ZYXEL

www.zyxel.com

Switch Series

Zyxel GS1920 / GS2210 / GS2220 / GS3700 /

XGS1930 / XGS2210 / XGS3700 / XGS4600 /

XS1920 / XS1930 / XS3700 / XS3800

Edition 2020.1

Handbook

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

Copyright © 2020 ZyXEL

Contents

Basic principles for network management 8
1.1 How to change the switch management IP address to avoid accessing the wrong device 8
1.1.1 Configuration in the Switch-2 9
1.1.2 Test the Result 11
1.2 How to configure the switch with a device name to avoid accessing the wrong device 12
1.2.1 Configuration in Switch-1 13
1.2.2 Test the Result 14
1.3 How to configure the switch to update the time from an NTP server 15
1.3.1 Configuration in Switch 16
1.3.2 Test the Result 17
1.3.3 What could go wrong? 19
1.4 How to configure the switch to backup events on a SYSLOG server 20
1.4.1 Configure the Switch-1 21
1.4.2 Test the Result 23
1.4.3 What could go wrong? 24
1.5 How to configure the switch with a port name to quickly identify directly connected devices 25
1.5.1 Configure Switch-1 26
1.5.2 Test the Result 27
1.6 How to collect the Diagnostic Info 28
1.6.1 Collect the Diagnostic Info from web GUI 29
1.6.2 Test the Result 30
1.7 How to change the default administrator password 31
1.7.1 Change the default administrator password 32
1.7.2 Test the Result 33
1.8 How to configure a whitelist for remote management to prevent unauthorized access 34
1.8.1 Configure the whitelist of the remote management 35
1.8.2 Test the Result 36

1.8.3 What could go wrong? 37
Designing the Local Area Network 38
2.1 How to configure the switch to separate traffic between departments using VLAN 38
2.1.1 Configure Switch-1 39
2.1.2 Configure Switch-2 42
2.1.3 Test the Result 44
2.2 How to configure the switch to route traffic across VLANs 45
2.2.1 Configure VLAN 10 46
2.2.2 Configure VLAN 20 48
2.2.3 Set the gateway on PC-1 and PC-2 50
2.2.4 Test the Result 52
2.2.5 What could go wrong 53
2.3 How to configure the switch to perform DHCP service in a VLAN 54
2.3.1 Configure VLAN 10 55
2.3.2 Configure VLAN 20 57
2.3.3 Configure the Switch and PC 59
2.3.4 Test the Result 62
2.3.5 What Could Go Wrong 63
2.4 How to Configure the Switch to Translate Customer VLAN to Service Provider VLAN 64
2.4.1 Configuration on the Core Switch 66
2.4.2 Configuration on the Edge Switch 68
2.4.3 Test the Results 70
Improving Network Reliability 73
3.1 How to configure a stacked switch to ensure high server availability 73
3.1.1 Configure Switch-1 and Switch-2 for Stacking 74
3.1.2 Configure Link Aggregation on Stacked switch 76
3.1.3 Configure Link Aggregation on Switch-3 77
3.1.4 Test the Result 78
3.1.5 What Could Go Wrong 79
3.2 How to configure RSTP in a ring topology 80
3.2.1 Configure Switch 81
3.2.2 Test the Result 84
3.2.3 What Could Go Wrong 86

3.3 How to configure VRRP to provide hosts with a redundant gateway 87
3.3.1 Configuration in the Gateway-A 88
3.3.2 Configuration in the Gateway-B 91
3.3.3 Test the Result 94
3.3.4 What Could Go Wrong? 96
3.4 How to configure bandwidth control to limit incoming or outgoing traffic rate 97
3.4.1 Configure Switch 98
3.4.2 Test the Result 99
3.5 How to configure ACL to rate limit IP traffic 100
3.5.1 Configure VLAN and Route Traffic 101
3.5.2 Configure the Classifier 102
3.5.3 Configure the ACL (Policy Rule) 104
3.5.4 Test the Result 106
3.5.5 What Could Go Wrong 108
3.6 How to Implement VRRP with Multiple Routing Interface Combine with HA-pro Using Zyxel Enterprise Switch 109
3.6.1 Configuration 111
3.6.2 Verification 126
3.6.3 What may go wrong? 127
3.7 How to Configure the Switch to Tunnel Layer 2 Protocol Packets Through Service Provider Network 128
3.7.1 Configuration on the Edge Switch 130
3.7.2 Configuration on the Customer Switch 134
3.7.3 Test the Results 136
3.7.4 What Could Go Wrong 137
Designing an IPTV Network 138
4.1 Introduction for IGMP 138
4.1.1 What are General Queries and Group Specific Queries? 138
4.1.2 What are IGMP Snooping Querier Modes? 138
4.1.3 What are the differences between IGMP Snooping fast/normal/immediate leave? 139
4.2 How to configure IGMP routing for multicast clients in a different LAN 140
4.2.1 Configure Switch-1 141

4.2.2 Configure Switch-2 142
4.2.3 Test the Result 143
4.2.4 What Could Go Wrong 144
4.3 How to configure IGMP Snooping for multicast clients in the same LAN 145
4.3.1 Configure Switch 146
4.3.2 Test the Result 147
Network Security 148
5.1 How to configure the port security to limit the number of connected devices 148
5.1.1 Configure Switch-1 149
5.1.2 Test the Result 150
5.1.3 What Could Go Wrong 151
5.2 How to configure MAC filter to block unwanted traffic 152
5.2.1 Configure Switch-1 153
5.2.2 Test the Result 154
5.2.3 What Could Go Wrong 155
5.3 How to configure the switch to prevent IP scanning 156
5.3.1 Configuration in the Switch 157
5.3.2 Test the Result 158
5.3.3 What Could Go Wrong? 161
5.4 How to Configure the Switch and RADIUS Server to Provide Network Access through 802.1x Port Authentication 162
5.4.1 Configuration in the Switch 163
5.4.2 Configuration in the RADIUS-Server 165
5.4.3 Test the Result 166
5.4.4 What May Go Wrong? 170
5.5 How to configure the switch to send unauthorized users in a guest VLAN 171
5.5.1 Configure 802.1x Port Authentication on the Switch 172
5.5.2 Configure VLAN for Guest VLAN 172
5.5.3 Configure Guest VLAN for Failed Authentication 172
5.5.4 Configure the RadiusServer 173
5.5.5 Configure the setting on User-A, User-B and Guest 174
5.5.6 Test the Result 176
5.5.7 What Could Go Wrong 178

5.6 How to Configure the Switch and RADIUS Server to Provide Network Access through Device MAC Address 180
5.6.1 Configuration in the Switch 181
5.6.2 Configuration in the RADIUS-Server 183
5.6.3 Test the Result 184
5.6.4 What Could Go Wrong? 185
5.7 How to configure the switch to prevent ARP spoofing 186
5.7.1 Configuration in the Switch 187
5.7.2 Test the Result 189
5.7.3 What Could Go Wrong? 190
5.8 How to Configure the Switch to Protect Against Rogue DHCP Servers 191
5.8.1 Configuration in the Switch 192
5.8.2 Test the Result 195
5.8.3 What Could Go Wrong? 196
5.9 How to configure IPSG static binding for trusted network devices. 197
5.9.1 Configuration in the Switch 198
5.9.2 Test the Result 199
5.10 How to configure ACL to block unwanted traffic 200
5.10.1 Configure VLAN and Route Traffic 201
5.10.2 Configure the Classifier 202
5.10.3 Configure the Policy Rule 204
5.10.4 Test the Result 205
5.10.5 What Could Go Wrong 206
5.11 How to use ACL to mirror traffic of a specific criteria 207
5.11.1 Configuration of ACL 209
5.11.2 Test the Result 213
5.11.3 What May Go Wrong 214
5.12 How to Separate Traffic through L2 Port Isolation 215
5.12.1 Configuration in the Switch 218
5.12.2 Test the Result 220
5.12.3 What May Go Wrong 222
Implementing VOIP 223
6.1 How to configure an IP Phone's VLAN using LLDP-MED 223
6.1.1 Configure VLAN for IP Phone 224
6.1.2 Configure Switch 225

6.1.3 Test the Result 227
6.1.4 What Could Go Wrong 228
6.2 How to configure the switch to separate VOIP traffic from data traffic 229
6.2.1 Configure VLAN 100 for IP Phone 230
6.2.2 Configure Voice VLAN 231
6.2.3 Test the Result 232
6.2.4 What Could Go Wrong 233
6.3 How to configure the switch to improve Voice traffic quality 234
6.3.1 Configure VLAN for voice traffic 235
6.3.2 Configure Voice VLAN 236
6.3.3 Configure Mirroring (For "Test the Result") 237
6.3.4 Test the Result 238
6.3.5 What Could Go Wrong 239
6.4 How to Configure Voice VLAN on Zyxel Switch 240
6.4.1 Configuration 241
6.4.2 Test the result 244
6.4.3 What Could Go Wrong 245

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.

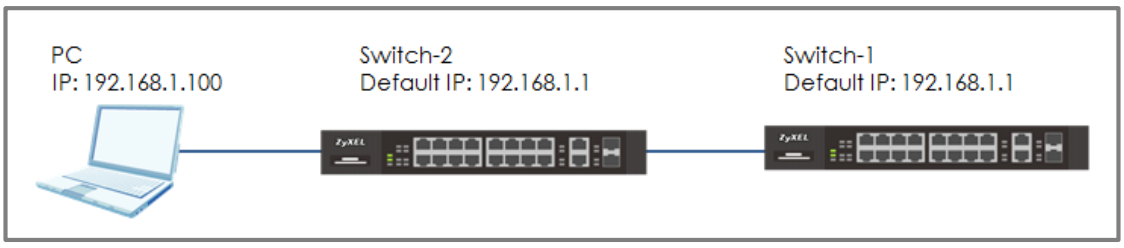


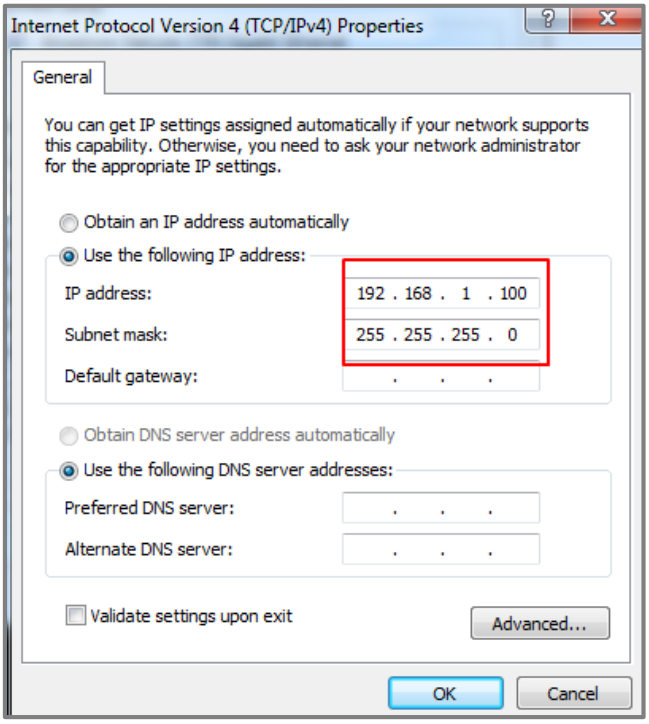
Figure 1 Two switches are using the same default IP address

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 XGS4600-32 (Firmware Version: V4.50).

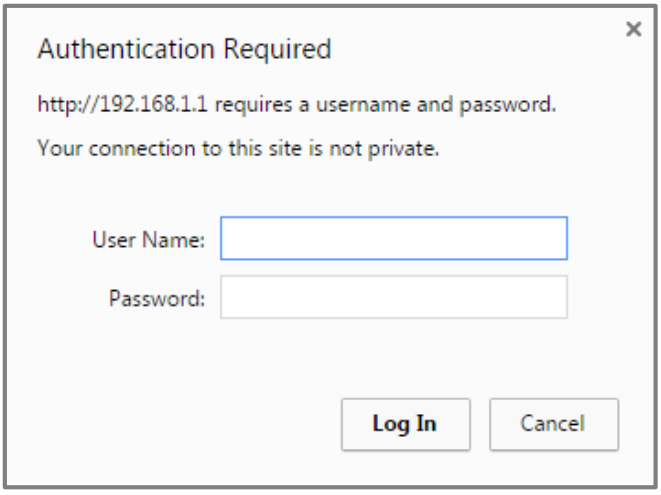
1.1.1 Configuration in the Switch-2

1 Disconnect the link between Switch-1 and Switch-2.

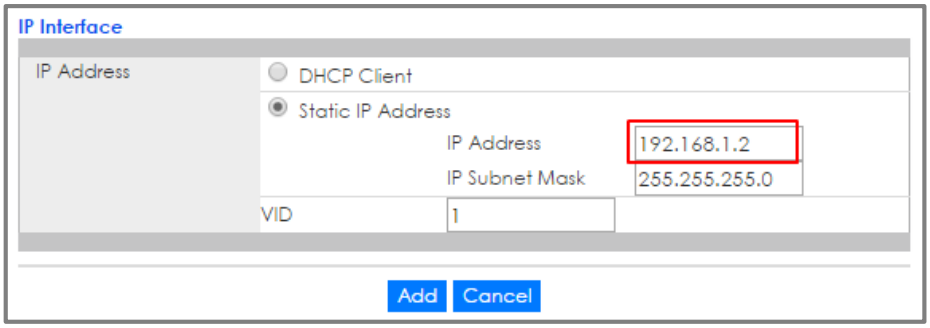
2 Set the PC's IP address on to the same subnet as the switches. For example, set the PC IP address as **192.168.1.100**.



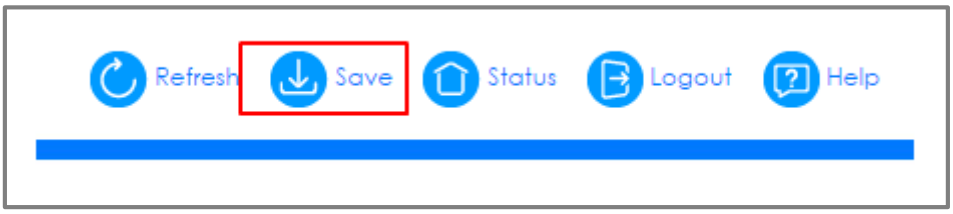
3 Open a browser (IE, Chrome, Safari, Firefox, etc.…). Go to website **http://192.168.1.1** (default management IP address). Key in "**username: admin**; **password: 1234**" and log in.



4 Enter the webpage and go to **Menu > Basic Setting > IP Setup > IP Configuration**. Set the IP address you prefer, for example **192.168.1.2**. Then click **Add**.

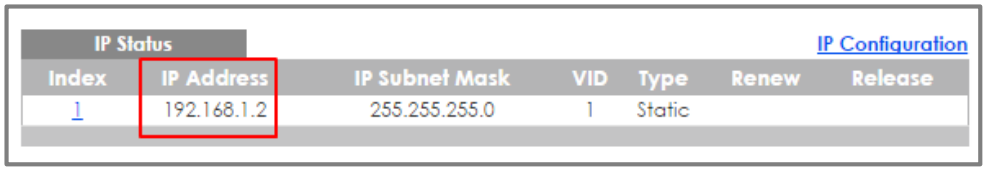


5 Log back in using the new IP address **192.168.1.2**. After logging in again, remember to click the **Save** icon to save the new configurations.



1.1.2 Test the Result

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



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 (XGS4600 in this example).

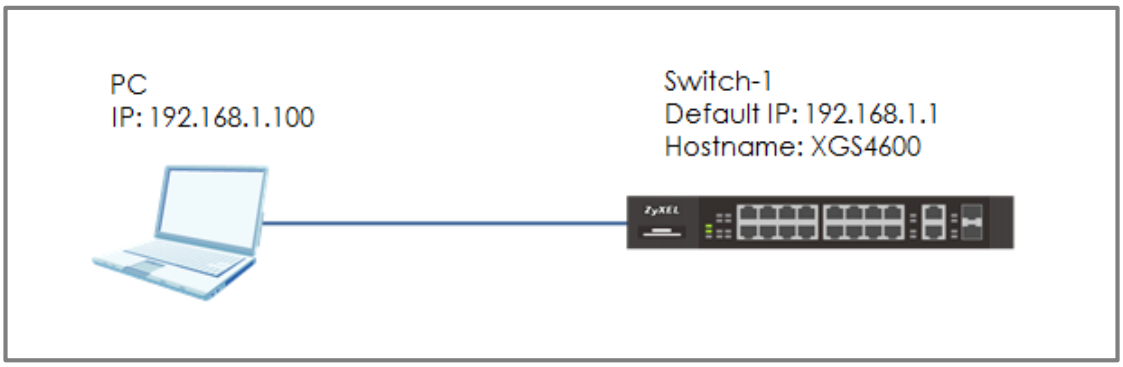
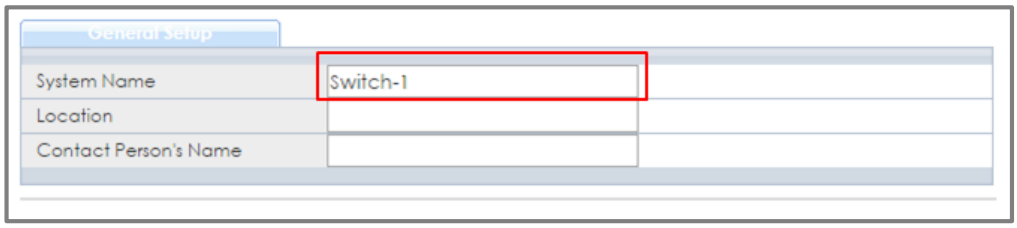


Figure 2 Change the device name of the switch

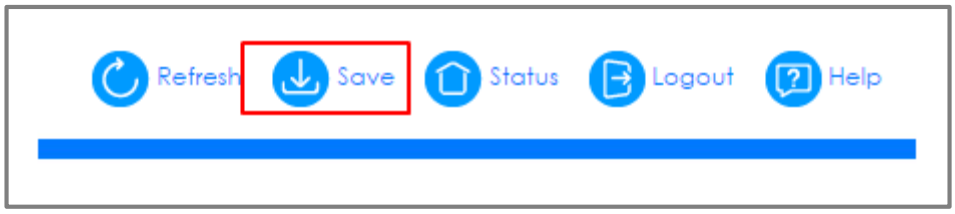
Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using XGS4600-32 (Firmware Version: V4.50).

1.2.1 Configuration in Switch-1

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

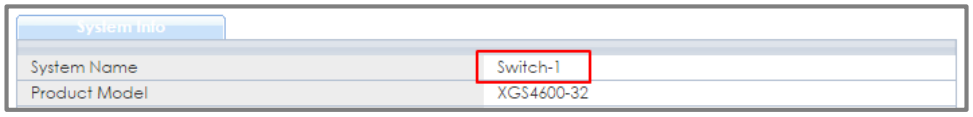


2 Click "**Save**" to save the configuration.



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.



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.

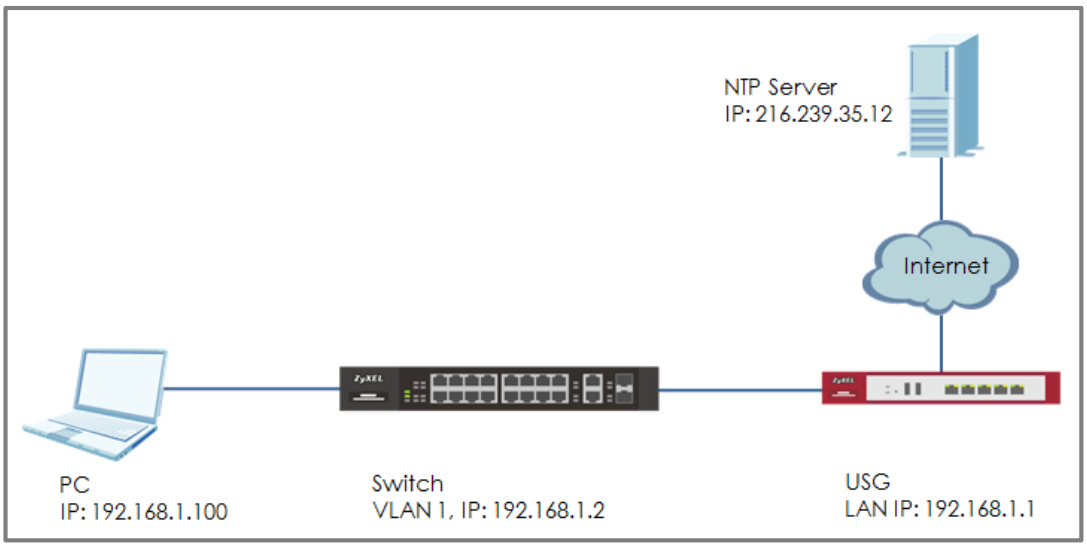
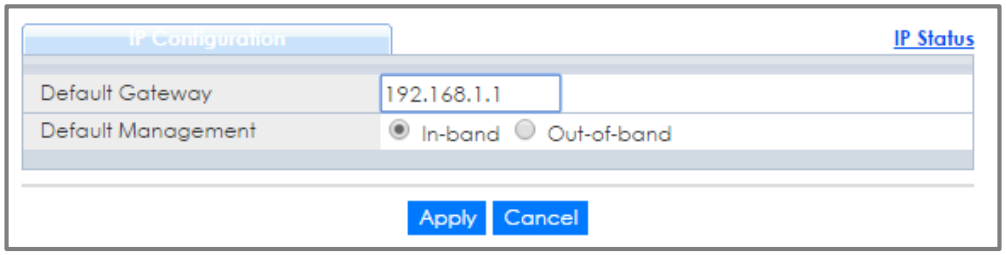


Figure 3 Set up Switch to get time from NTP Server

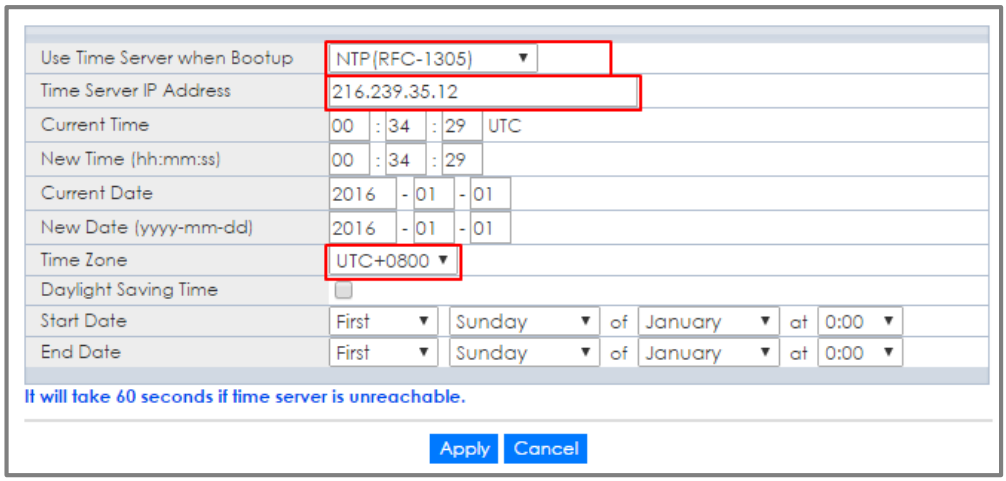
Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using XGS4600-32 (Firmware Version: V4.50). We use google free public NTP server (216.239.35.12) to be our NTP server. 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

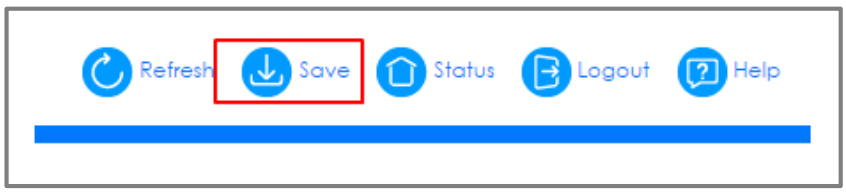
1 Enter the web GUI and go to **Menu > Basic Setting > IP Setup > IP Configuration**. Set the default Gateway as USG IP: **192.168.1.1**. Then click "**Apply**".



2 Go to **Menu > Basic Setting > 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**".

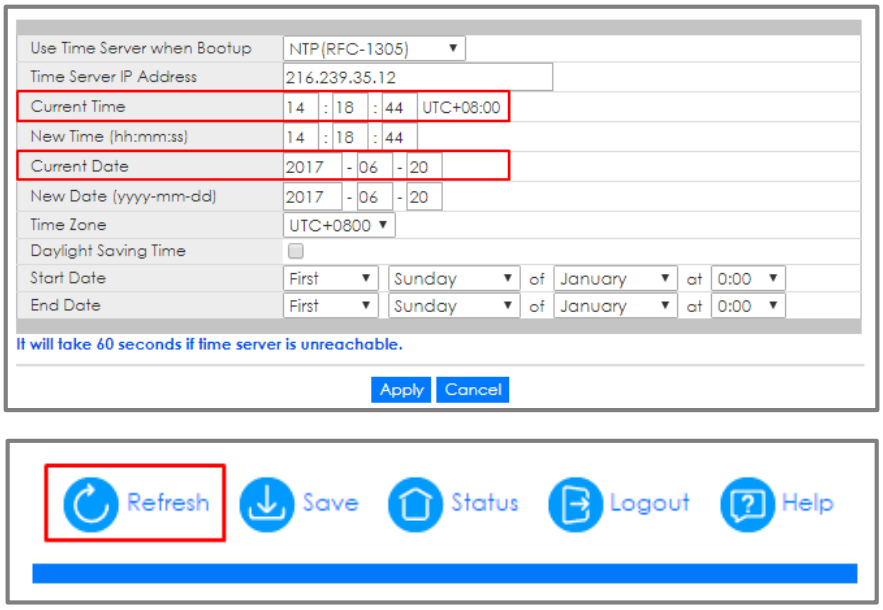


3 Click **Save** to save the configuration.

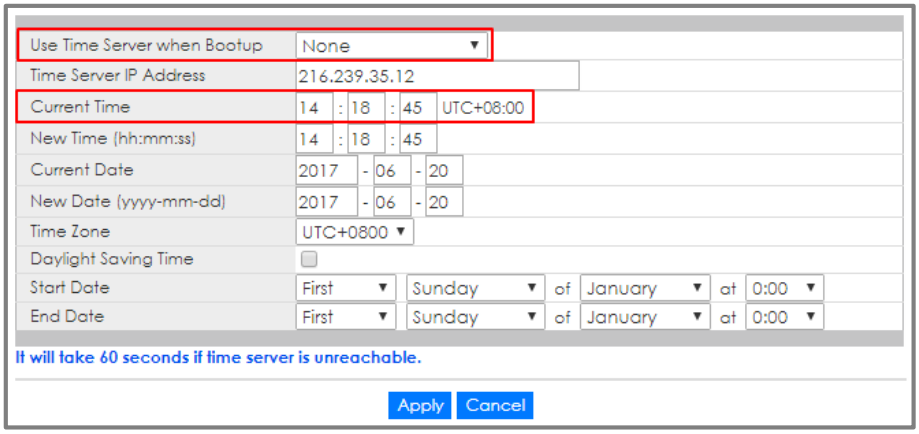


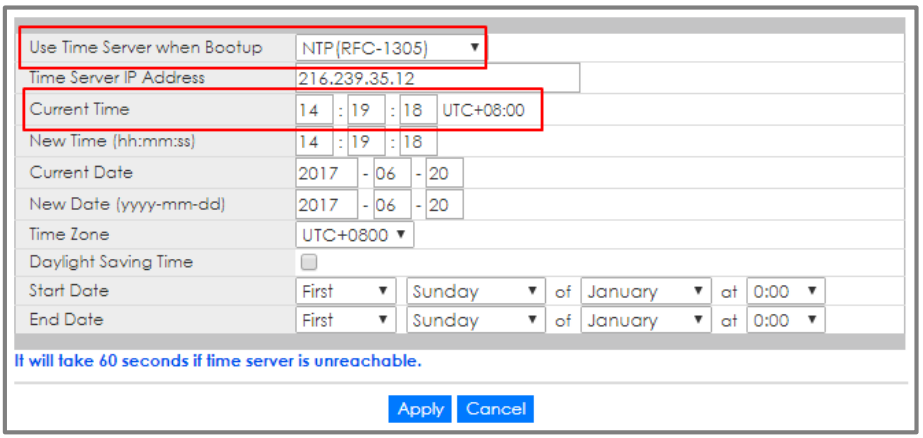
1.3.2 Test the Result

1 Go to **Menu > Basic Setting > 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**".



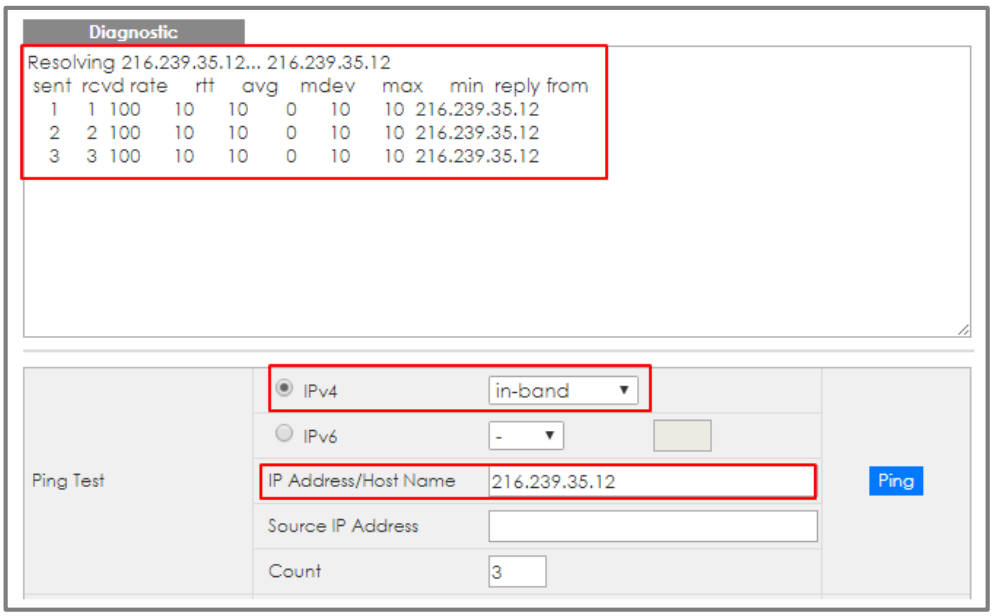
2 Try to select the "User Time Server when Bootup" as **None**. Few second later, change back to **NTP(RFC-1305)**. The time will still update to the current time.




Use Time Server when Bootup
NTP(RFC-1305)
Time Server IP Address
216.239.35.12
Current Time
14 : 19 : 18 UTC+08:00
New Time (hh:mm:ss)
14 : 19 : 18
Current Date
2017 - 06 - 20
New Date (yyyy-mm-dd)
2017 - 06 - 20
Time Zone
UTC+0800
Daylight Saving Time
Start Date
First Sunday of January at 0:00
End Date
First Sunday of January at 0:00
It will take 60 seconds if time server is unreachable.
Apply
Cancel

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 > Management > Diagnostic**. Select IPv4 as **in-band** and type the IP address of NTP Server (216.239.35.12) into the IP Address field. Click "**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.

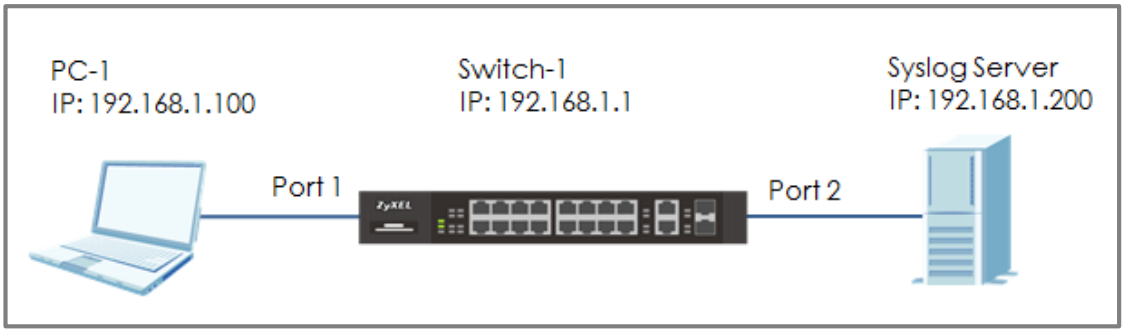
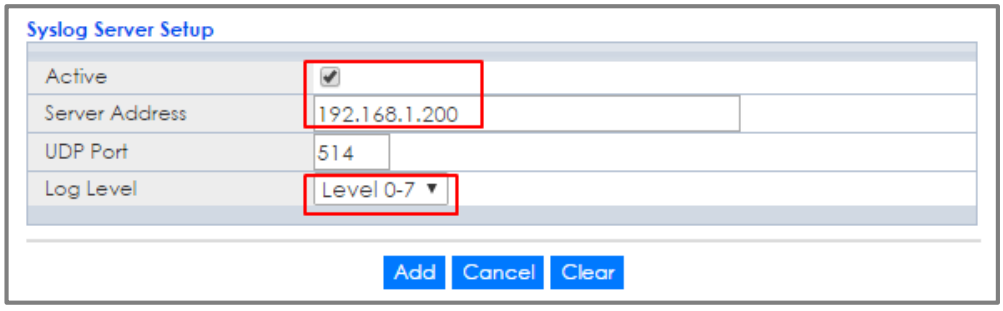


Figure 4 Upload the syslog automatically to the server

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 XGS4600-32 (Firmware Version: V4.50).

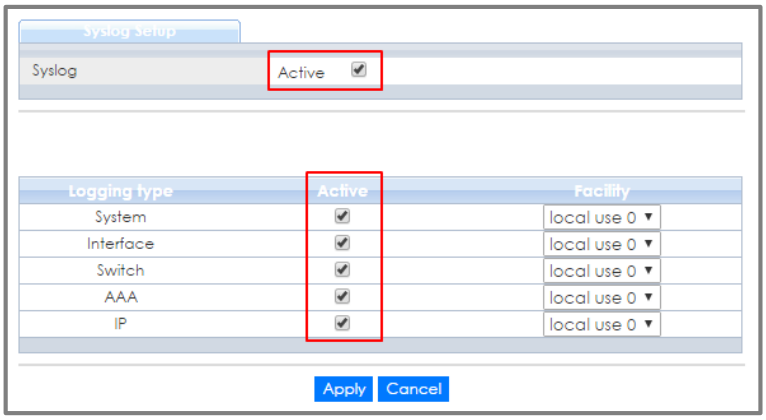
1.4.1 Configure the Switch-1

1 Enter the web GUI and go to **Menu > Management > Syslog Setup > Syslog Server Setup**. **Activate** the syslog server setup 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 "**Add**".

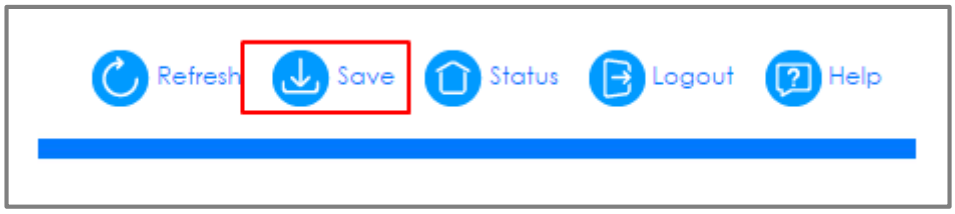


Note:
Log Level refers to which events should be sent to the Syslog Server. Severity: Emergency (0), Alert (1), Critical (2), Error (3), Warning (4), Notice (5), Informational (6), and Debug (7).

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



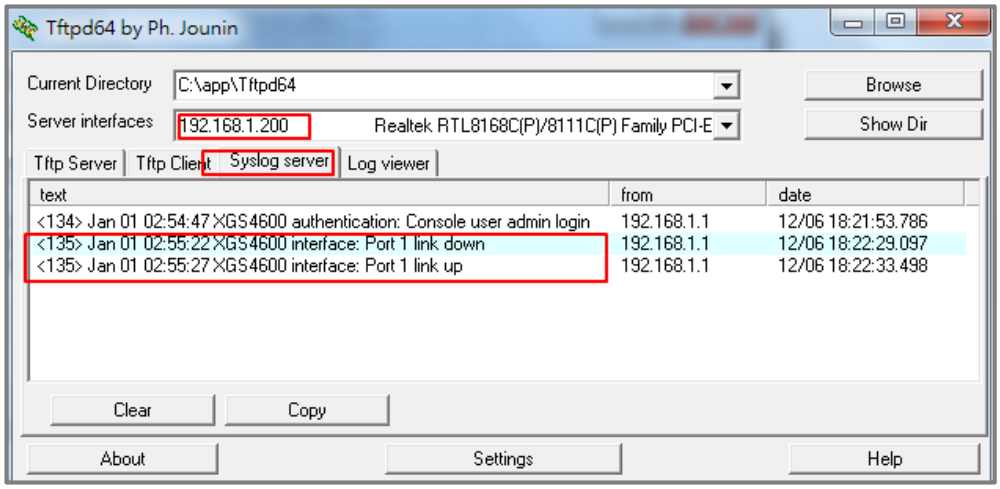
3 Click **Save** to save the configuration.



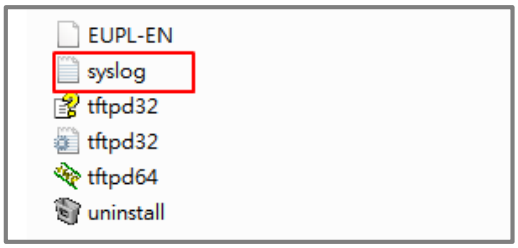
1.4.2 Test the Result

1 Unplug and re-plug PC-1 from the switch.

2 The Syslog Server should receive an event log from the switch.



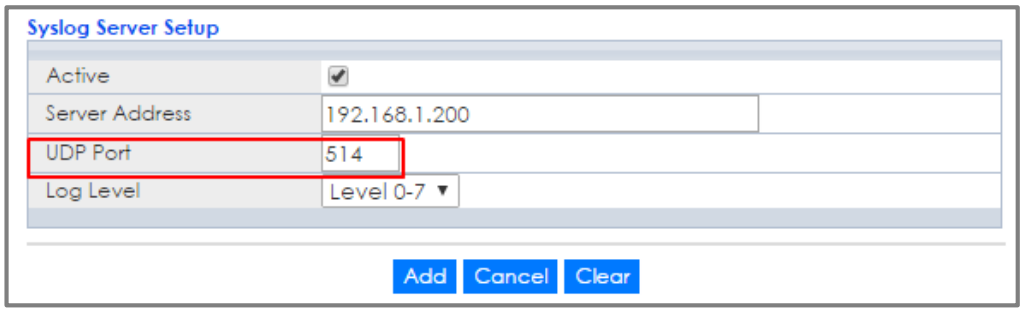
3 We can also check the **directory** ("C:\app\Tftpd64" in this example) to find out if a text file is created on the Syslog Server.



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**).



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 and quickly identify which port connects to which device, location, or section of the network.

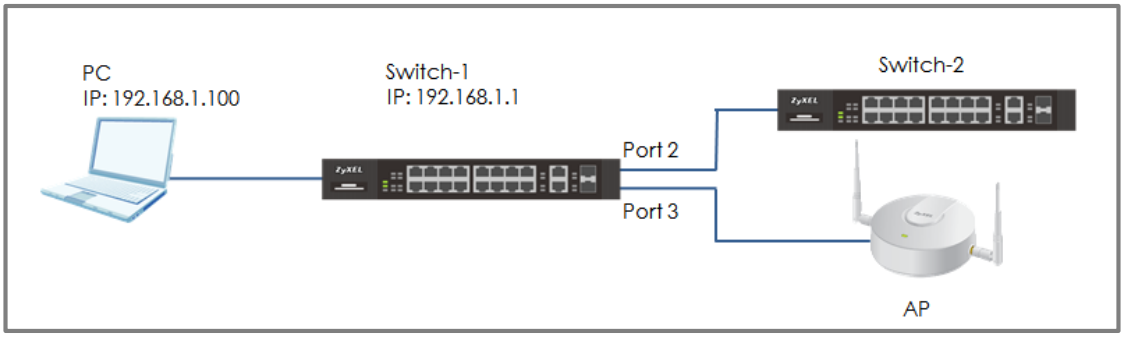
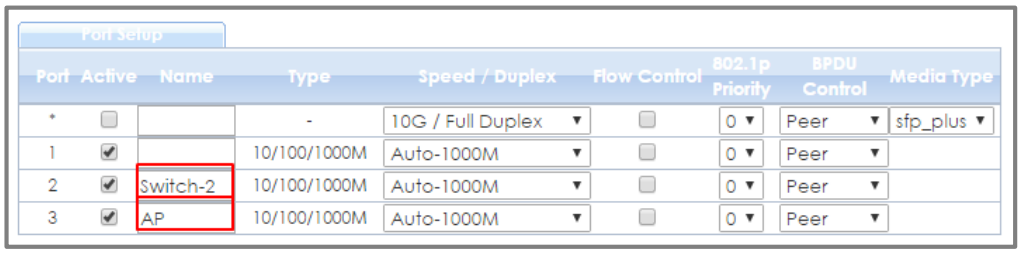


Figure 5 Configure the port name of the switch

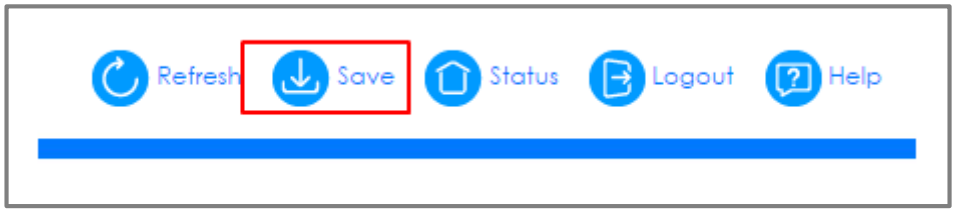
Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using XGS4600-32 (Firmware Version: V4.50).

1.5.1 Configure Switch-1

1 Enter the web GUI and go to **Menu > Basic Setting > 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**".

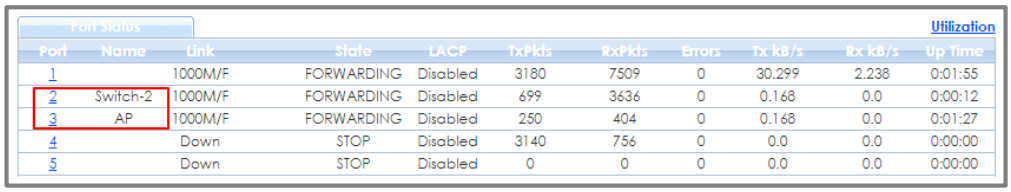


2 Click **Save** to save the configuration.



1.5.2 Test the Result

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



Port Status

Utilization

Port	Name	Link	State	LACP	TxPkts	RxPkts	Errors	Tx kB/s	Rx kB/s	Up Time
1		1000M/F	FORWARDING	Disabled	3180	7509	0	30.299	2.238	0:01:55
2	Switch-2	1000M/F	FORWARDING	Disabled	699	3636	0	0.168	0.0	0:00:12
3	AP	1000M/F	FORWARDING	Disabled	250	404	0	0.168	0.0	0:01:27
4		Down	STOP	Disabled	3140	756	0	0.0	0.0	0:00:00
5		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00

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.

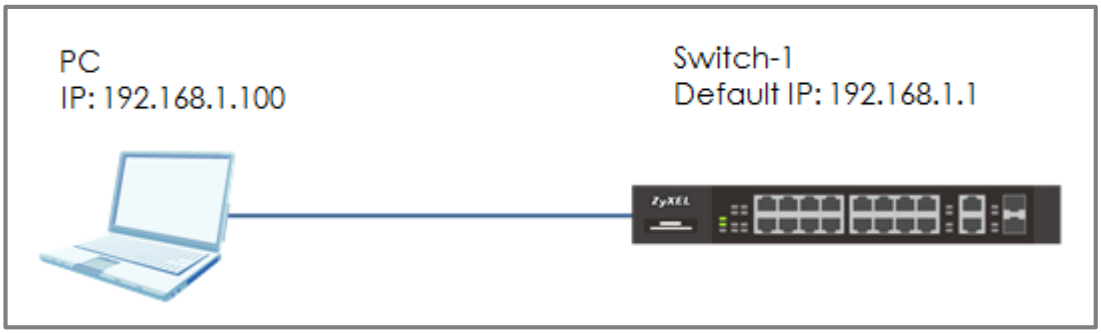
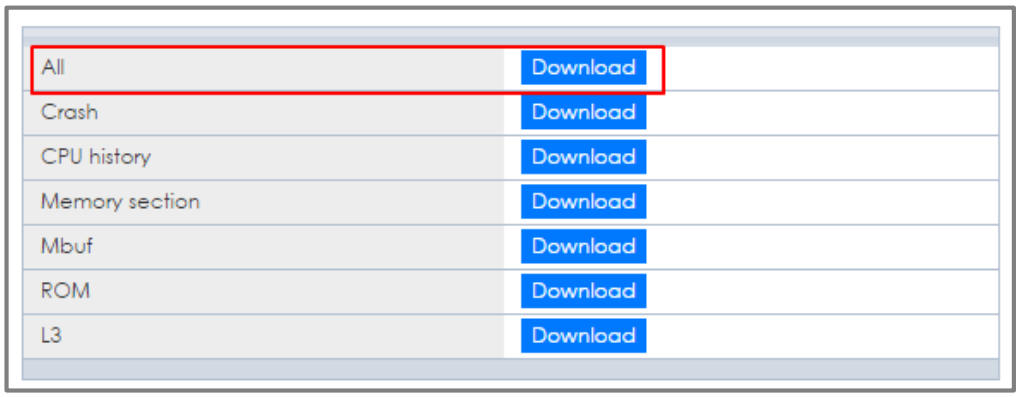


Figure 6 Collect the Diagnostic Info from web GUI

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 XGS4600-32 (Firmware Version: V4.50).

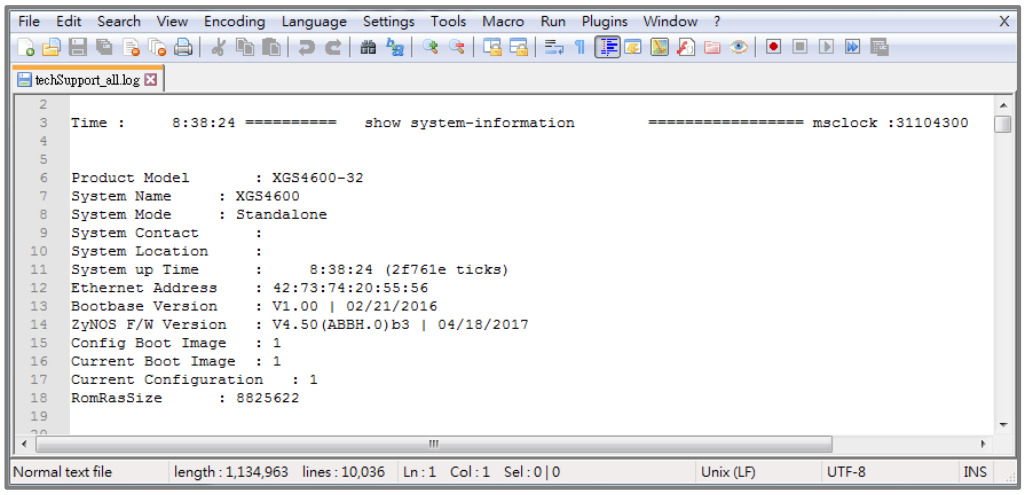
1.6.1 Collect the Diagnostic Info from web GUI

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



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.)



1.7 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.

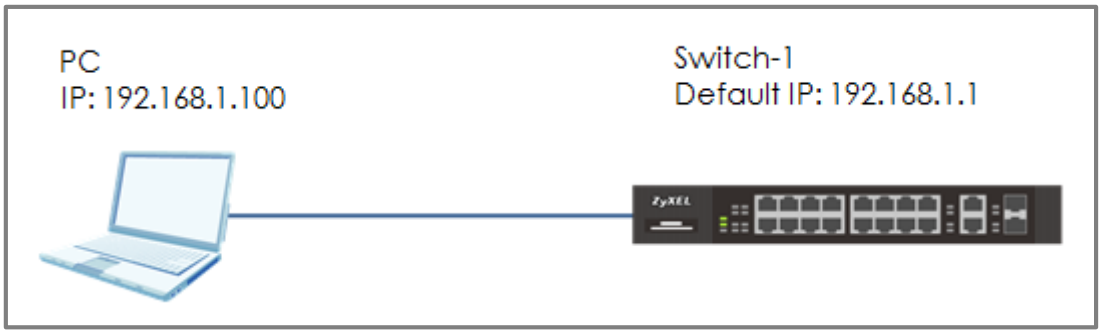
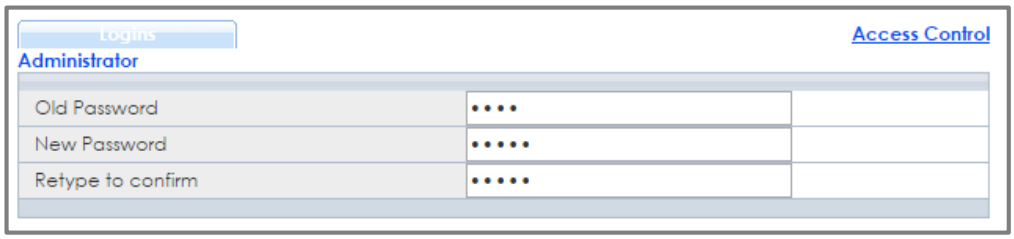


Figure 7 Change the default administrator password

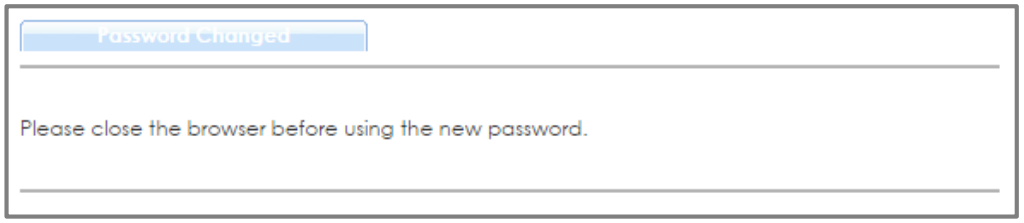
Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using XGS4600-32 (Firmware Version: V4.50).

1.7.1 Change the default administrator password

1 Enter the web GUI and go to **Menu > Management > Access Control > Logins >** **Click Here**. Enter the Old Password and New Password. Then click "**Apply**".

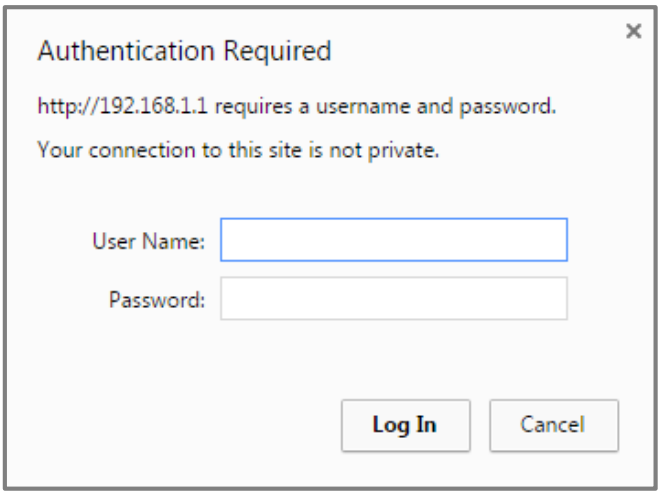


2 After clicking the "**Apply**", the browser will show a message similar below.



1.7.2 Test the Result

1 Close the web GUI and login again with the **OLD** password. The "Authentication Required" window will pop up again.



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…..).

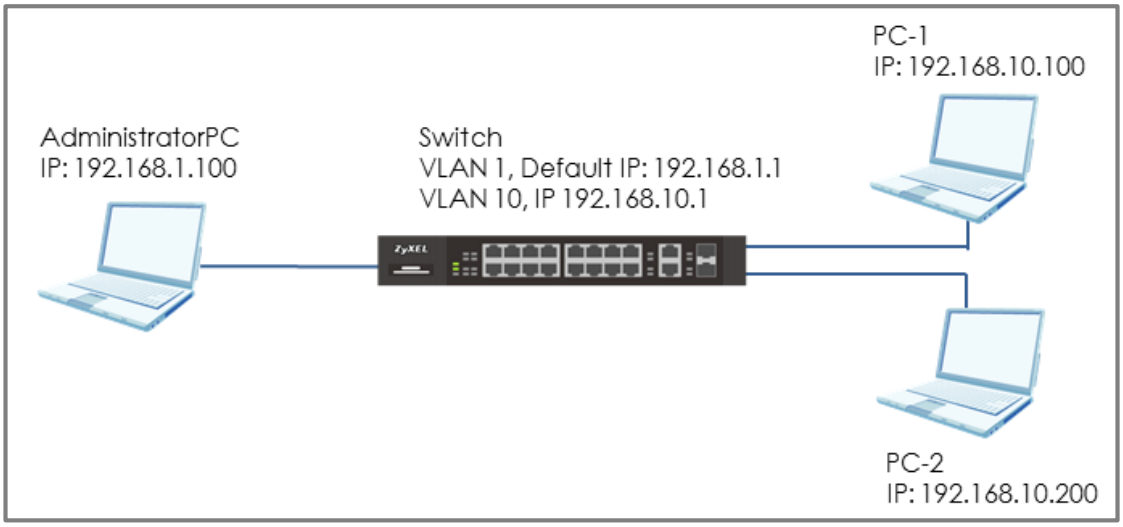
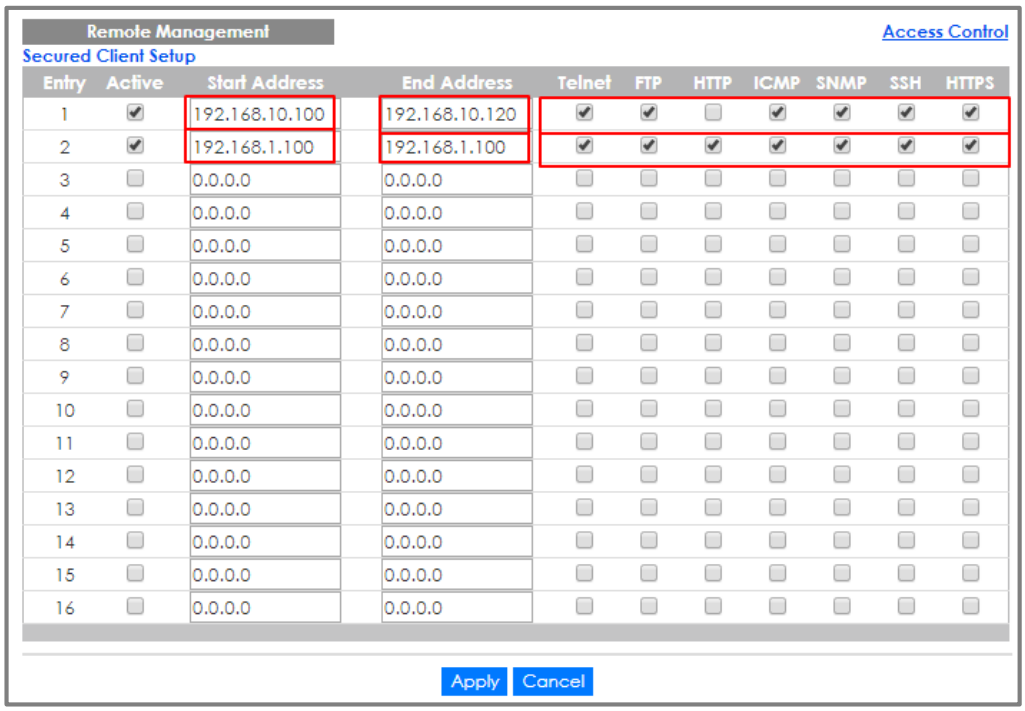


Figure 8 Configure the whitelist for remote management

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 XGS4600-32 (Firmware Version: V4.50).

1.8.1 Configure the whitelist of the remote management

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



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.

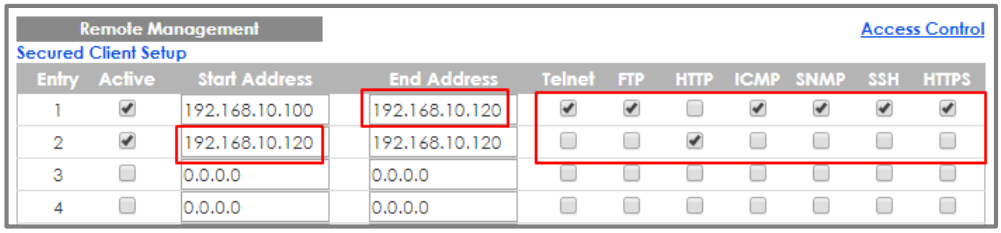
2 The PC-2 (192.168.10.200) is not in the range which is allowed to access the Switch. PC-2 cannot access or ping the switch's management IP address.

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

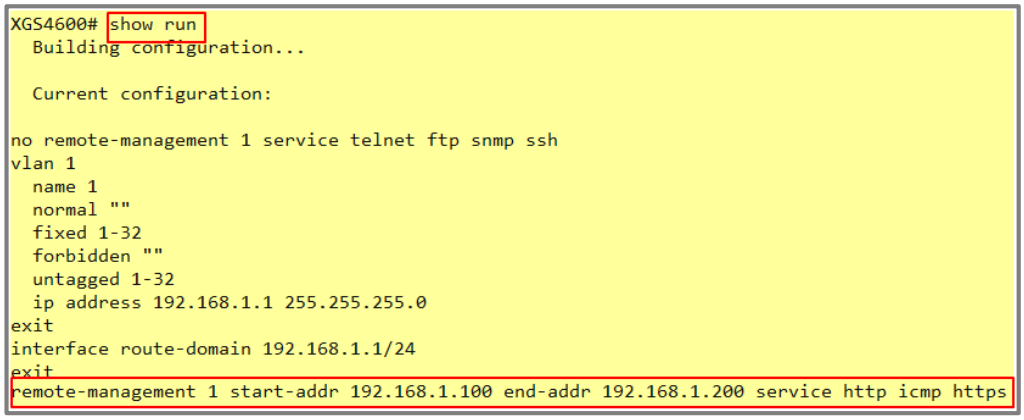
1.8.3 What could go wrong?

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 accidently. The result is that all types of services are **ALLOWED** for **192.168.10.120**.



2 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.



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.

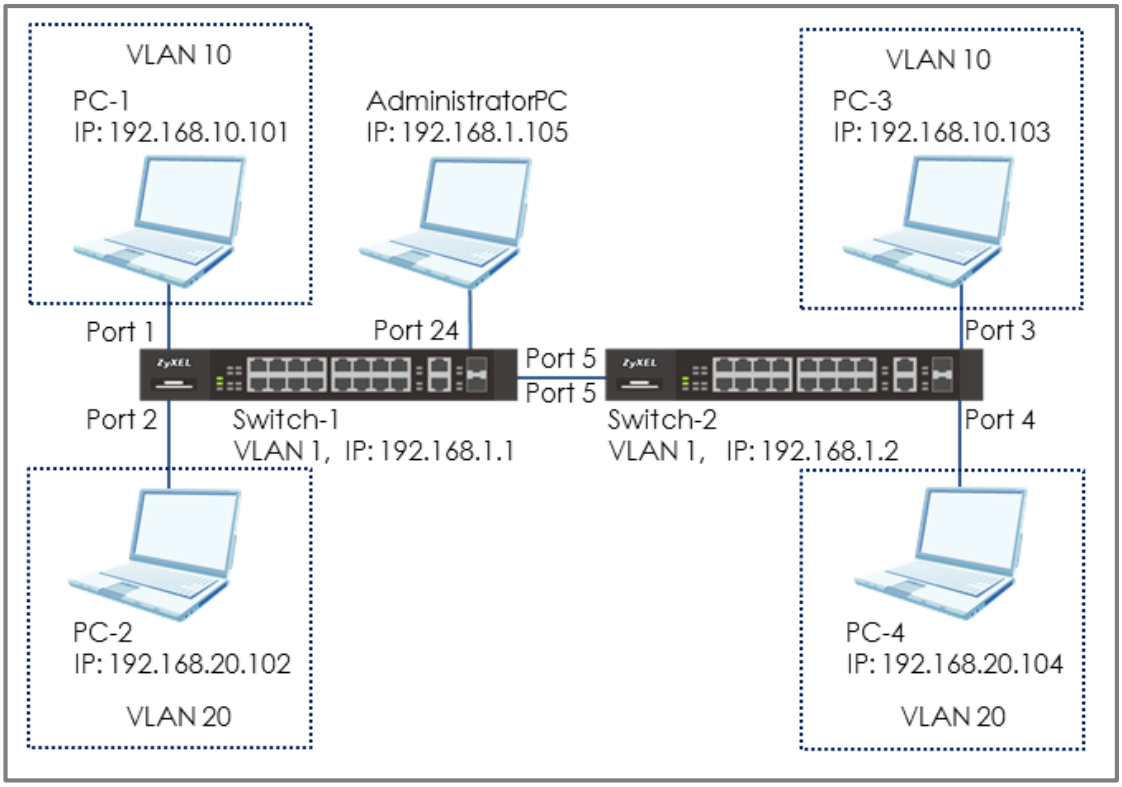
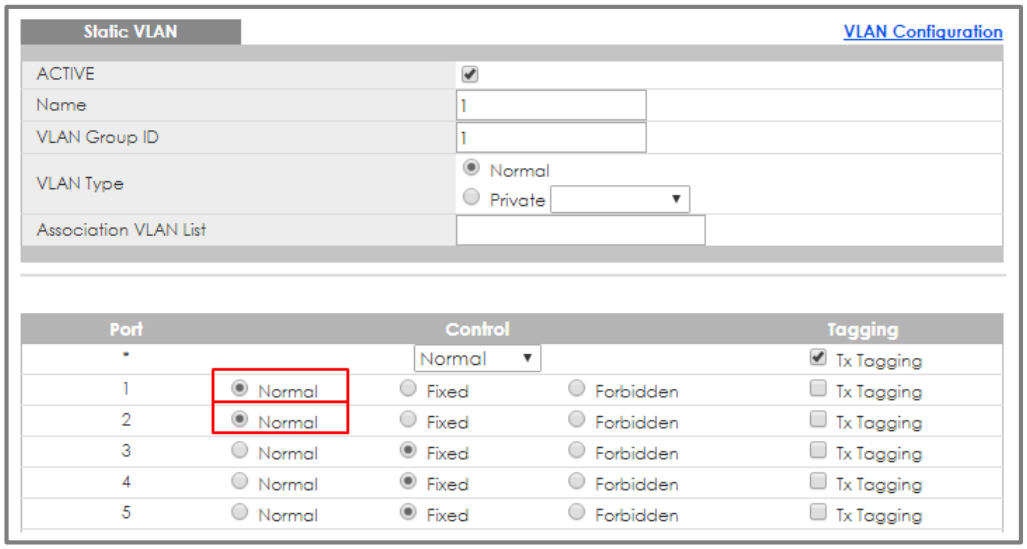


Figure 9 Set up VLAN to separate the traffic between departments

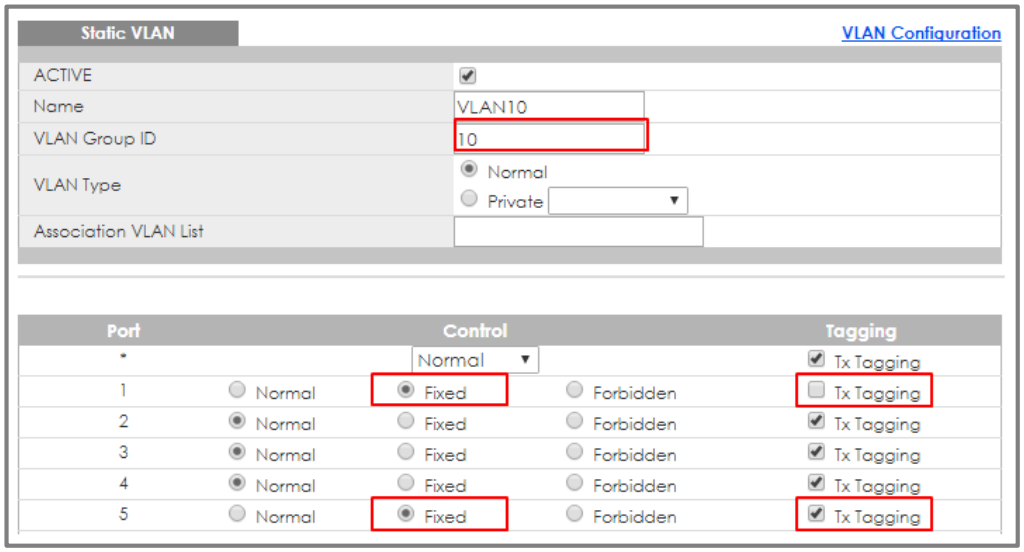
Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using XGS4600-32 (Firmware Version: V4.50).

2.1.1 Configure Switch-1

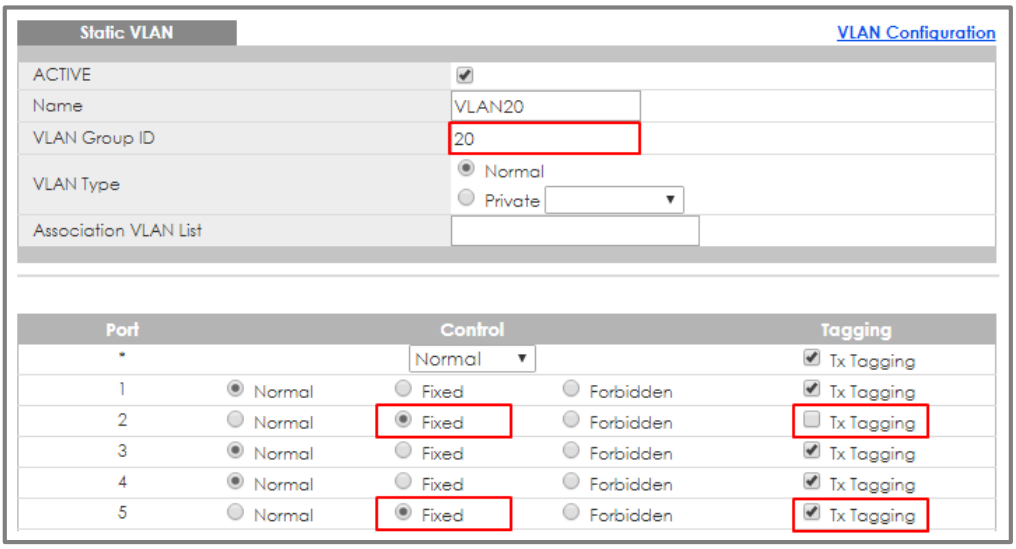
1 Use AdministratorPC to set **VLAN 1** in **Switch-1**: Port 1, 2 as **Normal** port. (Prevent VLAN 1 broadcast packets to port 1, 2). Enter the web GUI and go to **Menu > Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup > VID > 1**. Select port 1, 2 as **Normal**. Click "**Add**".



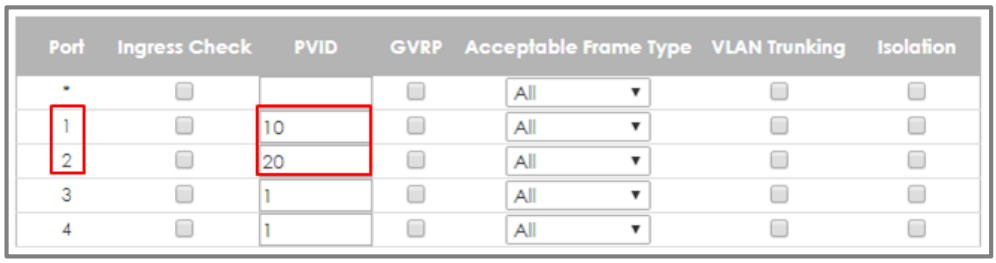
2 Use AdministratorPC to create **VLAN 10** in **Switch-1**: Enter the web GUI and go to **Menu > Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup**. Check the "ACTIVE" box. Type the Name and VLAN Group ID=**10**. Select port **1**, **5** as **Fixed** and uncheck Tx Tagging (**Untagged**) on port 1 and check Tx Tagging (**Tagged**) on port 5. Click "**Apply**".



3 Use AdministratorPC to create **VLAN 20** in **Switch-1**: Enter the web GUI and go to **Menu > Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup**. Check the "ACTIVE" box. 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**".



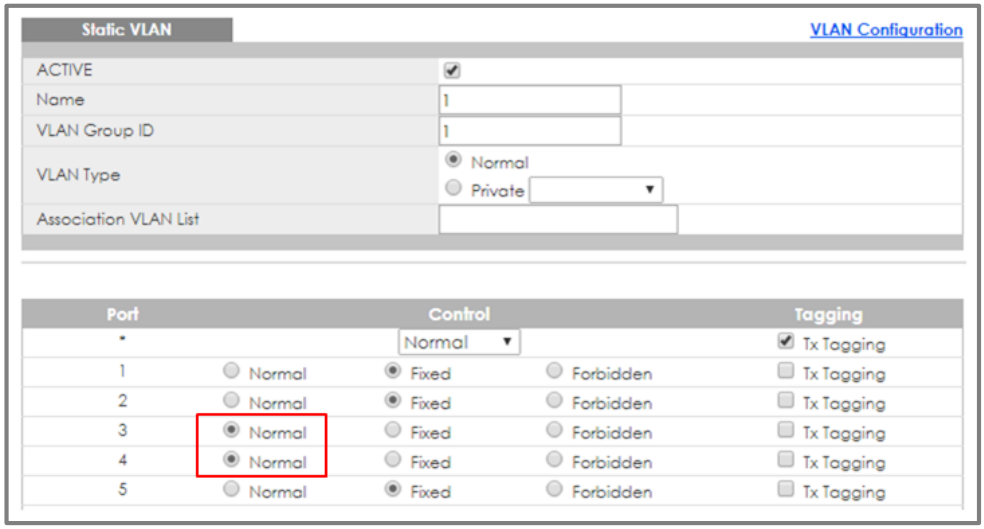
4 Set the PVID on **Switch-1**: Go to **Menu > Advanced Application > VLAN > VLAN Configuration > VLAN Port Setup**. Set port 1 as PVID=**10** (VLAN 10) and port 2 as PVID=**20** (VLAN 20).



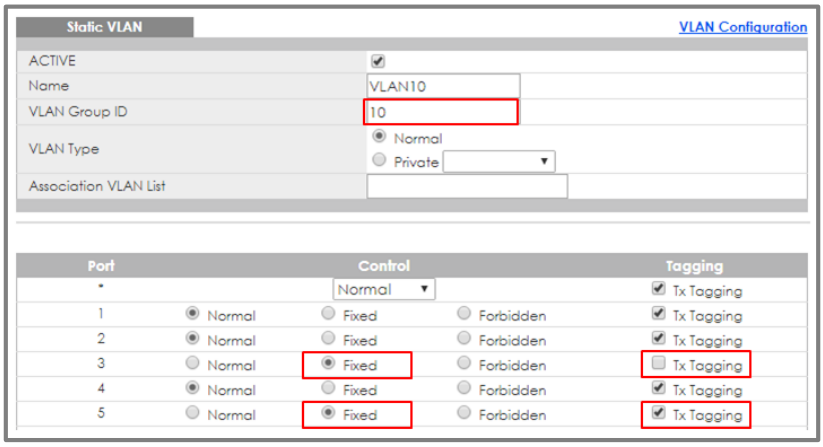
Port	Ingress Check	PVID	GVRP	Acceptable Frame Type	VLAN Trunking	Isolation
*	☐		☐	All	☐	☐
1	☐	10	☐	All	☐	☐
2	☐	20	☐	All	☐	☐
3	☐	1	☐	All	☐	☐
4	☐	1	☐	All	☐	☐

2.1.2 Configure Switch-2

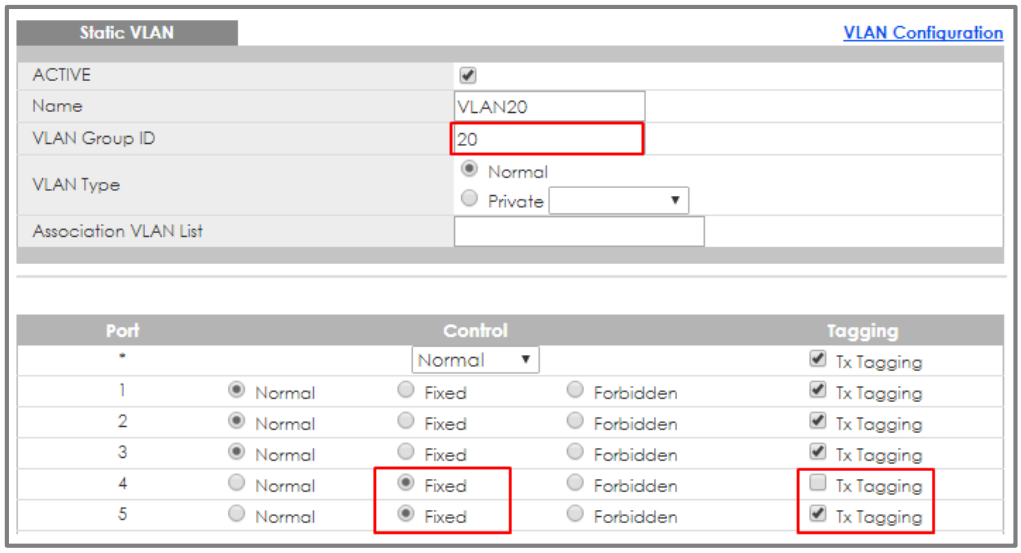
1 Use AdministratorPC to set **VLAN 1** in **Switch-2**: Port 3, 4 as **Normal** port (this prevents VLAN 1 from broadcasting packets to port 3, 4). Enter the web GUI and go to **Menu > Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup > VID > 1**. Select port 3, 4 as **Normal**. Click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



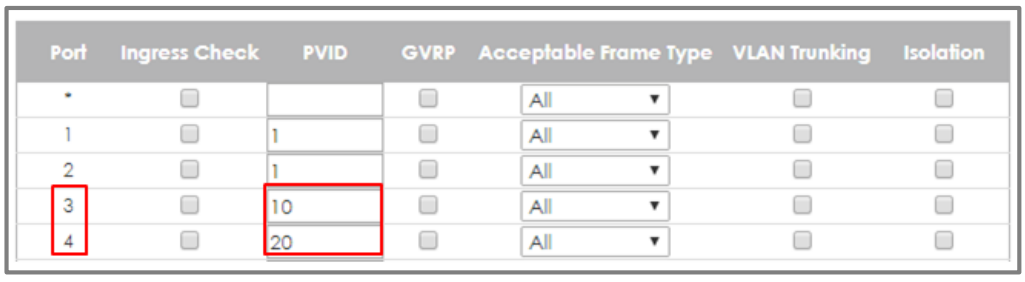
2 Use AdministratorPC to create **VLAN 10** in **Switch-2**. Enter the web GUI and go to **Menu > Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup**. Check the "ACTIVE" box. Type the Name and VLAN Group ID=**10**. Select port 3, 5 as **Fixed** and uncheck Tx Tagging (**Untagged**) on port 3 and check Tx Tagging (**tagged**) on port **5**. Click "**Apply**".



3 Use AdministratorPC to create VLAN 20 in **Switch-2**. Enter the web GUI and go to **Menu > Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup**. Check the "ACTIVE" box. 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**".



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



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.
PING: transmit failed. General failure.
PING: transmit failed. General failure.
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.
PING: transmit failed. General failure.
PING: transmit failed. General failure.
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.

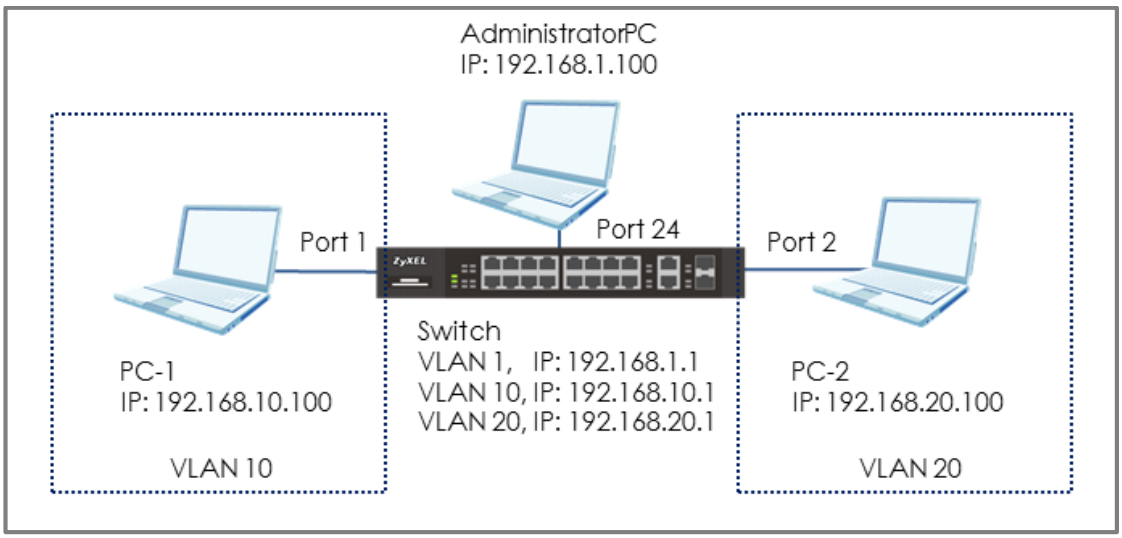
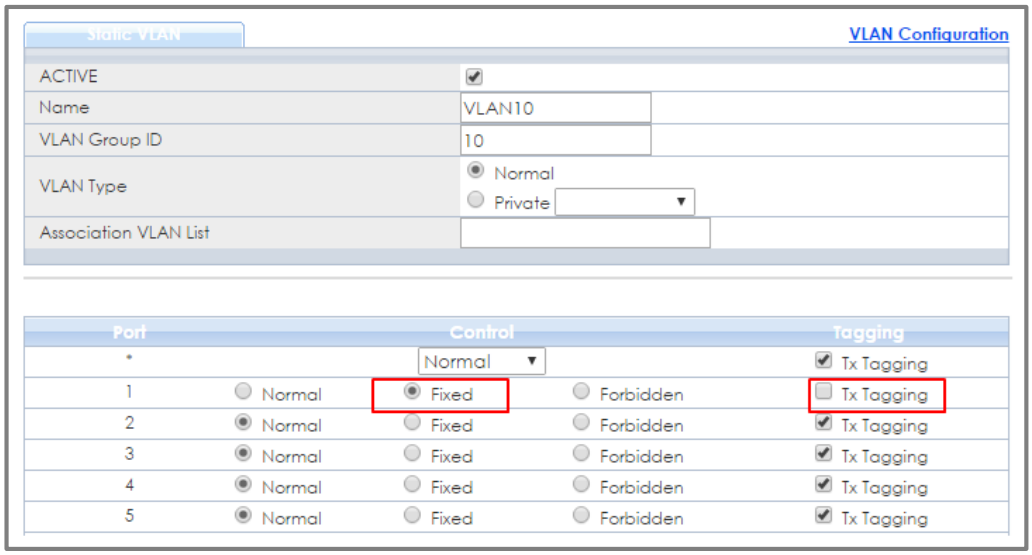


Figure 10 Set up switch to route traffic across VLANs

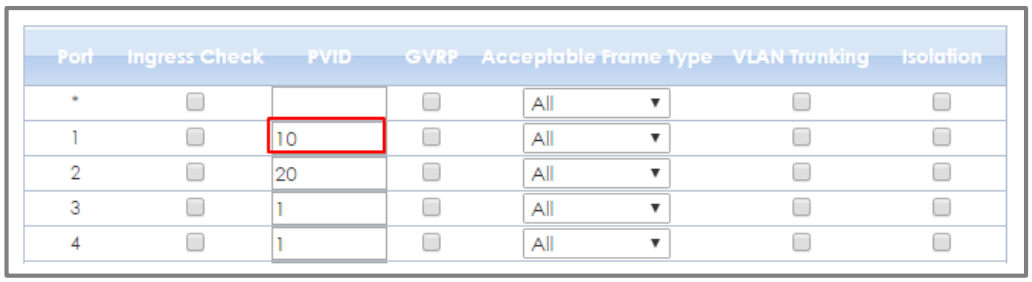
Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using XGS4600-32 (Firmware Version: V4.50).

2.2.1 Configure VLAN 10

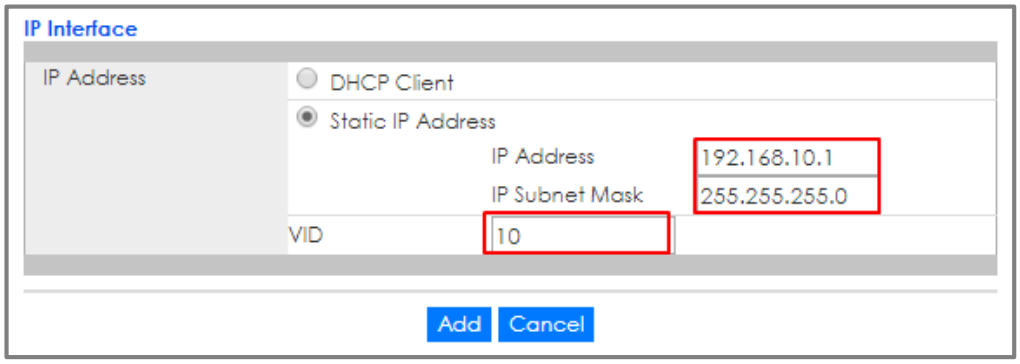
1 Use AdministratorPC to create VLAN 10. Enter the web GUI and go to **Menu > Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup**. Check the ACTIVE box. Type the Name and VLAN Group ID=**10**. Select port **1** as **Fixed** and uncheck Tx Tagging (Untagged). Click "**Apply**".



2 Go to **Menu > Advanced Application > VLAN > VLAN Configuration > VLAN Port Setup**. Set the PVID. Set port **1** as PVID=**10** (VLAN 10). Click "**Apply**".

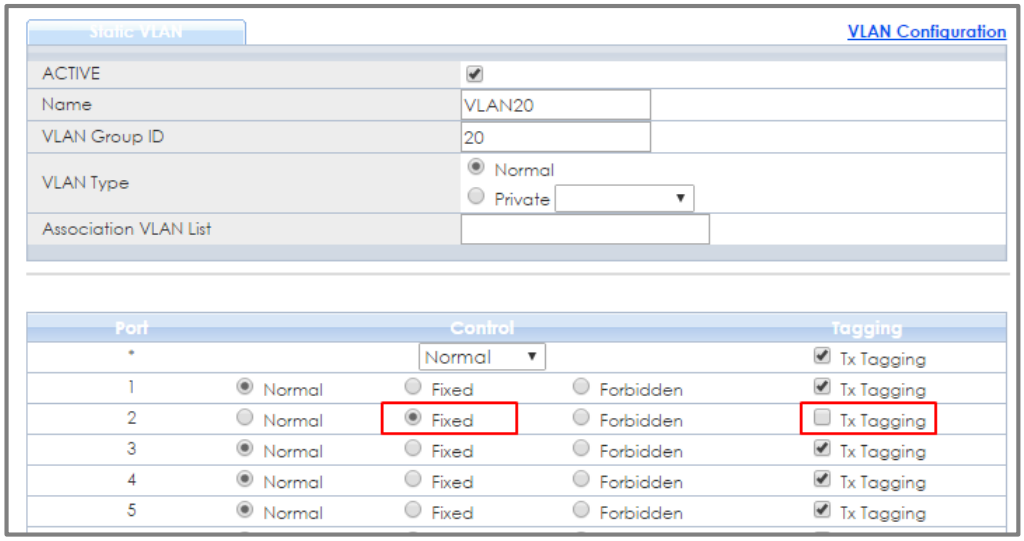


3 Create a Static IP Address for Switch in **VLAN 10** (To be the gateway in VLAN 10): Go to **Menu > Basic Setting > IP Setup > IP Configuration > IP Interface**. Set the Static IP Address: **192.168.10.1** for Switch in VLAN 10. Click "**Add**".

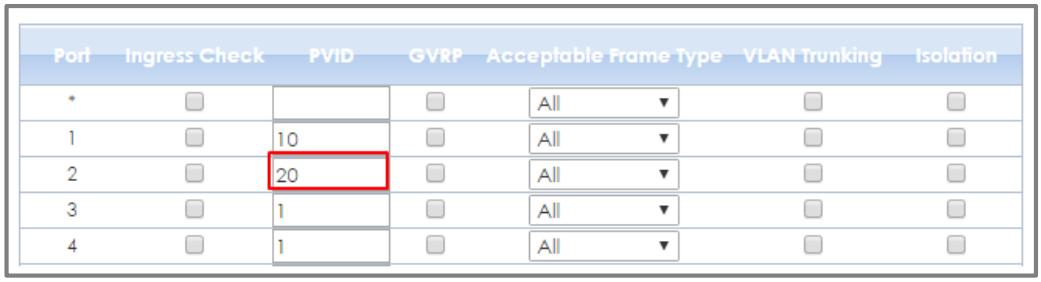


2.2.2 Configure VLAN 20

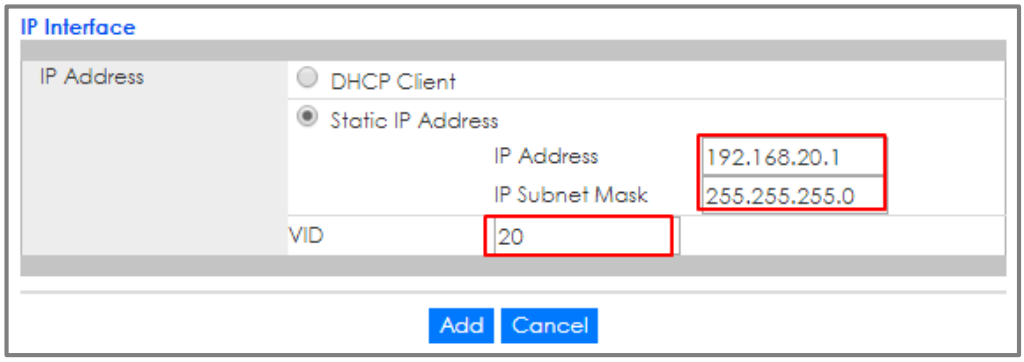
1 Create VLAN 20. Follow the same steps. Go to **Menu > Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup**. Check the ACTIVE box. Type the Name and VLAN Group ID=**20**. Select port **2** as **Fixed** and uncheck Tx Tagging (Untagged). Click "**Apply**".



2 Go to **Menu > Advanced Application > VLAN > VLAN Configuration > VLAN Port Setup**. Set the PVID. Set port **2** as PVID=**20** (VLAN 20). Click "**Apply**".

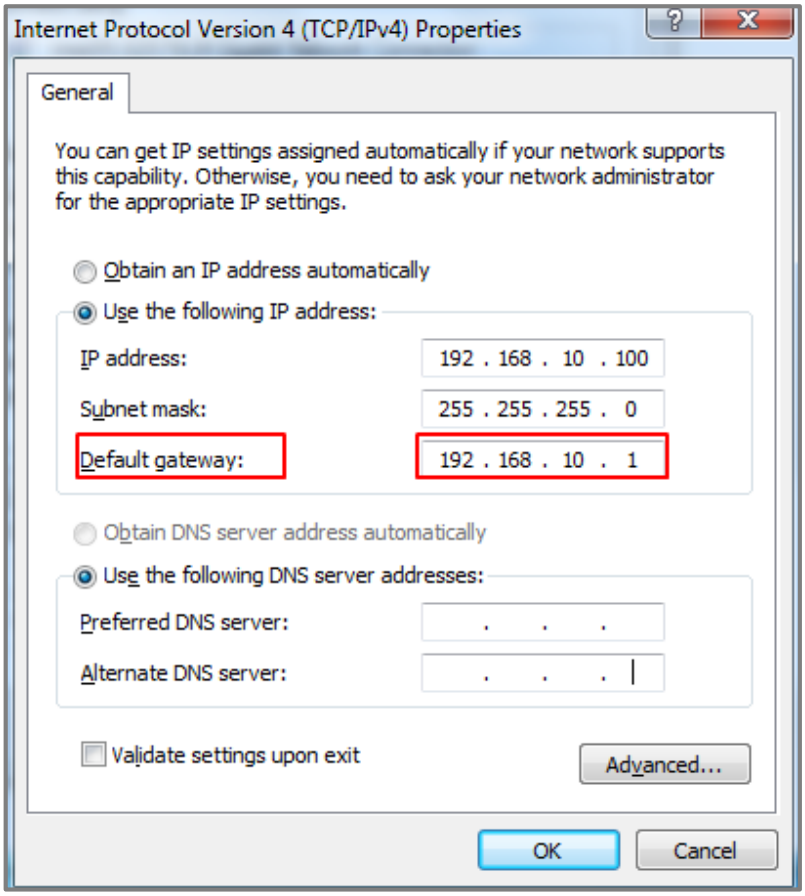


3 Create a Static IP Address for Switch in VLAN 20 (To be the gateway in VLAN 20). Go to **Menu > Basic Setting > IP Setup > IP Configuration > IP Interface**. Set a Static IP Address: **192.168.20.1** for Switch in **VLAN 20**. Click "**Add**".

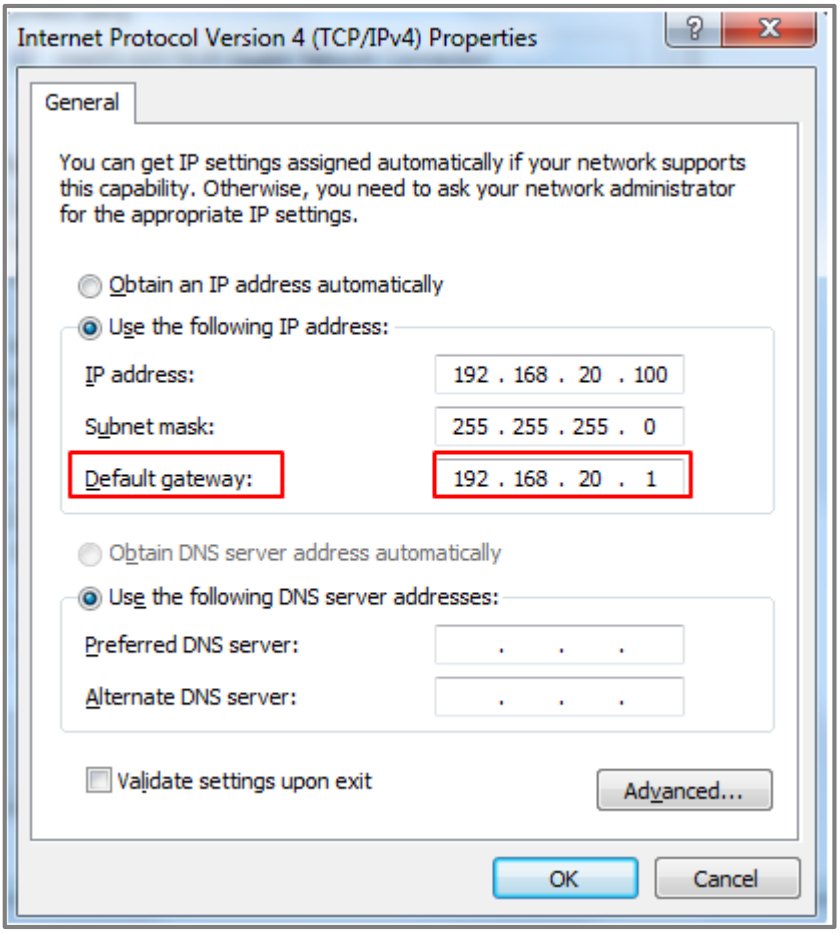


2.2.3 Set the gateway on PC-1 and PC-2

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

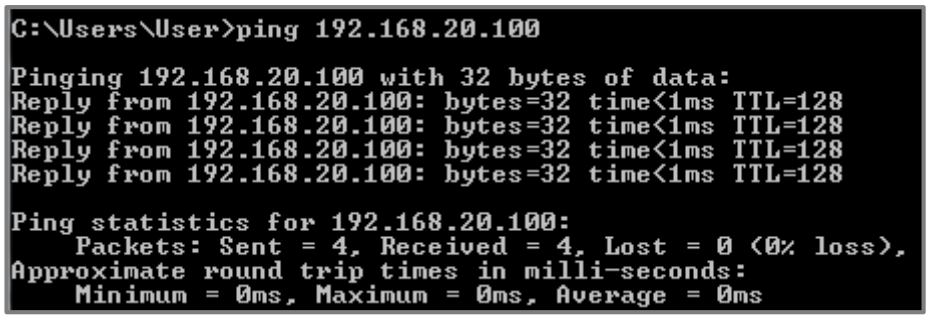


2 Set the Gateway of PC-2 as **192.168.20.1** (The Static IP Address of Switch in **VLAN 20**).



2.2.4 Test the Result

1 PC-1 can ping PC-2 successfully.



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.

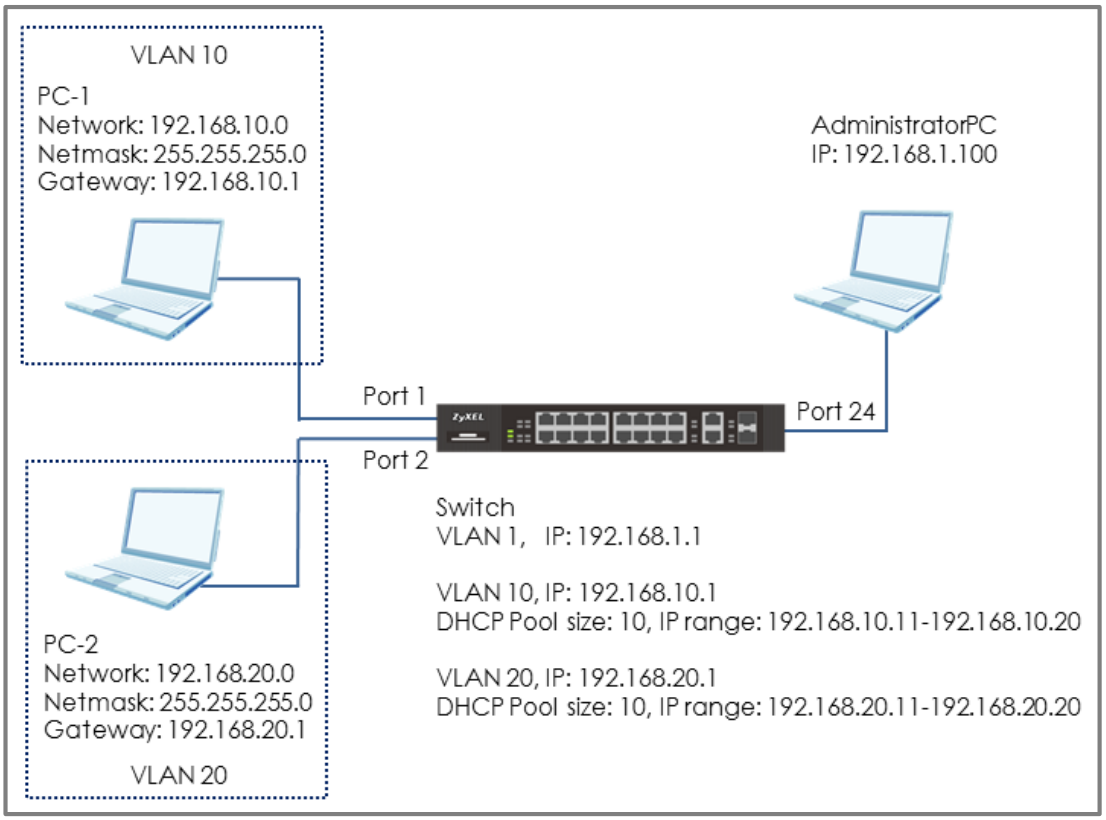
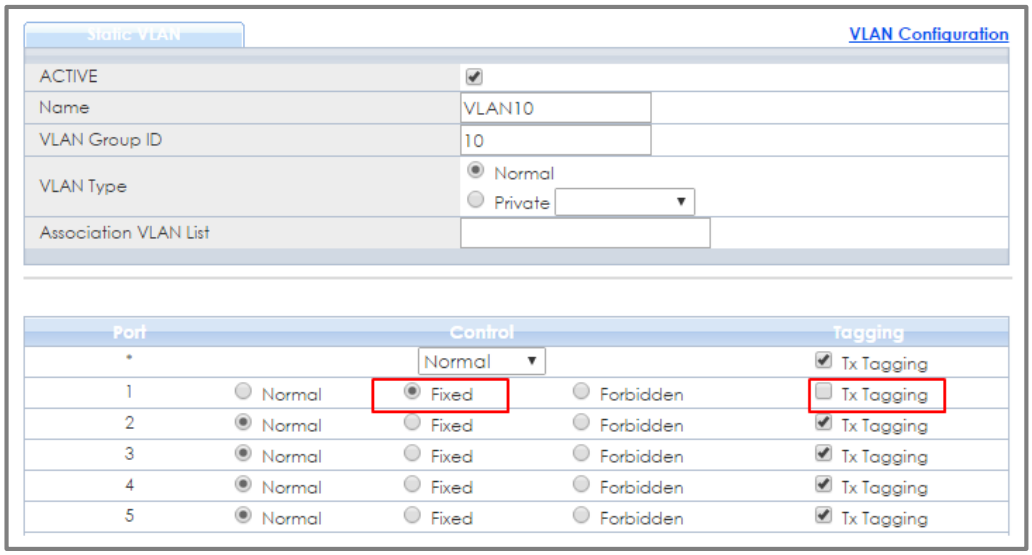


Figure 11 Perform DHCP service in different VLAN

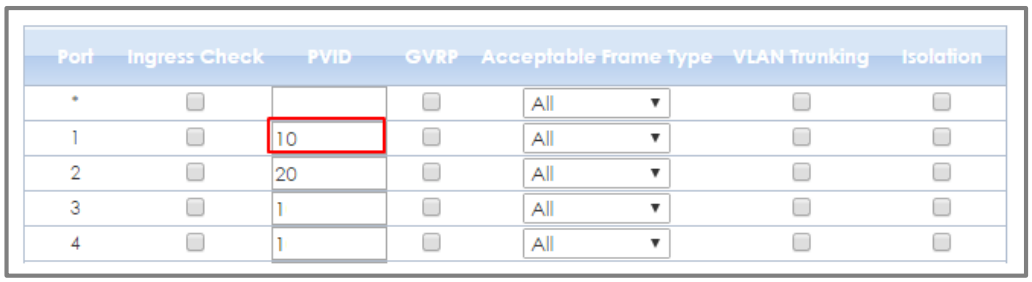
Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using XGS4600-32 (Firmware Version: V4.50).
Only L3 Switch supports the function of DHCP Server. (The models: 3700 series, 4500 series and 4600 series)

2.3.1 Configure VLAN 10

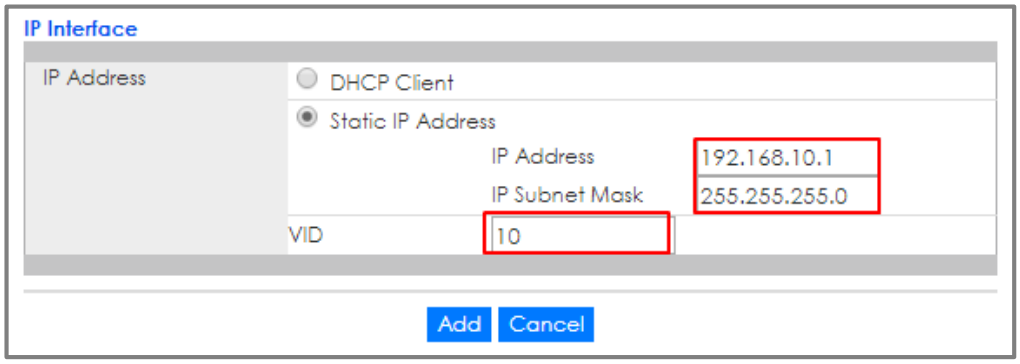
1 Use AdministratorPC to create VLAN 10. Enter the web GUI and go to **Menu > Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup**. Check the ACTIVE box. Type the Name and VLAN Group ID=**10**. Select port **1** as **Fixed** and uncheck Tx Tagging (Untagged). Click "**Apply**".



2 Go to **Menu > Advanced Application > VLAN > VLAN Configuration > VLAN Port Setup**. Set the PVID. Set port **1** as PVID=**10** (VLAN 10). Click "**Apply**".

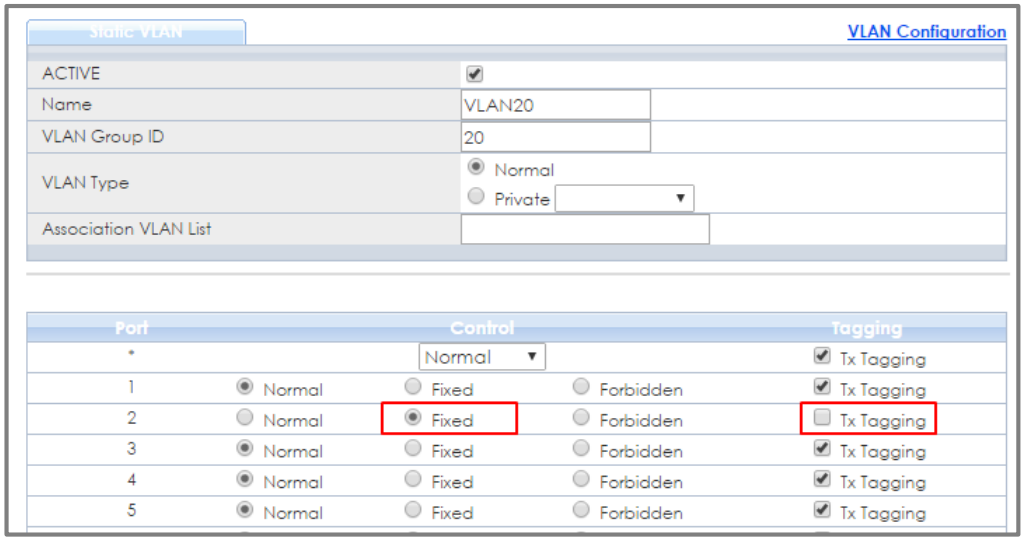


3 Create a Static IP Address for Switch in **VLAN 10** (IP Address to be DHCP Server in VLAN 10): Go to **Menu > Basic Setting > IP Setup > IP Configuration > IP Interface**. Set the Static IP Address: **192.168.10.1** for Switch in VLAN 10. Click "**Add**".

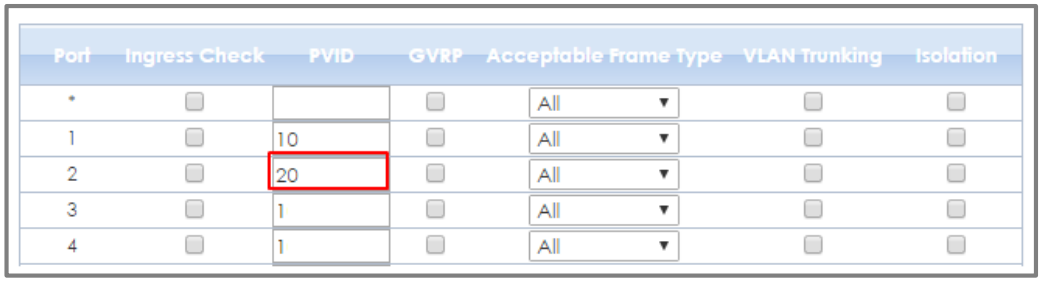


2.3.2 Configure VLAN 20

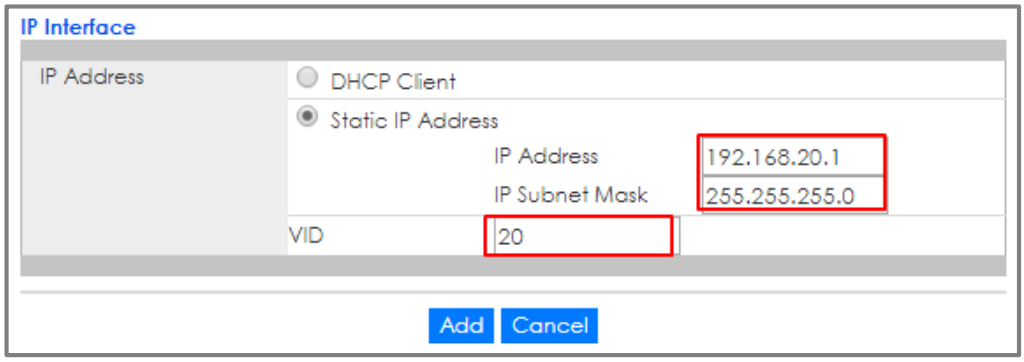
1 Create VLAN 20. Follow the same steps. Go to **Menu > Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup**. Check the ACTIVE box. Type the Name and VLAN Group ID=**20**. Select port **2** as **Fixed** and uncheck Tx Tagging (Untagged). Click "**Apply**".



2 Go to **Menu > Advanced Application > VLAN > VLAN Configuration > VLAN Port Setup**. Set the PVID. Set port **2** as PVID=**20** (VLAN 20). Click "**Apply**".

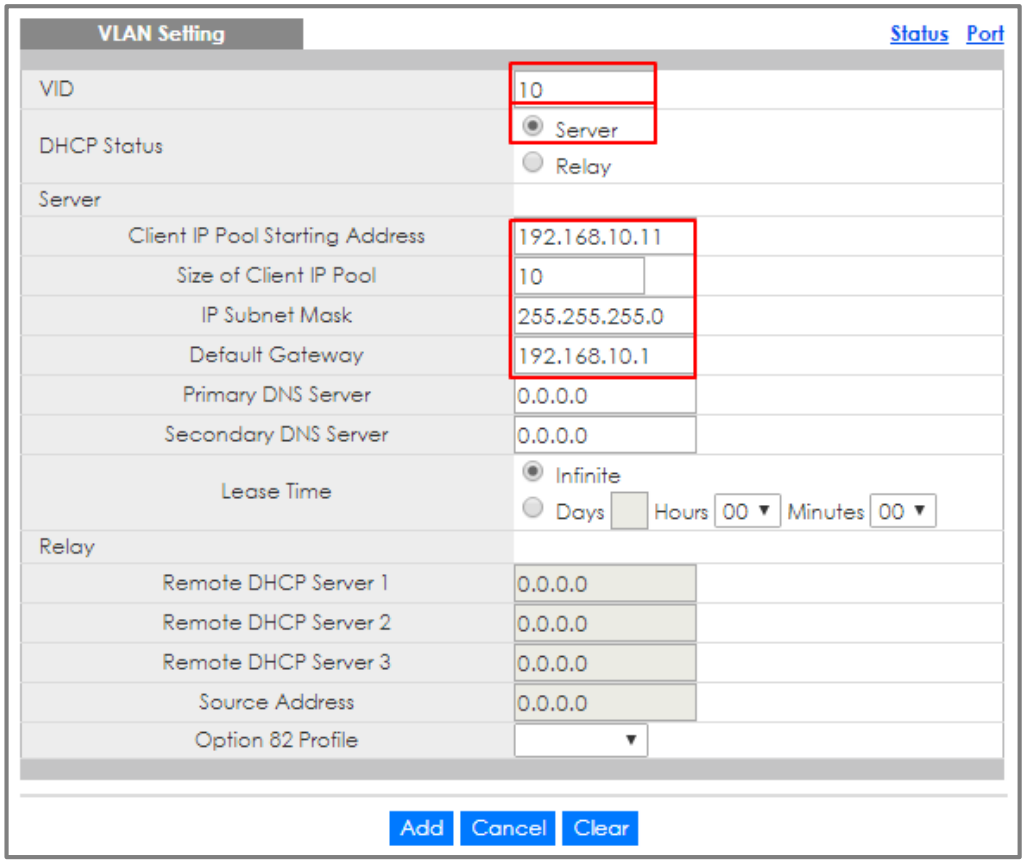


3 Create Static IP Address for Switch in VLAN 20 (IP Address to be DHCP Server in VLAN 20): Go to **Menu > Basic Setting > IP Setup > IP Configuration > IP Interface**. Set the Static IP Address: **192.168.20.1** for Switch in **VLAN 20**. Click "**Add**".



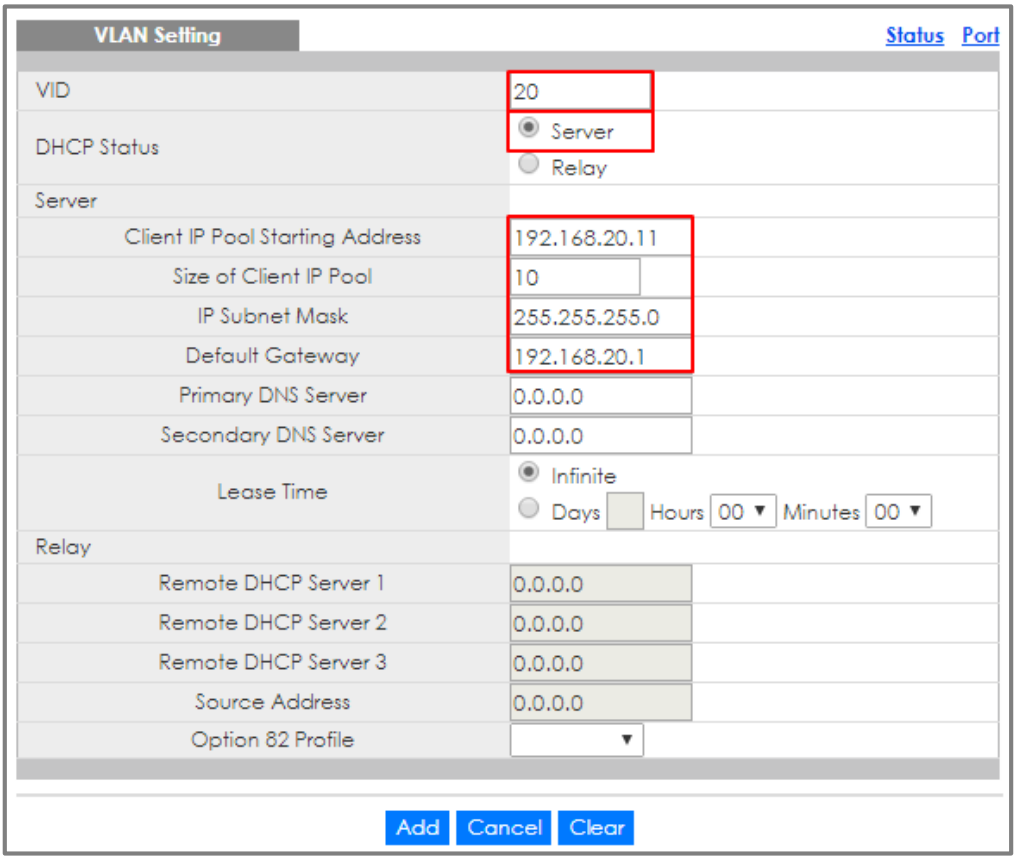
2.3.3 Configure the Switch and PC

1 Set up DHCP Server in **VLAN 10**: Go to **Menu > IP Application > DHCP > DHCPv4 > Click Here > VLAN**. Set up the VID (VLAN of PC-1) and DHCP Status as **Server**. 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".



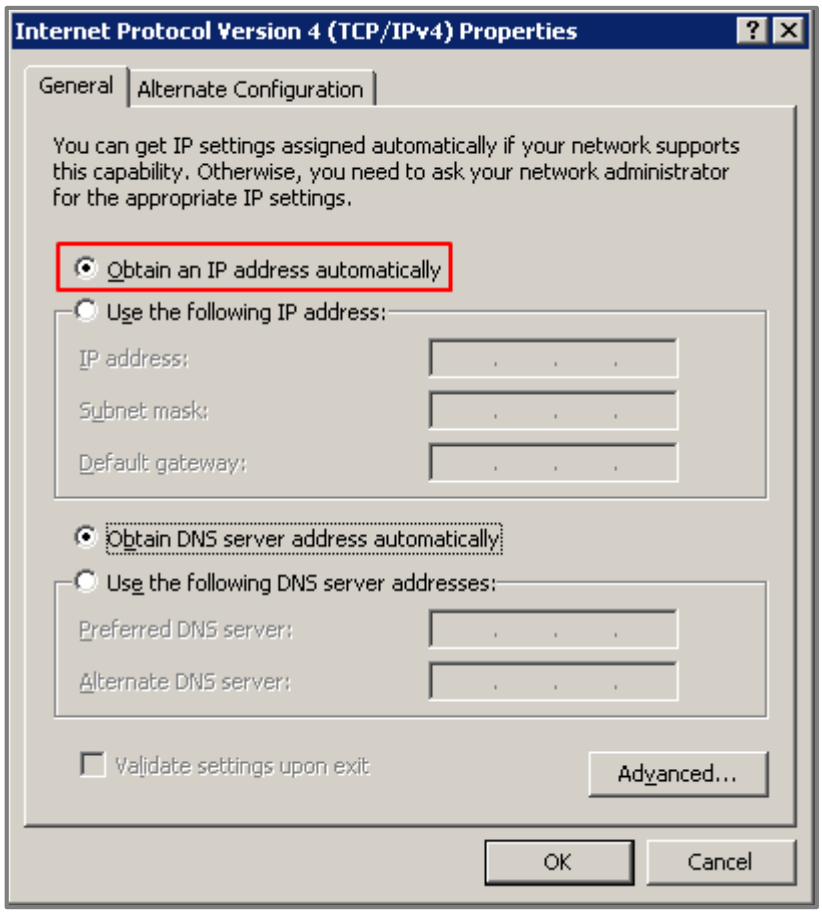
Note:
In this example, the pool size is 10 and the starting IP address is 192.168.10.11. Therefore, the IP range that the DHCP Server will assign is between 192.168.10.11 and 192.168.10.20.

2 Set up DHCP Server in **VLAN 20**: Go to **Menu > IP Application > DHCP > DHCPv4 > Click Here > VLAN**. Set up the VID (VLAN of PC-2) and DHCP Status as **Server**. 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".



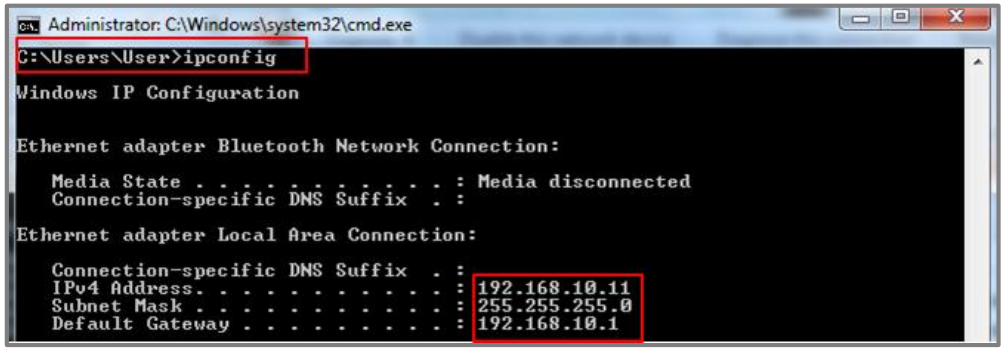
Note:
In this example, the pool size is 10 and the starting IP address is 192.168.20.11. Therefore, the IP range that the DHCP Server will assign is between 192.168.20.11 and 192.168.20.20.

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

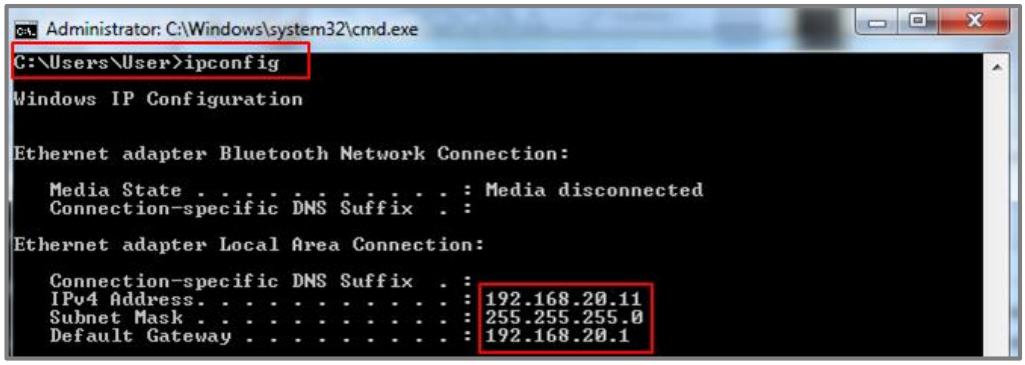


2.3.4 Test the Result

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.**



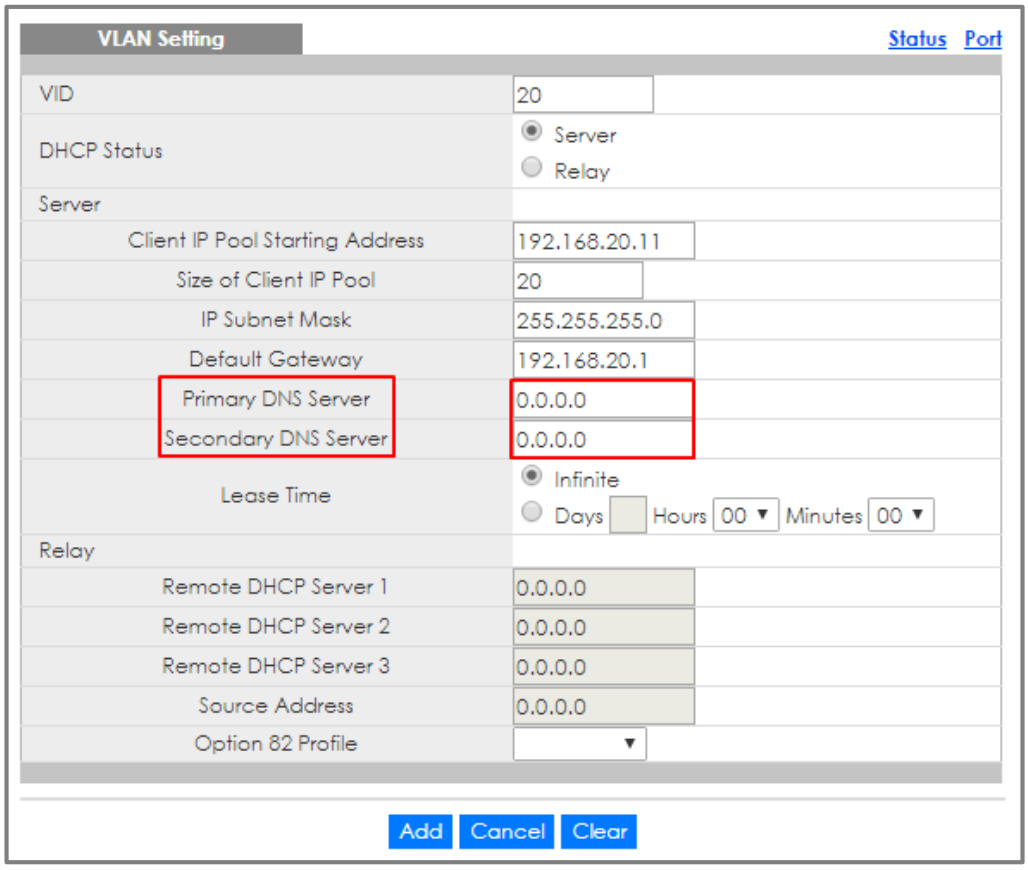
2 PC-2 can get the IP Address assigned by Switch successfully. We can check this by using the command "**ipconfig**" in command prompt. PC-2 will get an IP address in the range of: **192.168.20.11-192.168.20.20** and the gateway is **192.168.20.1.**



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.

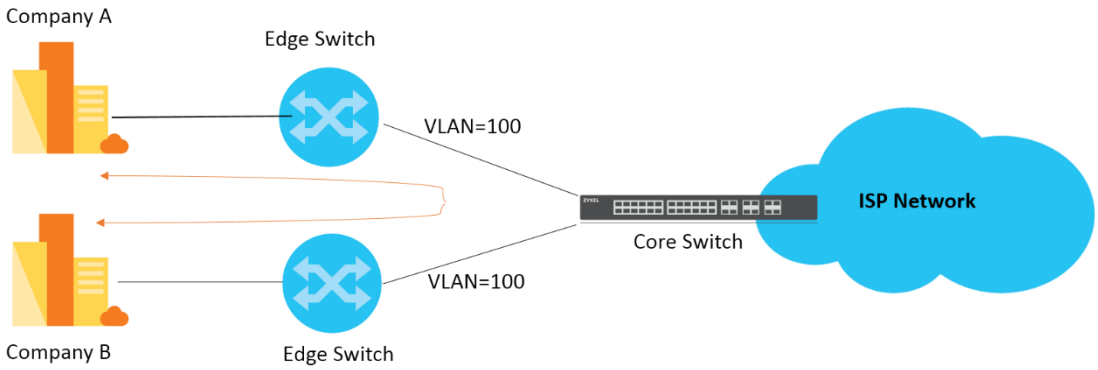
2 If you want to surf the Internet using a URL or domain name, please remember to set up **DNS Server**.



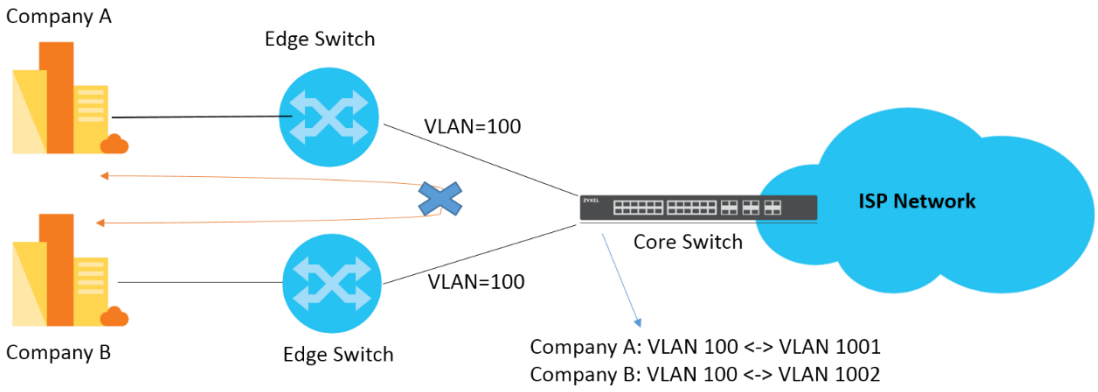
2.4 How to Configure the Switch to Translate Customer VLAN to Service Provider VLAN

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.

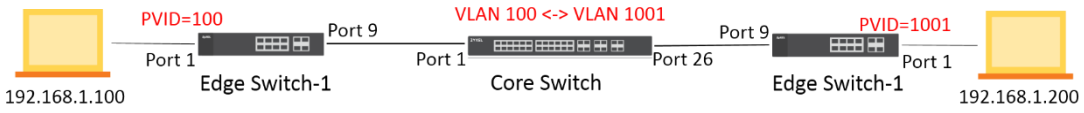
VLAN Mapping also can be used to prevent traffic from forwarding between different customers when they use the same VLAN in their own networks. In the following example, both of company A and company B use the same VLAN 10. When company A sends traffic to an ISP network, the traffic is possible to be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



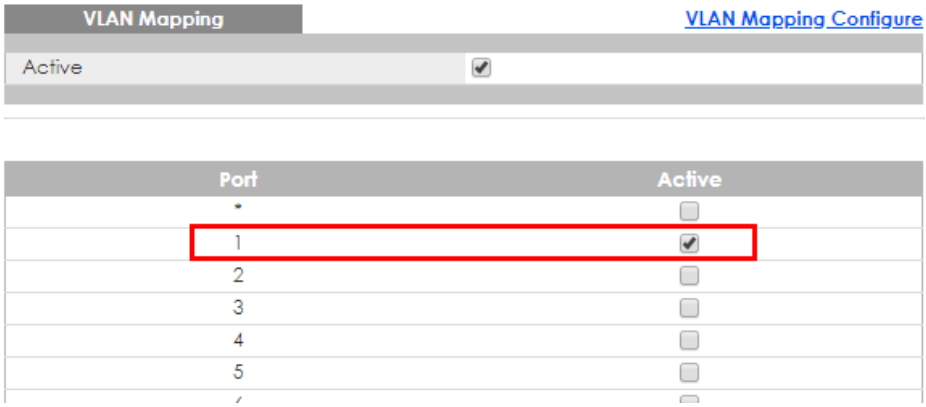
The following example will instruct how an administrator configures a switch to achieve VLAN translation.



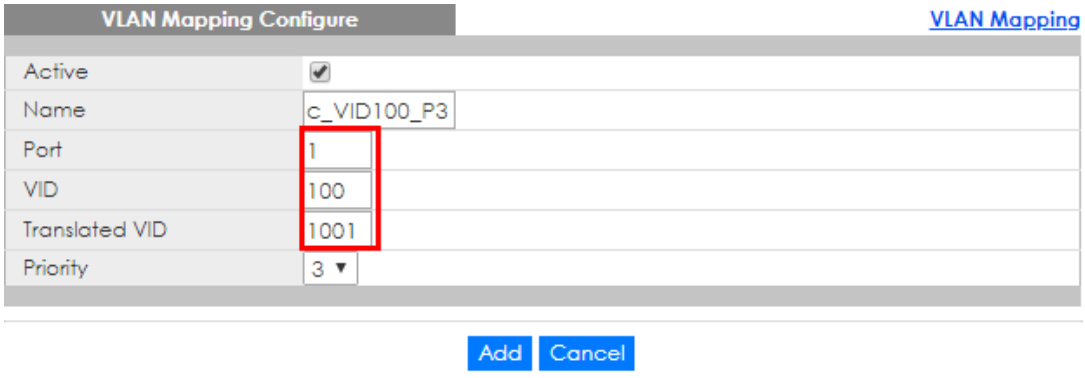
Note:
The example was tested using two GS2210 as edge switches, and one XGS4600 as a core switch.

2.4.1 Configuration on the Core Switch

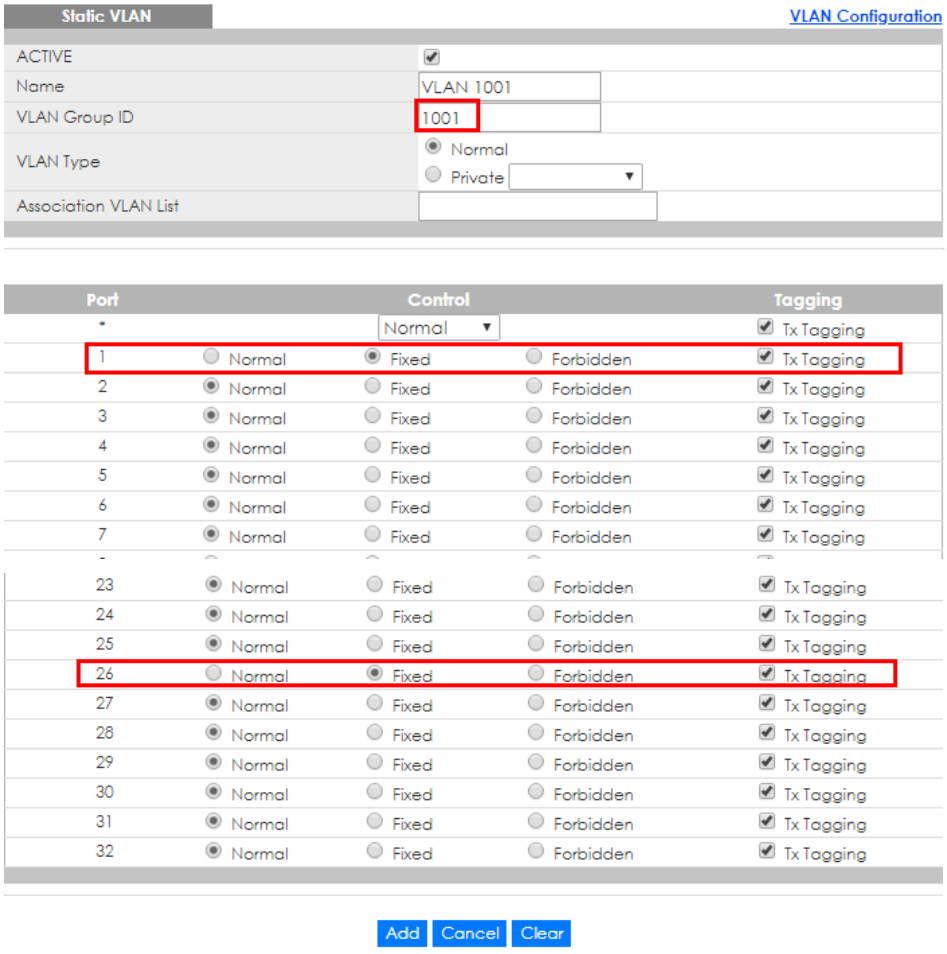
1 Access to the web GUI, Go to **Menu > Advanced Application > VLAN Mapping.** Check the **Active** box and activate port **1**.



2 Go to **Menu > Advanced Application > VLAN Mapping > Configure**. Check the **Active** box 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".



3 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, 26** as **Fixed**, and click "**Apply**".

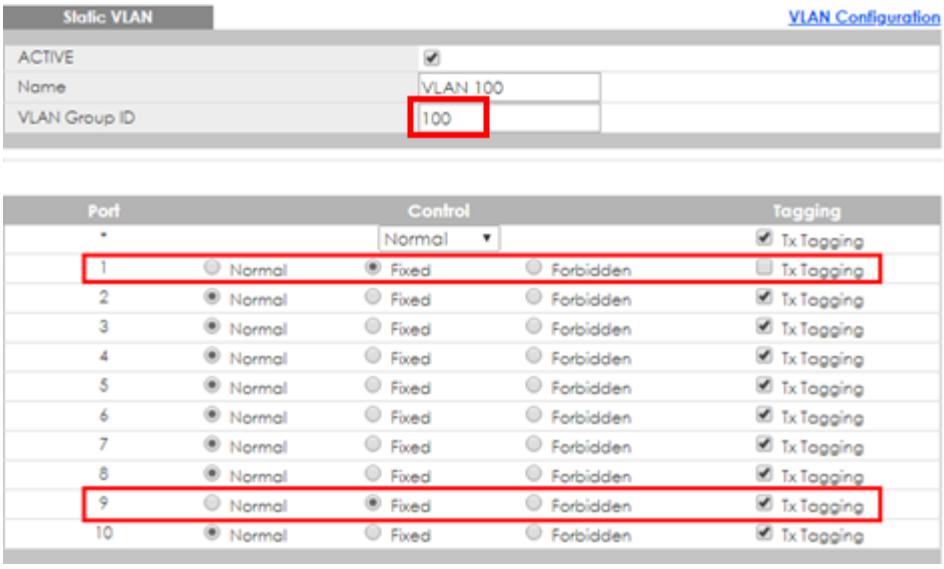


Note:

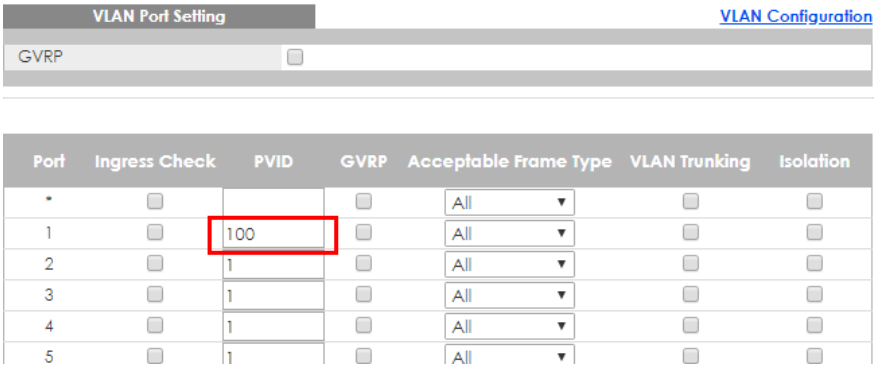
Create a Static VLAN only for the Translated VLAN, and set both of ports as members for the Translated VLAN. Otherwise the packets from the Translated VLAN received on port 26 will NOT be forwarded to port 1.

2.4.2 Configuration on the Edge Switch

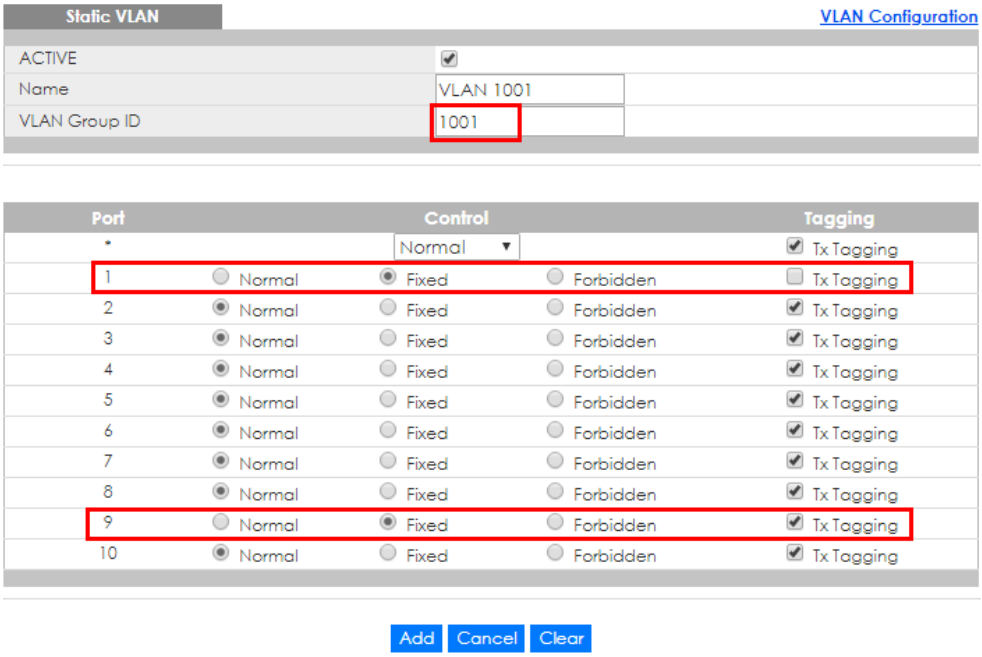
1 Setup **Customer Switch-1:** Access to the web GUI. Go to **Menu > Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup**. Check the **Active** box, type the **Name** and VLAN Group ID= as **100**. Select port **1** as **Fixed** and uncheck Tx Tagging (Untagged). Select port **9** as **Fixed**, and click "**Apply**".



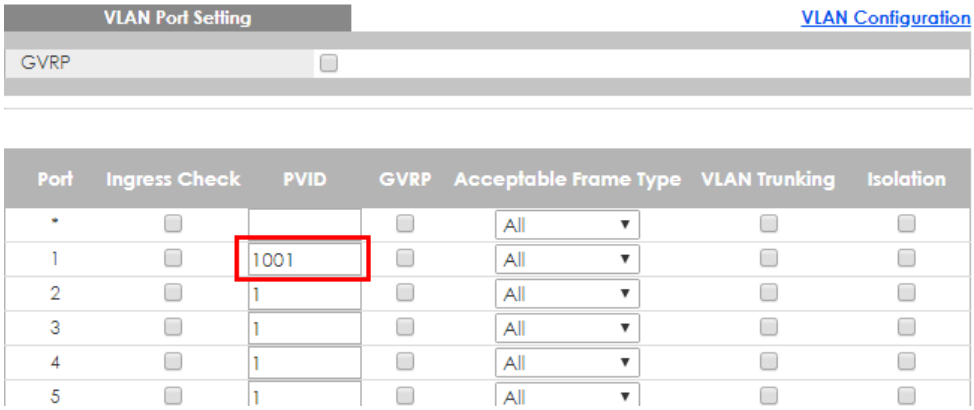
2 Setup **Customer Switch-1:** Go to **Menu > Advanced Application > VLAN > VLAN Configuration > VLAN Port Setup**. Set port **1** PVID= as **100** (VLAN 100), and click "**Apply**".



3 Setup **Customer Switch-2:** 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**".



4 Setup **Customer Switch-2:** Go to **Menu > Advanced Application > VLAN > VLAN Configuration > VLAN Port Setup**. Set port **1** PVID= as **1001** (VLAN 1001), and click "**Apply**".

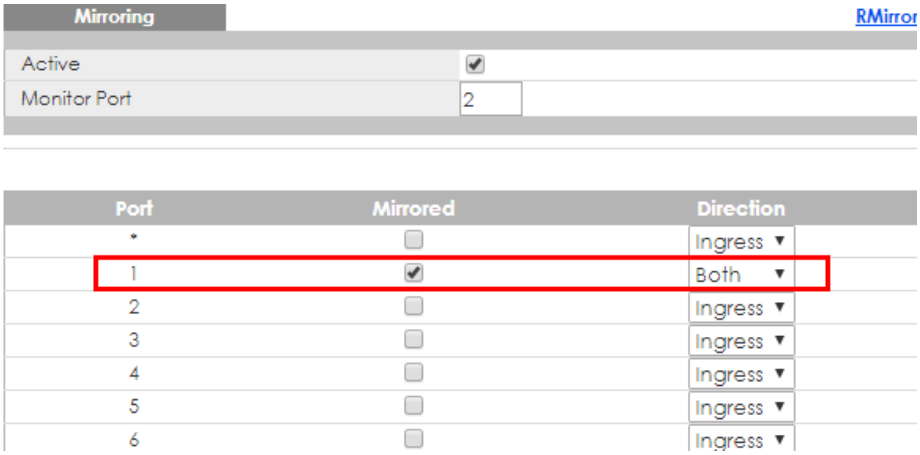


2.4.3 Test the Results

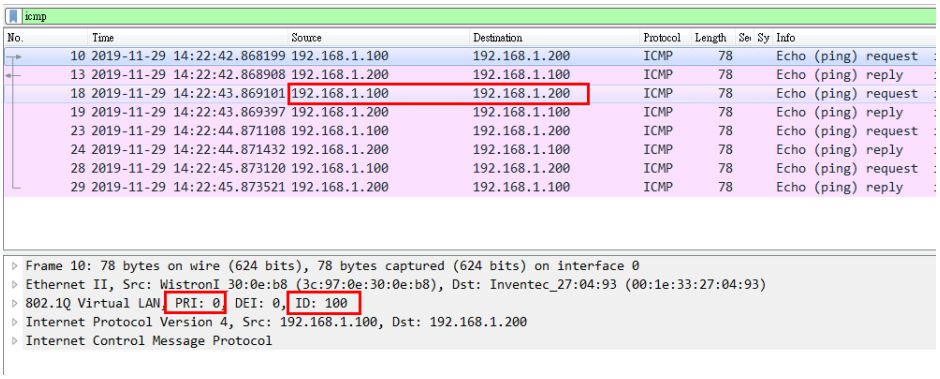
1 PC-1 can ping PC-2 successfully.

```
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
Reply from 192.168.1.200: bytes=32 time<1ms TTL=128
Reply from 192.168.1.200: bytes=32 time<1ms TTL=128
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
```

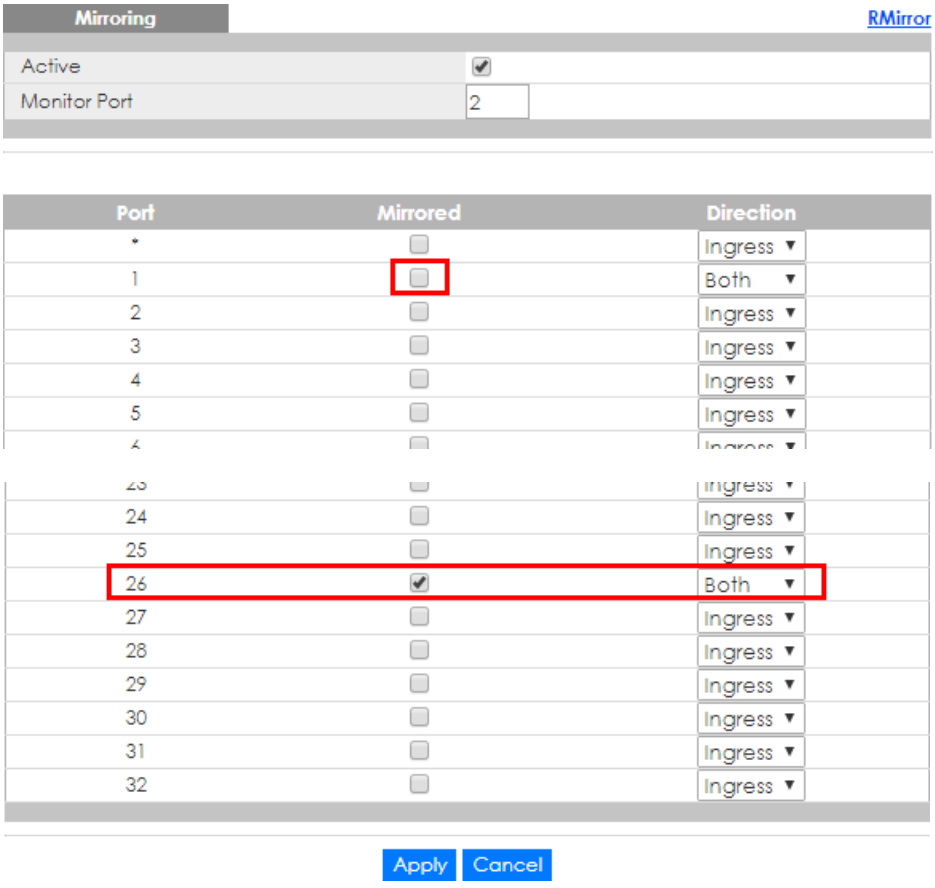
2 Configure Mirroring to verify the VLAN ID/Priority value in the packets which are received on **port 1** of the core switch, and ensure they are the original value (**VLAN=100/Priority=0**). Access to the web GUI and go to **Menu > Advanced Application > Mirroring**. Check the "**Active**" box. Set 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**".



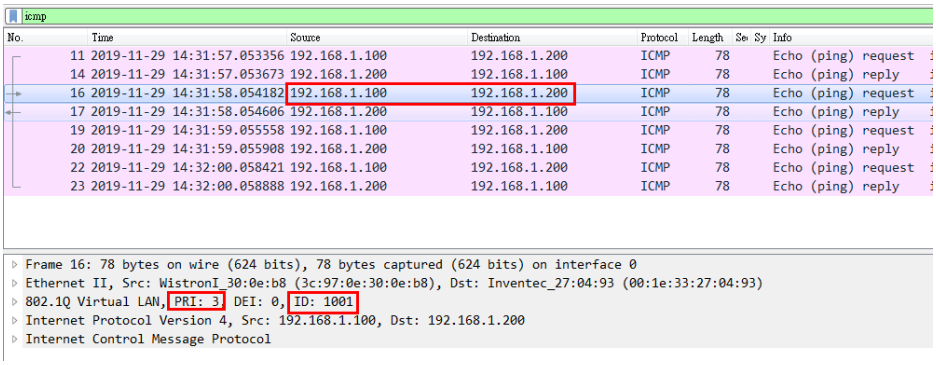
3 Connect with another PC to port 2 of the core switch. Open **wireshark** to monitor the packets, and filter "**icmp**".



4 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**".



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



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.

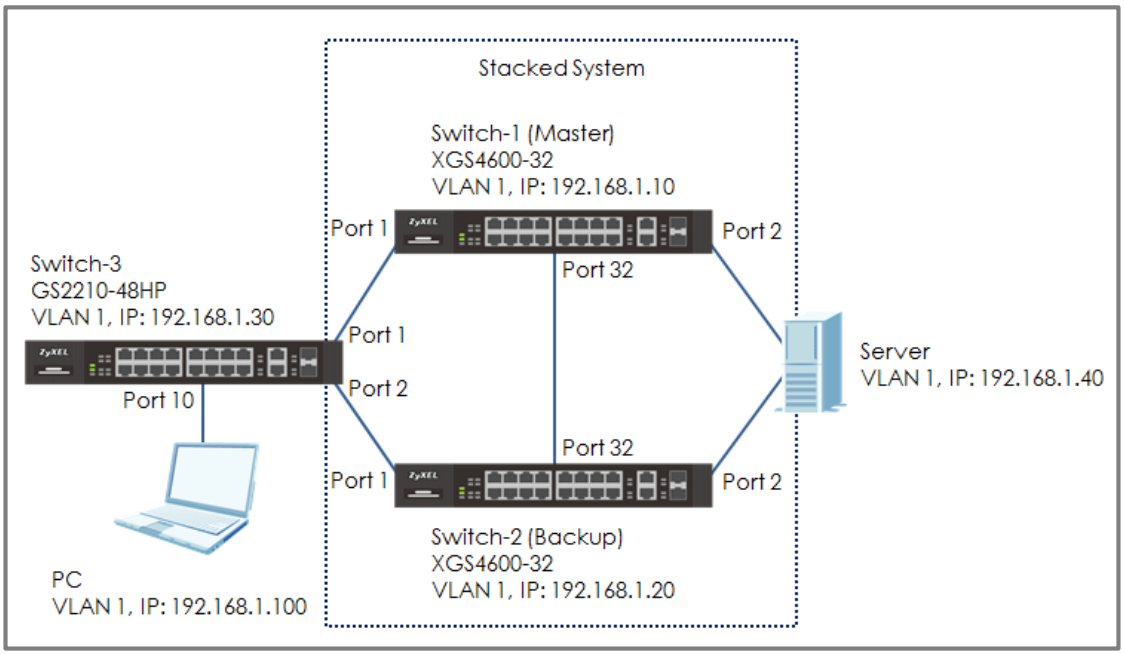
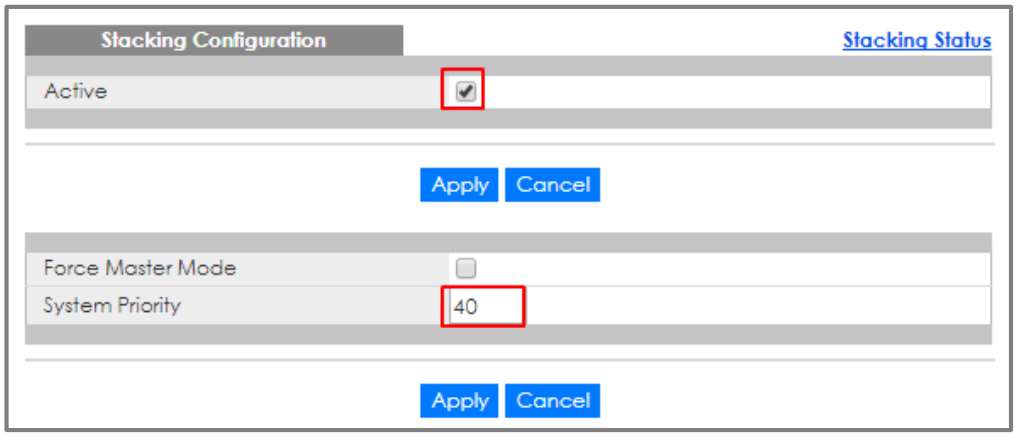


Figure 12 Configure the stacked switch

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 XGS4600-32 (Firmware Version: V4.50) and GS2210-48HP (Firmware Version: V4.30).

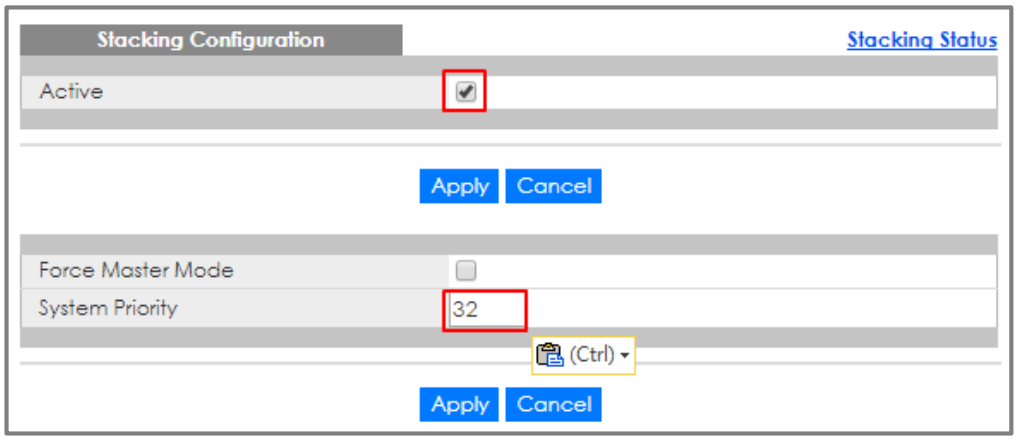
3.1.1 Configure Switch-1 and Switch-2 for Stacking

1 Set up **Switch-1**: Enter the web GUI and go to **Menu > Basic Setting > Stacking > Configuration**. Key in the system priority (The higher the number is, the higher priority it is to become a master) and click "Apply". Check "Active" and click "Apply". Switch-1 will reboot.



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 > Basic Setting > Stacking > Configuration**. Key in the system priority (The higher the number is, the higher priority it is to become a master) and click "Apply". Check "Active" and click "Apply". Switch-2 will reboot.



3 Connect Switch-1 and Switch-2 together on port 32 using a 10-Gigabit transceiver.

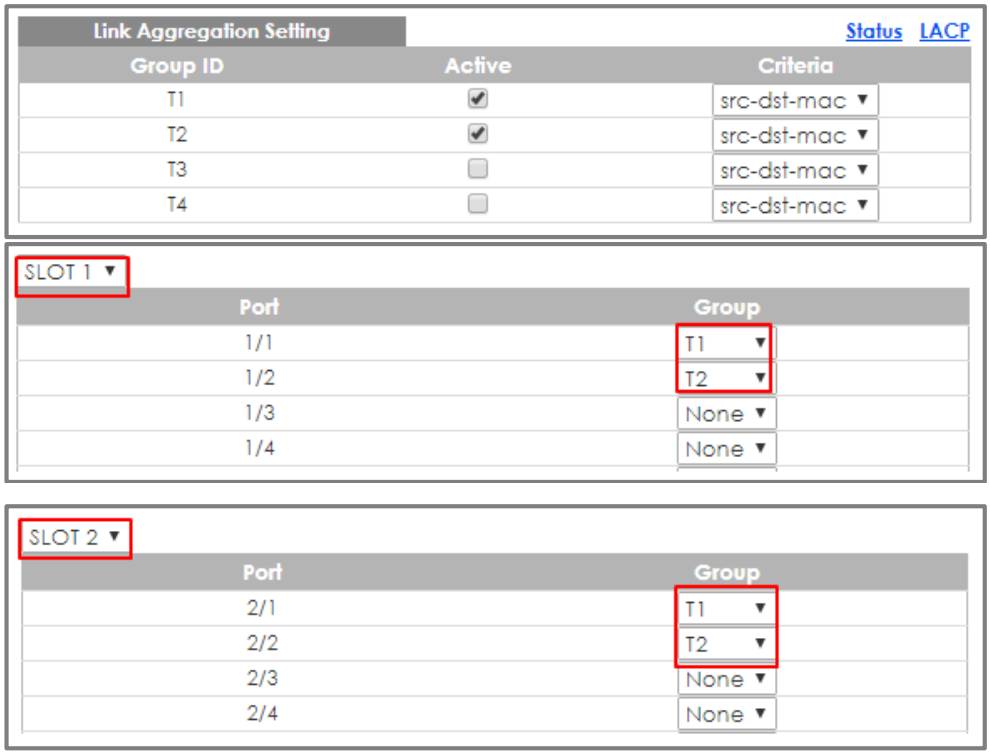
> Note:
> The last two ports are usually reserved for stacking channels when the switch is in stacking mode. These are ports 31 and 32 for the XGS4600-32 switch. If you are using other stackable models, please refer to the user manual to confirm the ports used for stacking.

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".

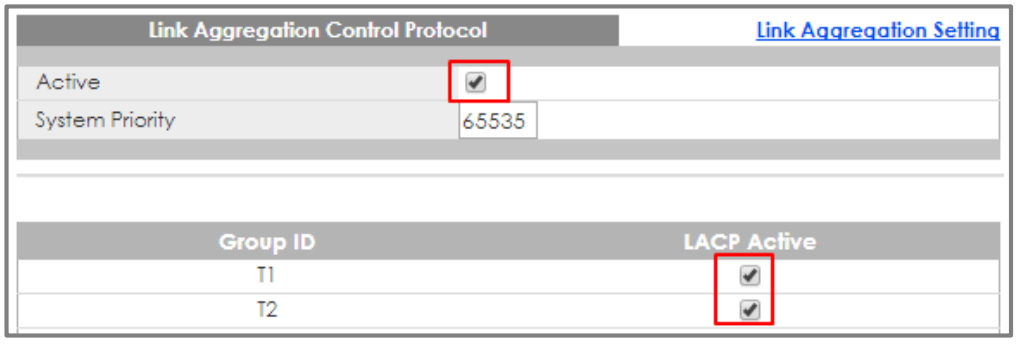
5 Remember to save the configuration.

3.1.2 Configure Link Aggregation on Stacked switch

1 Connect to the stacked switch. Enter web GUI and go to **Menu > Advanced Application > 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".

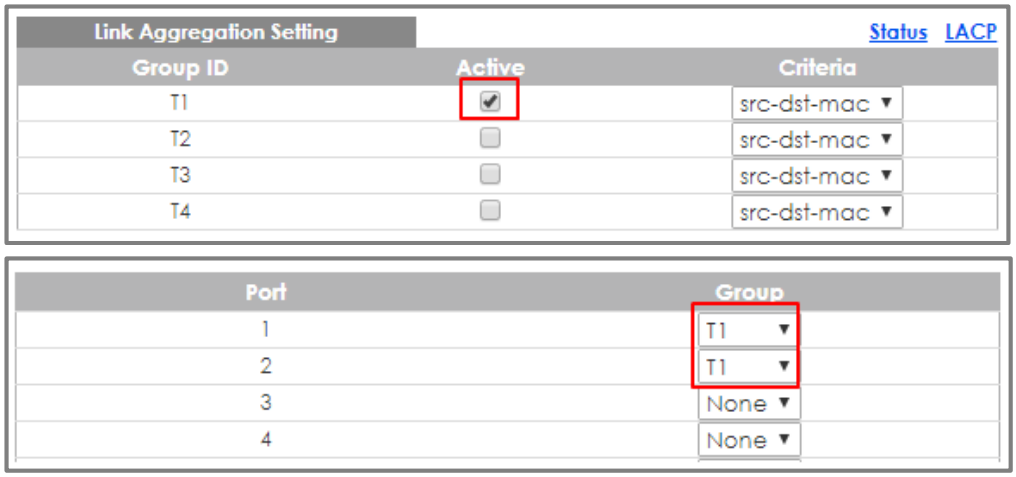


2 Go to **Menu > Advanced Application > Link Aggregation > Link Aggregation Setting >LACP**. Check the "Active" box, as well as for T1 and T2.

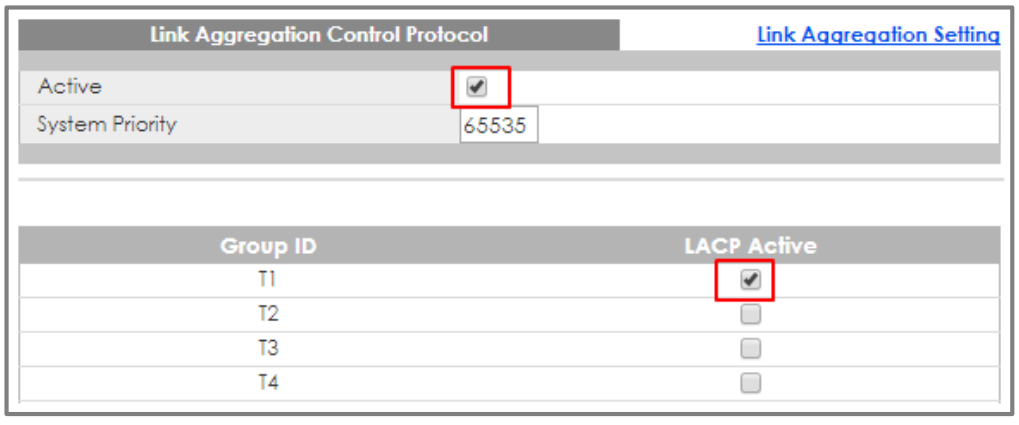


3.1.3 Configure Link Aggregation on Switch-3

1 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".



2 Go to **Menu > Advanced Application > Link Aggregation > Link Aggregation Setting >LACP**. Check the "Active" box and T1. Click "Apply".



3.1.4 Test the Result

1 Configure Link Aggegation 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=9ms 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=9ms 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<1ms 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
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.

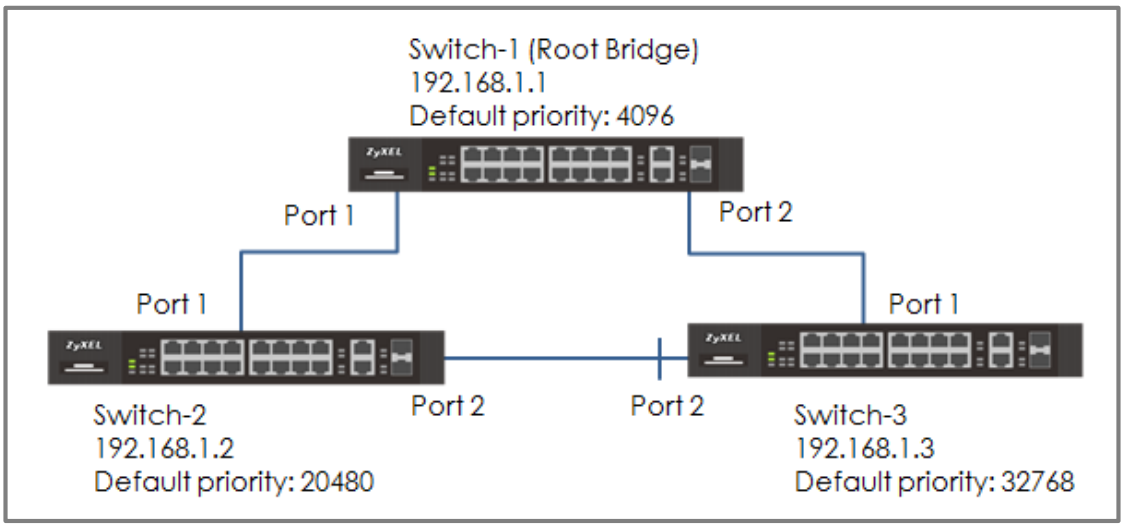


Figure 13 Configure RSTP in a ring topology

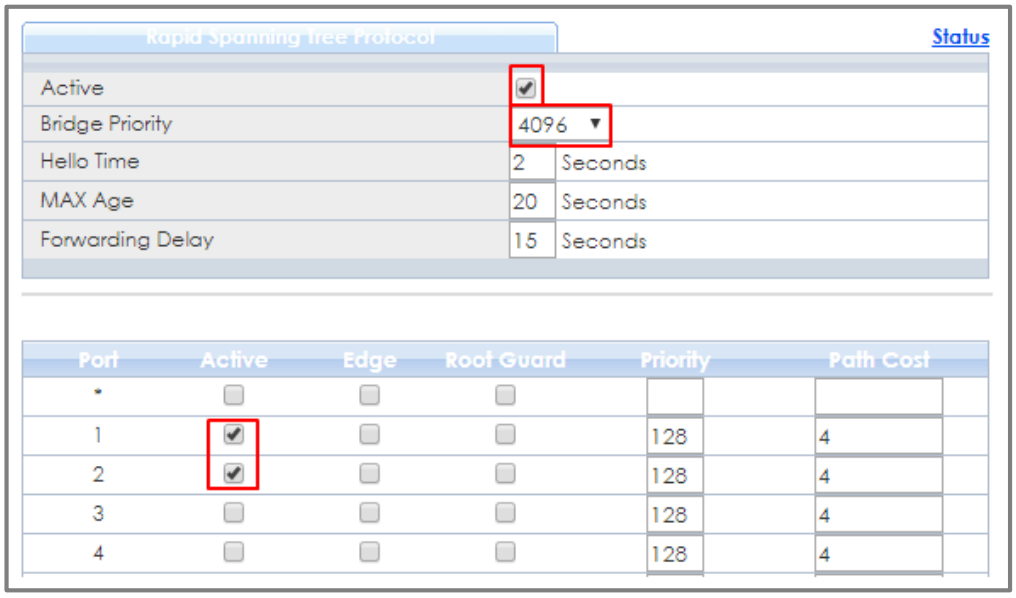
Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using XGS4600-32 (Firmware Version: V4.50).

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.

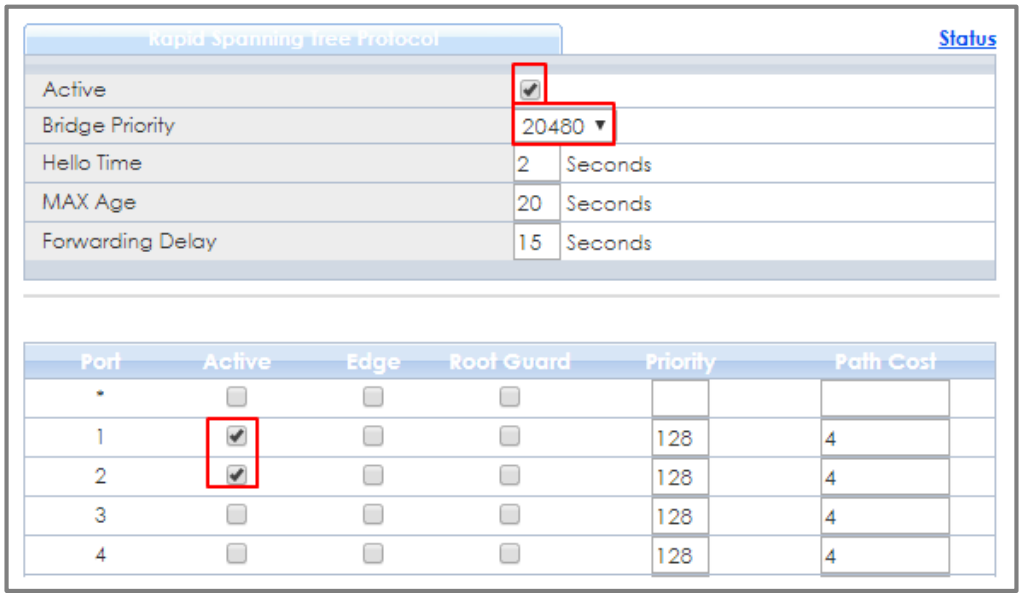
2 Set up **Switch-1**: Enter the web GUI. Go to **Menu > Advanced Application > Spanning Tree Protocol > Configuration**. Check if the Spanning Tree Configuration is **Rapid Spanning Tree**. If not, select it and click "**Apply**".

3 Set up **Switch-1**: Enter the web GUI. Go to **Menu > Advanced Application > Spanning Tree Protocol > RSTP**. Check the "**Active**" box. Set the Bridge Priority = **4096**. Active port **1**, **2**. Click "**Apply**".



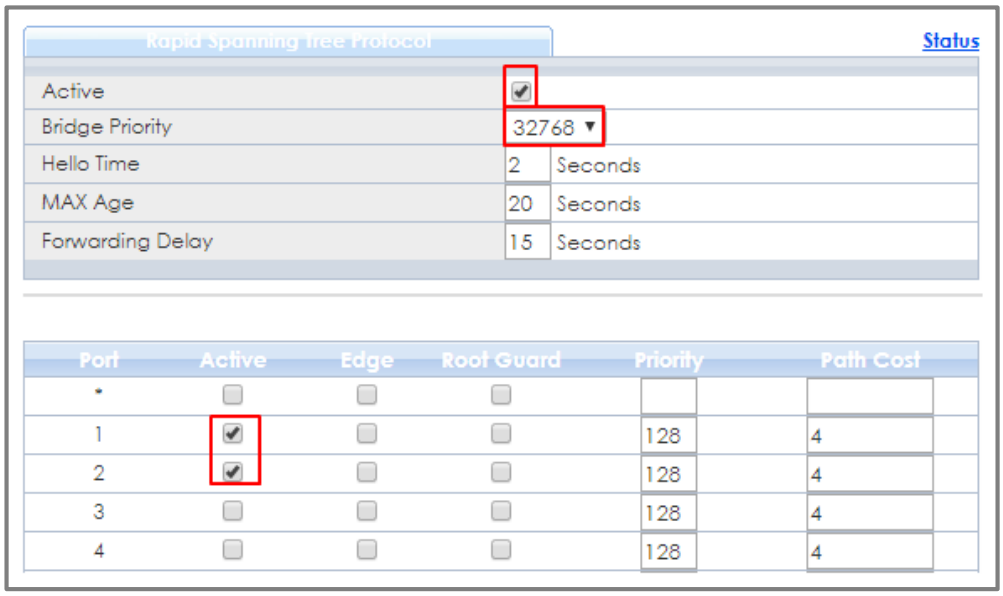
4 Set up **Switch-2**: Enter the web GUI. Go to **Menu > Advanced Application > Spanning Tree Protocol > Configuration**. Check if the Spanning Tree Configuration is **Rapid Spanning Tree**. If not, select it and click "**Apply**".

5 Set up **Switch-2**: Enter the web GUI. Go to **Menu > Advanced Application > Spanning Tree Protocol > RSTP**. Check the "**Active**" box. Set the Bridge Priority = **20480**. Active port **1**, **2**. Click "**Apply**".



6 Set up **Switch-3**: Enter the web GUI. 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**".

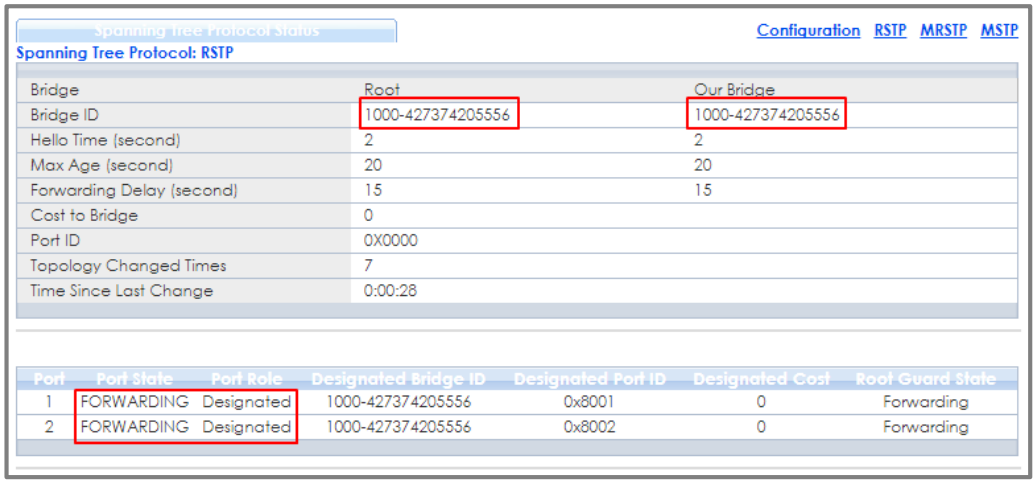
7 Set up **Switch-3**: Enter the web GUI. Go to **Menu > Advanced Application > Spanning Tree Protocol > RSTP**. Check the "**Active**" box. Set the Bridge Priority = **32768**. Active port **1**, **2**. Click "**Apply**".



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 > Advanced Application > Spanning Tree Protocol**. The Root Bridge ID and the Our Bridge ID should be the same. This means that Switch-1 is the Root Bridge. Both port 1 and 2 should be in **FORWARDING** state, while both their Port Roles are **Designated Ports**.



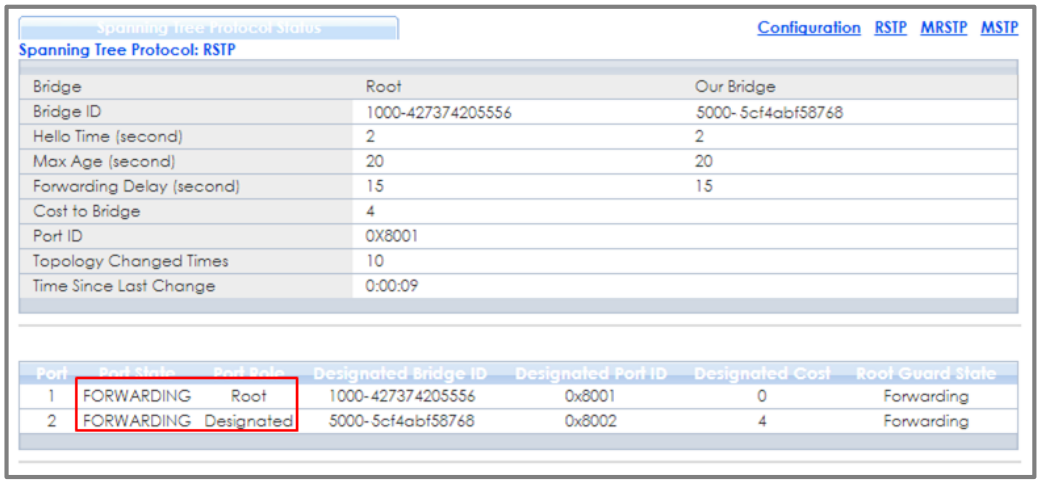
Spanning Tree Protocol Status — Configuration | RSTP | MRSTP | MSTP

Spanning Tree Protocol: RSTP

Bridge	Root	Our Bridge
Bridge ID	1000-427374205556	1000-427374205556
Hello Time (second)	2	2
Max Age (second)	20	20
Forwarding Delay (second)	15	15
Cost to Bridge	0	
Port ID	0X0000	
Topology Changed Times	7	
Time Since Last Change	0:00:28	

Port	Port State	Port Role	Designated Bridge ID	Designated Port ID	Designated Cost	Root Guard State
1	FORWARDING	Designated	1000-427374205556	0x8001	0	Forwarding
2	FORWARDING	Designated	1000-427374205556	0x8002	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 1 should be the **Root Port** in **FORWARDING** state, while port 2 should be a **Designated Port** also in **FORWARDING** state.



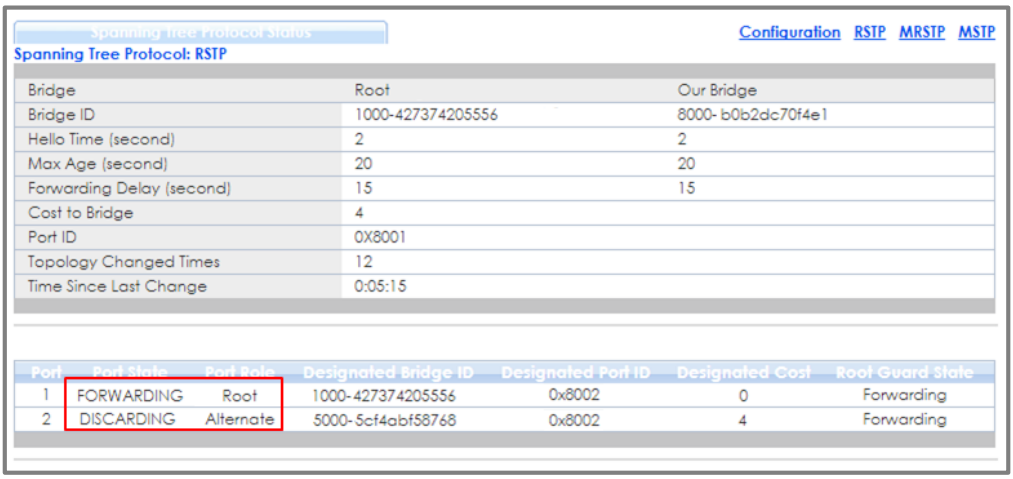
Spanning Tree Protocol Status — Configuration | RSTP | MRSTP | MSTP

Spanning Tree Protocol: RSTP

Bridge	Root	Our Bridge
Bridge ID	1000-427374205556	5000-5cf4abf58768
Hello Time (second)	2	2
Max Age (second)	20	20
Forwarding Delay (second)	15	15
Cost to Bridge	4	
Port ID	0X8001	
Topology Changed Times	10	
Time Since Last Change	0:00:09	

Port	Port State	Port Role	Designated Bridge ID	Designated Port ID	Designated Cost	Root Guard State
1	FORWARDING	Root	1000-427374205556	0x8001	0	Forwarding
2	FORWARDING	Designated	5000-5cf4abf58768	0x8002	4	Forwarding

3 Verify the status of **Switch-3**: Go to **Menu > Advanced Application > Spanning Tree Protocol.** Check the port status of Switch-3. Port 1 should be the **Root Port** in **FORWARDING** state, while Port 2 is an **Alternate Port** in **DISCARDING** state.



Spanning Tree Protocol Status

Configuration RSTP MRSTP MSTP

Spanning Tree Protocol: RSTP

Bridge	Root	Our Bridge
Bridge ID	1000-427374205556	8000- b0b2dc70f4e1
Hello Time (second)	2	2
Max Age (second)	20	20
Forwarding Delay (second)	15	15
Cost to Bridge	4	
Port ID	0X8001	
Topology Changed Times	12	
Time Since Last Change	0:05:15	

Port	Port State	Port Role	Designated Bridge ID	Designated Port ID	Designated Cost	Root Guard State
1	FORWARDING	Root	1000-427374205556	0x8002	0	Forwarding
2	DISCARDING	Alternate	5000-5cf4abf58768	0x8002	4	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.

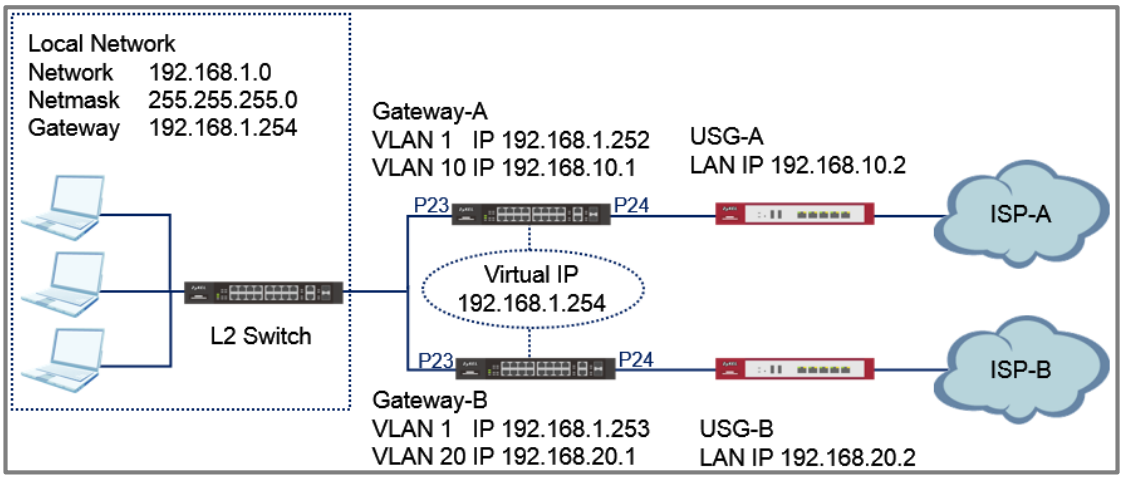


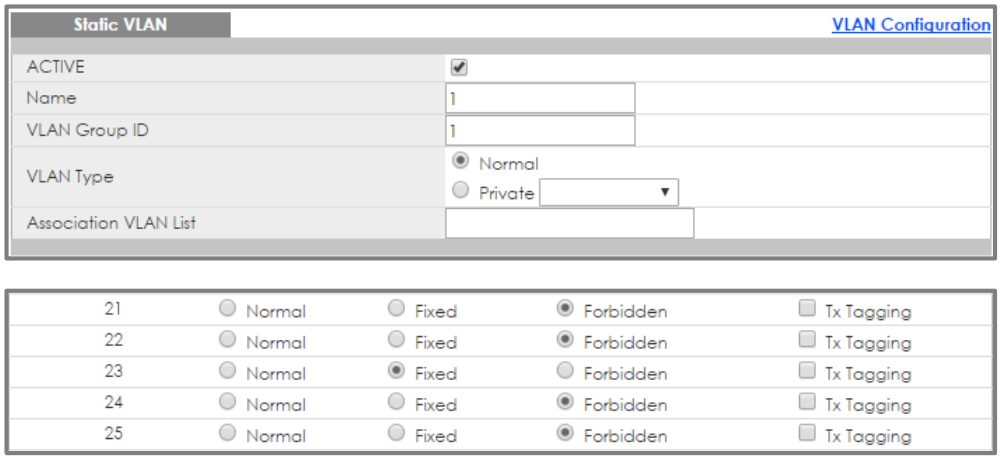
Figure 14 Two gateways running VRRP on the same LAN

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 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 XGS4600 series switch.

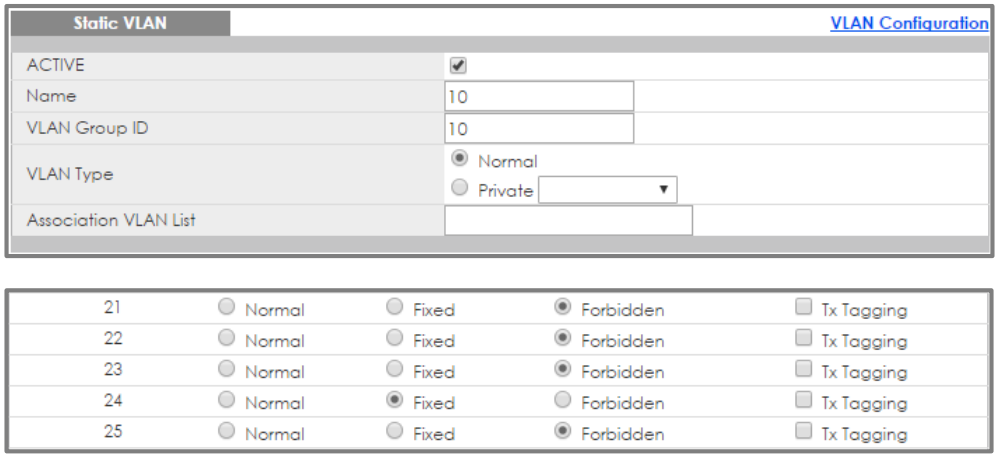
3.3.1 Configuration in the Gateway-A

1 Access the Gateway-A's web GUI.

2 Go to **Advance Application > VLAN > VLAN Configuration > Static VLAN Setup**. Create/Edit VLAN 1 to make sure only Port 23 is a fixed port. Click **Add**.

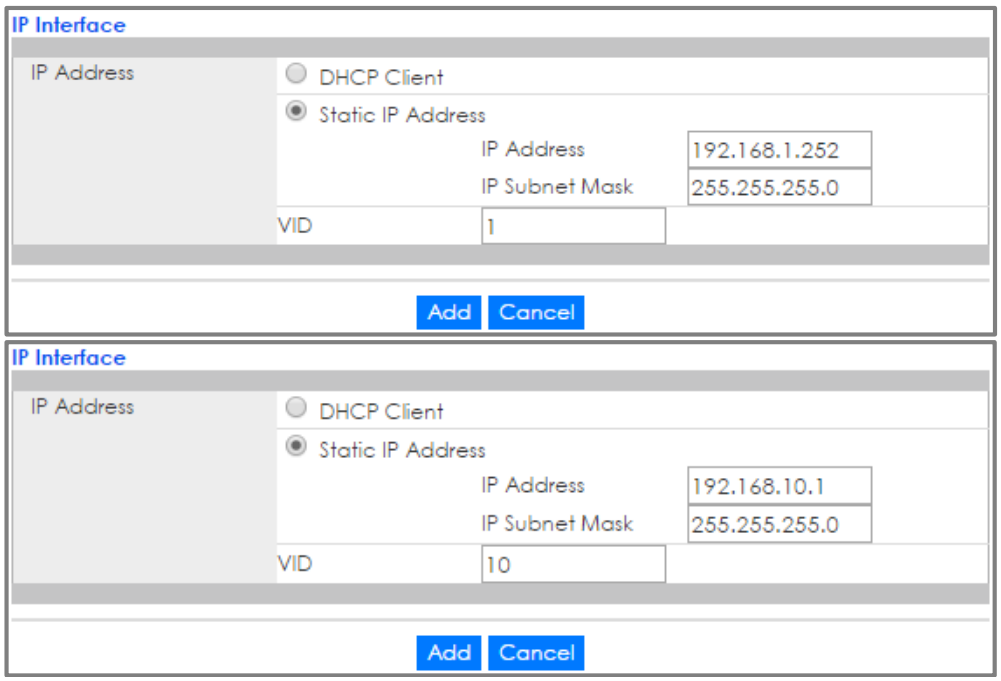


3 Go to **Advance Application > VLAN > VLAN Configuration > Static VLAN Setup**. Create/Edit VLAN 10 to make sure only Port 24 is a fixed port. Click **Add**.

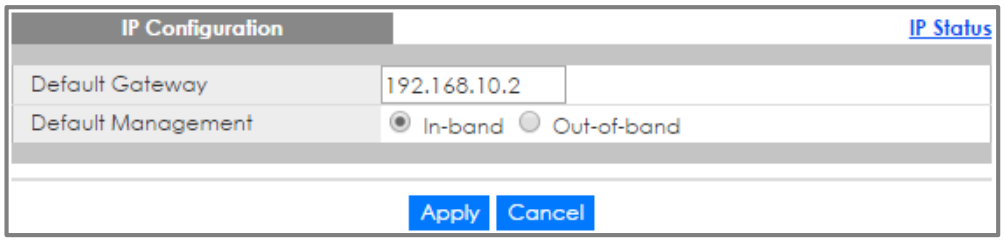


4 Go to **Advance Application > VLAN > VLAN Configuration > VLAN Port Setup**. Configure port 24 with PVID 10. Click **Apply**.

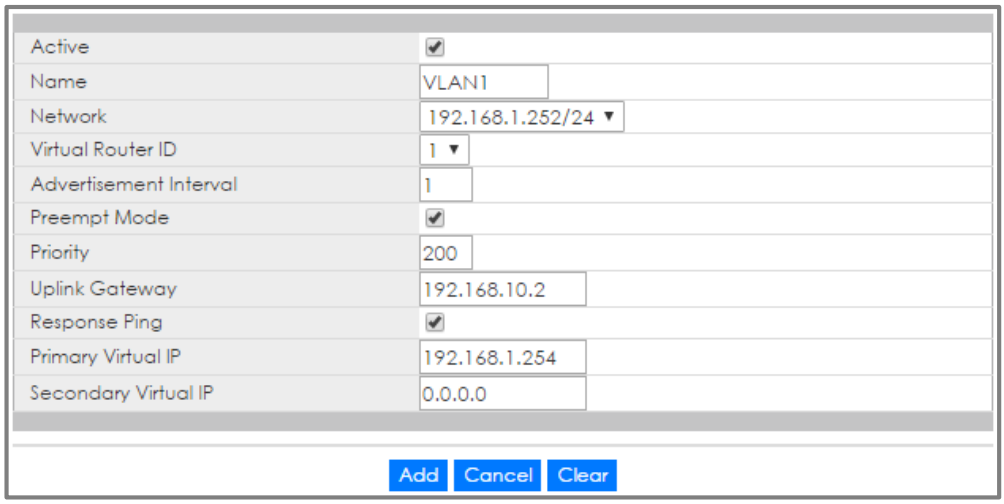
5 Go to **Basic Setting > IP Setup**. Configure the IP address for VLAN 1. Click **Add** and do the same for VLAN 10.



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



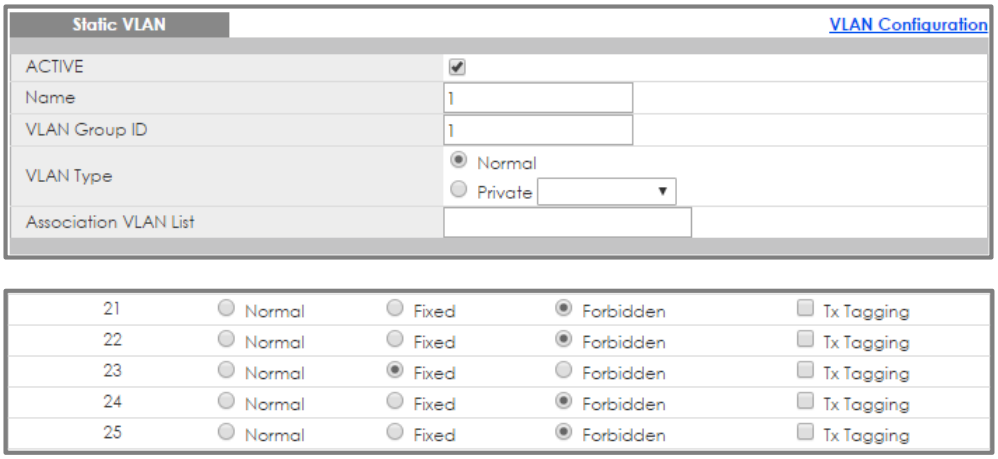
7 Go to **IP Application > VRRP > Configuration**. Enable VRRP for network "192.168.1.252/24". Make sure that the priority is "200". Click **Add**.



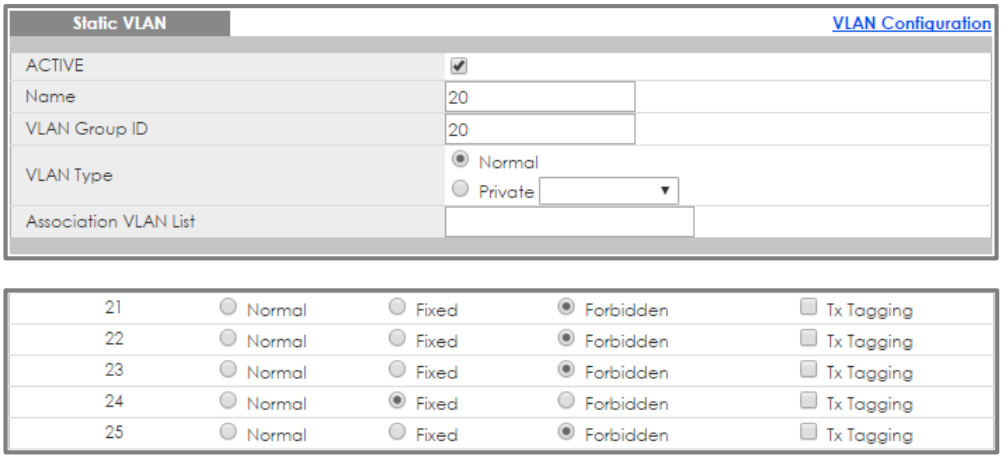
3.3.2 Configuration in the Gateway-B

1 Access the Gateway-B's web GUI.

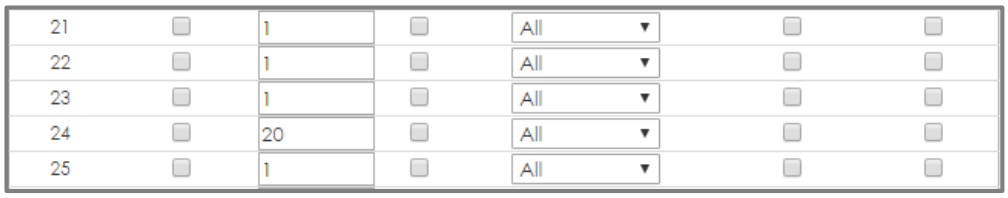
2 Go to **Advance Application > VLAN > VLAN Configuration > Static VLAN Setup**. Create/Edit VLAN 1 to make sure only Port 23 is a fixed port. Click **Add**.



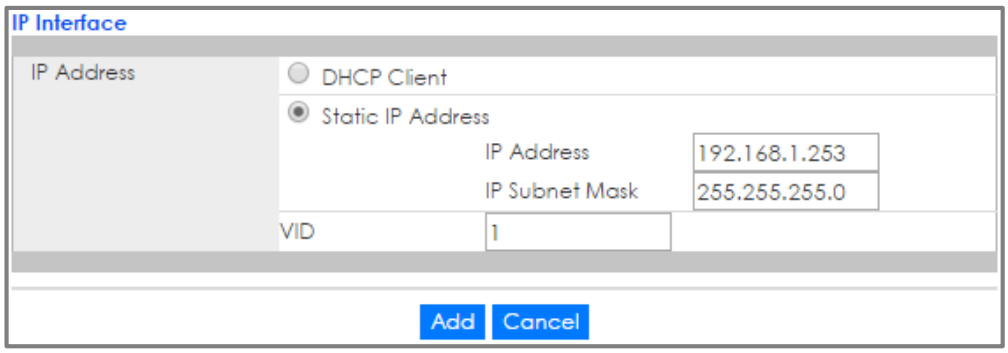
3 Go to **Advance Application > VLAN > VLAN Configuration > Static VLAN Setup**. Create/Edit VLAN 20 to make sure only Port 24 is a fixed port. Click **Add**.

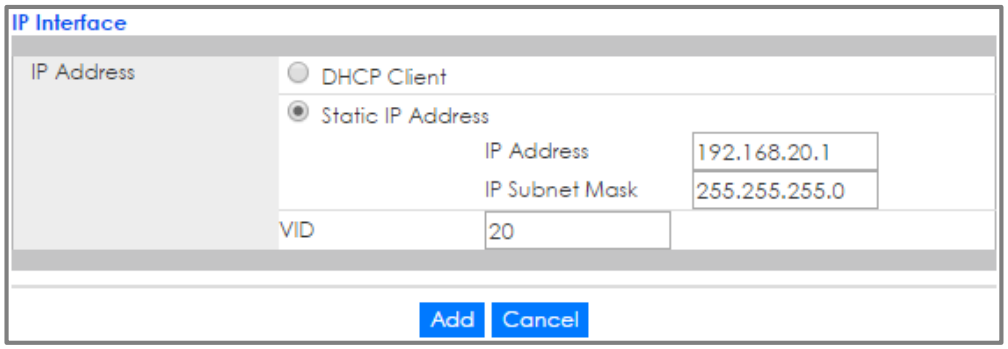


4 Go to **Advance Application > VLAN > VLAN Configuration > VLAN Port Setup**. Configure port 24 with PVID 20. Click **Apply**.

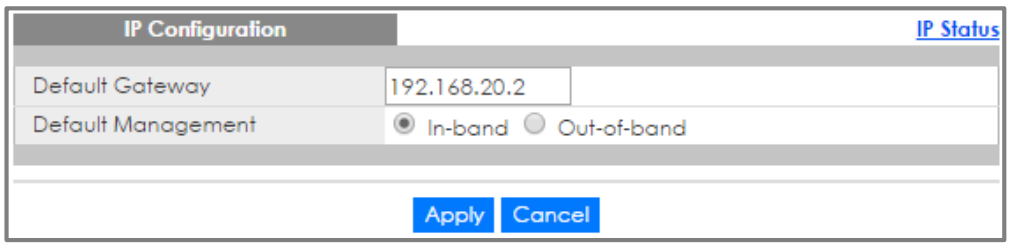


5 Go to **Basic Setting > IP Setup**. Configure the IP address for VLAN 1. Click **Add** and do the same for VLAN 20.

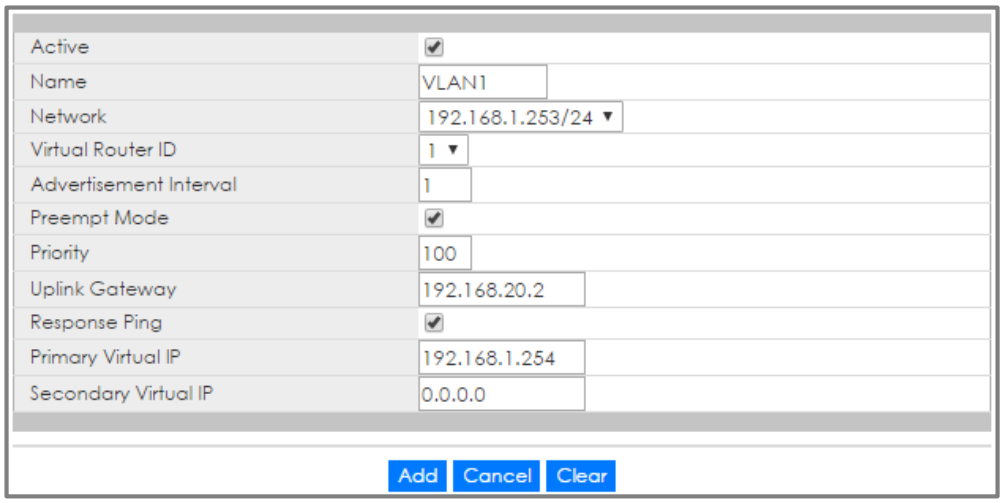




6 Go to **Basic Setting > IP Setup**. Configure the Default Gateway. Click **Apply**.



7 Go to **IP Application > VRRP > Configuration**. Enable VRRP for network "192.168.1.252/24". Click **Add**.



3.3.3 Test the Result

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

VRRP Status — Configuration

Index	Network	VRID	VR Status	Uplink Status
1	192.168.1.252/24	1	Master	Alive

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

VRRP Status — Configuration

Index	Network	VRID	VR Status	Uplink Status
1	192.168.1.253/24	1	Backup	Alive

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

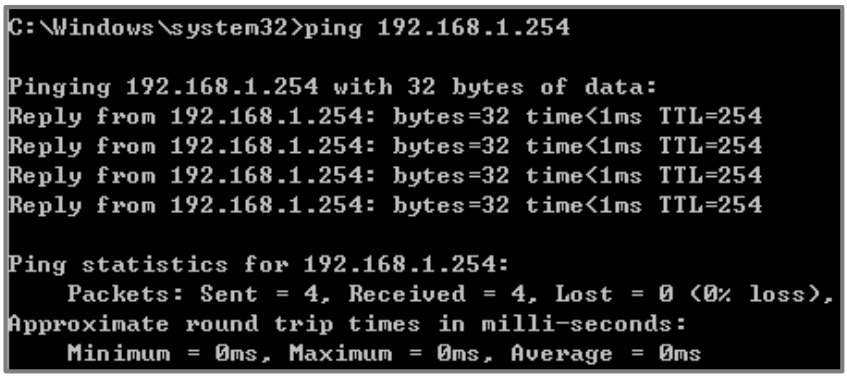
Routing Table Status

Index	Destination	Gateway	Interface	Metric	Type	Uptime
1	192.168.1.0/24	192.168.1.252	192.168.1.252	1	LOCAL	0:00:54
2	192.168.10.0/24	192.168.10.1	192.168.10.1	1	LOCAL	0:00:44
3	127.0.0.0/16	127.0.0.1	127.0.0.1	1	LOCAL	138:42:02
4	default	192.168.10.2	192.168.10.1	1	STATIC	0:00:23

Routing Table Status

Index	Destination	Gateway	Interface	Metric	Type	Uptime
1	192.168.1.0/24	192.168.1.253	192.168.1.253	1	LOCAL	0:04:41
2	192.168.20.0/24	192.168.20.1	192.168.20.1	1	LOCAL	0:04:29
3	127.0.0.0/16	127.0.0.1	127.0.0.1	1	LOCAL	139:13:20
4	default	192.168.20.2	192.168.20.1	1	STATIC	0:03:45

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



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 be 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 (FTPServer). PC will either be uploading files or downloading files from the FTP Server.

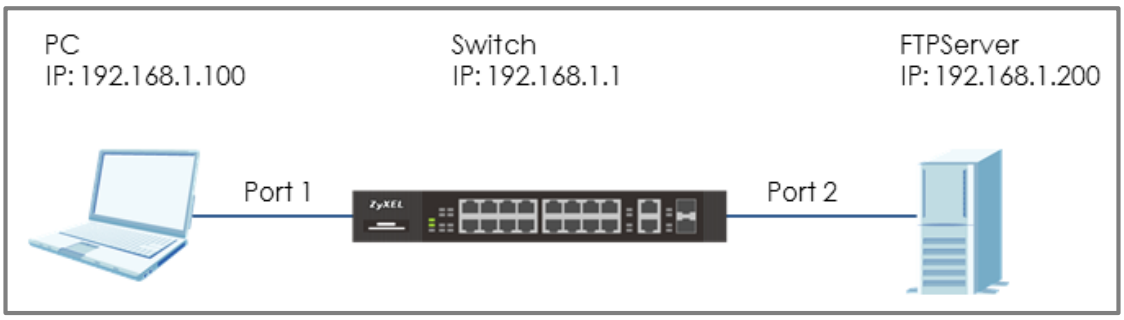
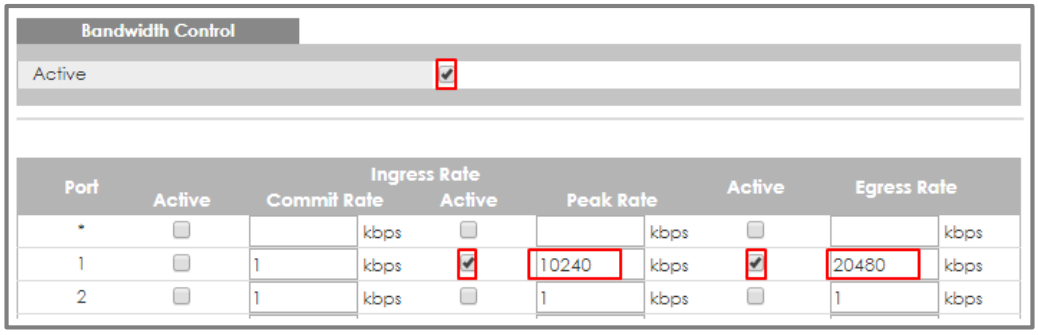


Figure 15 Configure bandwidth control to limit the traffic rate

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 XGS4600-32 (Firmware Version: V4.50).

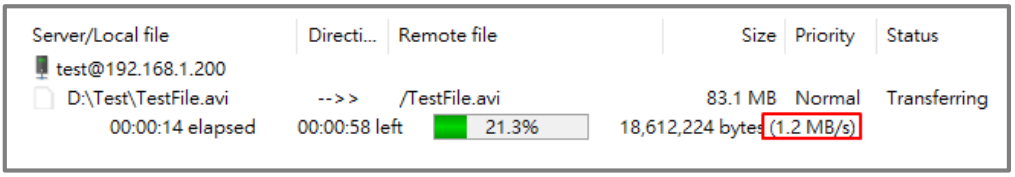
3.4.1 Configure Switch

1 Enter the web GUI. Go to **Menu > Advanced Application > Bandwidth Control**. Check the "**Active**" box. 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**".

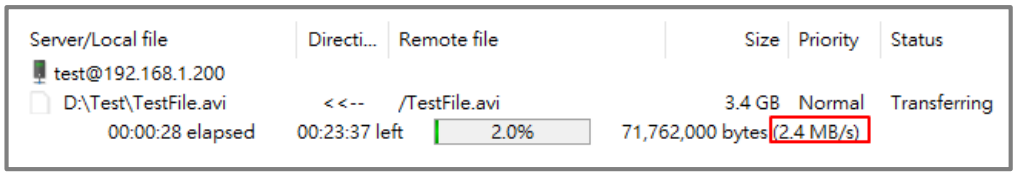


3.4.2 Test the Result

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).



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).



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.

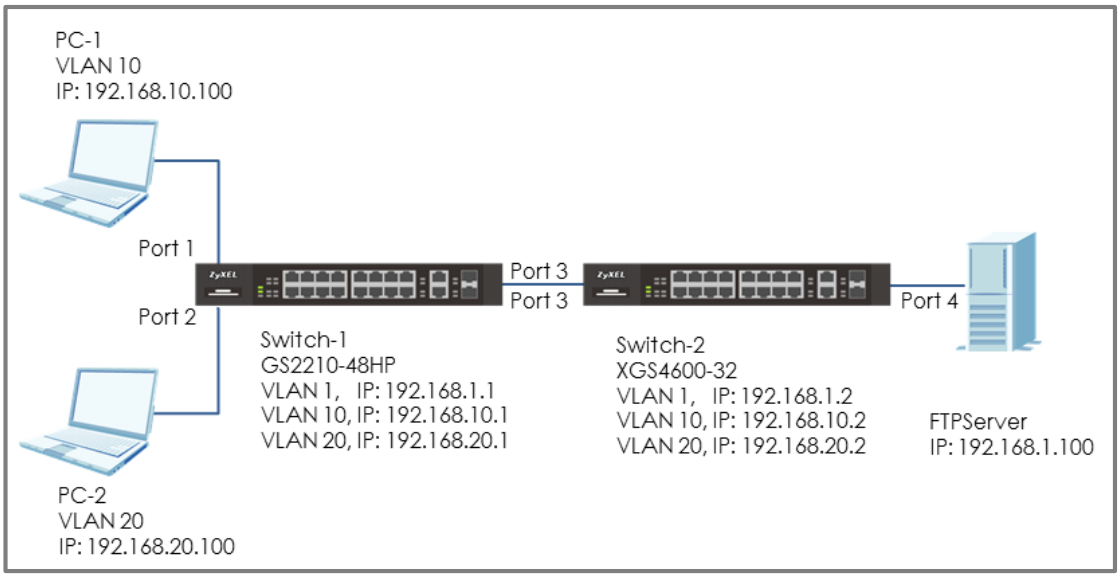


Figure 16 Configure ACL to rate limit VLAN traffic

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 XGS4600-32 (Firmware Version: V4.50) and GS2210-48HP (Firmware Version: V4.30).

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**).

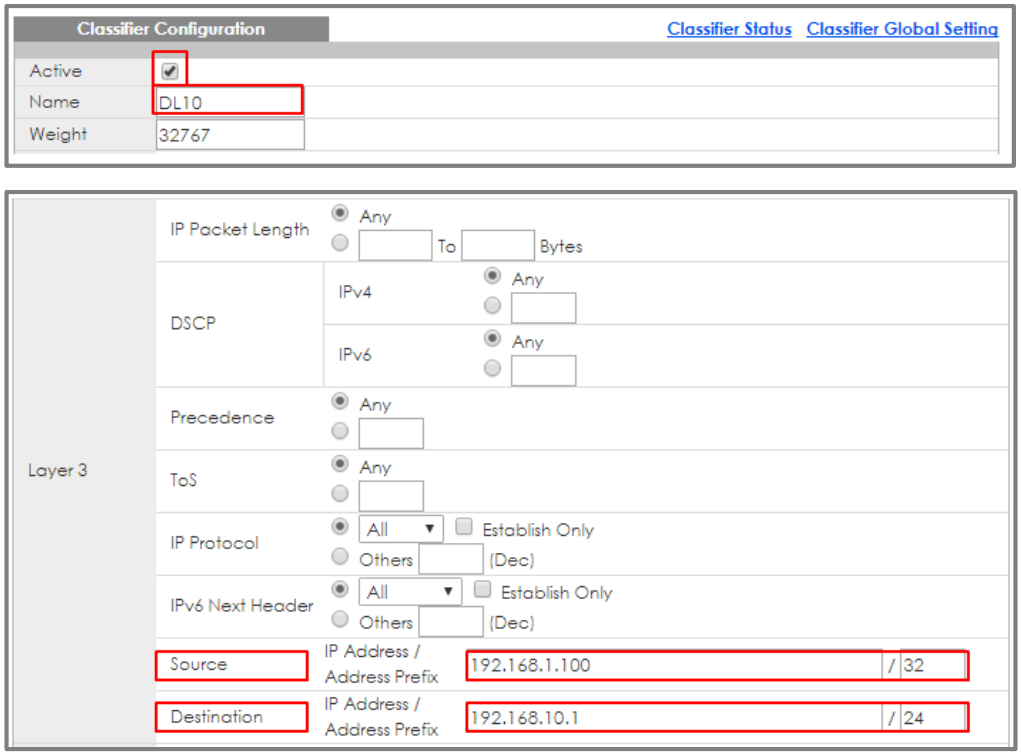
2 Configure the route traffic on Switch-1 and Switch-2 (Please refer to the topic: **2.2 How to configure the switch to route traffic across VLANs**)

3.5.2 Configure the Classifier

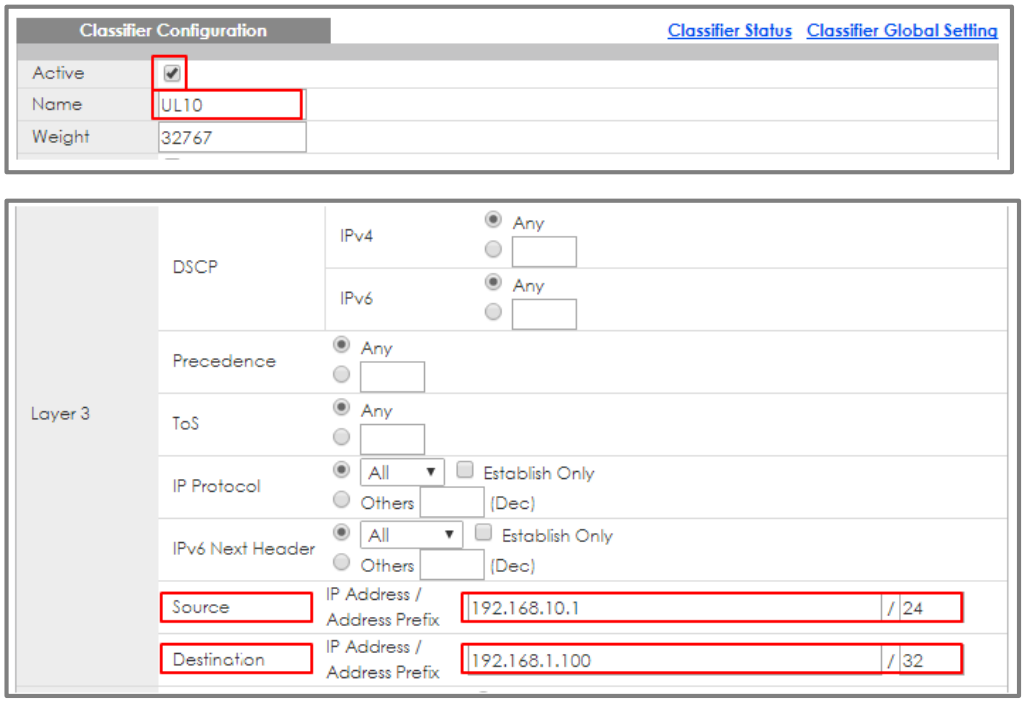
1 Set up the **Classifier** on Switch-2: Go to **Menu > Advanced Application > Classifier > Classifier Configuration**. Set up 4 Classifier: Classifier for download and upload in VALN 10 and VLAN 20. Therefore, there are total 4 Classifiers.

> 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: Check the "Active" box 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".



3 The Classifier for upload traffic in VLAN 10: Check the "Active" box 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".



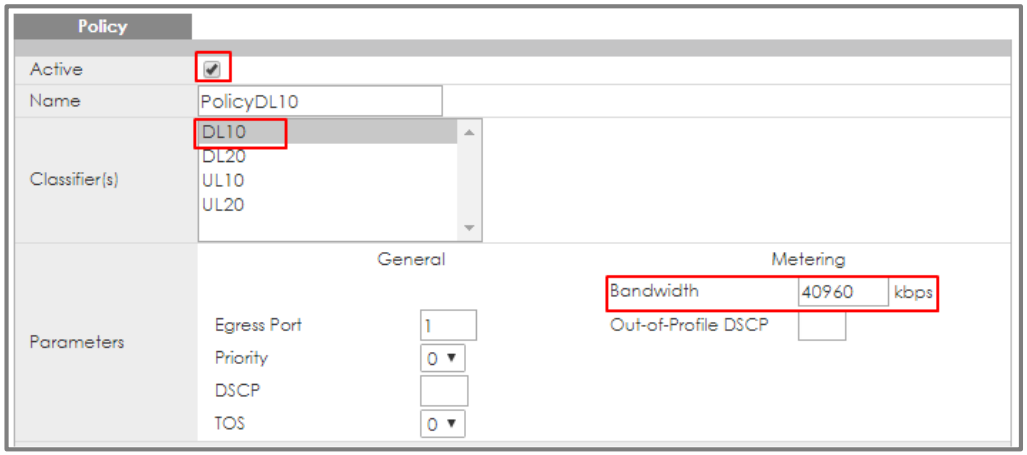
4 The Classifier of download in VLAN 20: Check the "Active" and key in the Name. Set **Layer 3 > Destination** as **192.168.20.0/24** (Means the destination is in VLAN 20) and **Source** as 192.168.1.100/32 (Means the source is FTPServer). Press "Add".

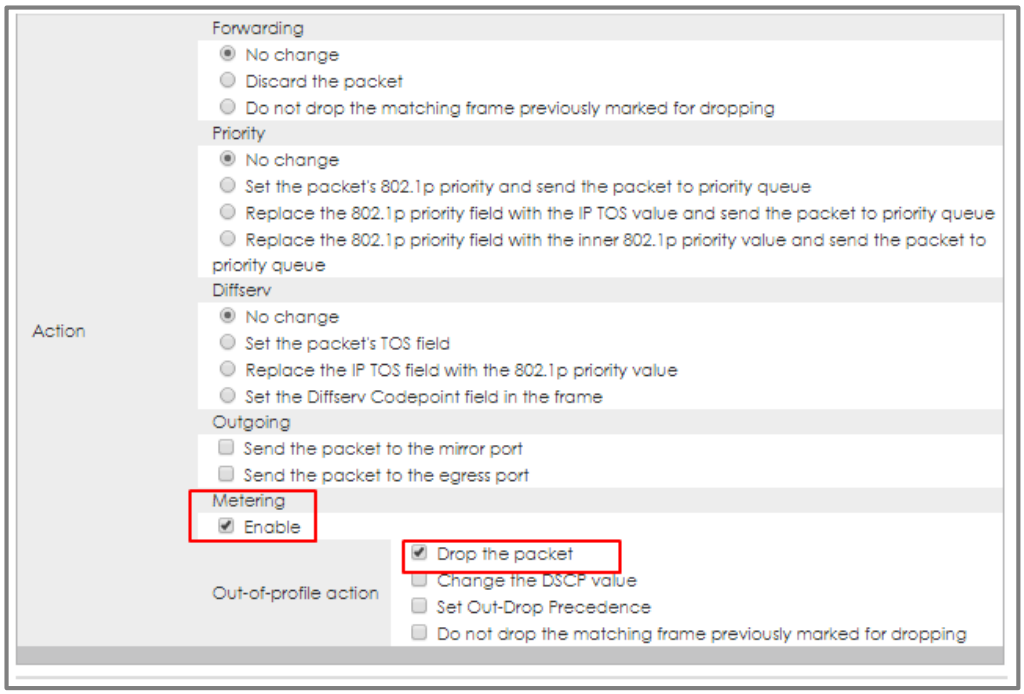
5 The Classifier of upload in VLAN 20: Check the "Active" and key in the Name. Set **Layer 3 > Destination** as **192.168.1.100/32** (Means the destination is FTPServer) and **Source** as **192.168.20.0/24** (Means the source is from VLAN 20). Press "Add".

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 > Advanced Application > Policy Rule**.

2 The Policy Rule of download traffic in VLAN 10: Check the "Active" box 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".





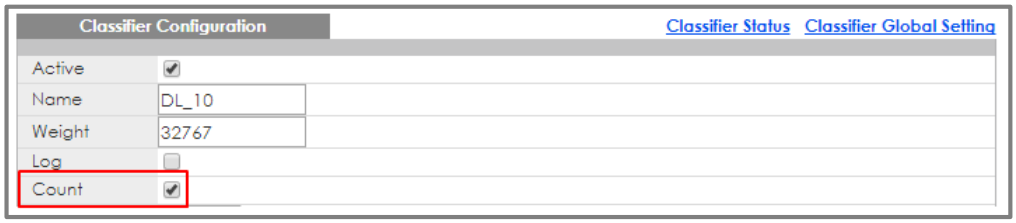
3 The Policy Rule of upload in VLAN 10: Check the "Active" and key in the Name. Select the Classifier of upload in VLAN 10 (UP10). Set up the action to do if match this Classifier: **Bandwidth Metering**=20480 kbps. Enable **Metering** and set the **Out-of-profile action** as "**Drop the packet**". Press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

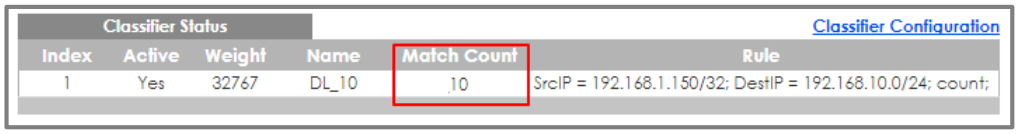
4 The Policy Rule of download in VLAN 20: Check the "Active" and key in the Name. Select the Classifier of download in VLAN 20 (DP20). Set up the action to do if match this Classifier: **Bandwidth Metering**=20480 kbps. Enable **Metering** and set the **Out-of-profile action** as "**Drop the packet**".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

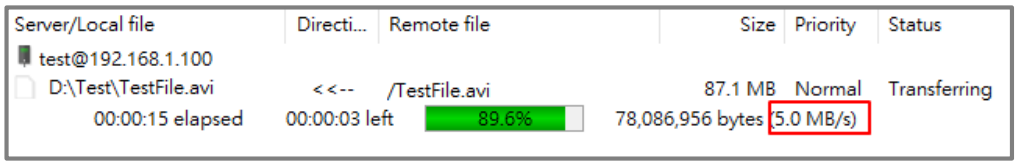
3.5.4 Test the Result

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.

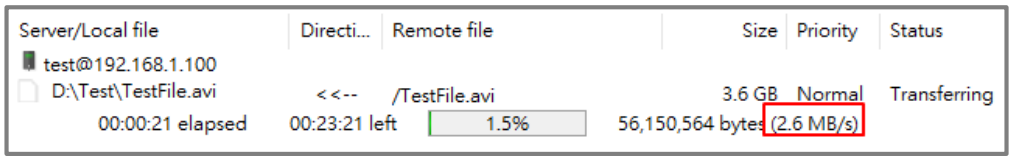




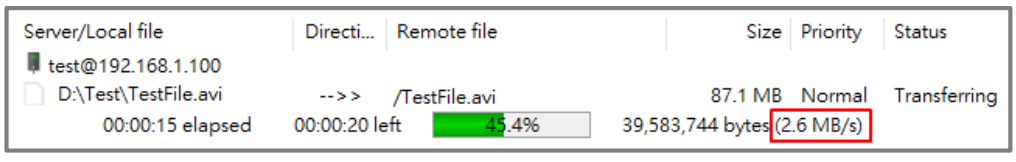
2 Use PC-1 to download a file from the FTP Server. Transfer rate should be more or less 5 MB/s (or 40960 Mb/s).



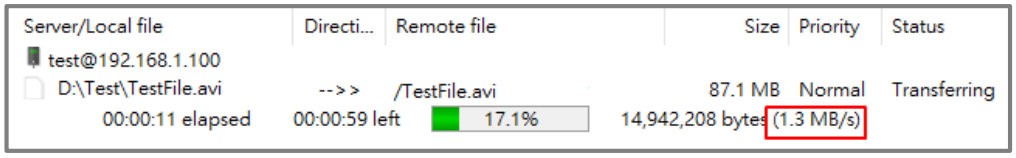
3 Use PC-1 to upload a file to the FTP Server. Transfer rate should be more or less 2.6 MB/s (or 20480 Mb/s).



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).



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).

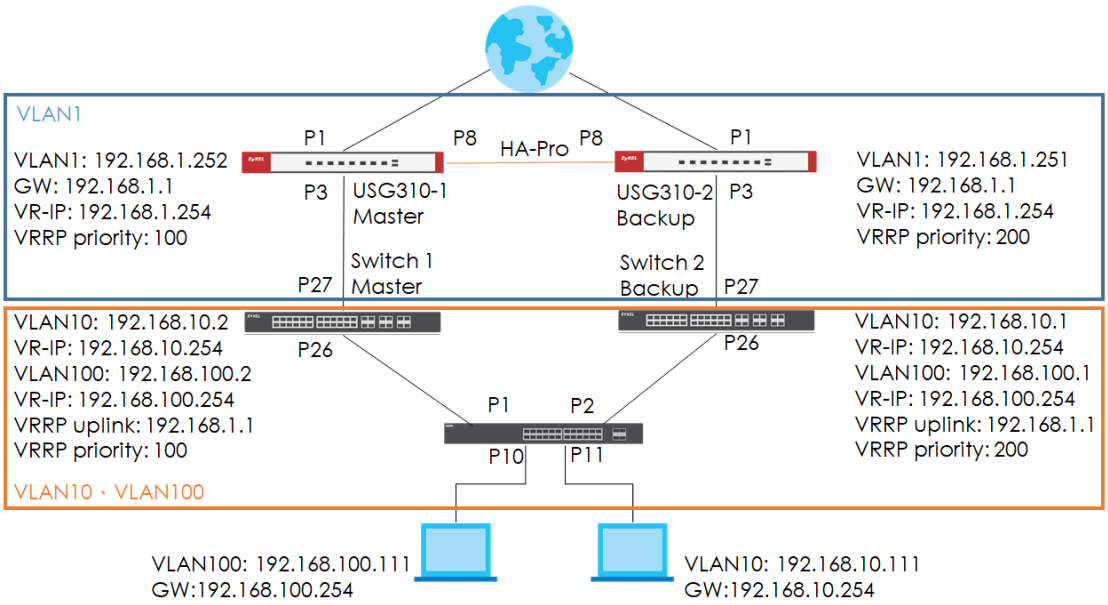


3.5.5 What Could Go Wrong

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.

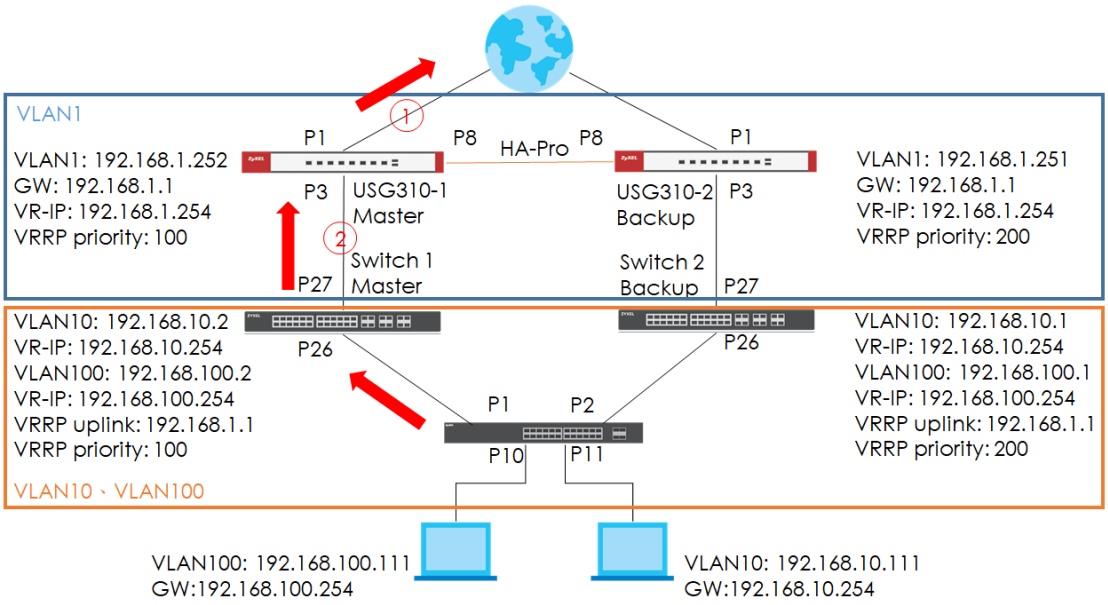


Figure 1

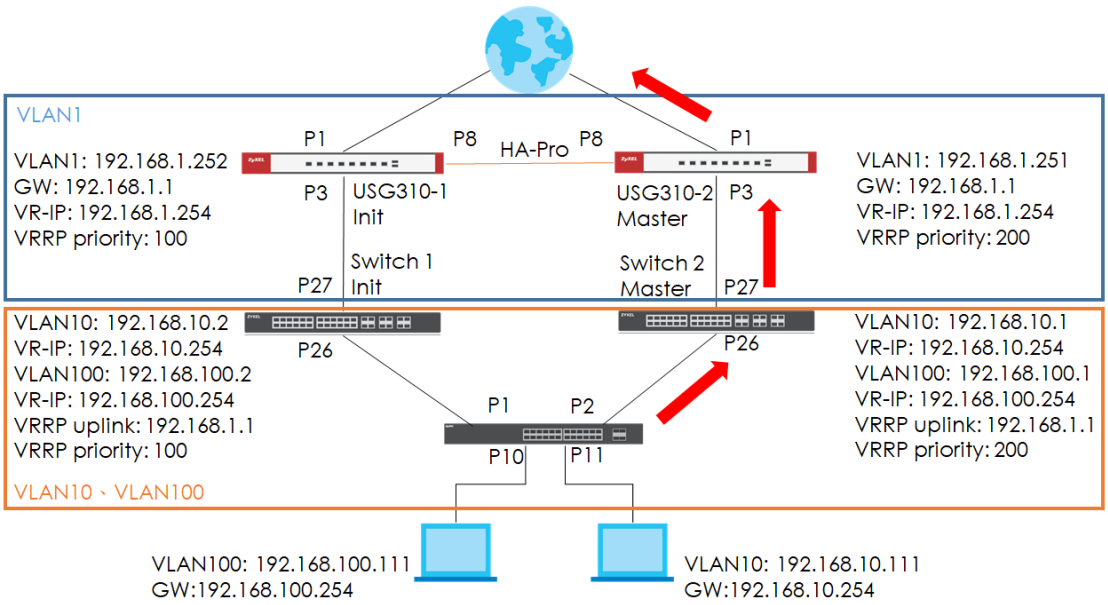


Figure 2

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

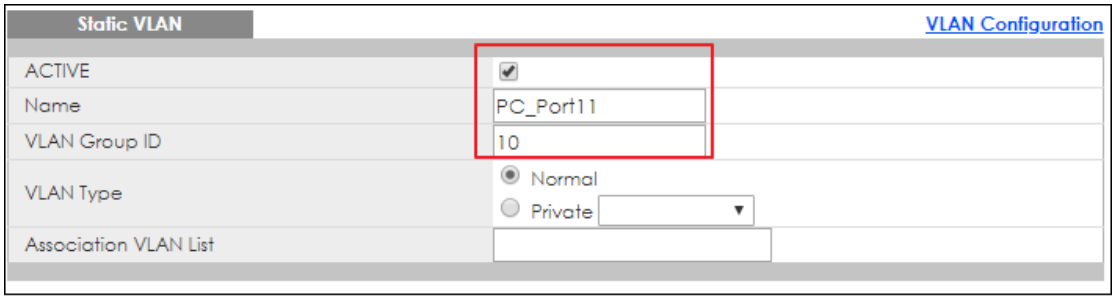
L3 Switch:

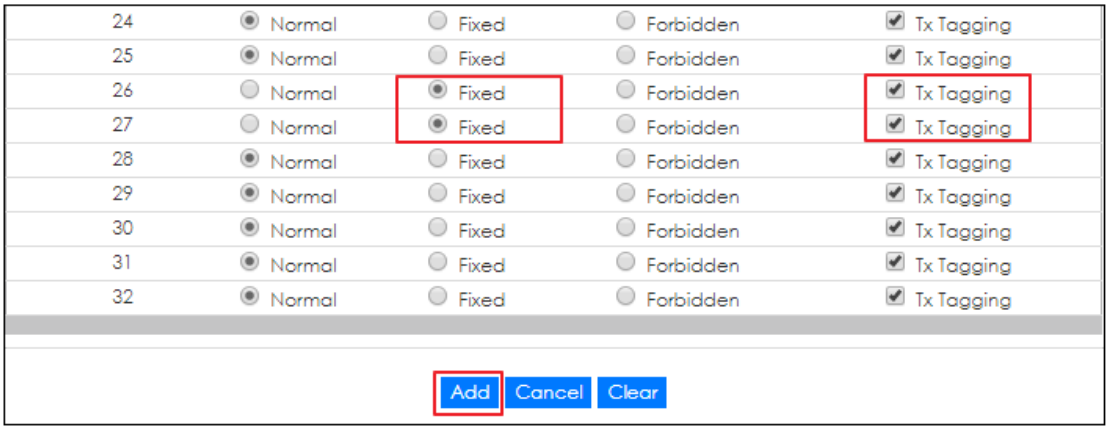
1. Access switch-1(Master) web GUI

2. Go to **Advanced Application > VLAN > VLAN Configuration >Static VLAN Setup**

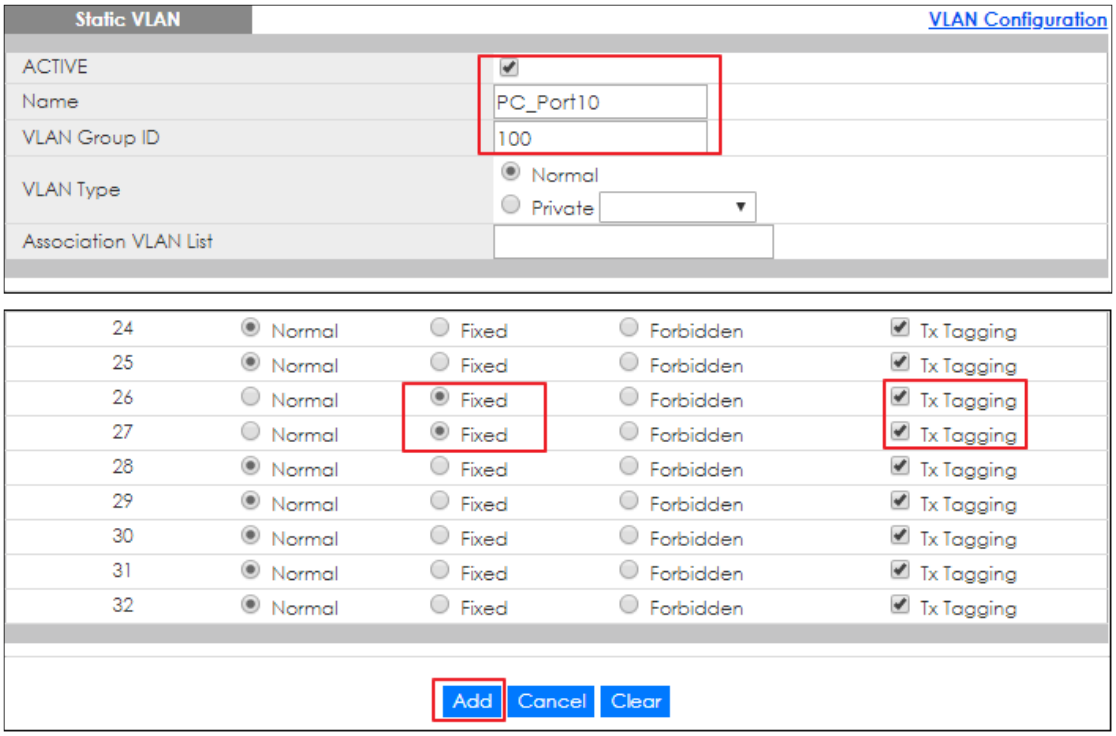
3. Create VLAN 10 and VLAN 100 for host.

VLAN 10:



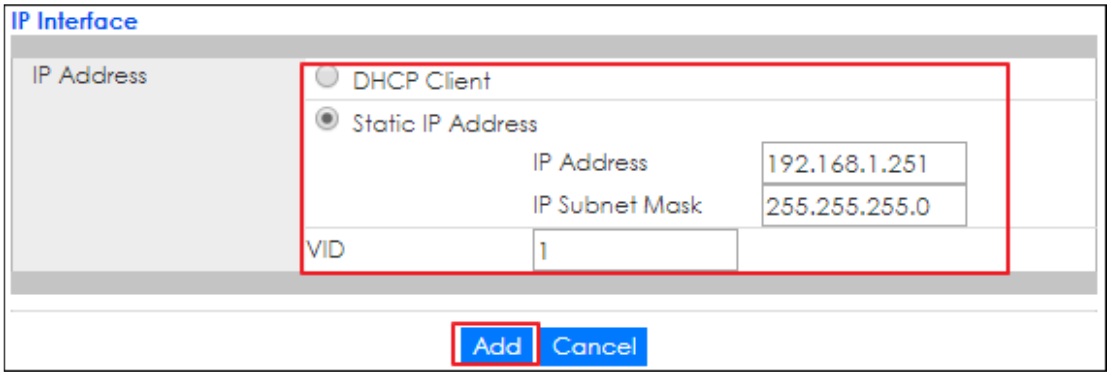


VLAN 100:



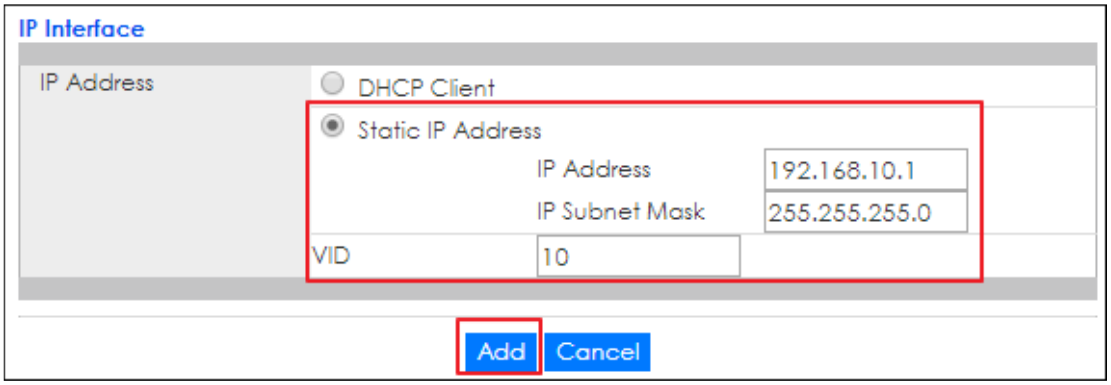
4. Got to the **Basic Setting >IP Setup > IP Configuration**

5. Configure IP interface to VLAN 1 for uplink.

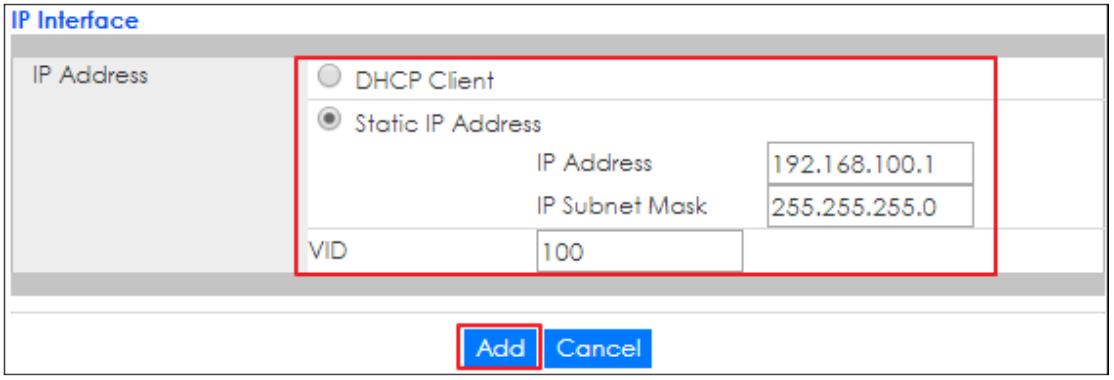


6. Configure IP interface to VLAN 10 & VLAN 100 for hosts.

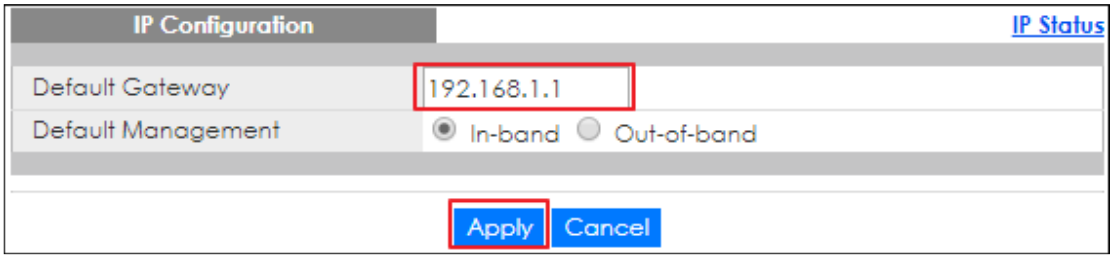
VLAN 10:



VLAN 100:



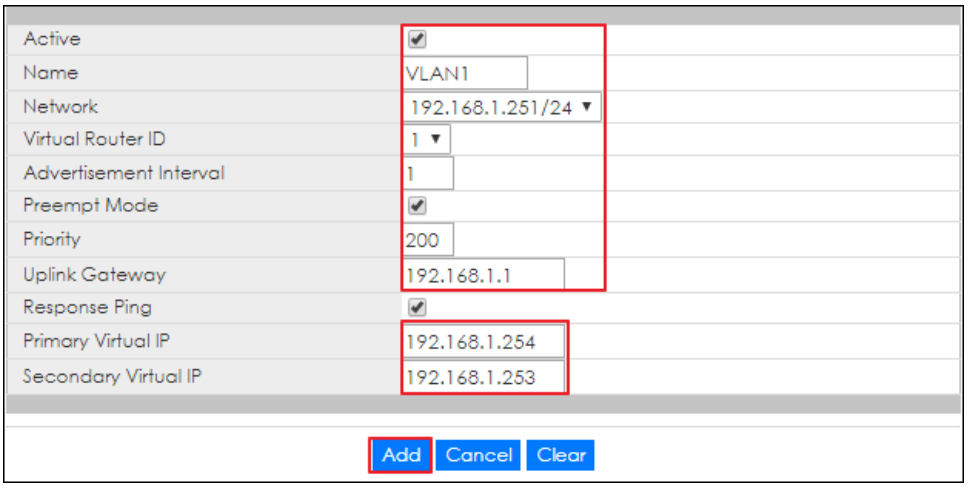
7. Configure IP default gateway for VLAN 1 interface.



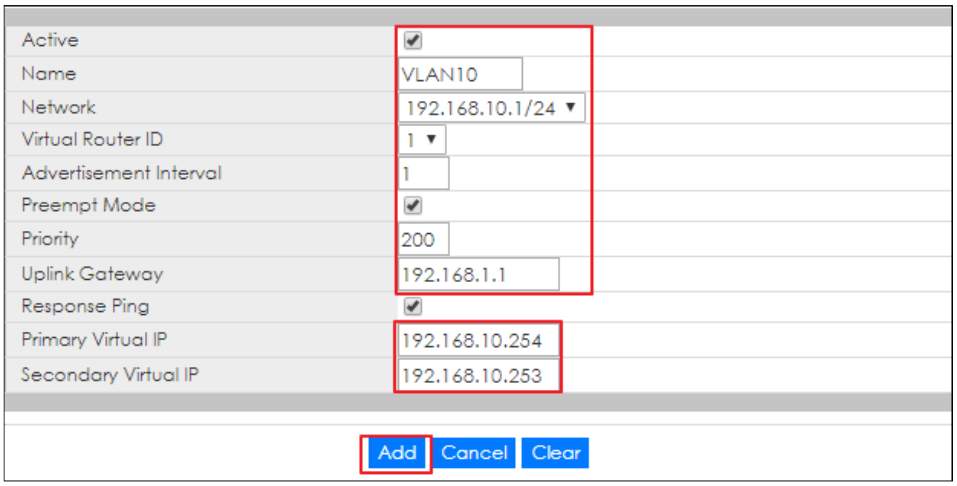
8. Go to **IP Application > VRRP > Configuration**

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.

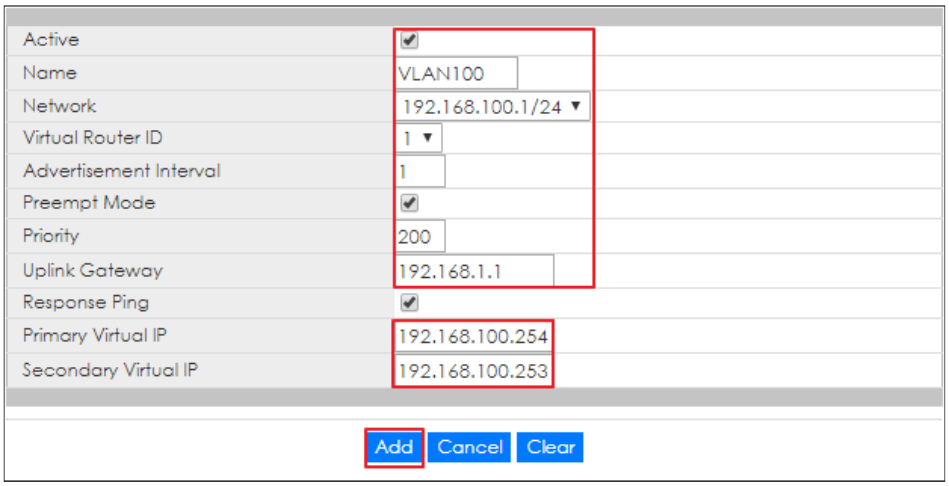
VLAN 1:



VLAN 10:



VLAN 100:

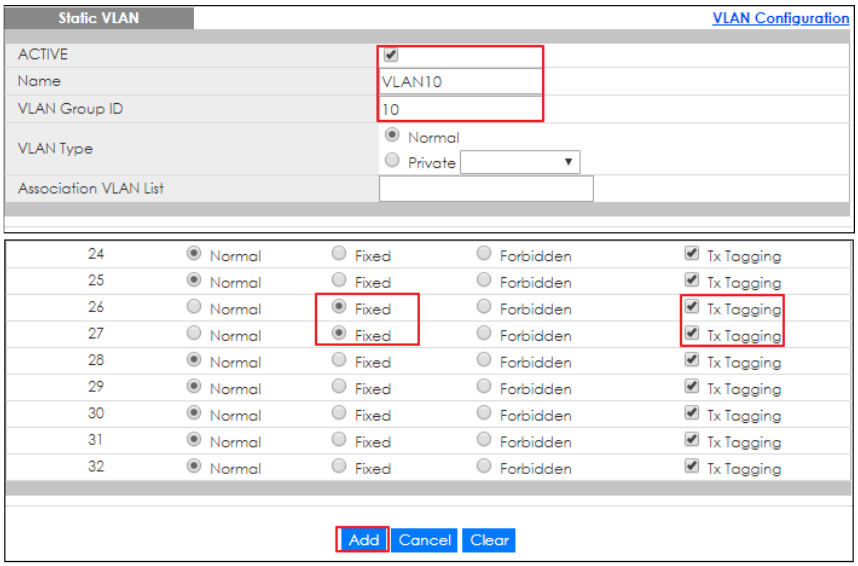


10. Access the Switch-2 (Backup) web GUI.

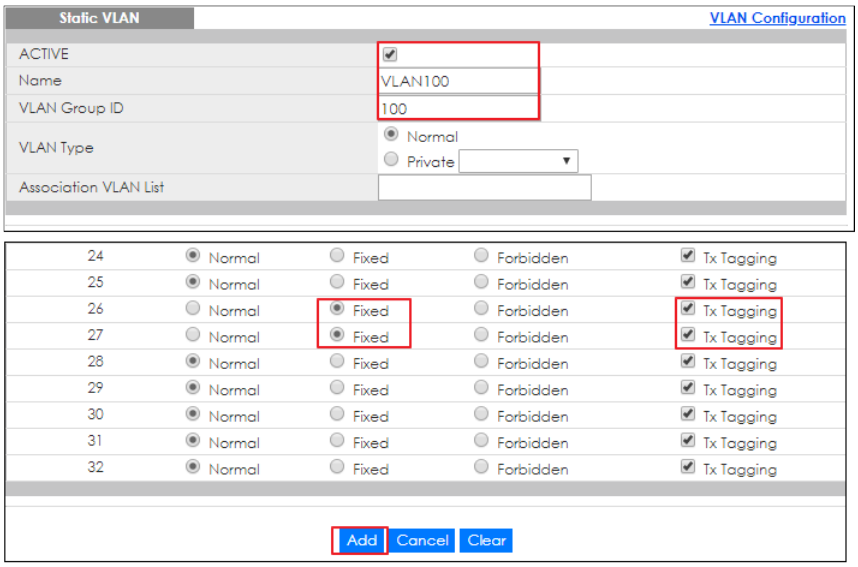
11. Go to **Advanced Application > VLAN > VLAN Configuration >Static VLAN Setup**

12. Create VLAN 10 & VLAN 100 for hosts.

VLAN 10:



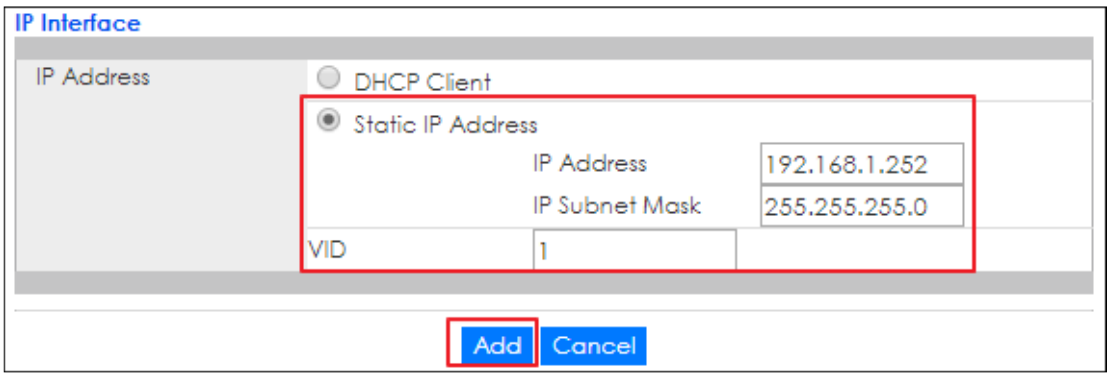
VLAN 100:



13. Go to **Basic Settings > IP Setup > IP Configuration**

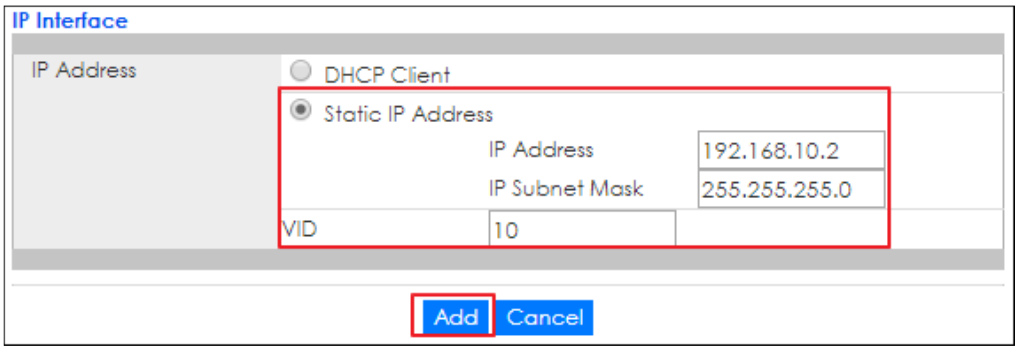
14. Configure IP interface on VLAN 1 for uplink.

VLAN 1:

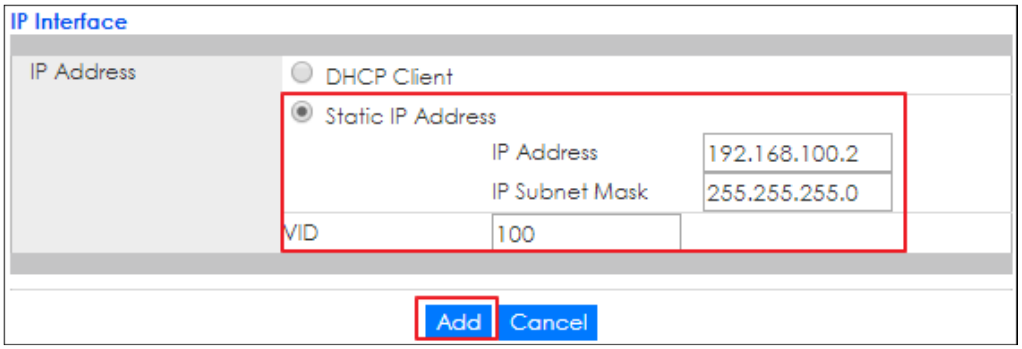


15. Configure IP interface on VLAN 10 & VLAN 100 for hosts.

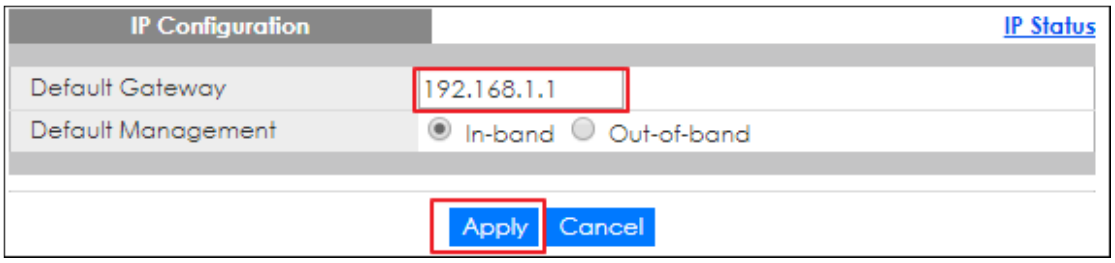
VLAN 10:



VLAN 100:



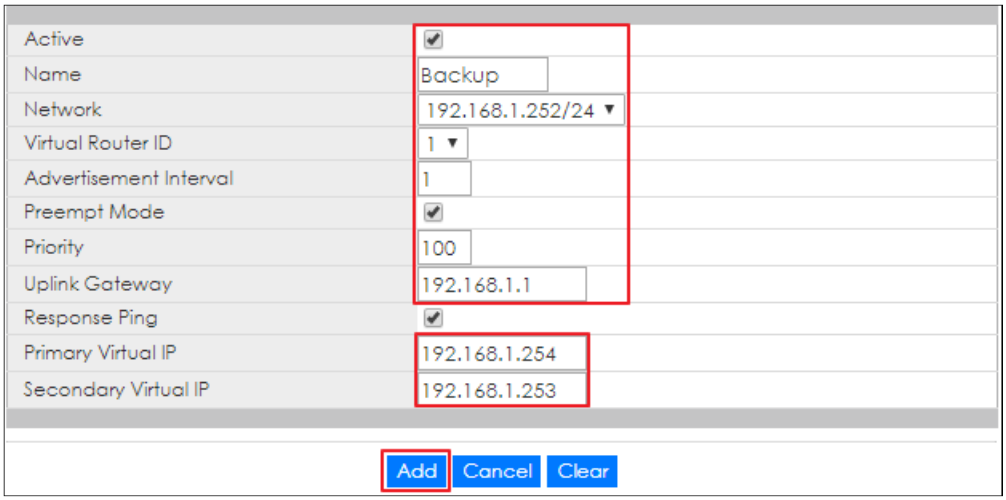
16. Configure IP default gateway on VLAN 1 for the uplink.



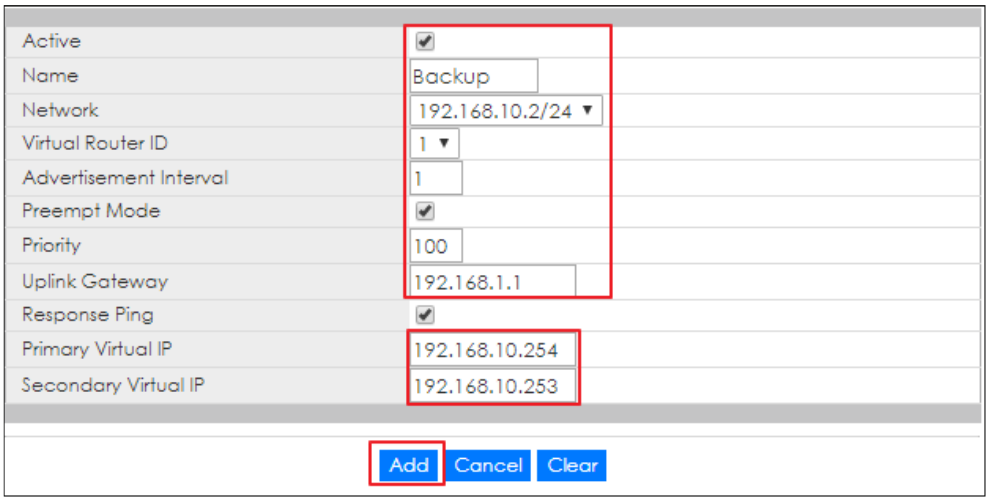
17. Go to **IP Application > VRRP > Configuration**

18. 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.

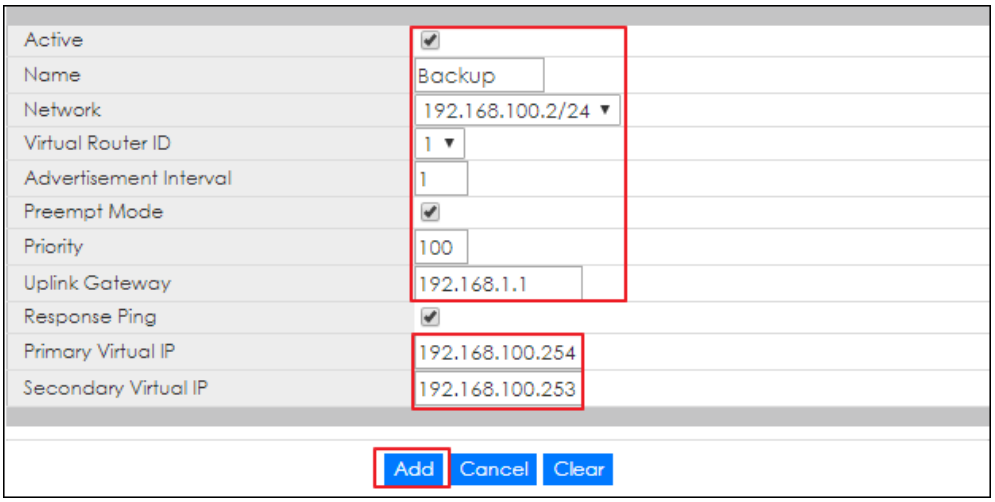
VLAN 1:



VLAN 10:



VLAN 100:



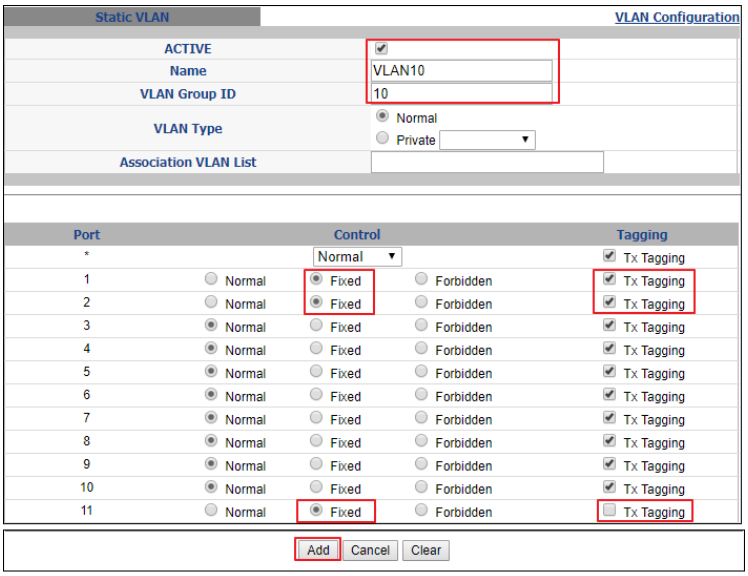
L2 switch:

1. Access layer 2 switch via web GUI.

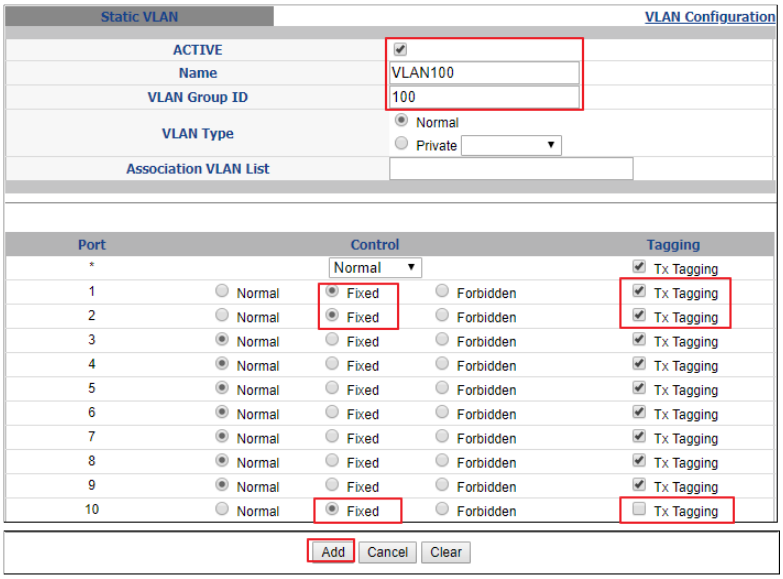
2. Go to **Advanced Application > VLAN > VLAN Configuration >Static VLAN Setup.**

3. Configure VLAN 10 & VLAN 100 for hosts.

VLAN 10:



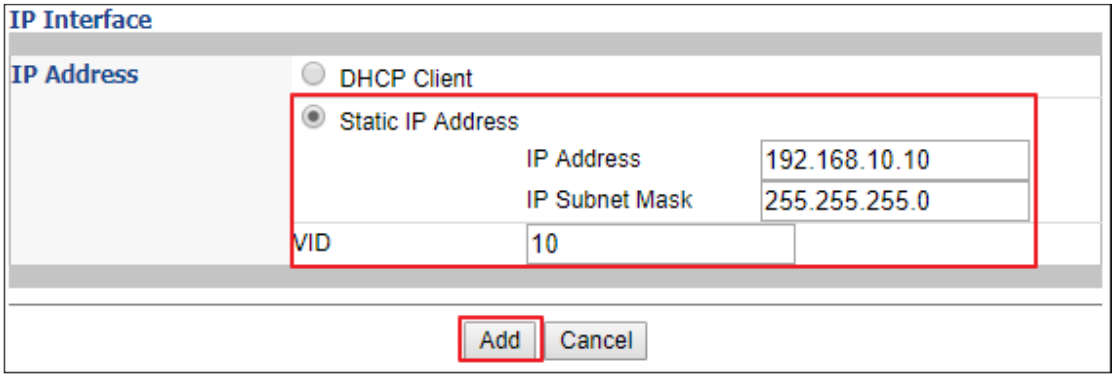
VLAN 100:



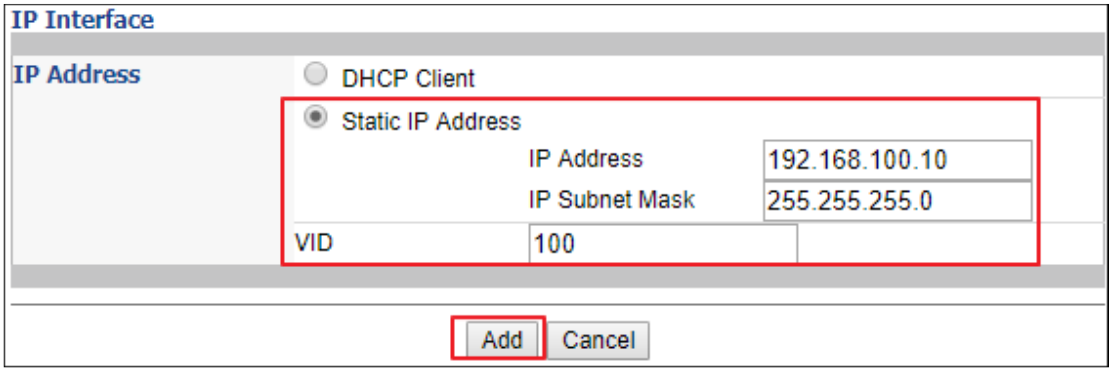
4. Go to **Basic Setting > IP Setup > IP Configuration**

5. Configure IP interface for VLAN 10 & VLAN 100

VLAN 10:

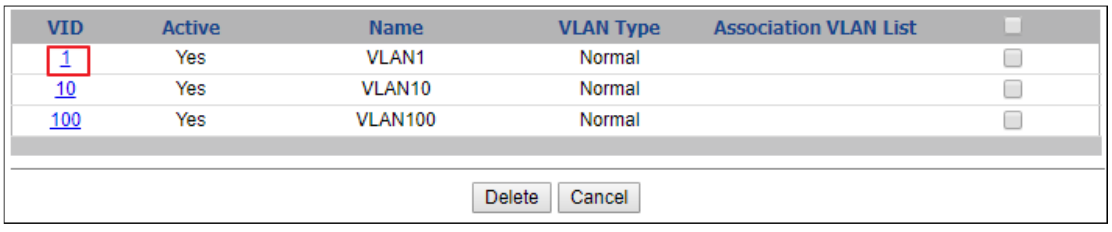


VLAN 100:

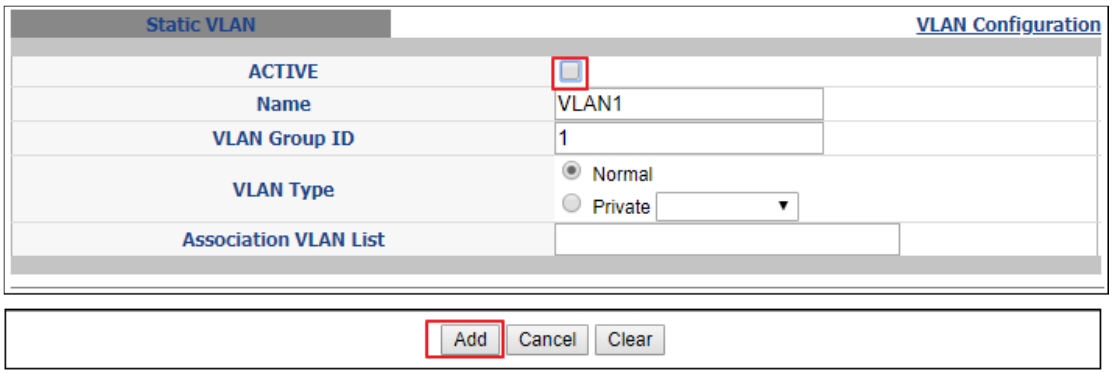


6. Go to **Advanced Application > VLAN > VLAN Configuration> Static VLAN Setup**

7. Enter VLAN 1 to inactivate VLAN.

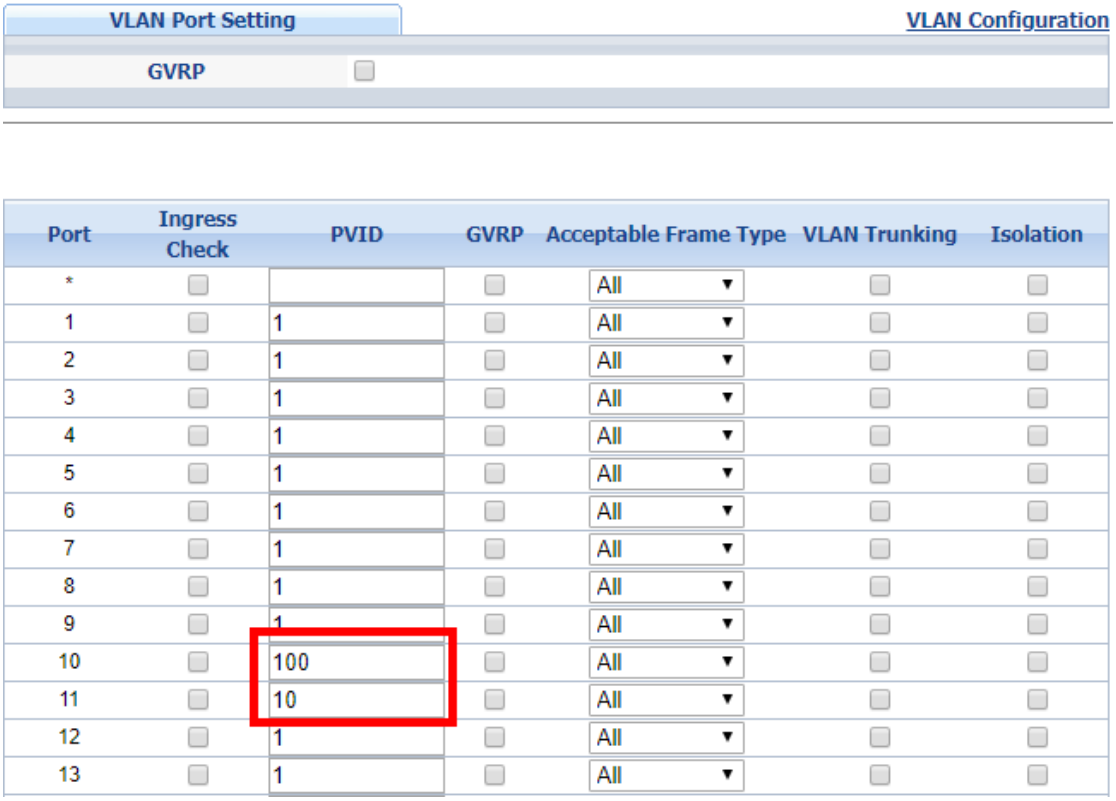


8. Uncheck the "Active" to inactive VLAN 1 then click Add.



9. Go to **Advanced Application > VLAN > VLAN Configuration> VLAN Port Setting**

10. Configure PVID on port 10 & 11



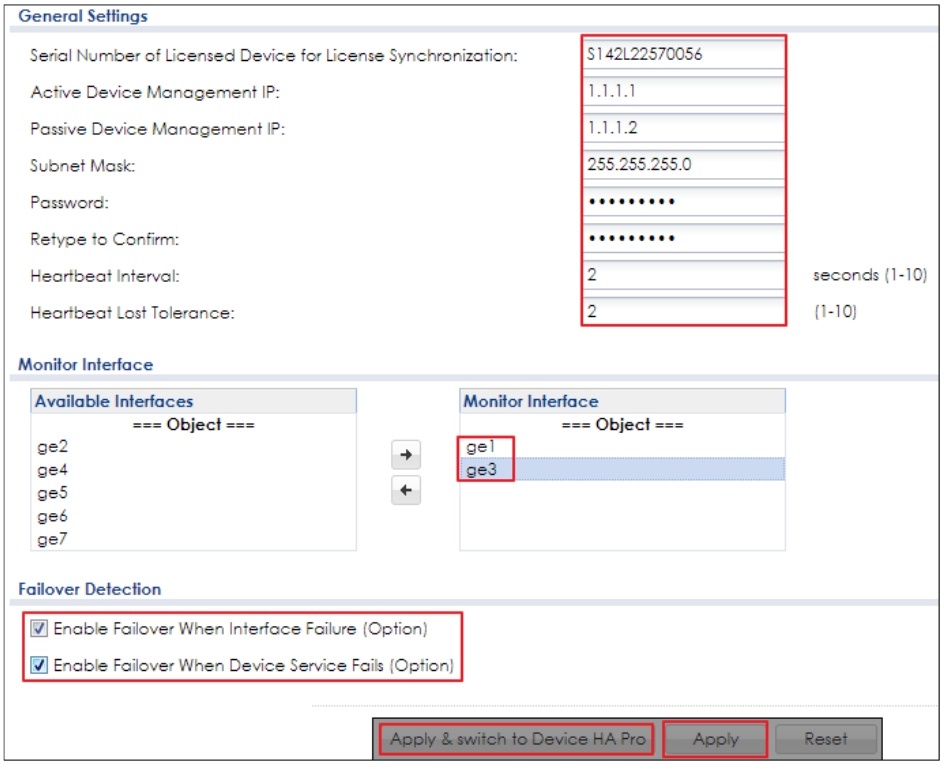
Port	Ingress Check	PVID	GVRP	Acceptable Frame Type	VLAN Trunking	Isolation
*	☐		☐	All	☐	☐
1	☐	1	☐	All	☐	☐
2	☐	1	☐	All	☐	☐
3	☐	1	☐	All	☐	☐
4	☐	1	☐	All	☐	☐
5	☐	1	☐	All	☐	☐
6	☐	1	☐	All	☐	☐
7	☐	1	☐	All	☐	☐
8	☐	1	☐	All	☐	☐
9	☐	1	☐	All	☐	☐
10	☐	100	☐	All	☐	☐
11	☐	10	☐	All	☐	☐
12	☐	1	☐	All	☐	☐
13	☐	1	☐	All	☐	☐

Gateway:

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

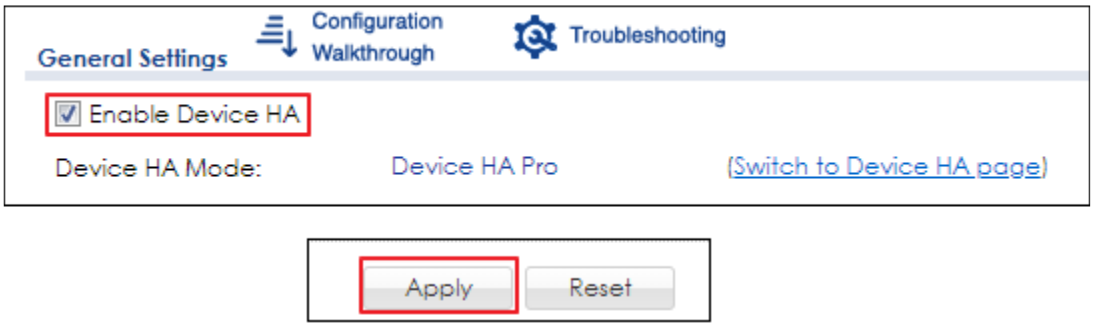
2. Go to **Configuration > Device HA > Device HA Pro**

3. 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.



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

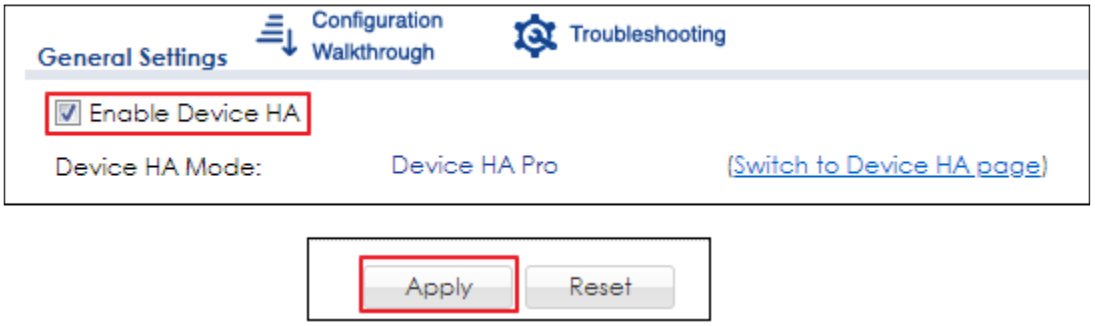
5. Enable the Device HA on General Settings.



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

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

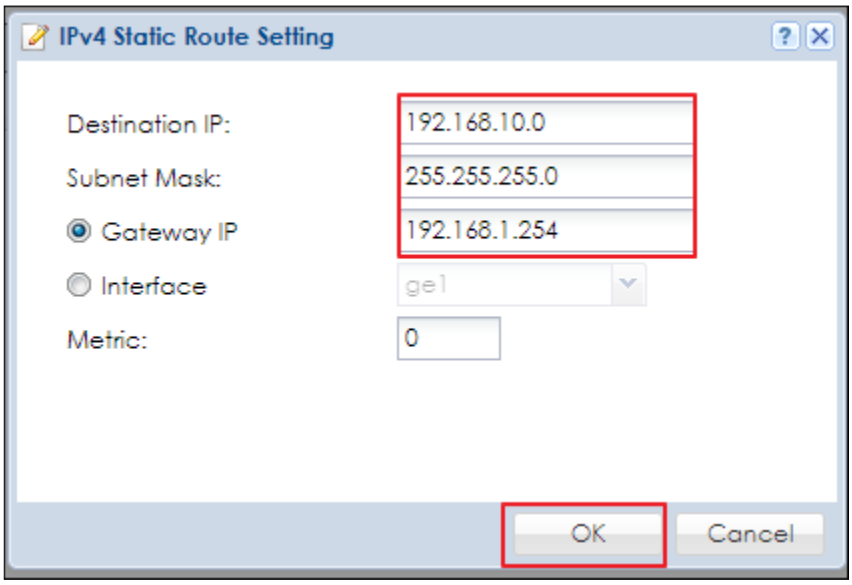
8. Enable the Device HA on General Settings.



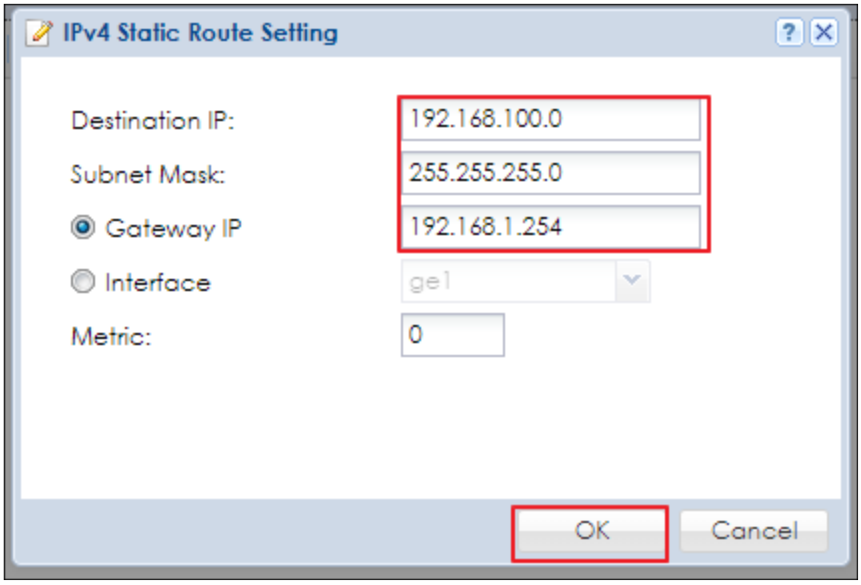
9. Go to **Configuration > Routing > Static Route**

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



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 **IP Application > VRRP**, the figure below is the successful VRRP status due to switch-1 can reach the gateway IP.

VRRP Status — Configuration

Index	Network	VRID	VR Status	Uplink Status
1	192.168.100.1/24	1	Master	Alive
2	192.168.10.1/24	1	Master	Alive
3	192.168.1.251/24	1	Master	Alive

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.

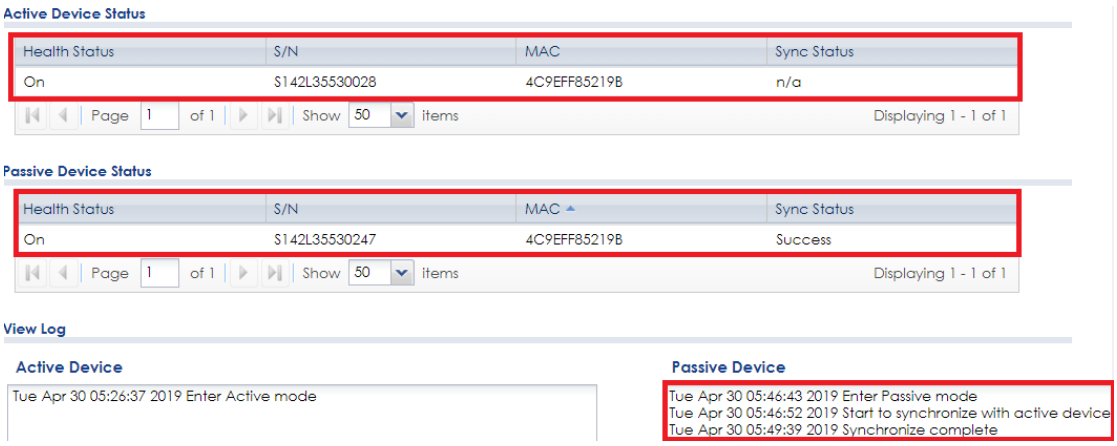
VRRP Status — Configuration

Index	Network	VRID	VR 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.



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

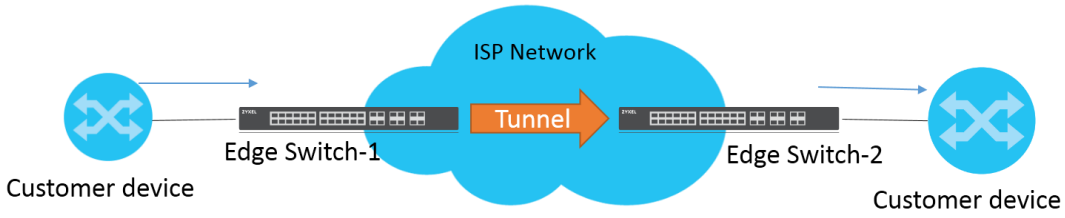
3.6.3 What may go wrong?

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.



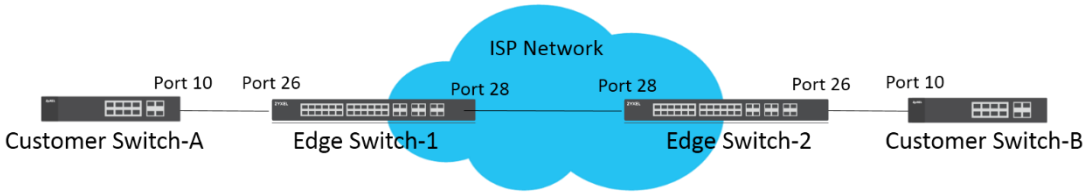
When Edge switch-1 receives Layer-2 protocol packets, it will encapsulate these packets and rewrite their destination MAC addresses with a specific MAC address. All the switches inside the service provider network treat these encapsulated packets as data packets and forward them to the other side. When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

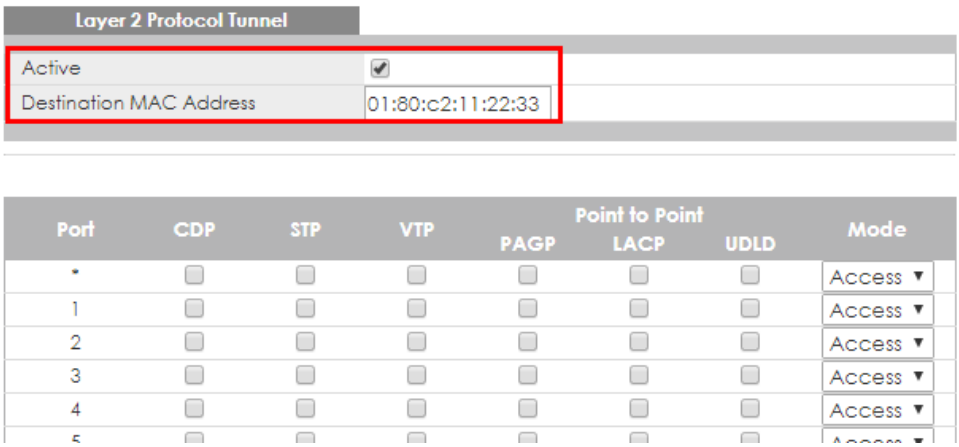
The following example will instruct how an administrator configures a switch to tunnel STP packets through a service provider network.



Note:
The example was tested using two XGS4600 as edge switches, and two GS2210 as customer switches.

3.7.1 Configuration on the Edge Switch

1 Setup **Edge Switch-1**: Access to the web GUI. Go to **Advanced Application > Layer 2 Protocol Tunneling**. Check "**Active**", and set the "**Destination MAC Address**".



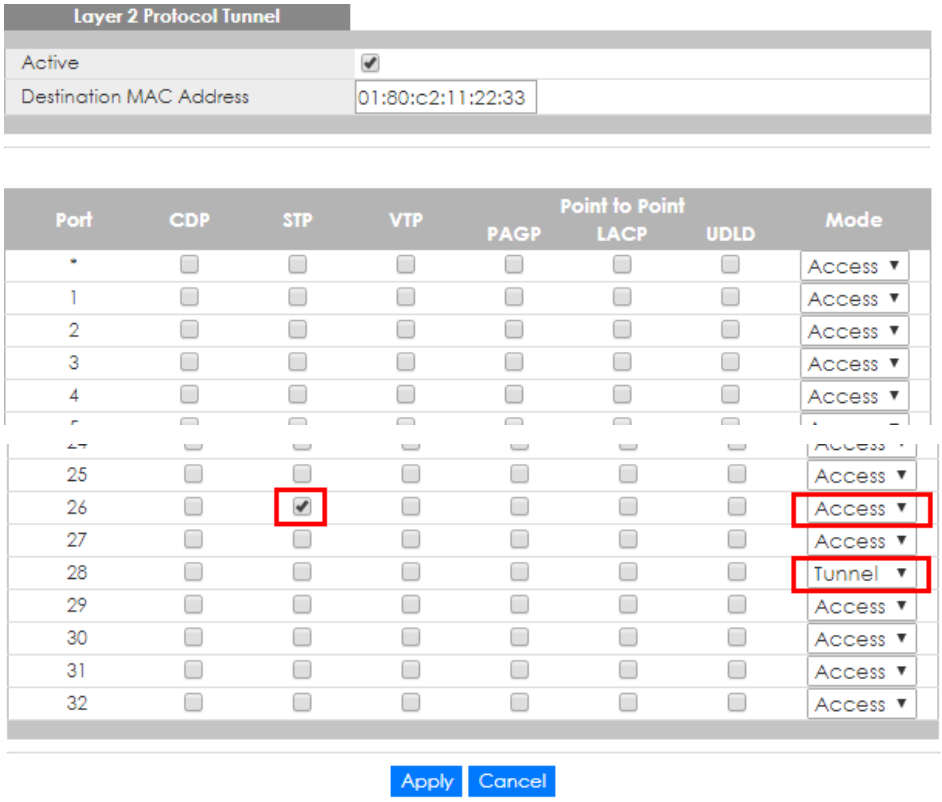
Note:
Destination MAC Address can be either a unicast MAC address or a multicast MAC address.

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.

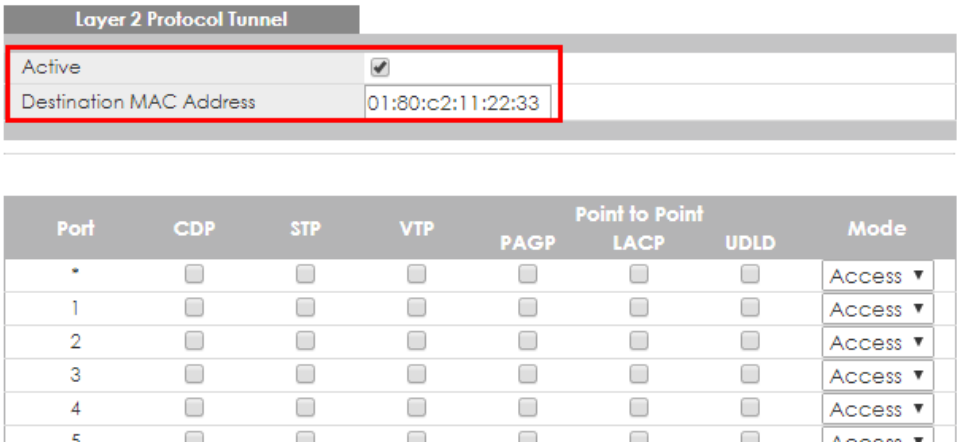
2 Setup **Edge Switch-1**: On the same page. Check "**STP**" and set "**Mode**" as "**Access**" on port 26 which connects to the customer switch.

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**".



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 **Advanced Application > Layer 2 Protocol Tunneling**. Activate Layer 2 Protocol Tunnel, and set the "Destination MAC Address".



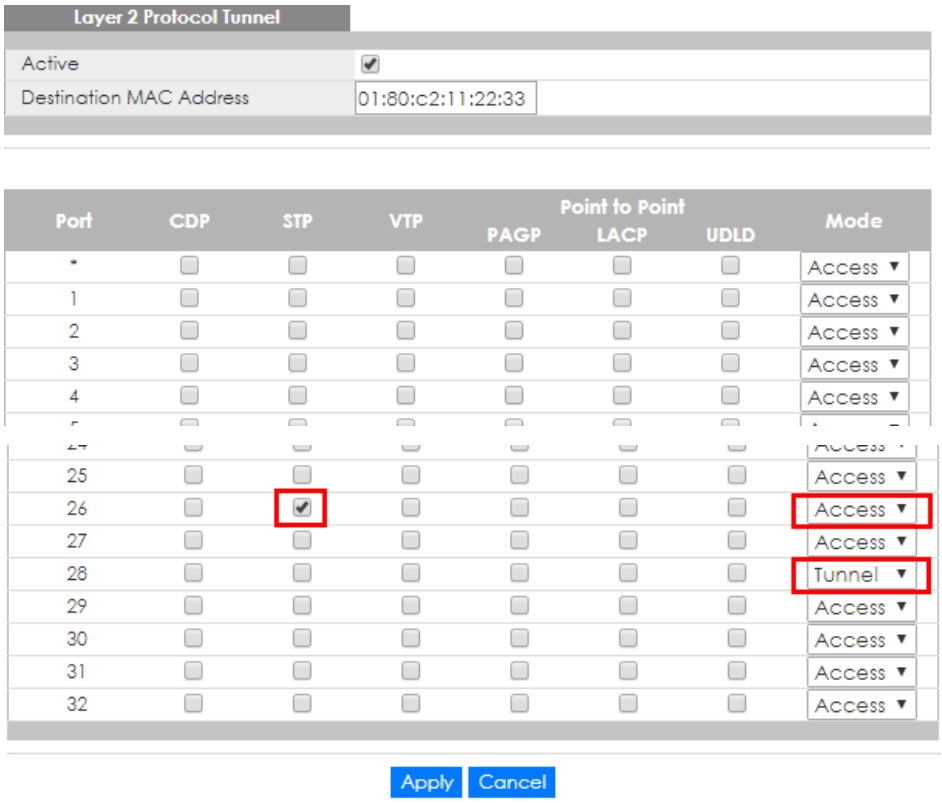
Note:
Destination MAC Address can be either a unicast MAC address or multicast MAC address.

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.

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".



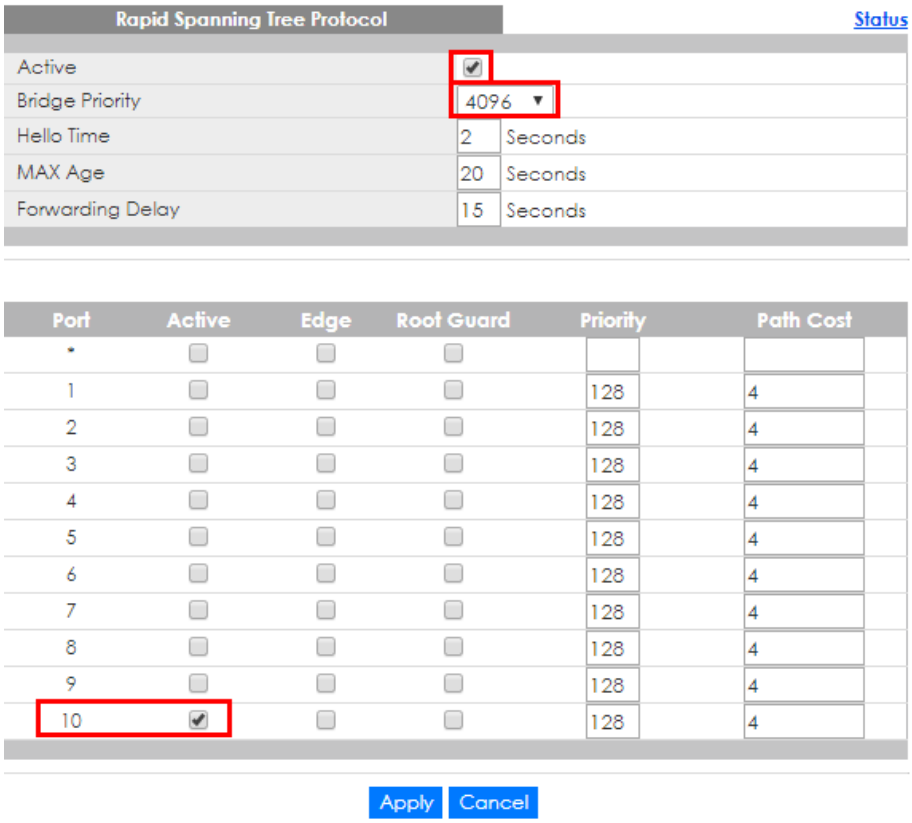
Note:
Activate L2PT services for supported protocols on the access port(s) only.

3.7.2 Configuration on the Customer Switch

1 Setup **Customer Switch-A:** Access to the Web GUI. Go to **Menu > 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.

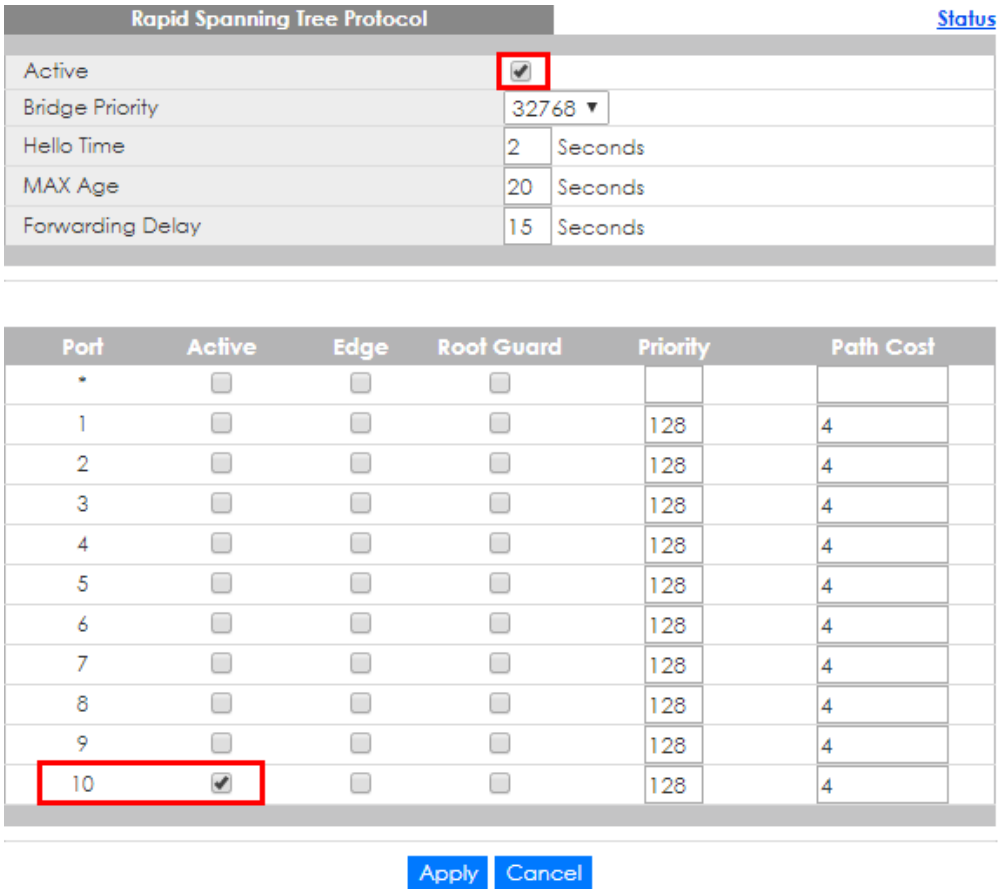
2 Set up **Customer Switch-A**: Enter the web GUI. Go to **Menu > Advanced Application > Spanning Tree Protocol > RSTP**. Check the "**Active**" box, and set the Bridge Priority = **4096.** Activate port **10**, and click "**Apply**".



3 Setup **Customer Switch-B:** Access to the Web GUI. 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**".

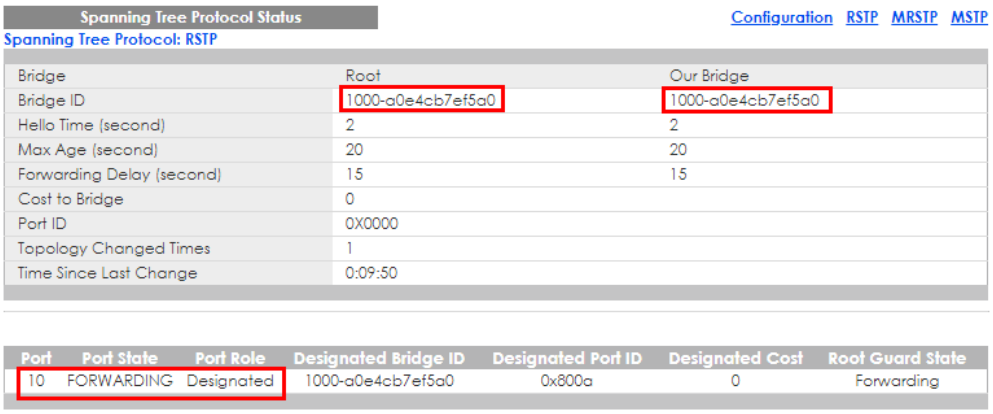
4 Set up **Customer Switch-B**: Enter the web GUI. Go to **Menu > Advanced Application > Spanning Tree Protocol > RSTP**.

Check the "**Active**" box. Activate port **10**, and click "**Apply**".



3.7.3 Test the Results

1 Verify the status of **Customer Switch-A**: Go to **Menu > Advanced Application > 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 Status

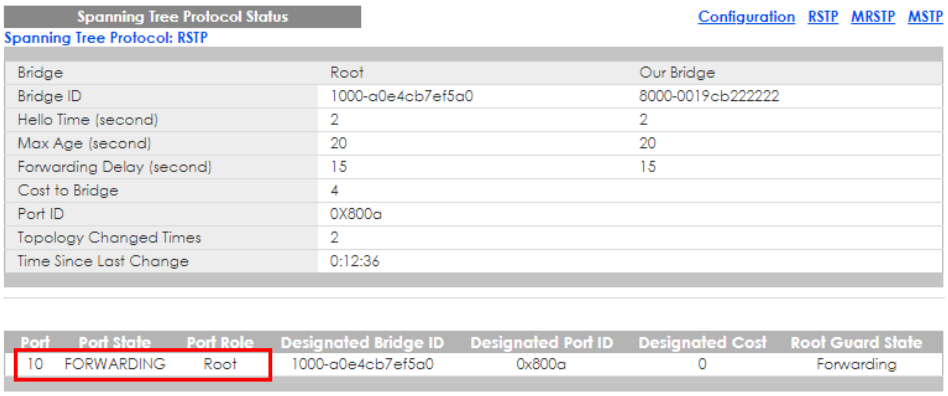
Configuration RSTP MRSTP MSTP

Spanning Tree Protocol: RSTP

Bridge	Root	Our Bridge
Bridge ID	1000-a0e4cb7ef5a0	1000-a0e4cb7ef5a0
Hello Time (second)	2	2
Max Age (second)	20	20
Forwarding Delay (second)	15	15
Cost to Bridge	0	
Port ID	0X0000	
Topology Changed Times	1	
Time Since Last Change	0:09:50	

Port	Port State	Port Role	Designated Bridge ID	Designated Port ID	Designated Cost	Root Guard State
10	FORWARDING	Designated	1000-a0e4cb7ef5a0	0x800a	0	Forwarding

2 Verify the status of **Customer Switch-B**: Go to **Menu > Advanced Application > Spanning Tree Protocol.** Check the port status of Customer Switch-A. Port 10 should be the **Root Port** in **FORWARDING** state.



Spanning Tree Protocol Status

Configuration RSTP MRSTP MSTP

Spanning Tree Protocol: RSTP

Bridge	Root	Our Bridge
Bridge ID	1000-a0e4cb7ef5a0	8000-0019cb222222
Hello Time (second)	2	2
Max Age (second)	20	20
Forwarding Delay (second)	15	15
Cost to Bridge	4	
Port ID	0X800a	
Topology Changed Times	2	
Time Since Last Change	0:12:36	

Port	Port State	Port Role	Designated Bridge ID	Designated Port ID	Designated Cost	Root Guard State
10	FORWARDING	Root	1000-a0e4cb7ef5a0	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.

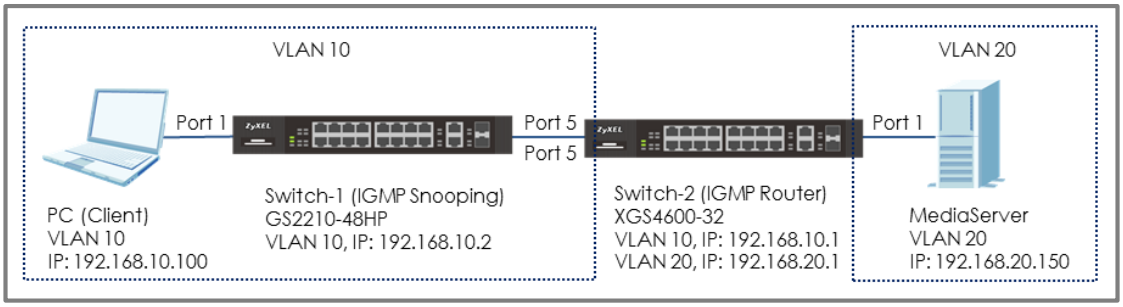


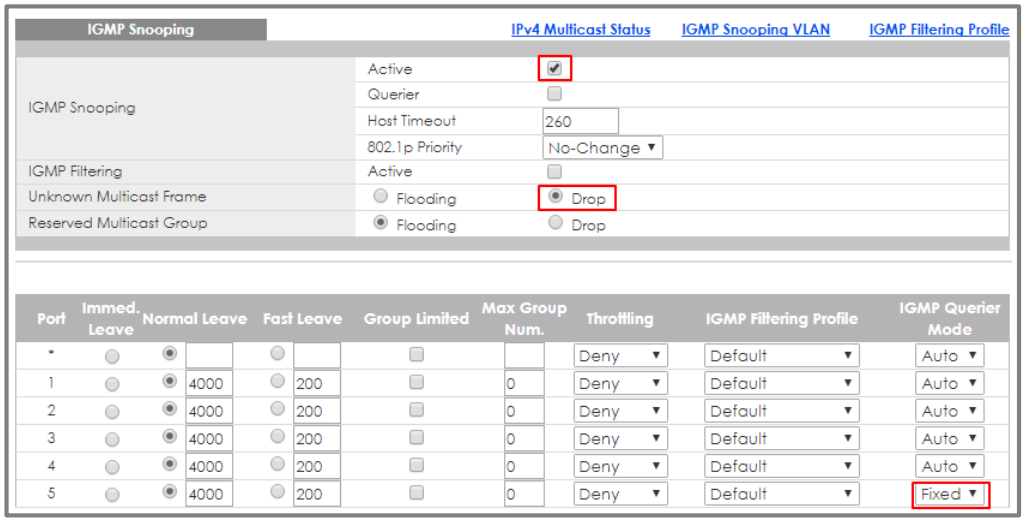
Figure 17 Configure IGMP routing for multicast clients in different VLAN

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 XGS4600-32 (Firmware Version: V4.50) and GS2210-48HP (Firmware Version: V4.30).

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 > Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping**. Check the "Active" box and select Unknown Multicast Frame as **Drop**. Select the port 5 as **Fixed**. Click "Apply".

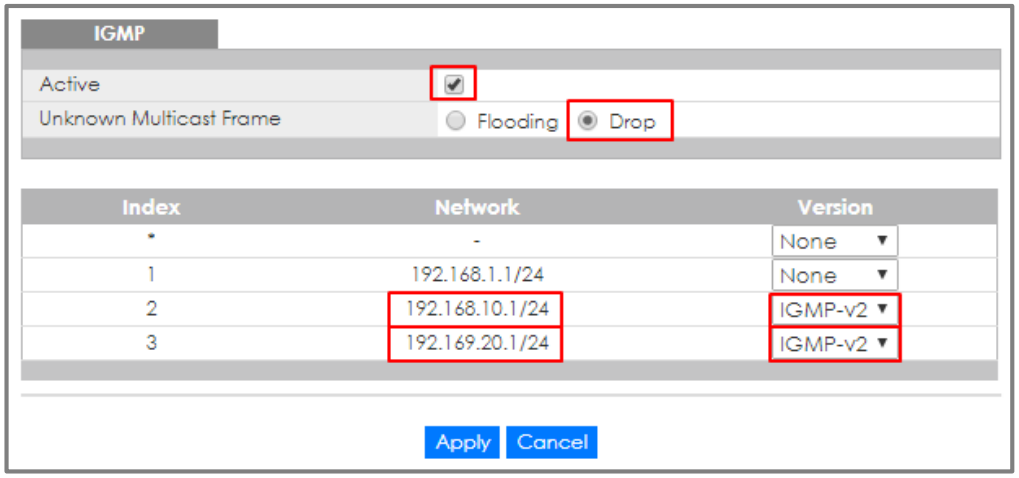


4.2.2 Configure Switch-2

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**.

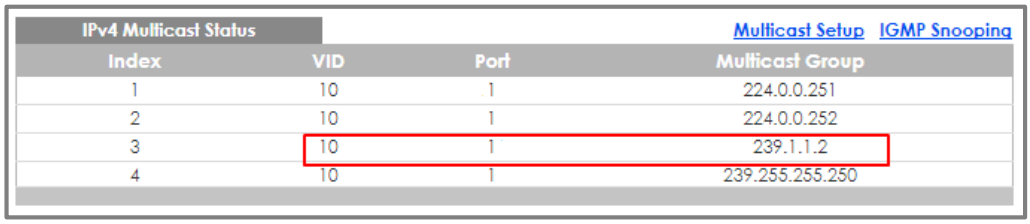
2 Configure the IP addresses for Switch on BOTH VLAN 10 and VLAN 20 as shown in the figure. Please refer to the topic: **1.1 How to change the switch management IP address to avoid accessing the wrong device**.

3 Configure the IGMP Routing: Enter the web GUI and go to **Menu > IP Application > IGMP**. Check the "Active" box and select VLAN 10 and VLAN 20 as IGMP-v2. Select "Unknown Multicast Frame" as "**Drop**". Click "Apply".



4.2.3 Test the Result

1. Play the stream on MediaServer 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 > Advanced Application > Multicast > IPv4 Multicast**. PC connected to port 10 joins the Multicast Group-239.1.1.2.



IPv4 Multicast Status

Multicast Setup IGMP Snooping

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

4.2.4 What Could Go Wrong

1 The Switch-2 (IGMP Router) must contain both VLAN of MediaServer (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 steaming servers in the same VLAN. When MediaServer 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.

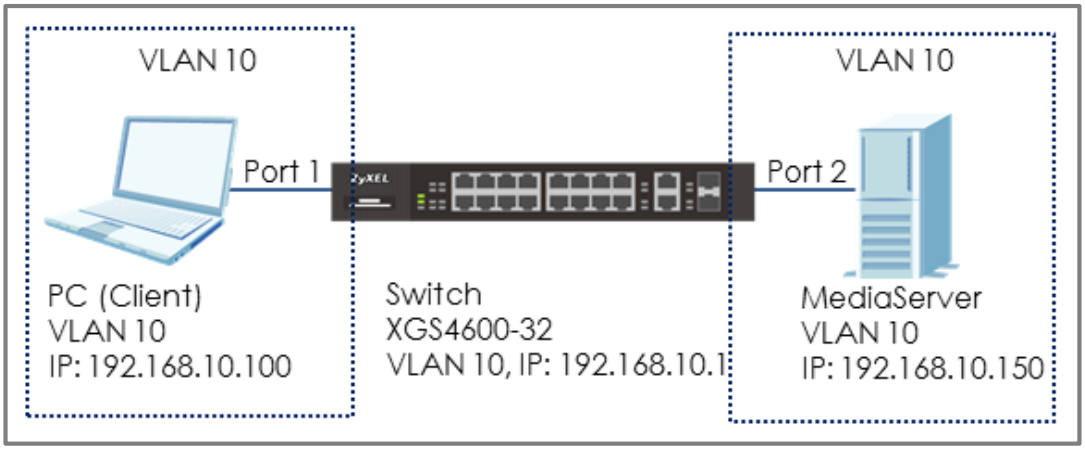


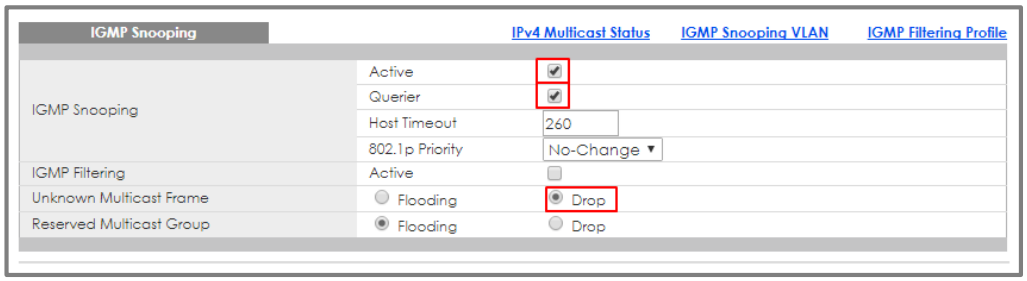
Figure 18 Configure IGMP Snooping for multicast clients in the same LAN

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 XGS4600-32 (Firmware Version: V4.50).

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 > Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping**. Check the "Active" box and select Unknown Multicast Frame as **Drop**. Check **Querier**. Click "Apply".



4.3.2 Test the Result

1 Play the stream on MediaServer 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 > Advanced Application > Multicast > IPv4 Multicast**. PC connected to port 2 joins Multicast Group-239.1.1.1.

IPv4 Multicast Status

Multicast Setup IGMP Snooping

Index	VID	Port	Multicast Group
1	10	1	224.0.0.251
2	10	1	224.0.0.252
3	10	1	239.255.255.250
4	10	2	224.0.0.251
5	10	2	224.0.0.252
6	10	2	239.1.1.1
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.

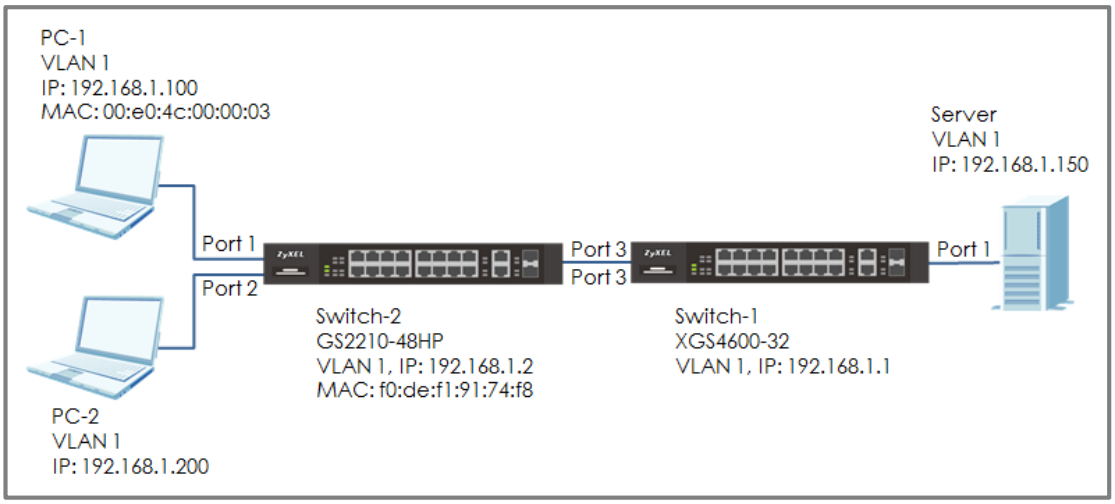
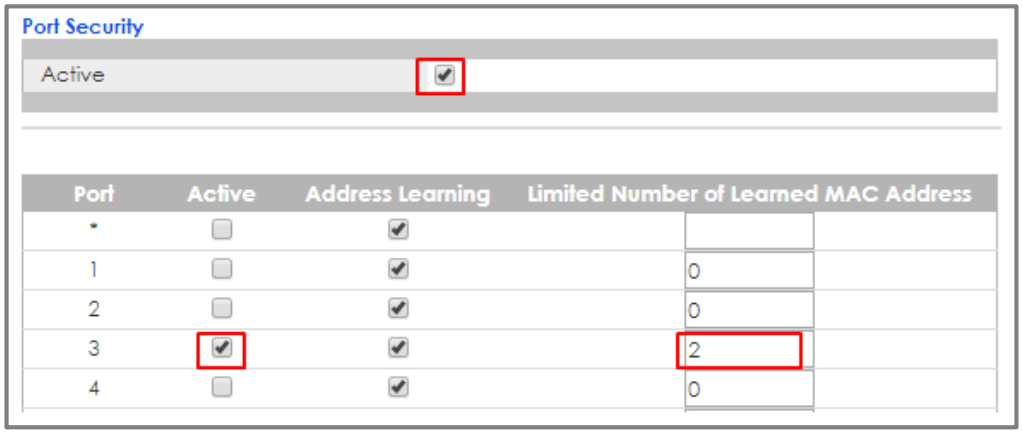


Figure 19 Configure the port security to limit the number of connected devices

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 XGS4600-32 (Firmware Version: V4.50) and GS2210-48HP (Firmware Version: V4.30).

5.1.1 Configure Switch-1

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



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.
Reply from 192.168.1.200: Destination host unreachable.
Reply from 192.168.1.200: Destination host unreachable.
Reply from 192.168.1.200: Destination host unreachable.

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

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

Index	MAC Address	VID	Port	Type
1	00:23:54:2e:98:b9	1	1	Dynamic
2	00:e0:4c:00:00:03	1	3	Dynamic
3	42:73:74:20:55:56	1	CPU	Static
4	f0:de:f1:91:74:f8	1	3	Dynamic

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.

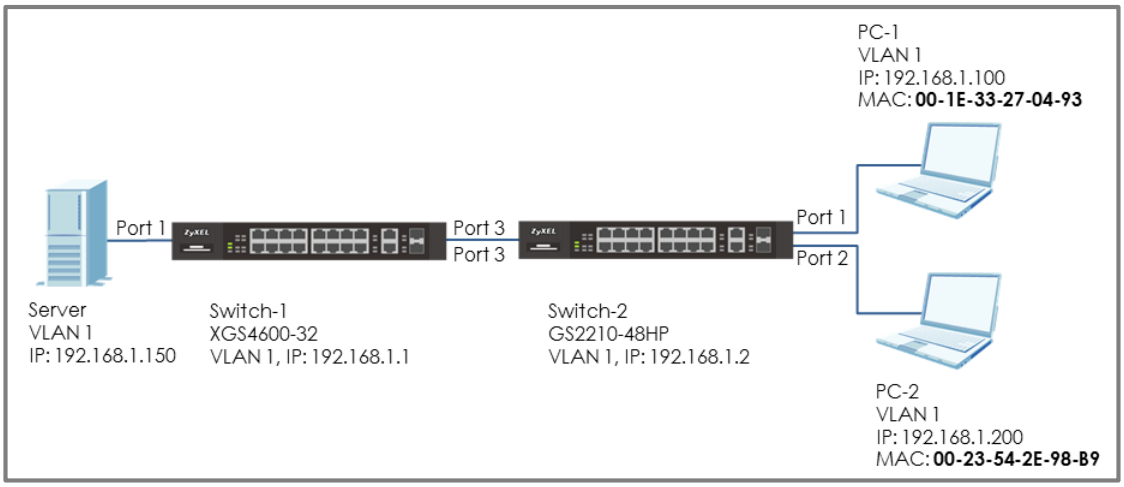
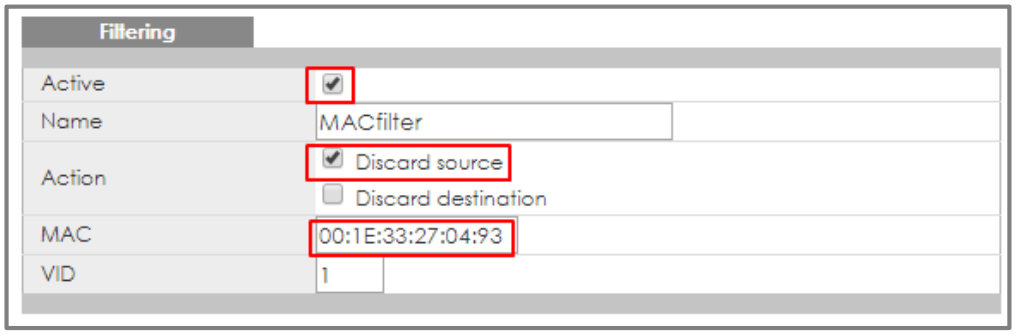


Figure 20 Configure MAC filter to block unwanted traffic

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 XGS4600-32 (Firmware Version: V4.50) and GS2210-48HP (Firmware Version: V4.30).

5.2.1 Configure Switch-1

1 Enter web GUI and go to **Menu > Advanced Application > Filtering**. Check the "Active" box and set the filter Name. Choose the Action as "**Discard source**". Key in the MAC you want to block and the VID. Click "Add".



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.
Reply from 192.168.1.100: Destination host unreachable.
Reply from 192.168.1.100: Destination host unreachable.
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.

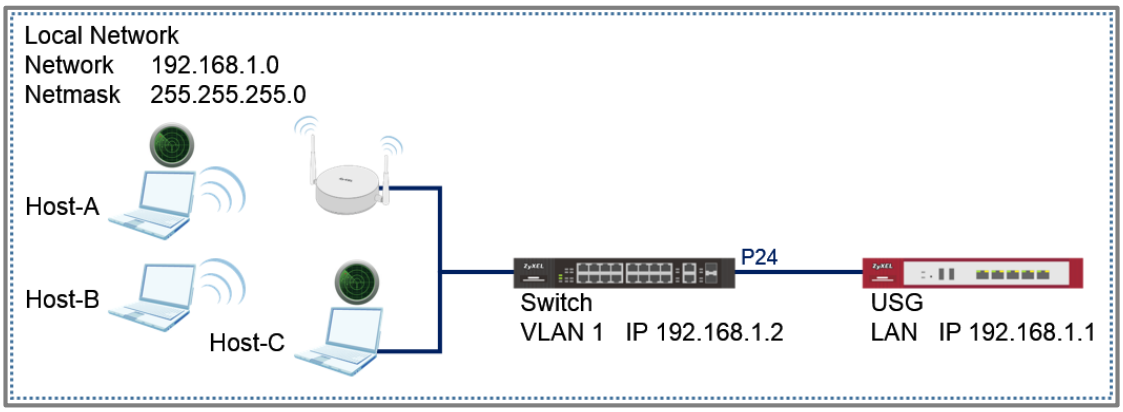


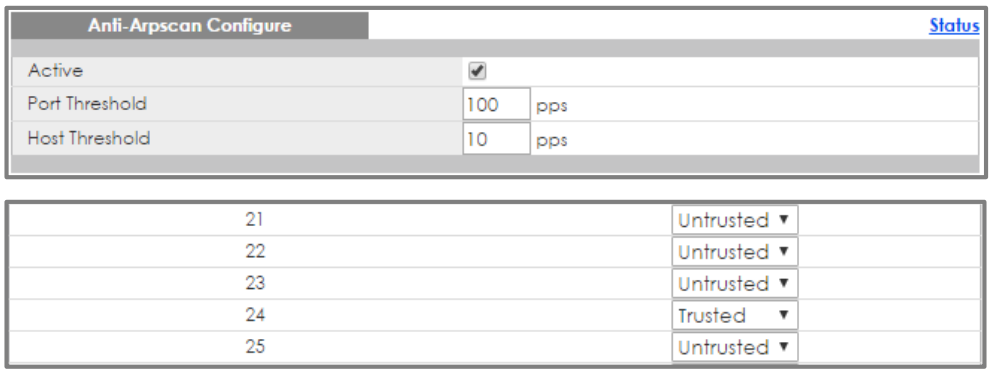
Figure 21 IP Scanning from Wired and Wireless Devices

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 XGS4600 series switch.

5.3.1 Configuration in the Switch

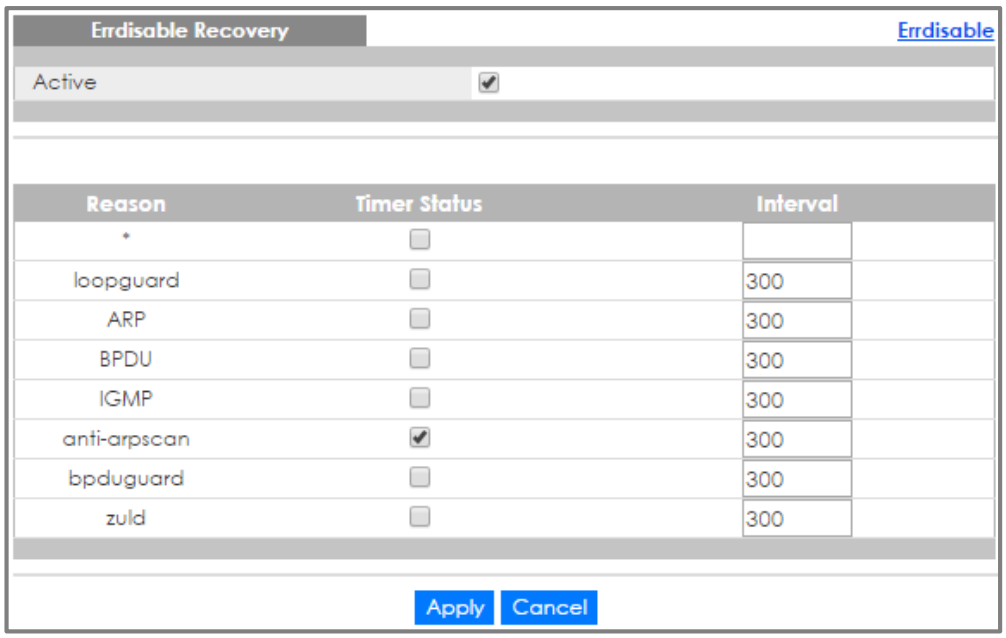
1 Access the Switch's Web GUI.

2 Go to **Advance Application > Anti-Arpscan > Configure**. Check the **Active** box and configure the uplink port (port 24) as "Trusted" state. Click **Apply**.



-Optional-

3 Go to **Advance Application > Errdisable > Errdisable Recovery**. Check the Active box and anti-arpscan box. Click **Apply**.

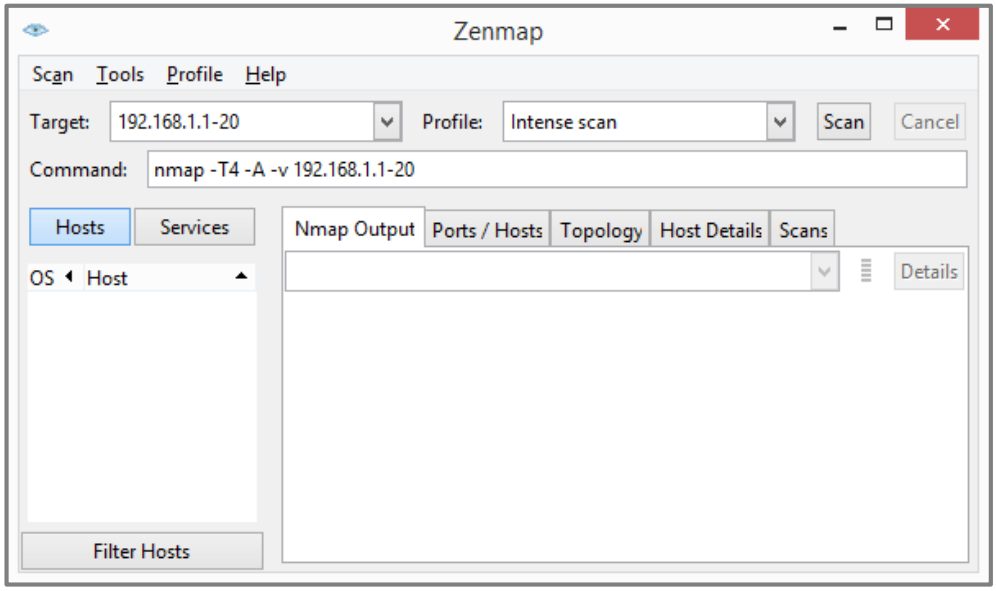


5.3.2 Test the Result

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 **Advance Application > Anti-Arpscan > Host Status**. An entry for Host-A should appear with an "Err-Disable" state.

Filtered host

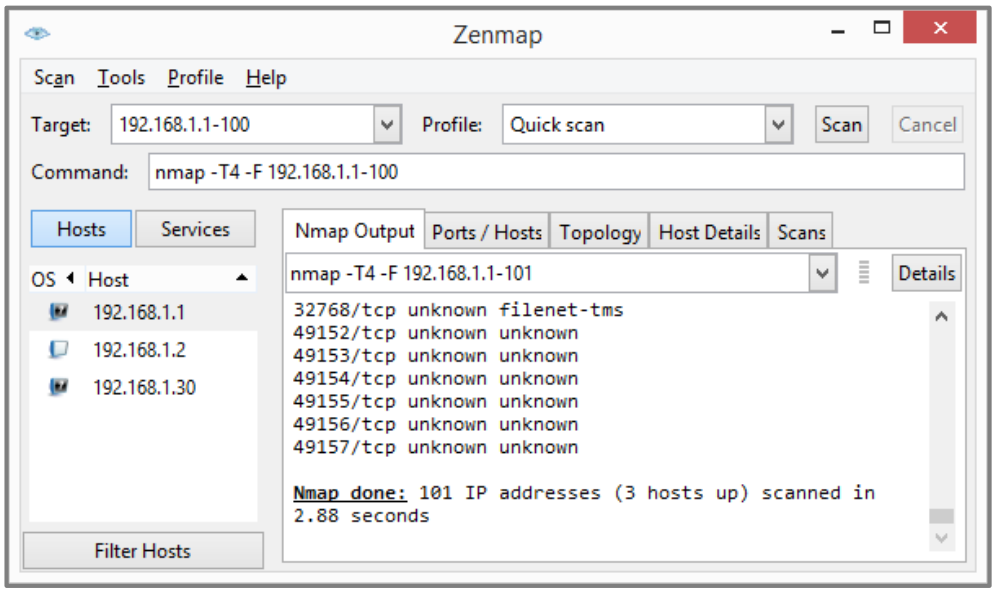
Index	Host IP	MAC	VLAN	Port	State
1	192.168.1.30	74:d4:35:f4:6b:4e	1	1	Err-Disable

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 **Advance Application > Anti-Arpscan**. Port 2 should now be in an Err-disabled state.

Anti-Arpscan Status — Host Status | Trust Host | Configure

Anti-Arpscan is enabled

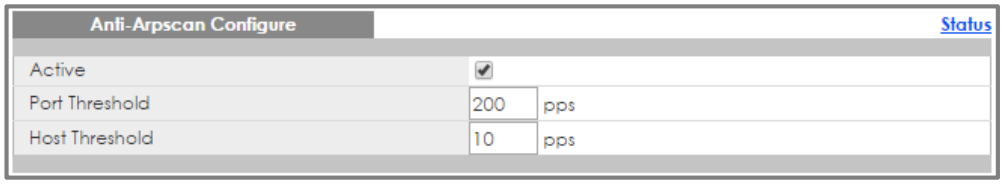
Port	Trusted	State
1	No	Forwarding
2	No	Err-disable
3	No	Forwarding
4	No	Forwarding
5	No	Forwarding

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 **Advance Application > Anti-Arpscan**. If so, consider increasing the **Port Threshold** in **Advance Application > Anti-Arpscan > Configure**.



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.

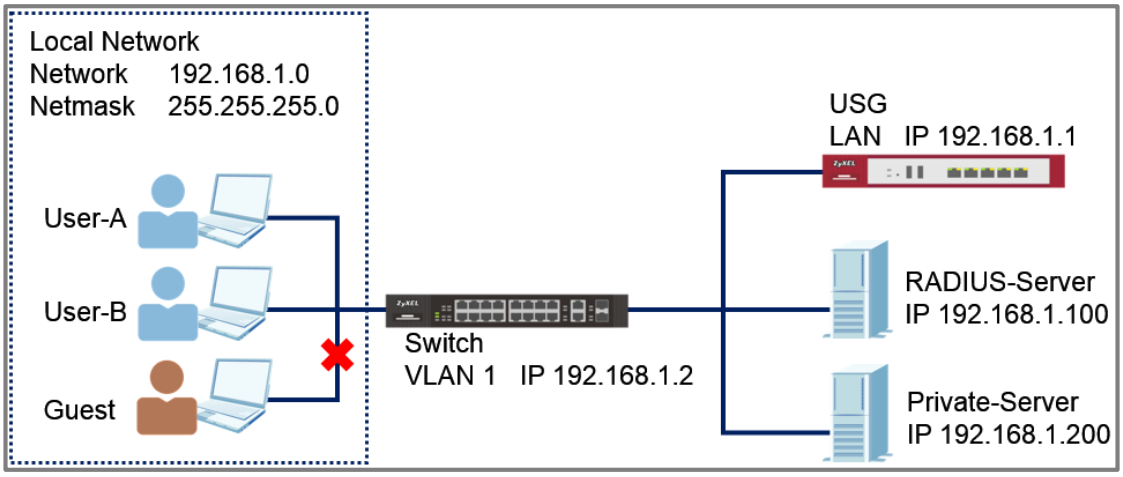


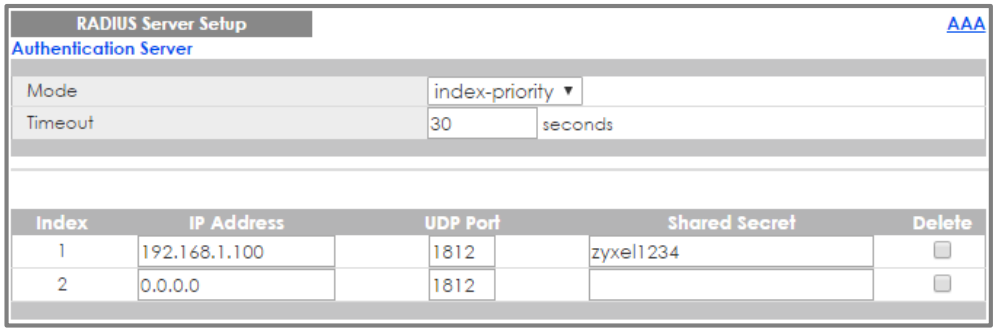
Figure 22 802.1x Port Authentication Providing Access to Authorized Users

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 XGS4600 series switch.

5.4.1 Configuration in the Switch

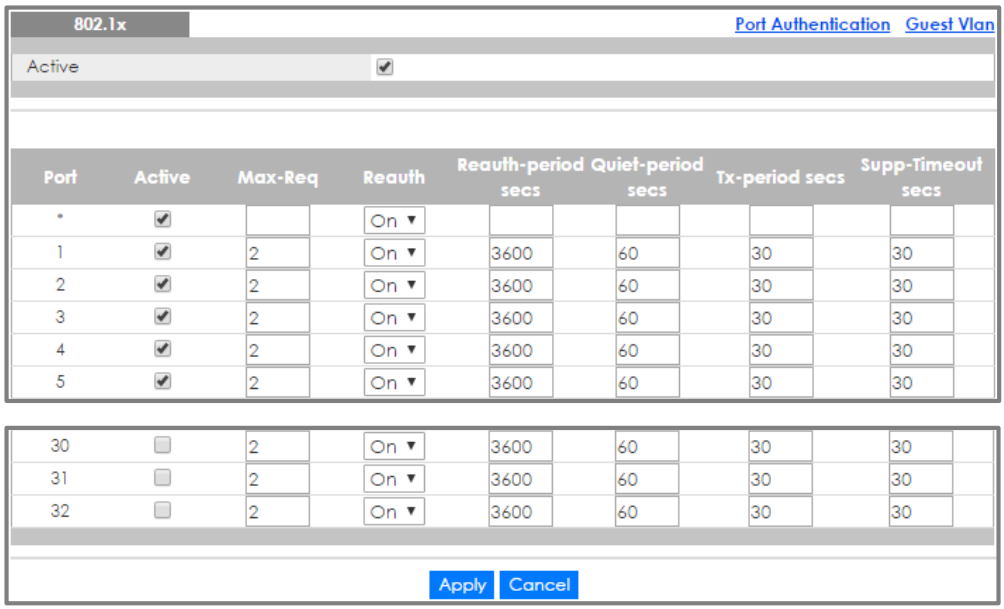
1 Access the **Switch**'s Web GUI.

2 Go to **Advance Application > AAA > RADIUS Server Setup**. Configure the RADIUS server's IP address and set the shared secret. Click **Apply**.



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

3 Go to **Advance Application > Port Authentication > 802.1x**. 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**.


802.1x
Port Authentication
Guest Vlan
Active
Port
Active
Max-Req
Reauth
Reauth-period secs
Quiet-period secs
Tx-period secs
Supp-Timeout secs
* On 3600 60 30 30
1 2 On 3600 60 30 30
2 2 On 3600 60 30 30
3 2 On 3600 60 30 30
4 2 On 3600 60 30 30
5 2 On 3600 60 30 30
30 2 On 3600 60 30 30
31 2 On 3600 60 30 30
32 2 On 3600 60 30 30
Apply
Cancel

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.

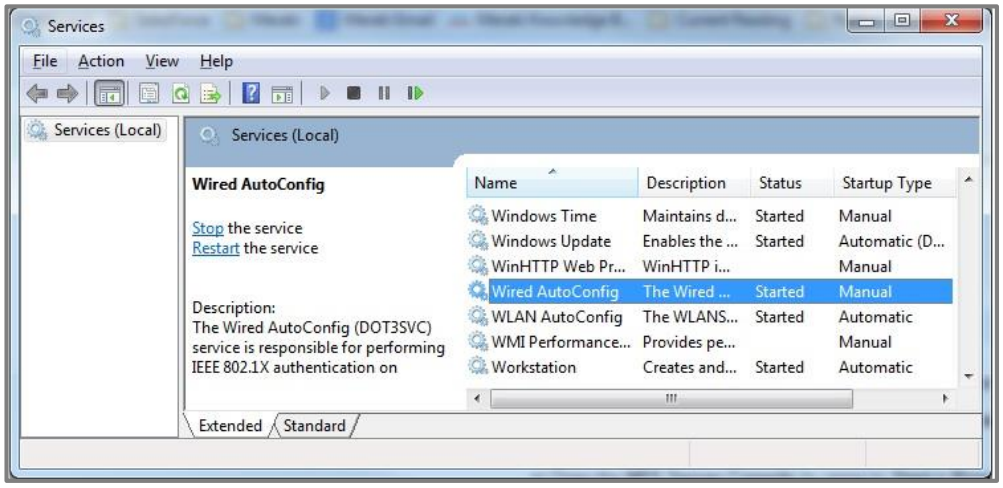
```
root@dhcppc68:/etc/freeradius# stop freeradius
stop: Unknown instance:
root@dhcppc68:/etc/freeradius# start freeradius
freeradius start/running, process 8800
root@dhcppc68:/etc/freeradius#
```

5.4.3 Test the Result

1 Access **User-A**, **User-B**, and **Guest** device.

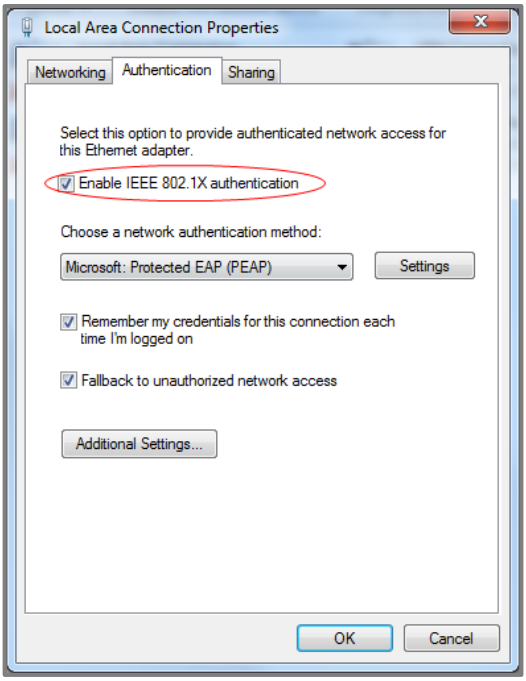
2 If using Windows OS, click the **Start button** and type **services.msc** into the search box.

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

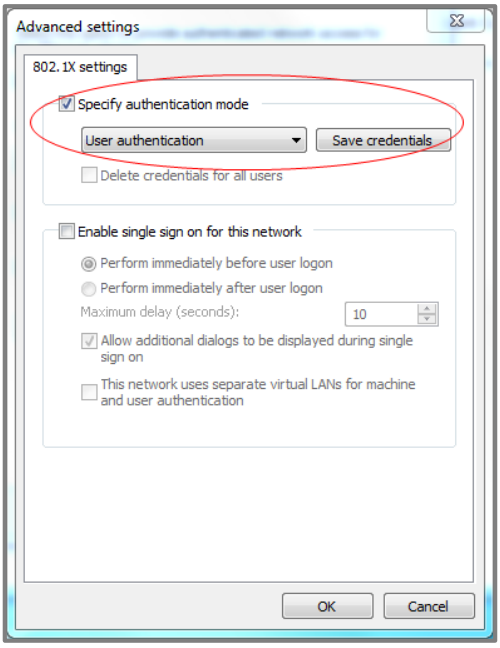


4 Right-click on your network adapter and select **Properties**.

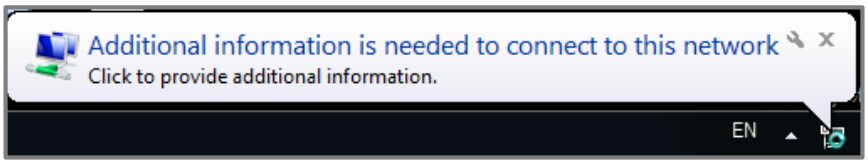
5 Click on the Authentication tab and check "**Enable IEEE 802.1X authentication**". Make sure that the network authentication method is **Microsoft: Protected EAP (PEAP)**



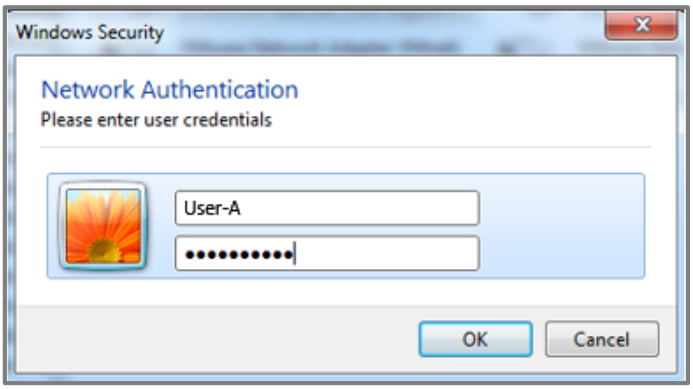
6 Click on **Additional Settings**, select **Specify authentication mode** and specify **User authentication**.



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.



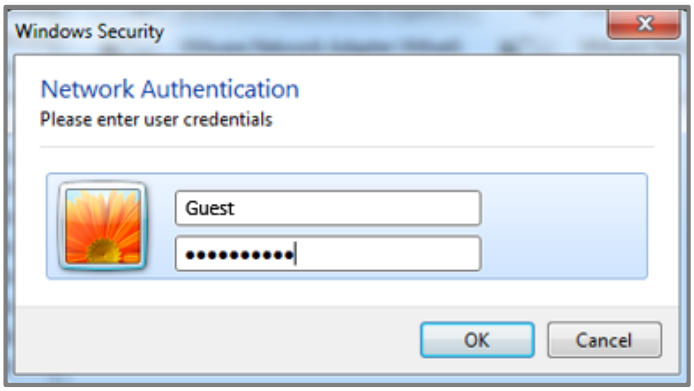
8 Enter the username (**User-A**) and password (**zyxeluserA**) which must be consistent with the RADIUS-Server's user profile settings.



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.

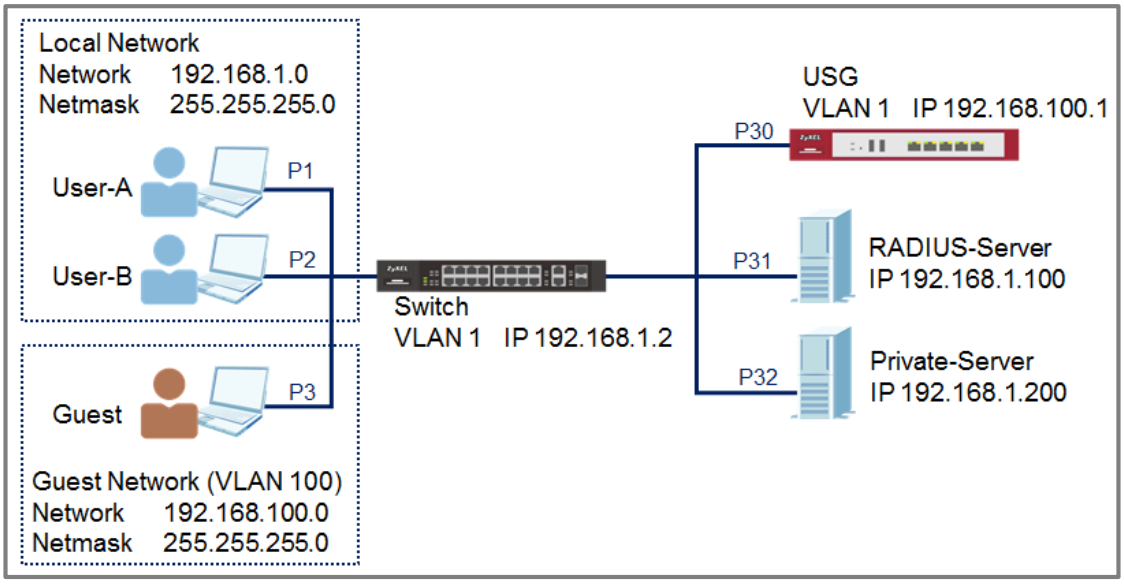


Figure 23 Configure the switch to send unauthorized user in Guest VLAN

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 XGS4600-32 (Firmware Version: V4.50).

5.5.1 Configure 802.1x Port Authentication on the Switch

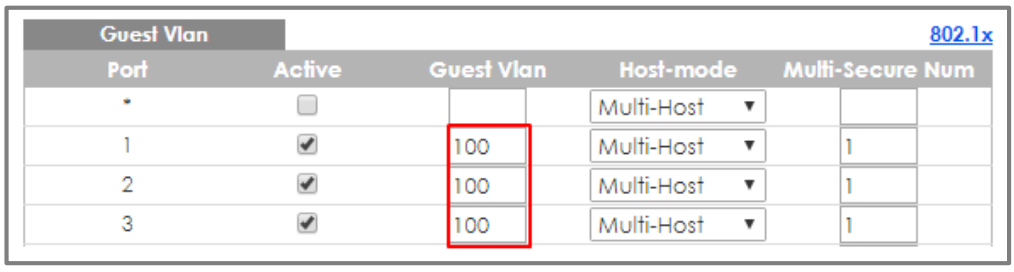
1 Configure 802.1x on all towards users. Do not enable Port Authentication on ports to the USG, RADIUS-Server, and Private-Server. To configure Port Authentication, please refer to the topic: **5.4 How to Configure the Switch and RADIUS Server to Provide Network Access through 802.1x Port Authentication.**

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



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.

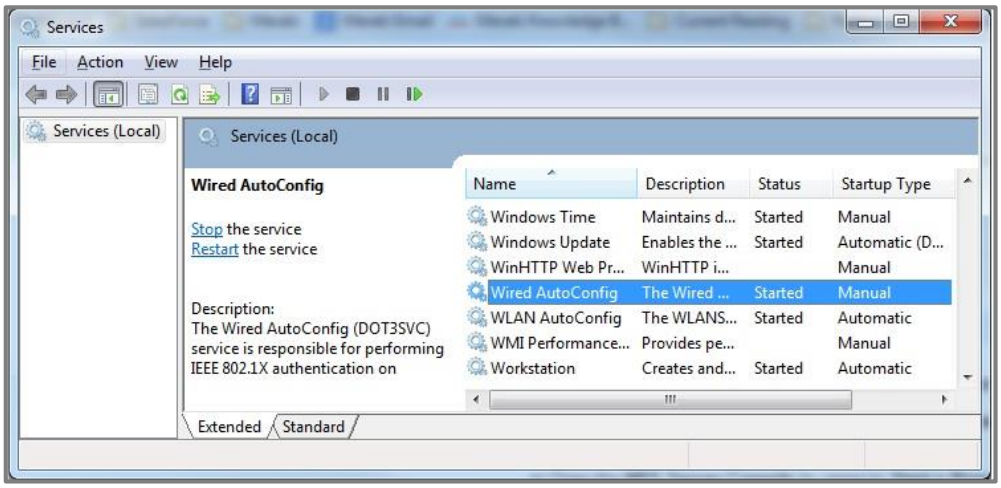
```
user  Cleartest-Password :="user1234"
      Service-Type = Administrative-User
```

3 Restart FreeRADIUS service.

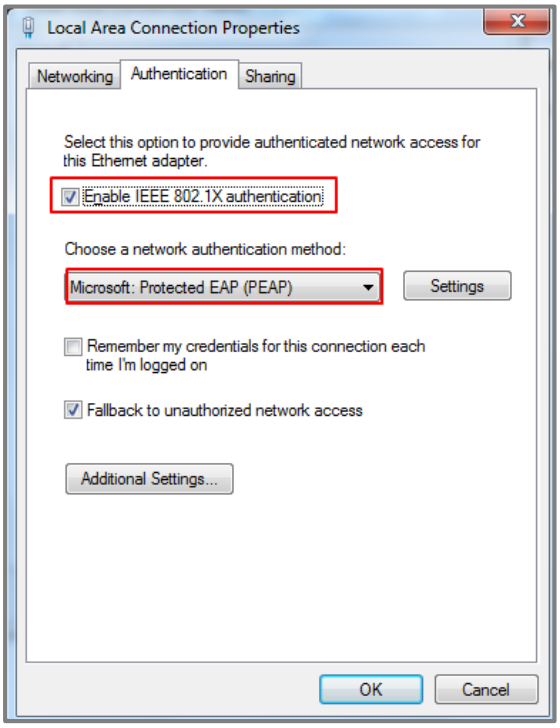
```
root@dhcppc68:/etc/freeradius# stop freeradius
stop: Unknown instance:
root@dhcppc68:/etc/freeradius# start freeradius
freeradius start/running, process 8800
```

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

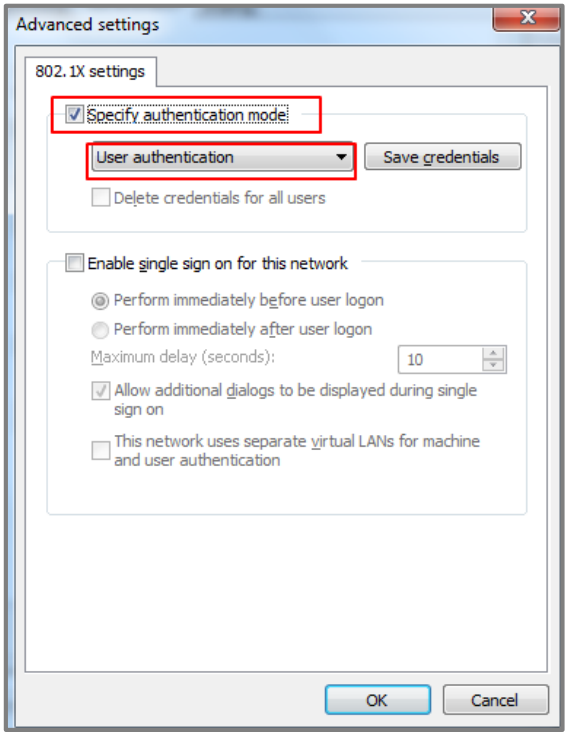
1 In the **Services** window, locate the service named **Wired AutoConfig**. Make sure the service status is "Started".



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)**".

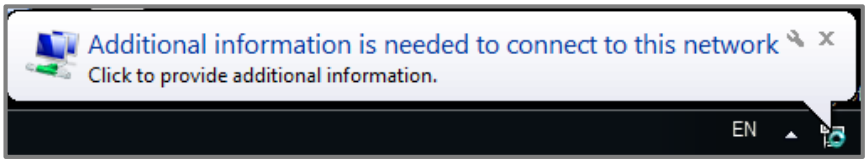


3 Click on **Additional Settings**, select **Specify authentication mode** and specify **User authentication**.

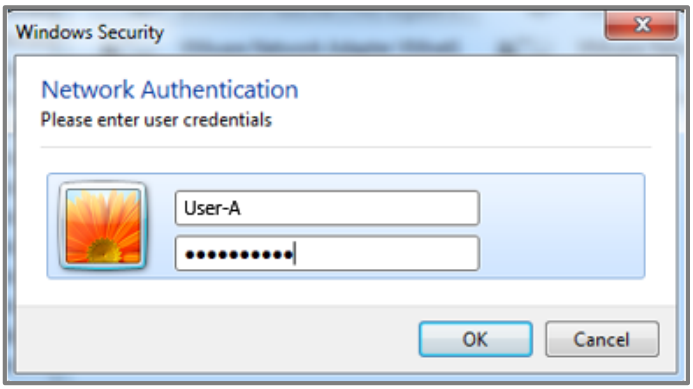


5.5.6 Test the Result

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 > Management > MAC Table > Search**)

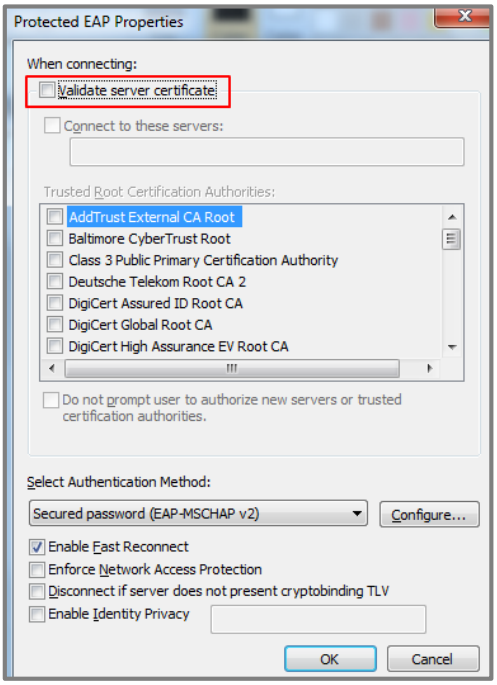
Index	MAC Address	VID	Port	Type
1	00:1e:33:27:04:93	100	3	Dynamic
2	20:6a:8a:39:fe:a9	1	12	Dynamic
3	3c:97:0e:30:0e:b8	1	12	Dynamic
4	42:73:74:20:55:56	1	CPU	Static
5	42:73:74:20:55:56	100	CPU	Static
6	60:31:97:71:6d:15	1	12	Dynamic
7	60:31:97:71:6d:21	1	12	Dynamic
8	74:d4:35:f4:6b:4e	1	12	Dynamic
9	84:ef:18:95:08:e4	1	12	Dynamic
10	a0:8c:fd:1c:c0:b1	1	12	Dynamic
11	b8:ec:a3:0f:cf:9f	1	12	Dynamic
12	c8:6c:87:9f:51:f0	1	12	Dynamic
13	f0:de:f1:91:74:f8	100	1	Dynamic
14	fc:3f:db:39:66:80	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 **Advance Application > VLAN > VLAN Configuration > Static VLAN Setup**.

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 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.

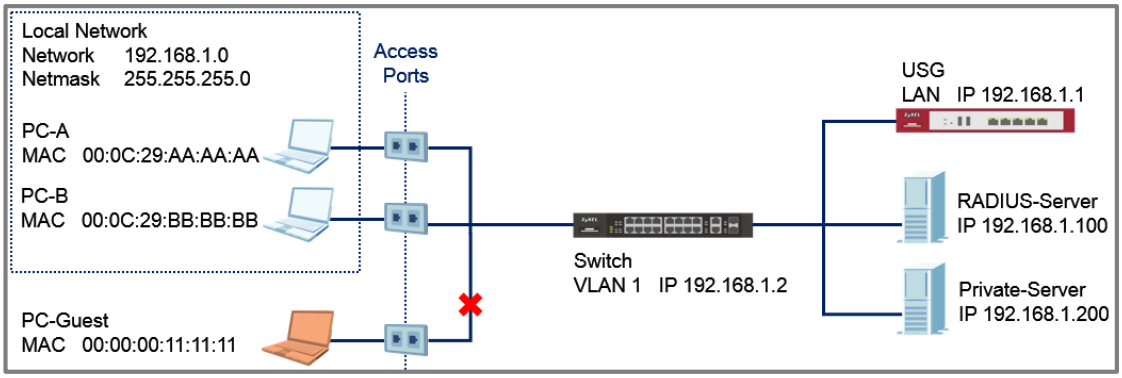


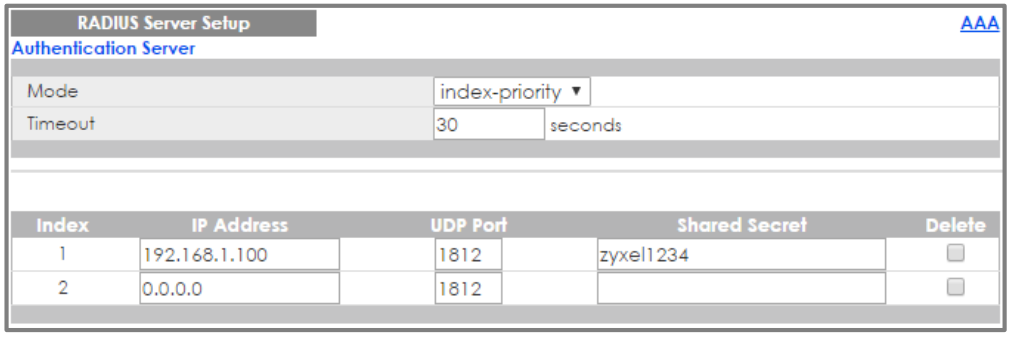
Figure 24 802.1x Port Authentication Providing Access to Authorized Devices

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 XGS4600 series switch.

5.6.1 Configuration in the Switch

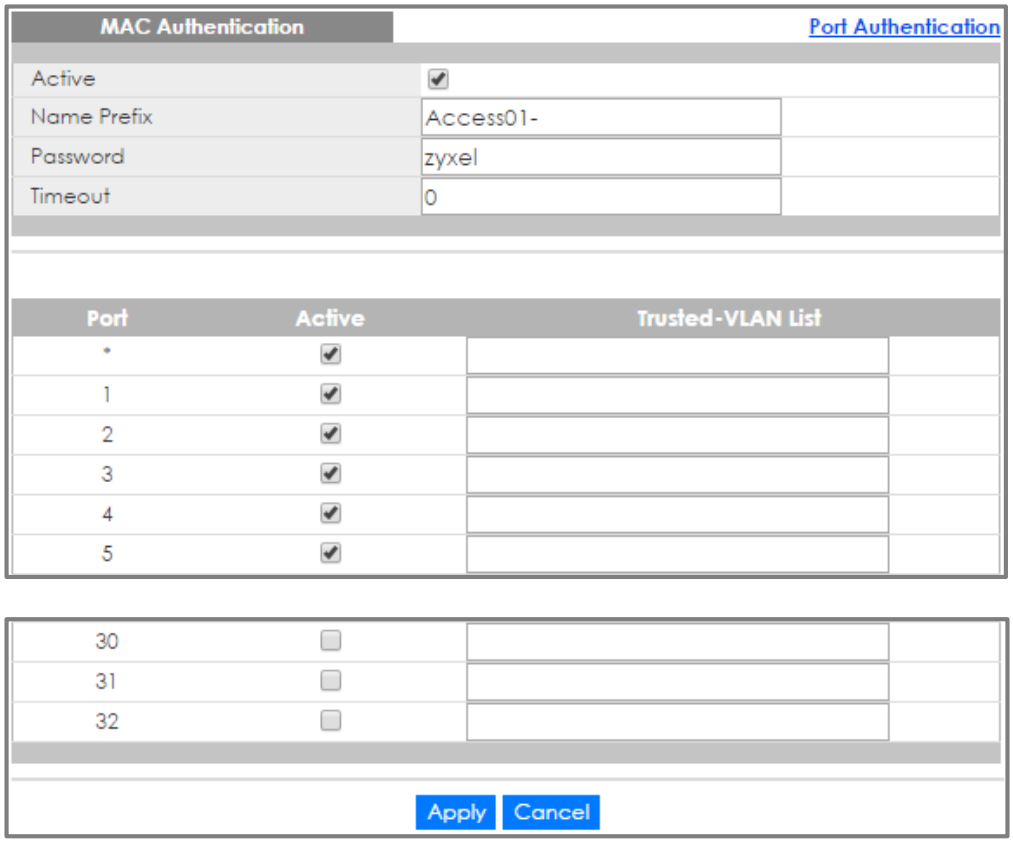
1 Access the **Switch**'s Web GUI.

2 Go to **Advance Application > AAA > RADIUS Server Setup**. Configure the RADIUS server's IP address and set the shared secret. Click **Apply**.



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

3 Go to **Advance Application > Port Authentication > MAC Authentication**. 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**.



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@dhcppc68:/etc/freeradius# stop freeradius
stop: Unknown instance:
root@dhcppc68:/etc/freeradius# start freeradius
freeradius start/running, process 8800
root@dhcppc68:/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.

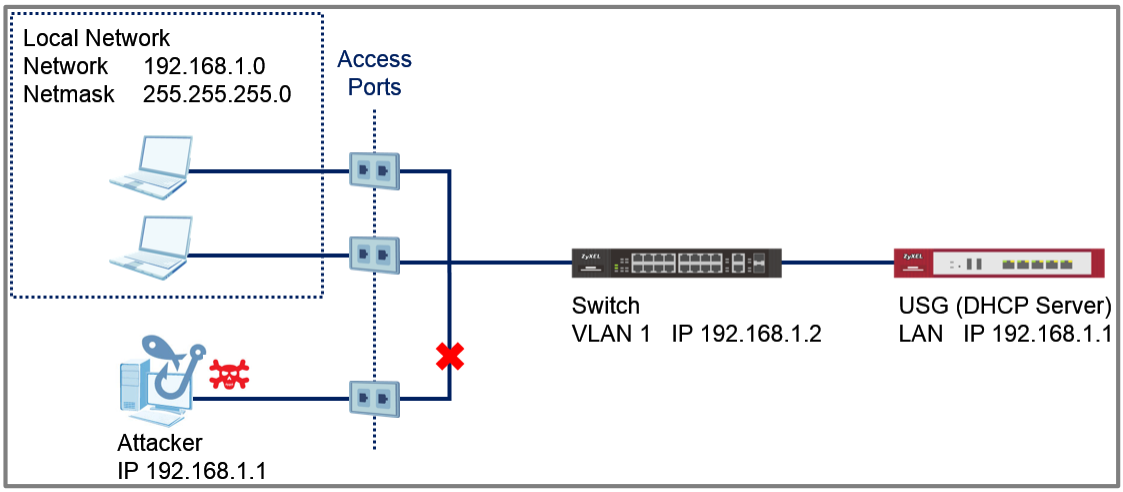


Figure 25 Attacker Using the Same IP Address as the USG

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 XGS4600 series switch.

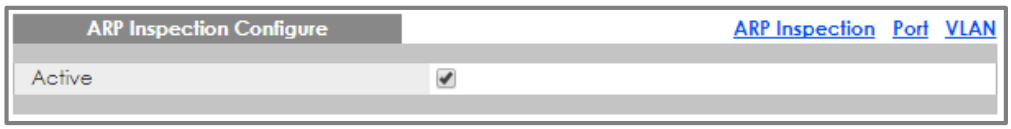
5.7.1 Configuration in the Switch

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

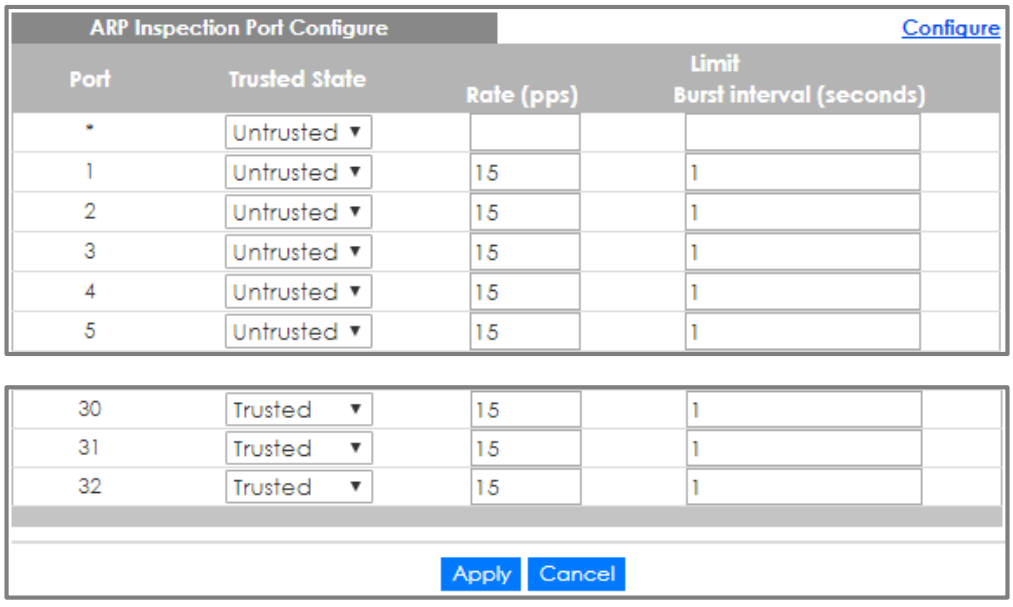
2 Configure **DHCP Snooping** (Refer to section **5.6.1**).

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

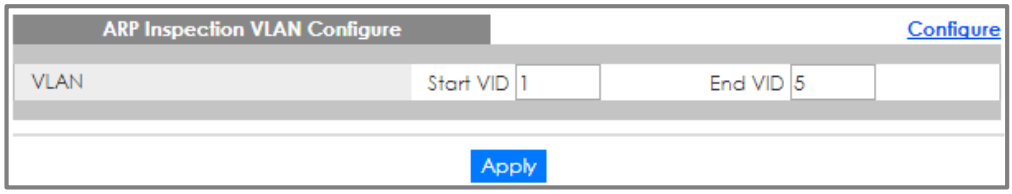
3 Go to **Advance Application > IP Source Guard > IPv4 Source Guard Setup > ARP Inspection > Configure**. Check the Active box to globally enable ARP Inspection.



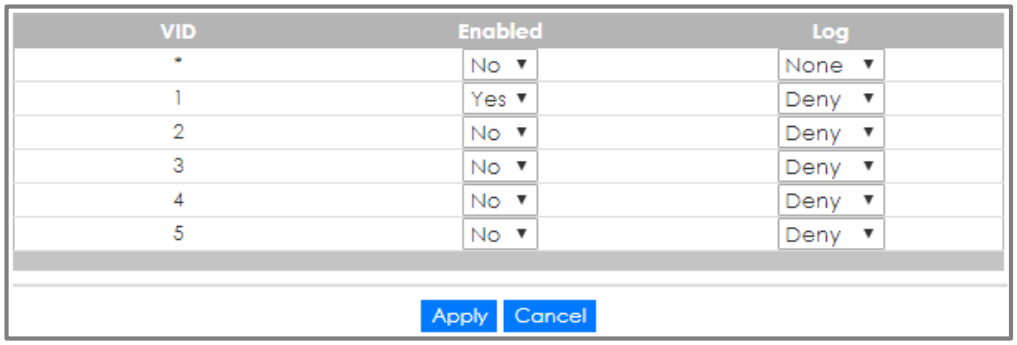
4 Go to **Advance Application > IP Source Guard > IPv4 Source Guard Setup > ARP Inspection > Configure > Port**. Set all access ports as untrusted ports. Ports to the USG or other network components should be trusted ports. Click **Apply**.



5 Go to **Advance Application > IP Source Guard > IPv4 Source Guard Setup > ARP Inspection > Configure > VLAN**. Input the Start VID and End VID. Make sure that the PVID of the access ports are included in this range. Click **Apply**.



6 After inputting the VID range, a list of VID should appear below. Select **Yes** for the access ports' VLAN. Click **Apply**.



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 **Advance Application > IP Source Guard > IPv4 Source**. An entry should appear in the IP Source Guard Table.

IP Source Guard | IPSG | Static Binding | DHCP Snooping | ARP Inspection

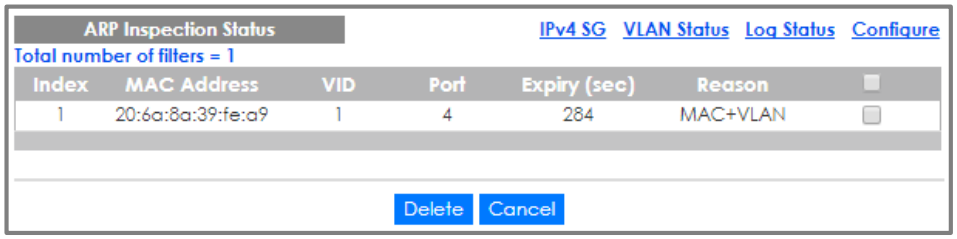
Index	MAC Address	IP Address	Lease	Type	VID	Port
1	20:6a:8a:39:fe:a9	192.168.1.30	2d23h59m40s	dhcp-snooping	1	1

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.



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.

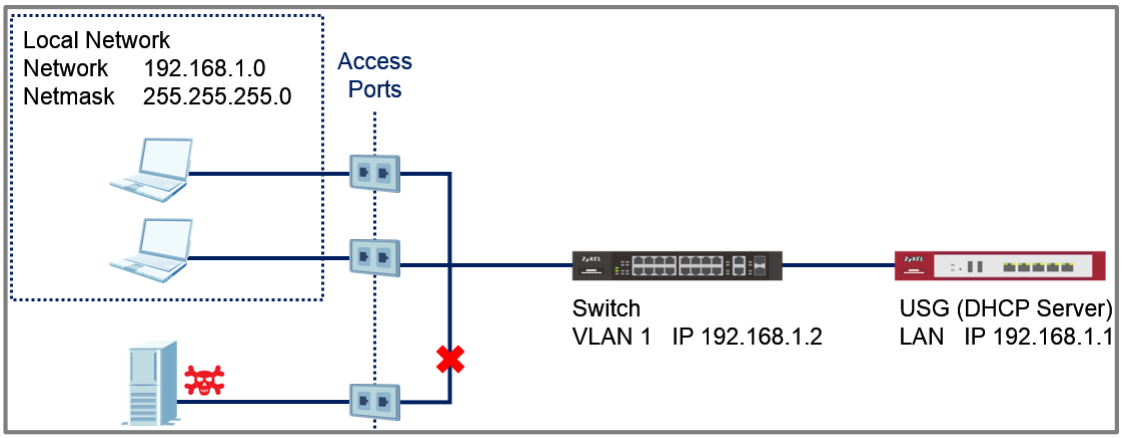


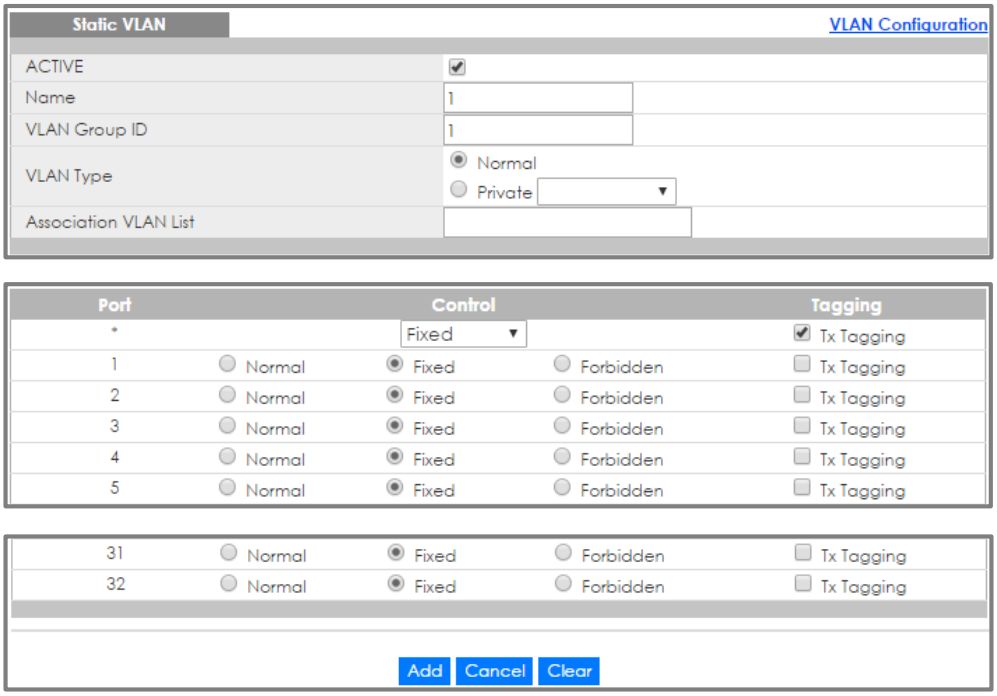
Figure 26 Fake DHCP Server Connected through Publicly Accessible Ports

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 XGS4600 series switch.

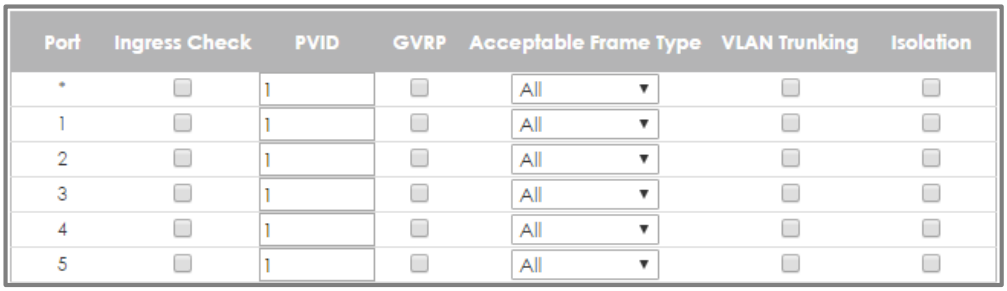
5.8.1 Configuration in the Switch

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

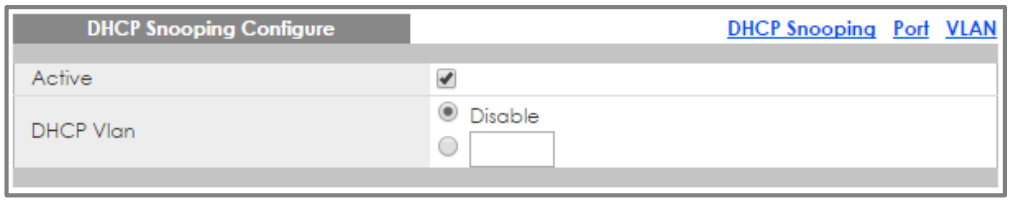
2 Go to Go to **Advance Application > VLAN > VLAN Configuration > Static VLAN Setup**. For this example, all traffic entering access ports are sent to VLAN 1. VLAN 1 should be fixed and untagged for all access ports. Click **Add**.



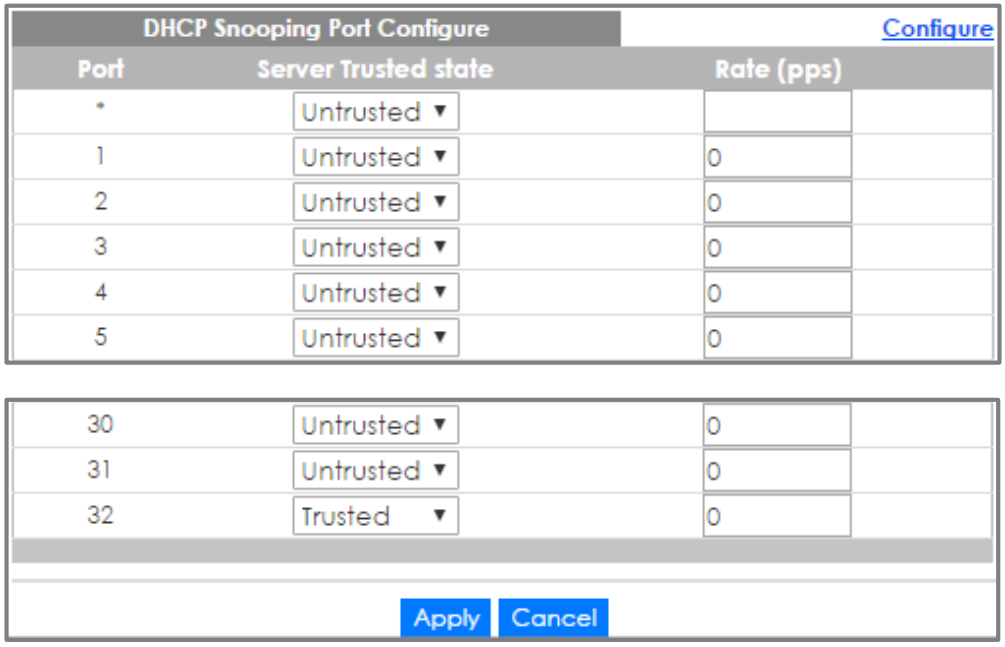
3 Go to **Advance Application > VLAN > VLAN Configuration > VLAN Port Setup**. Configure all access ports with PVID 1. Click **Apply**.



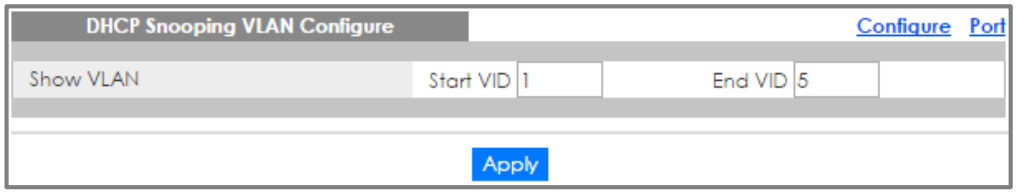
4 Go to **Advance Application > IP Source Guard > IPv4 Source Guard Setup > DHCP Snooping > Configure**. Check the Active box under DHCP Snooping Configure. Click **Apply**.



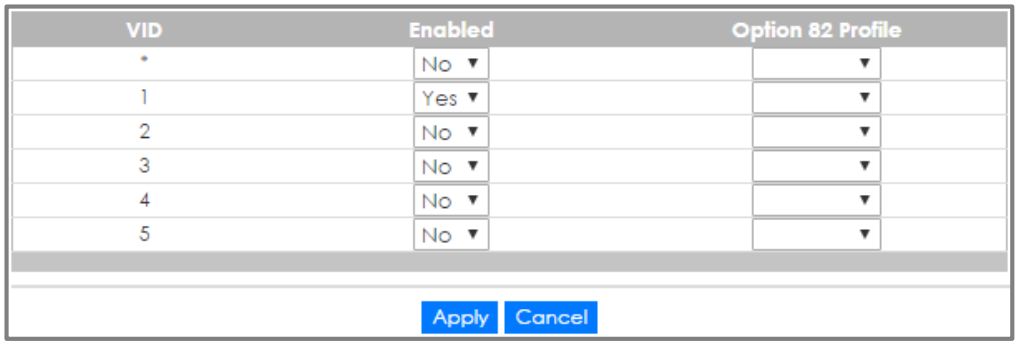
5 Go to **Advance Application > IP Source Guard > IPv4 Source Guard Setup > DHCP Snooping > Configure > Port**. Set all access ports as untrusted ports. Ports to the USG or other network components should be trusted ports. Click **Apply**.



6 Go to **Advance Application > IP Source Guard > IPv4 Source Guard Setup > DHCP Snooping > Configure > VLAN**. Input the Start VID and End VID. Make sure that the PVID of the access ports are included in this range. Click **Apply**.



7 After inputting the VID range, a list of VID should appear below. Select **Yes** for the access ports' VLANs. Click **Apply**.



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 **Advance Application > IP Source Guard > IPv4 Source Guard Setup > DHCP Snooping > Configure > Port**.
   b. Verify the PVID of the port to this DHCP client. Make sure that DHCP snooping is enabled for that VLAN in **Advance Application > IP Source Guard > IPv4 Source Guard Setup > DHCP Snooping > Configure > VLAN**.

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 **Advance Application > IP Source Guard > IPv4 Source Guard Setup > DHCP Snooping > Configure > Port**.
   b. Make sure that both redundant ports are trusted ports in **Advance Application > IP Source Guard > IPv4 Source Guard Setup > DHCP Snooping > Configure > Port** 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 in 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.

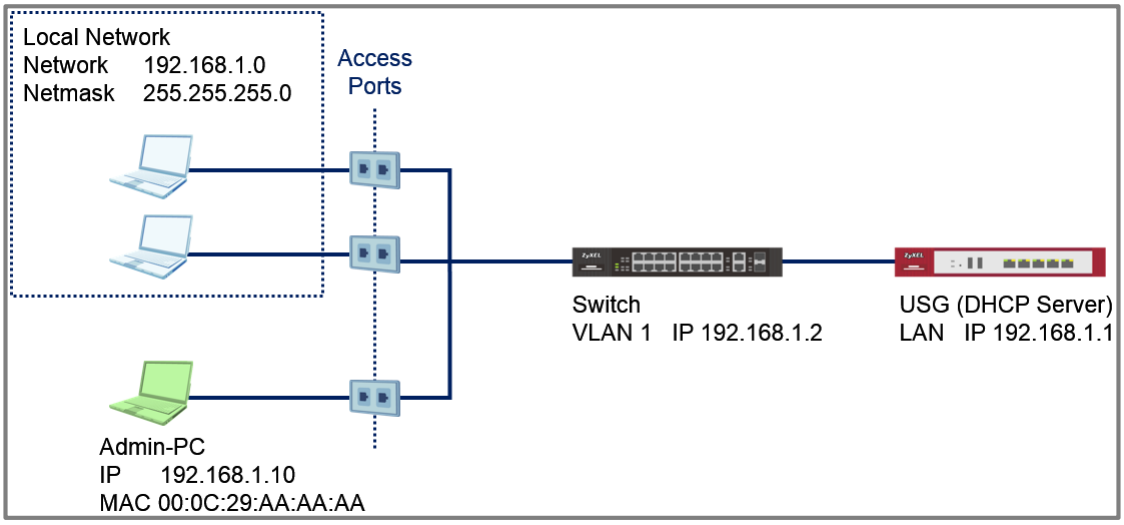


Figure 27 Administrator Device Using a Static IP Address Connected on an Access Port

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 XGS4600 series switch.

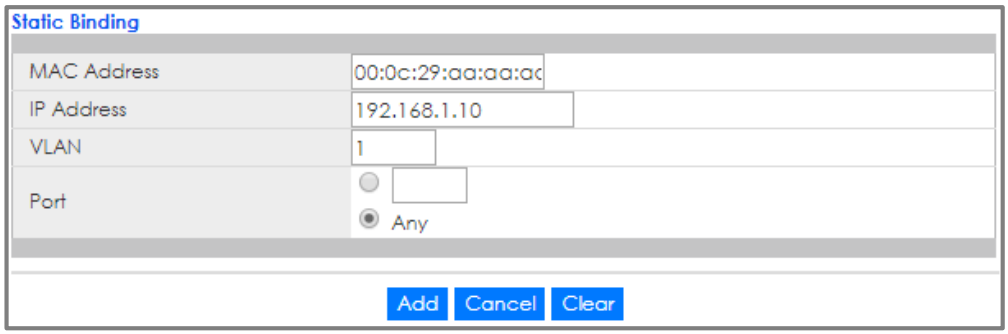
5.9.1 Configuration in the Switch

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

2 Configure **ARP Inspection** (Refer to section **5.7.1**).

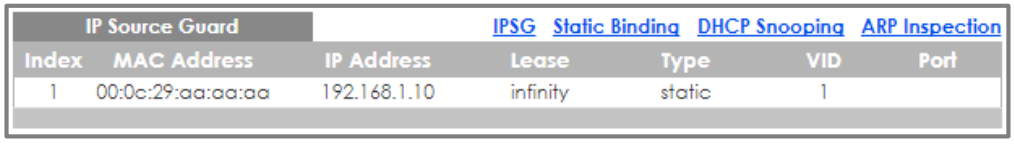
> Note:
> DHCP Snooping and ARP Inspection must be enabled when applying Static Binding.

3 Go to **Advance Application > IP Source Guard > IPv4 Source Guard Setup > Static Binding**. 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 **Add**.



5.9.2 Test the Result

1 Go to **Advance Application > 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.



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.

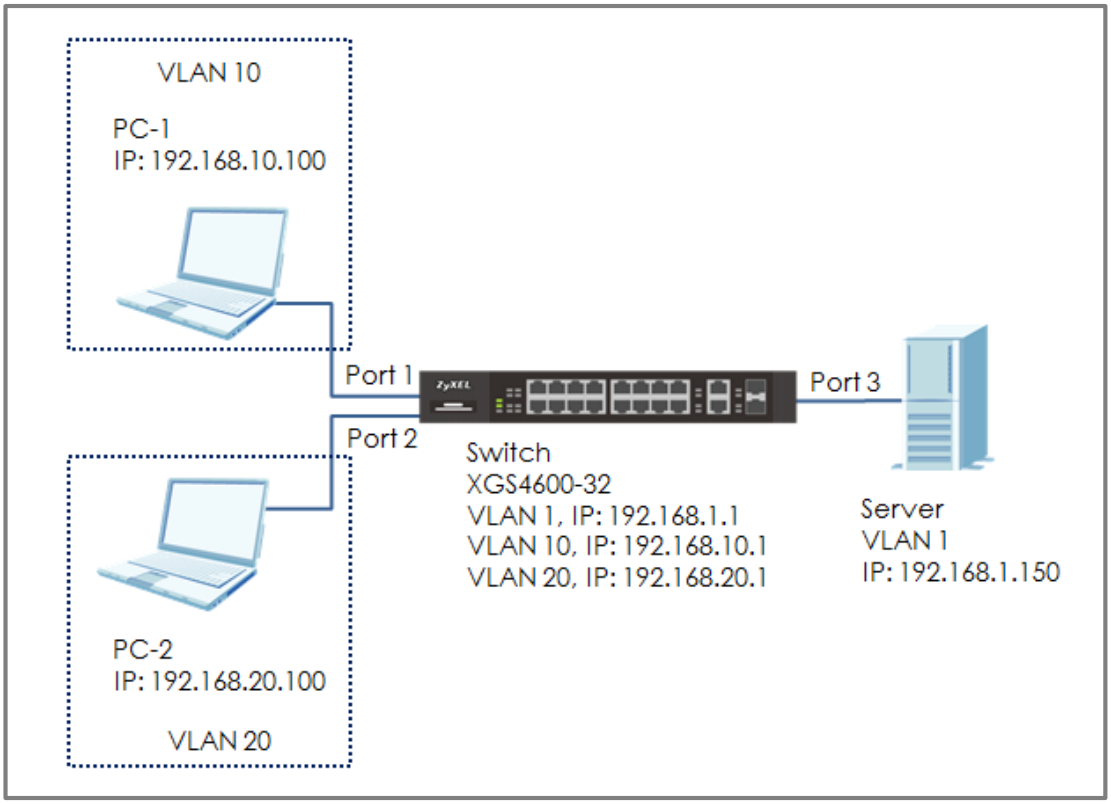


Figure 21 Configure ACL to block unwanted traffic

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 XGS4600-32 (Firmware Version: V4.50).

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**).

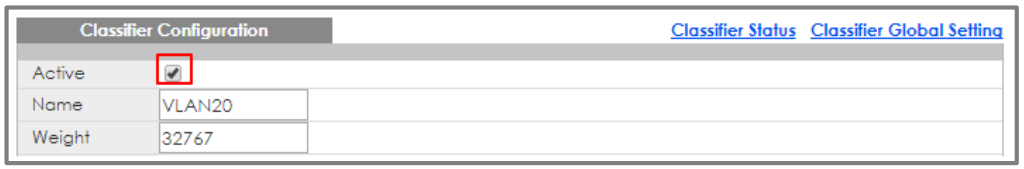
2 Configure the VLAN IP interfaces on Switch (Please refer to the topic: **2.2 How to configure the switch to route traffic across VLANs**)

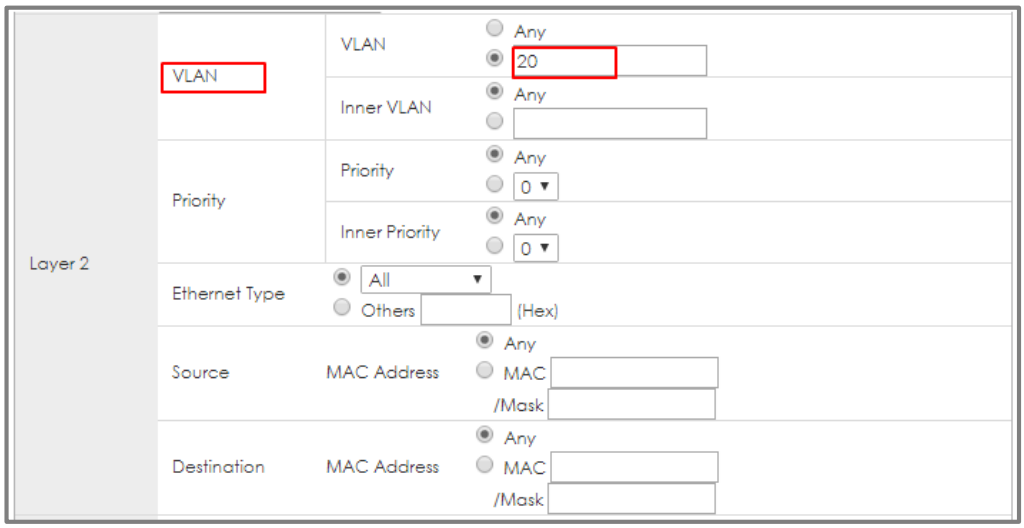
5.10.2 Configure the Classifier

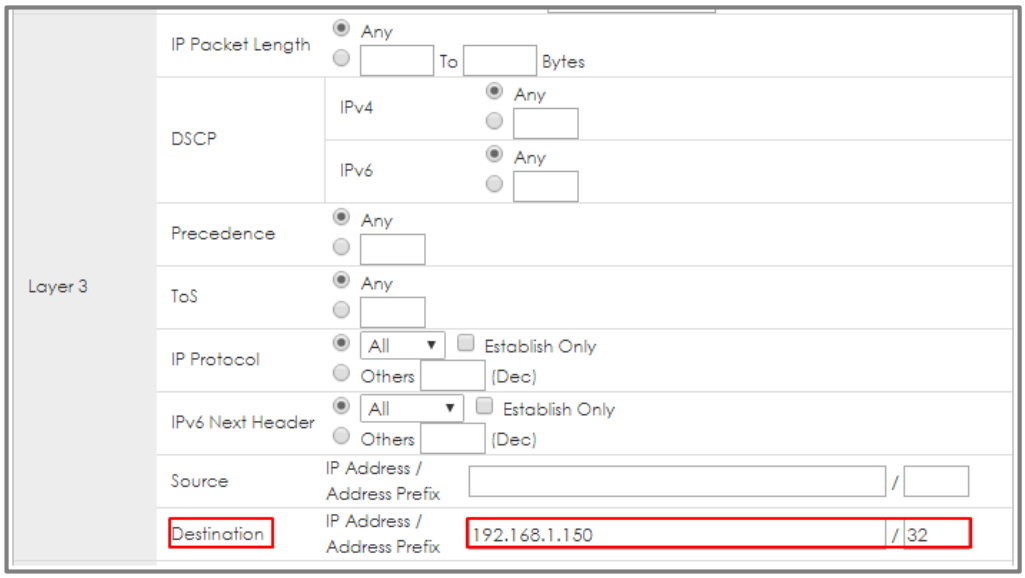
1 Set up the Classifier: Go to **Menu > Advanced Application > Classifier > Classifier Configuration**. Set up Classifier: For VLAN 20.

> 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".

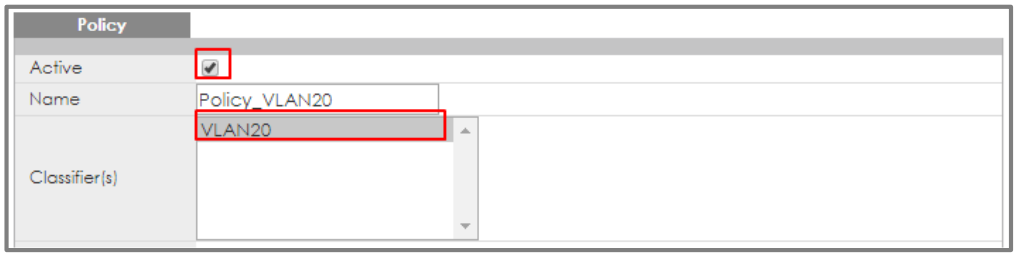





Layer 3
IP Packet Length
Any
To
Bytes
DSCP
IPv4
Any
IPv6
Any
Precedence
Any
ToS
Any
IP Protocol
All
Establish Only
Others
(Dec)
IPv6 Next Header
All
Establish Only
Others
(Dec)
Source
IP Address / Address Prefix
Destination
IP Address / Address Prefix
192.168.1.150
/ 32

5.10.3 Configure the Policy Rule

1 Set up the **Policy Rule**: Go to **Menu > Advanced Application > Policy Rule**. 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".



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
```

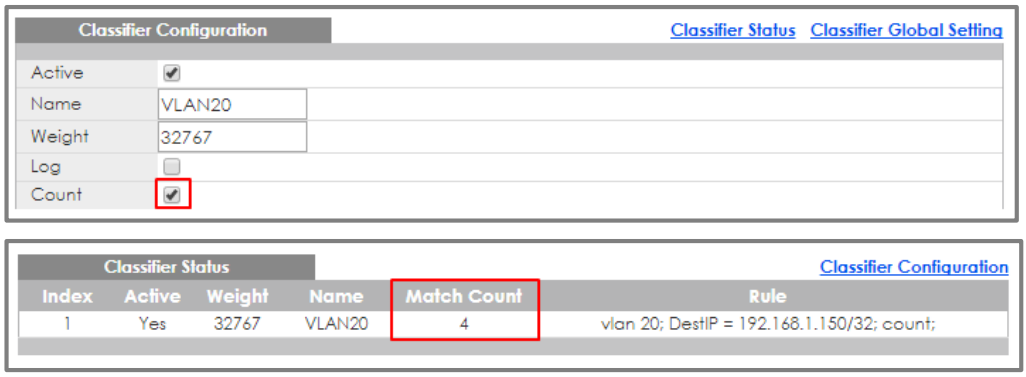
2 Due to the ACL setting, the PC-2 (VLAN 20) cannot ping Server successfully.

```
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.

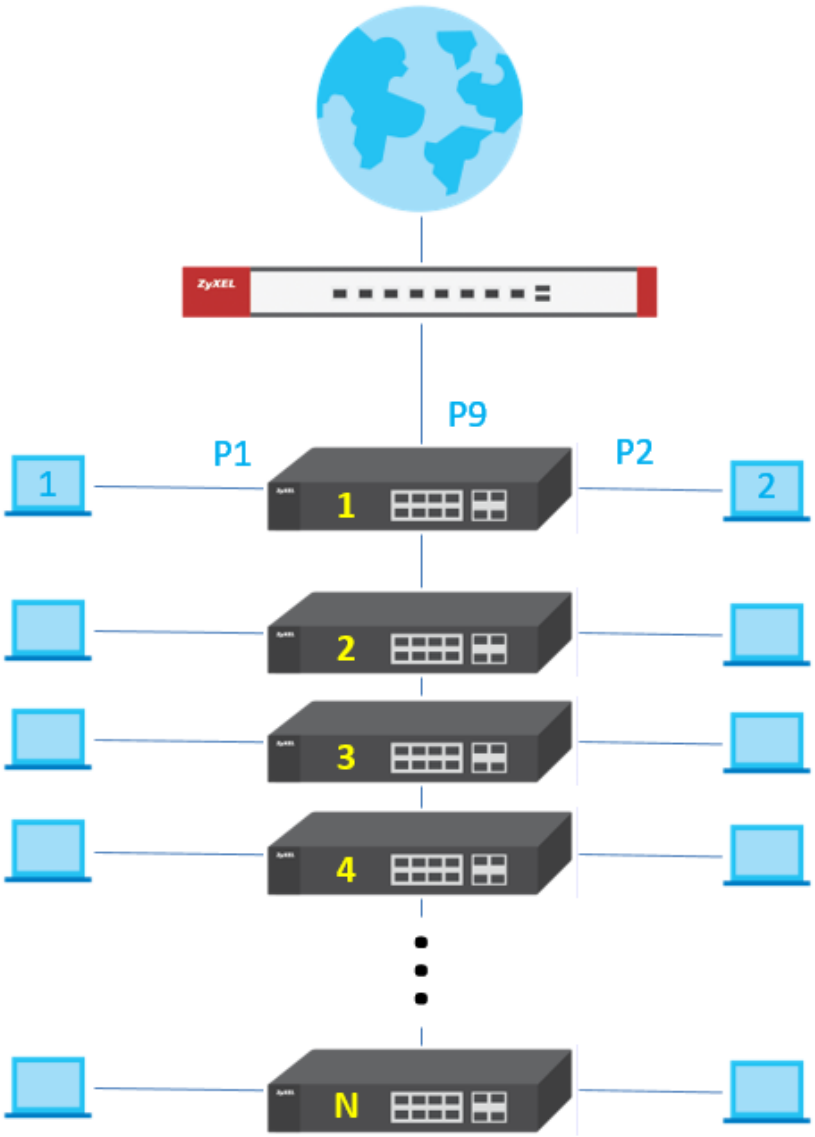
2 Go to **Menu > Advanced Application > Classifier**. Check "Count". If the traffic matches the classifier, the Match Count for this classifier should be increasing every time the web page refreshes.



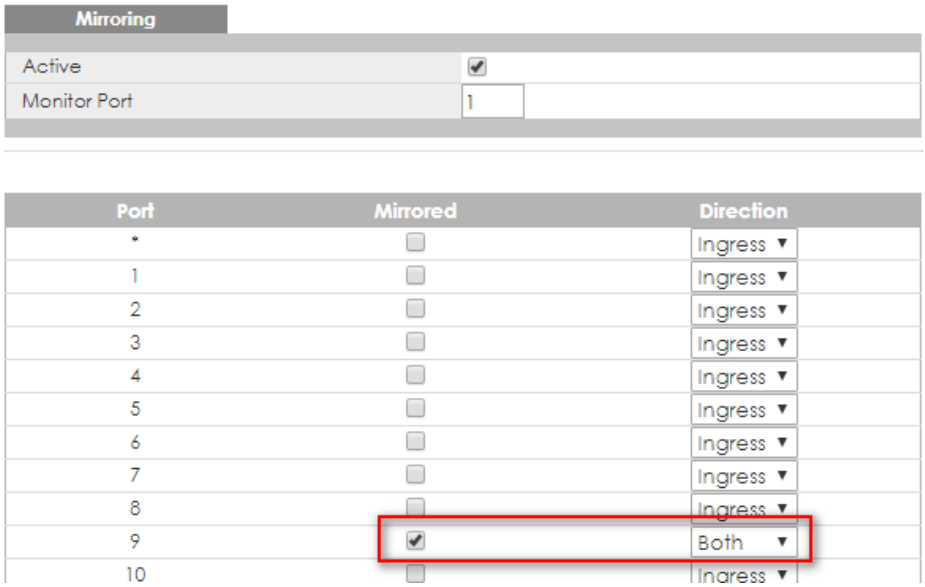
5.11 How to use ACL to mirror traffic of a specific criteria

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.

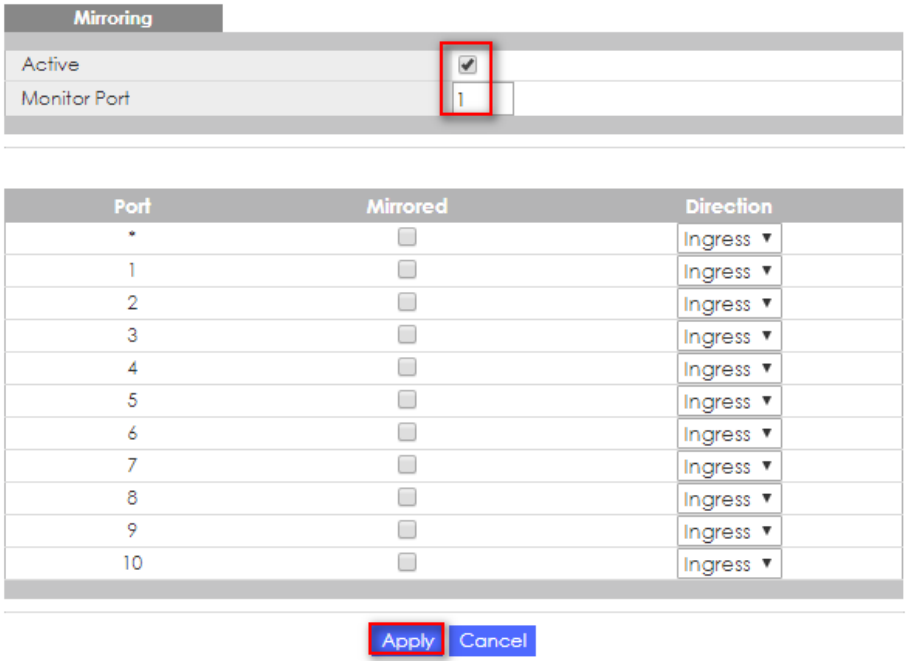
In the following content, it contains a detailed procedure "filtering" the mirrored packets by implementing ACL mirroring in order to monitor traffic of a specific criteria.

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

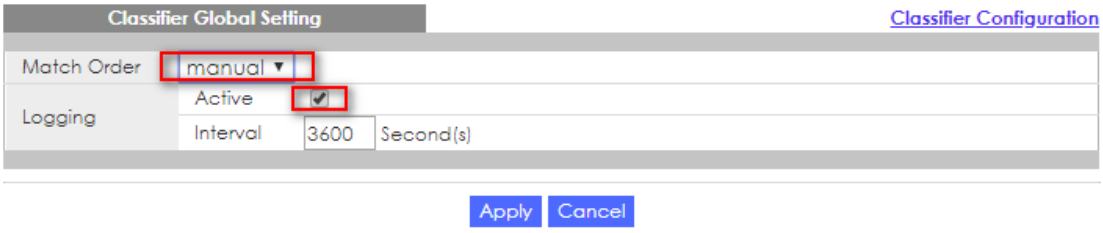
5.11.1 Configuration of ACL

1 Access the web GUI of the Switch-1.

2 Go to **Advanced Application > Mirroring**.
Activate and set port 1 as the Monitor Port.



3 Go to **Advanced Application > Classifier > Classifier Configuration > Classifier Global Setting**.
Set Match Order as "manual", activate "Logging", and apply.

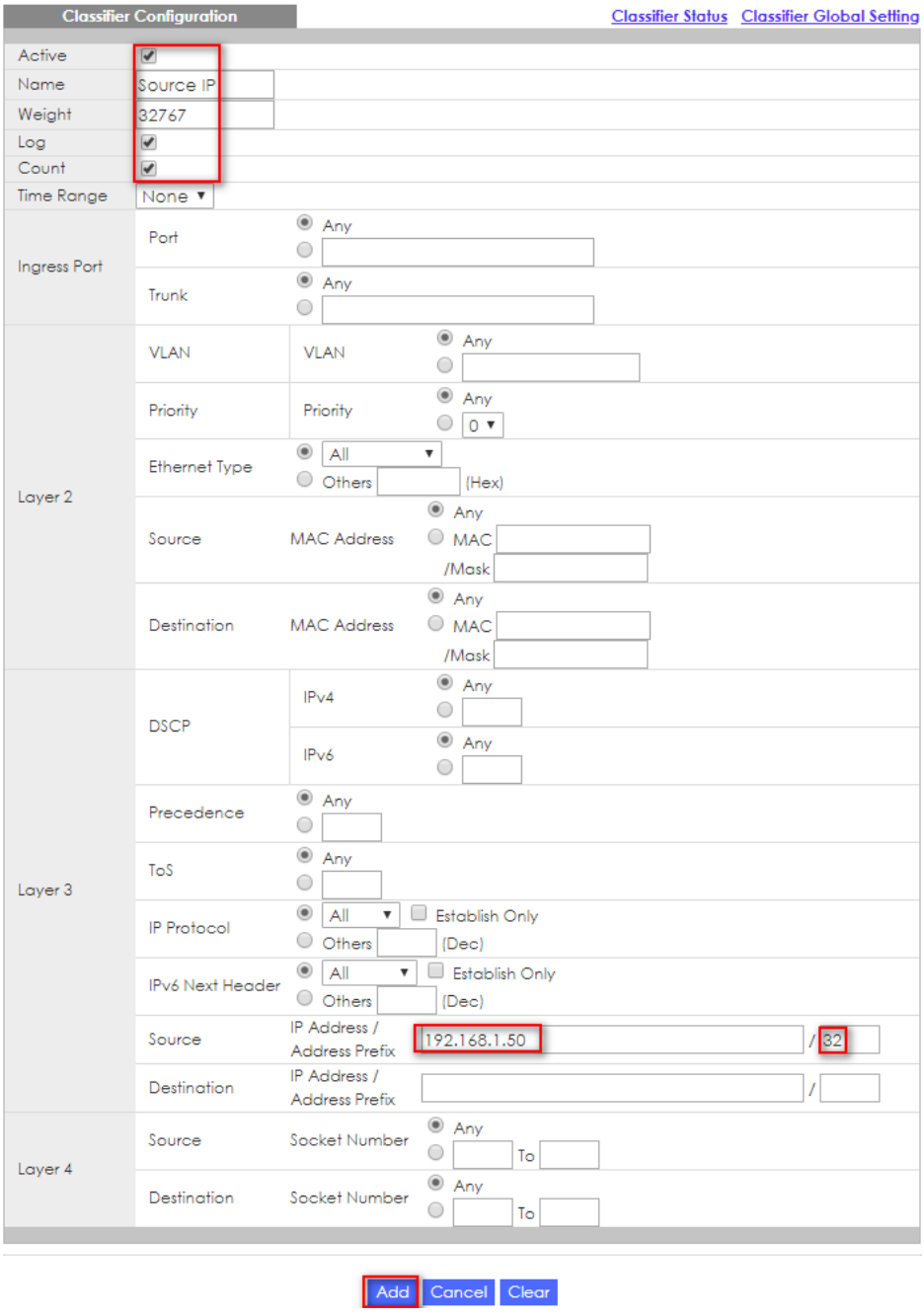


4 Go to **Advanced Application > Classifier > Classifier Configuration**.

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.

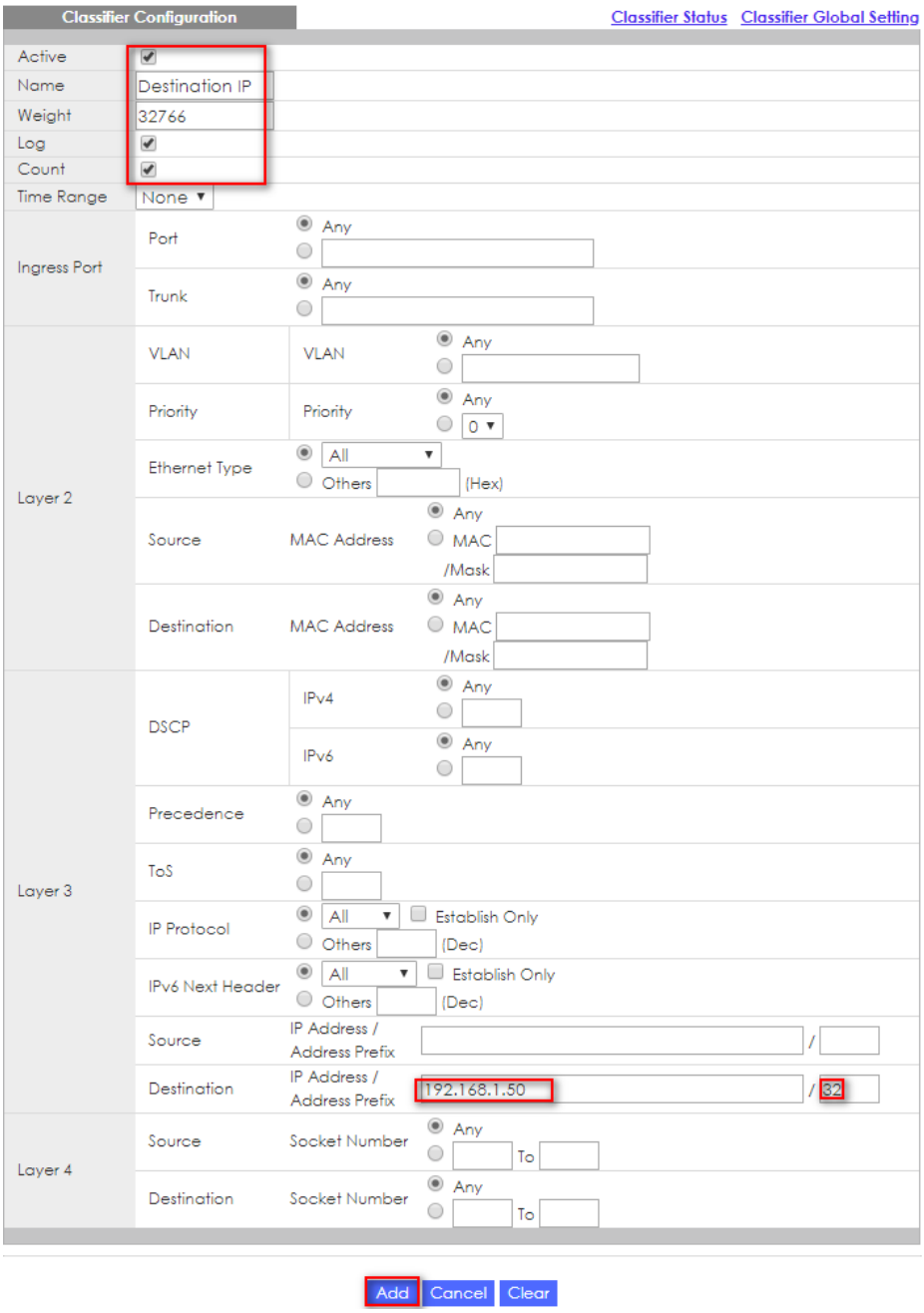


5 Go to **Advanced Application > Classifier > Classifier Configuration**.

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.

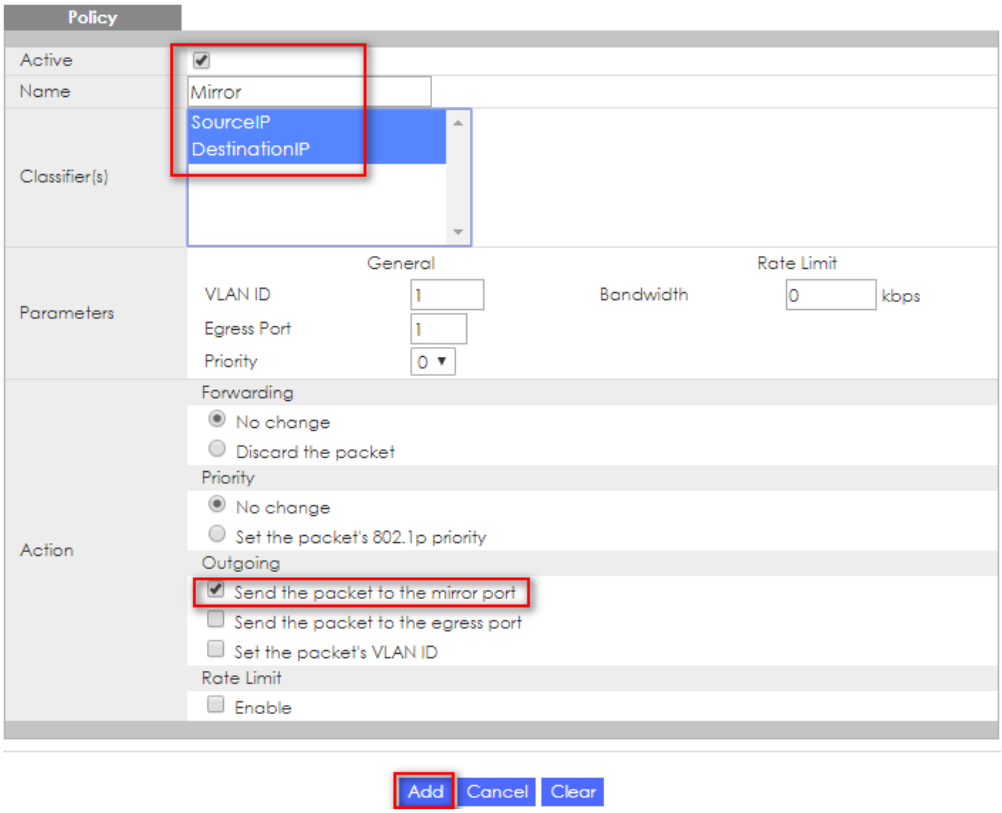


6 Go to **Advanced Application > Policy Rule.**

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.



5.11.2 Test the Result

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

Classifier Status — Classifier Configuration

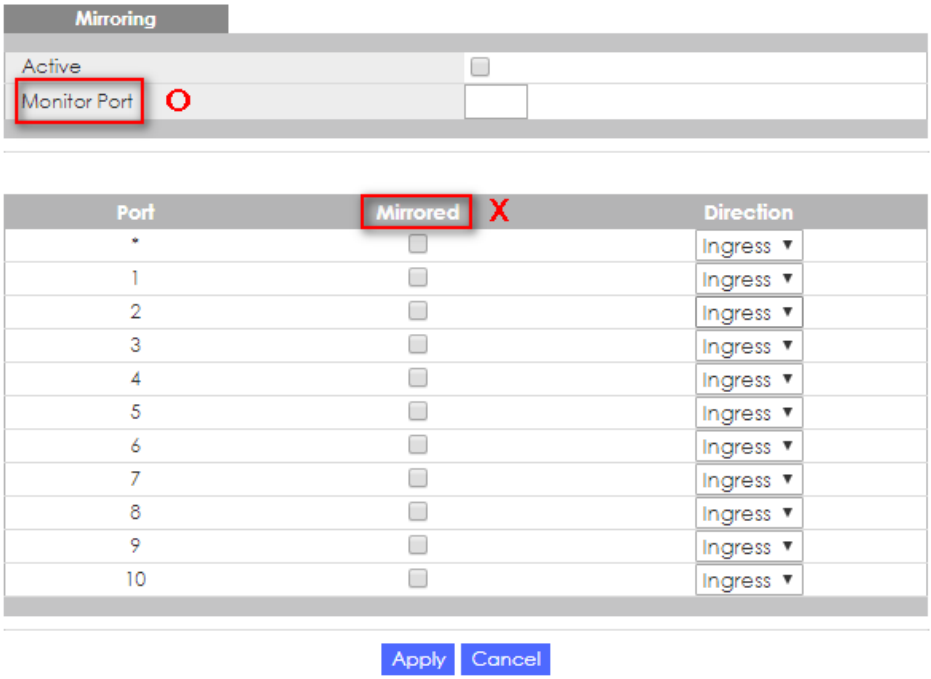
Index	Active	Weight	Name	Match Count	Rule
1	Yes	32767	Source IP	147	SrcIP = 192.168.1.50/32; count; log;
2	Yes	32766	Destination IP	104	DestIP = 192.168.1.50/32; count; log;

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

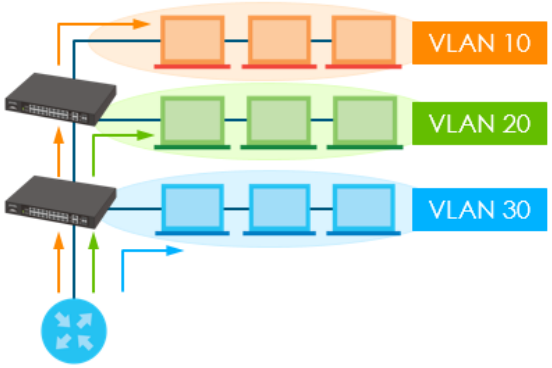
5.11.3 What May Go Wrong

1 In **Advanced Application > 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 **Advanced Application > Mirroring**.

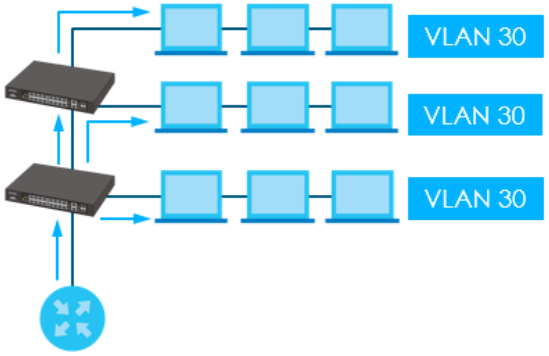


5.12 How to Separate Traffic through L2 Port Isolation

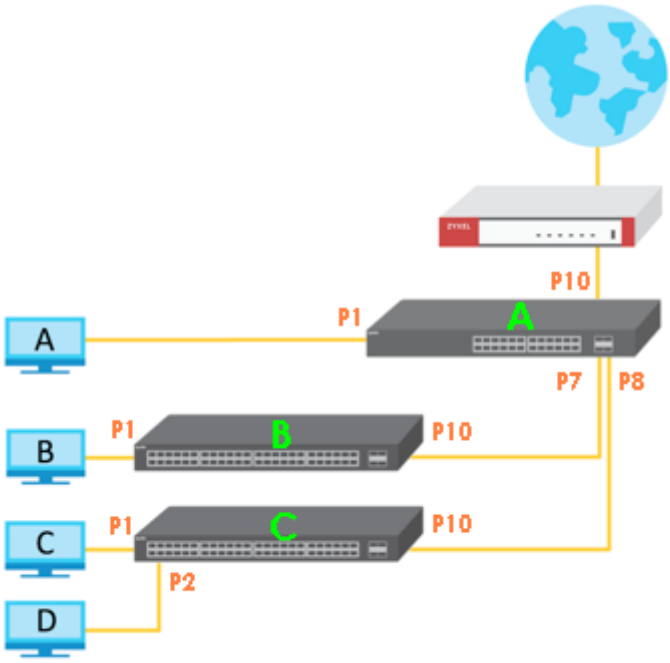
It's a common application that we desire to separate or isolate the mutual traffic between various clients/devices on switches in a network environment.
The most intuitive implementation is to create different VLANs to logically segment a LAN into different broadcast domains to achieve the goal.



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 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 **Advanced Application -> VLAN -> VLAN Configuration -> VLAN Port Setup** to separate traffic between specific ports despite belonging to the same VLAN.



Name	Device	VLAN	IP Address	Subnet Mask
Gateway	USG310	1	192.168.1.254	255.255.255.0
Switch A	GS2210-8	1	192.168.1.1	255.255.255.0
Switch B	GS2210-8	1	192.168.1.2	255.255.255.0
Switch C	GS2210-8	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 GS2210-8 to achieve the goal.

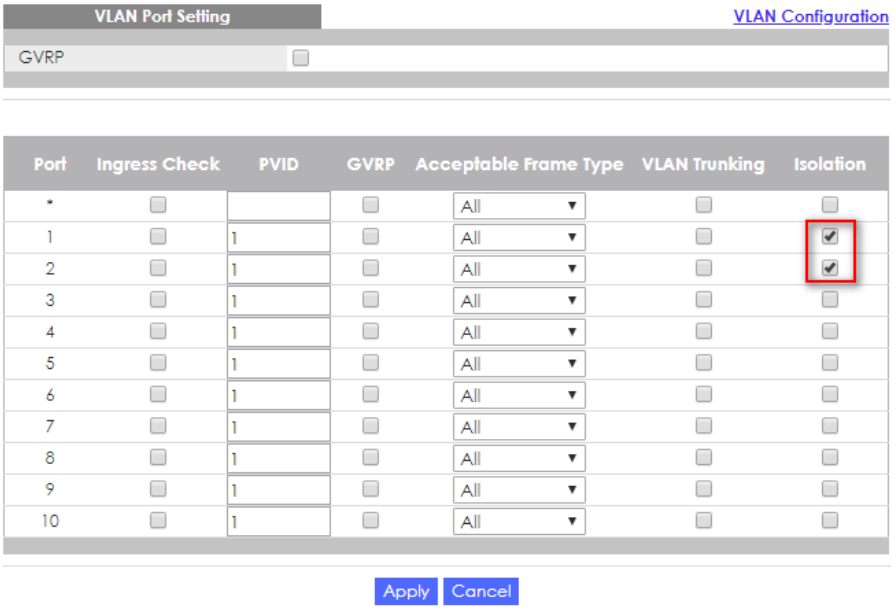
Note:
All network addresses and subnet masks are used as examples in this article. Please replace them with your actual network configuration.

5.12.1 Configuration in the Switch

1 Access Switch C's web GUI.

2 Go to Advance Application > VLAN > VLAN Configuration > VLAN Port Setup

Check Port Isolation for port 1 & 2.

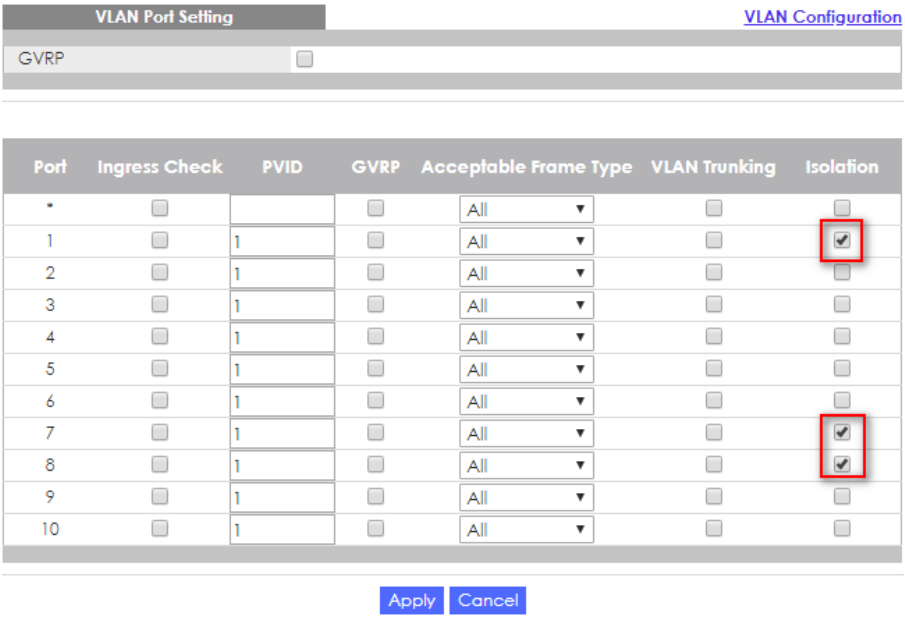


Note:
If there are multiple clients under switch B, follow the same configuration pattern as Switch C. In this case, it's unnecessary since there's only one client under switch B.

3 Access Switch A's web GUI.

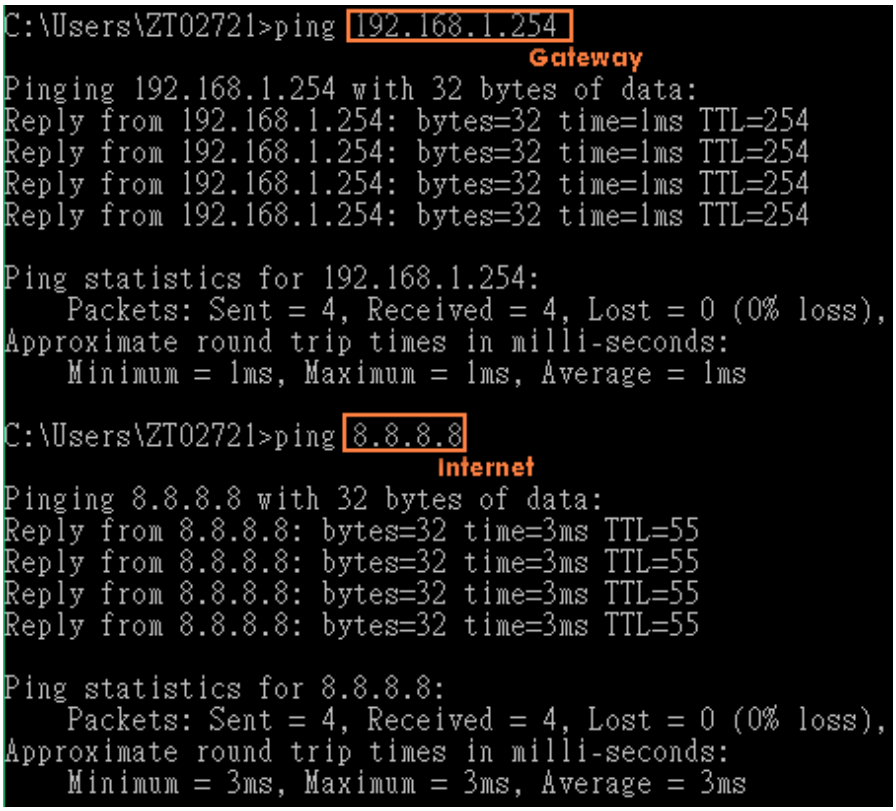
4 Go to Advance Application > VLAN > VLAN Configuration > VLAN Port Setup

Check Port Isolation for port 1, 7 & 8.

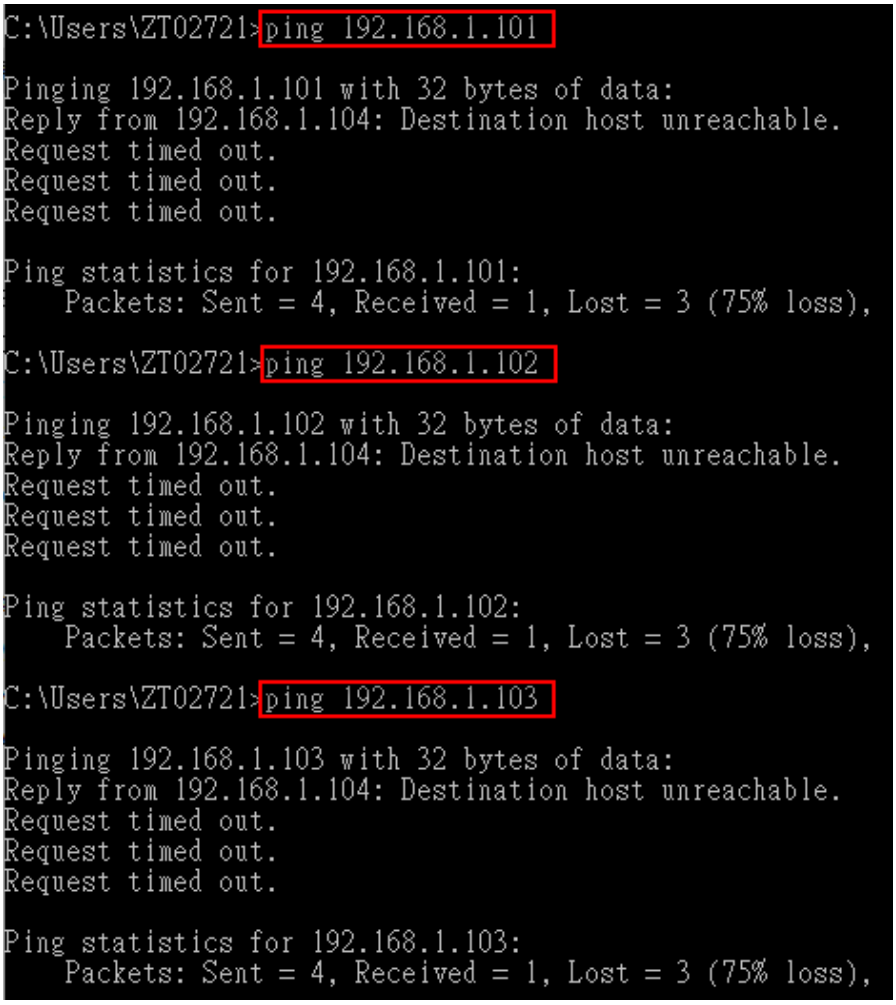


5.12.2 Test the Result

1 Client D can ping Gateway and surf the internet.



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



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.

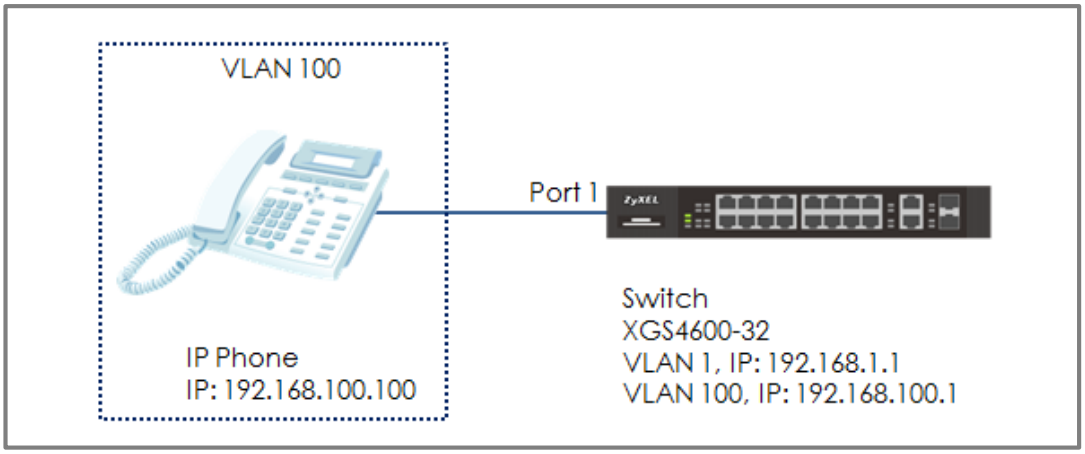


Figure 23 Configure LLDP-MED to assign an IP Phone's VLAN

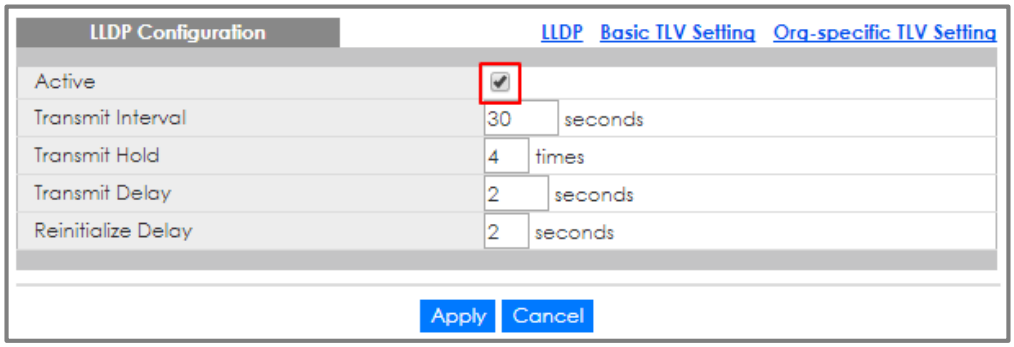
Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using XGS4600-32 (Firmware Version: V4.50).

6.1.1 Configure VLAN for IP Phone

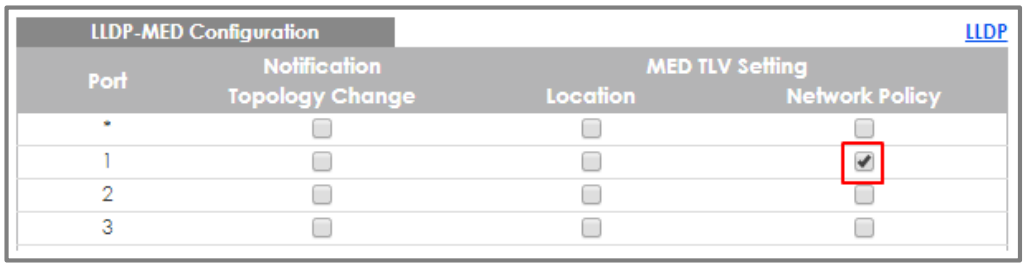
1 Configure VLAN 100 on Switch (Please refer to the topic: **2.1 How to configure the switch to separate traffic between departments**). VLAN 100 is created for the IP Phone.

6.1.2 Configure Switch

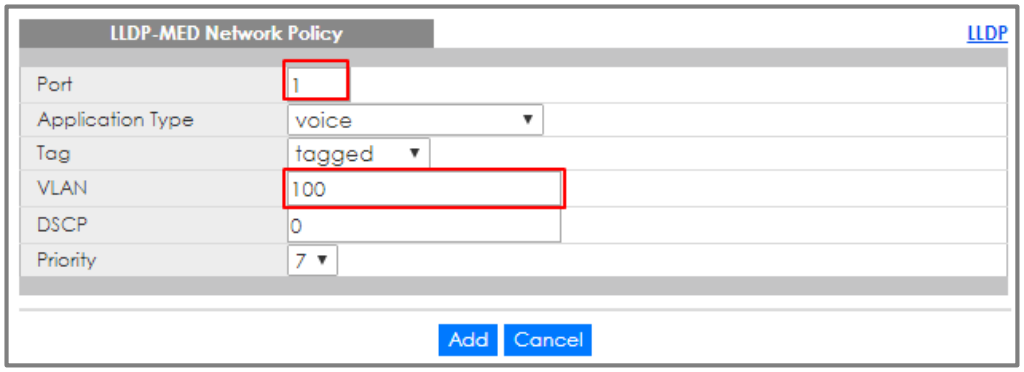
1 Enter the web GUI and go to **Menu > Advanced Application > LLDP > LLDP Configuration**. Make sure that the LLDP configuration is active.



2 Enter web GUI and go to **Menu > Advanced Application > LLDP > LLDP-MED Configuration**. Check the "Network Policy" on port 1 (the port that connects to the IP Phone).

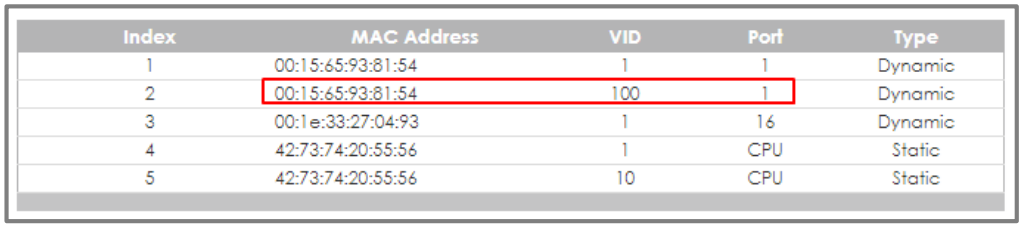


3 Enter the web GUI and go to **Menu > Advanced Application > LLDP > LLDP-MED Network Policy**. Key in the port number as 1 and the VLAN we want to assign the IP Phone to (VLAN 100) and leave DSCP as "0". We can also set the Priority. Click "Add".


LLDP-MED Network Policy
LLDP
Port
1
Application Type
voice
Tag
tagged
VLAN
100
DSCP
0
Priority
7
Add
Cancel

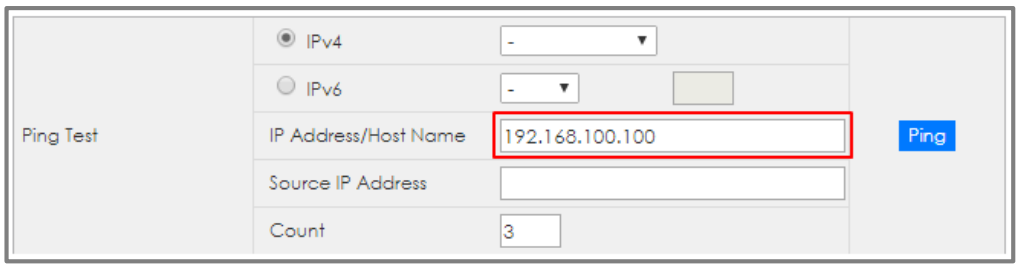
6.1.3 Test the Result

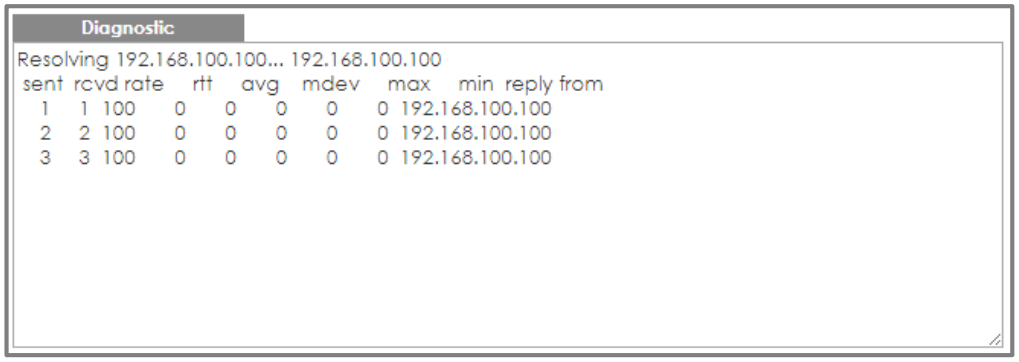
1 Go to **Menu > Management > MAC Table > Search.** Check the MAC table. The IP Phone's MAC address should be in VLAN 100.



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	00:1e:33:27:04:93	1	16	Dynamic
4	42:73:74:20:55:56	1	CPU	Static
5	42:73:74:20:55:56	10	CPU	Static

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





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.

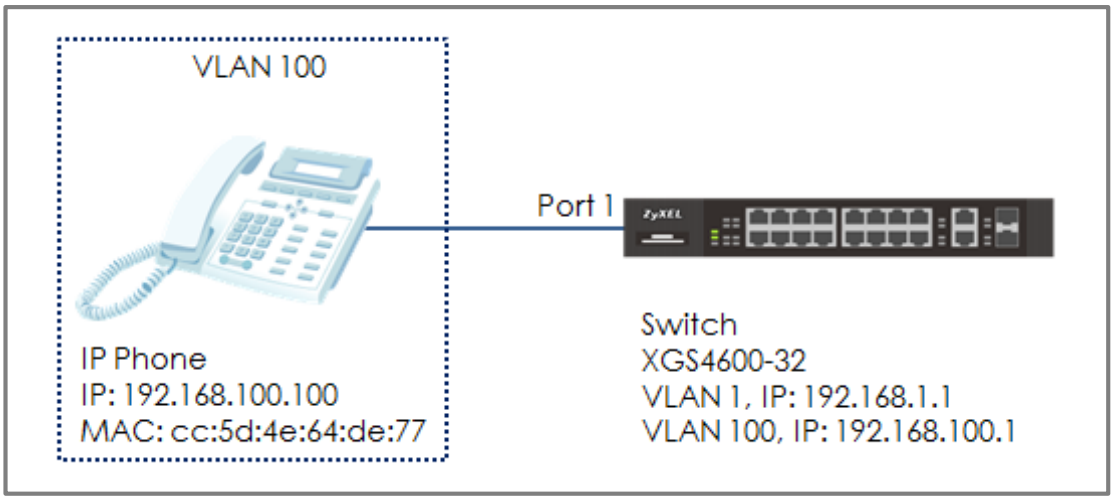


Figure 24 Configure Voice VLAN to separate VOIP traffic from data traffic

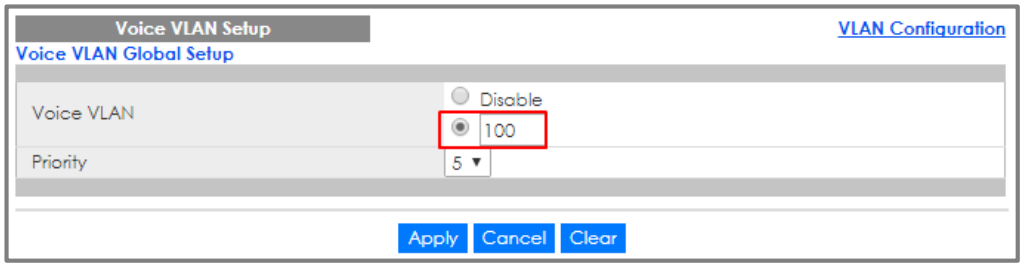
Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using XGS4600-32 (Firmware Version: V4.50).

6.2.1 Configure VLAN 100 for IP Phone

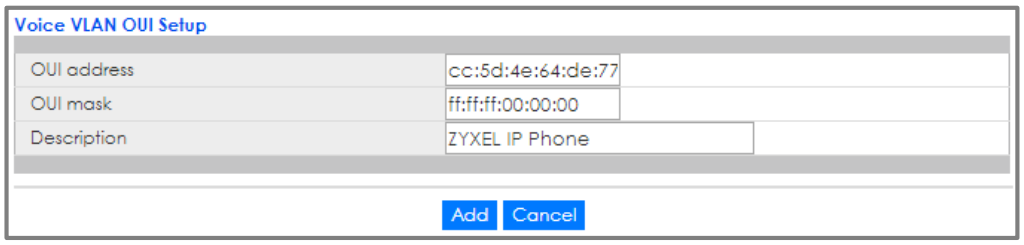
1 Configure VLAN 100 on Switch (Please refer to the topic: **2.1 How to configure the switch to separate traffic between departments**). VLAN 100 is created as the Voice VLAN for the IP Phone.

6.2.2 Configure Voice VLAN

1 Enter the web GUI and go to: **Menu > Advanced Application > VLAN > VLAN Configuration > Voice VLAN Setup**. Input the Voice VLAN. In this example, it is VLAN 100. Click "Apply".



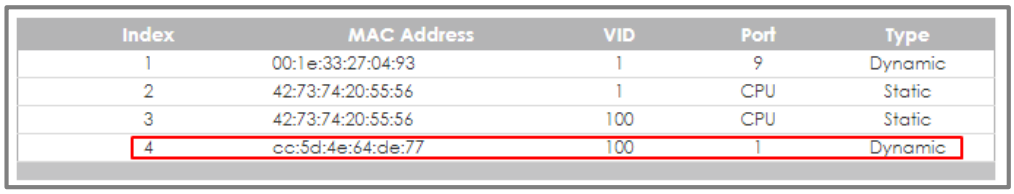
2 Configure the OUI Setup: Enter the web GUI and go to: **Menu > Advanced Application > VLAN > VLAN Configuration > Voice VLAN Setup**. Set the OUI address. (You can key in the MAC address.) In this example, it is cc:5d:4e:64:de:77. Set up the OUI mask as **ff:ff:ff**:00:00:00. Click "Add".



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

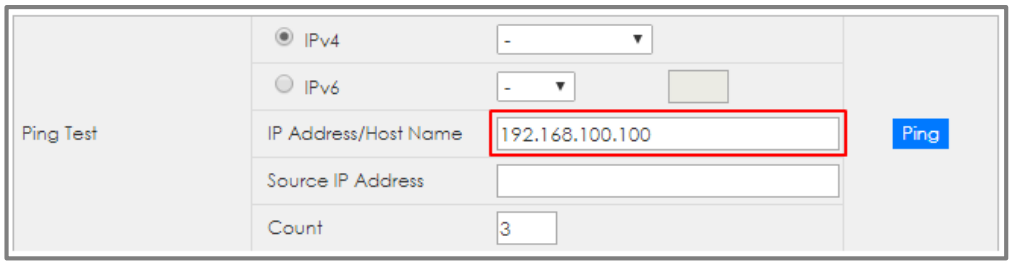
6.2.3 Test the Result

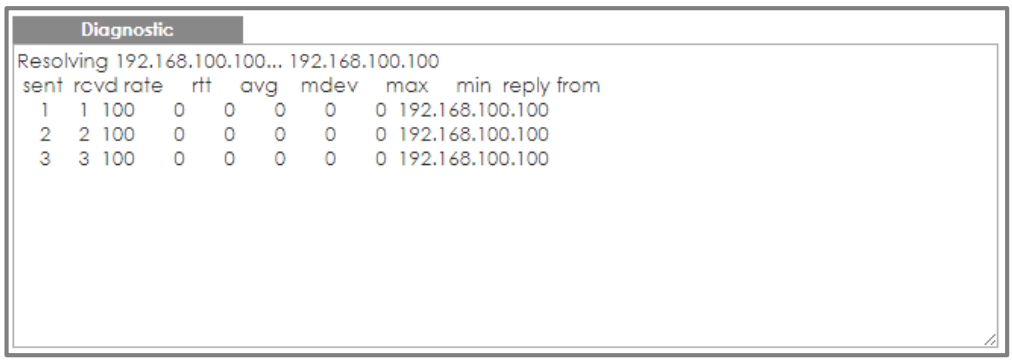
1 Go to **Menu > Management > MAC Table > Search.** Check the MAC address table. The IP Phone is assigned to VLAN 100.



Index	MAC Address	VID	Port	Type
1	00:1e:33:27:04:93	1	9	Dynamic
2	42:73:74:20:55:56	1	CPU	Static
3	42:73:74:20:55:56	100	CPU	Static
4	cc:5d:4e:64:de:77	100	1	Dynamic

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





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.

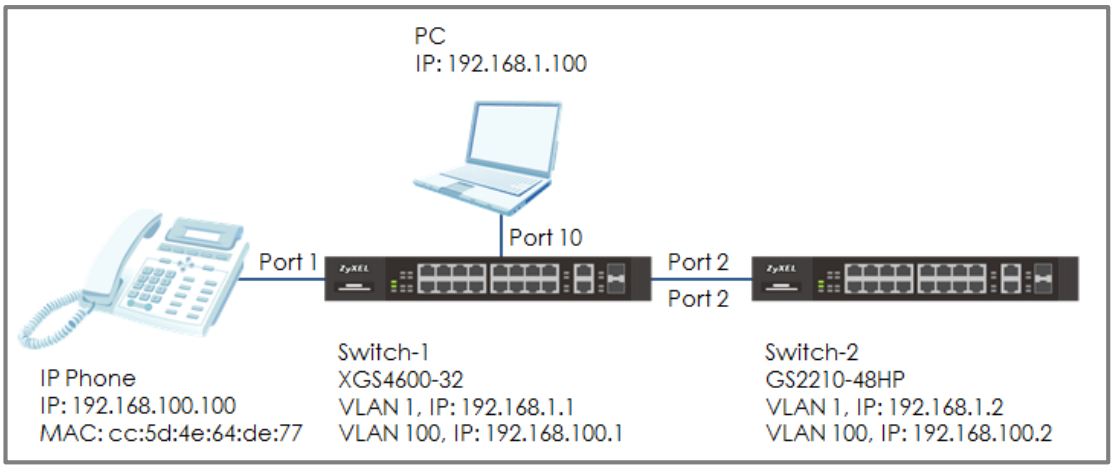


Figure 25 Configure Voice VLAN to separate VOIP traffic from data traffic

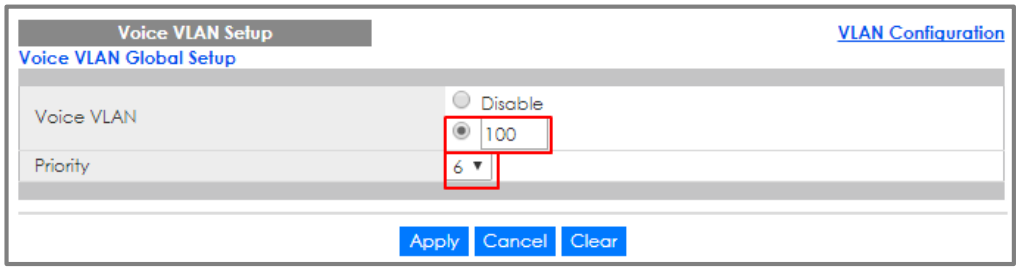
Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using XGS4600-32 (Firmware Version: V4.50) and GS2210-48HP (Firmware Version: V4.30).

6.3.1 Configure VLAN for voice traffic

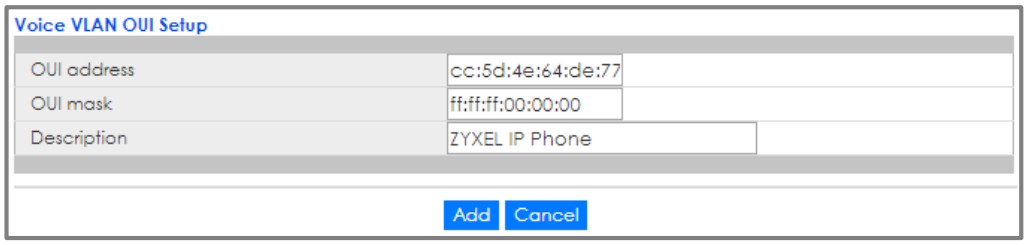
1 Configure VLAN 100 on Switch-1 and Switch-2. (Please refer to the topic: **2.1 How to configure the switch to separate traffic between departments**). VLAN 100 is created for the Voice VLAN. Make sure that devices in VLAN 100 can communicate across Switch-1 and Switch-2.

6.3.2 Configure Voice VLAN

1 Enter the web GUI and go to: **Menu > Advanced Application > VLAN > VLAN Configuration > Voice VLAN 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".



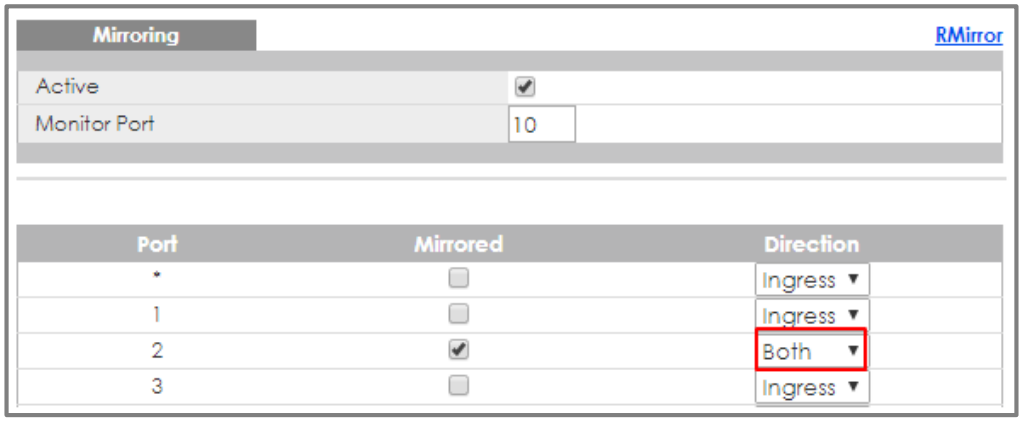
2 Configure the OUI Setup: Enter the web GUI and go to: **Menu > Advanced Application > VLAN > VLAN Configuration > Voice VLAN Setup**. Set the OUI address. (You can key in the MAC address.) In this example, it is cc:5d:4e:64:de:77. Set up the OUI mask as **ff:ff:ff**:00:00:00. Click "Add".



Note:
This will instruct the switch to process any traffic from devices with MAC address between cc:5d:4e:**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 > Advanced Application > 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".

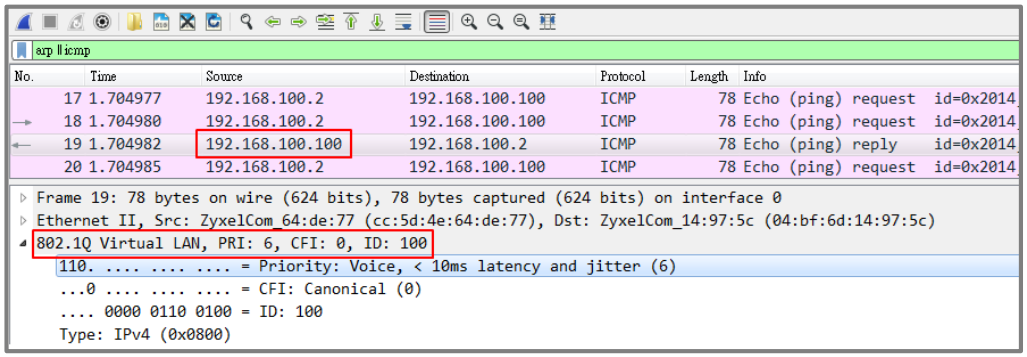


6.3.4 Test the Result

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".



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).

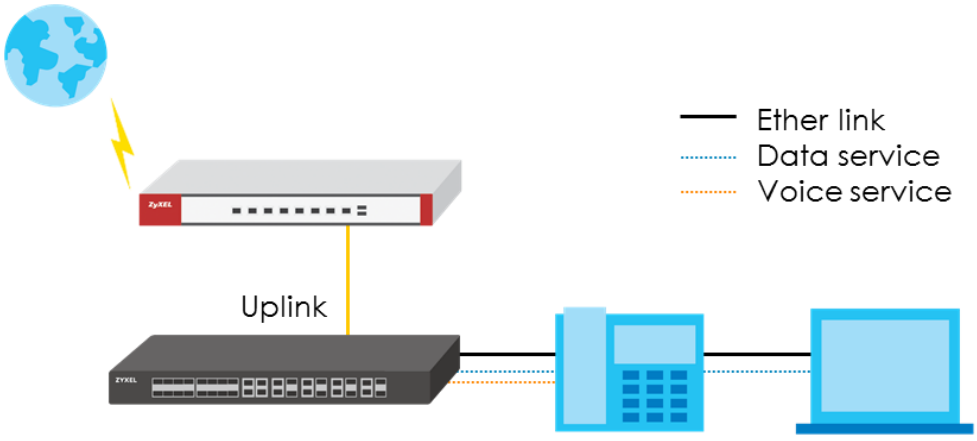
b. If the IP Phone is VLAN **enabled** and this VLAN is different from the switch's **Voice VLAN**: The Switch will **not** apply any changes on the VOIP traffic of the IP Phone.

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.

6.4 How to Configure Voice VLAN on Zyxel Switch

Use voice VLAN to separate voice packets from other service packets. Prioritize the voice packet to enhance the voice quality and user



Nowadays IP phones are commonly used in office environments, to give voice traffic a higher priority is an important consideration when designing a network.

Common scenario of the installation, the IP phone is connected to a switch on one end while linking the PC or laptop on the other end bridging both devices. In this case, Voice VLAN is an important feature used to easily mark and prioritize voice packets from IP phone, separating data packets from the PC.

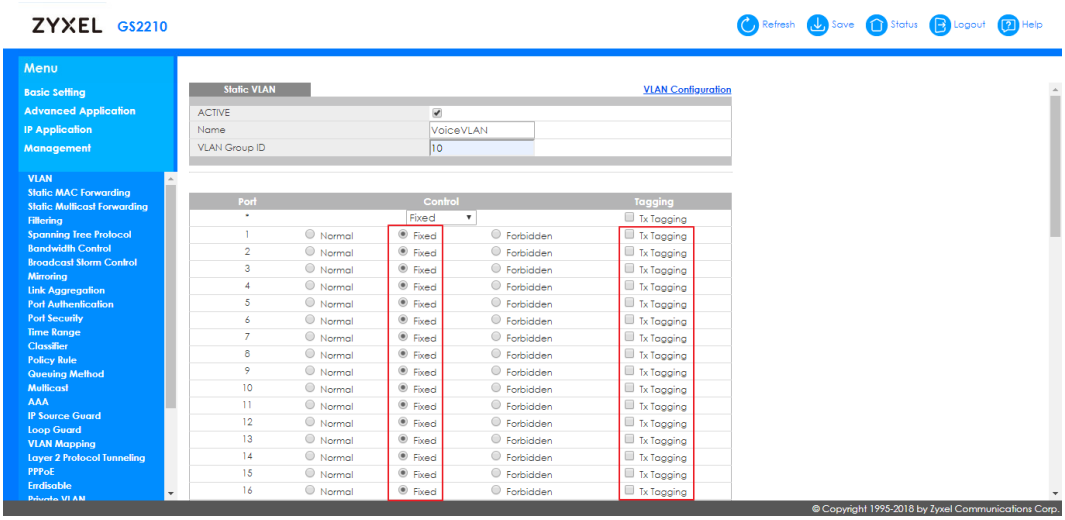
In the following configuration guide, the goal to achieve is to separate traffic between the IP phone and PC without having to set individual VLAN tags for them. The Switch will add VLAN tags for voice & data packets separately upon receiving them and then forwarded to the uplink.

6.4.1 Configuration

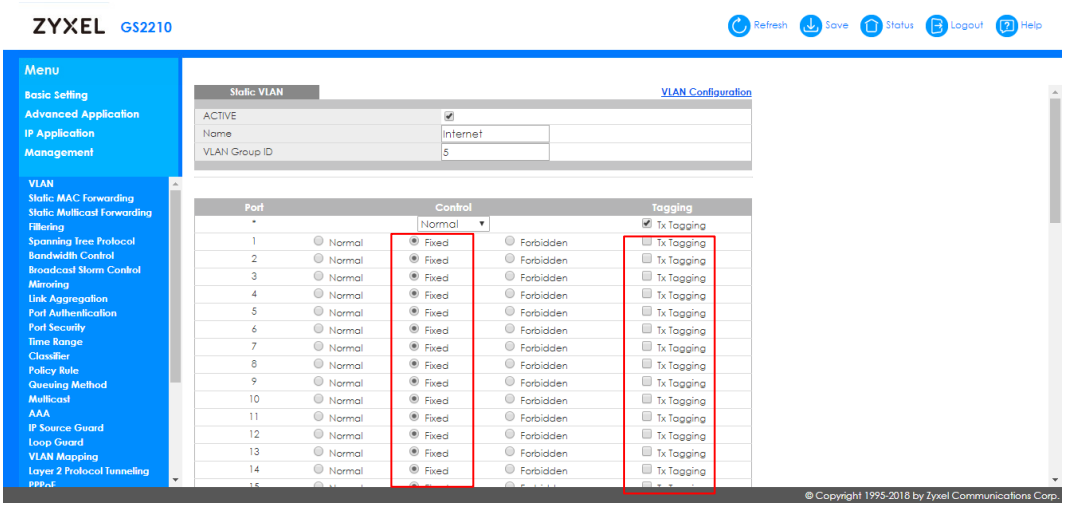
The following steps for standalone switch configuration is applicable to the GS1920 smart managed switch series and above.

Create VLAN interfaces

Create a VLAN for voice packets transmission, select ports which are connected to IP phone, unselect Tx tagging as to save efforts of configuring VLAN on each phones.

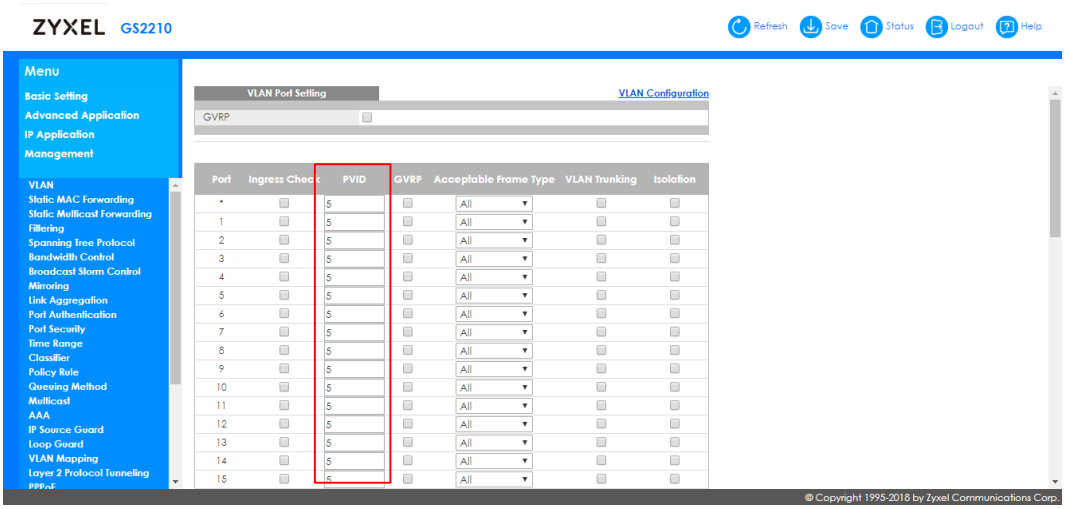


Create another VLAN for data packets, select member ports, unselect Tx tagging.



On the uplink port enable Tx Tagging to transmit packets with VLAN tags.

Configure PVID to separate data packets from voice packets. PVID number should be same as the VLAN number created for data packets.

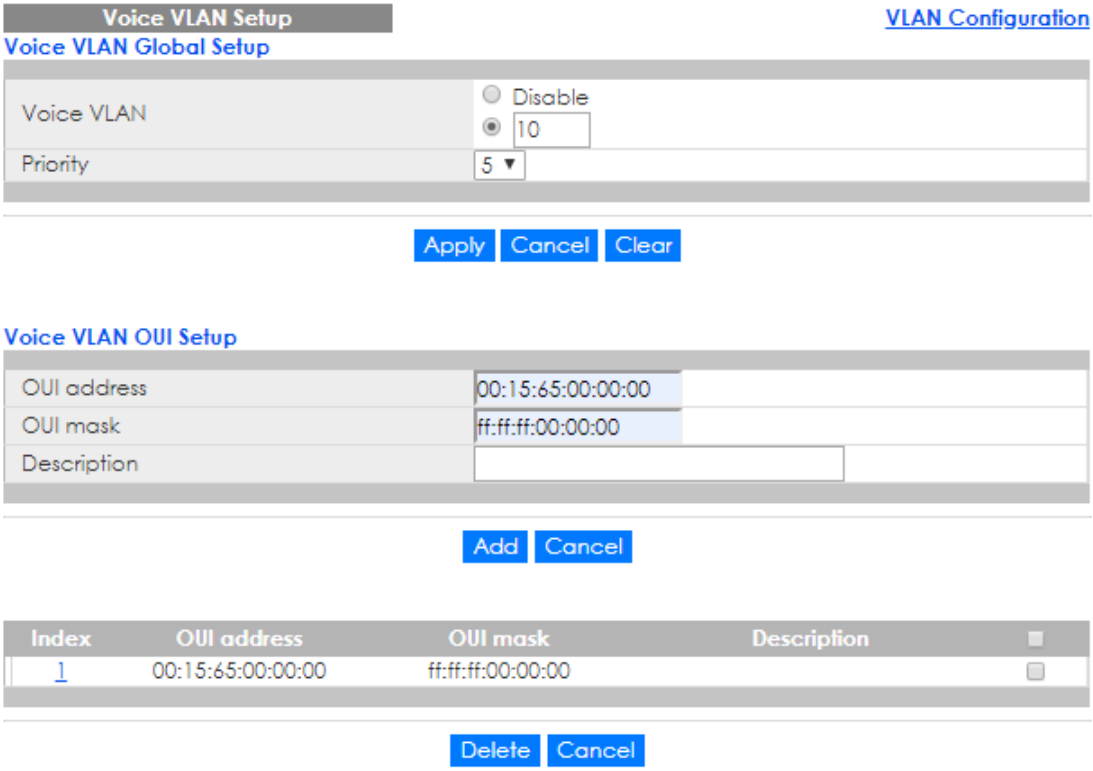


After setting PVID for data packets, next step is to configure "Voice VLAN" feature for the switch to identify the voice packets.

Configure Voice VLAN

Configure Voice VLAN number and priority to prioritize the voice packets. Voice VLAN number should be same as the VLAN number created earlier for voice service packets.

Specify the OUI addresses. OUI are the first 3 bytes of a MAC address that represents the vendor. Through specifying the IP phone MAC address, the switch can identify voice traffic accordingly. Zyxel switch supports up to 6 vendor OUIs.

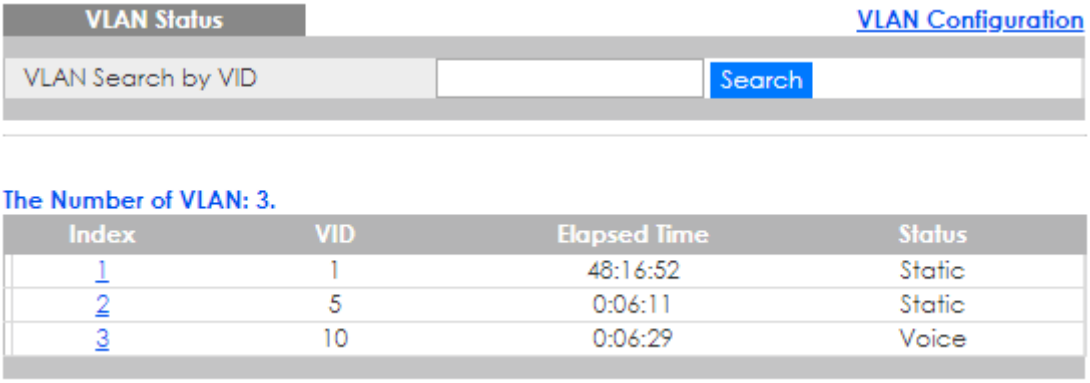


Note:

This guide demonstrates the ease of configuring Voice VLAN on standalone switches. In general, separating VLANs and determine rules for data and voice achieved the goal of prioritizing voice traffic without additional configuration on the IP phones. The applicable model for standalone switches are of GS1920 series and above.

6.4.2 Test the result

Go to the VLAN Configuration to check the VLAN status, you will see the status of VLAN 10 is Voice VLAN.



Index	VID	Elapsed Time	Status
1	1	48:16:52	Static
2	5	0:06:11	Static
3	10	0:06:29	Voice

Check mac address table and you will see the mac address of IP phone is VLAN 10 and the mac address of PC is VLAN 5

Index	MAC Address	VID	Port	Type
1	00:15:65:93:81:54	10	13	Dynamic
2	00:1e:33:28:0a:84	5	13	Dynamic
3	38:d5:47:8d:0b:91	1	24	Dynamic

6.4.3 What Could Go Wrong

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).