set the priority of Switch-1 higher than Switch-2. Therefore, Switch-1 will become the Master.

- 2 Set up **Switch-2**: Enter the web GUI and go to **Menu > System > Stacking > Stacking Setup**. Key in the system priority (The higher the number is, the higher priority it is to become a master) and click "Apply". Enable the **Active** setting and click "Apply". Switch-2 will reboot.



Stacking Setup

Active ON OFF

Force Master Mode OFF ON

System Priority

- 3 Connect Switch-1 and Switch-2 together on port 28 using a 10-Gigabit transceiver.



Note:

The last four ports are usually reserved for stacking channels when the switch is in stacking mode. These are ports 25, 26, 27, and 28 for the XS3800-28 switch. If you are using other stackable models, please refer to the user manual to confirm the ports used for stacking.

- 4 Switch-1 and Switch-2 becomes a stacked switch. The Stack ID LED on the front panel of the switches should display "1" and "2".

- 5 Remember to save the configuration.

3.1.2 Configure Link Aggregation on Stacked switch

- 1 Connect to the stacked switch. Enter web GUI and go to **Menu > Port > Link Aggregation > Link Aggregation Setting**. Active T1 and T2. Select SLOT 1 and set the Group of port 1/1 and 1/2 as T1 and T2, respectively. Click "Apply". Select SLOT 2 and set the Group of port 2/1 and 2/2 as T1 and T2 respectively. Click "Apply".

Group ID	Active	Criteria
T1	<input checked="" type="checkbox"/>	src-dst-mac
T2	<input checked="" type="checkbox"/>	src-dst-mac

SLOT 1	Port	Group
SLOT 1	1/1	T1
	1/2	T2

SLOT 2	Port	Group
SLOT 2	2/1	T1
	2/2	T2

- 2 Go to **Menu > Port > Link Aggregation > Link Aggregation Control Protocol**. Check the "Active" box, as well as for T1 and T2.

Active	<input checked="" type="checkbox"/>
System Priority	65535

Group ID	LACP Active
T1	<input checked="" type="checkbox"/>
T2	<input checked="" type="checkbox"/>

3.1.3 Configure Link Aggregation on Switch-3

- 1 Go to **Menu > Port > Link Aggregation > Link Aggregation setting**. (If you are using V4.70 firmware, please go to **Menu > Advanced Application > Link Aggregation > Link Aggregation Setting**.) Check the Active box for T1 and select the port 1 and 2 as Group T1. Click "Apply".

Group ID	Active	Criteria
T1	<input checked="" type="checkbox"/>	src-dst-mac
T2	<input type="checkbox"/>	src-dst-mac

Port	Group
1	T1
2	T1
3	None
4	None

- 3 Go to **Menu > Port > Link Aggregation > Link Aggregation Control Protocol**. (If you are using V4.70 firmware, please go to **Menu > Advanced Application > Link Aggregation > Link Aggregation Setting >LACP**.) Check the “Active” box, as well as for T1.

Active	<input checked="" type="checkbox"/>
System Priority	65535
Group ID	LACP Active
T1	<input checked="" type="checkbox"/>
T2	<input type="checkbox"/>
T3	<input type="checkbox"/>

3.1.4 Test the Result

- 1 Configure Link Aggregation between the Server's two NIC and connect these ports to port 1/2 and 2/2 of the stacked switch.
- 2 Use PC to ping the Server (192.168.1.40). After few times of ping, try to shut down Switch-1 (Master down). The ping will display "timed out" a few times and then ping will be successful again when Switch-2 (Backup) becomes the new Master.

```
C:\Users\User>ping 192.168.1.40 -t
Pinging 192.168.1.40 with 32 bytes of data:
Reply from 192.168.1.40: bytes=32 time=4ms TTL=254
Reply from 192.168.1.40: bytes=32 time<1ms TTL=254
Reply from 192.168.1.40: bytes=32 time=2ms TTL=254
Reply from 192.168.1.40: bytes=32 time=28ms TTL=254
Reply from 192.168.1.40: bytes=32 time=9ms TTL=254
Reply from 192.168.1.40: bytes=32 time=20ms TTL=254
Reply from 192.168.1.40: bytes=32 time<1ms TTL=254
Reply from 192.168.1.40: bytes=32 time=9ms TTL=254
Reply from 192.168.1.40: bytes=32 time=9ms TTL=254
Reply from 192.168.1.40: bytes=32 time<1ms TTL=254
Reply from 192.168.1.40: bytes=32 time=9ms TTL=254
Request timed out.
Request timed out.
Reply from 192.168.1.40: bytes=32 time=21ms TTL=254
Reply from 192.168.1.40: bytes=32 time<1ms TTL=254
Reply from 192.168.1.40: bytes=32 time<1ms TTL=254
```

3.1.5 What Could Go Wrong

- 1** The stacking ports are usually the last 2 ports of the switch. If you connect the two switches using a non-stacking port, you will find that the two switches will not form a stacking system.
- 2** Remember to save the configuration before doing the test. If you forget to save the configuration, after rebooting, all the configurations will be lost. Therefore, the Link Aggregation will disappear.

3.2 How to configure RSTP in a ring topology

The example shows administrators how to set up RSTP (Rapid Spanning Tree Protocol) in the ring topology to implement network redundancy.

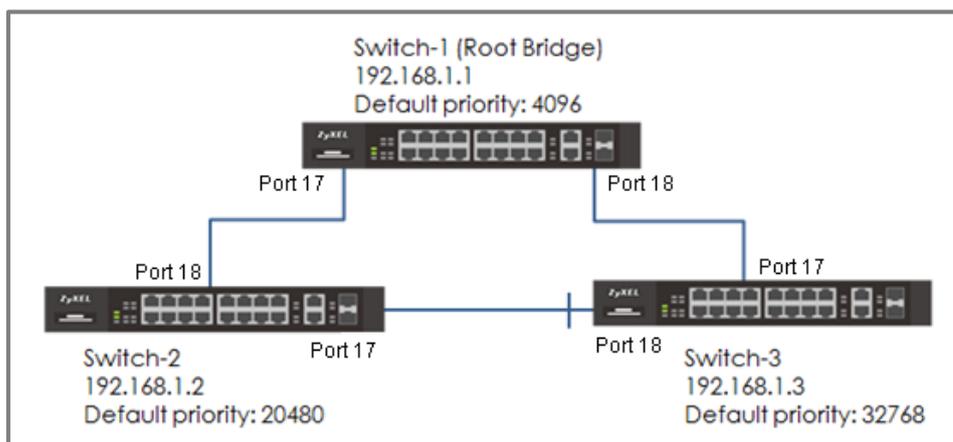


Figure 13 Configure RSTP in a ring topology

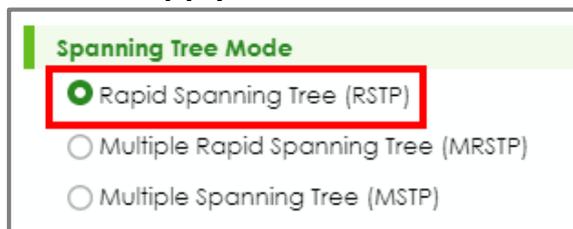


Note:

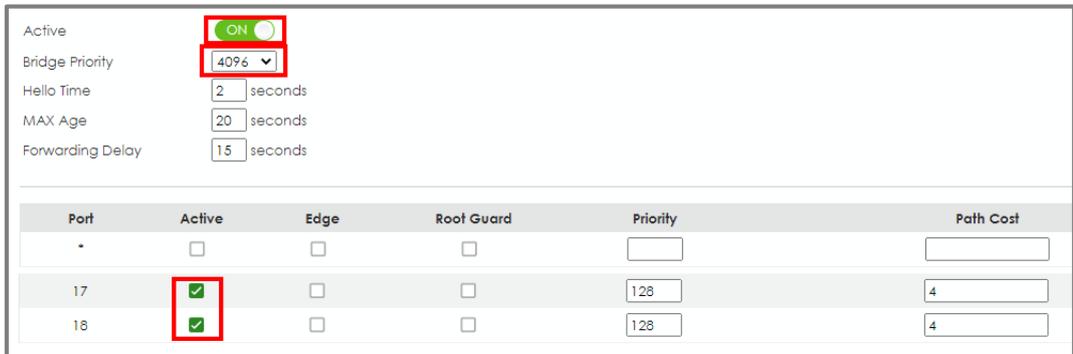
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using XS3800-28 (Firmware Version: V4.80).

3.2.1 Configure Switch

- 1 Make sure that the link between **Switch-2** and **Switch-3** is not connected to prevent unintended loops before finishing the RSTP setup.
- 2 Set up **Switch-1**: Enter the web GUI. Go to **Menu > Switching > Spanning Tree Protocol > Spanning Tree Setup**. Check if the Spanning Tree Configuration is **Rapid Spanning Tree**. If not, select it and click “**Apply**”.



- 3 Set up **Switch-1**: Enter the web GUI. Go to **Menu > Switching > Spanning Tree Protocol > RSTP**. Enable the **Active** setting. Set the Bridge Priority = **4096**. Active port **17, 18**. Click “**Apply**”.



- 4 Set up **Switch-2**: Enter the web GUI. Go to **Menu > Switching > Spanning Tree Protocol > Spanning Tree Setup**. Check if the Spanning Tree Configuration is **Rapid Spanning Tree**. If not, select it and click “**Apply**”.
- 5 Set up **Switch-2**: Enter the web GUI. Go to **Menu > Switching > Spanning Tree Protocol > RSTP**. Enable the **Active** setting. Set the Bridge Priority = **20480**. Active port **17, 18**. Click “**Apply**”.

Active ON

Bridge Priority

Hello Time seconds

MAX Age seconds

Forwarding Delay seconds

Port	Active	Edge	Root Guard	Priority	Path Cost
*	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
17	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="128"/>	<input type="text" value="2"/>
18	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="128"/>	<input type="text" value="2"/>

6 Set up **Switch-3**: Enter the web GUI. Go to **Menu > Switching > Spanning Tree Protocol > Spanning Tree Setup**. Check if the Spanning Tree Configuration is **Rapid Spanning Tree**. If not, select it and click **"Apply"**.

7 Set up **Switch-3**: Enter the web GUI. Go to **Menu > Switching > Spanning Tree Protocol > RSTP**. Enable the **Active** setting. Set the Bridge Priority = **32768**. Active port **17, 18**. Click **"Apply"**.

Active ON

Bridge Priority

Hello Time seconds

MAX Age seconds

Forwarding Delay seconds

Port	Active	Edge	Root Guard	Priority	Path Cost
*	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
17	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="128"/>	<input type="text" value="2"/>
18	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="128"/>	<input type="text" value="2"/>

8 Finally, connect the link between **Switch-2** and **Switch-3**.

3.2.2 Test the Result

- 1 Verify the status of **Switch-1**: Go to **Menu > Switching > Spanning Tree Protocol > Spanning Tree Protocol Status**. The Root Bridge ID and the Our Bridge ID should be the same. This means that Switch-1 is the Root Bridge. Both port 17 and 18 should be in **FORWARDING** state, while both their Port Roles are **Designated Ports**.

Spanning Tree Protocol: RSTP						
Root Bridge			Our Bridge			
Bridge ID	1000-0019cb000001		1000-0019cb000001			
Hello Time (seconds)	2		2			
Max Age (seconds)	20		20			
Forwarding Delay (seconds)	15		15			
Cost to Bridge	0					
Port ID	0x0000					
Topology Changed Times	5					
Time Since Last Change	0:00:07					
Port	Port State	Port Role	Designated Bridge ID	Designated Port ID	Designated Cost	Root Guard State
17	FORWARDING	Designated	1000-0019cb000001	0x8011	0	Forwarding
18	FORWARDING	Designated	1000-0019cb000001	0x8012	0	Forwarding

- 2 Verify the status of **Switch-2**: Go to **Menu > Advanced Application > Spanning Tree Protocol**. Check the port status of Switch-2. Port 18 should be the **Root Port** in **FORWARDING** state, while port 17 should be a **Designated Port** also in **FORWARDING** state.

Spanning Tree Protocol: RSTP						
Root Bridge			Our Bridge			
Bridge ID	1000-0019cb000001		5000-bc9911cba365			
Hello Time (seconds)	2		2			
Max Age (seconds)	20		20			
Forwarding Delay (seconds)	15		15			
Cost to Bridge	2					
Port ID	0x8012					
Topology Changed Times	4					
Time Since Last Change	0:00:55					
Port	Port State	Port Role	Designated Bridge ID	Designated Port ID	Designated Cost	Root Guard State
17	FORWARDING	Designated	5000-bc9911cba365	0x8011	2	Forwarding
18	FORWARDING	Root	1000-0019cb000001	0x8011	0	Forwarding

- 3 Verify the status of **Switch-3**: Go to **Menu > Advanced Application > Spanning Tree Protocol**. Check the port status of Switch-3. Port 17 should be the **Root Port** in **FORWARDING** state, while Port 18 is an **Alternate Port** in **DISCARDING** state.

Spanning Tree Protocol: RSTP

	Root Bridge	Our Bridge
Bridge ID	1000-0019cb000001	8000-bc9911cb365
Hello Time (seconds)	2	2
Max Age (seconds)	20	20
Forwarding Delay (seconds)	15	15
Cost to Bridge	2	
Port ID	0x8011	
Topology Changed Times	1	
Time Since Last Change	0:02:45	

Port	Port State	Port Role	Designated Bridge ID	Designated Port ID	Designated Cost	Root Guard State
17	FORWARDING	Root	1000-0019cb000001	0x8012	0	Forwarding
18	DISCARDING	Alternate	8000-bc9911cb365	0x8011	2	Forwarding

3.2.3 What Could Go Wrong

- 1 If your Root Bridge is not the device you expected:
 - a. Decrease the Spanning Tree priority of this device.
 - b. Increase the Spanning Tree priority of the other devices.

The switch with the **LOWEST** bridge priority will be the Root Bridge. If the priority is the same, the switch **LOWEST MAC address** will be the Root Bridge.

- 2 If it is not possible to access the management of the switches and the switch's port LEDs are constantly flashing, you can recover management access by removing or disconnecting any redundant links to break the ring topology. This frequently occurs before Spanning Tree is configured on the devices or if Spanning Tree is configured incorrectly.

3.3 How to configure VRRP to provide hosts with a redundant gateway

This example shows how to configure gateway redundancy. **Virtual Router Redundancy Protocol (VRRP)** is a feature that allows two gateways to use the same IP address. This allows hosts in the local network continues access to the Internet in the event of a failure on one of the gateways.

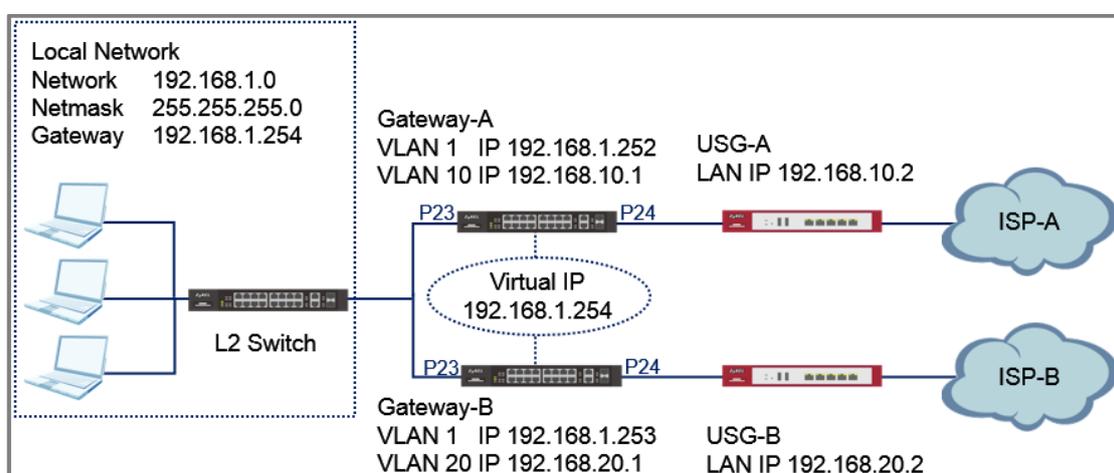


Figure 14 Two gateways running VRRP on the same LAN



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. Only the GS/XGS/XS3700 Series Switch, XS3800 Series Switch and XGS4600 Series Switch supports VRRP.

The L2 Switch can be any Zyxel switch using default configurations.

This example relies on two different Internet Service Providers (ISP) for Internet access.

All UI displayed in this article are taken from the XGS3800 series switch.

3.3.1 Configuration in the Gateway-A

- 1 Access the Gateway-A's web GUI.
- 2 Go to **Menu > Switching > VLAN > VLAN Setup > Static VLAN Setup**. Create/Edit VLAN 1 to make sure only Port 23 is a fixed port. Click **Add**.

Port	Control			Tagging
*		Normal		<input checked="" type="checkbox"/> Tx Tagging
22	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
23	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
24	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging

- 3 Go to **Menu > Switching > VLAN > VLAN Setup > Static VLAN Setup**. Create/Edit VLAN 10 to make sure only Port 24 is a fixed port. Click **Add**.

Active ON

Name

VLAN Group ID

VLAN Type Normal Private

Association VLAN List

Port	Control	Tagging
*	Normal	<input checked="" type="checkbox"/> Tx Tagging
22	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
23	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
24	<input type="radio"/> Normal <input checked="" type="radio"/> Fixed <input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging

4 Go to **Menu > Switching > VLAN > VLAN Setup > VLAN Port Setup**. Configure port 24 with PVID 10. Click **Apply**.

Port	Ingress Check	PVID	Acceptable Frame Type
*	<input type="checkbox"/>	<input type="text" value=""/>	All
22	<input type="checkbox"/>	1	All
23	<input type="checkbox"/>	1	All
24	<input type="checkbox"/>	10	All

5 Go to **Menu > System > IP Setup > IP Setup > IP Interface > Add/Edit**. Configure the IP address for VLAN 1. Click **Add** and do the same for VLAN 10.

DHCP Client

Option-60

Static IP Address

IP Address

IP Subnet Mask

VID

DHCP Client
 Option-60
 Class-ID
 Static IP Address
 IP Address
 IP Subnet Mask
 VID

- 6 Go to **Menu > System > IP Setup > IP Setup > IP Setup**. Configure the In-band Default Gateway. Click **Apply**.

IP Setup
 Default Gateway
 Domain Name Server 1
 Domain Name Server 2
 Default Management In-band Out-of-band

- 7 Go to **Menu > Networking > VRRP > VRRP Setup**. Enable VRRP for network "192.168.1.252/24". Make sure that the priority is "200". Click **Add**.

Active ON
 Name
 Network
 Virtual Router ID
 Advertisement Interval(s)
 Preempt Mode
 Priority
 Uplink Gateway
 Response Ping
 Primary Virtual IP
 Secondary Virtual IP

3.3.2 Configuration in the Gateway-B

- 1 Access the Gateway-B's web GUI.
- 2 Go to **Menu > Switching > VLAN > VLAN Setup > Static VLAN Setup**. Create/Edit VLAN 1 to make sure only Port 23 is a fixed port. Click **Add**.

Port	Control			Tagging
-	Normal			<input checked="" type="checkbox"/> Tx Tagging
22	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
23	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
24	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging

- 3 Go to **Menu > Switching > VLAN > VLAN Setup > Static VLAN Setup**. Create/Edit VLAN 20 to make sure only Port 24 is a fixed port. Click **Add**.

Active ON

Name

VLAN Group ID

VLAN Type
 Normal
 Private

Association VLAN List

Port	Control	Tagging
-	<input type="text" value="Normal"/>	<input checked="" type="checkbox"/> Tx Tagging
22	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
23	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
24	<input type="radio"/> Normal <input checked="" type="radio"/> Fixed <input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging

- 4 Go to **Menu > Switching > VLAN > VLAN Setup > VLAN Port Setup**. Configure port 24 with PVID 20. Click **Apply**.

Port	Ingress Check	PVID	Acceptable Frame Type
-	<input type="checkbox"/>	<input type="text" value=""/>	All <input type="text" value="v"/>
22	<input type="checkbox"/>	<input type="text" value="1"/>	All <input type="text" value="v"/>
23	<input type="checkbox"/>	<input type="text" value="1"/>	All <input type="text" value="v"/>
24	<input type="checkbox"/>	<input type="text" value="20"/>	All <input type="text" value="v"/>

- 5 Go to **Menu > System > IP Setup > IP Setup > IP Interface > Add/Edit**. Configure the IP address for VLAN 1. Click **Add** and do the same for VLAN 20.

DHCP Client

Option-60

Static IP Address

IP Address

IP Subnet Mask

VID

<input type="radio"/> DHCP Client	
Option-60	<input checked="" type="checkbox"/>
Class-ID	<input type="text" value="Zyxel Corporation"/>
<input checked="" type="radio"/> Static IP Address	
IP Address	<input type="text" value="192.168.20.1"/>
IP Subnet Mask	<input type="text" value="255.255.255.0"/>
VID	<input type="text" value="20"/>
<input type="button" value="Apply"/> <input type="button" value="Clear"/> <input type="button" value="Cancel"/>	

- 6 Go to **Menu > System > IP Setup > IP Setup > IP Setup**. Configure the Default Gateway. Click **Apply**.

IP Setup	
Default Gateway	<input type="text" value="192.168.20.2"/>
Domain Name Server 1	<input type="text"/>
Domain Name Server 2	<input type="text"/>
Default Management	<input checked="" type="radio"/> In-band <input type="radio"/> Out-of-band

- 7 Go to **Menu > Networking > VRRP > VRRP Setup**. Enable VRRP for network "192.168.1.252/24". Click **Add**.

Active	<input checked="" type="checkbox"/>
Name	<input type="text" value="VLAN1"/>
Network	<input type="text" value="192.168.1.253/24"/>
Virtual Router ID	<input type="text" value="1"/>
Advertisement Interval(s)	<input type="text" value="1"/>
Preempt Mode	<input checked="" type="checkbox"/>
Priority	<input type="text" value="100"/>
Uplink Gateway	<input type="text" value="192.168.20.2"/>
Response Ping	<input checked="" type="checkbox"/>
Primary Virtual IP	<input type="text" value="192.168.1.254"/>
Secondary Virtual IP	<input type="text" value="0.0.0.0"/>
<input type="button" value="Apply"/> <input type="button" value="Clear"/> <input type="button" value="Cancel"/>	

3.3.3 Test the Result

- 1 Verify that Gateway-A is the Master VRRP Router. Go to **Menu > Networking > VRRP**. VR Status should display **Master**.

Index	Network	Virtual Router ID	Virtual Router Status	Uplink Status
1	192.168.1.252/24	1	Master	Active

- 2 Verify that Gateway-B is the Backup VRRP Router. Go to **Menu > Networking > VRRP**. VR Status should display **Backup**.

Index	Network	Virtual Router ID	Virtual Router Status	Uplink Status
1	192.168.1.253/24	1	Backup	Active

- 3 Verify that Gateway-A and Gateway-B has a default route to their respective USG in **Menu > Monitor > Routing Table > IPv4 Routing Table**.

Index	Destination	Gateway	Interface	Metric	Type	Uptime
1	192.168.10.0/24	192.168.10.1	192.168.10.1	1	LOCAL	0:07:08
2	192.168.1.0/24	192.168.1.252	192.168.1.252	1	LOCAL	0:40:22
3	127.0.0.0/16	127.0.0.1	127.0.0.1	1	LOCAL	2:09:30
4	default	192.168.10.2	192.168.10.1	1	STATIC	0:06:35

Index	Destination	Gateway	Interface	Metric	Type	Uptime
1	192.168.20.0/24	192.168.20.1	192.168.20.1	1	LOCAL	0:06:46
2	192.168.1.0/24	192.168.1.253	192.168.1.253	1	LOCAL	0:30:53
3	127.0.0.0/16	127.0.0.1	127.0.0.1	1	LOCAL	5:41:32
4	default	192.168.20.2	192.168.20.1	1	STATIC	0:06:00

- 4 Configure the Host with a Static IP. The Host should be able to ping the virtual IP address **192.168.1.254**.

```
C:\Windows\system32>ping 192.168.1.254

Pinging 192.168.1.254 with 32 bytes of data:
Reply from 192.168.1.254: bytes=32 time<1ms TTL=254

Ping statistics for 192.168.1.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

- 5 Disconnect port 23 or port 24 of Gateway-A. Hosts should still be able to ping the virtual IP address **192.168.1.254**.

3.3.4 What Could Go Wrong?

- 1 If the hosts are not able to access the Internet when Gateway-A has been disconnected from the network, the following problems may have occurred:
 - a. Verify that the hosts and Gateway-B IP interface are in the same subnet and VLAN.
 - b. Check for link failures on port 23 or port 24 of Gateway-B.
 - c. Check whether Gateway-B has a default route to USG-B.

3.4 How to configure bandwidth control to limit incoming or outgoing traffic rate

This example shows administrators how to configure bandwidth control to manage traffic rates. We can limit either incoming traffic, outgoing traffic, or both. In this example, we use two computers: FTP Client (PC) and FTP Server (FTP Server). PC will either be uploading files or downloading files from the FTP Server.

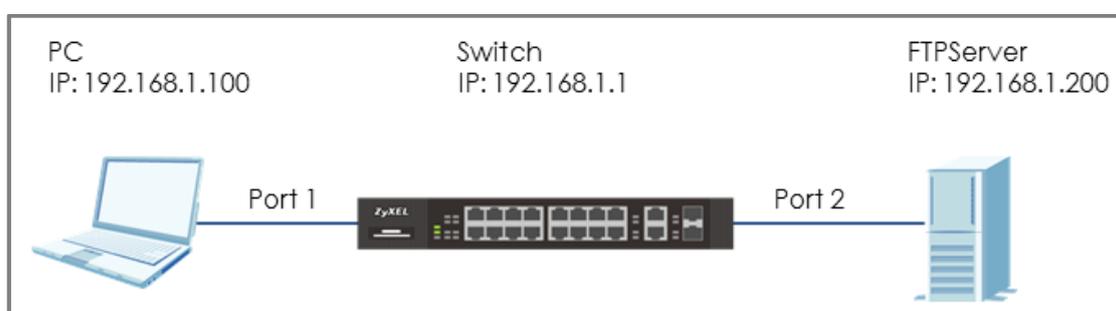


Figure 15 Configure bandwidth control to limit the traffic rate



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 XGS2220-30 (Firmware Version: V4.80).

3.4.1 Configure Switch

- 1 Enter the web GUI. Go to **Menu > Switching > QoS > Bandwidth Control**. Switch **on** the Bandwidth Control. Key in the rate in **Ingress Rate (PC Upload rate) = 10240 kbps** and **Egress Rate (PC Download rate) = 20480 kbps**. Remember to check the port **“Active”** boxes as well. Click **“Apply”**.

Active

Port	Active	Ingress Rate	Active	Egress Rate
*	<input type="checkbox"/>	<input type="text"/> kbps	<input type="checkbox"/>	<input type="text"/> kbps
1	<input checked="" type="checkbox"/>	<input type="text" value="10240"/> kbps	<input checked="" type="checkbox"/>	<input type="text" value="20480"/> kbps
2	<input type="checkbox"/>	<input type="text" value="64"/> kbps	<input type="checkbox"/>	<input type="text" value="64"/> kbps
3	<input type="checkbox"/>	<input type="text" value="64"/> kbps	<input type="checkbox"/>	<input type="text" value="64"/> kbps
4	<input type="checkbox"/>	<input type="text" value="64"/> kbps	<input type="checkbox"/>	<input type="text" value="64"/> kbps

3.4.2 Test the Result

- 1 Use PC to upload a file to the FTP Server. Transfer rate should be more or less 1.2 MB/s (or 10240 Mb/s).

Server/Local file	Directi...	Remote file	Size	Priority	Status
test@192.168.1.200					
D:\Test\TestFile.avi	-->>	/TestFile.avi	83.1 MB	Normal	Transferring
00:00:14 elapsed	00:00:58 left		18,612,224 bytes		1.2 MB/s

- 2 Use PC to download a file from the FTP Server. Transfer rate should be more or less 2.4 MB/s (or 20480 Mb/s).

Server/Local file	Directi...	Remote file	Size	Priority	Status
test@192.168.1.200					
D:\Test\TestFile.avi	<<--	/TestFile.avi	3.4 GB	Normal	Transferring
00:00:28 elapsed	00:23:37 left		71,762,000 bytes		2.4 MB/s

3.5 How to configure ACL to rate limit IP traffic

In some networks, it is necessary to configure rate limits among VLANs. For example, VLAN 10 is for employees within the organization; VLAN 20 is for guests. By rate limiting VLAN 20, we can ensure better bandwidth or network performance for users in VLAN 10. This example shows administrators how to configure ACL to rate limit VLAN traffic. Results are verified by observing and comparing the upload and download rate between VLAN 10 and VLAN 20.

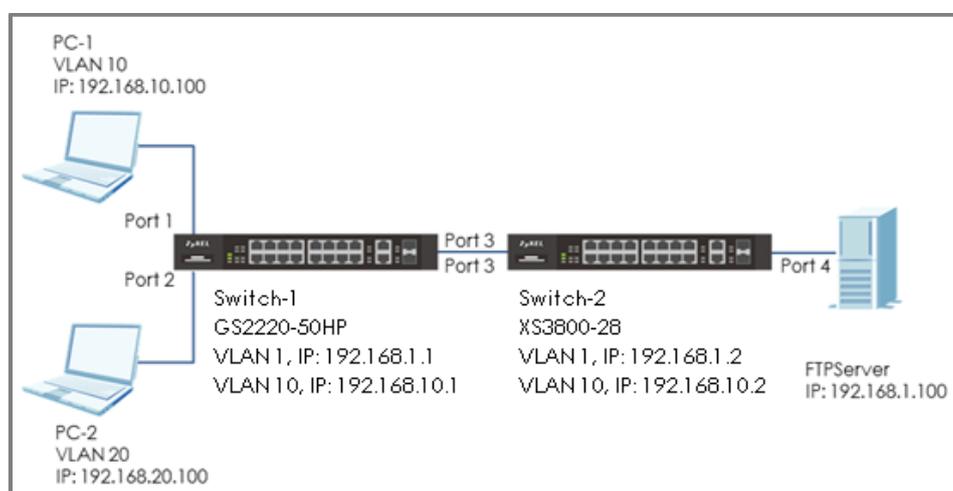


Figure 16 Configure ACL to rate limit VLAN traffic



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 XGS2220-30 (Firmware Version: V4.80) and GS2220-50HP (Firmware Version: V4.80).

3.5.1 Configure VLAN and Route Traffic

- 1 Configure the VLAN setting (VLAN 10 and VLAN 20) on Switch-1 and Switch-2 (Please refer to the topic: **2.1 How to configure the switch to separate traffic between departments**).
- 2 Configure the route traffic on Switch-1 and Switch-2 (Please refer to the topic: **2.2 How to configure the switch to route traffic across VLANs**)

3.5.2 Configure the Classifier

- 1 Set up the **Classifier** on Switch-2: Go to **Menu > Security > Classifier > Classifier Setup**. Set up 4 Classifier: Classifier for download and upload in VALN 10 and VLAN 20. Therefore, there are total 4 Classifiers.

 **Note:**
ACL causes traffic that matches the criteria of a **Classifier** to follow its corresponding **Policy Rule**.

- 2 The Classifier for download traffic in VLAN 10: Enable the **Active** setting and key in the Name. Set **Layer 3 > Destination** as **192.168.10.0/24** (Means the destination is in VLAN 10) and **Source** as **192.168.1. 100/32** (Means the source is FTPServer). Press "Add".

Active	<input checked="" type="checkbox"/> ON
Name	DL10
Weight	32767
Layer 3	
IPv4 DSCP	<input checked="" type="radio"/> Any <input type="radio"/> []
IPv6 DSCP	<input checked="" type="radio"/> Any <input type="radio"/> []
Precedence	<input checked="" type="radio"/> Any <input type="radio"/> []
ToS	<input checked="" type="radio"/> Any <input type="radio"/> []
IP Protocol	<input checked="" type="radio"/> All <input type="checkbox"/> Establish Only <input type="radio"/> Others [] (Dec)
IPv6 Next Header	<input checked="" type="radio"/> All <input type="checkbox"/> Establish Only <input type="radio"/> Others [] (Dec)
Source IP Address/Prefix	192.168.1.100 / 32
Destination IP Address/Prefix	192.168.10.1 / 24

- 3 The Classifier for upload traffic in VLAN 10: Enable the **Active** setting and key in the Name. Set **Layer 3 > Destination** as **192.168.1.100/32** (Means the destination is FTPServer) and **Source** as **192.168.10.0/24** (Means the source is from VLAN 10). Press "Add".

Active	<input checked="" type="checkbox"/>	ON
Name	<input type="text" value="UL10"/>	
Weight	<input type="text" value="32767"/>	
Layer 3		
IPv4 DSCP	<input checked="" type="radio"/> Any	<input type="text"/>
IPv6 DSCP	<input checked="" type="radio"/> Any	<input type="text"/>
Precedence	<input checked="" type="radio"/> Any	<input type="text"/>
ToS	<input checked="" type="radio"/> Any	<input type="text"/>
IP Protocol	<input checked="" type="radio"/> All <input type="checkbox"/> Establish Only	<input type="text"/> (Dec)
IPv6 Next Header	<input checked="" type="radio"/> All <input type="checkbox"/> Establish Only	<input type="text"/> (Dec)
Source IP Address/Prefix	<input type="text" value="192.168.10.1"/> / <input type="text" value="24"/>	
Destination IP Address/Prefix	<input type="text" value="192.168.1.100"/> / <input type="text" value="32"/>	

- 4 The Classifier of download in VLAN 20: Check the "Active" and key in the Name. Set **Layer 3 > Destination** as **192.168.20.0/24** (Means the destination is in VLAN 20) and **Source** as 192.168.1.100/32 (Means the source is FTPServer). Press "Add".
- 5 The Classifier of upload in VLAN 20: Check the "Active" and key in the Name. Set **Layer 3 > Destination** as **192.168.1.100/32** (Means the destination is FTPServer) and **Source** as **192.168.20.0/24** (Means the source is from VLAN 20). Press "Add".

3.5.3 Configure the ACL (Policy Rule)

- 1 Set up the **Policy Rule** on Switch-2: In section 3.5.2, we created 4 Classifiers. We can find that they are shown in the Policy Rule window for us to match. Go to **Menu > Security > Policy Rule > Add/Edit**.
- 2 The Policy Rule of download traffic in VLAN 10: Enable the **Active** setting and key in the Name. Select the Classifier of download in VLAN 10 (DL10). Set up the action to do if match this Classifier: **Bandwidth Metering=40960** kbps. Enable **Metering** and set the **Out-of-profile action** (Means what to do if the rate is over the bandwidth) as **“Drop the packet”** (Means Switch-2 will drop the traffic which is over the bandwidth). Press **“Add”**.

Source & Destination	
Active	<input checked="" type="checkbox"/>
Name	<input type="text" value="PolicyDL10"/>
Classifier(s)	<input type="text" value="DL10"/> DL20 UL10 UL20
General Parameters	
Vlan ID	<input type="text" value="1"/>
Egress Port	<input type="text" value="1"/>
Priority	<input type="text" value="0"/>
DSCP	<input type="text"/>
TOS	<input type="text" value="0"/>
Metering Parameters	
Bandwidth	<input type="text" value="40960"/> kbps
Out of Profile DSCP	<input type="text"/>

Action	
Forwarding	<input checked="" type="radio"/> No change <input type="radio"/> Discard the packet
Priority	<input checked="" type="radio"/> No change <input type="radio"/> Set the packet's 802.1p priority <input type="radio"/> Replace the 802.1p priority field with the inner 802.1p priority value
Diffserv	<input checked="" type="radio"/> No change <input type="radio"/> Set the packet's TOS field <input type="radio"/> Set the Diffserv Codepoint field in the frame
Outgoing	<input type="checkbox"/> Send the packet to the mirror port <input type="checkbox"/> Send the packet to the egress port <input type="checkbox"/> Set the packet's VlanID
Metering	<input checked="" type="checkbox"/> ON
	Out of profile action <input checked="" type="checkbox"/> Drop the packet <input type="checkbox"/> Change the DSCP value

- 3 The Policy Rule of upload in VLAN 10: Check the "Active" and key in the Name. Select the Classifier of upload in VLAN 10 (UP10). Set up the action to do if match this Classifier: **Bandwidth Metering**=20480 kbps. Enable **Metering** and set the **Out-of-profile action** as "**Drop the packet**". Press "Add".

- 4 The Policy Rule of download in VLAN 20: Check the "Active" and key in the Name. Select the Classifier of download in VLAN 20 (DP20). Set up the action to do if match this Classifier: **Bandwidth Metering**=20480 kbps. Enable **Metering** and set the **Out-of-profile action** as "**Drop the packet**". Press "Add".

- 5 The Policy Rule of upload in VLAN 20: Check the "Active" and key in the Name. Select the Classifier of upload in VLAN 20 (UP20). Set up the action to do if match this Classifier: **Bandwidth Metering**=10240 kbps. Enable **Metering** and set the **Out-of-profile action** as "**Drop the packet**". Press "Add".

3.5.4 Test the Result

- 1 Go to **Menu > Advanced Application > Classifier**. Check "Count". If the traffic matches the classifier, the Match Count for this classifier should be increasing every time the web page refreshes.

Active	<input checked="" type="checkbox"/>
Name	DL10
Weight	32767
Log	<input type="checkbox"/>
Count	<input checked="" type="checkbox"/>

Index	Active	Weight	Name	Match Count	Rule
1	<input checked="" type="checkbox"/>	32767	DL10	10	SrcIP = 192.168.1.100/32; DestIP = 192.168.10.1/24; count:

- 2 Use PC-1 to download a file from the FTP Server. Transfer rate should be more or less 5 MB/s (or 40960 Mb/s).

Server/Local file	Directi...	Remote file	Size	Priority	Status
test@192.168.1.100					
D:\Test\TestFile.avi	<<--	/TestFile.avi	87.1 MB	Normal	Transferring
00:00:15 elapsed	00:00:03 left	<div style="width: 89.6%; background-color: green;">89.6%</div>	78,086,956 bytes	5.0 MB/s	

- 3 Use PC-1 to upload a file to the FTP Server. Transfer rate should be more or less 2.6 MB/s (or 20480 Mb/s).

Server/Local file	Directi...	Remote file	Size	Priority	Status
test@192.168.1.100					
D:\Test\TestFile.avi	<<--	/TestFile.avi	3.6 GB	Normal	Transferring
00:00:21 elapsed	00:23:21 left	<div style="width: 1.5%; background-color: green;">1.5%</div>	56,150,564 bytes	2.6 MB/s	

- 4 Use PC-2 to download a file from the FTP Server. Transfer rate should be more or less 2.6 MB/s (or 20480 Mb/s).

Server/Local file	Directi...	Remote file	Size	Priority	Status
test@192.168.1.100					
D:\Test\TestFile.avi	-->>	/TestFile.avi	87.1 MB	Normal	Transferring
00:00:15 elapsed	00:00:20 left	<div style="width: 45.4%; background-color: green;">45.4%</div>	39,583,744 bytes	2.6 MB/s	

- 5 Use PC-2 to upload a file to the FTP Server. Transfer rate should be more or less 1.2 MB/s (or 10240 Mb/s).

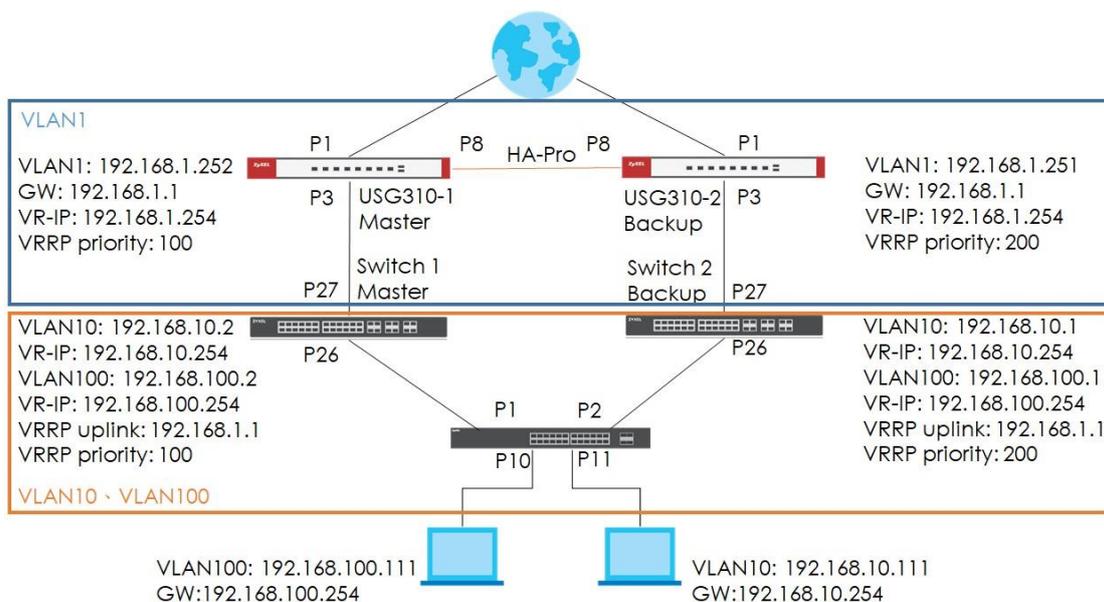
Server/Local file	Directi...	Remote file	Size	Priority	Status
test@192.168.1.100					
D:\Test\TestFile.avi	-->>	/TestFile.avi	87.1 MB	Normal	Transferring
00:00:11 elapsed	00:00:59 left	 17.1%	14,942,208 bytes	(1.3 MB/s)	

3.5.5 What Could Go Wrong

- 1 When setting up the Classifier, remember to consider both the source and destination of the traffic. In the example, if we only set up the source as VLAN 10 (192.168.10.0/24) during file upload the Server, but didn't set up the destination (Server IP: 192.168.1.150), it will cause all the traffic to be rate limited when the PC try to send traffic to others from VLAN 10.

3.6 How to Implement VRRP with Multiple Routing Interface Combine with HA-pro Using Zyxel Enterprise Switch

In the previous chapter, we have introduced VRRP and how to configure it to do redundancy. However, the example in the chapter is talking about how to do redundancy when a company has two Internet Service Provider (ISP). In fact, some companies may only have one ISP and there is only one gateway device connected to it. What if the cable connected between ISP and gateway device is not working or the cable is bitten by a mouse. Or, the gateway device somehow has an abnormal behavior. These situations may cause a single point failure and the customers can't connect to the Internet. To avoid this failure happen, we can use two gateway devices and combine VRRP with HA-pro to do the redundancy.



Upon the topology, the normal traffic flow will be like figure 1. However, somehow the gateway device USG310-1 (Master) or the link 1 or 2 has some issues. It will cause all hosts that connected to Switch-1 (Master) not be able to surf the Internet.

In this situation, VRRP & Device HA-Pro is a very useful method to provide redundancy. USG310-2 (Backup) will take all over as the Master and clockwise for Switch-2 (Backup) to ensure that all of the hosts can still access the Internet. For now, the traffic flow will be like figure 2.

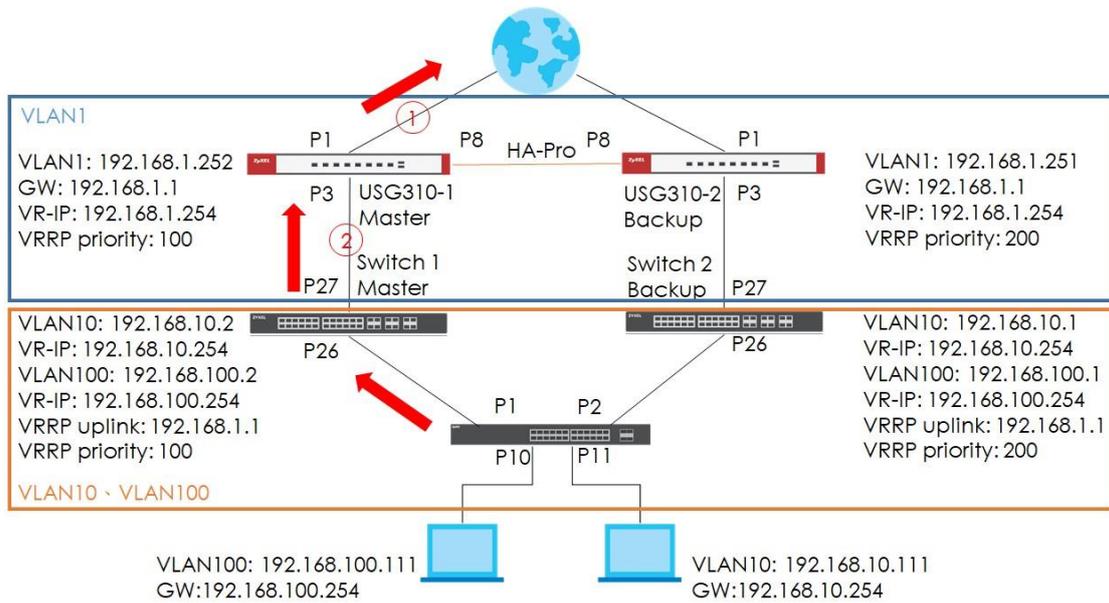


Figure 1

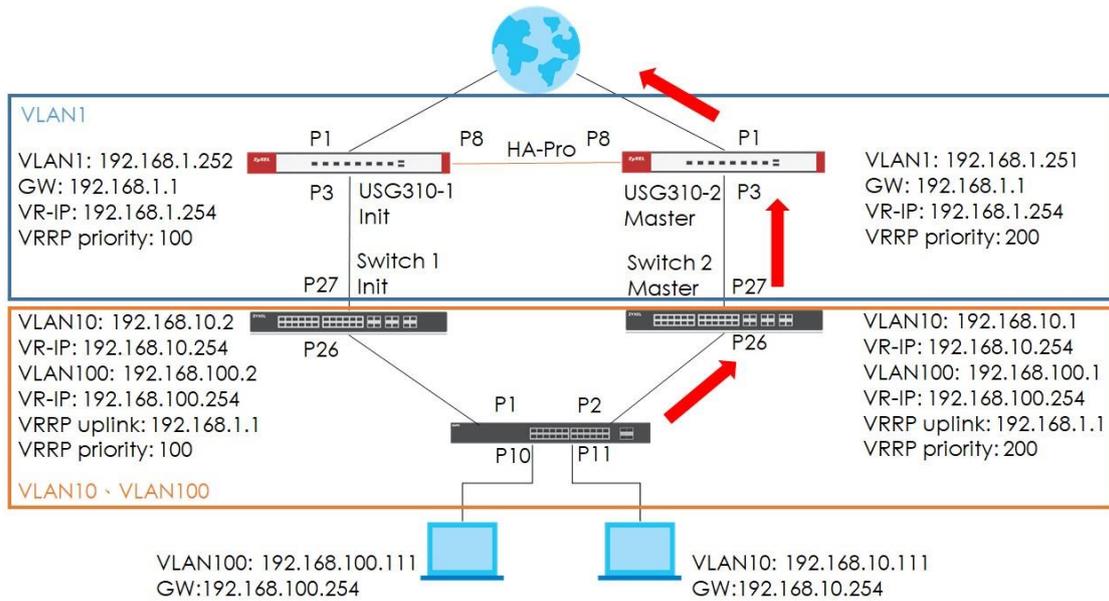


Figure 2



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.

3.6.1 Configuration

L3 Switch (XS3800) (Firmware version: 4.80):

1. Access switch-1 (Master) web GUI
2. Go to **Menu > Switching > VLAN > VLAN Setup > Static VLAN Setup > Add/Edit.**
3. Create VLAN 10 and VLAN 100 for host.

VLAN 10:

Active	<input checked="" type="checkbox"/>		
Name	PC_Port11		
VLAN Group ID	10		
VLAN Type	<input checked="" type="radio"/> Normal <input type="radio"/> Private		
Association VLAN List			
Port	Control		Tagging
*	Normal		<input checked="" type="checkbox"/> Tx Tagging
26	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input checked="" type="checkbox"/> Tx Tagging
27	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input checked="" type="checkbox"/> Tx Tagging

VLAN 100:

Port	Control	Tagging
*	Normal	<input checked="" type="checkbox"/> Tx Tagging
26	<input checked="" type="radio"/> Fixed	<input checked="" type="checkbox"/> Tx Tagging
27	<input checked="" type="radio"/> Fixed	<input checked="" type="checkbox"/> Tx Tagging

4. Got to **Menu > System > IP Setup > IP Setup > IP Interface**

5. Configure IP interface to VLAN 1 for uplink.

DHCP Client
Option-60
Class-ID Zyxel Corporation

Static IP Address
IP Address 192.168.1.251
IP Subnet Mask 255.255.255.0
VID 1

Apply Clear Cancel

6. Configure IP interface to VLAN 10 & VLAN 100 for hosts.

VLAN 10:

A configuration window for IP settings. At the top, there is a radio button for "DHCP Client" which is unselected. Below it, "Option-60" is checked with a green checkmark, and "Class-ID" is set to "Zyxel Corporation". The "Static IP Address" radio button is selected and highlighted with a red box. Under "Static IP Address", the "IP Address" field contains "192.168.10.1", the "IP Subnet Mask" field contains "255.255.255.0", and the "VID" field contains "10". At the bottom, there are three buttons: "Apply" (green), "Clear" (grey), and "Cancel" (grey).

VLAN 100:

A configuration window for IP settings, identical to the one above but for VLAN 100. The "VID" field now contains "100". The "Static IP Address" section and its fields are highlighted with a red box.

7. Configure IP default gateway for VLAN 1 interface.

An "IP Setup" configuration window. The "Default Gateway" field contains "192.168.1.1" and is highlighted with a red box. Below it are two empty text boxes for "Domain Name Server 1" and "Domain Name Server 2". At the bottom, the "Default Management" section has two radio buttons: "In-band" (selected and highlighted with a red box) and "Out-of-band" (unselected).

8. Go to **Menu > Networking > VRRP > VRRP Setup**

9. Configure VRRP on all VLAN interface, "Response Ping" is optional. However, if response ring is inactive, you won't be able to ping virtual IP.

VLAN 1:

Active	<input checked="" type="checkbox"/>
Name	<input type="text" value="VLAN1"/>
Network	<input type="text" value="192.168.1.251/24"/>
Virtual Router ID	<input type="text" value="1"/>
Advertisement Interval(s)	<input type="text" value="1"/>
Preempt Mode	<input checked="" type="checkbox"/>
Priority	<input type="text" value="200"/>
Uplink Gateway	<input type="text" value="192.168.1.1"/>
Response Ping	<input checked="" type="checkbox"/>
Primary Virtual IP	<input type="text" value="192.168.1.254"/>
Secondary Virtual IP	<input type="text" value="192.168.1.253"/>
<input type="button" value="Apply"/> <input type="button" value="Clear"/> <input type="button" value="Cancel"/>	

VLAN 10:

Active	<input checked="" type="checkbox"/>
Name	<input type="text" value="VLAN10"/>
Network	<input type="text" value="192.168.10.1/24"/>
Virtual Router ID	<input type="text" value="1"/>
Advertisement Interval(s)	<input type="text" value="1"/>
Preempt Mode	<input checked="" type="checkbox"/>
Priority	<input type="text" value="200"/>
Uplink Gateway	<input type="text" value="192.168.1.1"/>
Response Ping	<input checked="" type="checkbox"/>
Primary Virtual IP	<input type="text" value="192.168.10.254"/>
Secondary Virtual IP	<input type="text" value="192.168.10.253"/>
<input type="button" value="Apply"/> <input type="button" value="Clear"/> <input type="button" value="Cancel"/>	

VLAN 100:

10. Access the Switch-2 (Backup) web GUI.

11. Go to **Menu > Switching > VLAN > VLAN Setup > Static VLAN Setup > Add/Edit.**

12. Create VLAN 10 & VLAN 100 for hosts.

VLAN 10:

Port	Control	Tagging
-	Normal	<input checked="" type="checkbox"/> Tx Tagging
26	<input checked="" type="radio"/> Fixed	<input checked="" type="checkbox"/> Tx Tagging
27	<input checked="" type="radio"/> Fixed	<input checked="" type="checkbox"/> Tx Tagging

VLAN 100:

Port	Control	Tagging
*	Normal	<input checked="" type="checkbox"/> Tx Tagging
26	<input type="radio"/> Normal <input checked="" type="radio"/> Fixed	<input type="radio"/> Forbidden <input checked="" type="checkbox"/> Tx Tagging
27	<input type="radio"/> Normal <input checked="" type="radio"/> Fixed	<input type="radio"/> Forbidden <input checked="" type="checkbox"/> Tx Tagging

13. Go to **Menu > System > IP Setup > IP Setup > IP Interface**

14. Configure IP interface on VLAN 1 for uplink.

VLAN 1:

DHCP Client
Option-60
Class-ID Zyxel Corporation

Static IP Address

IP Address 192.168.1.252
IP Subnet Mask 255.255.255.0
VID 1

Apply Clear Cancel

15. Configure IP interface on VLAN 10 & VLAN 100 for hosts.

VLAN 10:

IP configuration form for VLAN 100. The form includes radio buttons for DHCP Client and Static IP Address. The Static IP Address option is selected. Fields include Option-60 (checked), Class-ID (Zyxel Corporation), IP Address (192.168.10.2), IP Subnet Mask (255.255.255.0), and VID (10). Buttons for Apply, Clear, and Cancel are at the bottom.

VLAN 100:

IP configuration form for VLAN 100. The form includes radio buttons for DHCP Client and Static IP Address. The Static IP Address option is selected. Fields include Option-60 (checked), Class-ID (Zyxel Corporation), IP Address (192.168.100.2), IP Subnet Mask (255.255.255.0), and VID (100). Buttons for Apply, Clear, and Cancel are at the bottom.

16. Configure IP default gateway on VLAN 1 for the uplink.

IP Setup form. The Default Gateway field is highlighted with a red box and contains the value 192.168.1.1. Other fields include Domain Name Server 1, Domain Name Server 2, and Default Management (In-band selected, Out-of-band unselected). Buttons for Apply, Clear, and Cancel are at the bottom.

17. Go to **Menu > Networking > VRRP > VRRP Setup**.

18. Configure VRRP on all VLAN interface, "Response Ping" is optional. However, if response ping is inactive, you won't be able to ping virtual IP.

VLAN 1:

Active	<input checked="" type="checkbox"/>
Name	Backup
Network	192.168.1.252/24
Virtual Router ID	1
Advertisement Interval(s)	1
Preempt Mode	<input checked="" type="checkbox"/>
Priority	100
Uplink Gateway	192.168.1.1
Response Ping	<input checked="" type="checkbox"/>
Primary Virtual IP	192.168.1.254
Secondary Virtual IP	192.168.1.253

VLAN 10:

Active	<input checked="" type="checkbox"/>
Name	Backup
Network	192.168.10.2/24
Virtual Router ID	1
Advertisement Interval(s)	1
Preempt Mode	<input checked="" type="checkbox"/>
Priority	100
Uplink Gateway	192.168.1.1
Response Ping	<input checked="" type="checkbox"/>
Primary Virtual IP	192.168.10.254
Secondary Virtual IP	192.168.10.253

VLAN 100:

Active	<input checked="" type="checkbox"/>
Name	Backup
Network	192.168.100.2/24
Virtual Router ID	1
Advertisement Interval(s)	1
Preempt Mode	<input checked="" type="checkbox"/>
Priority	100
Uplink Gateway	192.168.1.1
Response Ping	<input checked="" type="checkbox"/>
Primary Virtual IP	192.168.100.254
Secondary Virtual IP	192.168.100.253

L2 switch (GS1920) (Firmware version: 4.80):

1. Access layer 2 switch via web GUI.
2. Go to **Menu > Switching > VLAN > VLAN Setup > Static VLAN Setup**. (If you are using V4.70 firmware, please go to **Menu > Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup**.)
3. Configure VLAN 10 & VLAN 100 for hosts.

VLAN 10:

Active ON

Name

VLAN Group ID

Port	Control			Tagging
*	Normal			<input checked="" type="checkbox"/> Tx Tagging
1	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
2	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
3	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
4	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
5	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
6	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
7	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
8	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
9	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
10	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
11	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
12	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging

VLAN 100:

Active ON

Name

VLAN Group ID

Port	Control			Tagging
*	Normal			<input checked="" type="checkbox"/> Tx Tagging
1	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
2	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
3	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
4	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
5	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
6	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
7	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
8	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
9	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
10	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
11	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
12	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging

- Go to **Menu > System > IP Setup > IP Setup** (If you are using V4.70 firmware, please go to **Basic Setting > IP Setup > IP Configuration**)

5. Configure IP interface for VLAN 10 & VLAN 100

VLAN 10:

VLAN 100:

6. Go to **Menu > Switching > VLAN > VLAN Setup > Static VLAN Setup**. (If you are using V4.70 firmware, please go to **Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup**)

7. Enter VLAN 1 to inactivate VLAN.

	VID	Active	Name
<input checked="" type="checkbox"/>	1	ON	VLAN1
<input type="checkbox"/>	10	ON	VLAN10
<input type="checkbox"/>	100	ON	VLAN100

8. Turn off the “Active” to inactive VLAN 1 then click Apply.

Active	<input type="radio"/> OFF
Name	VLAN1
VLAN Group ID	1

- Go to **Menu > Switching > VLAN > VLAN Setup > VLAN Port Setup**.
(If you are using V4.70 firmware, please go to **Advanced Application > VLAN > VLAN Configuration > VLAN Port Setting**)

- Configure PVID on port 10 & 11

Port	Ingress Check	PVID	Acceptable Frame Type
*	<input type="checkbox"/>		All
1	<input type="checkbox"/>	1	All
2	<input type="checkbox"/>	1	All
3	<input type="checkbox"/>	1	All
4	<input type="checkbox"/>	1	All
5	<input type="checkbox"/>	1	All
6	<input type="checkbox"/>	1	All
7	<input type="checkbox"/>	1	All
8	<input type="checkbox"/>	1	All
9	<input type="checkbox"/>	1	All
10	<input type="checkbox"/>	100	All
11	<input type="checkbox"/>	10	All
12	<input type="checkbox"/>	1	All

Gateway:

- Access USG310-1 (Master) web GUI.
- Go to **Configuration > Device HA > Device HA Pro**
- Configure device HA-pro on USG310-1, Active/Passive device management IP and password can be modified depends on your settings. Click "Apply & switch to Device HA pro first then click Apply.

General Settings

Serial Number of Licensed Device for License Synchronization: S142L22570056

Active Device Management IP: 1.1.1.1

Passive Device Management IP: 1.1.1.2

Subnet Mask: 255.255.255.0

Password:

Retype to Confirm:

Heartbeat Interval: 2 seconds (1-10)

Heartbeat Lost Tolerance: 2 (1-10)

Monitor Interface

Available Interfaces: ge2, ge4, ge5, ge6, ge7

Monitor Interface: ge1, ge3

Failover Detection

Enable Failover When Interface Failure (Option)

Enable Failover When Device Service Fails (Option)

Apply & switch to Device HA Pro Apply Reset

4. Go to **Configuration > Device HA > General**.

5. Enable the Device HA on General Settings.

Configuration Walkthrough Troubleshooting

Enable Device HA

Device HA Mode: Device HA Pro [\(Switch to Device HA page\)](#)

Apply Reset

6. Access the USG310-2(Backup) web GUI.

7. Go to **Configuration > Device HA > General**.

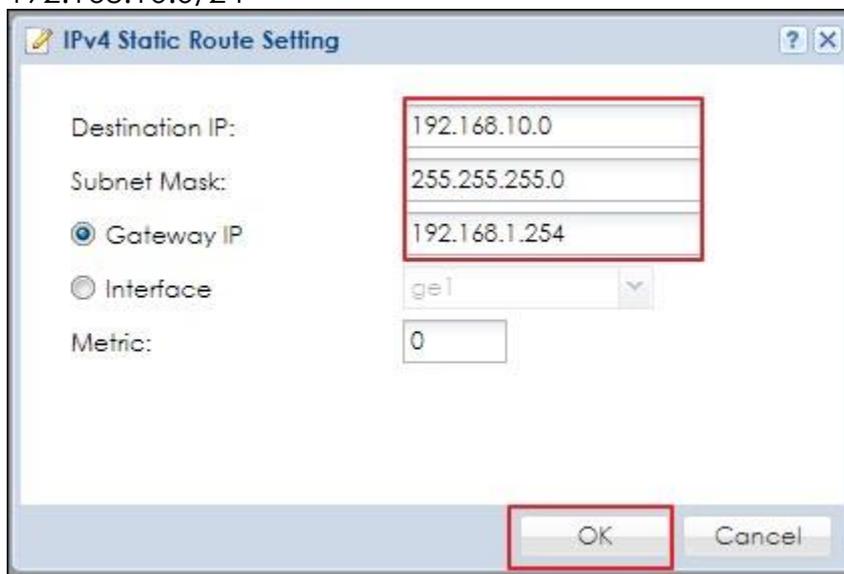
8. Enable the Device HA on General Settings.



9. Go to **Configuration > Routing > Static Route**

10. Configure the routing path for destination 192.168.100.0/24 & 192.168.10.0/24.

192.168.10.0/24



192.168.100.0/24

The screenshot shows a dialog box titled "IPv4 Static Route Setting". It contains the following fields and values:

Destination IP:	192.168.100.0
Subnet Mask:	255.255.255.0
<input checked="" type="radio"/> Gateway IP	192.168.1.254
<input type="radio"/> Interface	gel
Metric:	0

At the bottom right, there are "OK" and "Cancel" buttons. The "OK" button is highlighted with a red box.



Note:

Remember to finish all configurations before connecting the link between USG, otherwise it will not sync successfully.

3.6.2 Verification

L3 Switch (VRRP):

1. Access Switch-1 (Master) via web GUI.
2. Go to **Menu > Networking > VRRP**, the figure below is the successful VRRP status due to switch-1 can reach the gateway IP.

Index	Network	Virtual Router ID	Virtual Router Status	Uplink Status
1	192.168.100.1/24	1	Master	Active
2	192.168.10.1/24	1	Master	Active
3	192.168.1.251/24	1	Master	Active

3. Access Switch-2 (Backup) via web GUI.
4. Go to **IP Application > VRRP**,
5. The figure below is the successful VRRP status. It is normal that the status displays "Init" due to the USG310-2 still in backup status which is down. Therefore, the gateway is unreachable.

Index	Network	Virtual Router ID	Virtual Router Status	Uplink Status
1	192.168.100.2/24	1	Init	Dead
2	192.168.10.2/24	1	Init	Dead
3	192.168.1.252/24	1	Init	Dead



Note: "Init" VR status means that the gateway is not reachable.

Gateway (Device HA-Pro):

1. Access USG310-1 (Master) via web GUI.

2. Go to **Configuration > Device HA**, the figure below is the successful Device HA Pro status.

Active Device Status

Health Status	S/N	MAC	Sync Status
On	S142L35530028	4C9EFF85219B	n/a

Page 1 of 1 Show 50 items Displaying 1 - 1 of 1

Passive Device Status

Health Status	S/N	MAC	Sync Status
On	S142L35530247	4C9EFF85219B	Success

Page 1 of 1 Show 50 items Displaying 1 - 1 of 1

View Log

Active Device Tue Apr 30 05:26:37 2019 Enter Active mode	Passive Device Tue Apr 30 05:46:43 2019 Enter Passive mode Tue Apr 30 05:46:52 2019 Start to synchronize with active device Tue Apr 30 05:49:39 2019 Synchronize complete
--	---

- Note:
1. USG must be configured with "Static route" to send the traffic back to host.
 2. All hosts (e.g. PC) default gateway must be configured with VRRP primary

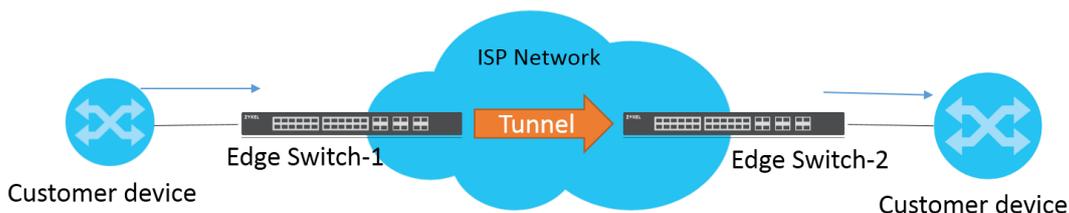
3.6.3 What may go wrong?

1. Switch VRRP uplink gateway must be configured with USG's IP.
2. Remember to configure the VLAN member on the downlink switch.

3.7 How to Configure the Switch to Tunnel Layer 2 Protocol Packets Through Service Provider Network

Zyxel switch models support Layer-2 Protocol Tunneling (L2PT) that allows edge switches to tunnel layer-2 protocol packets through service provider networks. It could be used when customer switches are located at different sites and connected across a service provider network.

Therefore, the customer networks can implement independent layer 2 protocol solutions. For example, it could provide a single and independent spanning tree domain for customer networks across a service provider network.



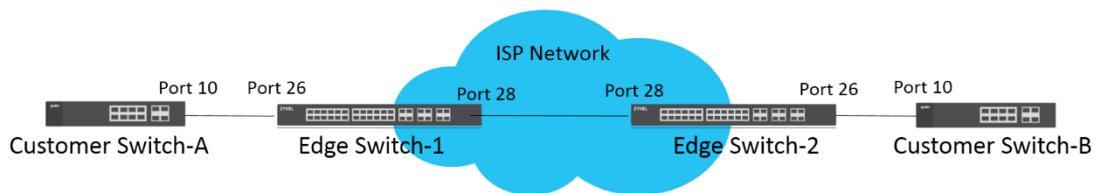
When Edge switch-1 receives Layer-2 protocol packets, it will encapsulate these packets and rewrite their destination MAC addresses with a specific MAC address. All the switches inside the service provider network treat these encapsulated packets as data packets and forward them to the other side. When Edge switch-2 receives these encapsulated packets, it will de-capsulate them and change their destination MAC addresses back to the original one before forwarding them to the destination switch.

Each port on edge switch has two modes:

- **Access** Port: For ingress ports which reside on the service provider's edge switch and connect to a customer switch, incoming layer 2 protocol packets received on an access port are encapsulated and forwarded to the tunnel ports.
- **Tunnel** Port: For egress ports which reside on the edge of the service provider's network and connect to another service provider's switch,

incoming encapsulated layer 2 protocol packets received on a tunnel port are decapsulated and sent to an access port.

The following example will instruct how an administrator configures a switch to tunnel STP packets through a service provider network.

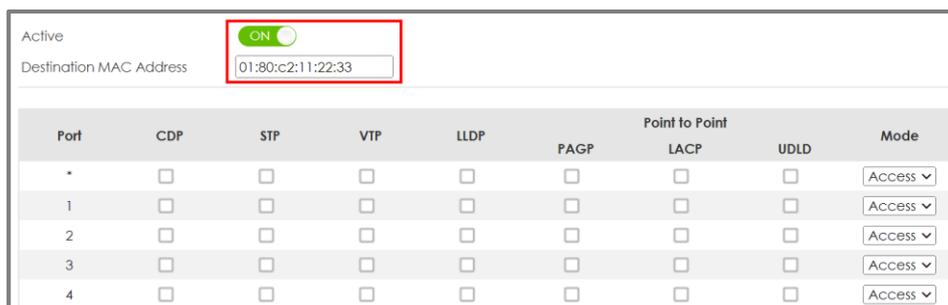


 Note:

The example was tested using two XS3800 (firmware version: 4.80) as edge switches, and two GS2220 (firmware version: 4.80) as customer switches.

3.7.1 Configuration on the Edge Switch

- 1 Setup **Edge Switch-1**: Access to the web GUI. Go to **Menu > Switching > Layer 2 Protocol Tunneling**. Enable the **Active** setting, and set the “**Destination MAC Address**”.



Port	CDP	STP	VTP	LLDP	Point to Point			Mode
					PAGP	LACP	UDLD	
*	<input type="checkbox"/>	Access ▾						
1	<input type="checkbox"/>	Access ▾						
2	<input type="checkbox"/>	Access ▾						
3	<input type="checkbox"/>	Access ▾						
4	<input type="checkbox"/>	Access ▾						



Note:

Destination MAC Address can be either a unicast MAC address or a multicast MAC address.

1. For **unicast** MAC address: make sure the MAC address does **NOT** exist in the MAC table of switches which reside in the service provider's network.
2. For **multicast** MAC address: make sure the MAC address is **NOT** used for specific protocols, such as STP, VTP,



Note:

All the edge switches in the service provider's network should use the **same** MAC address for encapsulation.

- 2 Setup **Edge Switch-1**: On the same page. Check “**STP**” and set “**Mode**” as “**Access**” on port 26 which connects to the customer switch.
- 3 Setup **Edge Switch-1**: On the same page. Set “**Mode**” as “**Tunnel**” on port 28 which connects to another edge switch in service provider's network, and click “**Apply**”.

Active

Destination MAC Address

Port	CDP	STP	VTP	LLDP	PAGP	Point to Point		UDLD	Mode
						LACP			
*	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Access ▾
1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Access ▾
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Access ▾
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Access ▾
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Access ▾
26	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Access ▾					
27	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Access ▾
28	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Tunnel ▾



Note:

Activate L2PT services for supported protocols on the access port(s) only.

- 4** Setup **Edge Switch-2**: Access to the web GUI. Go to **Menu > Switching > Layer 2 Protocol Tunneling**. Enable the **Active** setting, and set the "Destination MAC Address".

Active

Destination MAC Address

Port	CDP	STP	VTP	LLDP	PAGP	Point to Point		UDLD	Mode
						LACP			
*	<input type="checkbox"/>	Access ▾							
1	<input type="checkbox"/>	Access ▾							
2	<input type="checkbox"/>	Access ▾							
3	<input type="checkbox"/>	Access ▾							
4	<input type="checkbox"/>	Access ▾							



Note:

Destination MAC Address can be either a unicast MAC address or multicast MAC address.

- For **unicast** MAC address: make sure the MAC address does **NOT** exist in the MAC table of switches which reside in the service provider's network.
- For **multicast** MAC address: make sure the MAC address is **NOT** used for specific protocols, such as STP, VTP,

 Note:

All the edge switches in the service provider's network should use the **same** MAC address for encapsulation.

- 5 Setup **Edge Switch-2**: On the same page. Activate STP and set mode as "Access" on port 26 which connects to the customer switch.
- 6 Setup **Edge Switch-2**: On the same page. Set mode as "Tunnel" on port 28 which connects to another edge switch in service provider's network, and click "Apply".

Active

Destination MAC Address

Port	CDP	STP	VTP	LLDP	PAGP	Point to Point		Mode
						LACP	UDLD	
*	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Access ▾
1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Access ▾
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Access ▾
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Access ▾
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Access ▾
26	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Access ▾				
27	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Access ▾
28	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Tunnel ▾

 Note:

Activate L2PT services for supported protocols on the access port(s) only.

3.7.2 Configuration on the Customer Switch

- 1 Setup **Customer Switch-A**: Access to the Web GUI. Go to **Menu > Switching > Spanning Tree Protocol > Spanning Tree Setup**. (If you are using V4.70 firmware, please go to **Menu > Advanced Application > Spanning Tree Protocol > Configuration**.) Check if the Spanning Tree Configuration is **Rapid Spanning Tree**. If not, select it and click "**Apply**".



Note:

It is not necessary to enable STP on edge switches because edge switches only forwarding STP packets through tunnel.

- 2 Set up **Customer Switch-A**: Enter the web GUI. Go to **Menu > Switching > Spanning Tree Protocol > RSTP**. (If you are using V4.70 firmware, please go to **Menu > Advanced Application > Spanning Tree Protocol > RSTP**.) Enable the "**Active**" setting, and set the Bridge Priority = **4096**. Activate port **10**, and click "**Apply**".

Active	<input checked="" type="checkbox"/>				
Bridge Priority		4096			
Hello Time		2	seconds		
MAX Age		20	seconds		
Forwarding Delay		15	seconds		
Port	Active	Edge	Root Guard	Priority	Path Cost
-	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	128	4
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	128	4
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	128	4
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	128	4
5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	128	4
6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	128	4
7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	128	4
8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	128	4
9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	128	4
10	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	128	4

- 3 Setup **Customer Switch-B**: Access to the Web GUI. Go to **Menu > Switching > Spanning Tree Protocol > Spanning Tree Setup**. (If you are using V4.70 firmware, please go to **Menu > Advanced Application > Spanning Tree Protocol > Configuration**.) Check if the Spanning Tree Configuration is **Rapid Spanning Tree**. If not, select it and click **“Apply”**.

Spanning Tree Mode

- Rapid Spanning Tree (RSTP)
- Multiple Rapid Spanning Tree (MRSTP)
- Multiple Spanning Tree (MSTP)

- 4 Set up **Customer Switch-B**: Enter the web GUI. Go to **Menu > Switching > Spanning Tree Protocol > RSTP**. (If you are using V4.70 firmware, please go to **Menu > Advanced Application > Spanning Tree Protocol > RSTP**.) Enable the **“Active”** setting. Activate port **10**, and click **“Apply”**.

Active ON

Bridge Priority ▼

Hello Time seconds

MAX Age seconds

Forwarding Delay seconds

Port	Active	Edge	Root Guard	Priority	Path Cost
-	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value=""/>	<input type="text" value=""/>
1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="128"/>	<input type="text" value="4"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="128"/>	<input type="text" value="4"/>
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="128"/>	<input type="text" value="4"/>
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="128"/>	<input type="text" value="4"/>
5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="128"/>	<input type="text" value="4"/>
6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="128"/>	<input type="text" value="4"/>
7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="128"/>	<input type="text" value="4"/>
8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="128"/>	<input type="text" value="4"/>
9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="128"/>	<input type="text" value="4"/>
10	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="128"/>	<input type="text" value="4"/>

3.7.3 Test the Results

- 1 Verify the status of **Customer Switch-A**: Go to **Menu > Switching > Spanning Tree Protocol > Spanning Tree Protocol Status**. (If you are using V4.70 firmware, please go to **Menu > Advanced Application > Spanning Tree Protocol > Spanning Tree Protocol**.)
The Root Bridge ID and the Our Bridge ID should be the same. This means that Customer Switch-A is the Root Bridge. Port 10 should be in **FORWARDING** state, and its Port Role is **Designated Ports**.

Spanning Tree Protocol: RSTP

	Root Bridge	Our Bridge
Bridge ID	1000-bccf4fb7412f	1000-bccf4fb7412f
Hello Time (seconds)	2	2
Max Age (seconds)	20	20
Forwarding Delay (seconds)	15	15
Cost to Bridge	0	
Port ID	0x0000	
Topology Changed Times	1	
Time Since Last Change	0:00:11	

Port	Port State	Port Role	Designated Bridge ID	Designated Port ID	Designated Cost	Root Guard State
10	FORWARDING	Designated	1000-bccf4fb7412f	0x800a	0	Forwarding

- 2 Verify the status of **Customer Switch-B**: Go to **Menu > Switching > Spanning Tree Protocol > Spanning Tree Protocol Status**. (If you are using V4.70 firmware, please go to **Menu > Advanced Application > Spanning Tree Protocol > Spanning Tree Protocol**.)
Check the port status of Customer Switch-A. Port 10 should be the **Root Port** in **FORWARDING** state.

Spanning Tree Protocol: RSTP						
	Root Bridge		Our Bridge			
Bridge ID	1000-bccf4fb7412f		8000-0019cb000001			
Hello Time (seconds)	2		2			
Max Age (seconds)	20		20			
Forwarding Delay (seconds)	15		15			
Cost to Bridge	4					
Port ID	0x800a					
Topology Changed Times	1					
Time Since Last Change	0:02:24					

Port	Port State	Port Role	Designated Bridge ID	Designated Port ID	Designated Cost	Root Guard State
10	FORWARDING	Root	1000-bccf4fb7412f	0x800a	0	Forwarding

3.7.4 What Could Go Wrong

- 1 Make sure you configure the same destination MAC address of Layer-2 Protocol Tunneling on all the edge switches. Otherwise the encapsulated packets cannot be recognized during the forwarding process between the edge switches.

Designing an IPTV Network

4.1 Introduction for IGMP

Before we begin designing an IPTV Network, there are 3 important concepts of Zyxel's IGMP (Internet Group Management Protocol) and IGMP Snooping that administrators should be aware of.

4.1.1 What are General Queries and Group Specific Queries?

General Query: The querier will send query messages to the multicast clients to learn which multicast groups still have active members within the network.

Group Specific Query: When the client leaves a multicast group and sends a leave group message, the querier will send this query message to learn if a particular group has any other active members on a downlink port.

4.1.2 What are IGMP Snooping Querier Modes?

There are 3 Querier Modes: Auto, Fixed and Edge.

Fixed: To have the Switch always use the port as an IGMP query port. Select this when you connect an IGMP multicast server to the port.

Edge: Prevents the switch from using the port as an IGMP query port. The Switch will not keep any record of an IGMP router being connected to this port. The switch does not forward IGMP join or leave packets to this port.

Auto: The port behaves as a Fixed port if the port receives any IGMP queries. The port behaves as an Edge port if the port receives no IGMP queries within a period of time.

4.1.3 What are the differences between IGMP Snooping fast/normal/immediate leave?

Fast leave:

In fast leave mode, the switch itself sends out an IGMP Group-Specific Query (GSQ) message right after receiving an IGMP leave message from a host on a port. This determines whether other hosts connected to the

port should remain in the specific multicast group. This helps speed up the leave process.

Normal leave:

In normal leave mode, when the Switch receives an IGMP leave message from a host on a port, it forwards the message to the multicast router. The multicast router then sends out an IGMP Group-Specific Query (GSQ) message to determine whether other hosts connected to the port should remain in the specific multicast group. The switch forwards the query message to all hosts connected to the port and waits for IGMP reports from hosts to update the forwarding table.

Immediate leave:

Select this option to set the Switch to remove this port from the multicast tree once the ports receive an IGMP leave message. Select this option if there is only one host connected to this port.

4.2 How to configure IGMP routing for multicast clients in a different LAN

The example shows administrators how to configure IGMP routing on the Zyxel Layer 3 switch. This is necessary when the multicast clients are in a different LAN or VLAN from the streaming server.

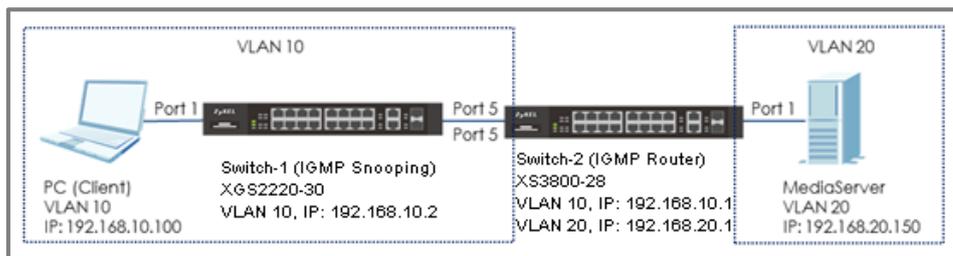


Figure 17 Configure IGMP routing for multicast clients in different VLAN



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 XS3800-28 (Firmware Version: V4.80) and XGS2220-30 (Firmware Version: V4.80).

4.2.1 Configure Switch-1

- 1 Configure the VLAN 10 on Switch-1. (Please refer to the topic: **2.1 How to configure the switch to separate traffic between departments**)
- 2 Configure the IGMP Snooping: Enter the web GUI and go to **Menu > Switching > Multicast > IPv4 Multicast > IGMP Snooping**. Enable the **Active** setting, and select Unknown Multicast Frame as **Drop**. Select the port 5 as **Fixed**. Click "Apply".

Active

Querier

Querier Version v3

Report Proxy

Host Timeout 260 seconds

802.1p Priority No-Change

IGMP Filtering Active

IGMP Snooping Smart Forward Active

Unknown Multicast Frame Flooding Drop Drop on VLAN

Unknown Multicast Frame to Querier Port Drop Forwarding Forwarding on VLAN

Reserved Multicast Group Flooding Drop

Port	Immediate Leave	Normal Leave	Fast Leave	Group Limited	Max Group Number	Throttling	IGMP Filtering Profile	IGMP Querier Mode
*	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	0	Deny	Default	Auto
1	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	0	Deny	Default	Auto
2	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	0	Deny	Default	Auto
3	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	0	Deny	Default	Auto
4	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	0	Deny	Default	Auto
5	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	0	Deny	Default	Fixed

4.2.2 Configure Switch-2

- 1 Configure the VLAN 10 and VLAN 20 on Switch-2. Please refer to the topic: **2.1 How to configure the switch to separate traffic between departments.**
- 2 Configure the IP addresses for Switch on BOTH VLAN 10 and VLAN 20 as shown in the figure. Please refer to the topic: **1.1 How to change the switch management IP address to avoid accessing the wrong device.**
- 3 Configure the IGMP Routing: Enter the web GUI and go to **Menu > NETWORKING > IGMP**. Enable the **Active** setting, and select VLAN 10 and VLAN 20 as IGMP-v2. Select “Unknown Multicast Frame” as “Drop”. Click “Apply”.

Index	Network	Version
*	-	IGMP-v2
1	192.168.1.6/24	None
2	192.168.10.1/24	IGMP-v2
3	192.168.20.1/24	IGMP-v2

4.2.3 Test the Result

- 1 Play the stream on Media Server using Multicast IP address 239.1.1.2.
- 2 Have PC send an IGMP join message for 239.1.1.2.
- 3 Go to **Menu > SWITCHING > Multicast > IPv4 Multicast**. PC connected to port 1 joins the Multicast Group-239.1.1.2.

Index	VID	Port	Multicast Group
1	10	2	224.0.0.251
2	10	2	224.0.0.252
3	10	2	239.1.1.2
4	10	2	239.255.255.250

4.2.4 What Could Go Wrong

- 1 The Switch-2 (IGMP Router) must contain both VLAN of Media Server (VLAN 20) and PC (Client) (VLAN 10) so that the IGMP stream can route successfully. If the stream is not received by the Client, try to check the configuration of the VLAN.

4.3 How to configure IGMP Snooping for multicast clients in the same LAN

The example shows administrators how to configure IGMP Snooping for multicast clients and streaming servers in the same VLAN. When Media Server multicasts the stream, IGMP snooping allows the switch to learn multicast groups without having the user to manually configure the each switch. This prevents the switch from flooding multicast streams on ports that have no members for these multicast addresses.

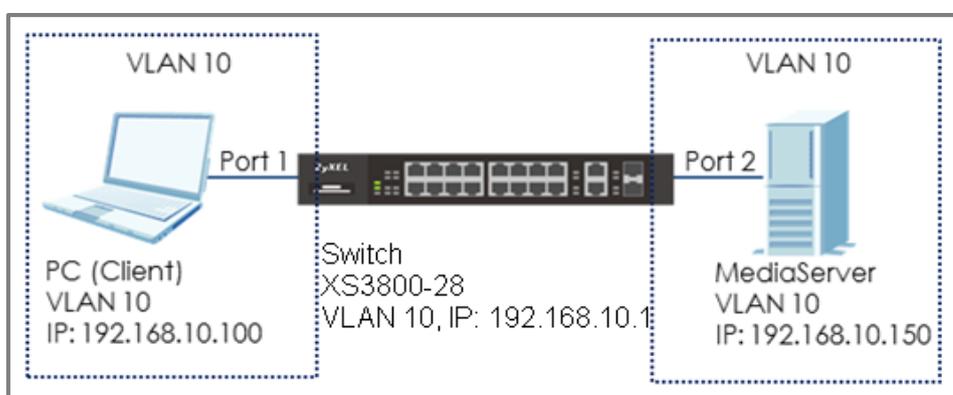


Figure 18 Configure IGMP Snooping for multicast clients in the same LAN



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 XS3800-30 (Firmware Version: V4.80).

4.3.1 Configure Switch

- 1 Configure the VLAN 10 on Switch. (Please refer to the topic: **2.1 How to configure the switch to separate traffic between departments**).
- 2 Configure the IGMP Snooping: Enter the web GUI and go to **Menu > Switching > Multicast > IPv4 Multicast > IGMP Snooping**. Enable the **Active** setting, and select Unknown Multicast Frame as **Drop**. Check **Querier**. Click "Apply".

Active	<input checked="" type="checkbox"/>
Querier	<input checked="" type="checkbox"/>
Querier Version	v3
Report Proxy	<input type="checkbox"/>
Host Timeout	260 seconds
802.1p Priority	No-Change
IGMP Filtering Active	<input type="checkbox"/>
IGMP Snooping Smart Forward Active	<input checked="" type="checkbox"/>
Unknown Multicast Frame	<input type="radio"/> Flooding <input checked="" type="radio"/> Drop <input type="radio"/> Drop on VLAN
Unknown Multicast Frame to Querier Port	<input checked="" type="radio"/> Drop <input type="radio"/> Forwarding <input type="radio"/> Forwarding on VLAN
Reserved Multicast Group	<input checked="" type="radio"/> Flooding <input type="radio"/> Drop

4.3.2 Test the Result

- 1 Play the stream on Media Server using Multicast IP address 239.1.1.1.
- 2 Have PC send an IGMP join message for 239.1.1.1.
- 3 Go to **Menu > Switching > Multicast > IPv4 Multicast**. PC connected to port 1 joins Multicast Group-239.1.1.1.

Index	VID	Port	Multicast Group
1	10	1	224.0.0.251
2	10	1	224.0.0.252
3	10	1	239.1.1.2
4	10	1	239.255.255.250
5	10	2	224.0.0.251
6	10	2	224.0.0.252
7	10	2	239.255.255.250

Network Security

5.1 How to configure the port security to limit the number of connected devices

The example shows administrators how to configure port security to limit the number of connected devices. In a real environment, port security controls the number of users connecting to a server.

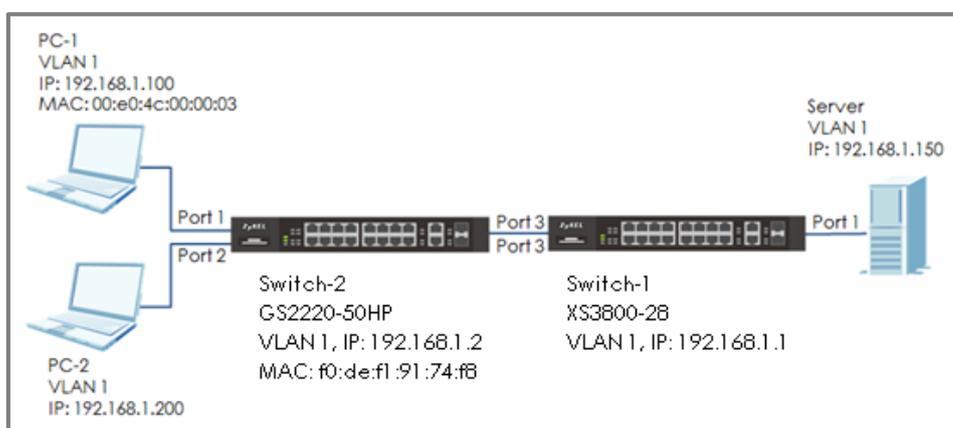


Figure 19 Configure the port security to limit the number of connected devices



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 XS3800-28 (Firmware Version: V4.80) and GS2220-50HP (Firmware Version: V4.80).

5.1.1 Configure Switch-1

- 1 Enter web GUI and go to **Menu > Security > Port Security**. Enable the **Active** setting. Check port 3 and set the "Limited Number of Learned MAC Address" to 2.

Port	Active	Address Learning	Limited Number of Learned MAC Address
*	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="2"/>
4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
5	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
6	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
7	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
8	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
9	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>



Note:

The Zyxel switch sends Link Layer Discovery Protocol (LLDP) packets every period of time by default. If Switch-2 does not support LLDP or is disabled, Limited Number of Learned MAC Address can be set to 1. Otherwise, set this to 2.

5.1.2 Test the Result

- 1 PC-1 can ping Server successfully.

```
C:\Users\User>ping 192.168.1.150

Pinging 192.168.1.150 with 32 bytes of data:
Reply from 192.168.1.150: bytes=32 time=766ms TTL=128
Reply from 192.168.1.150: bytes=32 time<1ms TTL=128
Reply from 192.168.1.150: bytes=32 time<1ms TTL=128
Reply from 192.168.1.150: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.150:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 766ms, Average = 191ms
```

- 2 Connect PC-2 to port 2.

- 3 PC-2 cannot ping Server.

```
C:\Users\User>ping 192.168.1.150

Pinging 192.168.1.150 with 32 bytes of data:
Reply from 192.168.1.200: Destination host unreachable.

Ping statistics for 192.168.1.150:
    Packets: Sent = 4, Received = 0 (0% loss),
```

- 4 Access Switch-1 web GUI. Go to **Menu > Monitor > MAC Table > Search**. The MAC Address Table should show MAC address of PC-1 (and Switch-2), but not the MAC address of PC-2.

Index	MAC Address	VID	Port	Type
1	bc:cf:4f:b7:4e:16	1	3	Dynamic
2	00:0e:1c:d6:ba:ee:6f	1	3	Dynamic
3	00:19:cb:00:00:01	1	CPU	Static

5.1.3 What Could Go Wrong

- 1 The MAC address of Switch-2 will also be learned in Switch-1 MAC address table. Therefore, remember to consider Switch-2's MAC address when setting the number of Limited Number of Learned MAC Address.

5.2 How to configure MAC filter to block unwanted traffic

The example shows administrators how to configure MAC filter to block unwanted traffic. In this example, Switch-1 will block traffic based on which device sends the packet or which device receives the packet.

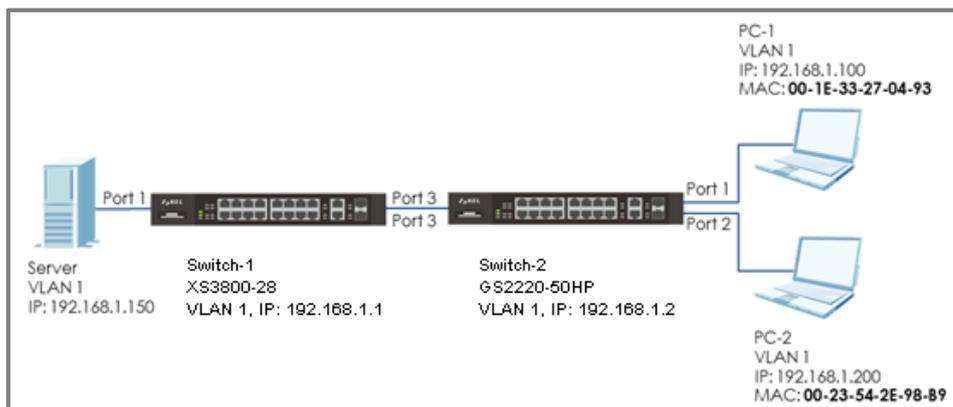


Figure 20 Configure MAC filter to block unwanted traffic



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 XS3800-28 (Firmware Version: V4.80) and GS2220-50HP (Firmware Version: V4.80).

5.2.1 Configure Switch-1

- 1 Enter web GUI and go to **Menu > Switching > Static MAC Filtering > Add/Edit**. Enable the **Active** setting and set the filter Name. Choose the Action as "**Discard source**". Key in the MAC you want to block and the VID. Click "Add".

Active ON

Name

Action Discard source
 Discard destination

MAC

VID



Note:

Use **Discard source** to drop traffic sent **by** the device with the configured MAC entry.

Use **Discard destination** to drop traffic sent **to** the device with the configured MAC entry.

5.2.2 Test the Result

- 1 PC-1 (with MAC address 00:1E:33:27:04:93) fails to ping Server.

```
C:\Users\User>ping 192.168.1.150

Pinging 192.168.1.150 with 32 bytes of data:
Reply from 192.168.1.100: Destination host unreachable.

Ping statistics for 192.168.1.150:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

- 2 PC-2 can ping Server successfully.

```
C:\Users\User>ping 192.168.1.150

Pinging 192.168.1.150 with 32 bytes of data:
Reply from 192.168.1.150: bytes=32 time=766ms TTL=128
Reply from 192.168.1.150: bytes=32 time<1ms TTL=128
Reply from 192.168.1.150: bytes=32 time<1ms TTL=128
Reply from 192.168.1.150: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.150:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 766ms, Average = 191ms
```

5.2.3 What Could Go Wrong

- 1 The MAC address set on Switch-1 should be identical to the MAC address of PC-1 so that the traffic can be blocked successfully.

5.3 How to configure the switch to prevent IP scanning

In this example, we will use **Anti-ARP Scan** to prevent attackers from identifying all network devices in the local area network. ARP Scanning is a method by which attackers send multiple ARP request packets in a very short period of time to flood across the entire broadcast domain.

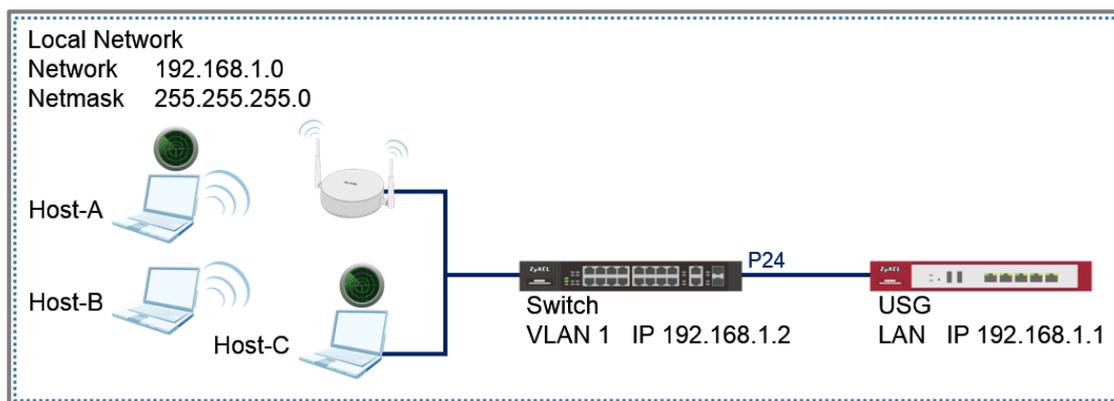


Figure 21 IP Scanning from Wired and Wireless Devices



Note:

All network IP addresses and subnet masks are used as examples in this article. The Access Point in this section uses the default Radio and SSID Profile. For this section, we will refer to "Zenmap" as the IP Scanning tool. All UI displayed in this article are taken from the XS3800 series switch.

5.3.1 Configuration in the Switch

- 1 Access the Switch's Web GUI.
- 2 Go to **Menu > Security > Anti-Arpscan > Anti-Arpscan Setup**. Enable the **Active** Setting. Configure the uplink port (port 24) as "Trusted" state. Click **Apply**.

Active

Port Threshold pps

Host Threshold pps

Port	Trusted State
*	Untrusted ▼
1	Untrusted ▼
2	Untrusted ▼
3	Untrusted ▼
4	Untrusted ▼
5	Untrusted ▼
6	Untrusted ▼
21	Untrusted ▼
22	Untrusted ▼
23	Untrusted ▼
24	Trusted ▼
25	Untrusted ▼

-Optional-

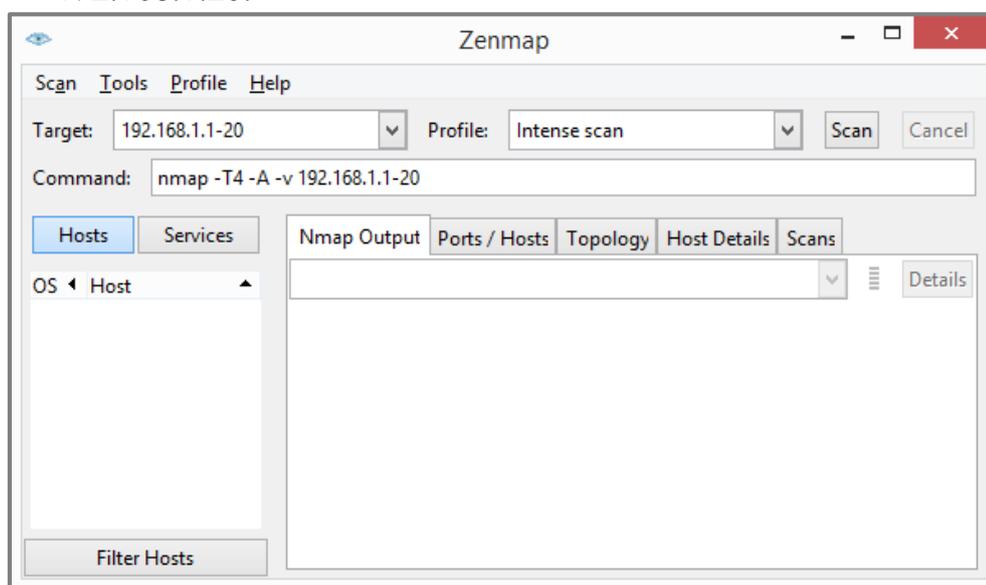
- 3 Go to **Menu > Security > Errdisable > Errdisable Recovery**. Enable the **Active** Setting and check the anti-arpscan box. Click **Apply**.

Active

Reason	Time Status	Interval
*	<input type="checkbox"/>	<input type="text"/>
loopguard	<input type="checkbox"/>	<input type="text" value="300"/>
ARP	<input type="checkbox"/>	<input type="text" value="300"/>
BPDU	<input type="checkbox"/>	<input type="text" value="300"/>
IGMP	<input type="checkbox"/>	<input type="text" value="300"/>
anti-arpscan	<input checked="" type="checkbox"/>	<input type="text" value="300"/>
bpduguard	<input type="checkbox"/>	<input type="text" value="300"/>
zuld	<input type="checkbox"/>	<input type="text" value="300"/>

5.3.2 Test the Result

- 1 Download and install an IP Scanning software into Host-A and Host-C.
- 2 Connect Host-A and Host-B via the Wireless Access Point.
- 3 Host-A should initiate a scan for IP address 192.168.1.1 to 192.168.1.20.



- 4 Host-A should no longer be able to reach the USG.

```
C:\Windows\system32>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Request timed out.
Request timed out.
Reply from 192.168.1.30: Destination host unreachable.
Reply from 192.168.1.30: Destination host unreachable.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
```

- 5 Access the Switch's Web GUI. Go to **Menu > Security > Anti-Arpscan > Anti-Arpscan Host Status**. An entry for Host-A should appear with an "Err-Disable" state.

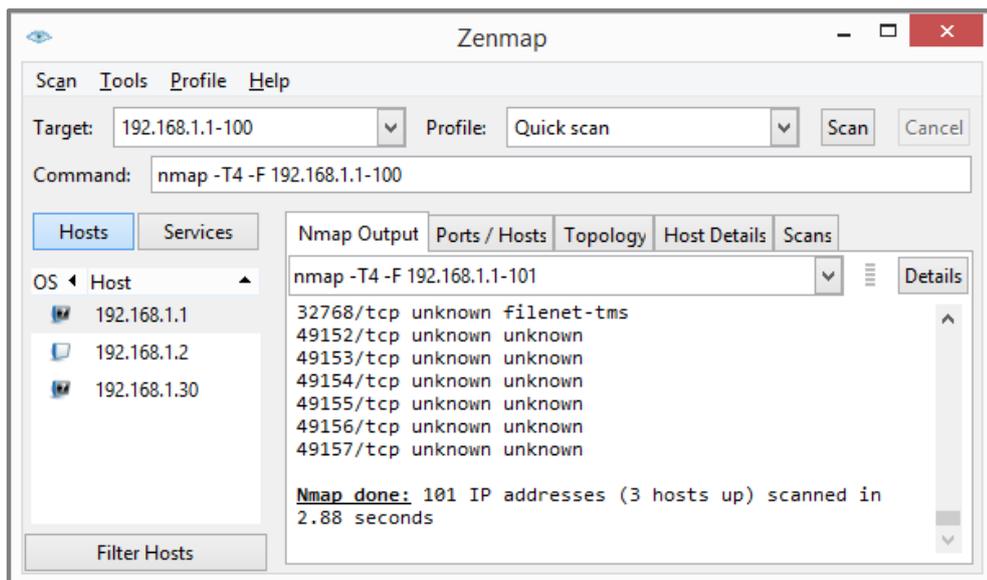
Index	Host IP	MAC Address	VLAN	Port	State
1	192.168.1.30	48:51:b7:37:e6:b9	1	26	Err-Disable



Note:

If Errdisable Recovery has been configured, the Host-A entry should recover after the Errdisable Recovery Interval. Host-A will be able to reach the USG, afterwards.

- 6 Host-B should still be able to reach the USG.
- 7 Connect Host-C to the Switch.
- 8 Host-C should perform a quick scan for IP address 192.168.1.1 to 192.168.1.100.



- 9 Host-C should no longer be able to reach the USG.

```
C:\Windows\system32>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Request timed out.
Request timed out.
Reply from 192.168.1.30: Destination host unreachable.
Reply from 192.168.1.30: Destination host unreachable.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
```

10 Access the Switch's Web GUI. Go to **Menu > Security > Anti-Arpscan > Anti-Arpscan Status**. Port 26 should now be in an Err-disabled state.

Anti-Arpscan is Enabled

Port	Trusted	State
1	OFF	Forwarding
25	OFF	Forwarding
26	OFF	Err-disable

 **Note:**
If Errdisable Recovery has been configured, Port 2 state should change to forwarding after the Errdisable Recovery Interval. Host-C will be able to reach the USG, afterwards.

5.3.3 What Could Go Wrong?

- 1 If access to servers or the local gateway is no longer possible after enabling Anti-Arpscan, make sure that only ports directly connected to hosts or Wireless Access Points are “untrusted”. Ports to servers and the local gateway should be “trusted”.

- 2 If all hosts connected through a Wireless Access Point can no longer reach the local gateway, check whether the port to the Wireless Access Point has changed to the err-disable state in **Menu > Security > Anti-Arpscan > Anti-Arpscan Status**. If so, consider increasing the **Port Threshold** in **Menu > Security > Anti-Arpscan > Anti-Arpscan Setup**.

Active	<input checked="" type="checkbox"/>
Port Threshold	200 pps
Host Threshold	10 pps
Port	Trusted State
*	Untrusted ▾
1	Untrusted ▾
2	Untrusted ▾
3	Untrusted ▾
4	Untrusted ▾

5.4 How to Configure the Switch and RADIUS Server to Provide Network Access through 802.1x Port Authentication

This example will instruct the administrator on how to configure the switch to provide access to machines that provides valid user credentials. With 802.1x Port Authentication, the organization can ensure that only authorized personnel can access core network resources.

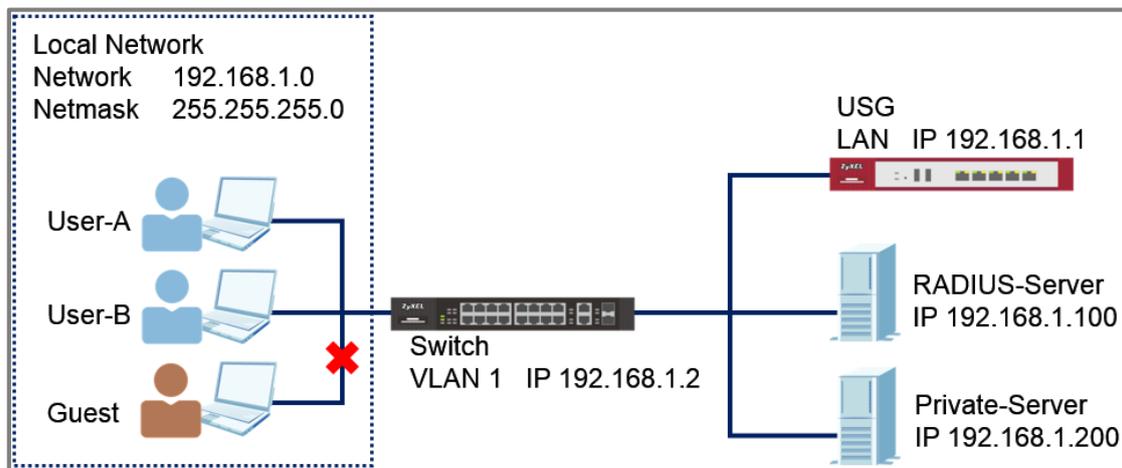


Figure 22 802.1x Port Authentication Providing Access to Authorized Users



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. The authentication server used in this example is FreeRADIUS running in Ubuntu server. All UI displayed in this article are taken from the XS3800 series switch.

5.4.1 Configuration in the Switch

- 1 Access the **Switch's** Web GUI.
- 2 Go to **Menu > Security > AAA > RADIUS Server Setup**. Configure the RADIUS server's IP address and set the shared secret. Click **Apply**.

Authentication Server

Mode:
 Timeout: seconds

Delete	Index	IP Address	UDP Port	Shared Secret	Encrypted Shared Secret
<input type="checkbox"/>	1	<input type="text" value="192.168.1.100"/>	1812	<input type="text" value="zyxel1234"/>	
<input type="checkbox"/>	2	<input type="text"/>	1812	<input type="text"/>	



Note:

The shared secret must match the secret of your RADIUS server's client profile.

- 3 Go to **Menu > Security > Port Authentication > 802.1x**. Enable the **Active** Setting. Check the 802.1x Active box as well as for all ports connected to end devices. Do not check active box of ports connected to either the **USG, RADIUS-Server, or Private-Server**.

Active: ON
 EAPOL flood: OFF

Port	Active	Max-Req	Reauth	Reauth-period secs	Quiet-period secs	Tx-period secs	Supp-Timeout secs
*	<input checked="" type="checkbox"/>	<input type="text"/>	On ▾	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
1	<input checked="" type="checkbox"/>	<input type="text" value="2"/>	On ▾	<input type="text" value="3600"/>	<input type="text" value="60"/>	<input type="text" value="30"/>	<input type="text" value="30"/>
2	<input checked="" type="checkbox"/>	<input type="text" value="2"/>	On ▾	<input type="text" value="3600"/>	<input type="text" value="60"/>	<input type="text" value="30"/>	<input type="text" value="30"/>
3	<input checked="" type="checkbox"/>	<input type="text" value="2"/>	On ▾	<input type="text" value="3600"/>	<input type="text" value="60"/>	<input type="text" value="30"/>	<input type="text" value="30"/>
4	<input checked="" type="checkbox"/>	<input type="text" value="2"/>	On ▾	<input type="text" value="3600"/>	<input type="text" value="60"/>	<input type="text" value="30"/>	<input type="text" value="30"/>
5	<input checked="" type="checkbox"/>	<input type="text" value="2"/>	On ▾	<input type="text" value="3600"/>	<input type="text" value="60"/>	<input type="text" value="30"/>	<input type="text" value="30"/>
6	<input checked="" type="checkbox"/>	<input type="text" value="2"/>	On ▾	<input type="text" value="3600"/>	<input type="text" value="60"/>	<input type="text" value="30"/>	<input type="text" value="30"/>
7	<input checked="" type="checkbox"/>	<input type="text" value="2"/>	On ▾	<input type="text" value="3600"/>	<input type="text" value="60"/>	<input type="text" value="30"/>	<input type="text" value="30"/>
8	<input checked="" type="checkbox"/>	<input type="text" value="2"/>	On ▾	<input type="text" value="3600"/>	<input type="text" value="60"/>	<input type="text" value="30"/>	<input type="text" value="30"/>
28	<input type="checkbox"/>	<input type="text" value="2"/>	On ▾	<input type="text" value="3600"/>	<input type="text" value="60"/>	<input type="text" value="30"/>	<input type="text" value="30"/>
29	<input type="checkbox"/>	<input type="text" value="2"/>	On ▾	<input type="text" value="3600"/>	<input type="text" value="60"/>	<input type="text" value="30"/>	<input type="text" value="30"/>
30	<input type="checkbox"/>	<input type="text" value="2"/>	On ▾	<input type="text" value="3600"/>	<input type="text" value="60"/>	<input type="text" value="30"/>	<input type="text" value="30"/>

5.4.2 Configuration in the RADIUS-Server

- 1 Edit the client profile in `/etc/freeradius/clients.conf`. Save the file and exit.

```
client 192.168.1.2 {
    secret = zyxel1234
    shortname = Switch
    nastype = other
}
```



Note:

The client IP address and secret must match the management IP and shared secret of the Switch.

- 2 Add the following user profiles in `/etc/freeradius/users`. Save the file and exit.

```
User-A Cleartext-Password := "zyxeluserA"
      Service-Type = Administrative-User

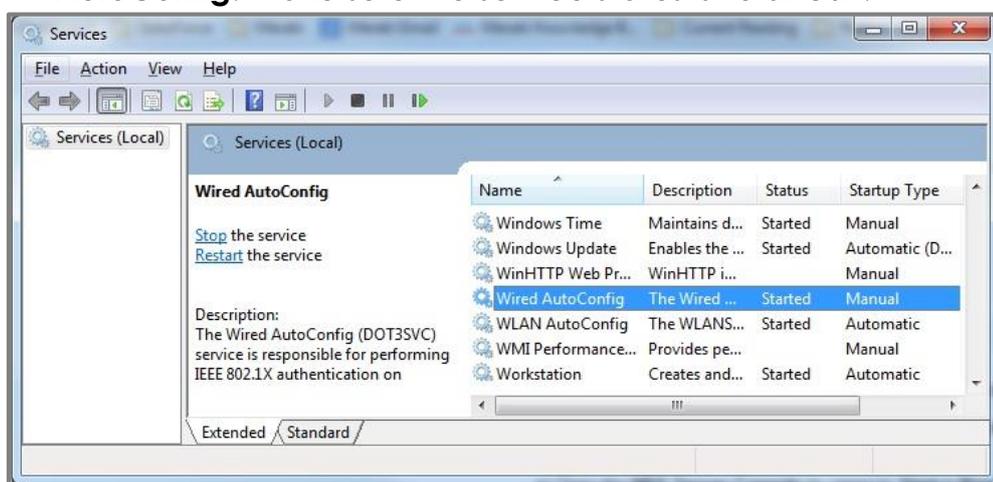
User-B Cleartext-Password := "zyxeluserB"
      Service-Type = Administrative-User
```

- 3 Restart FreeRADIUS service.

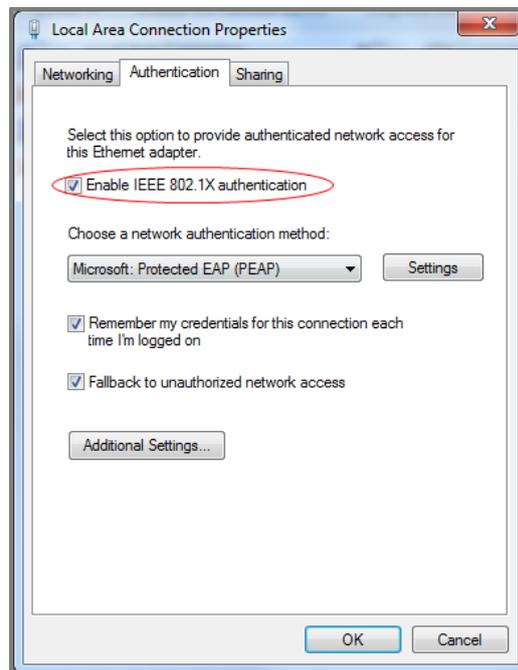
```
root@dhcpc68:/etc/freeradius# stop freeradius
stop: Unknown instance:
root@dhcpc68:/etc/freeradius# start freeradius
freeradius start/running, process 8800
root@dhcpc68:/etc/freeradius#
```

5.4.3 Test the Result

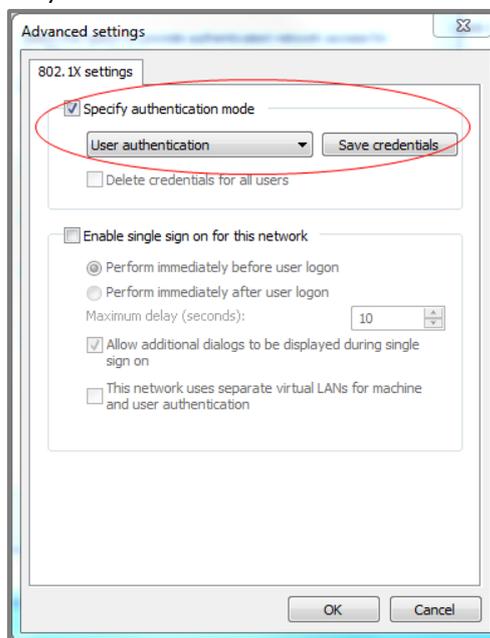
- 1 Access **User-A**, **User-B**, and **Guest** device.
- 2 If using Windows OS, click the **Start button** and type **services.msc** into the search box.
- 3 In the Services window, locate the service named **Wired AutoConfig**. Make sure the service status is "**Started**".



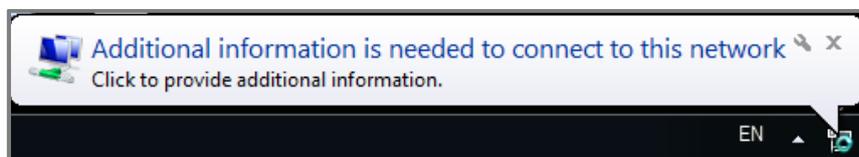
- 4 Right-click on your network adapter and select **Properties**.
- 5 Click on the Authentication tab and check "**Enable IEEE 802.1X authentication**". Make sure that the network authentication method is **Microsoft: Protected EAP (PEAP)**



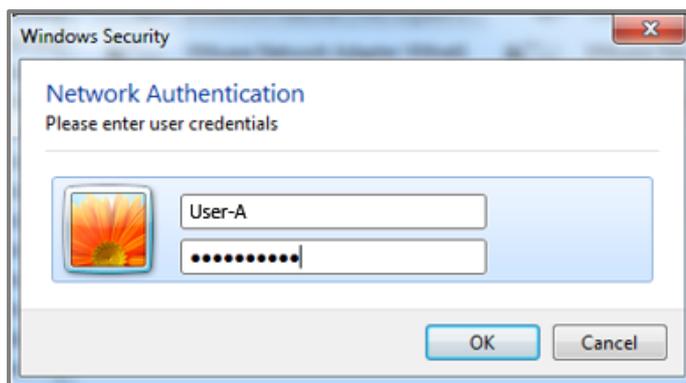
- 6 Click on **Additional Settings**, select **Specify authentication mode** and specify **User authentication**.



- 7 Connect User-A device to the **Switch**. User-A should show an **“Additional information is needed to connect to this network.”** pop-up message.

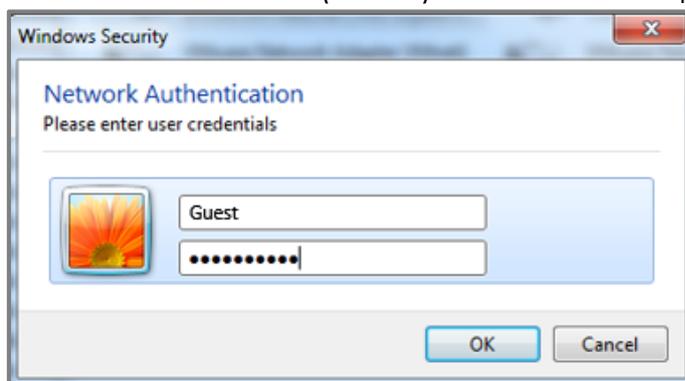


- 8 Enter the username (**User-A**) and password (**zyxeluserA**) which must be consistent with the RADIUS-Server's user profile settings.



- 9 Devices using User-A and User-B credentials can communicate with **USG** and **Private-Server**.
- 10 Connect User-A device to the **Switch**. User-A should show an **“Additional information is needed to connect to this network.”** pop-up message.

- 11 Enter the username (**Guest**) and a random password.



- 12 Device using Guest credentials cannot communicate with **USG** and **Private-Server**.

5.4.4 What May Go Wrong?

- 1 If the Switch does not allow access to users that submitted the correct credentials, the following problems may have occurred:
 - a. Usernames and passwords are case-sensitive. Make sure that the user input the correct lower-case or upper-case characters.
 - b. The RADIUS-server is unreachable. The Switch should be able to ping the RADIUS-Server at all times. Make sure network settings were configured correctly between Switch and RADIUS-Server.
 - c. The shared secret between the Switch and RADIUS-Server is not identical.

5.5 How to configure the switch to send unauthorized users in a guest VLAN

The example shows administrators how to use Guest VLAN for users that fails or used an invalid user credential during 802.1x port authentication. In a real application, we may need to allow guests to access the USG so that they can access the Internet, but still isolated from Private-Server. On the contrary, we have to allow the users with valid credentials to only access the Private-Server.

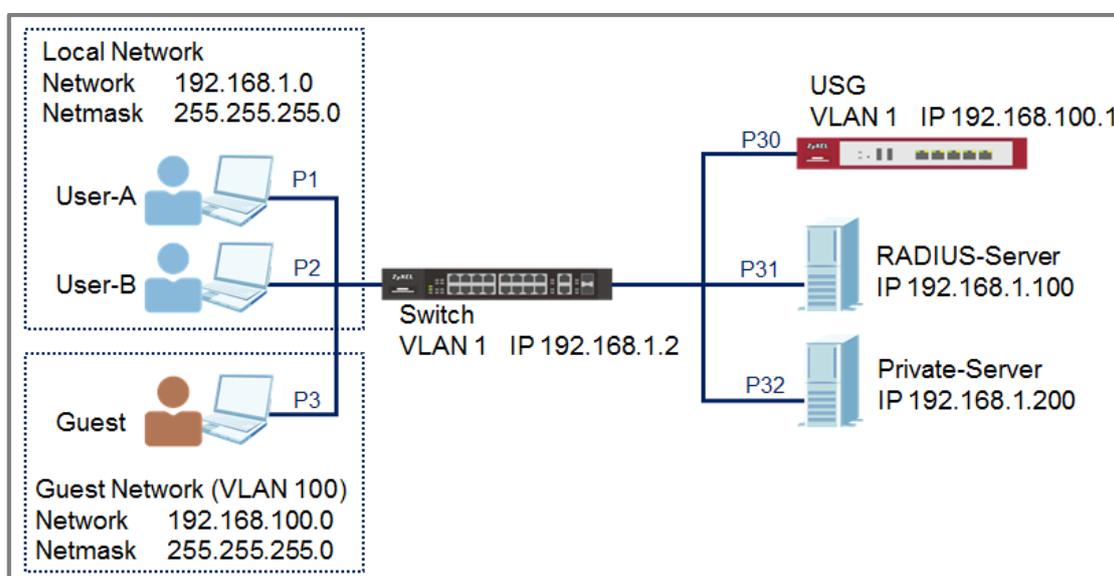


Figure 23 Configure the switch to send unauthorized user in Guest VLAN



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 XS3800-28 (Firmware Version: V4.80).

5.5.1 Configure 802.1x Port Authentication on the Switch

- 1 Configure 802.1x on all towards users. Do not enable Port Authentication on ports to the USG, RADIUS-Server, and Private-Server. To configure Port Authentication, please refer to the topic: **5.4 How to Configure the Switch and RADIUS Server to Provide Network Access through 802.1x Port Authentication.**

5.5.2 Configure VLAN for Guest VLAN

- 1 Configure the VLAN for Guest VLAN (**VLAN 100**) on Switch. **VLAN 100**: Set fixed port: 1, 2, 3, 30; untagged port: 1, 2, 3, 30; forbidden port: 31, 32; port 30: pvid=100. **VLAN 1**: Set forbidden port: 30. For isolating VLAN 1 and 100, please refer to the topic: **2.1 How to configure the switch to separate traffic between departments.**

5.5.3 Configure Guest VLAN for Failed Authentication

- 1 Go to **Menu > Security > Port Authentication > 802.1x > Guest Vlan**. Activate the Guest Vlan on port 1-3 and type the guest Vlan as **100**. Press "Apply".

Port	Active	Guest VLAN	Host-mode	Multi-secure Num
*	<input type="checkbox"/>		Multi-Host	
1	<input checked="" type="checkbox"/>	100	Multi-Host	1
2	<input checked="" type="checkbox"/>	100	Multi-Host	1
3	<input checked="" type="checkbox"/>	100	Multi-Host	1
4	<input type="checkbox"/>	1	Multi-Host	1
5	<input type="checkbox"/>	1	Multi-Host	1

5.5.4 Configure the RadiusServer

- 1 Edit the client profile in `/etc/freeradius/clients.conf`. Save the file and exit.

```
client 192.168.1.1 <
  secret = thisisasecret
  shortname = Switch
  nastype = other
>
```



Note:

The client IP address and secret must match the management IP and shared secret of the Switch.

- 2 Add the following user profiles in `/etc/freeradius/users`. Save the file and exit.

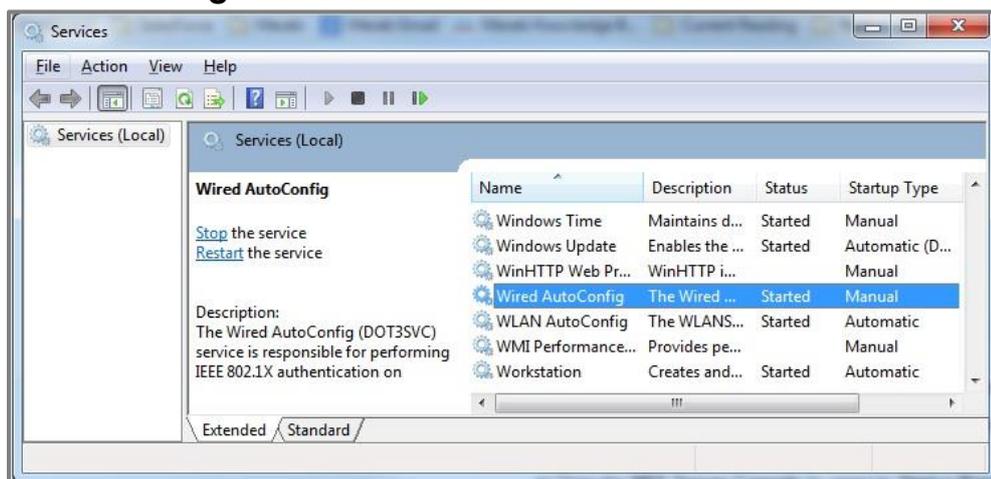
```
user Cleartest-Password := "user1234"
  Service-Type = Administrative-User
```

- 3 Restart FreeRADIUS service.

```
root@dhcpc68:/etc/freeradius# stop freeradius
stop: Unknown instance:
root@dhcpc68:/etc/freeradius# start freeradius
freeradius start/running, process 8800
```

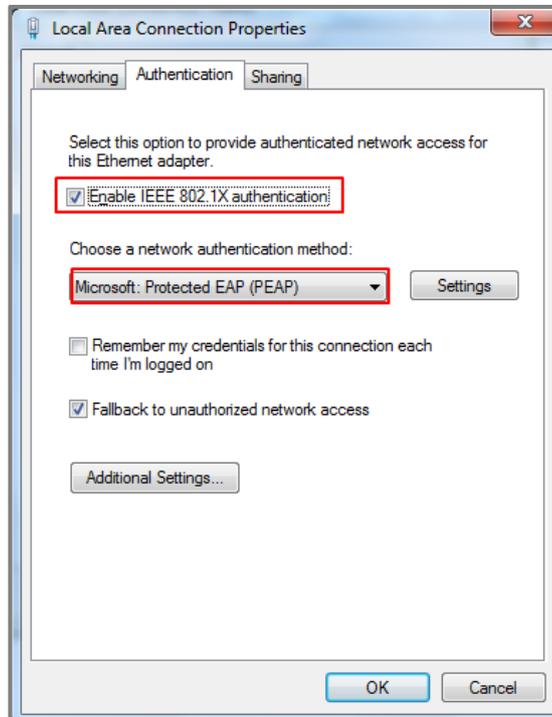
5.5.5 Configure the setting on User-A, User-B and Guest

- 1 In the **Services** window, locate the service named **Wired AutoConfig**. Make sure the service status is "Started".

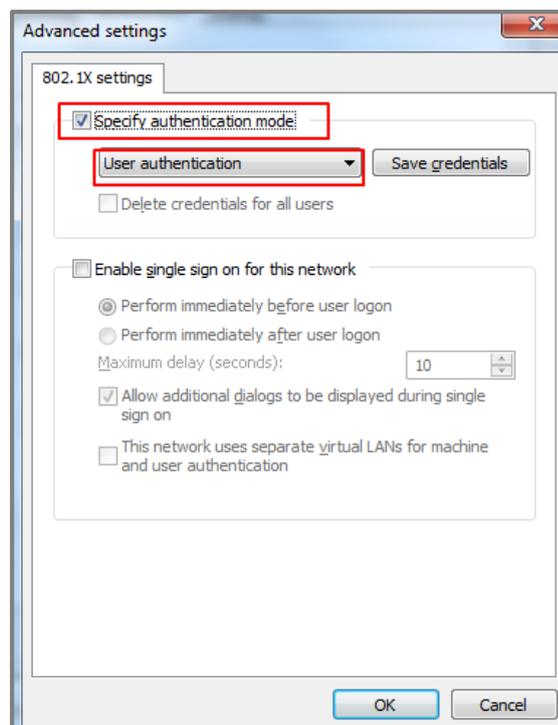


- 2 Right-click on your network adapter and select **Properties**. Click on the Authentication tab and check "**Enable IEEE**

802.1X authentication". Make sure that the network authentication method is "**Microsoft: Protected EAP (PEAP)**".

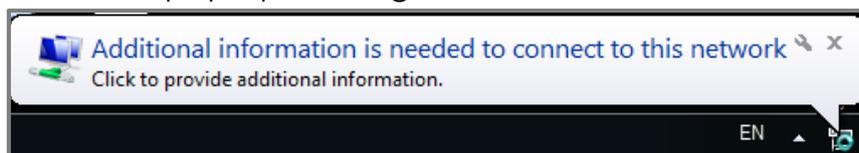


3 Click on **Additional Settings**, select **Specify authentication mode** and specify **User authentication**.

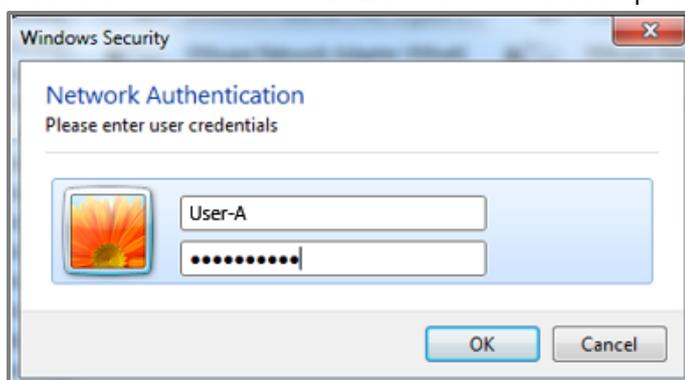


5.5.6 Test the Result

- 1 Disconnect and connect the PC with Switch. PC should show an “**Additional information is needed to connect to this network.**” pop-up message.



- 2 Enter the username (**User-A**) and password (**zyxeluserA**) which must be consistent with the RADIUS-Server's user profile settings.

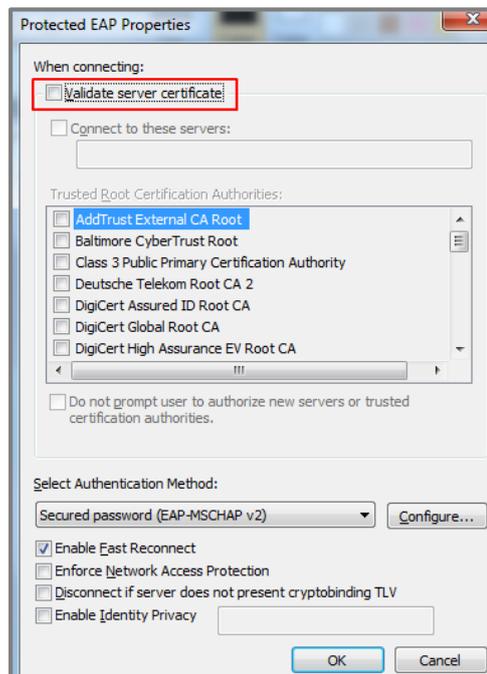


- 3 Devices using User-A and User-B credentials can communicate with Private-Server.
- 4 Connect User-A device to the Switch. User-A should show an “**Additional information is needed to connect to this network.**” pop-up message.
- 5 Enter the username (Guest) and a random password.
- 6 Device using Guest credentials cannot communicate with Private-Server, but it can communicate with USG.
- 7 Check the MAC table of the Switch. The device of users with wrong credentials are assigned to VLAN 100. (**Menu > Monitor > MAC Table > Search**)

Index	MAC Address	VID	Port	Type
1	bc:f1:71:35:59:c6	1	12	Dynamic
2	88:1f:a1:2b:13:90	1	12	Dynamic
3	fc:f5:28:51:e9:8d	1	12	Dynamic
4	00:30:88:de:4b:fe	1	12	Dynamic
5	80:38:fb:07:06:1b	1	12	Dynamic
6	b8:27:eb:d3:36:72	1	12	Dynamic
7	bc:cf:4f:fc:ac:1c	1	12	Dynamic
8	5c:e2:8c:69:85:b3	1	12	Dynamic
9	b8:ec:a3:28:60:57	1	12	Dynamic
10	c2:91:30:8e:5f:b7	1	12	Dynamic
11	20:d1:60:ff:36:70	1	12	Dynamic
12	00:0e:c6:ba:ee:ef	100	10	Dynamic
13	f2:be:aa:84:a2:92	1	12	Dynamic

5.5.7 What Could Go Wrong

- 1 If the PC doesn't pop up the authentication message after connecting the PC to the switch:
 - a. Try to use the Switch to ping Radius-Server. The Switch should be able to ping Radius-Server.
 - b. Right-click on your network adapter and select **Properties > Authentication > Additional settings**. Uncheck the "Validate server certificate".



- 2 If the shared secret setting of Switch and PC does **NOT** match, the authentication will fail.

- 3** If the authentication is fine, but the PC cannot ping Server, please check 801.1X Port Authentication configurations. Do **NOT** activate the authentication on the uplink port (port 2, 3, and 12).

- 4** If devices sent to the Guest VLAN cannot reach the USG, make sure that the switch has created and configured the Guest VLAN in **Menu > Switching > VLAN > VLAN Setup > Static VLAN**.

5.6 How to Configure the Switch and RADIUS Server to Provide Network Access through Device MAC Address

This example will instruct the administrator on how to configure the switch and RADIUS server to provide access to machines with specific MAC addresses. With MAC Authentication, the organization can ensure that only devices provided by the organization can access internal resources.

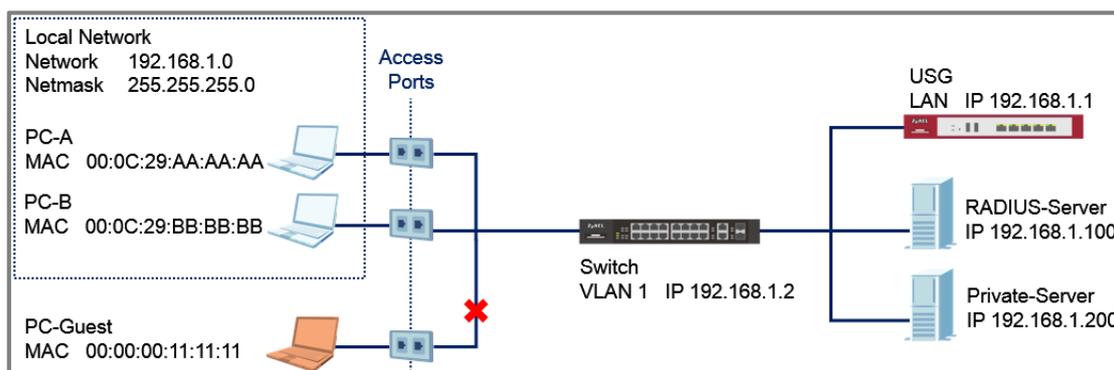


Figure 24 802.1x Port Authentication Providing Access to Authorized Devices



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. The authentication server used in this example is FreeRADIUS running in Ubuntu server. All UI displayed in this article are taken from the XS3800 series switch.

5.6.1 Configuration in the Switch

- 1 Access the **Switch's** Web GUI.
- 2 Go to **Menu > Security > AAA > RADIUS Server Setup**. Configure the RADIUS server's IP address and set the shared secret. Click **Apply**.

Delete	Index	IP Address	UDP Port	Shared Secret	Encrypted Shared Secret
<input type="checkbox"/>	1	192.168.1.100	1812	zyxel1234	
<input type="checkbox"/>	2		1812		



Note:

The shared secret must match the secret of your RADIUS server's client profile.

3 Go to **Menu > Security > Port Authentication > MAC Authentication**. Enable the **Active** Setting. Check the MAC Authentication Active box as well as for access ports. Do not check the active box of ports connected to either the **USG**, **RADIUS-Server**, or **Private-Server**.

Active ON OFF
 Name Prefix
 Delimiter
 Case Upper Lower
 Password Type Static MAC Address
 Password
 Timeout

Port	Active	Trusted-VLAN List
*	<input checked="" type="checkbox"/>	<input type="text"/>
1	<input checked="" type="checkbox"/>	<input type="text"/>
2	<input checked="" type="checkbox"/>	<input type="text"/>
3	<input checked="" type="checkbox"/>	<input type="text"/>
4	<input checked="" type="checkbox"/>	<input type="text"/>
5	<input checked="" type="checkbox"/>	<input type="text"/>
28	<input type="checkbox"/>	<input type="text"/>
29	<input type="checkbox"/>	<input type="text"/>
30	<input type="checkbox"/>	<input type="text"/>

5.6.2 Configuration in the RADIUS-Server

- 1 Edit the client profile in `/etc/freeradius/clients.conf`. Save the file and exit.

```
client 192.168.1.2 {  
    secret = zyxel1234  
    shortname = Switch  
    nastype = other  
}
```



Note:

The client IP address and secret must match the management IP and shared secret of the Switch.

- 2 Add the following user profiles in `/etc/freeradius/users`. Username format should be **<Name Prefix><MAC Address of your device>**. Save the file and exit.

```
Access01-00-0C-29-AA-AA-AA    Cleartext-Password := "zyxel"  
Access01-00-0C-29-BB-BB-BB    Cleartext-Password := "zyxel"
```

- 3 Restart FreeRADIUS service.

```
root@dhcpc68:/etc/freeradius# stop freeradius  
stop: Unknown instance:  
root@dhcpc68:/etc/freeradius# start freeradius  
freeradius start/running, process 8800  
root@dhcpc68:/etc/freeradius#
```

5.6.3 Test the Result

- 1 Connect **PC-A**, **PC-B**, and **PC-Guest** to the Switch.
- 2 PC-A and PC-B should be able to reach the USG and Private-Server.
- 3 PC-Guest should not be able to reach the USG and Private-Server.

5.6.4 What Could Go Wrong?

- 1 If the Switch does not allow access to authorized devices:
 - a. The RADIUS-Server's user profile must use all upper-case characters of the device's MAC Address separated by dashes (-) instead of colons (:).
 - b. Machines, like laptops or notebooks have more than one MAC addresses (LAN, Wireless, etc). Make sure that the correct MAC address is used in the RADIUS-Server's user profile.

- 2 If the Switch still does not allow access to authorized devices after correcting the Switch or RADIUS-Server configurations, wait for a few minutes before trying again. This is determined by the MAC Authentication's timeout value, where the default time a devices is re-validated is **300 seonds**.

5.7 How to configure the switch to prevent ARP spoofing

This example will instruct the administrator on how to configure the switch to protect the network from attackers using the same IP Addresses of core network components (ex. servers or gateways). ARP Spoofing is a type of attack that can cause either denial of services or an unwanted man-in-the-middle receiving sensitive information. IP Source Guard's ARP Inspection forces all clients connected to access ports to use the IP addresses provided by the administrator's dedicated DHCP server.

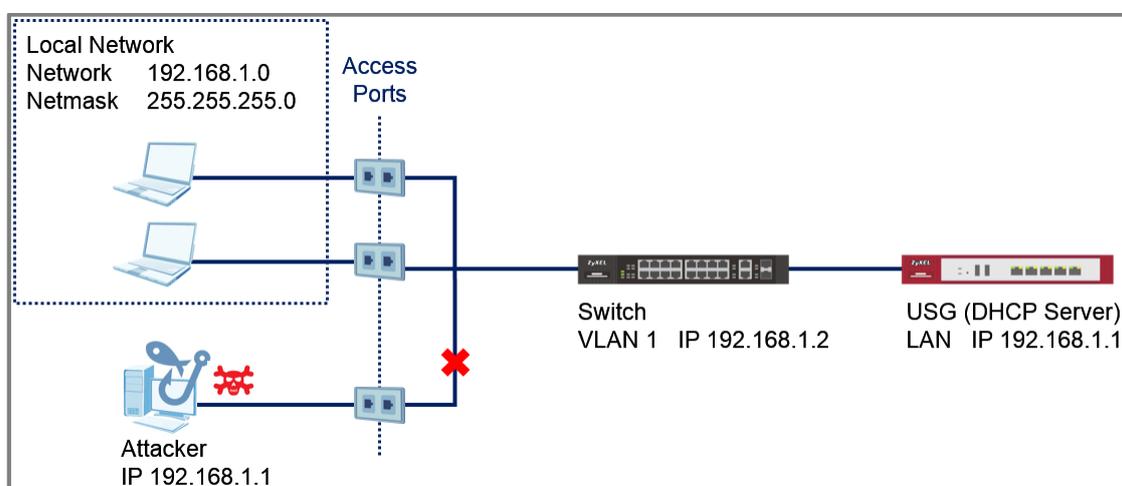


Figure 25 Attacker Using the Same IP Address as the USG



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. All UI displayed in this article are taken from the XS3800 series switch.

5.7.1 Configuration in the Switch

1 Access the **Switch's** Web GUI.

2 Configure **DHCP Snooping** (Refer to section 5.6.1).

Note:
DHCP Snooping must be enabled before configuring ARP Inspection.

3 Go to **Menu > Security > IPv4 Source Guard > ARP Inspection > ARP Insp. Setup**. Enable the Active setting to globally enable ARP Inspection.

4 Go to **Menu > Security > IPv4 Source Guard > ARP Inspection > ARP Insp. Port Setup**. Set all access ports as untrusted ports. Ports to the USG or other network components should be trusted ports. Click **Apply**.

Port	Trusted State	Limit	
		Rate (pps)	Burst Interval (seconds)
*	Untrusted ▼	<input type="text"/>	<input type="text"/>
1	Untrusted ▼	<input type="text" value="15"/>	<input type="text" value="1"/>
2	Untrusted ▼	<input type="text" value="15"/>	<input type="text" value="1"/>
3	Untrusted ▼	<input type="text" value="15"/>	<input type="text" value="1"/>
4	Untrusted ▼	<input type="text" value="15"/>	<input type="text" value="1"/>
5	Untrusted ▼	<input type="text" value="15"/>	<input type="text" value="1"/>
6	Untrusted ▼	<input type="text" value="15"/>	<input type="text" value="1"/>
7	Untrusted ▼	<input type="text" value="15"/>	<input type="text" value="1"/>
8	Untrusted ▼	<input type="text" value="15"/>	<input type="text" value="1"/>
9	Untrusted ▼	<input type="text" value="15"/>	<input type="text" value="1"/>
28	Trusted ▼	<input type="text" value="15"/>	<input type="text" value="1"/>
29	Trusted ▼	<input type="text" value="15"/>	<input type="text" value="1"/>
30	Trusted ▼	<input type="text" value="15"/>	<input type="text" value="1"/>

- 5 Go to **Menu > Security > IPv4 Source Guard Setup > ARP Inspection > ARP Insp. VLAN Setup**. A list of all active VLANs is displayed on this page. Select **Yes** for the access ports' VLAN. Click **Apply**.

Search VLAN by VID

The Number of VLANs: 5 « < Page 1 of 1 > »

VID	Enabled	Log
*	No <input type="button" value="v"/>	None <input type="button" value="v"/>
1	Yes <input type="button" value="v"/>	Deny <input type="button" value="v"/>
2	No <input type="button" value="v"/>	Deny <input type="button" value="v"/>
3	No <input type="button" value="v"/>	Deny <input type="button" value="v"/>
4	No <input type="button" value="v"/>	Deny <input type="button" value="v"/>
5	No <input type="button" value="v"/>	Deny <input type="button" value="v"/>

« < Page 1 of 1 > »

5.7.2 Test the Result

- 1 Connect a device using dynamic IP address in one of the **Switch**'s access ports. This device should be able to communicate with the USG.
- 2 After the device has successfully received an IP address, access the Switch's web GUI. Go to **Menu > Security > IPv4 Source Guard > IP Source Guard**. An entry should appear in the IP Source Guard Table.

IP Source Guard		Static Binding				
Index	IP Address	VID	MAC Address	Port	Lease	Type
1	192.168.1.30	1	00:0e:c6:ba:ee:6f	11	2d23h59m35s	DHCP-Snooping

- 3 Connect another device using a static IP address in one of the **Switch**'s other access port. In this example, the device will spoof the USG's IP address "192.168.1.1". This device will not be able to communicate with any other device across the **Switch**.

5.7.3 What Could Go Wrong?

- 1 If the devices in the Local Network cannot reach the USG, Make sure that DHCP Snooping is configured on the Switch, first.
- 2 If the devices in the Local Network still cannot reach the USG after configuring and enabling DHCP Snooping, wait for a few minutes before attempting to reach the USG again. ARP Inspection sends the device's MAC address into a filter table. This device must wait until the entry expires, indicated by the "Expiry (sec)" column.

Index	MAC Address	VID	Port	Expiry (sec)
1	bc:cf:4f:b7:44:5f	1	15	170

- 3 If some of the devices are not able to reach the USG, the following problems may have occurred:
 - a. Make sure that the port connected to the USG or other internal devices are trusted ports.
 - b. Make sure that all the clients in the network renews their DHCP configurations incase the Switch has undergone reboot.
 - c. Make sure that the DHCP server's pool has not run out of IP addresses.

5.8 How to Configure the Switch to Protect Against Rogue DHCP Servers

This example will instruct the administrator on how to configure the switch to protect the network from attackers sending false IP configurations to clients. DHCP Snooping blocks DHCP offers coming from an untrusted port. Untrusted ports are usually ports connected to office workstations or publicly accessible jacks.

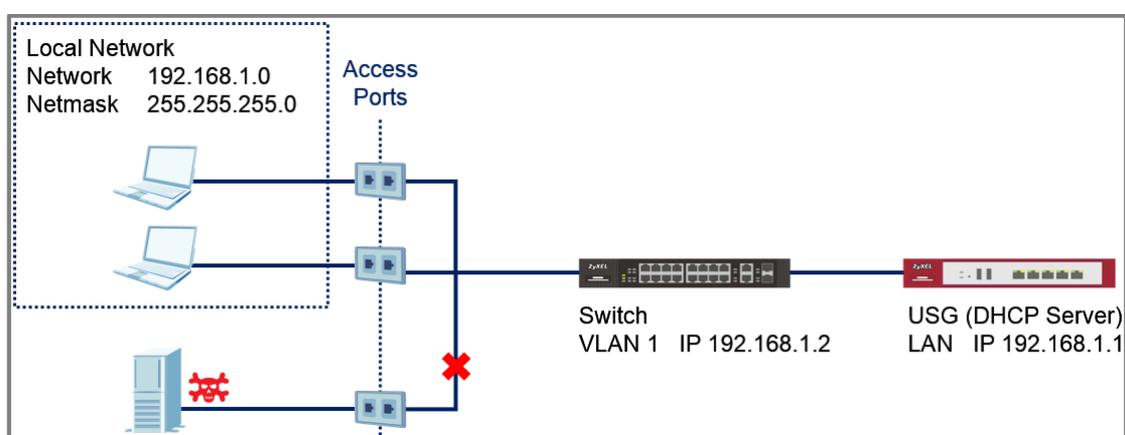


Figure 26 Fake DHCP Server Connected through Publicly Accessible Ports



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. All UI displayed in this article are taken from the XS3800 series switch.

5.8.1 Configuration in the Switch

- 1 Access the **Switch's** Web GUI.
- 2 Go to **Menu > Switching > VLAN > VLAN Setup > Static VLAN**.
For this example, all traffic entering access ports are sent to VLAN 1. Check VLAN 1 and click **Add/Edit**. VLAN 1 should be fixed and untagged for all access ports. Click **Add**.

Active ON

Name

VLAN Group ID

Port	Control			Tagging
*		<input checked="" type="radio"/> Fixed		<input checked="" type="checkbox"/> Tx Tagging
1	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
2	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
3	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
4	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
5	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
6	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
7	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
8	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
9	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
10	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
11	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
28	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
29	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
30	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging

- 3 Go to **Menu > Switching > VLAN > VLAN Setup > VLAN Port Setup**. Configure all access ports with PVID 1. Click **Apply**.

Port	Ingress Check	PVID	Acceptable Frame Type	VLAN Trunking	Isolation
*	<input type="checkbox"/>	<input type="text"/>	All <input type="button" value="v"/>	<input type="checkbox"/>	<input type="checkbox"/>
1	<input type="checkbox"/>	1 <input type="text"/>	All <input type="button" value="v"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	1 <input type="text"/>	All <input type="button" value="v"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	1 <input type="text"/>	All <input type="button" value="v"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	1 <input type="text"/>	All <input type="button" value="v"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>	1 <input type="text"/>	All <input type="button" value="v"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="checkbox"/>	1 <input type="text"/>	All <input type="button" value="v"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	<input type="checkbox"/>	1 <input type="text"/>	All <input type="button" value="v"/>	<input type="checkbox"/>	<input type="checkbox"/>
8	<input type="checkbox"/>	1 <input type="text"/>	All <input type="button" value="v"/>	<input type="checkbox"/>	<input type="checkbox"/>
9	<input type="checkbox"/>	1 <input type="text"/>	All <input type="button" value="v"/>	<input type="checkbox"/>	<input type="checkbox"/>
10	<input type="checkbox"/>	1 <input type="text"/>	All <input type="button" value="v"/>	<input type="checkbox"/>	<input type="checkbox"/>

- 4 Go to **Menu > Security > IPv4 Source Guard > DHCP Snooping > DHCP Snp. Setup**. Enable the Active setting. Click **Apply**.

DHCP Snooping Setup

Active ON

DHCP VLAN Disable

- Go to **Menu > Security > IPv4 Source Guard > DHCP Snooping > DHCP Snp. Port Setup**. Set all access ports as untrusted ports. Ports to the USG or other network components should be trusted ports. Click **Apply**.

Port	Server Trusted State	Rate (pps)
*	Untrusted ▾	<input type="text"/>
1	Untrusted ▾	0 <input type="text"/>
2	Untrusted ▾	0 <input type="text"/>
3	Untrusted ▾	0 <input type="text"/>
4	Untrusted ▾	0 <input type="text"/>
5	Untrusted ▾	0 <input type="text"/>
28	Untrusted ▾	0 <input type="text"/>
29	Untrusted ▾	0 <input type="text"/>
30	Trusted ▾	0 <input type="text"/>

- Go to **Menu > Security > IPv4 Source Guard > DHCP Snooping > DHCP Snp. VLAN Setup**. A list of all active VLANs is displayed on the page. Select **Yes** for the access ports' VLANs. Click **Apply**.

Search VLAN by VID

The Number of VLANs: 5

VID	Enabled	Option 82 Profile
*	No ▾	<input type="text"/>
1	Yes ▾	<input type="text"/>
2	No ▾	<input type="text"/>
3	No ▾	<input type="text"/>
4	No ▾	<input type="text"/>
5	No ▾	<input type="text"/>

Page 1 of 1

5.8.2 Test the Result

- 1** Connect the Rogue-DHCP on one of the access ports.
Create the following DHCP Pool on the LAN interface:
Starting IP Address : 172.16.1.10
End IP Address : 172.16.1.20

- 2** Connect DHCP clients on the other access ports. The clients should only be receiving IP Addresses provided by the USG.

5.8.3 What Could Go Wrong?

- 1 If the DHCP clients in the publicly accessible ports are using IP Addresses provided by the Rogue-DHCP:
 - a. Make sure that all ports connected to publicly accessible ports are an untrusted port in **Menu > Security > IPv4 Source Guard > DHCP Snooping > DHCP Snp. Port Setup**.
 - b. Verify the PVID of the port to this DHCP client. Make sure that DHCP snooping is enabled for that VLAN in **Menu > Security > IPv4 Source Guard > DHCP Snooping > DHCP Snp. VLAN Setup**.
 - c.
- 2 If the DHCP clients in the publicly accessible ports are not able to receive IP Addresses provided by the real DHCP server:
 - a. Make sure that the port to the real DHCP is a trust port in **Menu > Security > IPv4 Source Guard > DHCP Snooping > DHCP Snp. Port Setup**.
 - b. Make sure that both redundant ports are trusted ports in **Menu > Security > IPv4 Source Guard > DHCP Snooping > DHCP Snp. Port Setup** when using a ring topology.

5.9 How to configure IPSG static binding for trusted network devices

This example will instruct the administrator on how to configure the switch to allow an administrator device to use a static IP address on the access port even while ARP Inspection is enabled. This allows the administrator device more freedom and take advantage of IP-specific policies configured on the network while non-administrative devices must still use IP addresses offered by the real DHCP server.

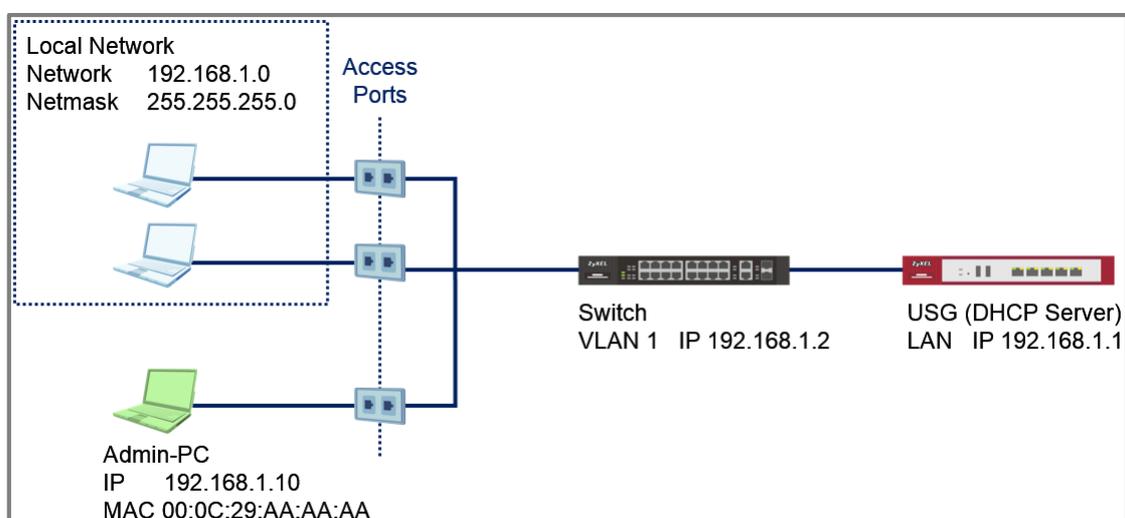


Figure 27 Administrator Device Using a Static IP Address Connected on an Access Port



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. All UI displayed in this article are taken from the XS3800 series switch.

5.9.1 Configuration in the Switch

- 1 Access the **Switch's** Web GUI.
- 2 Configure **ARP Inspection** (Refer to section **5.7.1**).



Note:

DHCP Snooping and ARP Inspection must be enabled when applying Static Binding.

- 3 Go to **Menu > Security > IPv4 Source Guard > IP Source Guard > Static Binding > Add/Edit**. Create a Static Binding entry using your device's MAC address and IP address. Input the VLAN and port that this device is allowed unrestricted access. Click **Apply**.

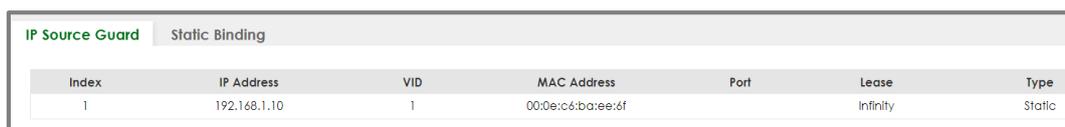
The screenshot shows a configuration form for Static Binding with the following fields and values:

IP Address	<input type="text" value="192.168.1.10"/>
VLAN	<input type="text" value="1"/>
MAC Address	<input type="radio"/> Any <input checked="" type="radio"/> <input type="text" value="00:0e:c6:ba:ee:6f"/>
Port	<input checked="" type="radio"/> Any <input type="radio"/> <input type="text"/>

Buttons: **Apply** (green), **Clear** (grey), **Cancel** (grey)

5.9.2 Test the Result

- 1 Go to **Menu > Security > IPv4 Source Guard > IP Source Guard**. An entry with your device's MAC Address and IP Address should appear with "Static" Type and "Infinity" Lease in the IP Source Guard Table.



Index	IP Address	VID	MAC Address	Port	Lease	Type
1	192.168.1.10	1	00:0e:c6:b0:ee:6f		Infinity	Static

- 2 Configure your Admin-PC with the Static IP address. In this example, we use "192.168.1.10". Connect this to any access port. This PC should be able to reach the USG.
- 3 Configure another random PC with this Static IP address. In this example, we use "192.168.1.10". This random PC should be able to reach the USG (due to a different MAC address).

5.10 How to configure ACL to block unwanted traffic

The example shows administrators how to use ACL to block unwanted traffic. We can set different criteria to identify unwanted traffic. The example will use ACL to prevent only a single host in VLAN 10 from accessing the Server.

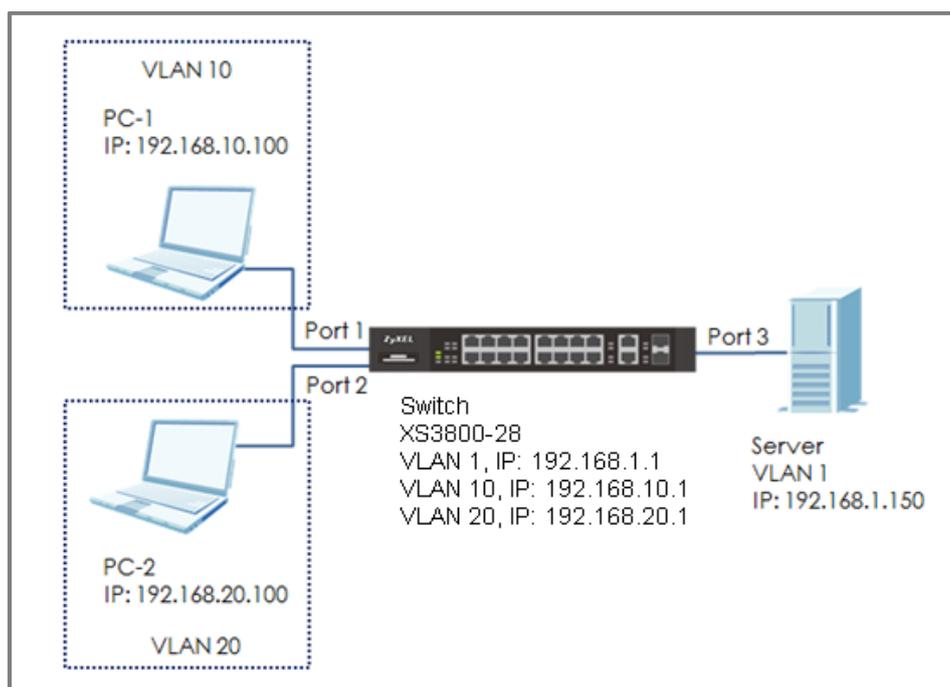


Figure 21 Configure ACL to block unwanted traffic



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 XS3800-28 (Firmware Version: V4.80).

5.10.1 Configure VLAN and Route Traffic

- 1** Configure the VLAN setting (VLAN 10 and VLAN 20) on Switch (Please refer to the topic: **2.1 How to configure the switch to separate traffic between departments**).
- 2** Configure the VLAN IP interfaces on Switch (Please refer to the topic: **2.2 How to configure the switch to route traffic across VLANs**)

5.10.2 Configure the Classifier

- 1 Set up the Classifier: Go to **Menu > Security > ACL > Classifier > Classifier Setup > Add/Edit**. Set up Classifier: For VLAN 20.



Note:

For more details about ACL, please refer to topic: **3.5 How to configure ACL to rate limit VLAN traffic**.

- 2 The Classifier of VLAN 20: Check the “Active” box and key in the classifier Name. Set **Layer 2 > VLAN** as **20** and **Layer 3 > Destination** as **192.168.1.150/32**. Press “Add”.

The screenshot shows the configuration page for an ACL Classifier. The 'Active' toggle is checked. The classifier name is 'VLAN 20'. The weight is set to 32767. Under the 'Ingress Port' section, 'Port' and 'Trunk' are both set to 'Any'. Under 'Layer 2', 'VLAN' is set to 20. Under 'Layer 3', 'Destination IP Address/Prefix' is set to 192.168.1.150/32. The 'Apply' button is highlighted in green.

5.10.3 Configure the Policy Rule

- 1 Set up the **Policy Rule**: Go to **Menu > Security > ACL > Policy Rule > Add/Edit**. The policy rule of VLAN 20: Check the "Active" and key in the Policy Rule Name. Select the Classifier in VLAN 20 (VLAN20). Set up the action to do if match this Classifier: **Action > Forwarding > Discard the packet**. Press "Add".

Source & Destination

Active: ON

Name: Policy VLAN 20

Classifier(s): VLAN20

General Parameters

Vlan ID: 1

Egress Port: 1

Priority: 0

DSCP:

TOS: 0

Metering Parameters

Bandwidth: 0 Kbps

Out of Profile DSCP:

Action

Bandwidth: 0 Kbps

Out of Profile DSCP:

Action

Forwarding: Discard the packet

Priority: No change

Diffserv: No change

Outgoing: Send the packet to the mirror port
 Send the packet to the egress port
 Set the packet's VlanID

Metering: OFF

Out of profile action: Drop the packet
 Change the DSCP value

Apply Clear Cancel

5.10.4 Test the Result

- 1 PC-1 can ping Server successfully.

```
C:\Users\User>ping 192.168.1.150

Pinging 192.168.1.150 with 32 bytes of data:
Reply from 192.168.1.150: bytes=32 time=766ms TTL=128
Reply from 192.168.1.150: bytes=32 time<1ms TTL=128
Reply from 192.168.1.150: bytes=32 time<1ms TTL=128
Reply from 192.168.1.150: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.150:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 766ms, Average = 191ms
```

- 2 Due to the ACL setting, the PC-2 (VLAN 20) cannot ping Server successfully.

```
C:\Users\User>ping 192.168.1.150

Pinging 192.168.1.150 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.150:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

5.10.5 What Could Go Wrong

- 1 When setting up the Classifier, remember to consider both source and destination. In the example, if we only created a policy rule for source VLAN 20, but didn't create the policy rule for destination IP (Server IP: 192.168.1.150), the switch will block all the traffic from VLAN 20 no matter where the destination is.
- 2 Go to **Menu > Security > ACL > Classifier > Classifier Setup**. Check your classifier, click **Add/Edit**, and check "Count". If the traffic matches the classifier, the Match Count for this classifier should be increasing every time the web page refreshes.

Active: ON

Name: VLAN 20

Weight: 32767

Log:

Count: Count

Time Range: None

Ingress Port

Port: Any

Trunk: Any

Layer 2

VLAN: 20

Priority: Any

Ethernet Type: All

Source MAC Address: Any

Destination MAC Address: Any

Layer 3

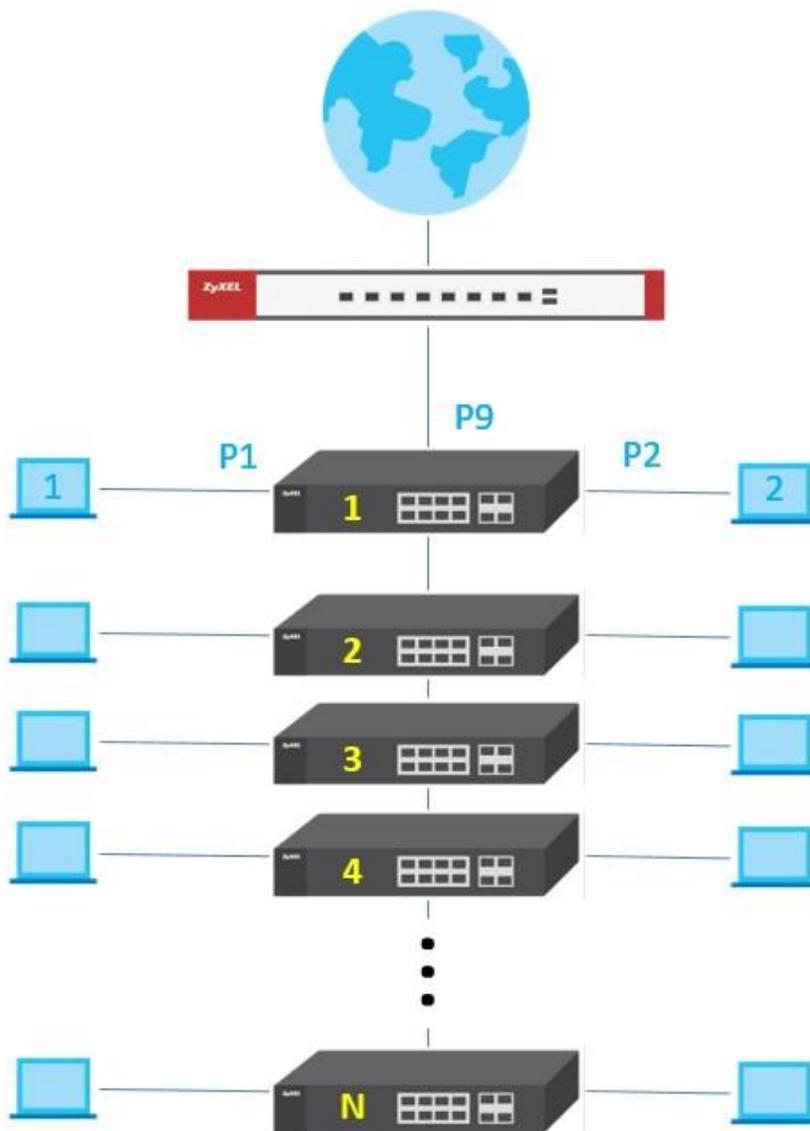
IPv4 DSCP: Any

Index	Active	Weight	Name	Match Count	Rule
1	<input checked="" type="checkbox"/> ON	32767	VLAN 20	20	vlan 20; DestIP = 192.168.1.150/32; count;

5.11 How to use ACL to mirror traffic of a specific criteria

The port mirroring feature allows user to duplicate a traffic flow to the monitor port in order to examine/monitor the traffic from the monitor port without interference. It's useful for troubleshooting or scenarios involving supervisory control.

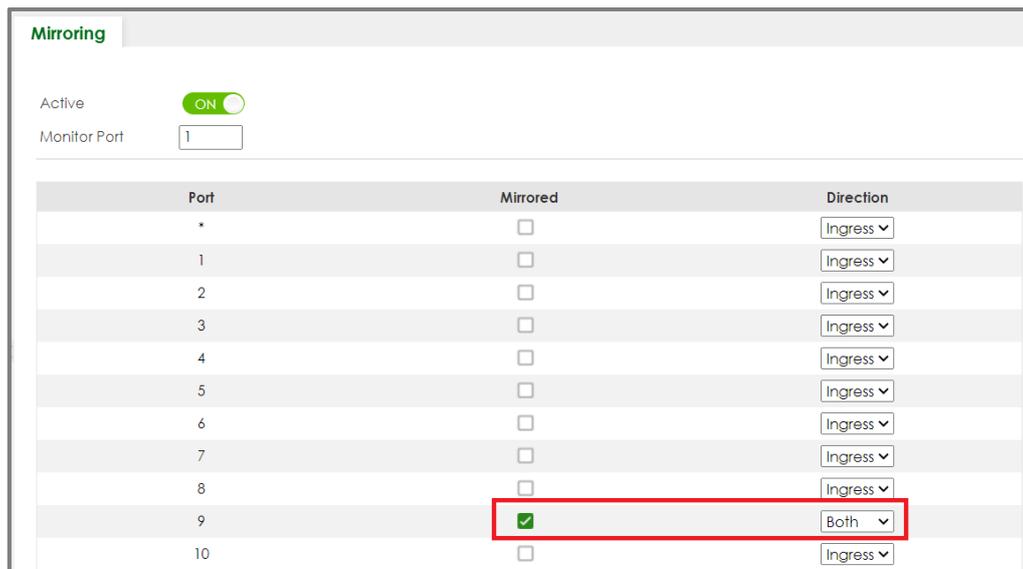
However, there are some cases that monitor port somehow receives numbers of various traffic when mirrored port is the up/down link port between devices. See the example below:



Let's say there are numerous switches and clients under switch 1 in the network.

In case that PC 1 is the monitor PC, and the goal is to monitor the communication between PC2 and the internet.

In general, port 1 will be set as the monitor port and port 9 should be the mirrored port with "both" directions.



The approach is intuitive but it sometimes leads to a large amount of mirrored packets since port 9 of switch 1 is the aggregated uplink port to internet in the topology, all the downlink traffic will be converged. It's inconvenient and troublesome to sort out the particular traffic to/from PC2 among an overload of miscellaneous info in the mirrored traffic.

In the following content, it contains a detailed procedure "filtering" the mirrored packets by implementing ACL mirroring in order to monitor traffic of a specific criteria.

Note:
All network addresses and subnet masks are used as examples in this article. Please replace them with your actual network configuration.

5.11.1 Configuration of ACL

- 1 Access the web GUI of the Switch-1.
- 2 Go to **Menu > Switching > Mirroring > Mirroring**. Activate and set port 1 as the Monitor Port.

Mirroring

Active ON

Monitor Port

Port	Mirrored	Direction
*	<input type="checkbox"/>	Ingress ▾
1	<input type="checkbox"/>	Ingress ▾
2	<input type="checkbox"/>	Ingress ▾
3	<input type="checkbox"/>	Ingress ▾
4	<input type="checkbox"/>	Ingress ▾
5	<input type="checkbox"/>	Ingress ▾
6	<input type="checkbox"/>	Ingress ▾
7	<input type="checkbox"/>	Ingress ▾
8	<input type="checkbox"/>	Ingress ▾
9	<input type="checkbox"/>	Ingress ▾
10	<input type="checkbox"/>	Ingress ▾
11	<input type="checkbox"/>	Ingress ▾
12	<input type="checkbox"/>	Ingress ▾
13	<input type="checkbox"/>	Ingress ▾
14	<input type="checkbox"/>	Ingress ▾

Apply Cancel

- 3 Go to **Menu > Security > ACL > Classifier > Classifier Global Setting**. Set Match Order as “manual”, activate “Logging”, and apply.

Match Order

Logging ON

Interval second(s)

- 4 **Menu > Security > ACL > Classifier > Classifier Setup > Add/Edit**. Activate with name “Source IP”, and Weight 32767. Check “Log”

& "Count". Set Source IP address as PC 2' IP, Address Prefix "32", and then click "Add" to create.

Active ON

Name

Weight

Log

Count

Time Range

Ingress Port

Port Any

Trunk Any

Layer 2

VLAN Any

Priority Any

Ethernet Type All Others (Hex)

Source MAC Address Any MAC/Mask /

Destination MAC Address Any MAC/Mask /

Layer 3

IPv4 DSCP Any

Active ON

Name

Weight

Log

Count

Time Range

Ingress Port

Port Any

Trunk Any

Layer 2

VLAN Any

Priority Any

Ethernet Type All Others (Hex)

Source MAC Address Any MAC/Mask /

Destination MAC Address Any MAC/Mask /

Layer 3

IPv4 DSCP Any

5 Menu > Security > ACL > Classifier > Classifier Setup > Add/Edit.

Activate with name "Destination IP", and Weight 32766. Check "Log" & "Count". Set Destination IP address as PC 2' IP, Address Prefix "32", and then click "Add" to create.

The screenshot shows the 'Classifier Setup' configuration page. The 'Active' toggle is set to 'ON'. The name is 'Destination IP' and the weight is '32766'. 'Log' and 'Count' are checked. The 'Destination IP Address/Prefix' field is set to '192.168.1.50 / 32'. The 'Apply' button is highlighted.

Active	<input checked="" type="radio"/> ON
Name	Destination IP
Weight	32766
Log	<input checked="" type="checkbox"/>
Count	<input checked="" type="checkbox"/>
Time Range	None
Ingress Port	
Port	<input checked="" type="radio"/> Any
Trunk	<input checked="" type="radio"/> Any
Layer 2	
VLAN	<input checked="" type="radio"/> Any
Priority	<input checked="" type="radio"/> Any
Ethernet Type	<input checked="" type="radio"/> All
Source MAC Address	<input checked="" type="radio"/> Any
Destination MAC Address	<input checked="" type="radio"/> Any
Layer 3	
IPv4 DSCP	<input checked="" type="radio"/> Any
IPv6 DSCP	<input checked="" type="radio"/> Any
Source MAC Address	<input checked="" type="radio"/> Any
Destination MAC Address	<input checked="" type="radio"/> Any
Layer 3	
IPv4 DSCP	<input checked="" type="radio"/> Any
IPv6 DSCP	<input checked="" type="radio"/> Any
Precedence	<input checked="" type="radio"/> Any
ToS	<input checked="" type="radio"/> Any
IP Protocol	<input checked="" type="radio"/> All
IPv6 Next Header	<input checked="" type="radio"/> All
Source IP Address/Prefix	
Destination IP Address/Prefix	192.168.1.50 / 32
Layer 4	
Source Socket Number	<input checked="" type="radio"/> Any
Destination Socket Number	<input checked="" type="radio"/> Any

6 Menu > Security > ACL > Policy Rule > Add/Edit.

Activate with name "Mirror". Select both "Source IP" and "Destination IP" for classifiers. Check "Send the packet to the mirror port" for Outgoing Action, and click "Add" to create.

Source & Destination

Active

Name

Classifier(s)

General Parameters

Vlan ID

Egress Port

Priority

DSCP

TOS

Metering Parameters

Bandwidth Kbps

Out of Profile DSCP

Action

Bandwidth Kbps

Out of Profile DSCP

Action

Forwarding No change
 Discard the packet

Priority No change
 Set the packet's 802.1p priority
 Replace the 802.1p priority field with the inner 802.1p priority value

Diffserv No change
 Set the packet's TOS field
 Set the Diffserv Codepoint field in the frame

Outgoing Send the packet to the mirror port
 Send the packet to the egress port
 Set the packet's VlanID

Metering OFF

Out of profile action

Drop the packet
 Change the DSCP value

5.11.2 Test the Result

- 1 Go to **Menu > Security > ACL > Classifier**. The match count number of both classifiers should increase as long as PC 2 is communicating with internet.

Classifier Status						
Index	Active	Weight	Name	Match Count	Rule	
1	ON	32767	Source IP	30	SrcIP = 192.168.1.50/32; count; log;	
2	ON	32766	Destination IP	28	DestIP = 192.168.1.50/32; count; log;	

- 2 Use Wireshark to conduct packet capturing on PC1. The mirrored traffic of PC2 should be included.

Source	Destination	Protocol	Length	VID	Info
192.168.1.50	192.168.1.1	ICMP	74		Echo (ping) request
192.168.1.50	192.168.1.147	ICMP	74		Echo (ping) request
192.168.1.50	192.168.1.147	ICMP	74		Echo (ping) request
192.168.1.147	192.168.1.50	ICMP	74		Echo (ping) reply
192.168.1.147	192.168.1.50	ICMP	74		Echo (ping) reply

5.11.3 What May Go Wrong

- 1 In **Menu > Security > ACL > Policy Rule**, there is the Outgoing Action "Send the packet to the mirror port". The mirror port here stands for the 「**Monitor Port**」 but **NOT** the 「**Mirrored Port**」 in **Menu > Switching > Mirroring > Mirroring**.

Mirroring

Active OFF

Monitor Port

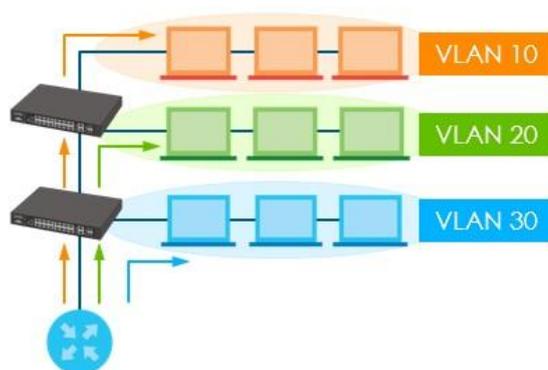
Port	Mirrored	Direction
*	<input type="checkbox"/>	Ingress ▼
1	<input type="checkbox"/>	Ingress ▼
2	<input type="checkbox"/>	Ingress ▼
3	<input type="checkbox"/>	Ingress ▼
4	<input type="checkbox"/>	Ingress ▼
5	<input type="checkbox"/>	Ingress ▼
6	<input type="checkbox"/>	Ingress ▼
7	<input type="checkbox"/>	Ingress ▼
8	<input type="checkbox"/>	Ingress ▼
9	<input type="checkbox"/>	Ingress ▼
10	<input type="checkbox"/>	Ingress ▼
11	<input type="checkbox"/>	Ingress ▼
12	<input type="checkbox"/>	Ingress ▼
13	<input type="checkbox"/>	Ingress ▼
14	<input type="checkbox"/>	Ingress ▼

Apply Cancel

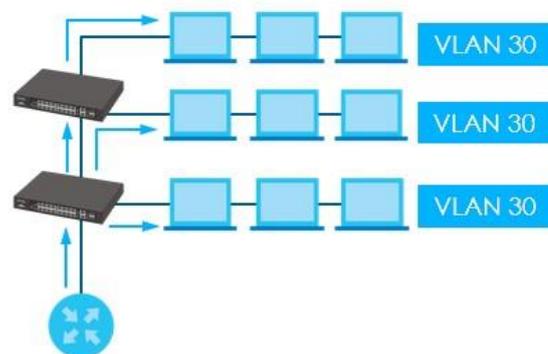
5.12 How to Separate Traffic through L2 Port Isolation

It's a common application that we desire to separate or isolate the mutual traffic between various clients/devices on switches in a network environment.

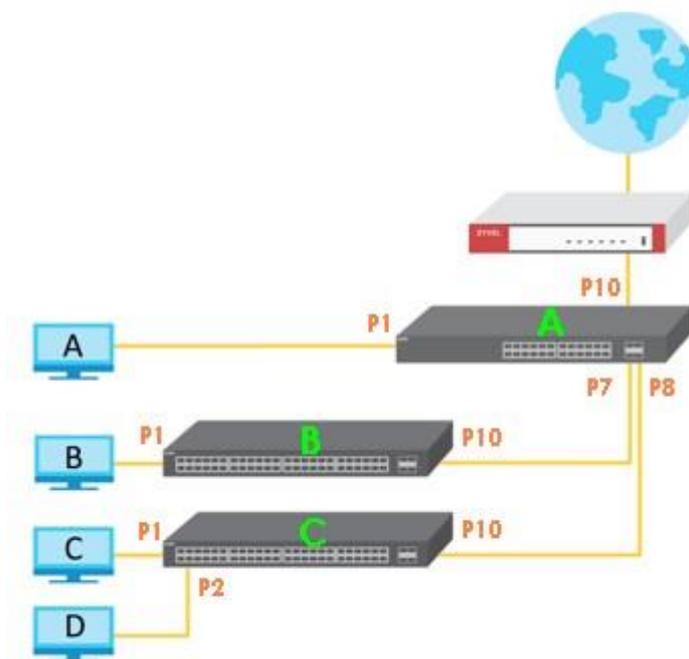
The most intuitive implementation is to create different VLANs to logically segment a LAN into different broadcast domains to achieve the goal.



However, there are certain circumstances that we may want the traffic between clients to be isolated, but yet clients still share the same subnet and VLAN. Let's say in a commercial hotel network, clients in different rooms may belong to the same subnet and VLAN to reach the internet, but there is no way that clients are able to communicate with each other.



On the Zyxel enterprise switch, we can use the feature "Port Isolation" in **Menu > Switching > VLAN > VLAN Setup > VLAN Port Setup** to separate traffic between specific ports despite belonging to the same VLAN.



Name	Device	VLAN	IP Address	Subnet Mask
Gateway	USG FLEX 500	1	192.168.1.254	255.255.255.0
Switch A	XGS2220-30	1	192.168.1.1	255.255.255.0
Switch B	XGS2220-30	1	192.168.1.2	255.255.255.0
Switch C	XGS2220-30	1	192.168.1.3	255.255.255.0
Client A	PC	1	192.168.1.101	255.255.255.0
Client B	PC	1	192.168.1.102	255.255.255.0
Client C	PC	1	192.168.1.103	255.255.255.0
Client D	PC	1	192.168.1.104	255.255.255.0

This is a scenario from customer's issue. All client PCs are in the same subnet and VLAN

By using L2 port isolation on the switches, the goals are:

1. Every PC can surf the internet.
2. Every PC cannot communicate with each other.

In the following content, a step-by-step procedure will be introduced of how to implement L2 port isolation using 3 x XGS2220-30 to achieve the goal.



Note:

All network addresses and subnet masks are used as examples in this article. Please replace them with your actual network configuration.

5.12.1 Configuration in the Switch

- 1 Access Switch C's web GUI.
- 2 Go to **Menu > Switching > VLAN > VLAN Setup > VLAN Port Setup**
Check Port Isolation for port 1 & 2.

Port	Ingress Check	PVID	Acceptable Frame Type	VLAN Trunking	Isolation
*	<input type="checkbox"/>	<input type="text"/>	All <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
1	<input type="checkbox"/>	1 <input type="text"/>	All <input type="text"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2	<input type="checkbox"/>	1 <input type="text"/>	All <input type="text"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3	<input type="checkbox"/>	1 <input type="text"/>	All <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	1 <input type="text"/>	All <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>	1 <input type="text"/>	All <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="checkbox"/>	1 <input type="text"/>	All <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	<input type="checkbox"/>	1 <input type="text"/>	All <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
8	<input type="checkbox"/>	1 <input type="text"/>	All <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
9	<input type="checkbox"/>	1 <input type="text"/>	All <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
10	<input type="checkbox"/>	1 <input type="text"/>	All <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
11	<input type="checkbox"/>	1 <input type="text"/>	All <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>



Note:

If there are multiple clients under switch B, follow the same configuration pattern as Switch C. In this case, it's unnecessary since there's only one client under switch B.

- 3 Access Switch A's web GUI.
- 4 Go to **Menu > Switching > VLAN > VLAN Setup > VLAN Port Setup**
Check Port Isolation for port 1, 7 & 8.

Port	Ingress Check	PVID	Acceptable Frame Type	VLAN Trunking	Isolation
*	<input type="checkbox"/>	<input type="text"/>	All <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
1	<input type="checkbox"/>	1 <input type="text"/>	All <input type="text"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2	<input type="checkbox"/>	1 <input type="text"/>	All <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	1 <input type="text"/>	All <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	1 <input type="text"/>	All <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>	1 <input type="text"/>	All <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="checkbox"/>	1 <input type="text"/>	All <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	<input type="checkbox"/>	1 <input type="text"/>	All <input type="text"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
8	<input type="checkbox"/>	1 <input type="text"/>	All <input type="text"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
9	<input type="checkbox"/>	1 <input type="text"/>	All <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
10	<input type="checkbox"/>	1 <input type="text"/>	All <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
11	<input type="checkbox"/>	1 <input type="text"/>	All <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>

5.12.2 Test the Result

- 1 Client D can ping Gateway and surf the internet.

```
C:\Users\ZT02721>ping 192.168.1.254
                               Gateway
Pinging 192.168.1.254 with 32 bytes of data:
Reply from 192.168.1.254: bytes=32 time=1ms TTL=254

Ping statistics for 192.168.1.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\ZT02721>ping 8.8.8.8
                               Internet
Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=3ms TTL=55

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 3ms, Average = 3ms
```

- 2 Client D cannot communicate with Client A, B, or C.

```
C:\Users\ZT02721>ping 192.168.1.101

Pinging 192.168.1.101 with 32 bytes of data:
Reply from 192.168.1.104: Destination host unreachable.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.101:
    Packets: Sent = 4, Received = 1, Lost = 3 (75% loss),

C:\Users\ZT02721>ping 192.168.1.102

Pinging 192.168.1.102 with 32 bytes of data:
Reply from 192.168.1.104: Destination host unreachable.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.102:
    Packets: Sent = 4, Received = 1, Lost = 3 (75% loss),

C:\Users\ZT02721>ping 192.168.1.103

Pinging 192.168.1.103 with 32 bytes of data:
Reply from 192.168.1.104: Destination host unreachable.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.103:
    Packets: Sent = 4, Received = 1, Lost = 3 (75% loss),
```

5.12.3 What May Go Wrong

- 1 L2 port isolation is port-based but not VLAN-based, that is, as long as particular ports are configured as isolation ports, they cannot communicate with each other no matter in the same VLAN or not.

Implementing VOIP

6.1 How to configure an IP Phone's VLAN using LLDP-MED

The example shows administrators how to use LLDP-MED to configure an IP Phone's VLAN ID. Any IP Phone connected to the switch will be assigned to the certain VLAN based on the switch's port. In the following topic, we will also introduce other ways to send VOIP traffic into a specific (Voice) VLAN. Implementing VOIP allows administrators the option to prioritize Voice traffic during network congestions, thus, preventing poor voice quality or miscommunications between IP Phones.

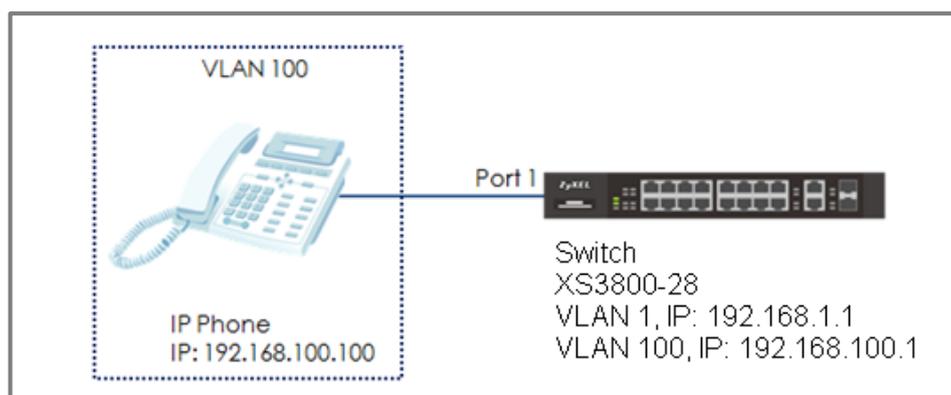


Figure 23 Configure LLDP-MED to assign an IP Phone's VLAN



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 XS3800-28 (Firmware Version: V4.80).

6.1.1 Configure VLAN for IP Phone

- 1 Configure VLAN 100 on Switch (Please refer to the topic: **2.1 How to configure the switch to separate traffic between departments**). VLAN 100 is created for the IP Phone.

6.1.2 Configure Switch

- 1 Enter the web GUI and go to **Menu > Port > LLDP > LLDP > LLDP Setup**. Make sure that the LLDP configuration is active.

Active

Transmit Interval seconds

Transmit Hold times

Transmit Delay seconds

Reinitialize Delay seconds

- 2 Enter web GUI and go to **Menu > Port > LLDP > LLDP MED > LLDP-MED Setup**. Check the “Network Policy” on port 1 (the port that connects to the IP Phone).

Port	Notification		MED TLV Setting	
	Topology Change	Location		Network Policy
*	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>
1	<input type="checkbox"/>	<input type="checkbox"/>		<input checked="" type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>

- 3 Enter the web GUI and go to **Menu > Port > LLDP > LLDP MED > LLDP-MED Network Policy > Add/Edit**. Key in the port number as 1 and the VLAN we want to assign the IP Phone to (VLAN 100) and leave DSCP as “0”. We can also set the Priority. Click “Add”.

Port

Application Type

Tag

VLAN

DSCP

Priority

6.1.3 Test the Result

- 1 Go to **Menu > Monitor > MAC Table > Search**. Check the MAC table. The IP Phone's MAC address should be in VLAN 100.

Index	MAC Address	VID	Port	Type
1	00:15:65:93:81:54	1	1	Dynamic
2	00:15:65:93:81:54	100	1	Dynamic
3	00:19:cb:00:00:01	1	CPU	Static
4	00:19:cb:00:00:01	100	CPU	Static
5	20:d1:60:ff:31:43	1	6	Dynamic
6	f0:76:1c:73:d2:1a	1	14	Dynamic

- 2 Enter the web GUI and go to **Menu > Maintenance > Diagnostic > Ping test**. Use Switch to ping the IP Phone. The switch can ping the IP Phone successfully.

Ping Test

IPv4
 IPv6

IP Address/Host Name:

Source IP Address:

Count:

```
Resolving 192.168.100.100... 192.168.100.100
sent rcvd rate rtt avg mdev max min reply from
1 1 100 4 4 0 4 4 192.168.100.100
2 2 100 1 4 1 4 1 192.168.100.100
3 3 100 1 4 2 4 1 192.168.100.100
```

6.1.4 What Could Go Wrong

- 1 If the MAC address of the IP Phone is not assigned to the VLAN 100 successfully, please check if the IP Phone supports LLDP-MED. LLDP-MED must be enabled on the switch.
- 2 Since the IP Phone is assigned a VLAN ID via the function of the **Network Policy** in LLDP-MED, the voice traffic from the switch must be tagged backed to the IP Phone. Port 1 in VLAN 100 on the Switch should be **tagged out** (Check TX tagging) so that the Switch can ping the IP Phone successfully.
- 3 Since the IP Phone is assigned a VLAN ID via the function of the **Network Policy** in LLDP-MED, please make sure the IP Phone either supports LLDP-MED, or has LLDP-MED enabled.

6.2 How to configure the switch to separate VOIP traffic from data traffic

The example shows administrators how to use Voice VLAN to separate untagged VOIP traffic from untagged data traffic. Unlike traditional VOIP applications, the Voice VLAN feature separates VOIP and data traffic as traffic **reaches the switch**. This means that the VLAN architecture begins on the switch and not on the IP Phones themselves.

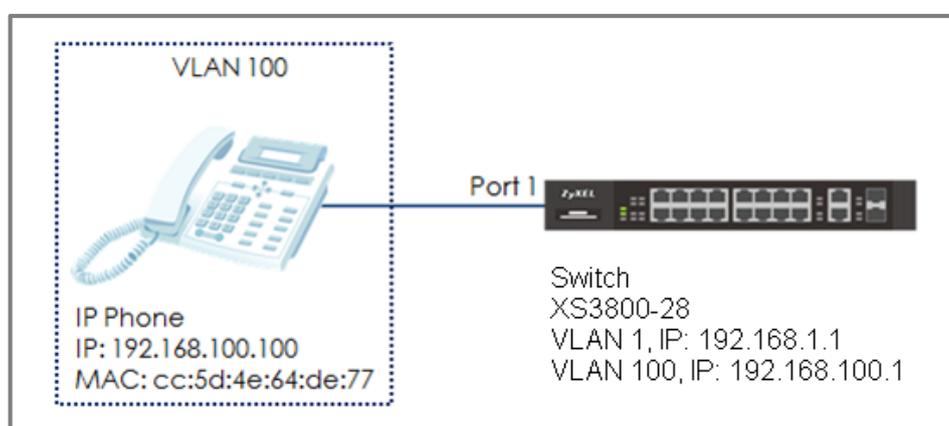


Figure 24 Configure Voice VLAN to separate VOIP traffic from data traffic



Note:

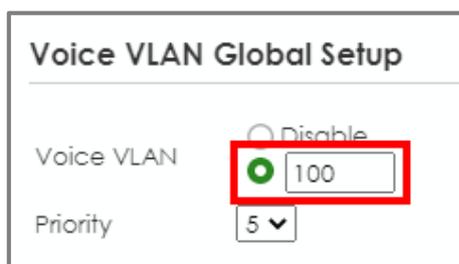
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using XS3800-28 (Firmware Version: V4.80).

6.2.1 Configure VLAN 100 for IP Phone

- 1 Configure VLAN 100 on Switch (Please refer to the topic: **2.1 How to configure the switch to separate traffic between departments**). VLAN 100 is created as the Voice VLAN for the IP Phone.

6.2.2 Configure Voice VLAN

- 1 Enter the web GUI and go to: **Menu > Switching > VLAN > Voice VLAN Setup > Voice VLAN Setup > Voice VLAN Global Setup**. Input the Voice VLAN. In this example, it is VLAN 100. Click “Apply”.



Voice VLAN Global Setup

Disable

Voice VLAN

Priority

- 2 Configure the OUI Setup: Enter the web GUI and go to: **Menu > Switching > VLAN > Voice VLAN Setup > Voice VLAN Setup > Voice VLAN OUI Setup**. Set the OUI address. (You can key in the MAC address.) In this example, it is 00:15:65:93:81:54. Set up the OUI mask as **ff:ff:ff:00:00:00**. Click “Add”.



OUI Address

OUI Mask

Description



Note:

This will instruct the switch to process any traffic from devices with MAC address between 00:15:65:**00:00:00** and cc:5d:4e:**ff:ff:ff** into the Voice VLAN.

6.2.3 Test the Result

- 1 Go to **Menu > Monitor > MAC Table > Search**. Check the MAC address table. The IP Phone is assigned to VLAN 100.

Index	MAC Address	VID	Port	Type
1	00:15:65:93:81:54	1	1	Dynamic
2	00:15:65:93:81:54	100	1	Dynamic
3	00:19:cb:00:00:01	1	CPU	Static
4	00:19:cb:00:00:01	100	CPU	Static
5	20:d1:60:ff:31:43	1	6	Dynamic
6	f0:76:1c:73:d2:1a	1	14	Dynamic

- 2 Enter web GUI and go to **Menu > Maintenance > Diagnostic > Ping test**. Use Switch to ping IP Phone. Switch can ping IP Phone successfully.

Ping Test

IPv4
 IPv6

IP Address/Host Name:

Source IP Address:

Count:

Ping

```

Resolving 192.168.100.100... 192.168.100.100
sent rcvd rate rtt avg mdev max min reply from
1 1 100 4 4 0 4 4 192.168.100.100
2 2 100 1 4 1 4 1 192.168.100.100
3 3 100 1 4 2 4 1 192.168.100.100
    
```

6.2.4 What Could Go Wrong

- 1 If the IP phone is not assigned to the voice VLAN, please verify the MAC address of the IP phone. The MAC address can usually be found on the label or sticker underneath the IP phones. This MAC address must be within the range of the Voice VLAN OUI settings.

- 2 Here are the expected behaviors of IP phones based on the different settings. If you find the behaviors of the IP Phone is not the same as your expectation, please refer below:
 - a. If the IP Phone is VLAN **enabled** and this VLAN is the same as **Voice VLAN**: The Switch will keep the Voice VLAN and assign the priority setting to the IP phone. The IP phone will only recognize the tagged traffic. In this case, port 1 in VLAN 100 on Switch should be set as **tagged out** (check the TX tagging box).
 - b. If the IP Phone is VLAN **enabled** and this VLAN is different from the switch's **Voice VLAN**: The Switch will **not** apply any changes on the VOIP traffic of the IP Phone.
 - c. If the IP Phone is VLAN **disabled**: The Switch will assign the Voice VLAN and priority setting to the IP phone's VOIP traffic. This setting causes the IP Phone to only send and receive **untagged** traffic. In this case, port 1 in VLAN 100 on Switch should be set as **untagged out** (uncheck the TX tagging box).

6.3 How to configure the switch to improve Voice traffic quality

The example shows administrators how to use Voice VLAN to improve Voice traffic. Like the introduction in topic 6.2, Voice VLAN not only groups voice traffic into an assigned VLAN, but also assign the voice traffic a certain priority. Administrators can use this priority to improve Voice traffic quality. The Voice VLAN priority can be applied to both tagged and untagged voice traffic.

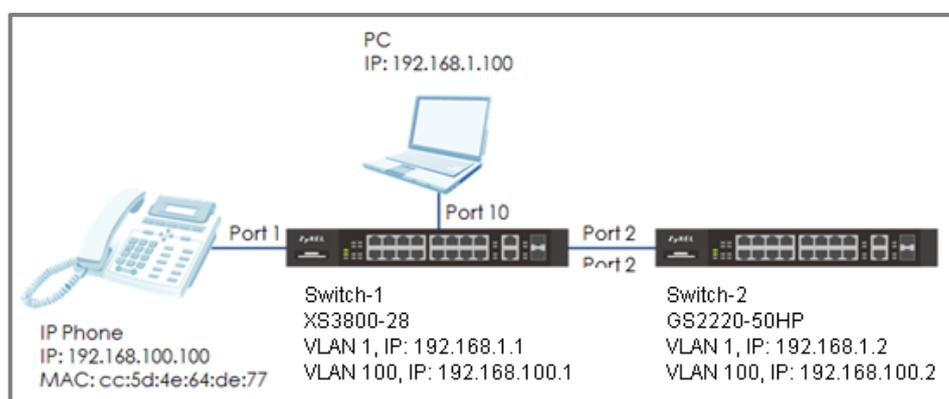


Figure 25 Configure Voice VLAN to separate VOIP traffic from data traffic

 Note:

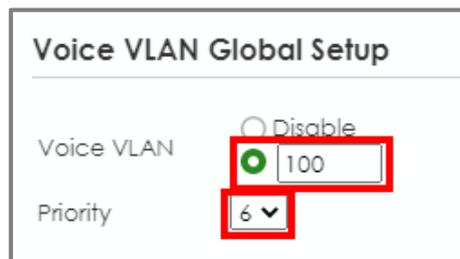
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using XS3800-28 (Firmware Version: V4.80) and GS2220-50HP (Firmware Version: V4.80).

6.3.1 Configure VLAN for voice traffic

- 1 Configure VLAN 100 on Switch-1 and Switch-2. (Please refer to the topic: **2.1 How to configure the switch to separate traffic between departments**). VLAN 100 is created for the Voice VLAN. Make sure that devices in VLAN 100 can communicate across Switch-1 and Switch-2.

6.3.2 Configure Voice VLAN

- 1 Enter the web GUI and go to: **Menu > Switching > VLAN > Voice VLAN Setup > Voice VLAN Setup > Voice VLAN Global Setup**. Key in the Voice VLAN. In this example, it is VLAN 100. Assign a priority to the traffic, for example, priority=6. Click "Add".



Voice VLAN Global Setup

Disable

Voice VLAN

Priority

- 2 Configure the OUI Setup: Enter the web GUI and go to: **Menu > Switching > VLAN > Voice VLAN Setup > Voice VLAN Setup > Voice VLAN OUI Setup**. Set the OUI address. (You can key in the MAC address.) In this example, it is 00:15:65:93:81:54. Set up the OUI mask as **ff:ff:ff:00:00:00**. Click "Add".



OUI Address

OUI Mask

Description



Note:

This will instruct the switch to process any traffic from devices with MAC address between 00:15:65:**00:00:00** and cc:5d:4e:**ff:ff:ff** into the Voice VLAN.

6.3.3 Configure Mirroring (For “Test the Result”)

- 1 To verify that results are acceptable, we have to use the mirroring function to check if the priority of the packet is what we assigned. Enter the web GUI and go to **Menu > Switching > Mirroring > Mirroring**. Check the “Active” box. Key in the Monitor port, which is used to monitor the traffic. Check the port we want to mirror. In this example, it is port 2. Select the direction as “Both”. Click “Apply”.

Active	<input checked="" type="checkbox"/>	
Monitor Port	<input type="text" value="10"/>	
Port	Mirrored	Direction
-	<input type="checkbox"/>	Ingress
1	<input type="checkbox"/>	Ingress
2	<input checked="" type="checkbox"/>	Both
3	<input type="checkbox"/>	Ingress

6.3.4 Test the Result

- 1 Connect the PC and Switch-1. Open **Wireshark** to monitor the packet. Filter "**arp || igmp**".
- 2 Use Switch-2 to ping IP Phone: Enter web GUI and go to **Menu > Management > Diagnostic > Ping test**. Switch-2 can ping IP Phone successfully.
- 3 Check the packet from IP Phone (**192.168.100.100**) on Wireshark. The VLAN header should indicate the assigned Voice VLAN priority "6".

No.	Time	Source	Destination	Protocol	Length	Info
17	1.704977	192.168.100.2	192.168.100.100	ICMP	78	Echo (ping) request id=0x2014
18	1.704980	192.168.100.2	192.168.100.100	ICMP	78	Echo (ping) request id=0x2014
19	1.704982	192.168.100.100	192.168.100.2	ICMP	78	Echo (ping) reply id=0x2014
20	1.704985	192.168.100.2	192.168.100.100	ICMP	78	Echo (ping) request id=0x2014

▶ Frame 19: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
 ▶ Ethernet II, Src: ZyxelCom 64:de:77 (cc:5d:4e:64:de:77), Dst: ZyxelCom_14:97:5c (04:bf:6d:14:97:5c)
 ▲ 802.1Q Virtual LAN, PRI: 6, CFI: 0, ID: 100
 110. = Priority: Voice, < 10ms latency and jitter (6)
 ...0 = CFI: Canonical (0)
 ... 0000 0110 0100 = ID: 100
 Type: IPv4 (0x0800)

6.3.5 What Could Go Wrong

- 1 If the priority is not the same as the setting in voice VLAN, please verify the MAC address of the IP phone. The MAC address can usually be found on the label or sticker underneath the IP phones. This MAC address must be within the range of the Voice VLAN OUI settings

- 2 Here are the expected behaviors of IP phones based on the different settings. If you find the behaviors of the IP Phone is not the same as your expectation, please refer below:
 - a. If the IP Phone is VLAN **enabled** and this VLAN is the same as **Voice VLAN**: The Switch will keep the Voice VLAN and assign the priority setting to the IP phone. The IP phone will only recognize the tagged traffic. In this case, port 1 in VLAN 100 on Switch should be set as **tagged out** (check the TX tagging box).
 - b. If the IP Phone is VLAN **enabled** and this VLAN is different from the switch's **Voice VLAN**: The Switch will **not** apply any changes on the VOIP traffic of the IP Phone.
 - c. If the IP Phone is VLAN **disabled**: The Switch will assign the Voice VLAN and priority setting to the IP phone's VOIP traffic. This setting causes the IP Phone to only send and receive **untagged** traffic. In this case, port 1 in VLAN 100 on Switch should be set as **untagged out** (uncheck the TX tagging box).

- 3 Some computer network cards may not support the 802.1Q (VLAN) information. If you don't see the 802.1Q information in Wireshark, you may need to use a different NIC. We recommend using USB network adapters.