

Switch Series

Zyxel GS1920 / GS2210 / XGS2210 / GS3700 /

XGS3700 / XGS4600 / XS1920 / XS3700 / XS3800

Edition 11/2018

Handbook

Default Login Details

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

Contents

Basic principles for network management	7
1.1 How to change the switch management IP address to avoid accessing the wrong device	7
1.1.1 Configuration in the Switch-2.....	8
1.1.2 Test the Result.....	10
1.2 How to configure the switch with a device name to avoid accessing the wrong device	11
1.2.1 Configuration in Switch-1	12
1.2.2 Test the Result.....	13
1.3 How to configure the switch to update the time from an NTP server	14
1.3.1 Configuration in Switch.....	15
1.3.2 Test the Result.....	16
1.3.3 What could go wrong?	18
1.4 How to configure the switch to backup events on a SYSLOG server	19
1.4.1 Configure the Switch-1	20
1.4.2 Test the Result.....	22
1.4.3 What could go wrong?	23
1.5 How to configure the switch with a port name to quickly identify directly connected devices	24
1.5.1 Configure Switch-1	25
1.5.2 Test the Result.....	26
1.6 How to collect the Diagnostic Info	27
1.6.1 Collect the Diagnostic Info from web GUI	28
1.6.2 Test the Result.....	29
1.7 How to change the default administrator password	30
1.7.1 Change the default administrator password	31
1.7.2 Test the Result.....	32
1.8 How to configure a whitelist for remote management to prevent unauthorized access	33
1.8.1 Configure the whitelist of the remote management	34
1.8.2 Test the Result.....	35
1.8.3 What could go wrong?	36
Designing the Local Area Network	37

2.1 How to configure the switch to separate traffic between departments using VLAN	37
2.1.1 Configure Switch-1	38
2.1.2 Configure Switch-2	41
2.1.3 Test the Result.....	43
2.2 How to configure the switch to route traffic across VLANs	44
2.2.1 Configure VLAN 10	45
2.2.2 Configure VLAN 20	47
2.2.3 Set the gateway on PC-1 and PC-2	49
2.2.4 Test the Result.....	51
2.2.5 What could go wrong.....	52
2.3 How to configure the switch to perform DHCP service in a VLAN	53
2.3.1 Configure VLAN 10	54
2.3.2 Configure VLAN 20	56
2.3.3 Configure the Switch and PC.....	58
2.3.4 Test the Result.....	61
2.3.5 What Could Go Wrong.....	62
Improving Network Reliability	63
3.1 How to configure a stacked switch to ensure high server availability	63
3.1.1 Configure Switch-1 and Switch-2 for Stacking	64
3.1.2 Configure Link Aggregation on Stacked switch	66
3.1.3 Configure Link Aggregation on Switch-3.....	67
3.1.4 Test the Result.....	68
3.1.5 What Could Go Wrong.....	69
3.2 How to configure RSTP in a ring topology.....	70
3.2.1 Configure Switch	71
3.2.2 Test the Result.....	74
3.2.3 What Could Go Wrong.....	76
3.3 How to configure VRRP to provide hosts with a redundant gateway	77
3.3.1 Configuration in the Gateway-A.....	78
3.3.2 Configuration in the Gateway-B	81
3.3.3 Test the Result.....	84
3.3.4 What Could Go Wrong?	86
3.4 How to configure bandwidth control to limit incoming or outgoing	

traffic rate	87
3.4.1 Configure Switch	88
3.4.2 Test the Result.....	89
3.5 How to configure ACL to rate limit IP traffic	90
3.5.1 Configure VLAN and Route Traffic	91
3.5.2 Configure the Classifier.....	92
3.5.3 Configure the ACL (Policy Rule)	94
3.5.4 Test the Result.....	96
3.5.5 What Could Go Wrong.....	98
Designing an IPTV Network.....	99
4.1 Introduction for IGMP	99
4.1.1 What are General Queries and Group Specific Queries?	99
4.1.2 What are IGMP Snooping Querier Modes?.....	99
4.1.3 What are the differences between IGMP Snooping fast/normal/immediate leave?	100
4.2 How to configure IGMP routing for multicast clients in a different LAN	101
4.2.1 Configure Switch-1	102
4.2.2 Configure Switch-2	103
4.2.3 Test the Result.....	104
4.2.4 What Could Go Wrong.....	105
4.3 How to configure IGMP Snooping for multicast clients in the same LAN	106
4.3.1 Configure Switch	107
4.3.2 Test the Result.....	108
Network Security.....	109
5.1 How to configure the port security to limit the number of connected devices	109
5.1.1 Configure Switch-1	110
5.1.2 Test the Result.....	111
5.1.3 What Could Go Wrong.....	112
5.2 How to configure MAC filter to block unwanted traffic	113
5.2.1 Configure Switch-1	114
5.2.2 Test the Result.....	115
5.2.3 What Could Go Wrong.....	116
5.3 How to configure the switch to prevent IP scanning.....	117

5.3.1 Configuration in the Switch	118
5.3.2 Test the Result.....	119
5.3.3 What Could Go Wrong?	122
5.4 How to Configure the Switch and RADIUS Server to Provide Network Access through 802.1x Port Authentication	123
5.4.1 Configuration in the Switch	124
5.4.2 Configuration in the RADIUS-Server	126
5.4.3 Test the Result.....	127
5.4.4 What May Go Wrong?.....	131
5.5 How to configure the switch to send unauthorized users in a guest VLAN	132
5.5.1 Configure 802.1x Port Authentication on the Switch	133
5.5.2 Configure VLAN for Guest VLAN	133
5.5.3 Configure Guest VLAN for Failed Authentication.....	133
5.5.4 Configure the RadiusServer	134
5.5.5 Configure the setting on User-A, User-B and Guest.....	135
5.5.6 Test the Result.....	137
5.5.7 What Could Go Wrong.....	139
5.6 How to Configure the Switch and RADIUS Server to Provide Network Access through Device MAC Address	141
5.6.1 Configuration in the Switch	142
5.6.2 Configuration in the RADIUS-Server	144
5.6.3 Test the Result.....	145
5.6.4 What Could Go Wrong?	146
5.7 How to configure the switch to prevent ARP spoofing	147
5.7.1 Configuration in the Switch	148
5.7.2 Test the Result.....	150
5.7.3 What Could Go Wrong?	151
5.8 How to Configure the Switch to Protect Against Rogue DHCP Servers	152
5.8.1 Configuration in the Switch	153
5.8.2 Test the Result.....	156
5.8.3 What Could Go Wrong?	157
5.9 How to configure IPSG static binding for trusted network devices.	158
5.9.1 Configuration in the Switch	159
5.9.2 Test the Result.....	160

5.10 How to configure ACL to block unwanted traffic	161
5.10.1 Configure VLAN and Route Traffic	162
5.10.2 Configure the Classifier	163
5.10.3 Configure the Policy Rule	165
5.10.4 Test the Result	166
5.10.5 What Could Go Wrong	167
Implementing VOIP	168
6.1 How to configure an IP Phone's VLAN using LLDP-MED.....	168
6.1.1 Configure VLAN for IP Phone.....	169
6.1.2 Configure Switch	170
6.1.3 Test the Result.....	172
6.1.4 What Could Go Wrong.....	173
6.2 How to configure the switch to separate VOIP traffic from data traffic	174
6.2.1 Configure VLAN 100 for IP Phone	175
6.2.2 Configure Voice VLAN.....	176
6.2.3 Test the Result.....	177
6.2.4 What Could Go Wrong.....	178
6.3 How to configure the switch to improve Voice traffic quality	179
6.3.1 Configure VLAN for voice traffic	180
6.3.2 Configure Voice VLAN.....	181
6.3.3 Configure Mirroring (For "Test the Result")	182
6.3.4 Test the Result.....	183
6.3.5 What Could Go Wrong.....	184

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.

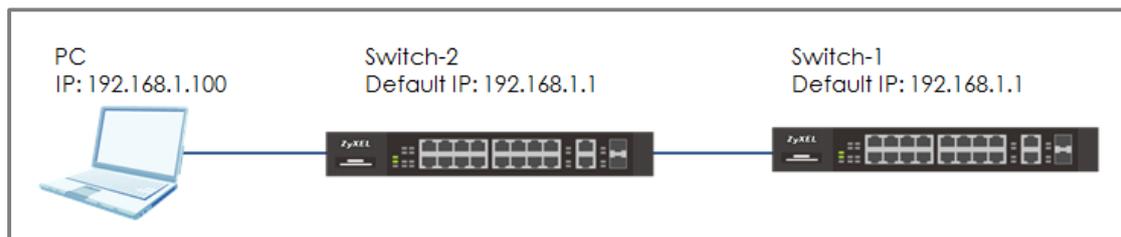


Figure 1 Two switches are using the same default IP address



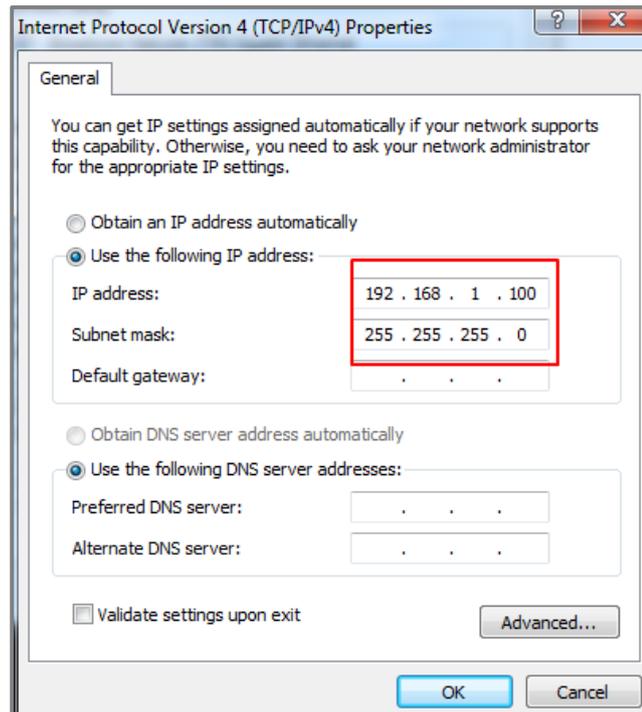
Note:

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).

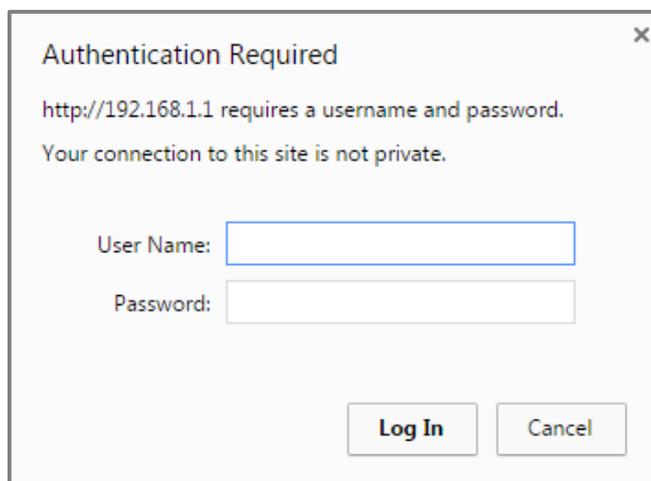
1.1.1 Configuration in the Switch-2

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

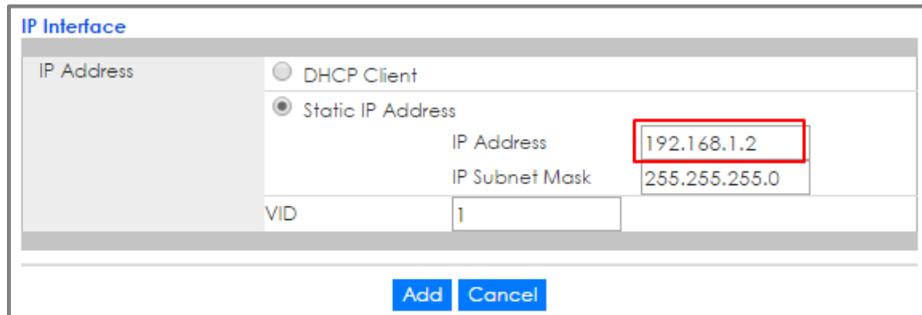
- 2 Set the PC's IP address on to the same subnet as the switches.
For example, set the PC IP address as **192.168.1.100**.



- 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**.



The screenshot shows the 'IP Interface' configuration page. It features a table with the following fields:

IP Interface	
IP Address	<input type="radio"/> DHCP Client
	<input checked="" type="radio"/> Static IP Address
	IP Address: 192.168.1.2
	IP Subnet Mask: 255.255.255.0
VID	1

At the bottom of the form, there are two buttons: 'Add' and 'Cancel'.

- 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**.

IP Status				IP Configuration		
Index	IP Address	IP Subnet Mask	VID	Type	Renew	Release
1	192.168.1.2	255.255.255.0	1	Static		

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

This example shows administrators how to use the Web GUI to manage device name and avoid accessing the wrong devices. As shown below, the PC connects with Switch-1 in the environment. In the default setting, device name (System Name) will be the model name (XGS4600 in this example).

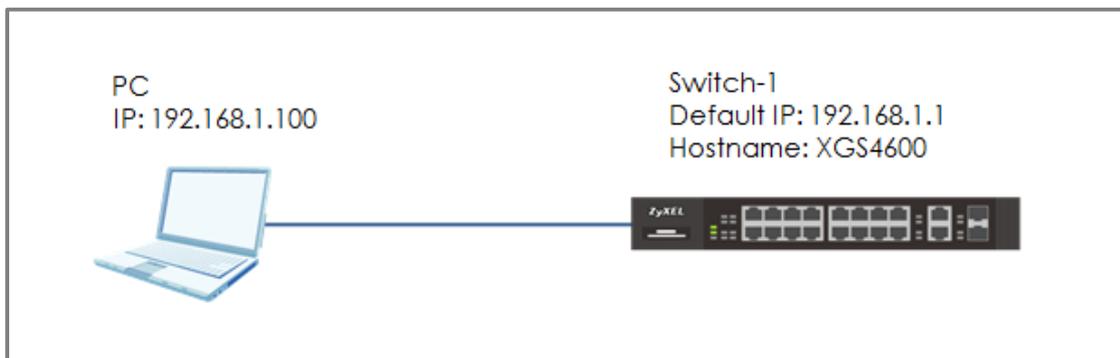


Figure 2 Change the device name of the switch

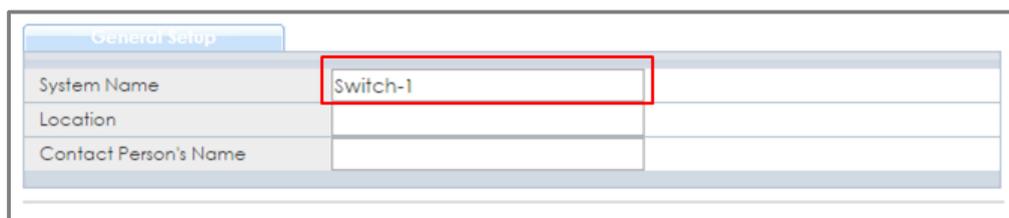


Note:

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).

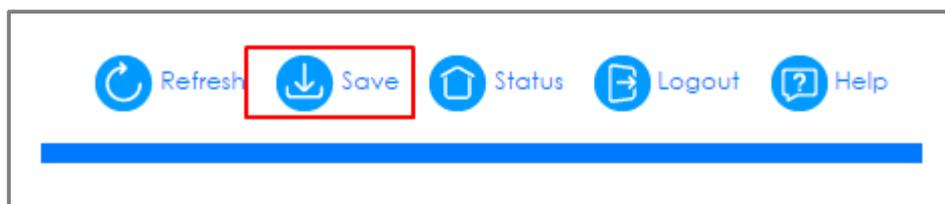
1.2.1 Configuration in Switch-1

- 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**.



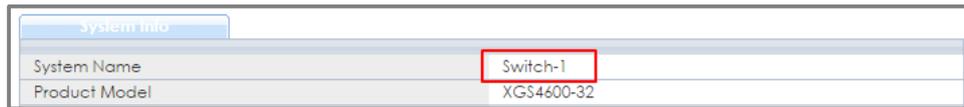
General Setup	
System Name	Switch-1
Location	
Contact Person's Name	

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



1.2.2 Test the Result

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



system info	
System Name	Switch-1
Product Model	XGS4600-32

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.

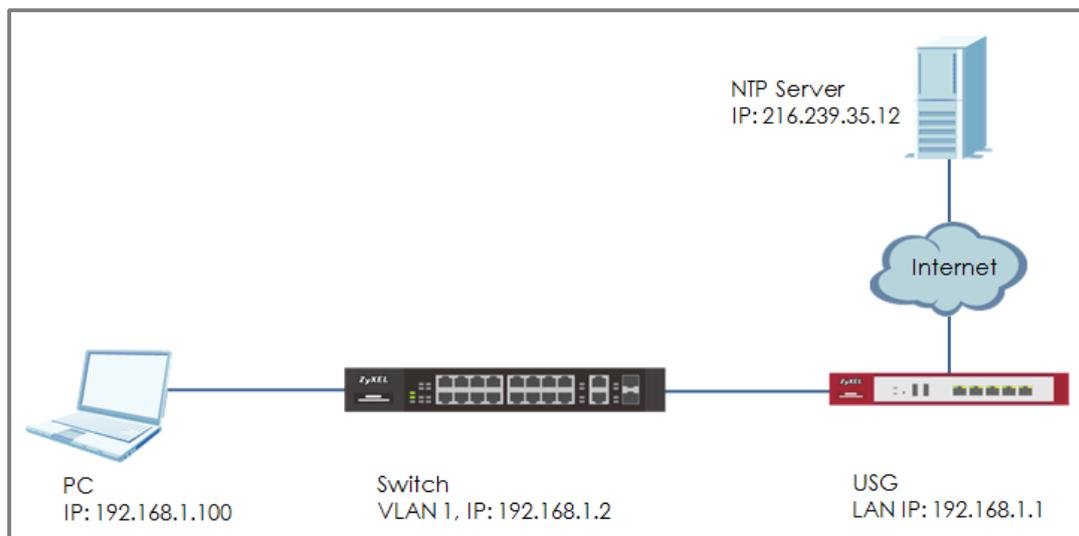


Figure 3 Set up Switch to get time from NTP Server

 **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”**.

IP Configuration		IP Status
Default Gateway	192.168.1.1	
Default Management	<input checked="" type="radio"/> In-band <input type="radio"/> Out-of-band	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

- 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”**.

Use Time Server when Bootup	NTP(RFC-1305) ▼		
Time Server IP Address	216.239.35.12		
Current Time	00	: 34	: 29 UTC
New Time (hh:mm:ss)	00	: 34	: 29
Current Date	2016	- 01	- 01
New Date (yyyy-mm-dd)	2016	- 01	- 01
Time Zone	UTC+0800 ▼		
Daylight Saving Time	<input type="checkbox"/>		
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.			
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>			

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

Refresh
 Save
 Status
 Logout
 Help

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”**.

Use Time Server when Bootup	NTP(RFC-1305) ▼		
Time Server IP Address	216.239.35.12		
Current Time	14	: 18	: 44 UTC+08:00
New Time (hh:mm:ss)	14	: 18	: 44
Current Date	2017	- 06	- 20
New Date (yyyy-mm-dd)	2017	- 06	- 20
Time Zone	UTC+0800 ▼		
Daylight Saving Time	<input type="checkbox"/>		
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](#)

 Refresh

 Save

 Status

 Logout

 Help

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

Use Time Server when Bootup	None ▼		
Time Server IP Address	216.239.35.12		
Current Time	14	: 18	: 45 UTC+08:00
New Time (hh:mm:ss)	14	: 18	: 45
Current Date	2017	- 06	- 20
New Date (yyyy-mm-dd)	2017	- 06	- 20
Time Zone	UTC+0800 ▼		
Daylight Saving Time	<input type="checkbox"/>		
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](#)

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	<input type="checkbox"/>		
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.

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"**.

The screenshot shows the 'Diagnostic' section of the ZyXel web interface. A table displays the results of a ping test to the IP address 216.239.35.12. The table is highlighted with a red border. Below the table, the 'Ping Test' configuration is visible, also with a red border around the IPv4 selection, mode, and IP address field. A blue 'Ping' button is located to the right of the configuration fields.

Diagnostic									
Resolving 216.239.35.12... 216.239.35.12									
	sent	rcvd	rate	rtt	avg	mdev	max	min	reply from
1	1	100	10	10	0	10	10	10	216.239.35.12
2	2	100	10	10	0	10	10	10	216.239.35.12
3	3	100	10	10	0	10	10	10	216.239.35.12

Ping Test configuration:

- Protocol: IPv4
- Mode: in-band
- IP Address/Host Name: 216.239.35.12
- Source IP Address: (empty)
- Count: 3

[Ping](#)

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

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

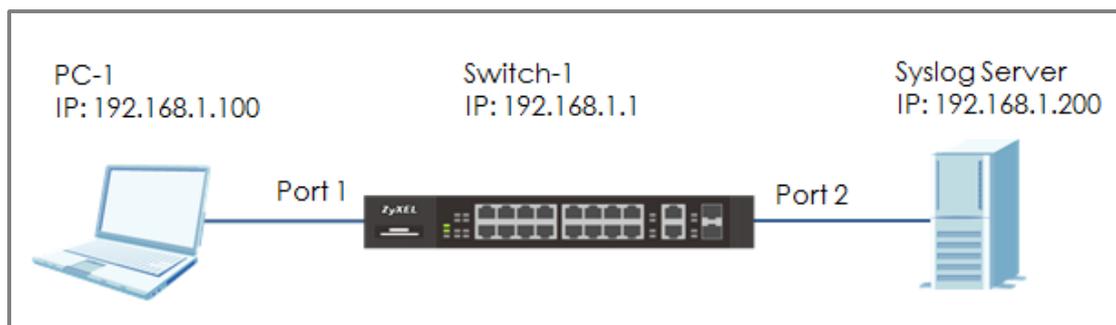


Figure 4 Upload the syslog automatically to the server



Note:

All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using 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"**.

Syslog Server Setup

Active	<input checked="" type="checkbox"/>
Server Address	192.168.1.200
UDP Port	514
Log Level	Level 0-7 ▼



Note:

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

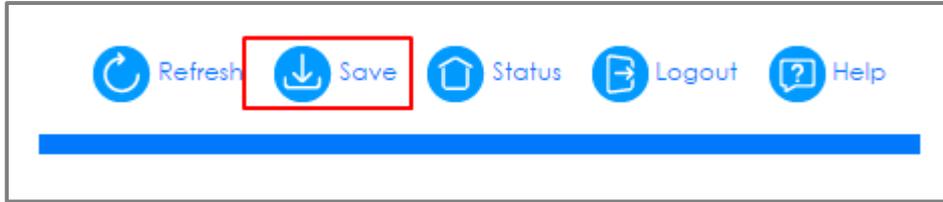
- 2 In the same page, activate the **Syslog** and activate the logging type you prefer. Also, remember to click **"Apply"**.

Syslog Setup

Syslog

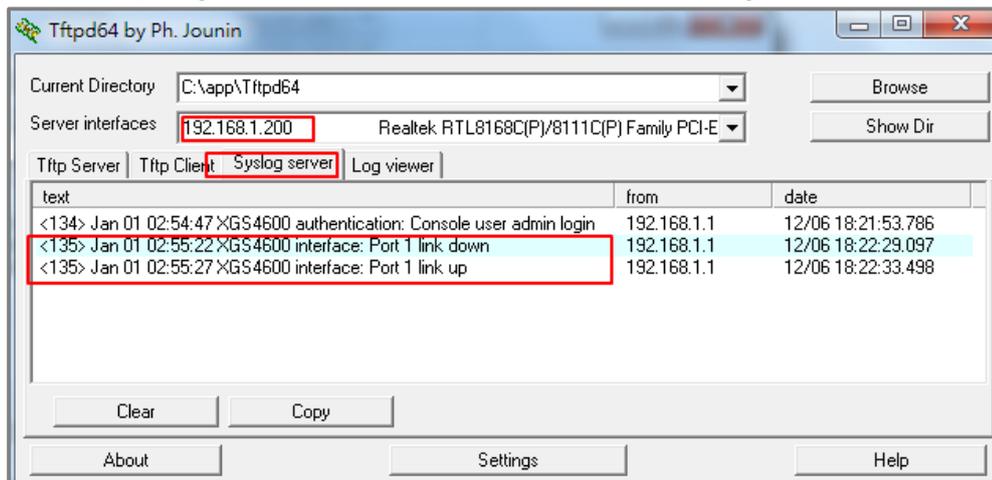
Logging type	Active	Facility
System	<input checked="" type="checkbox"/>	local use 0 ▼
Interface	<input checked="" type="checkbox"/>	local use 0 ▼
Switch	<input checked="" type="checkbox"/>	local use 0 ▼
AAA	<input checked="" type="checkbox"/>	local use 0 ▼
IP	<input checked="" type="checkbox"/>	local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

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

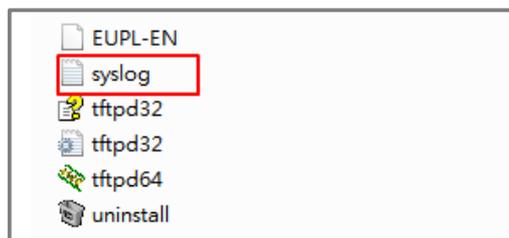


1.4.2 Test the Result

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

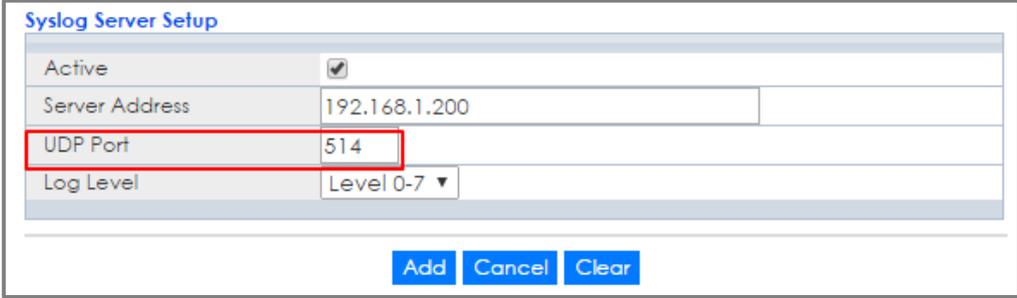


- 3 We can also check the **directory** ("C:\app\Tftpd64" in this example) to find out if a text file is created on the Syslog Server.



1.4.3 What could go wrong?

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



The screenshot shows the 'Syslog Server Setup' configuration page. It includes a table with the following fields and values:

Syslog Server Setup	
Active	<input checked="" type="checkbox"/>
Server Address	192.168.1.200
UDP Port	514
Log Level	Level 0-7 ▼

At the bottom of the form, there are three buttons: 'Add', 'Cancel', and 'Clear'.

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

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

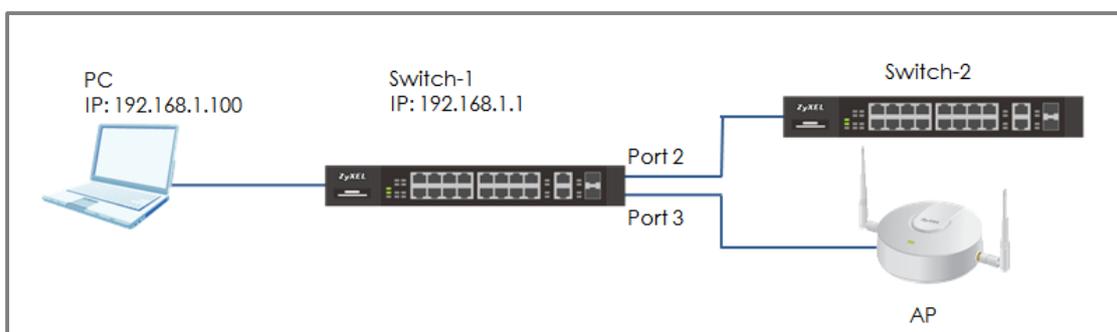


Figure 5 Configure the port name of the switch



Note:

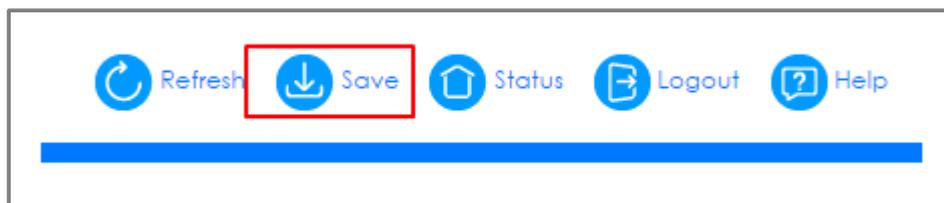
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using XGS4600-32 (Firmware Version: V4.50).

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”**.

Port	Active	Name	Type	Speed / Duplex	Flow Control	802.1p Priority	BPDU Control	Media Type
*	<input type="checkbox"/>		-	10G / Full Duplex	<input type="checkbox"/>	0	Peer	sfp_plus
1	<input checked="" type="checkbox"/>		10/100/1000M	Auto-1000M	<input type="checkbox"/>	0	Peer	
2	<input checked="" type="checkbox"/>	Switch-2	10/100/1000M	Auto-1000M	<input type="checkbox"/>	0	Peer	
3	<input checked="" type="checkbox"/>	AP	10/100/1000M	Auto-1000M	<input type="checkbox"/>	0	Peer	

- 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	Down	STOP	Disabled	3140	756	0	0.0	0.0	0:00:00
5	Down	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.

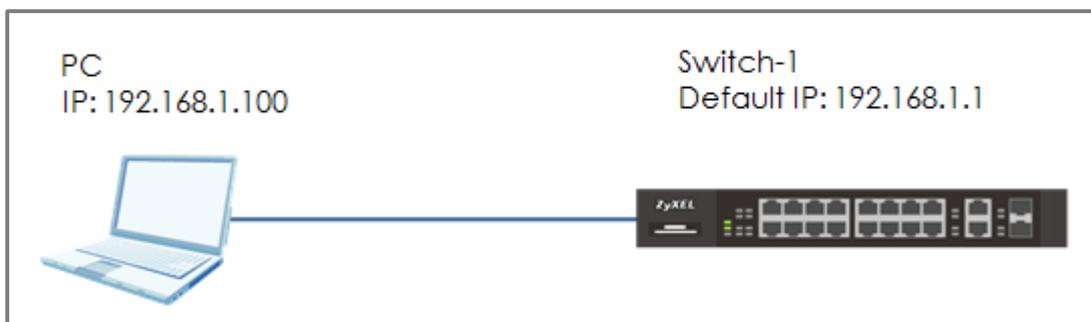


Figure 6 Collect the Diagnostic Info from web GUI

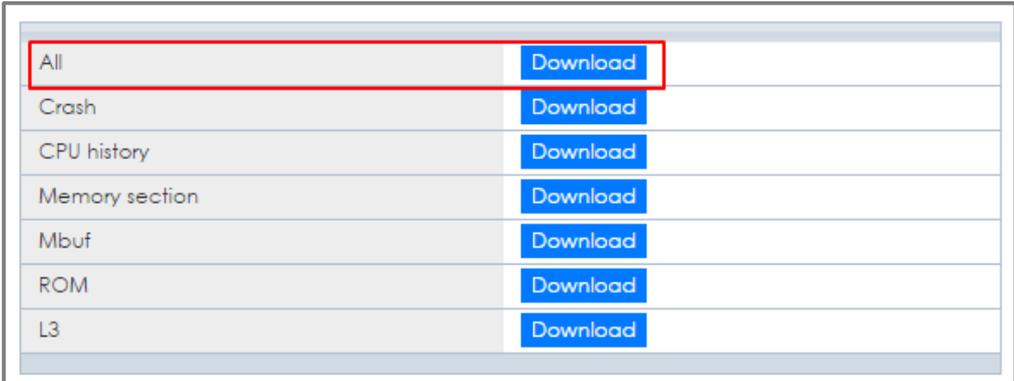


Note:

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

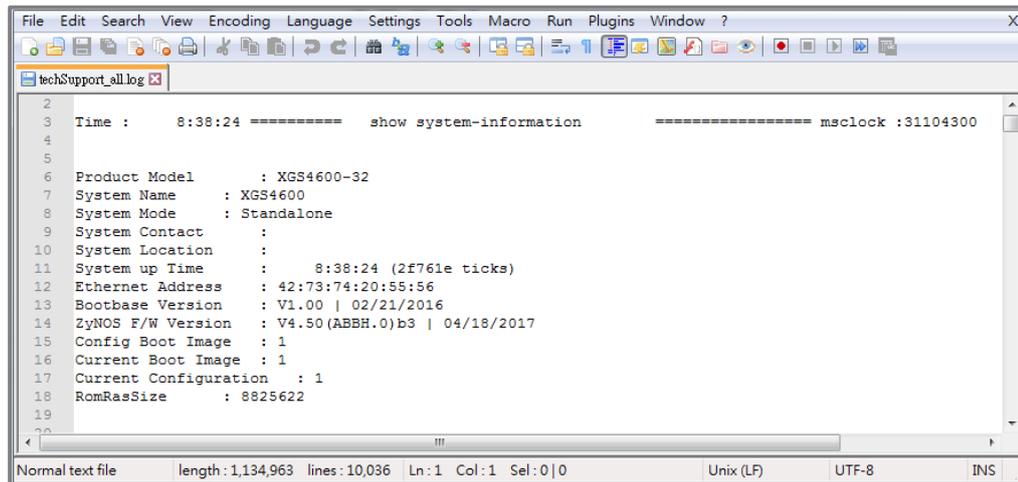
- 1 Enter the web GUI and go to **Menu > Management > Maintenance > Tech-Support > [Click Here](#)**. Click the Download button for **All**. You can also select the specific Diagnostic Info you need. (Ex: Crash, ROM,.....)



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

1.6.2 Test the Result

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



The screenshot shows a Notepad++ window titled 'techSupport_all.log'. The text content is as follows:

```
2  
3 Time :      8:38:24 ===== show system-information ===== msclock :31104300  
4  
5  
6 Product Model      : XGS4600-32  
7 System Name       : XGS4600  
8 System Mode       : Standalone  
9 System Contact    :  
10 System Location   :  
11 System up Time    :      8:38:24 (2f761e ticks)  
12 Ethernet Address  : 42:73:74:20:55:56  
13 Bootbase Version  : V1.00 | 02/21/2016  
14 ZyNOS F/W Version : V4.50(ABBH.0)b3 | 04/18/2017  
15 Config Boot Image : 1  
16 Current Boot Image : 1  
17 Current Configuration : 1  
18 RomRasSize       : 8825622  
19  
20
```

The status bar at the bottom indicates: Normal text file | length: 1,134,963 | lines: 10,036 | Ln: 1 | Col: 1 | Sel: 0 | 0 | Unix (LF) | UTF-8 | INS

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

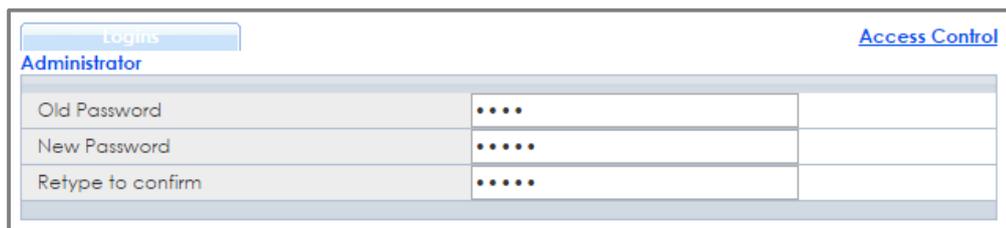


Note:

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).

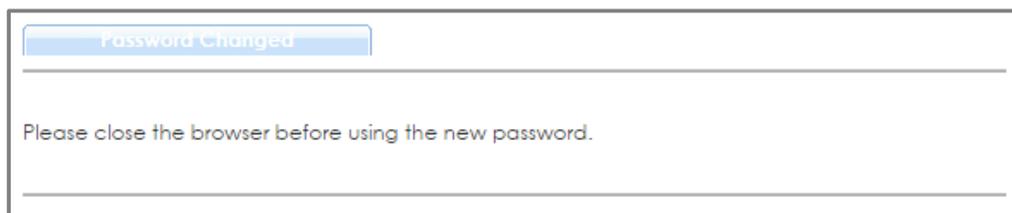
1.7.1 Change the default administrator password

- 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**".



Logins		Access Control
Administrator		
Old Password	
New Password	
Retype to confirm	

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

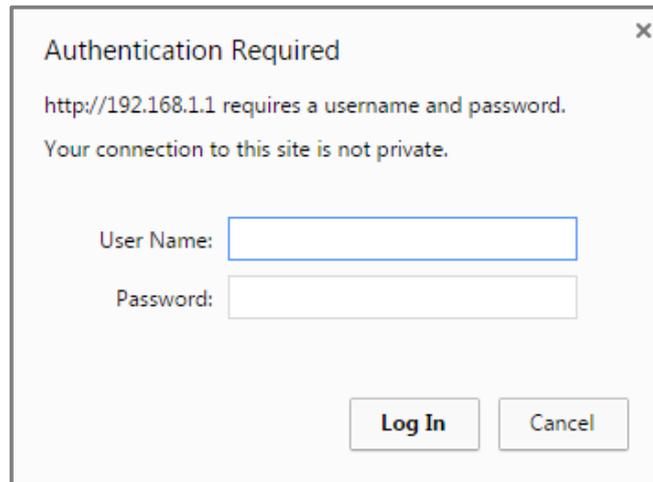


Password Changed

Please close the browser before using the new password.

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.



Authentication Required

http://192.168.1.1 requires a username and password.
Your connection to this site is not private.

User Name:

Password:

- 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.....).

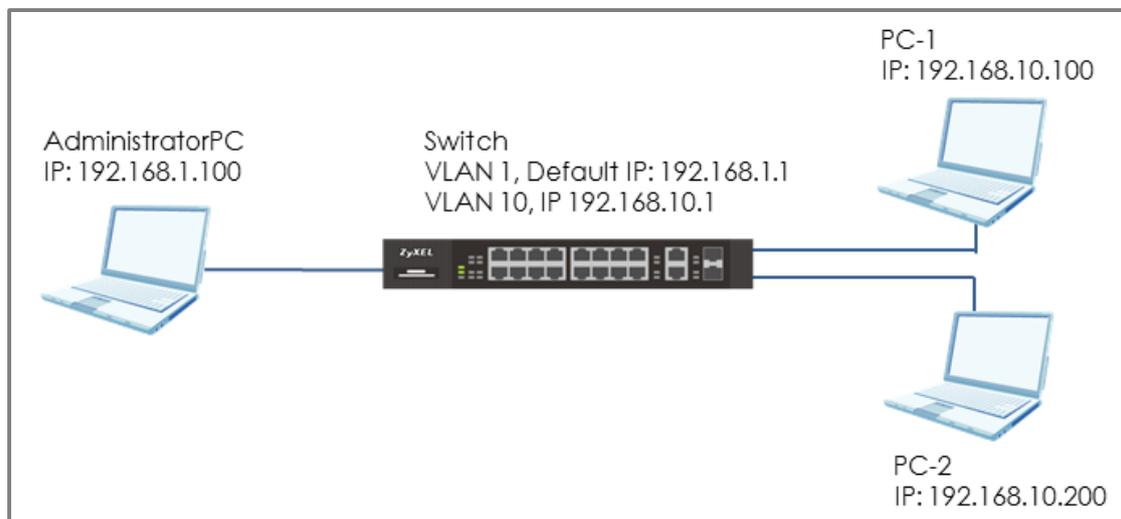


Figure 8 Configure the whitelist for remote management

 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).

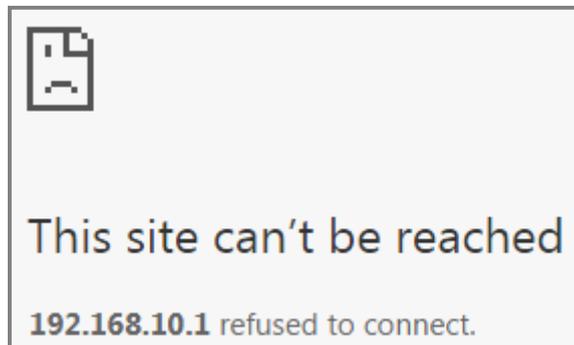
1.8.1 Configure the whitelist of the remote management

- 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”**.

Remote Management				Access Control							
Secured Client Setup				Telnet	FTP	HTTP	ICMP	SNMP	SSH	HTTPS	
Entry	Active	Start Address	End Address								
1	<input checked="" type="checkbox"/>	192.168.10.100	192.168.10.120	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
2	<input checked="" type="checkbox"/>	192.168.1.100	192.168.1.100	<input checked="" type="checkbox"/>							
3	<input type="checkbox"/>	0.0.0.0	0.0.0.0	<input type="checkbox"/>							
4	<input type="checkbox"/>	0.0.0.0	0.0.0.0	<input type="checkbox"/>							
5	<input type="checkbox"/>	0.0.0.0	0.0.0.0	<input type="checkbox"/>							
6	<input type="checkbox"/>	0.0.0.0	0.0.0.0	<input type="checkbox"/>							
7	<input type="checkbox"/>	0.0.0.0	0.0.0.0	<input type="checkbox"/>							
8	<input type="checkbox"/>	0.0.0.0	0.0.0.0	<input type="checkbox"/>							
9	<input type="checkbox"/>	0.0.0.0	0.0.0.0	<input type="checkbox"/>							
10	<input type="checkbox"/>	0.0.0.0	0.0.0.0	<input type="checkbox"/>							
11	<input type="checkbox"/>	0.0.0.0	0.0.0.0	<input type="checkbox"/>							
12	<input type="checkbox"/>	0.0.0.0	0.0.0.0	<input type="checkbox"/>							
13	<input type="checkbox"/>	0.0.0.0	0.0.0.0	<input type="checkbox"/>							
14	<input type="checkbox"/>	0.0.0.0	0.0.0.0	<input type="checkbox"/>							
15	<input type="checkbox"/>	0.0.0.0	0.0.0.0	<input type="checkbox"/>							
16	<input type="checkbox"/>	0.0.0.0	0.0.0.0	<input type="checkbox"/>							

1.8.2 Test the Result

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



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



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

1.8.3 What could go wrong?

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

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

Remote Management				Access Control						
Secured Client Setup				Telnet	FTP	HTTP	ICMP	SNMP	SSH	HTTPS
Entry	Active	Start Address	End Address							
1	<input checked="" type="checkbox"/>	192.168.10.100	192.168.10.120	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	<input checked="" type="checkbox"/>	192.168.10.120	192.168.10.120	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	0.0.0.0	0.0.0.0	<input type="checkbox"/>						
4	<input type="checkbox"/>	0.0.0.0	0.0.0.0	<input type="checkbox"/>						

- 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.

```
XGS4600# show run
Building configuration...

Current configuration:

no remote-management 1 service telnet ftp snmp ssh
vlan 1
 name 1
 normal ""
 fixed 1-32
 forbidden ""
 untagged 1-32
 ip address 192.168.1.1 255.255.255.0
exit
interface route-domain 192.168.1.1/24
exit
remote-management 1 start-addr 192.168.1.100 end-addr 192.168.1.200 service http icmp https
```



Note:

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

Designing the Local Area Network

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

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

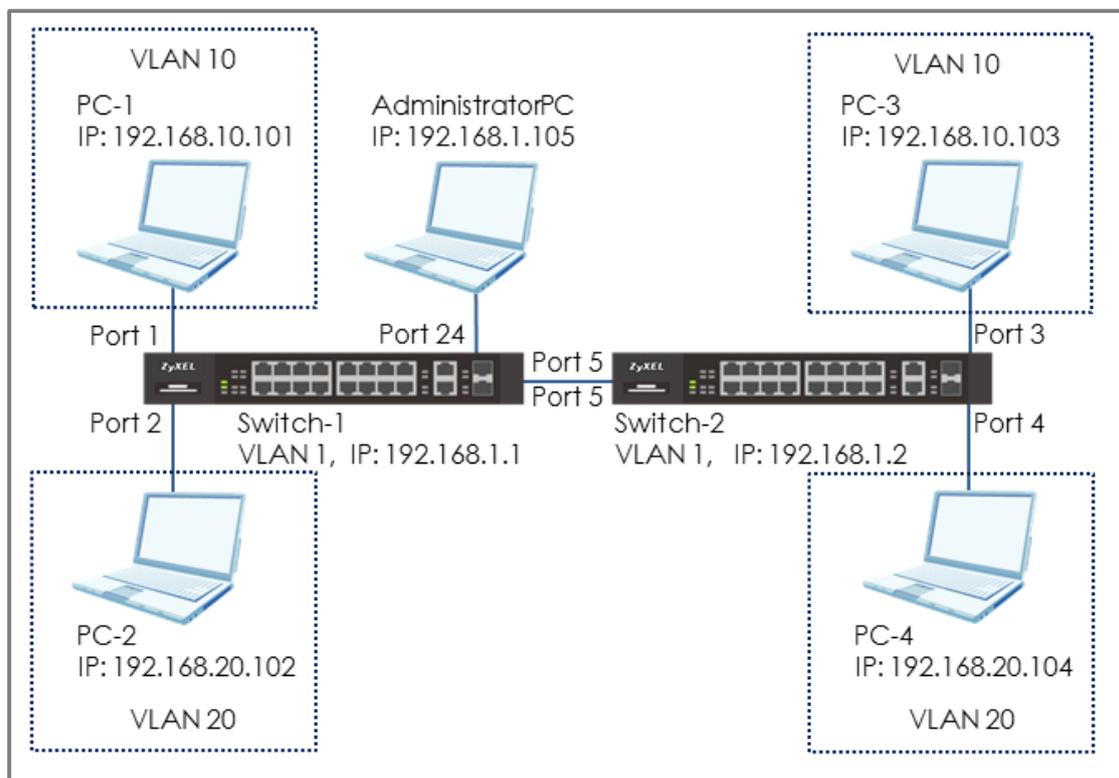


Figure 9 Set up VLAN to separate the traffic between departments



Note:

All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using 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”**.

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

- 2 Use AdministratorPC to create **VLAN 10** in **Switch-1**: Enter the web GUI and go to **Menu > 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”**.

Static VLAN
[VLAN Configuration](#)

ACTIVE	<input checked="" type="checkbox"/>
Name	VLAN10
VLAN Group ID	10
VLAN Type	<input checked="" type="radio"/> Normal <input type="radio"/> Private
Association VLAN List	

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

- Use AdministratorPC to create **VLAN 20** in **Switch-1**: Enter the web GUI and go to **Menu > 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**".

Static VLAN
[VLAN Configuration](#)

ACTIVE	<input checked="" type="checkbox"/>
Name	VLAN20
VLAN Group ID	20
VLAN Type	<input checked="" type="radio"/> Normal <input type="radio"/> Private
Association VLAN List	

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

- 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
-	<input type="checkbox"/>		<input type="checkbox"/>	All ▼	<input type="checkbox"/>	<input type="checkbox"/>
1	<input type="checkbox"/>	10	<input type="checkbox"/>	All ▼	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	20	<input type="checkbox"/>	All ▼	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	1	<input type="checkbox"/>	All ▼	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	1	<input type="checkbox"/>	All ▼	<input type="checkbox"/>	<input type="checkbox"/>

2.1.2 Configure Switch-2

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

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

- 2 Use AdministratorPC to create **VLAN 10** in **Switch-2**. Enter the web GUI and go to **Menu > 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"**.

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

- 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”.

Static VLAN		VLAN Configuration	
ACTIVE	<input checked="" type="checkbox"/>	Name	VLAN20
VLAN Group ID	20	VLAN Type	<input checked="" type="radio"/> Normal <input type="radio"/> Private
Association VLAN List			

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

- 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**.

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

2.1.3 Test the Result

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

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

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

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

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

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

2.2 How to configure the switch to route traffic across VLANs

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

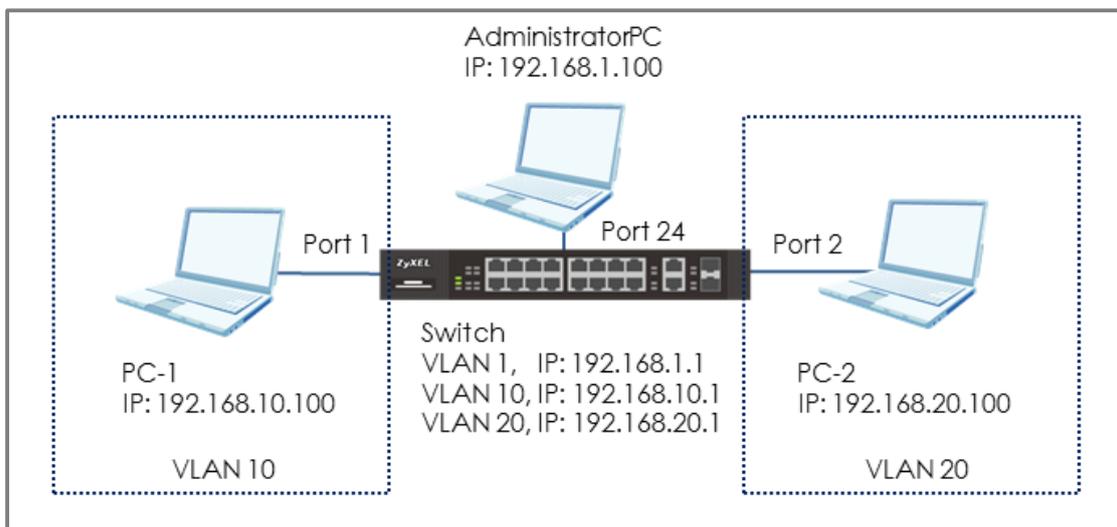


Figure 10 Set up switch to route traffic across VLANs



Note:

All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using 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”**.

Static VLAN		VLAN Configuration	
ACTIVE	<input checked="" type="checkbox"/>	Name	VLAN10
VLAN Group ID	10	VLAN Type	<input checked="" type="radio"/> Normal <input type="radio"/> Private
Association VLAN List			

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

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

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

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

The screenshot shows the 'IP Interface' configuration page. It features a 'Static IP Address' section with the following fields:

Field	Value
IP Address	192.168.10.1
IP Subnet Mask	255.255.255.0
VID	10

At the bottom of the form, there are two buttons: 'Add' and 'Cancel'.

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”**.

Static VLAN		VLAN Configuration	
ACTIVE	<input checked="" type="checkbox"/>	Name	VLAN20
VLAN Group ID	20	VLAN Type	<input checked="" type="radio"/> Normal <input type="radio"/> Private
Association VLAN List			

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

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

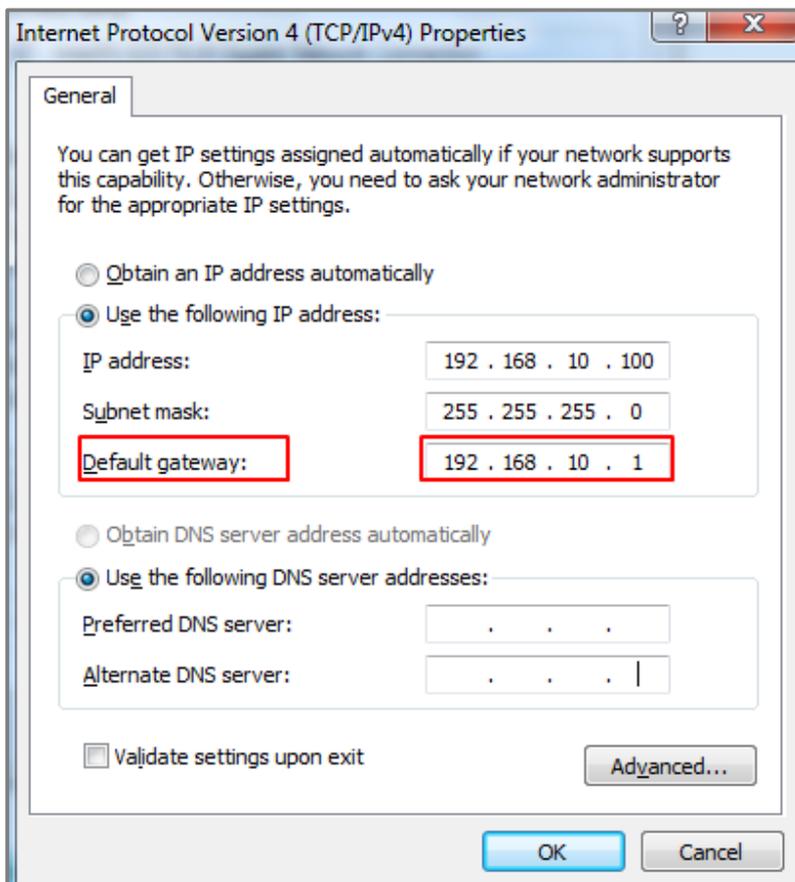
Port	Ingress Check	PVID	GVRP	Acceptable Frame Type	VLAN Trunking	Isolation
*	<input type="checkbox"/>		<input type="checkbox"/>	All	<input type="checkbox"/>	<input type="checkbox"/>
1	<input type="checkbox"/>	10	<input type="checkbox"/>	All	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>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

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

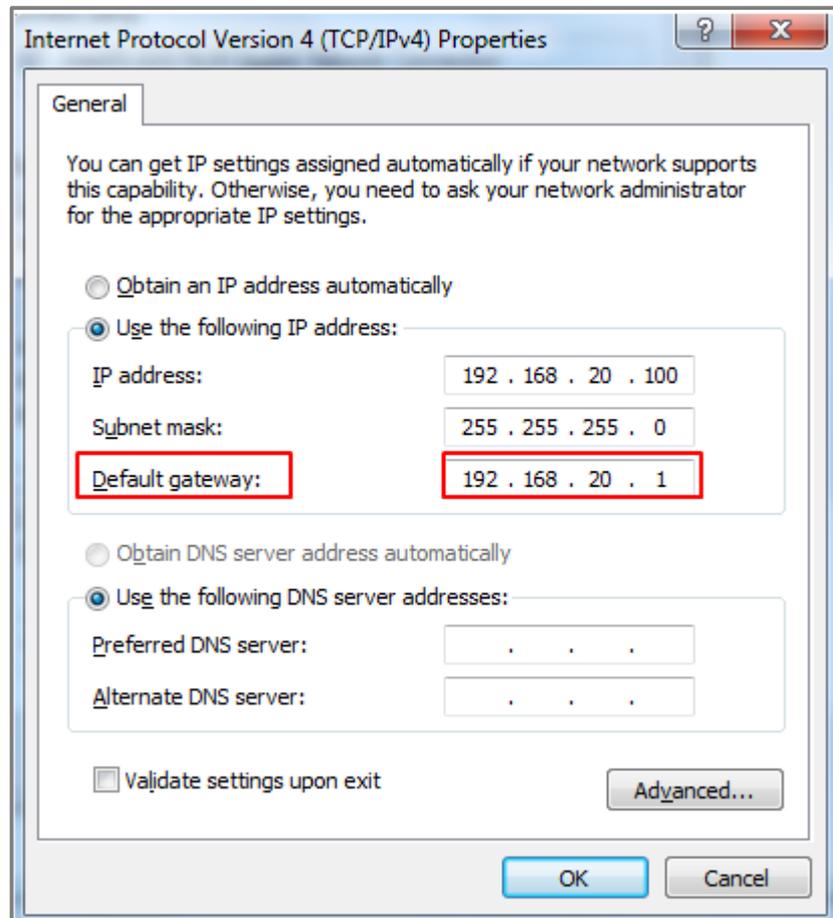
The screenshot shows the 'IP Interface' configuration window. On the left, there is a vertical tab labeled 'IP Address'. To the right, there are two radio buttons: 'DHCP Client' (unselected) and 'Static IP Address' (selected). Below the radio buttons, there are three input fields: 'IP Address' with the value '192.168.20.1', 'IP Subnet Mask' with the value '255.255.255.0', and 'VID' with the value '20'. At the bottom of the window, there are two buttons: 'Add' and 'Cancel'.

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

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



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



2.2.4 Test the Result

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

```
C:\Users\User>ping 192.168.20.100
Pinging 192.168.20.100 with 32 bytes of data:
Reply from 192.168.20.100: bytes=32 time<1ms TTL=128

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

2.2.5 What could go wrong

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

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

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

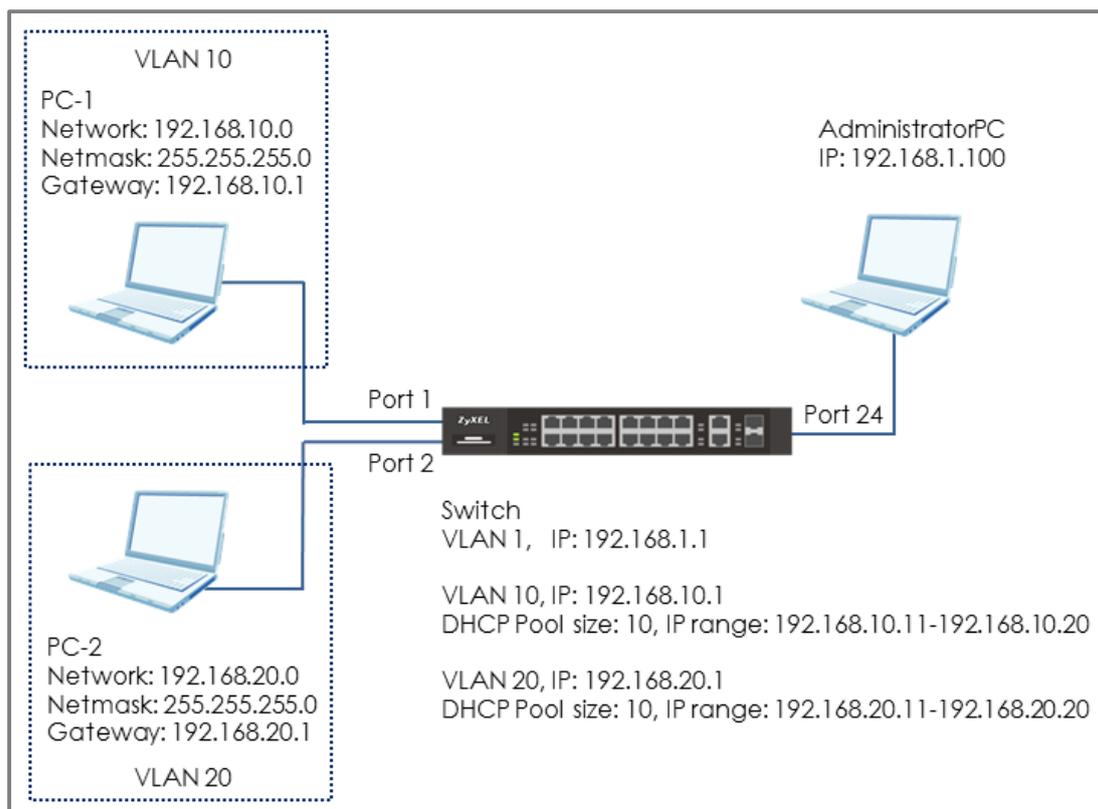


Figure 11 Perform DHCP service in different VLAN



Note:

All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using 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”**.

Static VLAN		VLAN Configuration	
ACTIVE	<input checked="" type="checkbox"/>	Name	VLAN10
VLAN Group ID	10	VLAN Type	<input checked="" type="radio"/> Normal <input type="radio"/> Private
Association VLAN List			

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

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

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

- 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**".

IP Interface

IP Address

DHCP Client

Static IP Address

IP Address: 192.168.10.1

IP Subnet Mask: 255.255.255.0

VID: 10

Add **Cancel**

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”**.

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

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

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

- 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"**.

The screenshot shows the 'IP Interface' configuration window. It has a title bar 'IP Interface' and a left sidebar with 'IP Address'. The main area contains two radio buttons: 'DHCP Client' (unselected) and 'Static IP Address' (selected). Below the radio buttons are three input fields: 'IP Address' with the value '192.168.20.1', 'IP Subnet Mask' with the value '255.255.255.0', and 'VID' with the value '20'. At the bottom of the window are two buttons: 'Add' and 'Cancel'.

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".

VLAN Setting		Status Port
VID	<input type="text" value="10"/>	
DHCP Status	<input checked="" type="radio"/> Server <input type="radio"/> Relay	
Server		
Client IP Pool Starting Address	<input type="text" value="192.168.10.11"/>	
Size of Client IP Pool	<input type="text" value="10"/>	
IP Subnet Mask	<input type="text" value="255.255.255.0"/>	
Default Gateway	<input type="text" value="192.168.10.1"/>	
Primary DNS Server	<input type="text" value="0.0.0.0"/>	
Secondary DNS Server	<input type="text" value="0.0.0.0"/>	
Lease Time	<input checked="" type="radio"/> Infinite <input type="radio"/> Days <input type="text" value=""/> Hours <input type="text" value="00"/> Minutes <input type="text" value="00"/>	
Relay		
Remote DHCP Server 1	<input type="text" value="0.0.0.0"/>	
Remote DHCP Server 2	<input type="text" value="0.0.0.0"/>	
Remote DHCP Server 3	<input type="text" value="0.0.0.0"/>	
Source Address	<input type="text" value="0.0.0.0"/>	
Option 82 Profile	<input type="text" value=""/>	



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.

- 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".

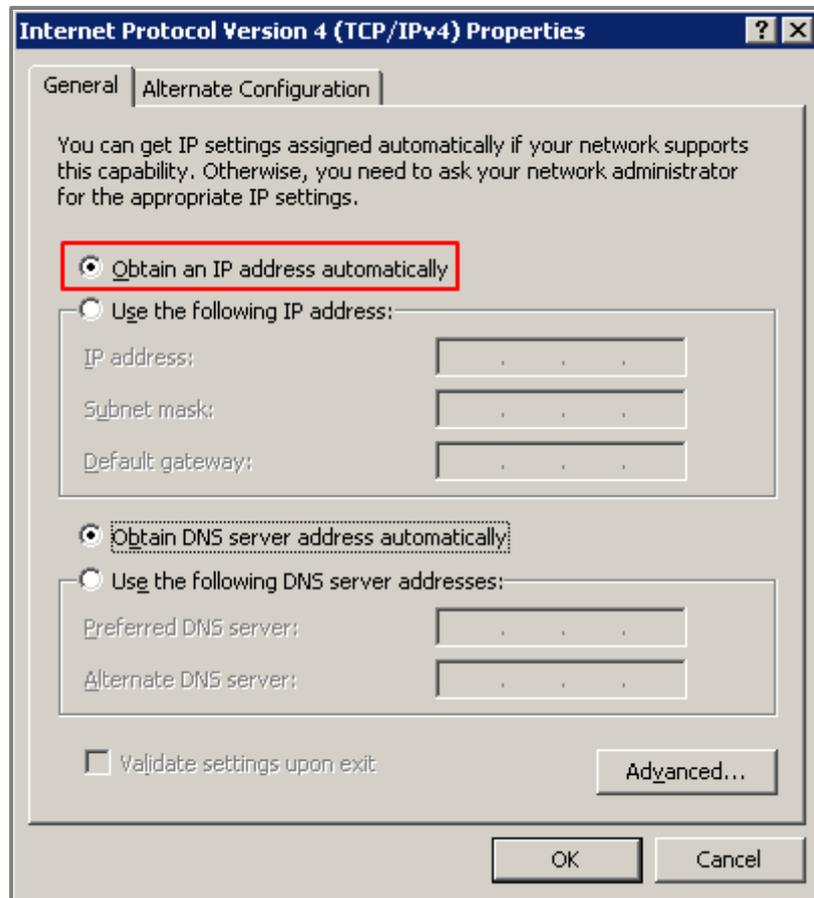
VLAN Setting		Status Port
VID	<input type="text" value="20"/>	
DHCP Status	<input checked="" type="radio"/> Server <input type="radio"/> Relay	
Server		
Client IP Pool Starting Address	<input type="text" value="192.168.20.11"/>	
Size of Client IP Pool	<input type="text" value="10"/>	
IP Subnet Mask	<input type="text" value="255.255.255.0"/>	
Default Gateway	<input type="text" value="192.168.20.1"/>	
Primary DNS Server	<input type="text" value="0.0.0.0"/>	
Secondary DNS Server	<input type="text" value="0.0.0.0"/>	
Lease Time	<input checked="" type="radio"/> Infinite <input type="radio"/> Days <input type="text" value=""/> Hours <input type="text" value="00"/> Minutes <input type="text" value="00"/>	
Relay		
Remote DHCP Server 1	<input type="text" value="0.0.0.0"/>	
Remote DHCP Server 2	<input type="text" value="0.0.0.0"/>	
Remote DHCP Server 3	<input type="text" value="0.0.0.0"/>	
Source Address	<input type="text" value="0.0.0.0"/>	
Option 82 Profile	<input type="text" value=""/>	



Note:

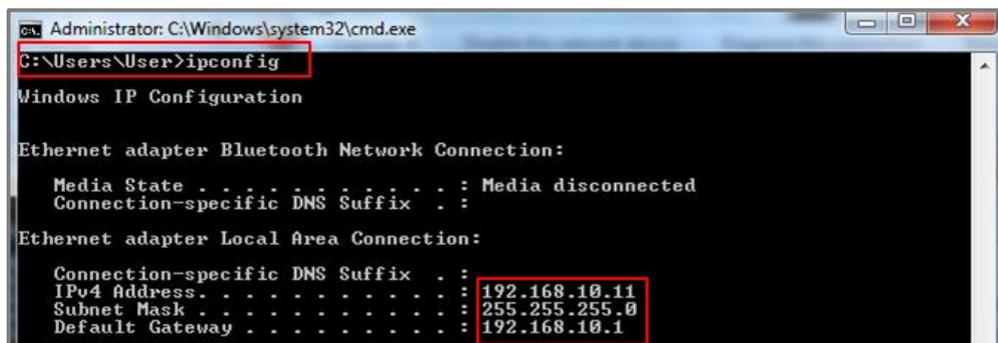
In this example, the pool size is 10 and the starting IP address is 192.168.20.11. Therefore, the IP range that the DHCP Server will assign is between 192.168.20.11 and 192.168.20.20.

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



2.3.4 Test the Result

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



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

Windows IP Configuration

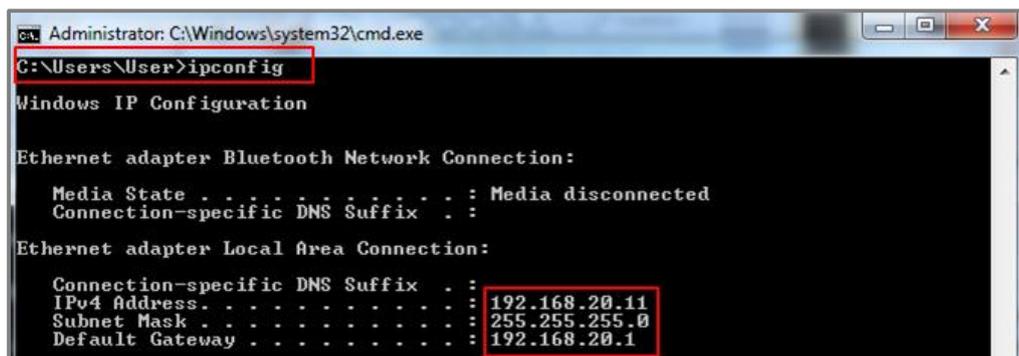
Ethernet adapter Bluetooth Network Connection:

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

Ethernet adapter Local Area Connection:

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

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



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

Windows IP Configuration

Ethernet adapter Bluetooth Network Connection:

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

Ethernet adapter Local Area Connection:

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

2.3.5 What Could Go Wrong

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

VLAN Setting		Status Port
VID	20	
DHCP Status	<input checked="" type="radio"/> Server <input type="radio"/> Relay	
Server		
Client IP Pool Starting Address	192.168.20.11	
Size of Client IP Pool	20	
IP Subnet Mask	255.255.255.0	
Default Gateway	192.168.20.1	
Primary DNS Server	0.0.0.0	
Secondary DNS Server	0.0.0.0	
Lease Time		
<input checked="" type="radio"/> Infinite <input type="radio"/> Days <input type="text"/> Hours <input type="text"/> Minutes <input type="text"/>		
Relay		
Remote DHCP Server 1	0.0.0.0	
Remote DHCP Server 2	0.0.0.0	
Remote DHCP Server 3	0.0.0.0	
Source Address	0.0.0.0	
Option 82 Profile		

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.

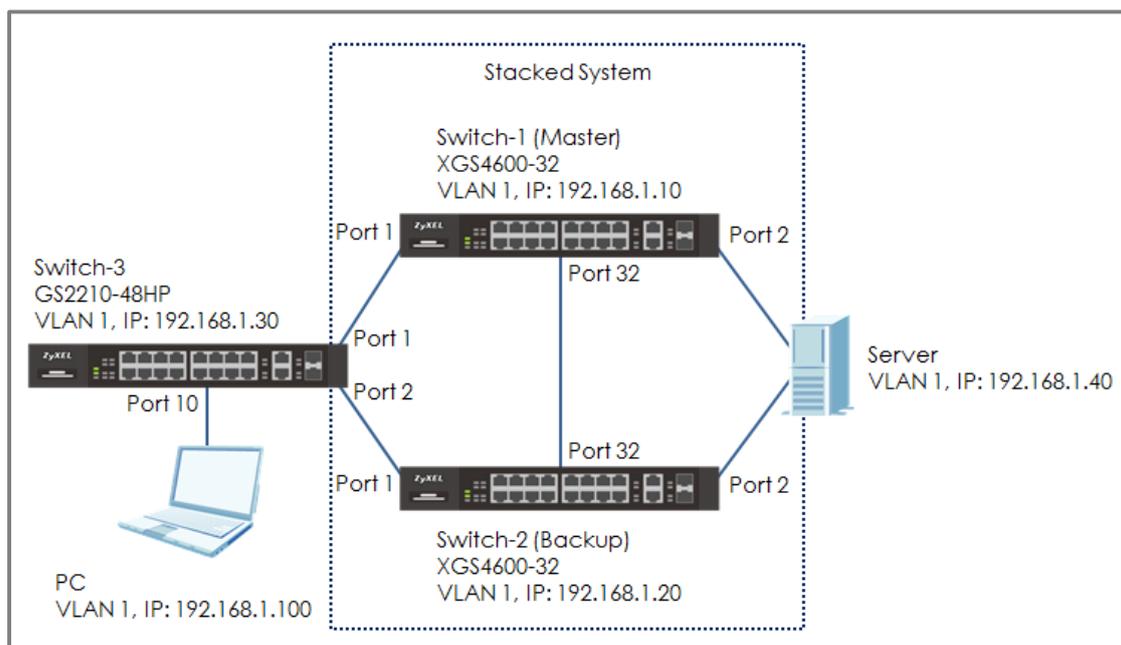


Figure 12 Configure the stacked switch



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.

The screenshot shows the 'Stacking Configuration' web interface. At the top, there is a 'Stacking Status' link. Below it, the 'Active' checkbox is checked and highlighted with a red box. Underneath, there are 'Apply' and 'Cancel' buttons. In the next section, the 'Force Master Mode' checkbox is unchecked. The 'System Priority' field contains the value '40' and is highlighted with a red box. Below this field, there are also 'Apply' and 'Cancel' buttons.



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.

The screenshot shows the 'Stacking Configuration' web interface for Switch-2. At the top, there is a 'Stacking Status' link. Below it, the 'Active' checkbox is checked and highlighted with a red box. Underneath, there are 'Apply' and 'Cancel' buttons. In the next section, the 'Force Master Mode' checkbox is unchecked. The 'System Priority' field contains the value '32' and is highlighted with a red box. Below this field, there are also 'Apply' and 'Cancel' buttons, along with a clipboard icon and '(Ctrl)' text.

- 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”.

Link Aggregation Setting			Status	LACP
Group ID	Active	Criteria		
T1	<input checked="" type="checkbox"/>	src-dst-mac ▼		
T2	<input checked="" type="checkbox"/>	src-dst-mac ▼		
T3	<input type="checkbox"/>	src-dst-mac ▼		
T4	<input type="checkbox"/>	src-dst-mac ▼		

SLOT 1 ▼		
Port	Group	
1/1	T1 ▼	
1/2	T2 ▼	
1/3	None ▼	
1/4	None ▼	

SLOT 2 ▼		
Port	Group	
2/1	T1 ▼	
2/2	T2 ▼	
2/3	None ▼	
2/4	None ▼	

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

Link Aggregation Control Protocol		Link Aggregation Setting
Active	<input checked="" type="checkbox"/>	
System Priority	65535	

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

3.1.3 Configure Link Aggregation on Switch-3

- 1 Go to **Menu > 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".

Link Aggregation Setting			Status	LACP
Group ID	Active	Criteria		
T1	<input checked="" type="checkbox"/>	src-dst-mac ▼		
T2	<input type="checkbox"/>	src-dst-mac ▼		
T3	<input type="checkbox"/>	src-dst-mac ▼		
T4	<input type="checkbox"/>	src-dst-mac ▼		

Port	Group
1	T1 ▼
2	T1 ▼
3	None ▼
4	None ▼

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

Link Aggregation Control Protocol		Link Aggregation Setting
Active	<input checked="" type="checkbox"/>	
System Priority	65535	

Group ID	LACP Active
T1	<input checked="" type="checkbox"/>
T2	<input type="checkbox"/>
T3	<input type="checkbox"/>
T4	<input type="checkbox"/>

3.1.4 Test the Result

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

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

3.1.5 What Could Go Wrong

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

3.2 How to configure RSTP in a ring topology

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

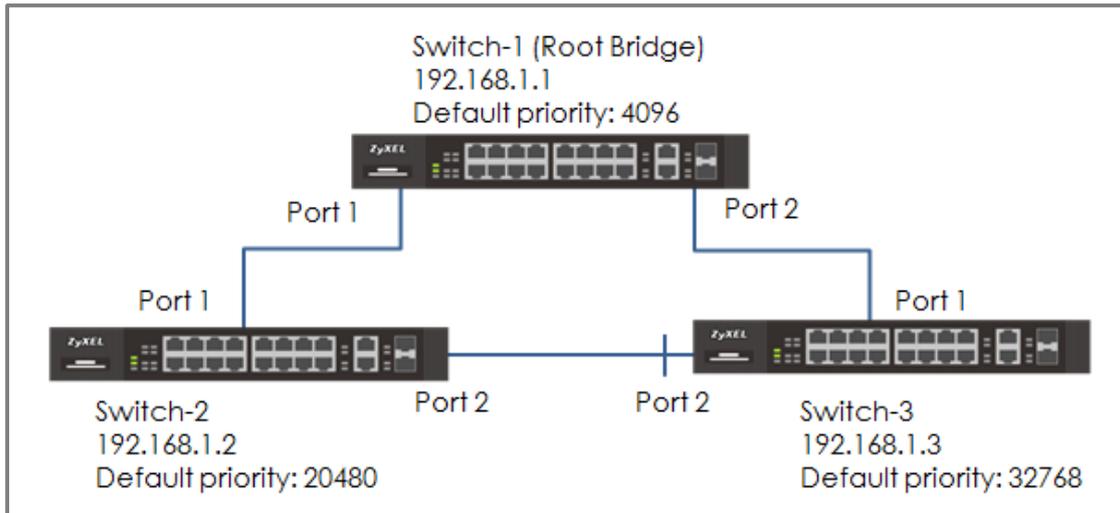


Figure 13 Configure RSTP in a ring topology

 Note:

All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using 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**”.

Port	Active	Edge	Root Guard	Priority	Path Cost
*	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	128	4
2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	128	4
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	128	4
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	128	4

- 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**".

The screenshot shows the 'Rapid Spanning Tree Protocol' configuration page. The 'Active' checkbox is checked. The 'Bridge Priority' is set to 20480. The 'Hello Time' is 2 seconds, 'MAX Age' is 20 seconds, and 'Forwarding Delay' is 15 seconds. Below this is a table for port configuration:

Port	Active	Edge	Root Guard	Priority	Path Cost
*	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	128	4
2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	128	4
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	128	4
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	128	4

- 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**".

Rapid Spanning Tree Protocol Status

Active	<input checked="" type="checkbox"/>
Bridge Priority	32768 ▼
Hello Time	2 Seconds
MAX Age	20 Seconds
Forwarding Delay	15 Seconds

Port	Active	Edge	Root Guard	Priority	Path Cost
*	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	128	4
2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	128	4
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	128	4
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	128	4

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						
Spanning Tree Protocol: RSTP						
		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						
Spanning Tree Protocol: RSTP						
		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.

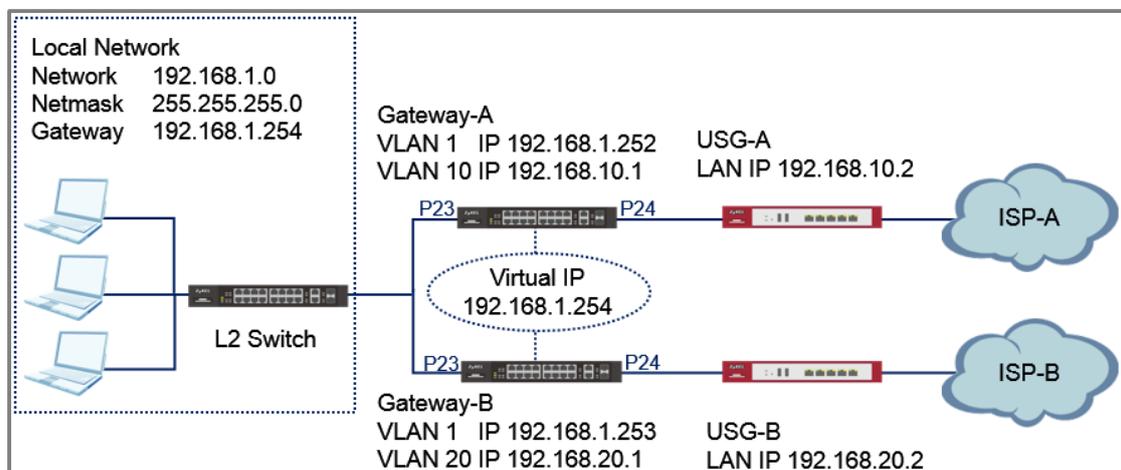


Figure 14 Two gateways running VRRP on the same LAN



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**.

Static VLAN		VLAN Configuration
ACTIVE	<input checked="" type="checkbox"/>	
Name	<input type="text" value="1"/>	
VLAN Group ID	<input type="text" value="1"/>	
VLAN Type	<input checked="" type="radio"/> Normal <input type="radio"/> Private <input type="text" value=""/>	
Association VLAN List	<input type="text"/>	

21	<input type="radio"/> Normal	<input type="radio"/> Fixed	<input checked="" type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
22	<input type="radio"/> Normal	<input type="radio"/> Fixed	<input checked="" type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
23	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
24	<input type="radio"/> Normal	<input type="radio"/> Fixed	<input checked="" type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
25	<input type="radio"/> Normal	<input type="radio"/> Fixed	<input checked="" type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging

- 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**.

Static VLAN		VLAN Configuration
ACTIVE	<input checked="" type="checkbox"/>	
Name	<input type="text" value="10"/>	
VLAN Group ID	<input type="text" value="10"/>	
VLAN Type	<input checked="" type="radio"/> Normal <input type="radio"/> Private <input type="text" value=""/>	
Association VLAN List	<input type="text"/>	

21	<input type="radio"/> Normal	<input type="radio"/> Fixed	<input checked="" type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
22	<input type="radio"/> Normal	<input type="radio"/> Fixed	<input checked="" type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
23	<input type="radio"/> Normal	<input type="radio"/> Fixed	<input checked="" type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
24	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
25	<input type="radio"/> Normal	<input type="radio"/> Fixed	<input checked="" type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging

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

21	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>	<input type="checkbox"/>
22	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>	<input type="checkbox"/>
23	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>	<input type="checkbox"/>
24	<input type="checkbox"/>	10	<input type="checkbox"/>	All	<input type="checkbox"/>	<input type="checkbox"/>
25	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>	<input type="checkbox"/>

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

IP Interface

IP Address

DHCP Client

Static IP Address

IP Address: 192.168.1.252

IP Subnet Mask: 255.255.255.0

VID: 1

[Add](#) [Cancel](#)

IP Interface

IP Address

DHCP Client

Static IP Address

IP Address: 192.168.10.1

IP Subnet Mask: 255.255.255.0

VID: 10

[Add](#) [Cancel](#)

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

IP Configuration [IP Status](#)

Default Gateway: 192.168.10.2

Default Management: In-band Out-of-band

[Apply](#) [Cancel](#)

- 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**.

Active	<input checked="" type="checkbox"/>
Name	VLAN1
Network	192.168.1.252/24 ▾
Virtual Router ID	1 ▾
Advertisement Interval	1
Preempt Mode	<input checked="" type="checkbox"/>
Priority	200
Uplink Gateway	192.168.10.2
Response Ping	<input checked="" type="checkbox"/>
Primary Virtual IP	192.168.1.254
Secondary Virtual IP	0.0.0.0

[Add](#) [Cancel](#) [Clear](#)

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**.

Static VLAN		VLAN Configuration
ACTIVE	<input checked="" type="checkbox"/>	
Name	<input type="text" value="1"/>	
VLAN Group ID	<input type="text" value="1"/>	
VLAN Type	<input checked="" type="radio"/> Normal <input type="radio"/> Private <input type="text" value=""/>	
Association VLAN List	<input type="text"/>	

21	<input type="radio"/> Normal	<input type="radio"/> Fixed	<input checked="" type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
22	<input type="radio"/> Normal	<input type="radio"/> Fixed	<input checked="" type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
23	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
24	<input type="radio"/> Normal	<input type="radio"/> Fixed	<input checked="" type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
25	<input type="radio"/> Normal	<input type="radio"/> Fixed	<input checked="" type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging

- 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**.

Static VLAN		VLAN Configuration
ACTIVE	<input checked="" type="checkbox"/>	
Name	<input type="text" value="20"/>	
VLAN Group ID	<input type="text" value="20"/>	
VLAN Type	<input checked="" type="radio"/> Normal <input type="radio"/> Private <input type="text" value=""/>	
Association VLAN List	<input type="text"/>	

21	<input type="radio"/> Normal	<input type="radio"/> Fixed	<input checked="" type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
22	<input type="radio"/> Normal	<input type="radio"/> Fixed	<input checked="" type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
23	<input type="radio"/> Normal	<input type="radio"/> Fixed	<input checked="" type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
24	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
25	<input type="radio"/> Normal	<input type="radio"/> Fixed	<input checked="" type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging

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

21	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>	<input type="checkbox"/>
22	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>	<input type="checkbox"/>
23	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>	<input type="checkbox"/>
24	<input type="checkbox"/>	20	<input type="checkbox"/>	All	<input type="checkbox"/>	<input type="checkbox"/>
25	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>	<input type="checkbox"/>

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

IP Interface

IP Address

DHCP Client

Static IP Address

IP Address

IP Subnet Mask

VID

IP Interface

IP Address

DHCP Client

Static IP Address

IP Address

IP Subnet Mask

VID

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

IP Configuration [IP Status](#)

Default Gateway

Default Management In-band Out-of-band

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

Active	<input checked="" type="checkbox"/>
Name	VLAN1
Network	192.168.1.253/24 ▼
Virtual Router ID	1 ▼
Advertisement Interval	1
Preempt Mode	<input checked="" type="checkbox"/>
Priority	100
Uplink Gateway	192.168.20.2
Response Ping	<input checked="" type="checkbox"/>
Primary Virtual IP	192.168.1.254
Secondary Virtual IP	0.0.0.0

[Add](#) [Cancel](#) [Clear](#)

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**.

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

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

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

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

3.3.4 What Could Go Wrong?

- 1 If the hosts are not 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 (FTP Server). PC will either be uploading files or downloading files from the FTP Server.

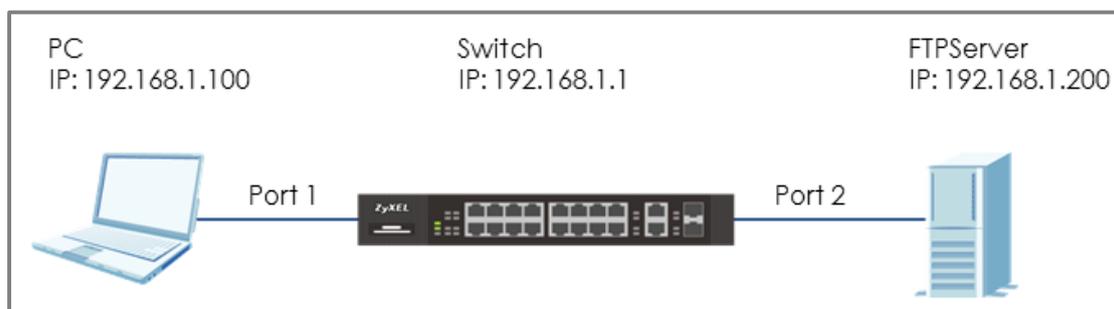


Figure 15 Configure bandwidth control to limit the traffic rate



Note:

All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using 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**”.

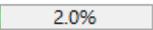
Bandwidth Control									
Active <input checked="" type="checkbox"/>									
Port	Active	Ingress Rate		Peak Rate		Egress Rate			
		Commit Rate	Active			Active			
*	<input type="checkbox"/>		<input type="checkbox"/>			<input type="checkbox"/>			
1	<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	10240		<input checked="" type="checkbox"/>	20480		
2	<input type="checkbox"/>	1	<input type="checkbox"/>	1		<input type="checkbox"/>	1		

3.4.2 Test the Result

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

Server/Local file	Directi...	Remote file	Size	Priority	Status
test@192.168.1.200					
D:\Test\TestFile.avi	-->>	/TestFile.avi	83.1 MB	Normal	Transferring
00:00:14 elapsed	00:00:58 left	 21.3%	18,612,224 bytes		1.2 MB/s

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

Server/Local file	Directi...	Remote file	Size	Priority	Status
test@192.168.1.200					
D:\Test\TestFile.avi	<<--	/TestFile.avi	3.4 GB	Normal	Transferring
00:00:28 elapsed	00:23:37 left	 2.0%	71,762,000 bytes		2.4 MB/s

3.5 How to configure ACL to rate limit IP traffic

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

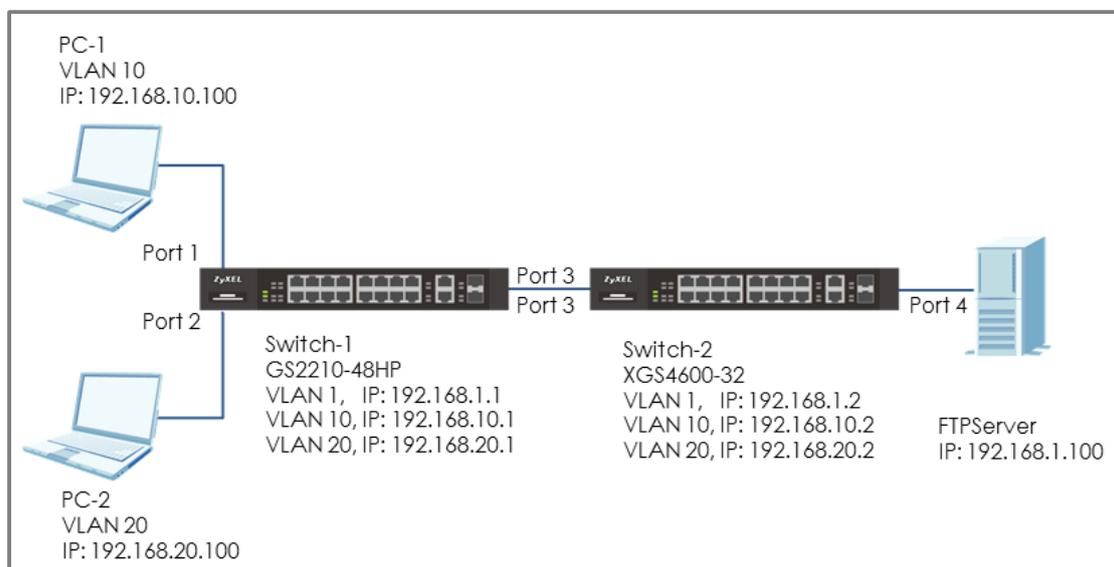


Figure 16 Configure ACL to rate limit VLAN traffic



Note:

All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using 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”.

Classifier Configuration		Classifier Status	Classifier Global Setting
Active	<input checked="" type="checkbox"/>		
Name	DL10		
Weight	32767		

Layer 3	IP Packet Length	<input checked="" type="radio"/> Any <input type="radio"/> [] To [] Bytes
	DSCP	IPv4 <input checked="" type="radio"/> Any <input type="radio"/> []
		IPv6 <input checked="" type="radio"/> Any <input type="radio"/> []
	Precedence	<input checked="" type="radio"/> Any <input type="radio"/> []
	ToS	<input checked="" type="radio"/> Any <input type="radio"/> []
	IP Protocol	<input checked="" type="radio"/> All <input type="checkbox"/> Establish Only <input type="radio"/> Others [] (Dec)
	IPv6 Next Header	<input checked="" type="radio"/> All <input type="checkbox"/> Establish Only <input type="radio"/> Others [] (Dec)
	Source	IP Address / Address Prefix: 192.168.1.100 /32
	Destination	IP Address / Address Prefix: 192.168.10.1 /24

- 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”.

Classifier Configuration		Classifier Status	Classifier Global Setting
Active	<input checked="" type="checkbox"/>		
Name	UL10		
Weight	32767		

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

- 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”.
- 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”.

Policy		
Active	<input checked="" type="checkbox"/>	
Name	PolicyDL10	
Classifier(s)	DL10 DL20 UL10 UL20	
Parameters	General	
	Egress Port	1
	Priority	0 ▼
	DSCP	
	TOS	0 ▼
	Metering	
	Bandwidth	40960 kbps
	Out-of-Profile DSCP	

The screenshot shows the configuration page for a Policy Rule. The 'Action' section is expanded, revealing several sub-sections:

- Forwarding:** Radio buttons for 'No change', 'Discard the packet', and 'Do not drop the matching frame previously marked for dropping'.
- Priority:** Radio buttons for 'No change', 'Set the packet's 802.1p priority and send the packet to priority queue', 'Replace the 802.1p priority field with the IP TOS value and send the packet to priority queue', and 'Replace the 802.1p priority field with the inner 802.1p priority value and send the packet to priority queue'.
- Diffserv:** Radio buttons for 'No change', 'Set the packet's TOS field', 'Replace the IP TOS field with the 802.1p priority value', and 'Set the Diffserv Codepoint field in the frame'.
- Outgoing:** Checkboxes for 'Send the packet to the mirror port' and 'Send the packet to the egress port'.
- Metering:** A checkbox labeled 'Enable' is checked and highlighted with a red box.
- Out-of-profile action:** A list of checkboxes: 'Drop the packet' (checked and highlighted with a red box), 'Change the DSCP value', 'Set Out-Drop Precedence', and 'Do not drop the matching frame previously marked for dropping'.

- 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.

Classifier Configuration		Classifier Status	Classifier Global Setting
Active	<input checked="" type="checkbox"/>		
Name	DL_10		
Weight	32767		
Log	<input type="checkbox"/>		
Count	<input checked="" type="checkbox"/>		

Classifier Status					Classifier Configuration
Index	Active	Weight	Name	Match Count	Rule
1	Yes	32767	DL_10	10	SrcIP = 192.168.1.150/32; DestIP = 192.168.10.0/24; count;

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

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

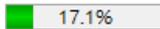
- 3 Use PC-1 to upload a file to the FTP Server. Transfer rate should be more or less 2.6 MB/s (or 20480 Mb/s).

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

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

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

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

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

3.5.5 What Could Go Wrong

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

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.

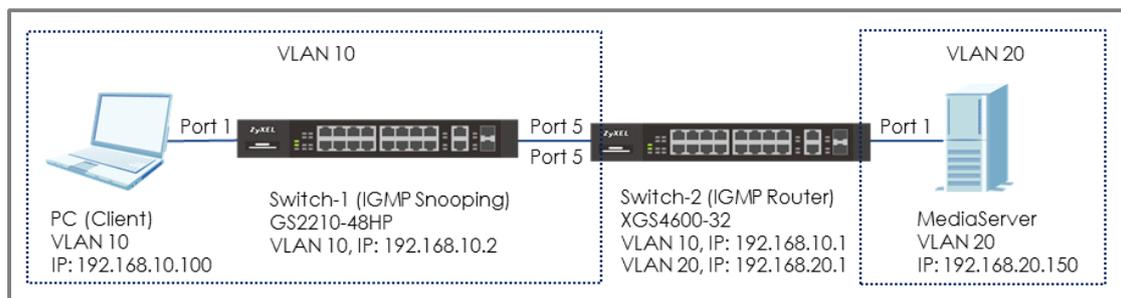


Figure 17 Configure IGMP routing for multicast clients in different VLAN



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".

IGMP Snooping										
IPv4 Multicast Status IGMP Snooping VLAN IGMP Filtering Profile										
IGMP Snooping		Active	<input checked="" type="checkbox"/>							
		Querier	<input type="checkbox"/>							
		Host Timeout	<input type="text" value="260"/>							
		802.1p Priority	<input type="text" value="No-Change"/>							
IGMP Filtering		Active	<input type="checkbox"/>							
Unknown Multicast Frame		<input type="radio"/> Flooding	<input checked="" type="radio"/> Drop							
Reserved Multicast Group		<input checked="" type="radio"/> Flooding	<input type="radio"/> Drop							

Port	Immed. Leave	Normal Leave	Fast Leave	Group Limited	Max Group Num.	Throttling	IGMP Filtering Profile	IGMP Querier Mode
*	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>		Deny	Default	Auto
1	<input type="radio"/>	<input checked="" type="radio"/> 4000	<input type="radio"/> 200	<input type="checkbox"/>	0	Deny	Default	Auto
2	<input type="radio"/>	<input checked="" type="radio"/> 4000	<input type="radio"/> 200	<input type="checkbox"/>	0	Deny	Default	Auto
3	<input type="radio"/>	<input checked="" type="radio"/> 4000	<input type="radio"/> 200	<input type="checkbox"/>	0	Deny	Default	Auto
4	<input type="radio"/>	<input checked="" type="radio"/> 4000	<input type="radio"/> 200	<input type="checkbox"/>	0	Deny	Default	Auto
5	<input type="radio"/>	<input checked="" type="radio"/> 4000	<input type="radio"/> 200	<input type="checkbox"/>	0	Deny	Default	Fixed

4.2.2 Configure Switch-2

- 1 Configure the VLAN 10 and VLAN 20 on Switch-2. Please refer to the topic: **2.1 How to configure the switch to separate traffic between departments.**
- 2 Configure the IP addresses for Switch on BOTH VLAN 10 and VLAN 20 as shown in the figure. Please refer to the topic: **1.1 How to change the switch management IP address to avoid accessing the wrong device.**
- 3 Configure the IGMP Routing: Enter the web GUI and go to **Menu > 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".

Index	Network	Version
•	-	None ▼
1	192.168.1.1/24	None ▼
2	192.168.10.1/24	IGMP-v2 ▼
3	192.169.20.1/24	IGMP-v2 ▼

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 streaming 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.

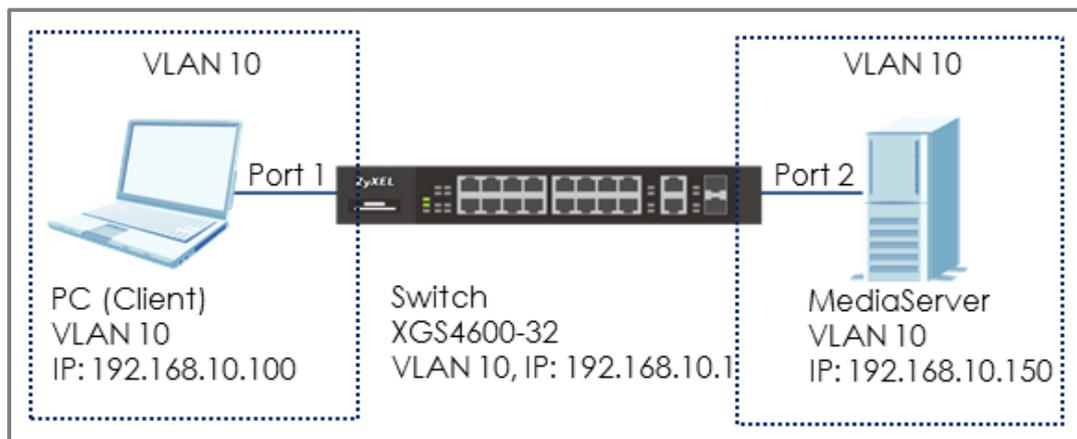


Figure 18 Configure IGMP Snooping for multicast clients in the same LAN



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".

IGMP Snooping		IPv4 Multicast Status	IGMP Snooping VLAN	IGMP Filtering Profile
IGMP Snooping	Active	<input checked="" type="checkbox"/>		
	Querier	<input checked="" type="checkbox"/>		
	Host Timeout	<input type="text" value="260"/>		
	802.1p Priority	<input type="text" value="No-Change"/>		
IGMP Filtering	Active	<input type="checkbox"/>		
Unknown Multicast Frame	<input type="radio"/> Flooding <input checked="" type="radio"/> Drop			
Reserved Multicast Group	<input checked="" type="radio"/> Flooding <input type="radio"/> Drop			

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.

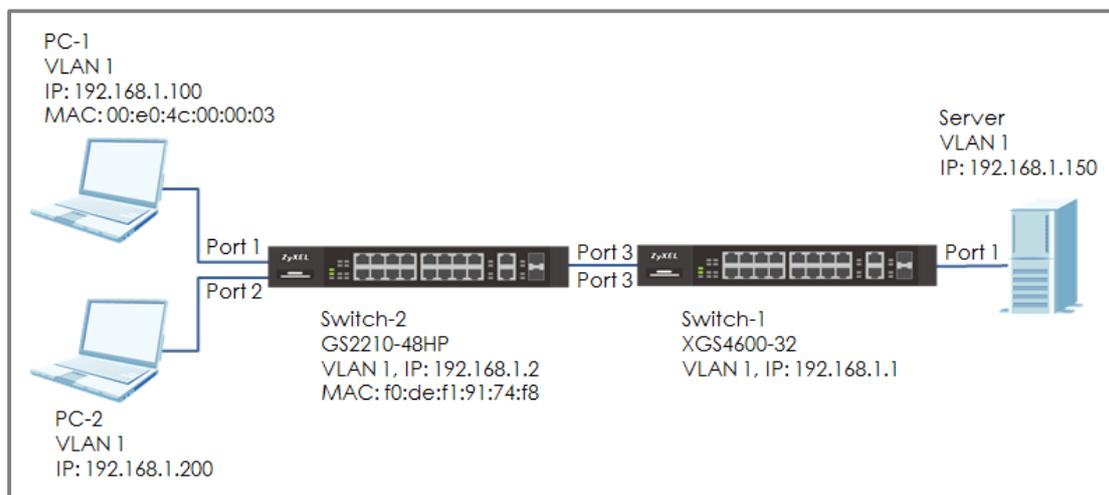


Figure 19 Configure the port security to limit the number of connected devices



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.

Port Security

Active

Port	Active	Address Learning	Limited Number of Learned MAC Address
*	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0
2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0
3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2
4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0



Note:

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

5.1.2 Test the Result

- 1 PC-1 can ping Server successfully.

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

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

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

- 2 Connect PC-2 to port 2.

- 3 PC-2 cannot ping Server.

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

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

Ping statistics for 192.168.1.150:
    Packets: Sent = 4, Received = 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 of PC-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.

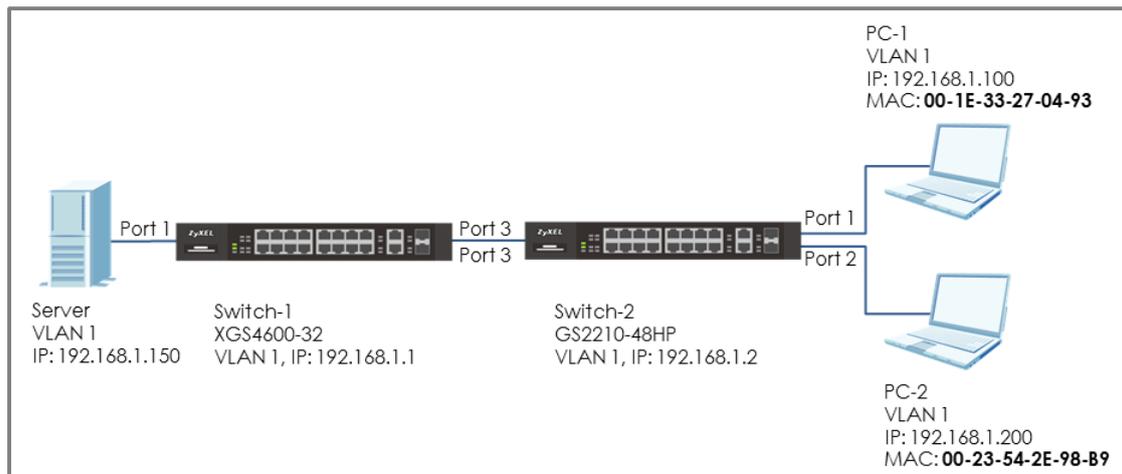


Figure 20 Configure MAC filter to block unwanted traffic



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”.

Filtering	
Active	<input checked="" type="checkbox"/>
Name	MACfilter
Action	<input checked="" type="checkbox"/> Discard source <input type="checkbox"/> Discard destination
MAC	00:1E:33:27:04:93
VID	1



Note:

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

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

5.2.2 Test the Result

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

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

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

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

- 2 PC-2 can ping Server successfully.

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

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

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

5.2.3 What Could Go Wrong

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

5.3 How to configure the switch to prevent IP scanning

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

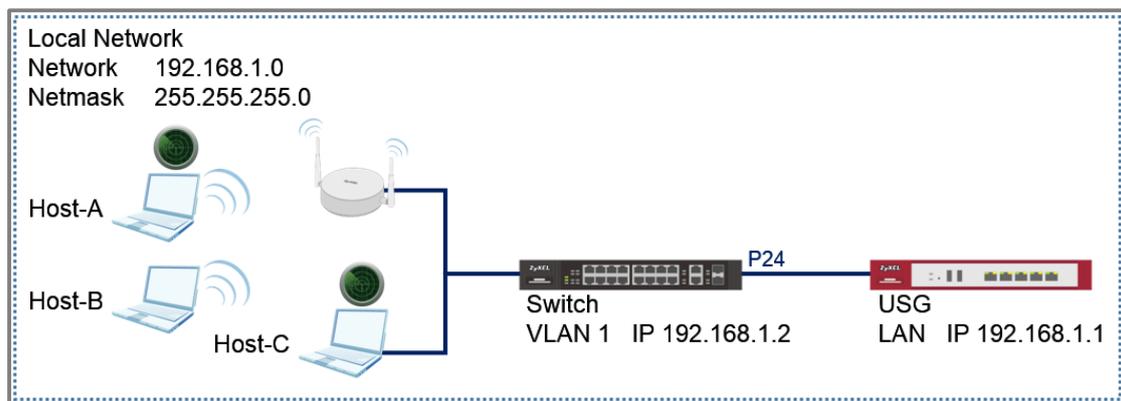


Figure 21 IP Scanning from Wired and Wireless Devices



Note:

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

Anti-Arpscan Configure
[Status](#)

Active	<input checked="" type="checkbox"/>	
Port Threshold	100	pps
Host Threshold	10	pps

	21		Untrusted ▼	
	22		Untrusted ▼	
	23		Untrusted ▼	
	24		Trusted ▼	
	25		Untrusted ▼	

-Optional-

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

Errdisable Recovery
[Errdisable](#)

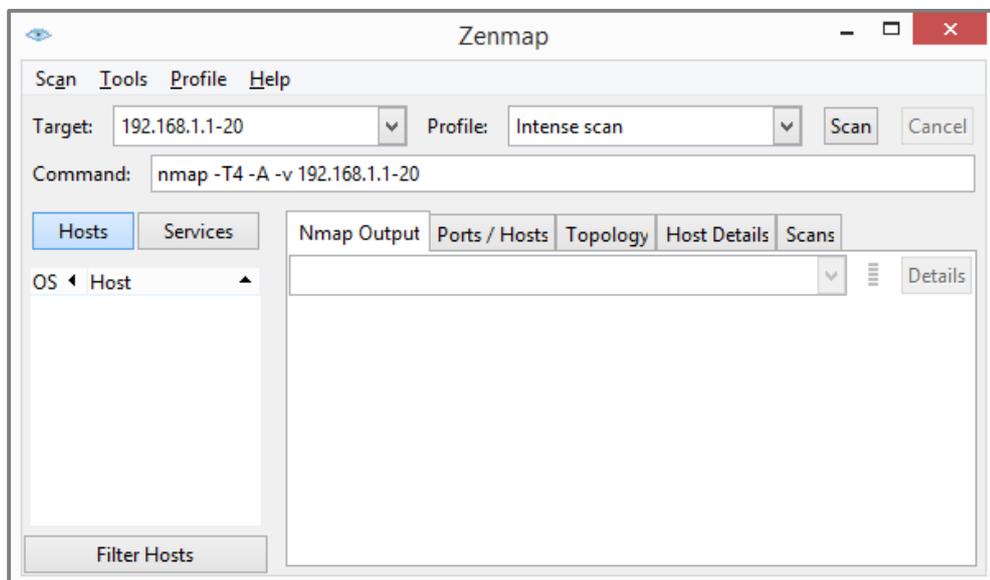
Active	<input checked="" type="checkbox"/>	
--------	-------------------------------------	--

Reason	Timer Status	Interval
*	<input type="checkbox"/>	
loopguard	<input type="checkbox"/>	300
ARP	<input type="checkbox"/>	300
BPDU	<input type="checkbox"/>	300
IGMP	<input type="checkbox"/>	300
anti-arpscan	<input checked="" type="checkbox"/>	300
bpduguard	<input type="checkbox"/>	300
zuid	<input type="checkbox"/>	300

Apply
Cancel

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.

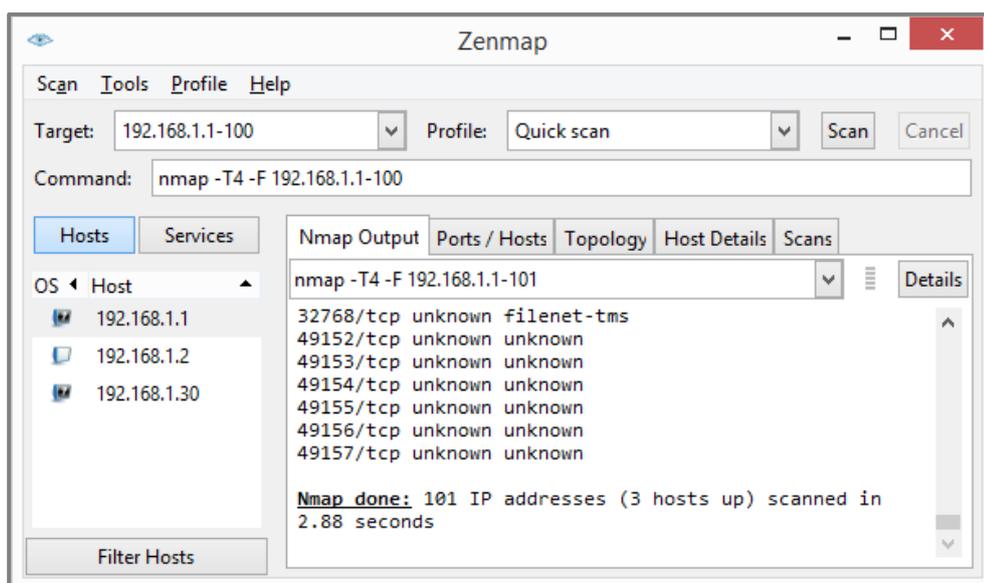
Filtered host					
Index	Host IP	MAC	VLAN	Port	State
1	192.168.1.30	74:d4:35:f4:6b:4e	1	1	Err-Disable



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**.

Anti-Arpscan Configure		Status
Active	<input checked="" type="checkbox"/>	
Port Threshold	200	pps
Host Threshold	10	pps

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.

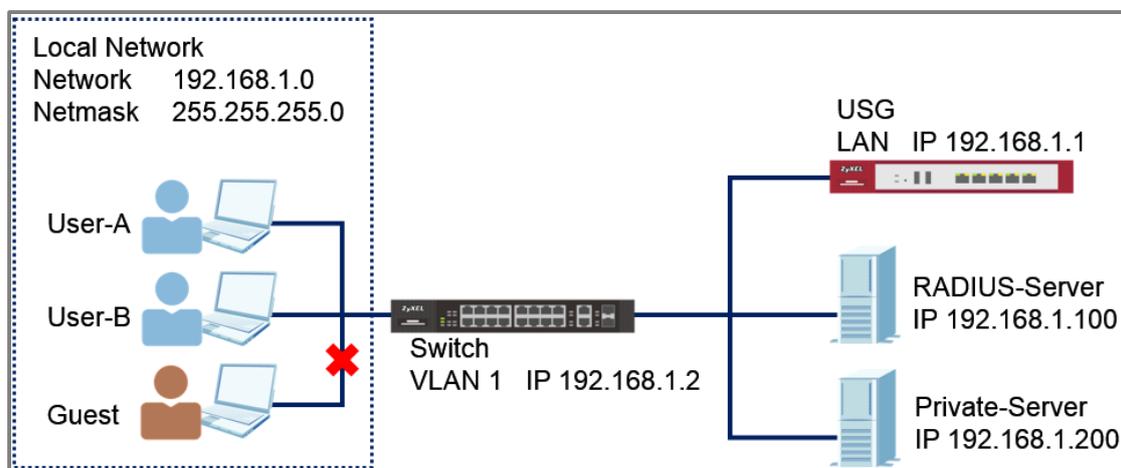


Figure 22 802.1x Port Authentication Providing Access to Authorized Users



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**.

RADIUS Server Setup
[AAA](#)

Authentication Server

Mode: ▼

Timeout: seconds

Index	IP Address	UDP Port	Shared Secret	Delete
1	192.168.1.100	1812	zyxel1234	<input type="checkbox"/>
2	0.0.0.0	1812		<input type="checkbox"/>



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
*	<input checked="" type="checkbox"/>		On ▼				
1	<input checked="" type="checkbox"/>	2	On ▼	3600	60	30	30
2	<input checked="" type="checkbox"/>	2	On ▼	3600	60	30	30
3	<input checked="" type="checkbox"/>	2	On ▼	3600	60	30	30
4	<input checked="" type="checkbox"/>	2	On ▼	3600	60	30	30
5	<input checked="" type="checkbox"/>	2	On ▼	3600	60	30	30
30	<input type="checkbox"/>	2	On ▼	3600	60	30	30
31	<input type="checkbox"/>	2	On ▼	3600	60	30	30
32	<input type="checkbox"/>	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

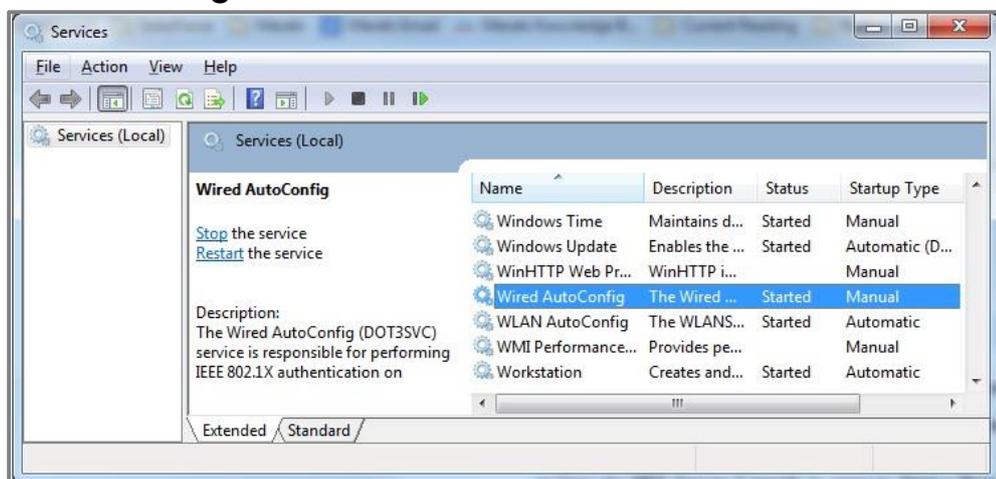
User-B Cleartext-Password := "zyxeluserB"
      Service-Type = Administrative-User
```

- 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#
```

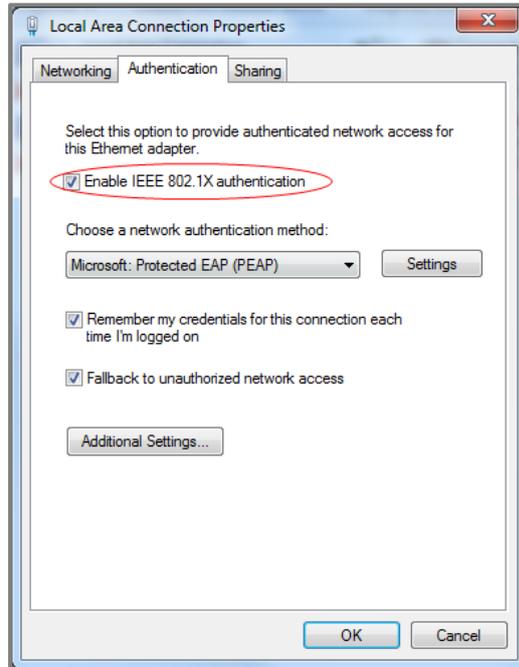
5.4.3 Test the Result

- 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"**.

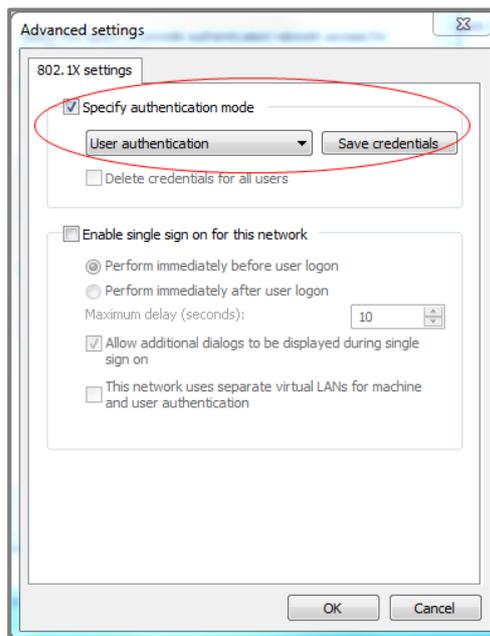


- 4 Right-click on your network adapter and select **Properties**.

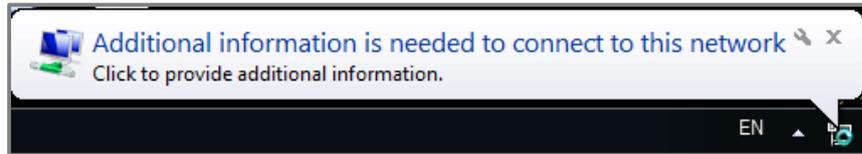
- 5 Click on the Authentication tab and check “**Enable IEEE 802.1X authentication**”. Make sure that the network authentication method is **Microsoft: Protected EAP (PEAP)**



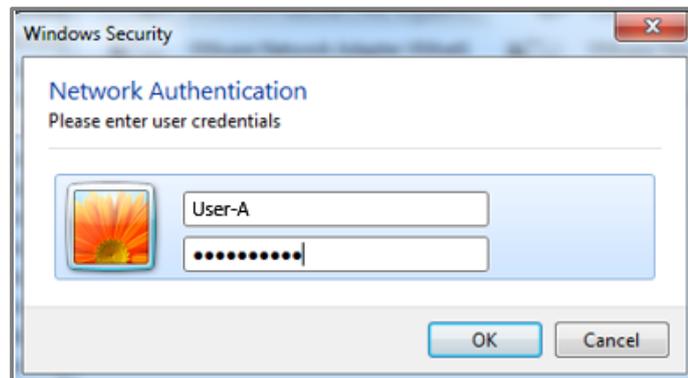
- 6 Click on **Additional Settings**, select **Specify authentication mode** and specify **User authentication**.



- 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.

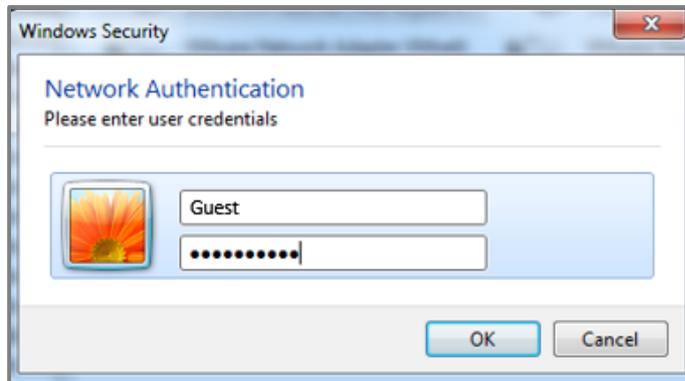


- 8 Enter the username (**User-A**) and password (**zyxeluserA**) which must be consistent with the RADIUS-Server's user profile settings.



- 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.

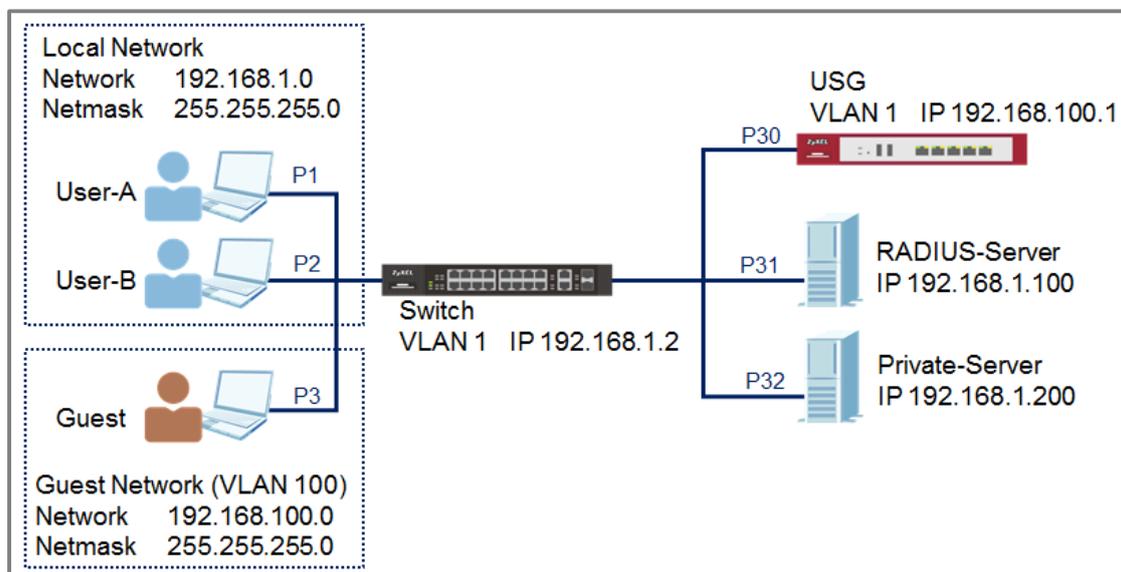


Figure 23 Configure the switch to send unauthorized user in Guest VLAN



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".

Guest Vlan					802.1x	
Port	Active	Guest Vlan	Host-mode	Multi-Secure Num		
*	<input type="checkbox"/>		Multi-Host ▼			
1	<input checked="" type="checkbox"/>	100	Multi-Host ▼	1		
2	<input checked="" type="checkbox"/>	100	Multi-Host ▼	1		
3	<input checked="" type="checkbox"/>	100	Multi-Host ▼	1		

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.

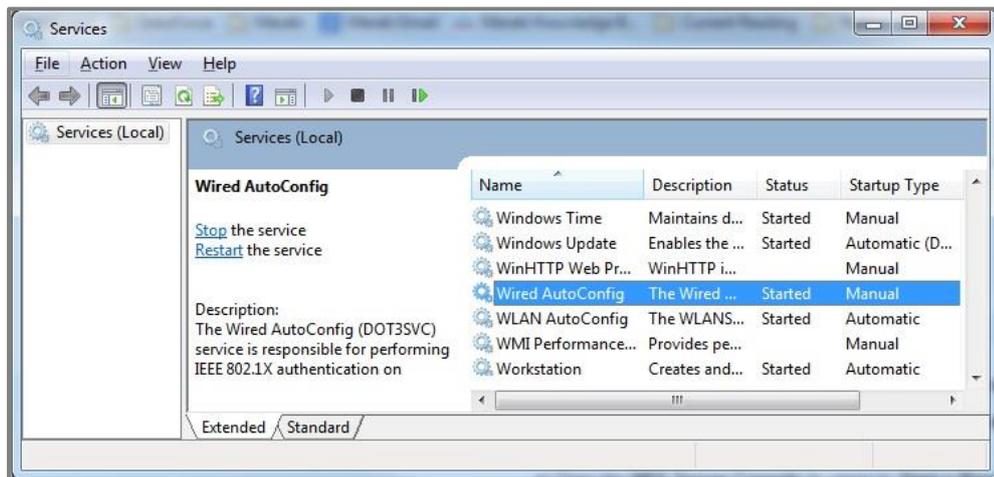
```
user Cleartest-Password := "user1234"
    Service-Type = Administrative-User
```

- 3 Restart FreeRADIUS service.

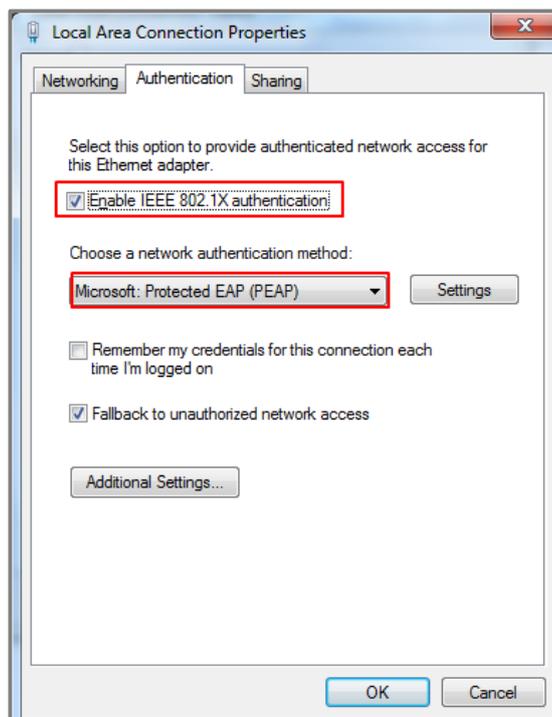
```
root@dhc68:/etc/freeradius# stop freeradius
stop: Unknown instance:
root@dhc68:/etc/freeradius# start freeradius
freeradius start/running, process 8800
```

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

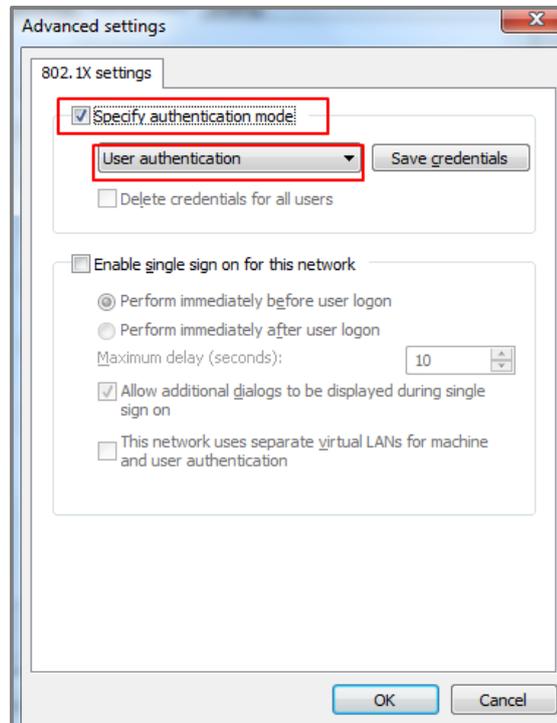
- 1 In the **Services** window, locate the service named **Wired AutoConfig**. Make sure the service status is "Started".



- 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)**".

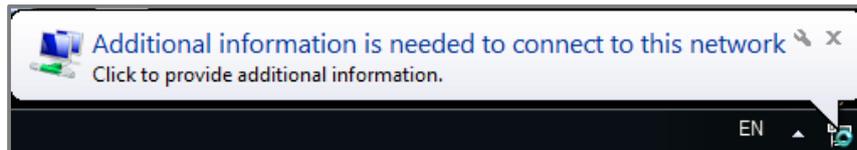


- 3 Click on **Additional Settings**, select **Specify authentication mode** and specify **User authentication**.

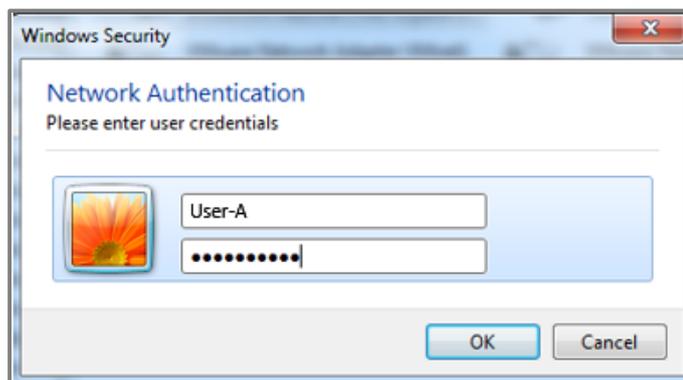


5.5.6 Test the Result

- 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.



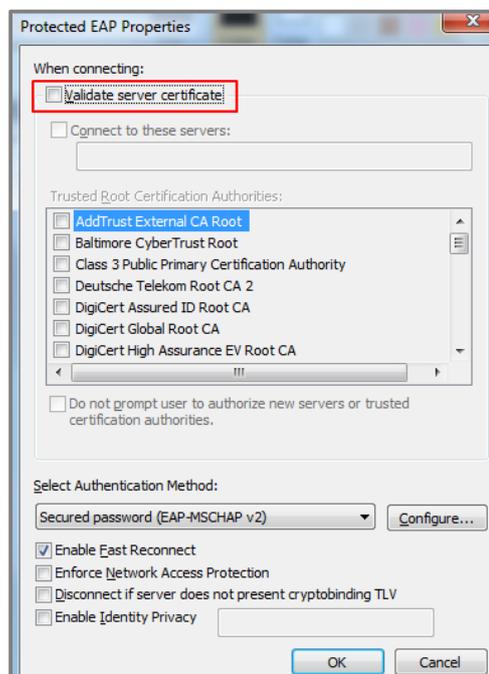
- 3 Devices using User-A and User-B credentials can communicate with Private-Server.
- 4 Connect User-A device to the Switch. User-A should show an **“Additional information is needed to connect to this network.”** pop-up message.
- 5 Enter the username (Guest) and a random password.
- 6 Device using 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.

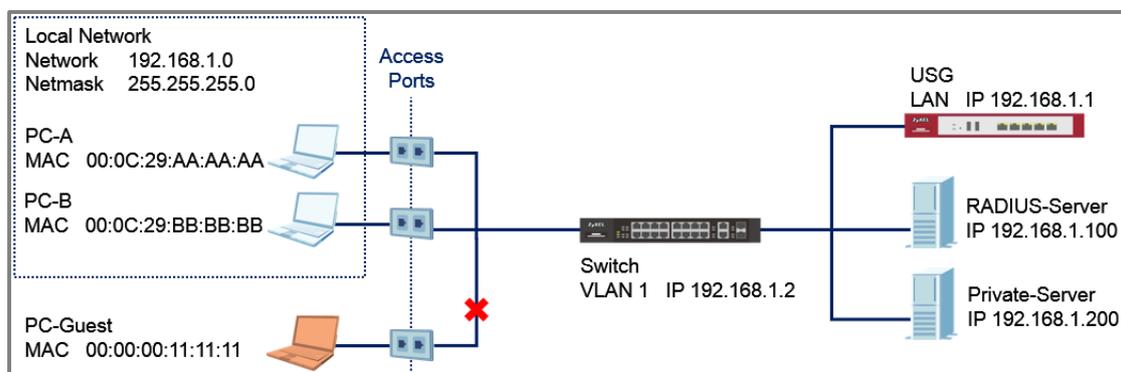


Figure 24 802.1x Port Authentication Providing Access to Authorized Devices



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**.

RADIUS Server Setup
[AAA](#)

Authentication Server

Mode:

Timeout: seconds

Index	IP Address	UDP Port	Shared Secret	Delete
1	192.168.1.100	1812	zyxel1234	<input type="checkbox"/>
2	0.0.0.0	1812		<input type="checkbox"/>



Note:

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

- 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**.

MAC Authentication		Port Authentication	
Active	<input checked="" type="checkbox"/>		
Name Prefix	Access01-		
Password	zyxel		
Timeout	0		

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

5.6.2 Configuration in the RADIUS-Server

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

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



Note:

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

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

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

- 3 Restart FreeRADIUS service.

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

5.6.3 Test the Result

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

5.6.4 What Could Go Wrong?

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

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

5.7 How to configure the switch to prevent ARP spoofing

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

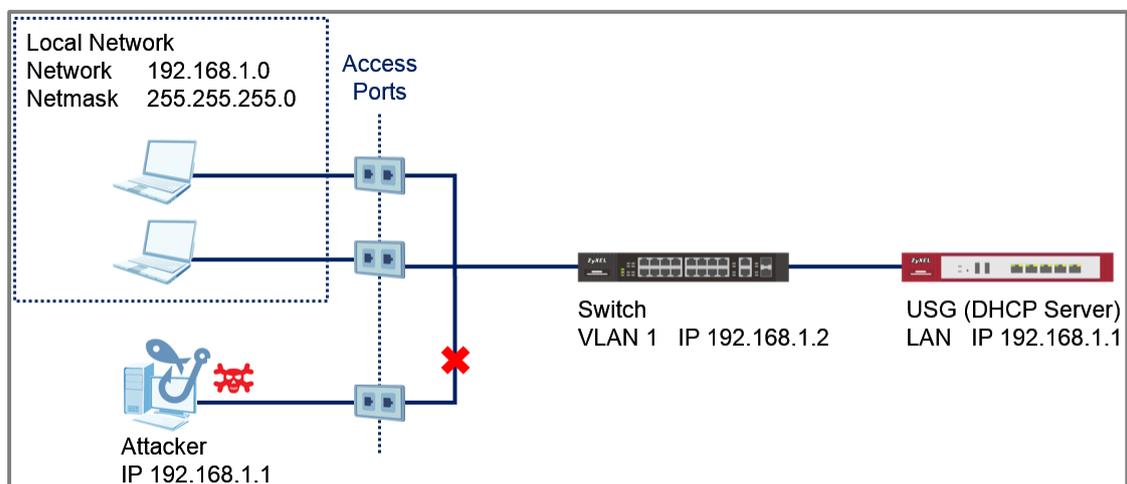


Figure 25 Attacker Using the Same IP Address as the USG



Note:

All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. All UI displayed in this article are taken from the 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.

ARP Inspection Configure		ARP Inspection Port VLAN
Active	<input checked="" type="checkbox"/>	

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**.

ARP Inspection Port Configure				Configure
Port	Trusted State	Rate (pps)	Limit	
			Burst interval (seconds)	
*	Untrusted ▼			
1	Untrusted ▼	15	1	
2	Untrusted ▼	15	1	
3	Untrusted ▼	15	1	
4	Untrusted ▼	15	1	
5	Untrusted ▼	15	1	
30	Trusted ▼	15	1	
31	Trusted ▼	15	1	
32	Trusted ▼	15	1	

- 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**.

ARP Inspection VLAN Configure				Configure
VLAN	Start VID	1	End VID	5
<input type="button" value="Apply"/>				

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

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

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**.

5.8 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.

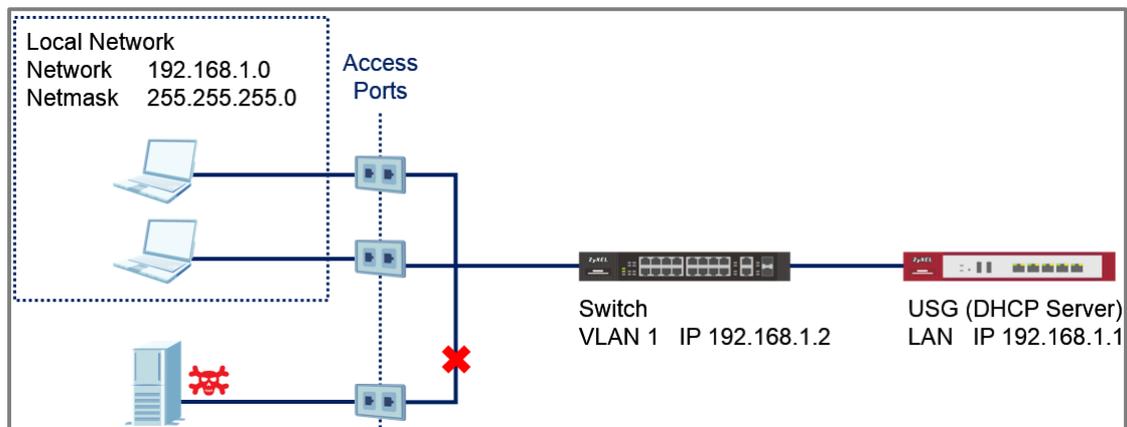


Figure 26 Fake DHCP Server Connected through Publicly Accessible Ports



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**.

Static VLAN		VLAN Configuration
ACTIVE	<input checked="" type="checkbox"/>	
Name	<input type="text" value="1"/>	
VLAN Group ID	<input type="text" value="1"/>	
VLAN Type	<input checked="" type="radio"/> Normal <input type="radio"/> Private <input type="text" value=""/>	
Association VLAN List	<input type="text"/>	

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

31	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
32	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging

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

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

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

DHCP Snooping Configure [DHCP Snooping](#) [Port](#) [VLAN](#)

Active

DHCP Vlan Disable

- 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**.

DHCP Snooping Port Configure [Configure](#)

Port	Server Trusted state	Rate (pps)
*	Untrusted ▼	
1	Untrusted ▼	0
2	Untrusted ▼	0
3	Untrusted ▼	0
4	Untrusted ▼	0
5	Untrusted ▼	0
30	Untrusted ▼	0
31	Untrusted ▼	0
32	Trusted ▼	0

[Apply](#) [Cancel](#)

- 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**.

DHCP Snooping VLAN Configure				Configure	Port
Show VLAN	Start VID	1	End VID	5	
<input type="button" value="Apply"/>					

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

VID	Enabled	Option 82 Profile
*	No ▼	▼
1	Yes ▼	▼
2	No ▼	▼
3	No ▼	▼
4	No ▼	▼
5	No ▼	▼
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

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 is enabled. This allows the administrator device more freedom and take advantage of IP-specific policies configured on the network while non-administrative devices must still use IP addresses offered by the real DHCP server.

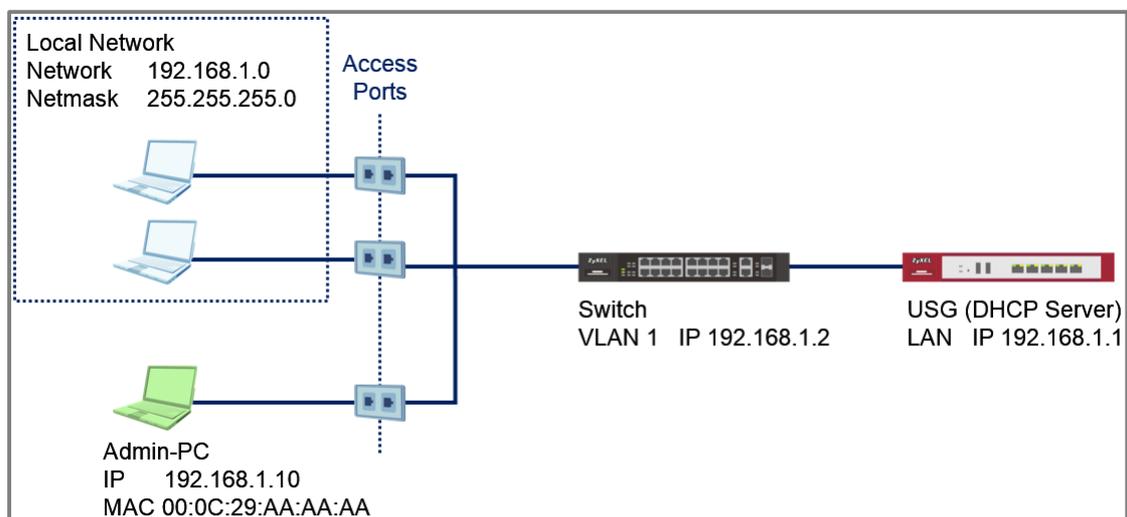


Figure 27 Administrator Device Using a Static IP Address Connected on an Access Port



Note:

All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. All UI displayed in this article are taken from the 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**.

Static Binding	
MAC Address	00:0c:29:aa:aa:ac
IP Address	192.168.1.10
VLAN	1
Port	<input type="radio"/> <input type="text"/> <input checked="" type="radio"/> Any
<input type="button" value="Add"/> <input type="button" value="Cancel"/> <input type="button" value="Clear"/>	

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.

IP Source Guard			IPSG	Static Binding	DHCP Snooping	ARP Inspection
Index	MAC Address	IP Address	Lease	Type	VID	Port
1	00:0c:29:aa:aa:aa	192.168.1.10	infinity	static	1	

- 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.

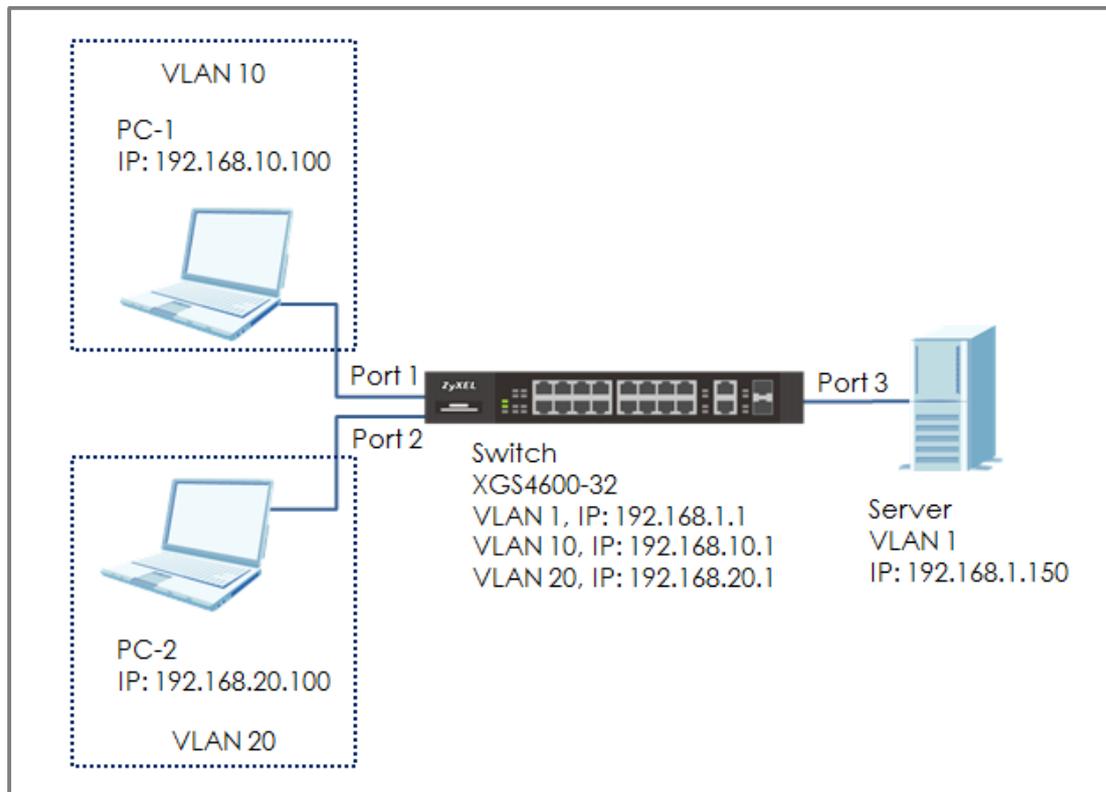


Figure 21 Configure ACL to block unwanted traffic



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”.

Classifier Configuration		Classifier Status	Classifier Global Setting
Active	<input checked="" type="checkbox"/>		
Name	VLAN20		
Weight	32767		

Layer 2	VLAN	<input type="radio"/> Any <input checked="" type="radio"/> 20	
	Inner VLAN	<input type="radio"/> Any <input type="text"/>	
	Priority	Priority	<input type="radio"/> Any <input type="text" value="0"/>
		Inner Priority	<input type="radio"/> Any <input type="text" value="0"/>
	Ethernet Type	<input checked="" type="radio"/> All <input type="radio"/> Others <input type="text"/> (Hex)	
	Source	<input type="radio"/> Any <input type="radio"/> MAC Address <input type="text"/> <input type="text"/> /Mask <input type="text"/>	
Destination	<input type="radio"/> Any <input type="radio"/> MAC Address <input type="text"/> <input type="text"/> /Mask <input type="text"/>		

Layer 3	IP Packet Length	<input checked="" type="radio"/> Any <input type="radio"/> [] To [] Bytes
	DSCP	IPv4 <input checked="" type="radio"/> Any <input type="radio"/> []
		IPv6 <input checked="" type="radio"/> Any <input type="radio"/> []
	Precedence	<input checked="" type="radio"/> Any <input type="radio"/> []
	ToS	<input checked="" type="radio"/> Any <input type="radio"/> []
	IP Protocol	<input checked="" type="radio"/> All <input type="checkbox"/> Establish Only <input type="radio"/> Others [] (Dec)
	IPv6 Next Header	<input checked="" type="radio"/> All <input type="checkbox"/> Establish Only <input type="radio"/> Others [] (Dec)
	Source	IP Address / 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”.

Policy	
Active	<input checked="" type="checkbox"/>
Name	Policy_VLAN20
Classifier(s)	VLAN20

Forwarding	
<input type="radio"/>	No change
<input checked="" type="radio"/>	Discard the packet
<input type="radio"/>	Do not drop the matching frame previously marked for dropping

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.

Classifier Configuration [Classifier Status](#) [Classifier Global Setting](#)

Active	<input checked="" type="checkbox"/>
Name	VLAN20
Weight	32767
Log	<input type="checkbox"/>
Count	<input checked="" type="checkbox"/>

Classifier Status [Classifier Configuration](#)

Index	Active	Weight	Name	Match Count	Rule
1	Yes	32767	VLAN20	4	vlan 20; DestIP = 192.168.1.150/32; count;

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.

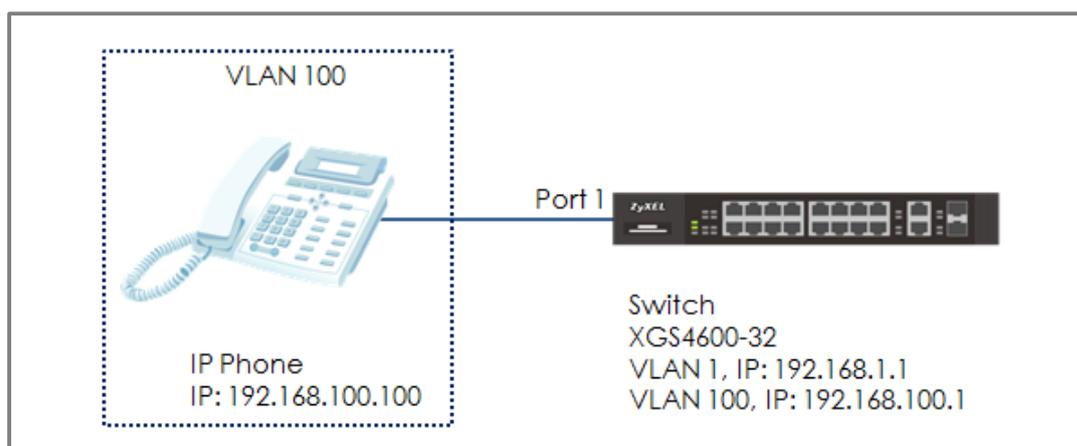


Figure 23 Configure LLDP-MED to assign an IP Phone's VLAN



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.

LLDP Configuration		LLDP Basic TLV Setting Org-specific TLV Setting
Active	<input checked="" type="checkbox"/>	
Transmit Interval	30	seconds
Transmit Hold	4	times
Transmit Delay	2	seconds
Reinitialize Delay	2	seconds

- 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).

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

- 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	<input type="text" value="1"/>	
Application Type	voice ▼	
Tag	tagged ▼	
VLAN	<input type="text" value="100"/>	
DSCP	0	
Priority	7 ▼	

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.

Ping Test

IPv4 -
 IPv6 -
 IP Address/Host Name 192.168.100.100
 Source IP Address
 Count 3

Diagnostic

Resolving 192.168.100.100... 192.168.100.100

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

6.1.4 What Could Go Wrong

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

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

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

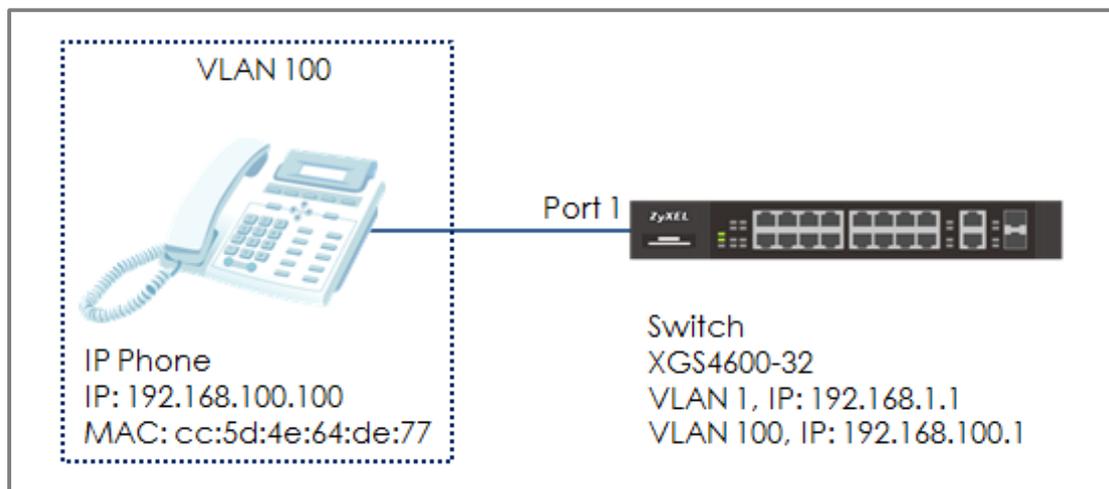


Figure 24 Configure Voice VLAN to separate VOIP traffic from data traffic



Note:

All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using 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".

Voice VLAN Setup		VLAN Configuration
Voice VLAN Global Setup		
Voice VLAN	<input type="radio"/> Disable <input checked="" type="radio"/> 100	
Priority	5 ▼	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/> <input type="button" value="Clear"/>		

- 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".

Voice VLAN OUI Setup	
OUI address	cc:5d:4e:64:de:77
OUI mask	ff:ff:ff:00:00:00
Description	ZYXEL IP Phone
<input type="button" value="Add"/> <input type="button" value="Cancel"/>	



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.

Ping Test

IPv4 - ▾
 IPv6 - ▾

IP Address/Host Name:

Source IP Address:

Count:

Diagnostic									
Resolving 192.168.100.100... 192.168.100.100									
	sent	rcvd	rate	rft	avg	mdev	max	min	reply from
1	1	100	0	0	0	0	0	0	192.168.100.100
2	2	100	0	0	0	0	0	0	192.168.100.100
3	3	100	0	0	0	0	0	0	192.168.100.100

6.2.4 What Could Go Wrong

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

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

6.3 How to configure the switch to improve Voice traffic quality

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

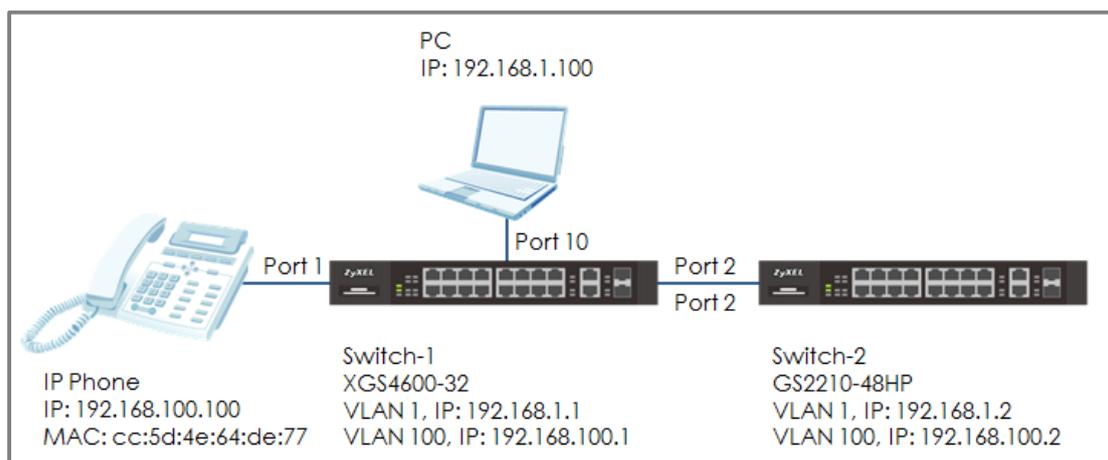


Figure 25 Configure Voice VLAN to separate VOIP traffic from data traffic



Note:

All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using 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".

Voice VLAN Setup	
Voice VLAN Global Setup	
VLAN Configuration	
Disable	<input type="radio"/>
Voice VLAN	<input type="text" value="100"/>
Priority	<input type="text" value="6"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/> <input type="button" value="Clear"/>	

- 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".

Voice VLAN OUI Setup	
OUI address	<input type="text" value="cc:5d:4e:64:de:77"/>
OUI mask	<input type="text" value="ff:ff:ff:00:00:00"/>
Description	<input type="text" value="ZYXEL IP Phone"/>
<input type="button" value="Add"/> <input type="button" value="Cancel"/>	



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”.

Mirroring		RMirror
Active	<input checked="" type="checkbox"/>	
Monitor Port	10	
Port	Mirrored	Direction
*	<input type="checkbox"/>	Ingress ▼
1	<input type="checkbox"/>	Ingress ▼
2	<input checked="" type="checkbox"/>	Both ▼
3	<input type="checkbox"/>	Ingress ▼

6.3.4 Test the Result

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

The screenshot shows a Wireshark capture of ICMP ping traffic. The packet list pane displays four packets (No. 17-20) between 192.168.100.2 and 192.168.100.100. Packet 19 is highlighted, showing it is an Echo (ping) reply from 192.168.100.100 to 192.168.100.2. The packet details pane for packet 19 shows the Ethernet II header and the 802.1Q Virtual LAN header. The 802.1Q header is expanded to show: Priority: Voice, < 10ms latency and jitter (6); CFI: Canonical (0); ID: 100. The Type is IPv4 (0x0800).

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

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

6.3.5 What Could Go Wrong

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

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

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