ZYXEL

www.zyxel.com

Switch Series

GS1350 Series

Edition 2020.1

Handbook

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

Contents

Basic principles for network management

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.

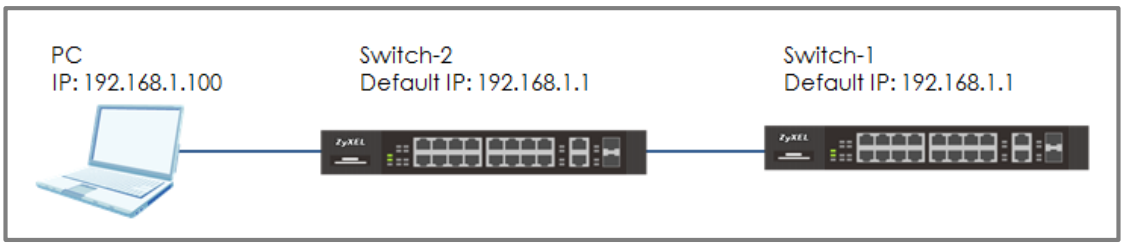


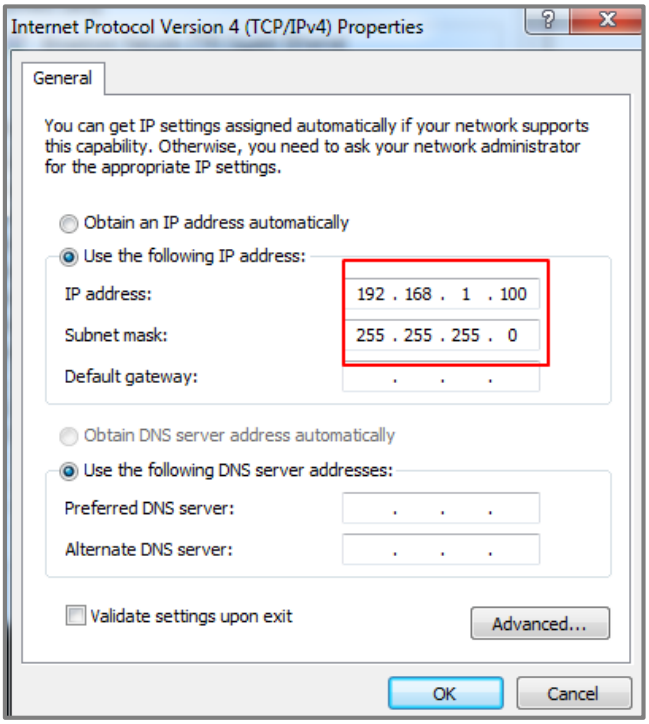
Figure 1 Two switches are using the same default IP address

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.

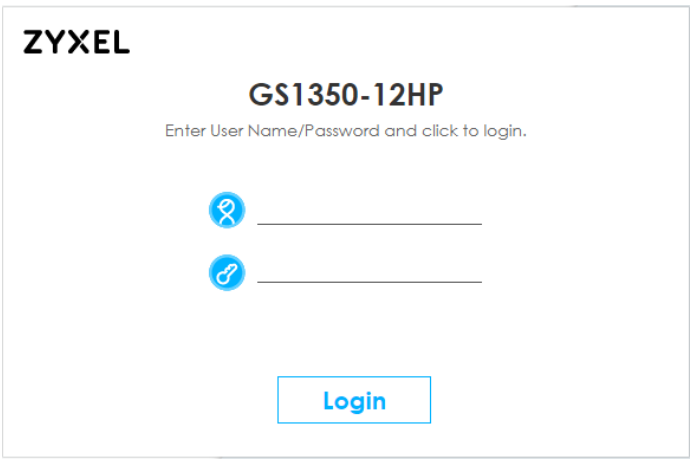
1.1.1 Configuration in the Switch-2

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

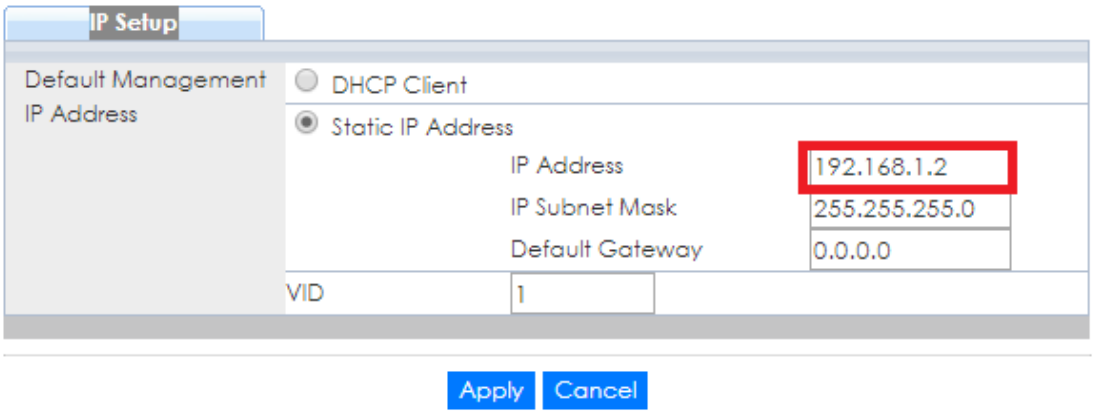
2 Set the PC's IP address on to the same subnet as the switches. For example, set the PC IP address as **192.168.1.100**.



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**. Set the IP address you prefer, for example **192.168.1.2**. Then click **Apply**.



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 click **Status > IP Address Information**. Check if the IP address is already configured as **192.168.1.2**.

IP Address Information	
IPV4 Address	192.168.1.2
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0

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.

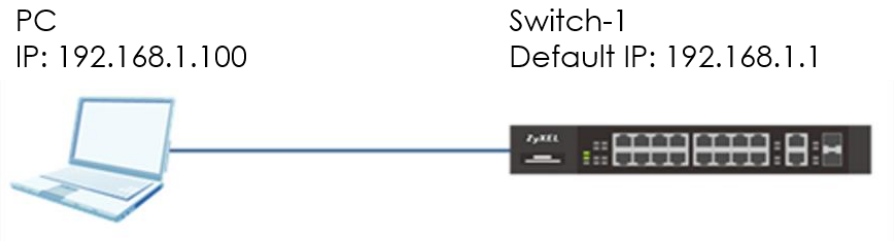


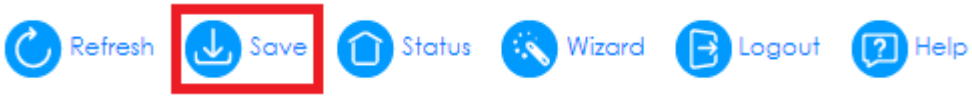
Figure 2 Change the device name of the switch

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.

1.2.1 Configuration in Switch-1

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

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



1.2.2 Test the Result

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

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

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

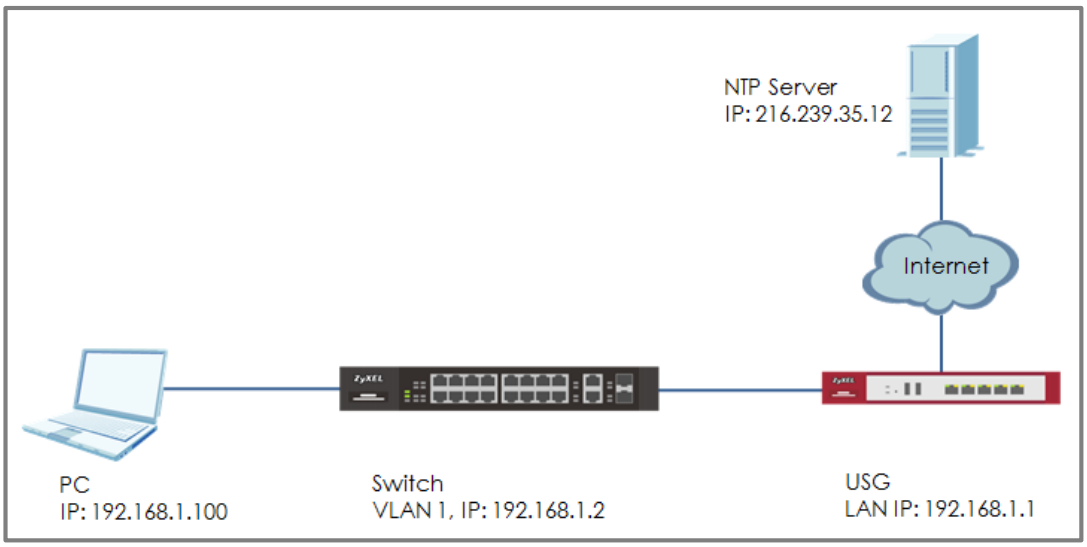
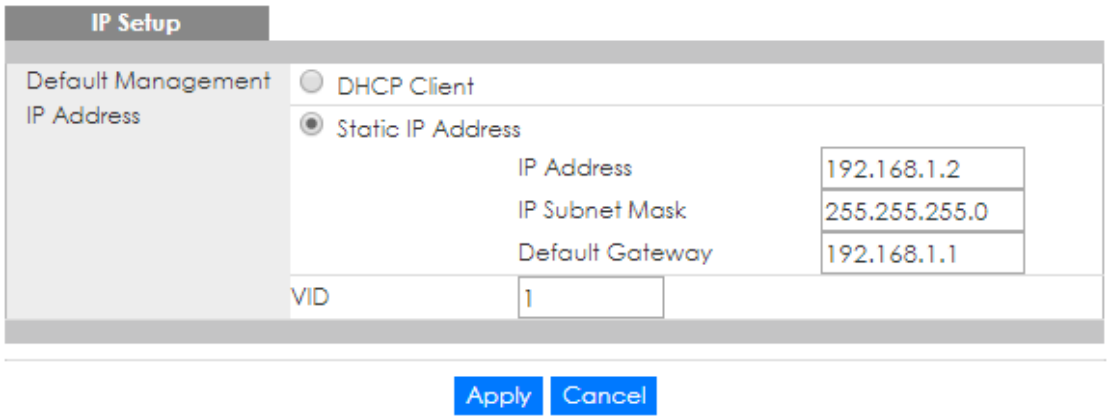


Figure 3 Set up Switch to get time from NTP Server

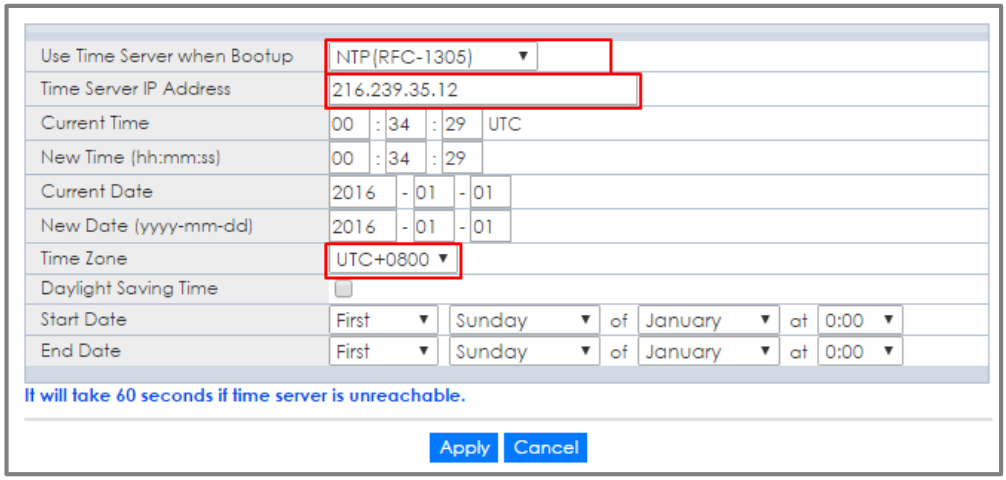
Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. We use google free public NTP server (216.239.35.12) to be our NTP server. You can also choose another available NTP server. Furthermore, due 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**. Set the default Gateway as USG IP: **192.168.1.1**. Then click "**Apply**".



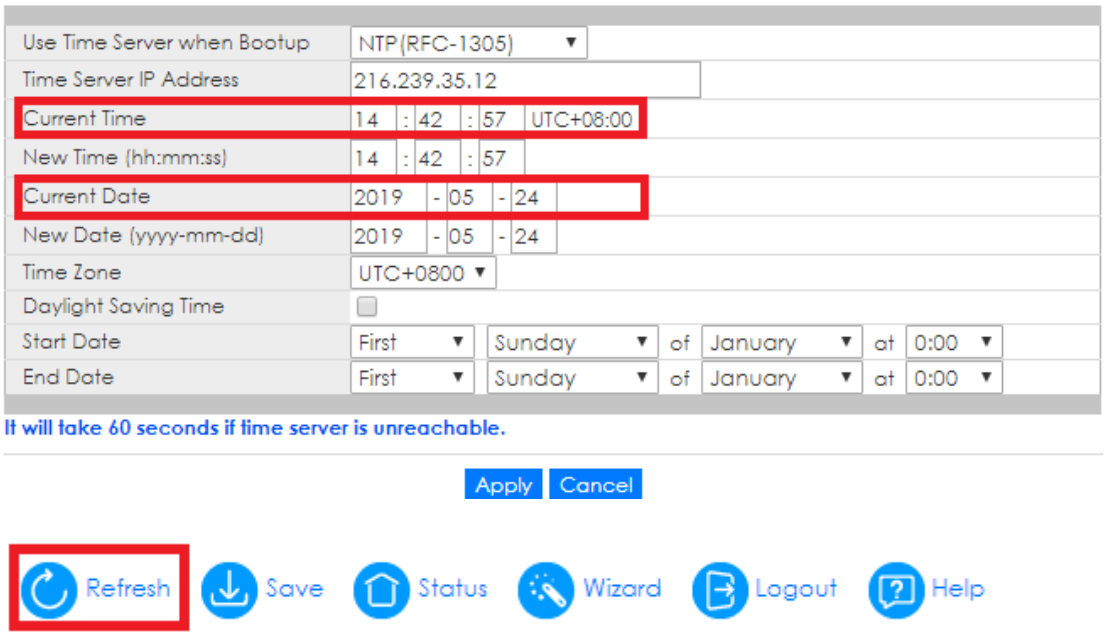
2 Go to **Menu > Basic Setting > General Setup**. Select "Use Time Server when Bootup" to **NTP(RFC-1305)** and set the "Time Server IP Address". In this scenario, we use the google free public NTP server (**216.239.35.12**) as an example. Also, select the "Time Zone" in your location. Finally, remember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



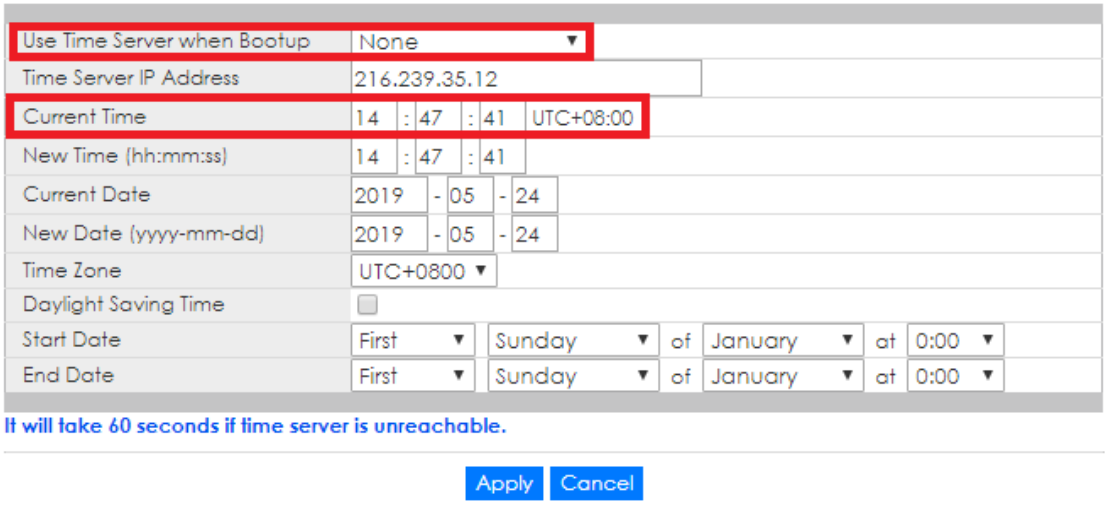
3 Click **Save** to save the configuration.

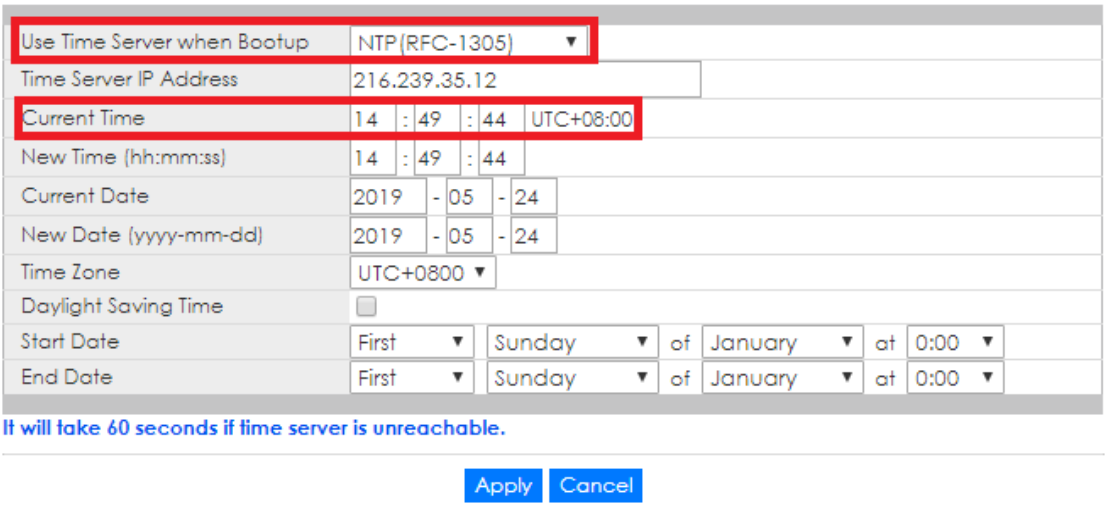
1.3.2 Test the Result

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



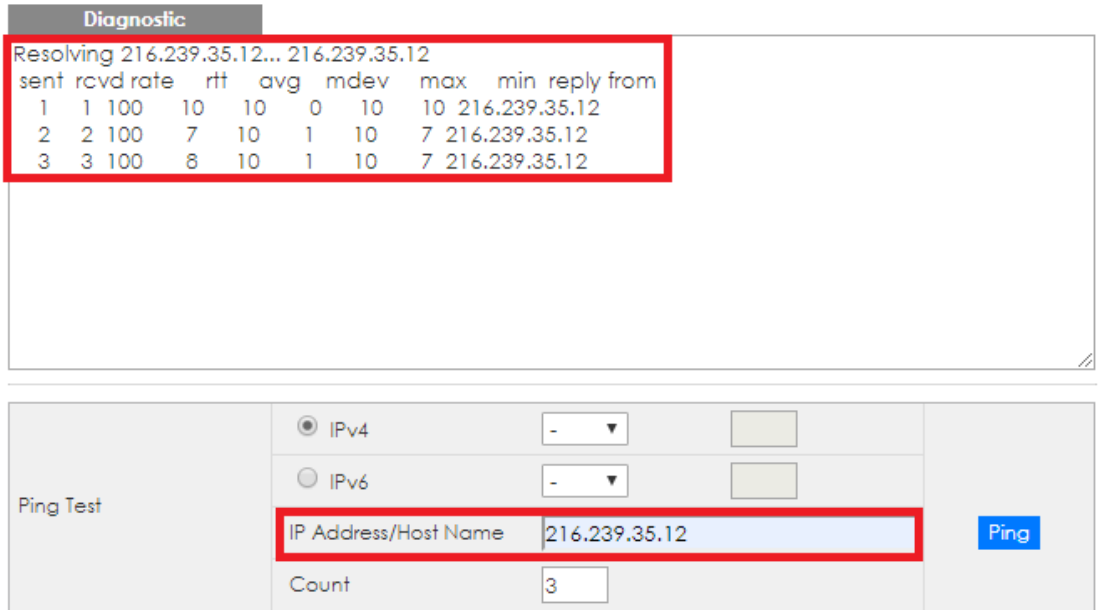
2 Try to select the "User Time Server when Bootup" as **None**. Few second later, change back to **NTP(RFC-1305)**. The time will still update to the current time.





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 and type the IP address of NTP Server (216.239.35.12) into the IP Address field. Click "**Ping**".



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

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

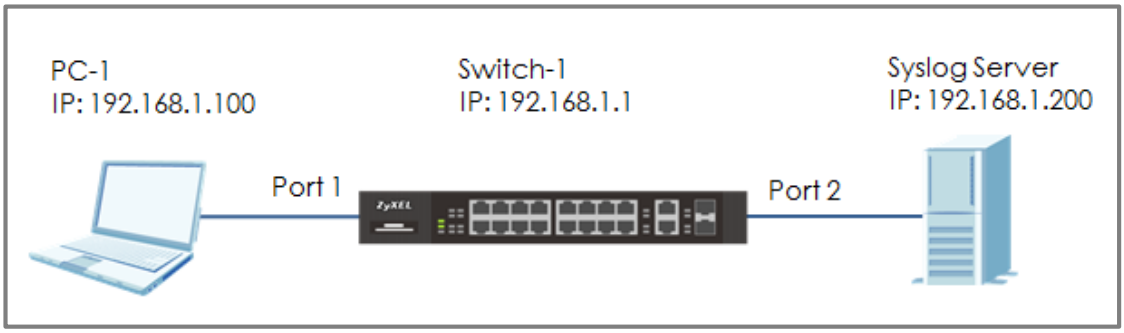
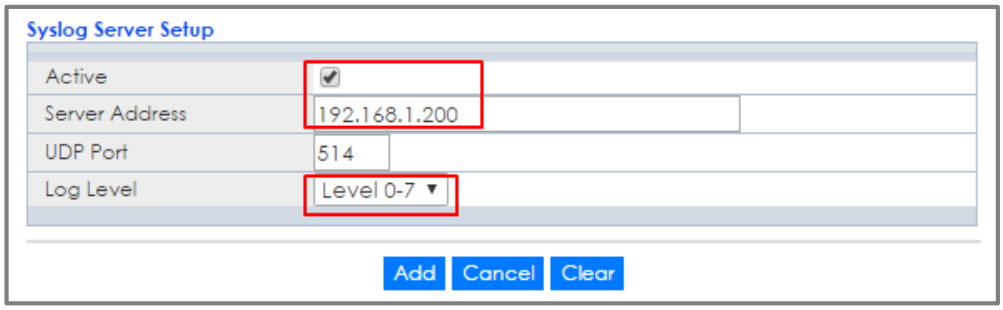


Figure 4 Upload the syslog automatically to the server

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

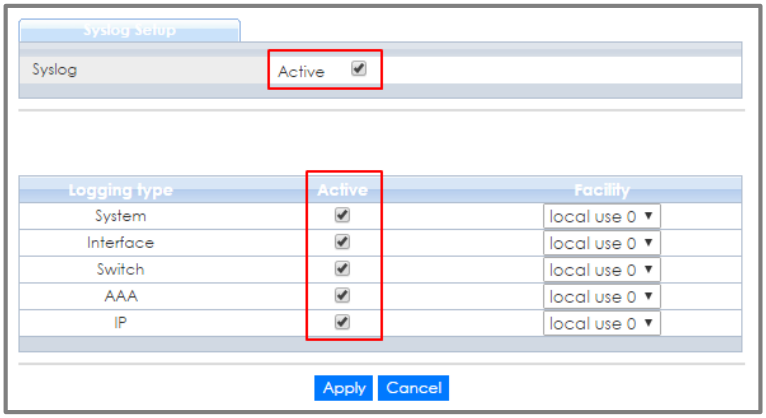
1.4.1 Configure the Switch-1

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

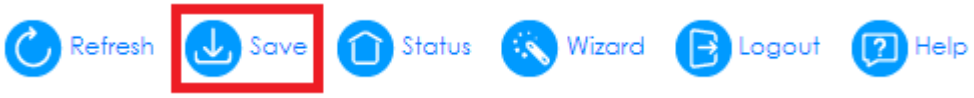


Note:
Log Level refers to which events should be sent to the Syslog Server.
Severity: Emergency (0), Alert (1), Critical (2), Error (3), Warning (4), Notice (5), Informational (6), and Debug (7).

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



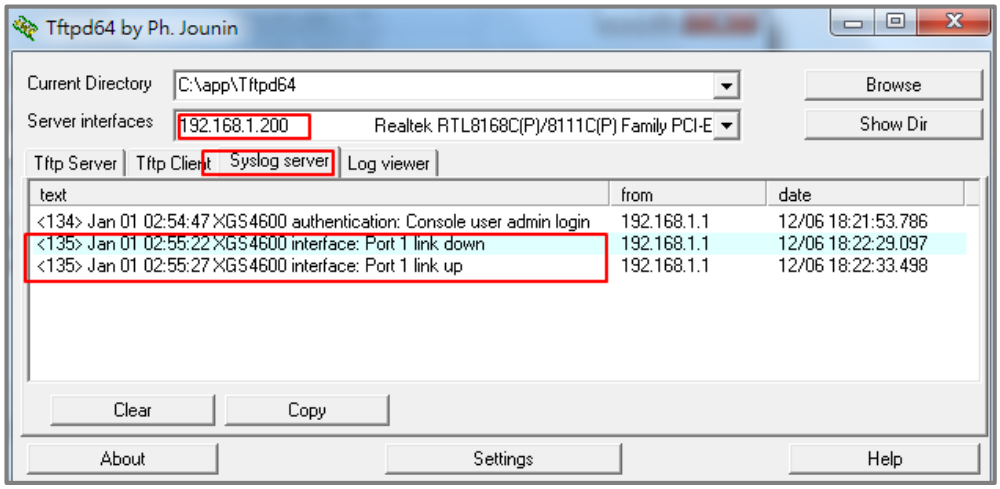
3 Click **Save** to save the configuration.



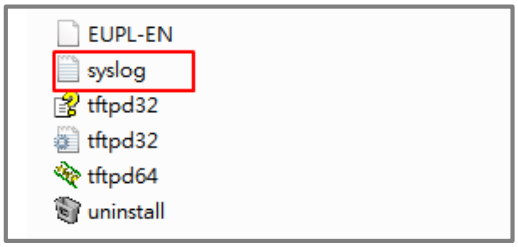
1.4.2 Test the Result

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

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



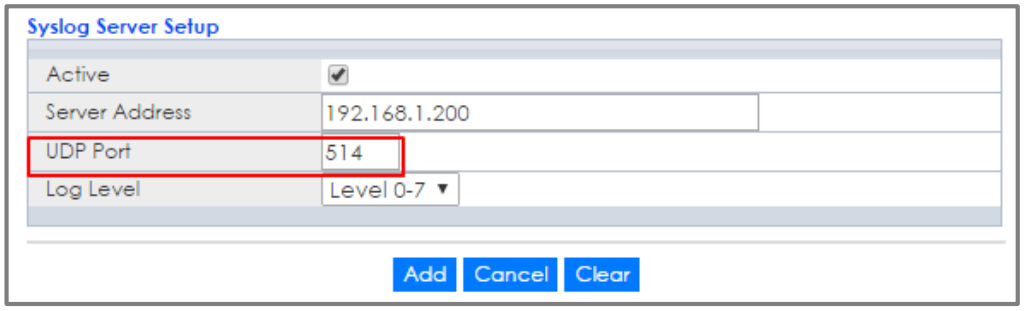
3 We can also check the **directory** ("C:\app\Tftpd64" in this example) to find out if a text file is created on the Syslog Server.



1.4.3 What could go wrong?

1 If Switch-1 and Syslog Server are in different subnets, remember to set **default gateway** so that Switch-1 and the Syslog Server can communicate with each other.

2 Confirm the service port number of the Switch-1 and the Syslog Server are the same. (Default service port for the Syslog Server in the Switch-1 is **514**).



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

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

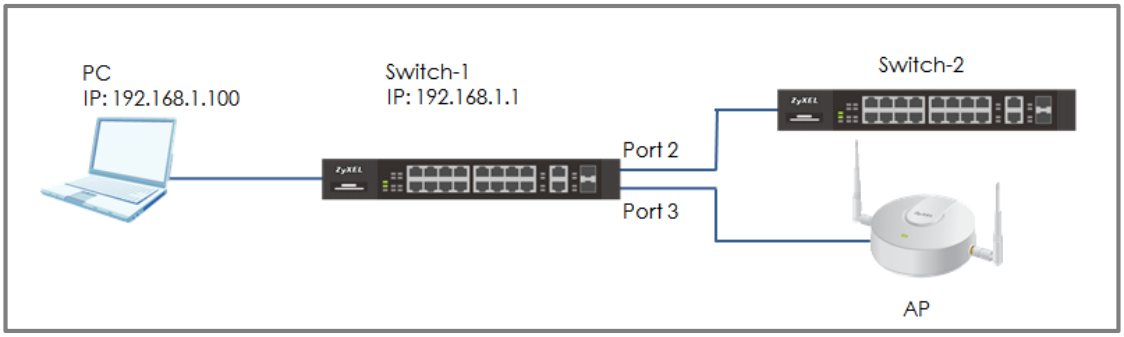
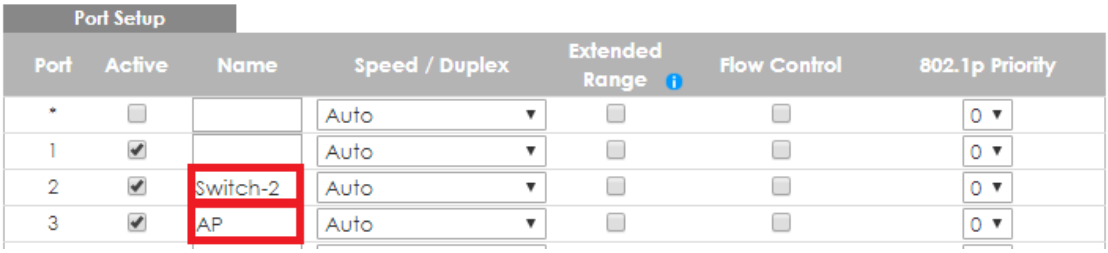


Figure 5 Configure the port name of the switch

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.

1.5.1 Configure Switch-1

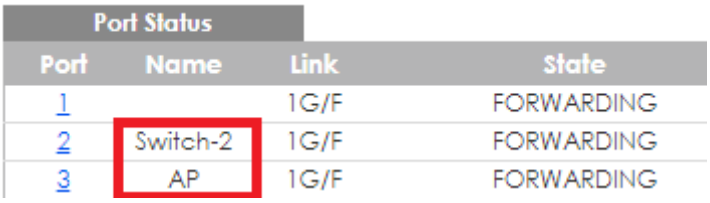
1 Enter the web GUI and go to **Menu > Basic Setting > Port Setup**. Type the name of each directly connected devices on the corresponding port name. For example, you can type Switch-2 in port 2 and AP in port 3. Then click "**Apply**".



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

1.5.2 Test the Result

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



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.

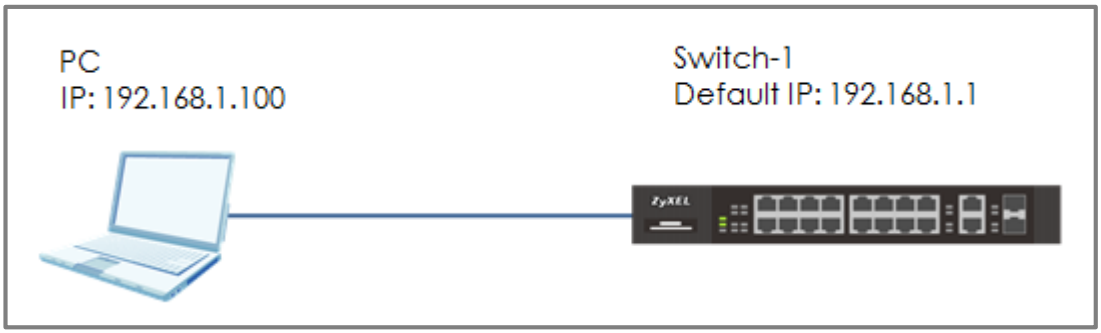
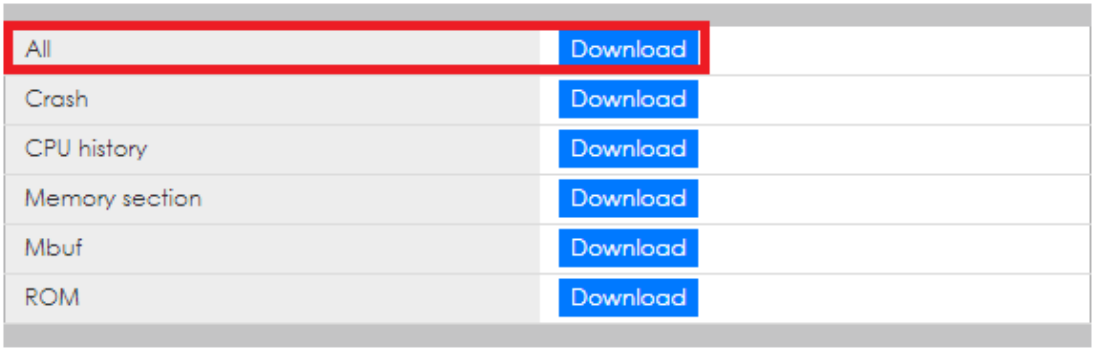


Figure 6 Collect the Diagnostic Info from web GUI

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.

1.6.1 Collect the Diagnostic Info from web GUI

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



1.6.2 Test the Result

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

techSupport_all_1.log

```
1
2
3  Time :    69:55:13 ==========   show system-information        ================= msclock :251713692
4
5
6  Product Model       : GS1350-12HP
7  System Name     : Switch-1
8  System Mode     : Standalone
9  System Contact      :
10 System Location     :
11 System up Time      :    69:55:13 (f00d89c ticks)
12 Ethernet Address    : 00:19:cb:00:00:01
13 Bootbase Version    : V1.00 | 02/22/2019
14 ZyNOS F/W Version   : V4.60(ABPJ.0)b5 | 04/08/2019
15 Hardware Version    : V1.0
16 Config Boot Image   : 1
17 Current Boot Image  : 1
18 Current Configuration   : 1
19 RomRasSize      : 5404132
20 Serial Number       : xxxxxxxxxxxxxxx
21 Register MAC Address    : 00:19:cb:00:00:01
22
23
```

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.

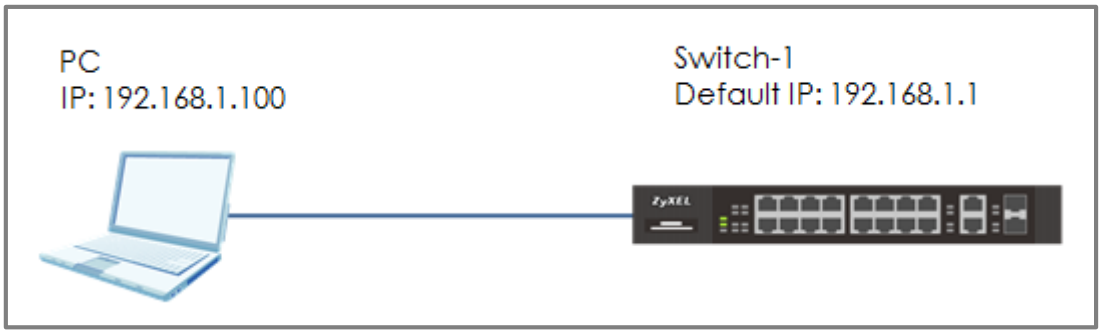
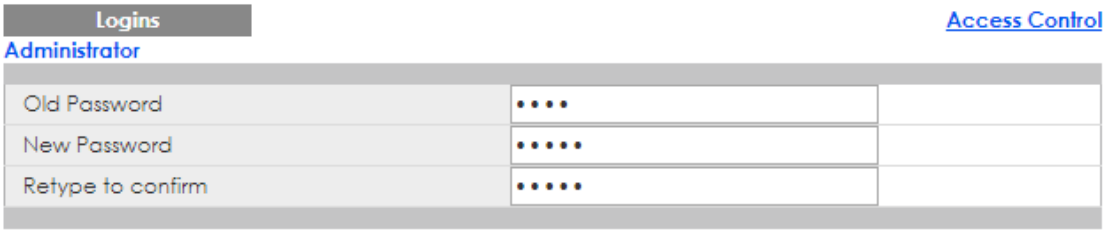


Figure 7 Change the default administrator password

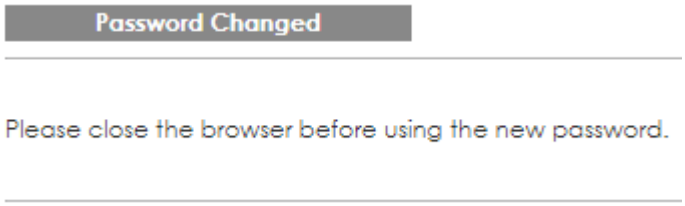
Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks.

1.7.1 Change the default administrator password

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

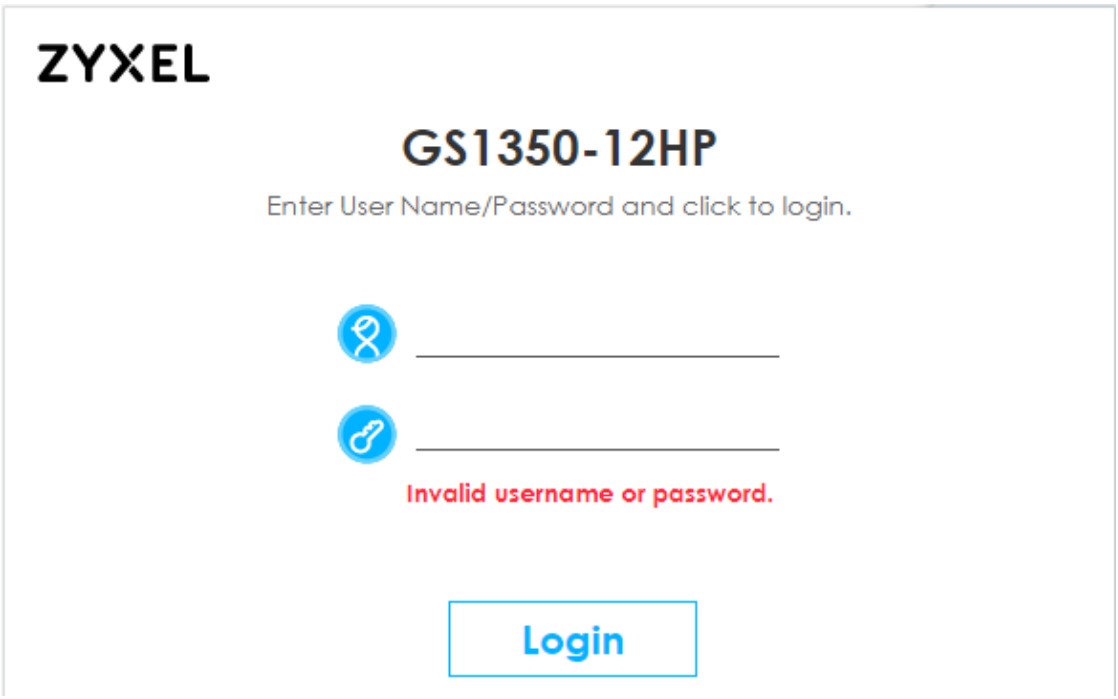


2 After clicking the "**Apply**", the browser will show a message similar below.



1.7.2 Test the Result

1 Close the web GUI and login again with the **OLD** password. The "Authentication Required" window will pop up again and show "**Invalid username or 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…..).

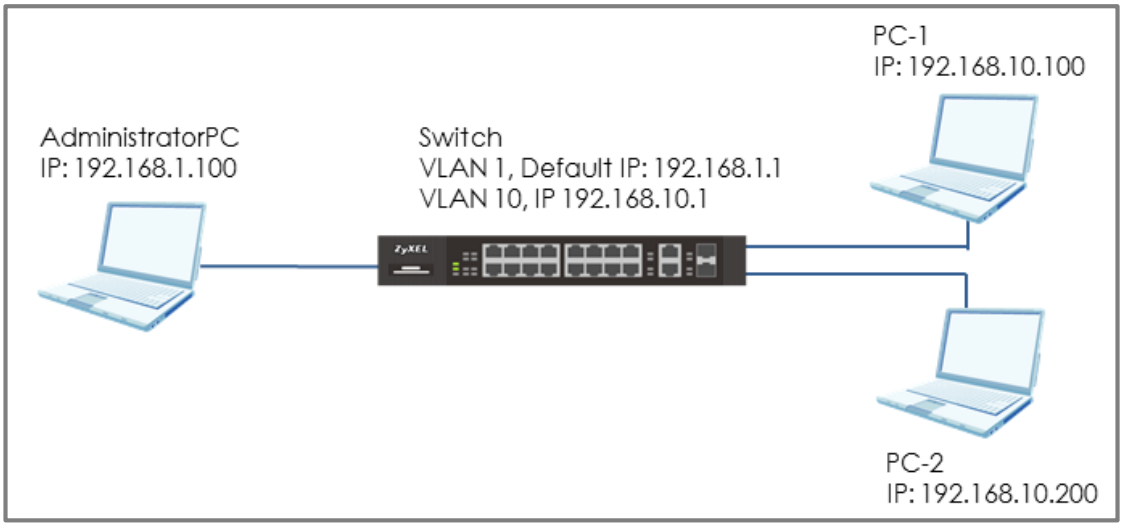
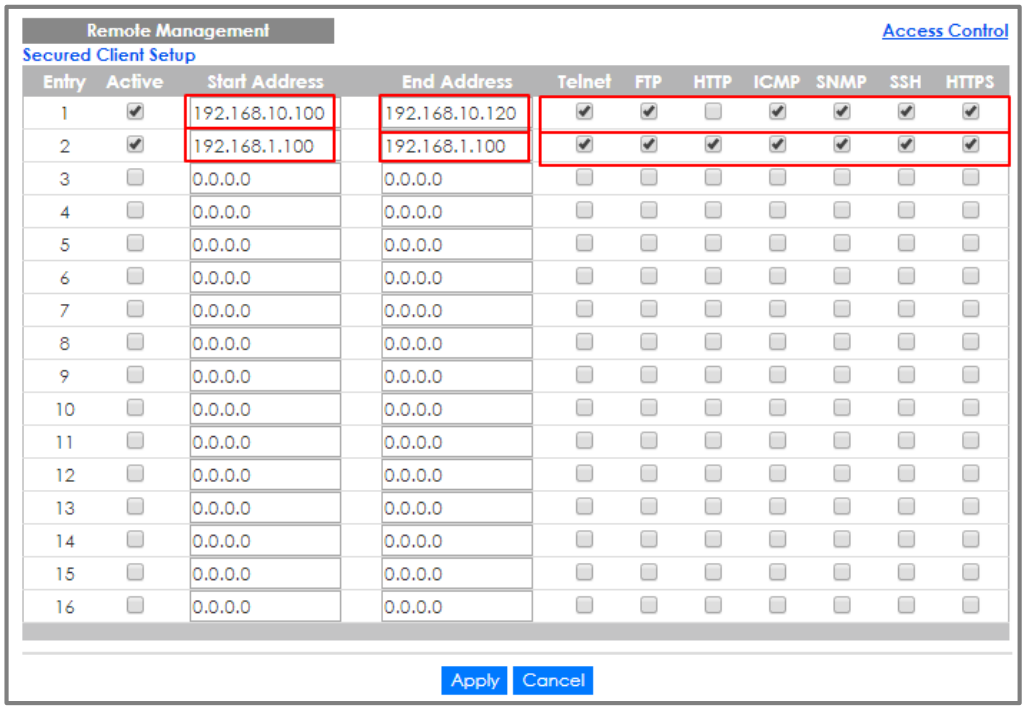


Figure 8 Configure the whitelist for remote management

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.

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 Administrator PC. Enter the range of IP addresses and the corresponding types of services that are allowed to access the Switch. Then click "**Apply**".



1.8.2 Test the Result

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

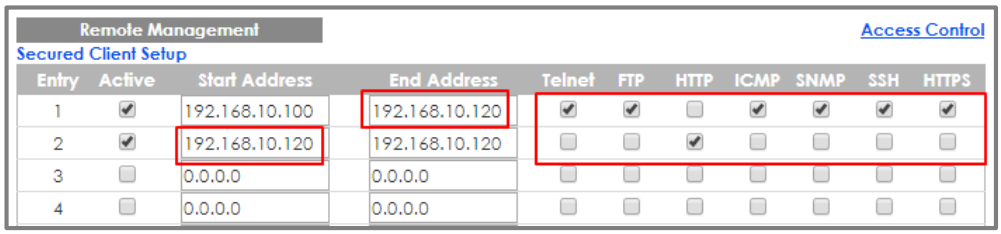
2 The PC-2 (192.168.10.200) is not in the range which is allowed to access the Switch. PC-2 cannot access or ping the switch's management IP address.

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

1.8.3 What could go wrong?

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

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



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

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.

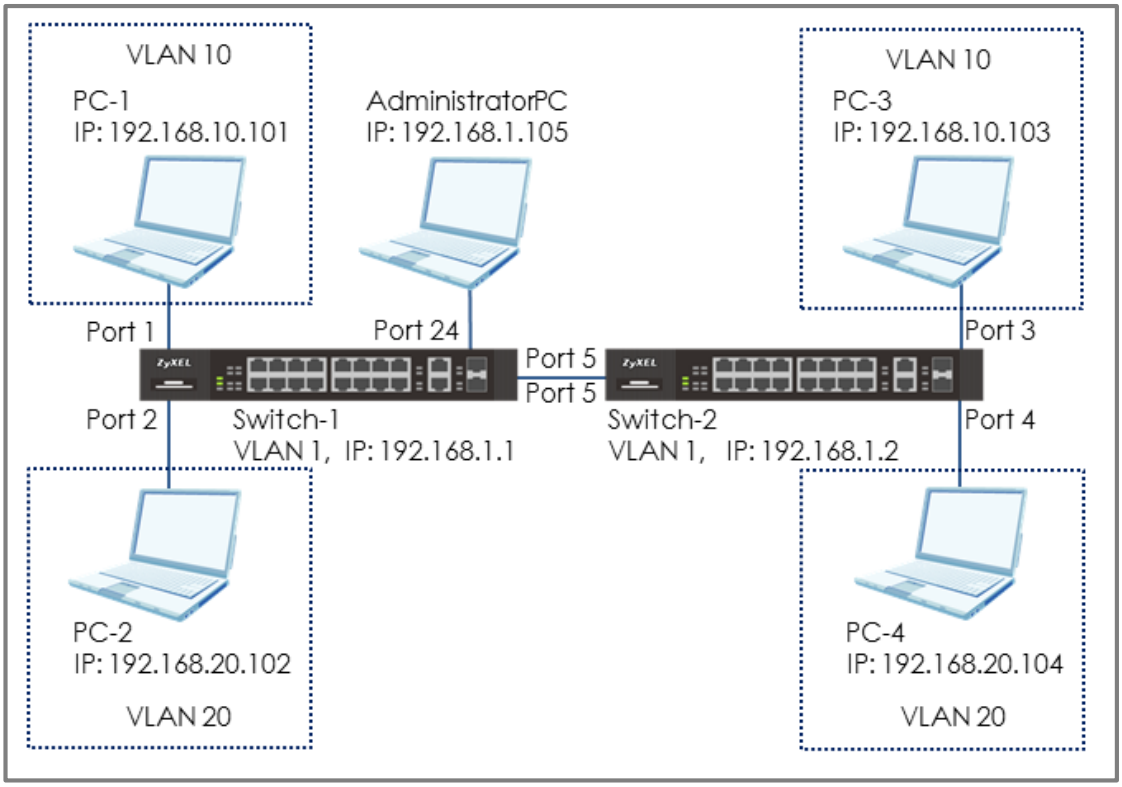
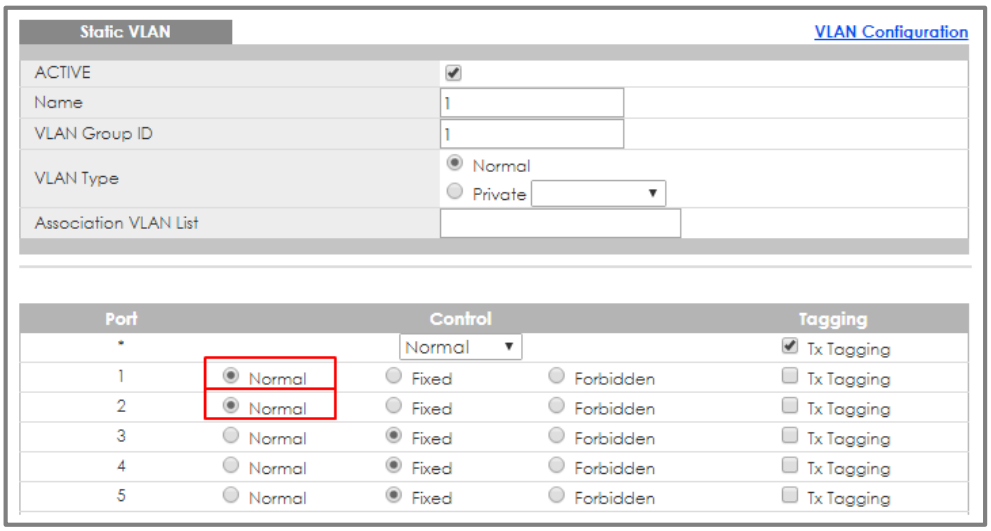


Figure 9 Set up VLAN to separate the traffic between departments

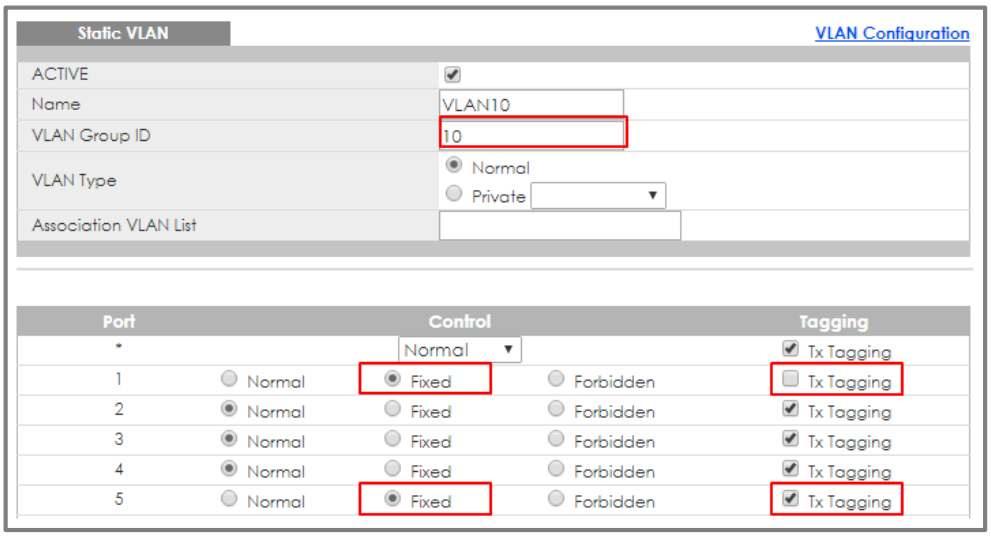
Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks.

2.1.1 Configure Switch-1

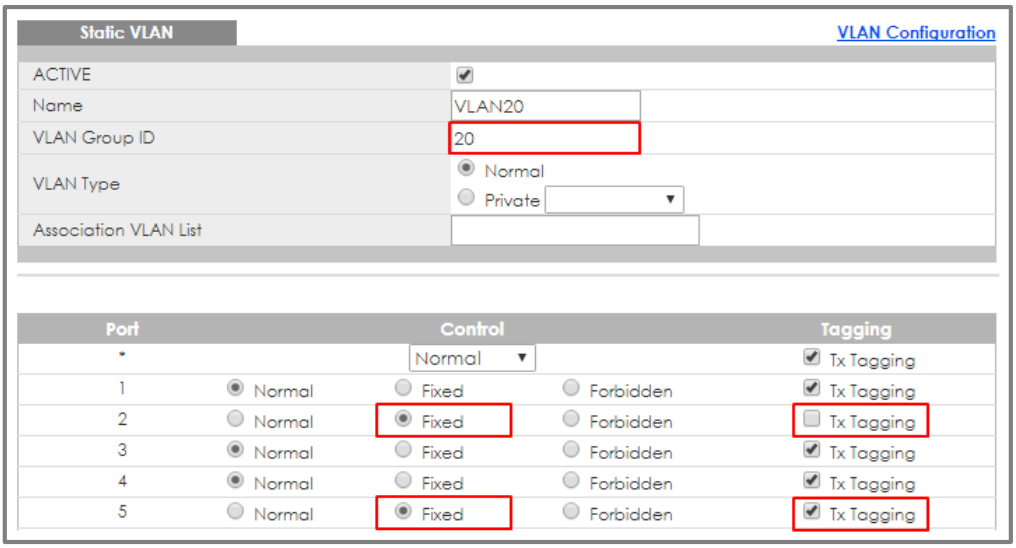
1 Use Administrator PC to set **VLAN 1** in **Switch-1**: Port 1, 2 as **Normal** port. (Prevent VLAN 1 broadcast packets to port 1, 2). Enter the web GUI and go to **Menu > Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup > VID > 1**. Select port 1, 2 as **Normal**. Click "**Add**".



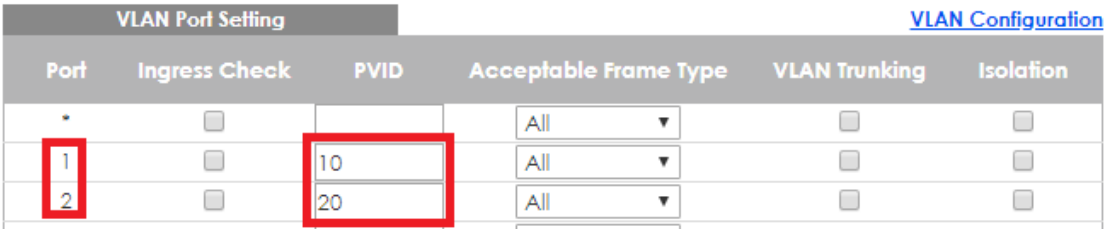
2 Use Administrator PC to create **VLAN 10** in **Switch-1**: Enter the web GUI and go to **Menu > Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup**. Check the "ACTIVE" box. Type the Name and VLAN Group ID=**10**. Select port **1**, **5** as **Fixed** and uncheck Tx Tagging (**Untagged**)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



3 Use Administrator PC to create **VLAN 20** in **Switch-1**: Enter the web GUI and go to **Menu > Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup**. Check the "ACTIVE" box. Type the Name and VLAN Group ID=**20**. Select port 2, 5 as Fixed and uncheck Tx Tagging (**Untagged**) on port **2** and check Tx Tagging (**tagged**) on port **5**. Click "**Apply**".

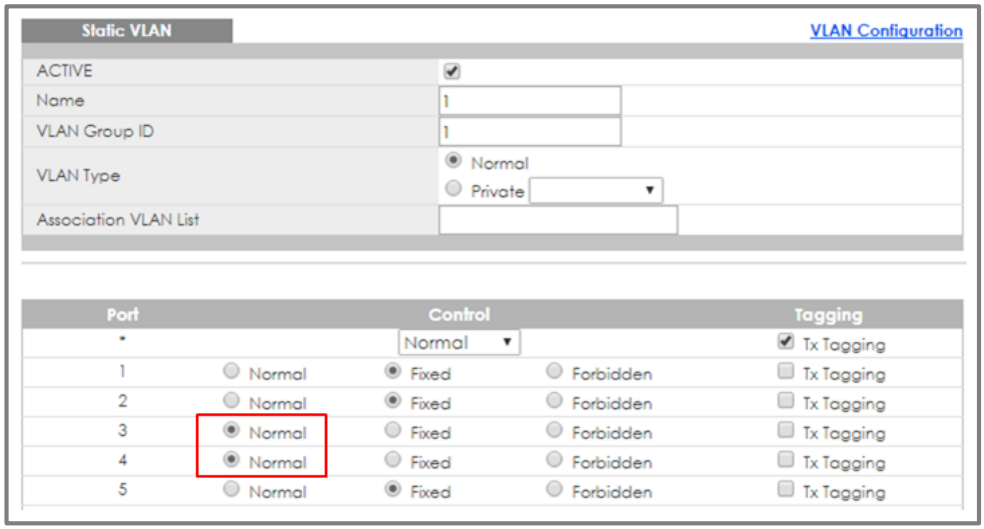


4 Set the PVID on **Switch-1**: Go to **Menu > Advanced Application > VLAN > VLAN Configuration > VLAN Port Setup**. Set port 1 as PVID=**10** (VLAN 10) and port 2 as PVID=**20** (VLAN 20).

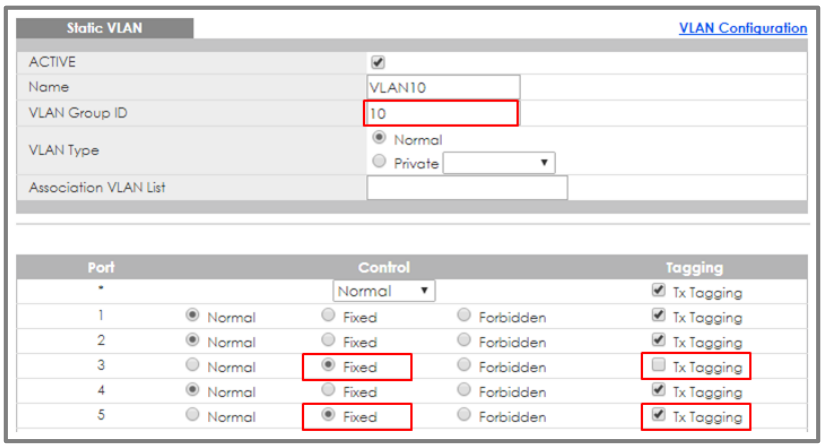


2.1.2 Configure Switch-2

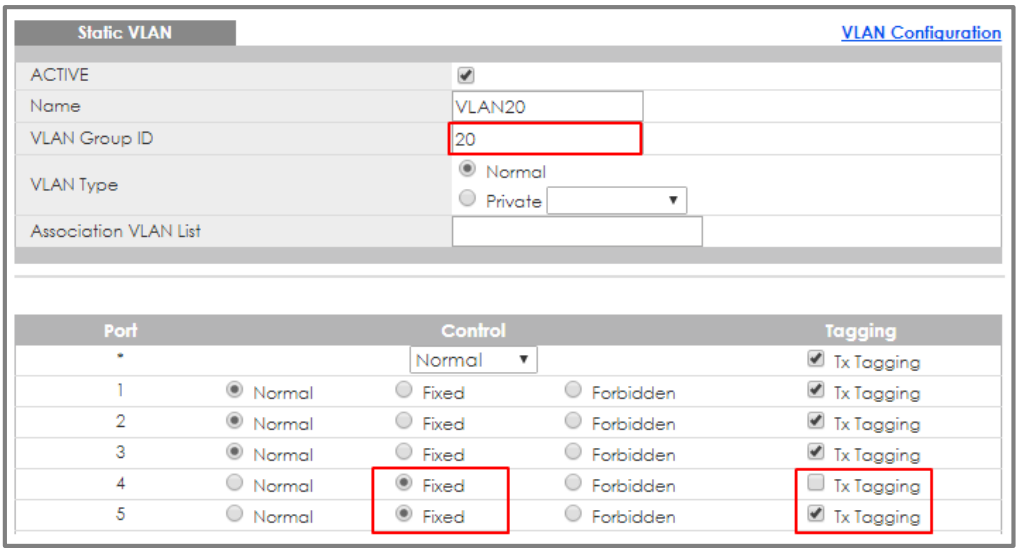
1 Use Administrator PC to set **VLAN 1** in **Switch-2**: Port 3, 4 as **Normal** port (this prevents VLAN 1 from broadcasting packets to port 3, 4). Enter the web GUI and go to **Menu > Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup > VID > 1**. Select port 3, 4 as **Normal**.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



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



3 Use Administrator PC to create VLAN 20 in **Switch-2**. Enter the web GUI and go to **Menu > Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup**. Check the "ACTIVE" box. Type the Name and VLAN Group ID=**20**. Select port 4, 5 as **Fixed** and uncheck Tx Tagging (**Untagged**) on port 4 and check Tx Tagging (**tagged**) on port 5. Click "**Apply**".



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

VLAN Port Setting — VLAN Configuration

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

2.1.3 Test the Result

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

```
C:\Users\User>ping 192.168.10.103 -t

Pinging 192.168.10.103 with 32 bytes of data:
Reply from 192.168.10.103: bytes=32 time<1ms TTL=128
Reply from 192.168.10.103: bytes=32 time<1ms TTL=128
Reply from 192.168.10.103: bytes=32 time<1ms TTL=128
```

```
C:\Users\User>ping 192.168.20.102

Pinging 192.168.20.102 with 32 bytes of data:
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.
```

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

```
C:\Users\User>ping 192.168.20.104 -t

Pinging 192.168.20.104 with 32 bytes of data:
Reply from 192.168.20.104: bytes=32 time<1ms TTL=128
Reply from 192.168.20.104: bytes=32 time<1ms TTL=128
Reply from 192.168.20.104: bytes=32 time<1ms TTL=128
```

```
C:\Users\User>ping 192.168.10.103

Pinging 192.168.10.103 with 32 bytes of data:
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.
```

Improving Network Reliability

3.1 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.

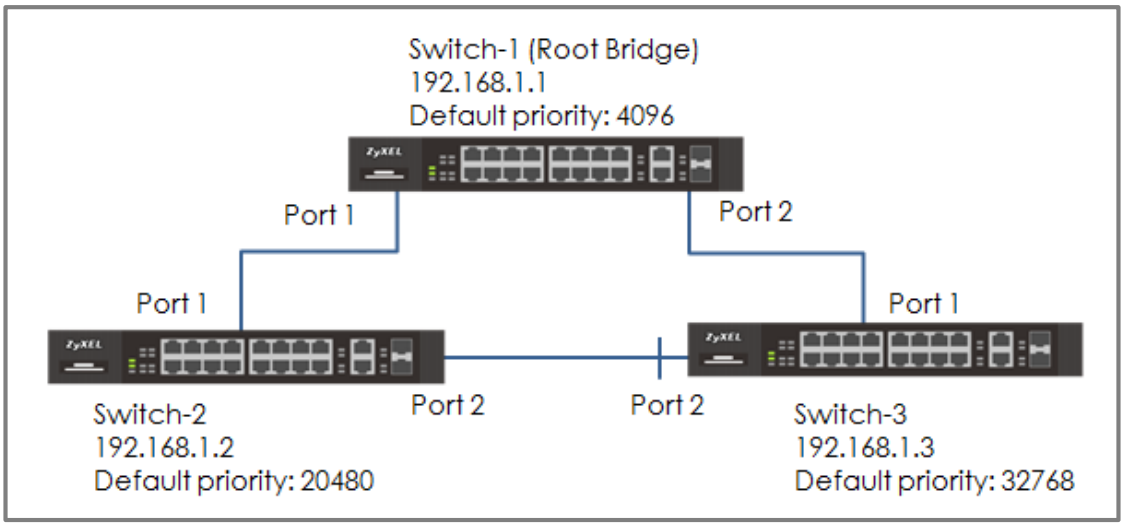


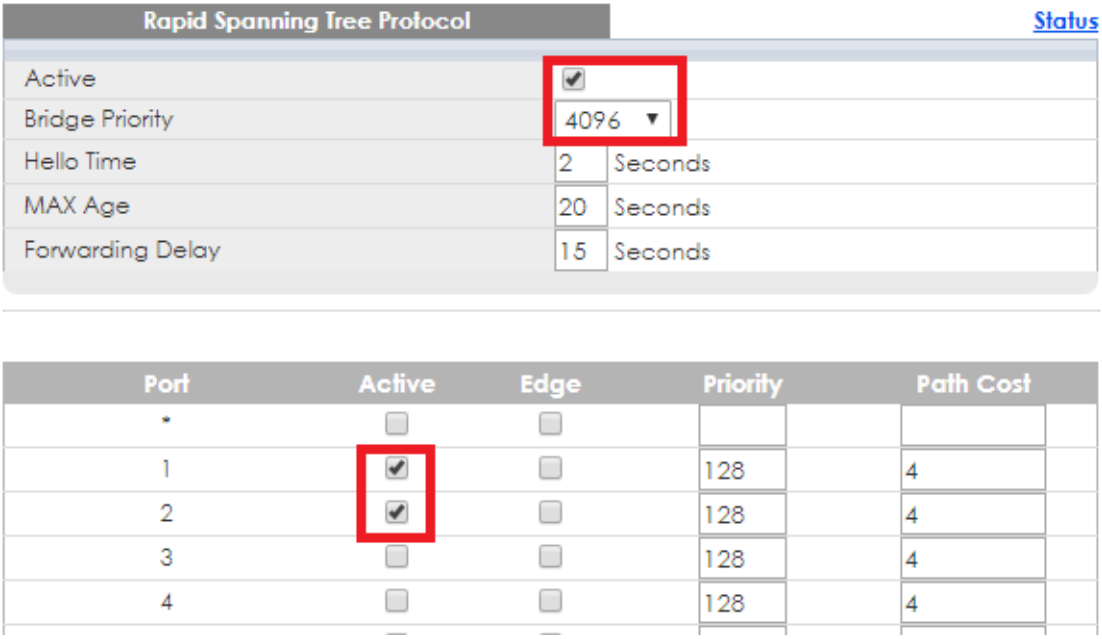
Figure 13 Configure RSTP in a ring topology

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.

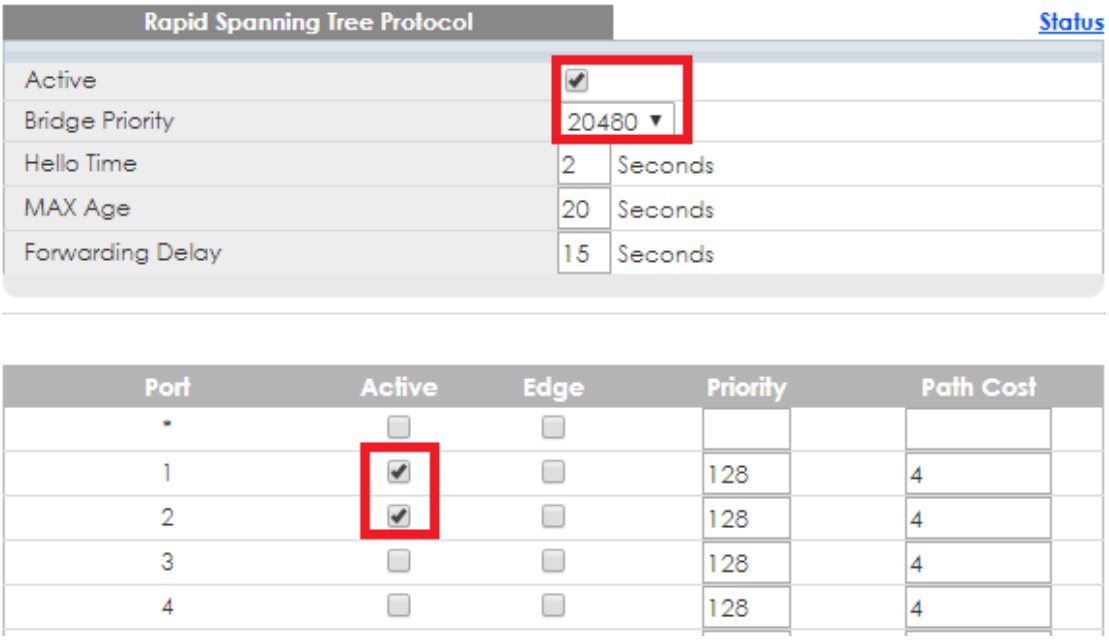
3.1.1 Configure Switch

1 Make sure that the link between **Switch-2** and **Switch-3** is not connected to prevent unintended loops before finishing the RSTP setup.

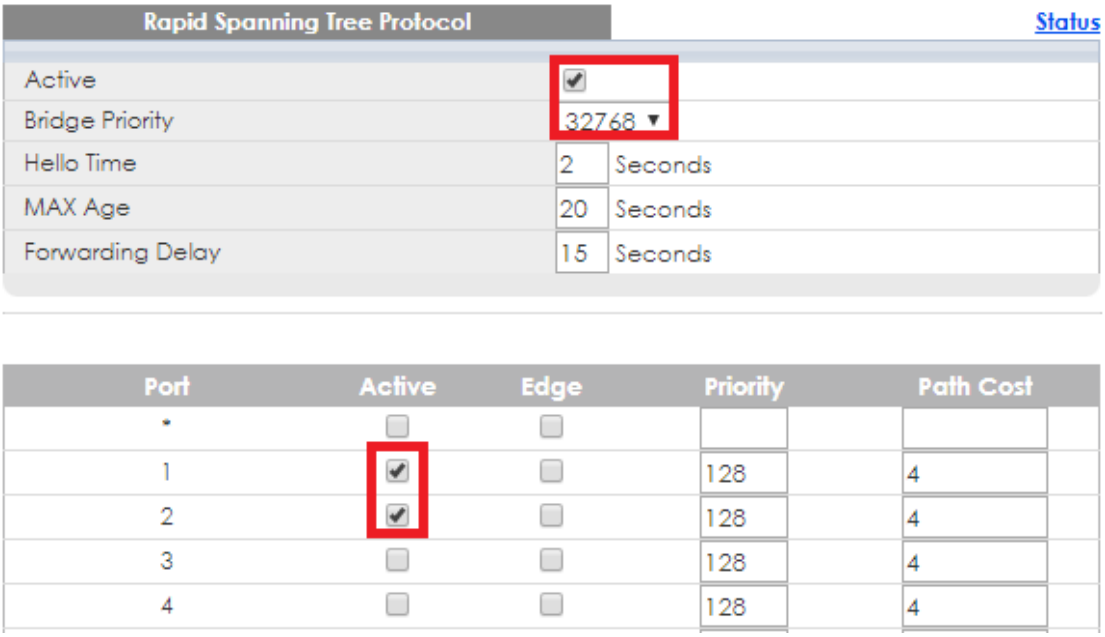
2 Set up **Switch-1**: Enter the web GUI. Go to **Menu > Advanced Application > Spanning Tree Protocol > RSTP**. Check the "**Active**" box. Set the Bridge Priority = **4096**. Active port **1**, **2**. Click "**Apply**".



3 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**".



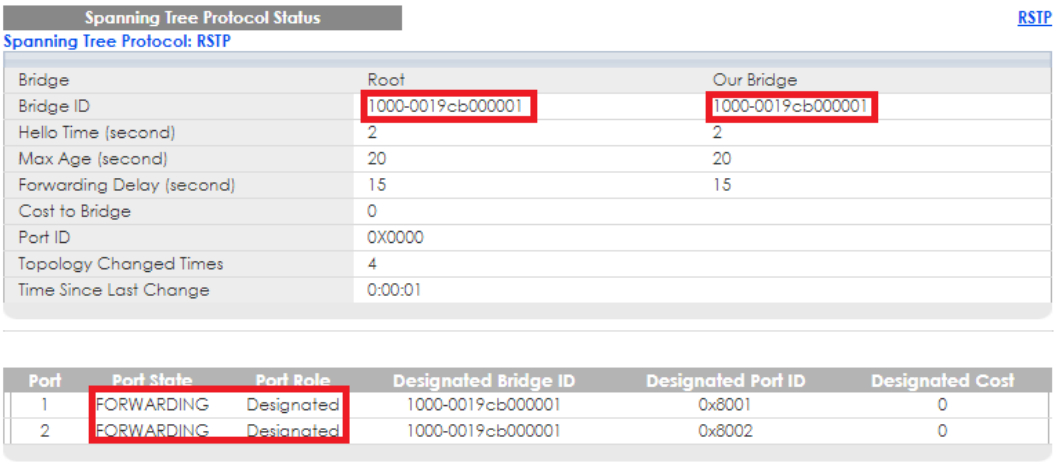
4 Set up **Switch-3**: Enter the web GUI. Go to **Menu > Advanced Application > Spanning Tree Protocol > RSTP**. Check the "**Active**" box. Set the Bridge Priority = **32768**. Active port **1**, **2**. Click "**Apply**".



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

3.1.2 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**.



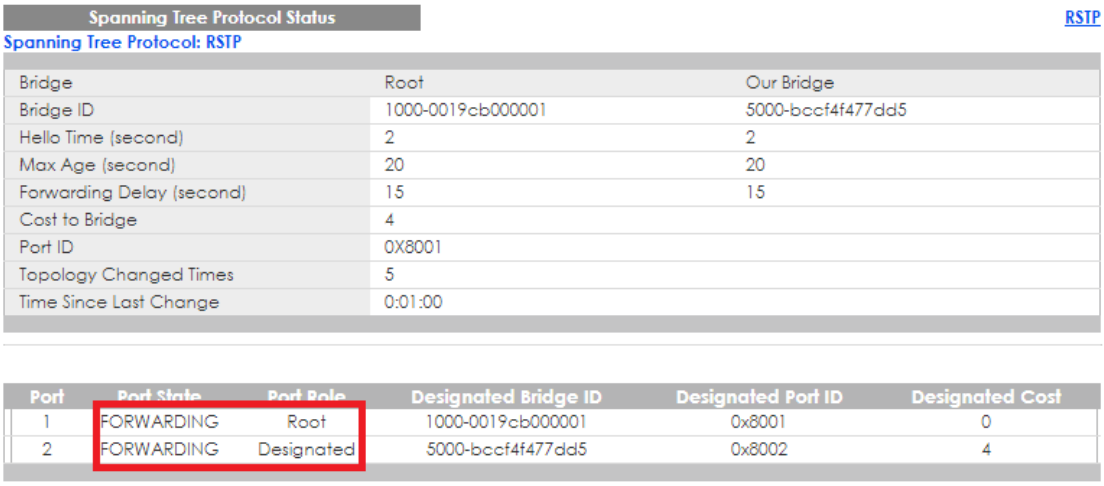
Spanning Tree Protocol Status — RSTP

Spanning Tree Protocol: RSTP

Bridge	Root	Our Bridge
Bridge ID	1000-0019cb000001	1000-0019cb000001
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	4	
Time Since Last Change	0:00:01	

Port	Port State	Port Role	Designated Bridge ID	Designated Port ID	Designated Cost
1	FORWARDING	Designated	1000-0019cb000001	0x8001	0
2	FORWARDING	Designated	1000-0019cb000001	0x8002	0

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.



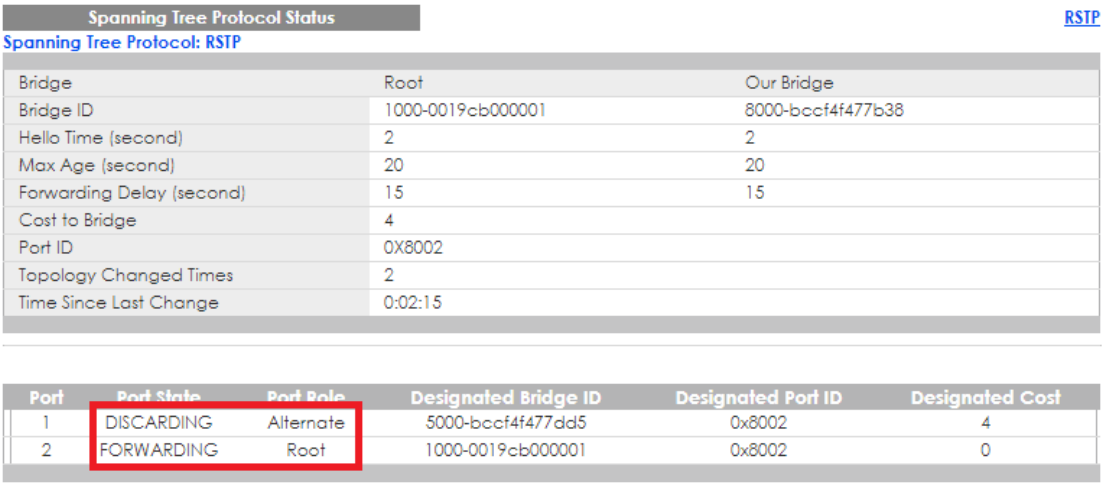
Spanning Tree Protocol Status — RSTP

Spanning Tree Protocol: RSTP

Bridge	Root	Our Bridge
Bridge ID	1000-0019cb000001	5000-bccf4f477dd5
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	5	
Time Since Last Change	0:01:00	

Port	Port State	Port Role	Designated Bridge ID	Designated Port ID	Designated Cost
1	FORWARDING	Root	1000-0019cb000001	0x8001	0
2	FORWARDING	Designated	5000-bccf4f477dd5	0x8002	4

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 — RSTP

Spanning Tree Protocol: RSTP

Bridge	Root	Our Bridge
Bridge ID	1000-0019cb000001	8000-bccf4f477b38
Hello Time (second)	2	2
Max Age (second)	20	20
Forwarding Delay (second)	15	15
Cost to Bridge	4	
Port ID	0X8002	
Topology Changed Times	2	
Time Since Last Change	0:02:15	

Port	Port State	Port Role	Designated Bridge ID	Designated Port ID	Designated Cost
1	DISCARDING	Alternate	5000-bccf4f477dd5	0x8002	4
2	FORWARDING	Root	1000-0019cb000001	0x8002	0

3.1.3 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.

3.2 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.

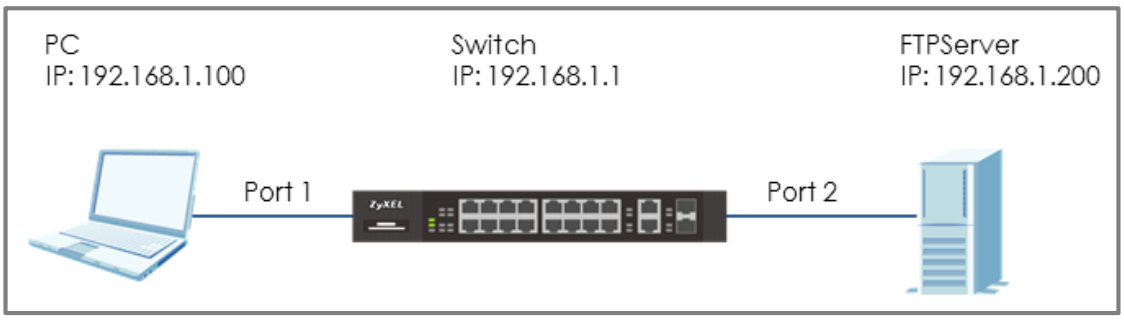
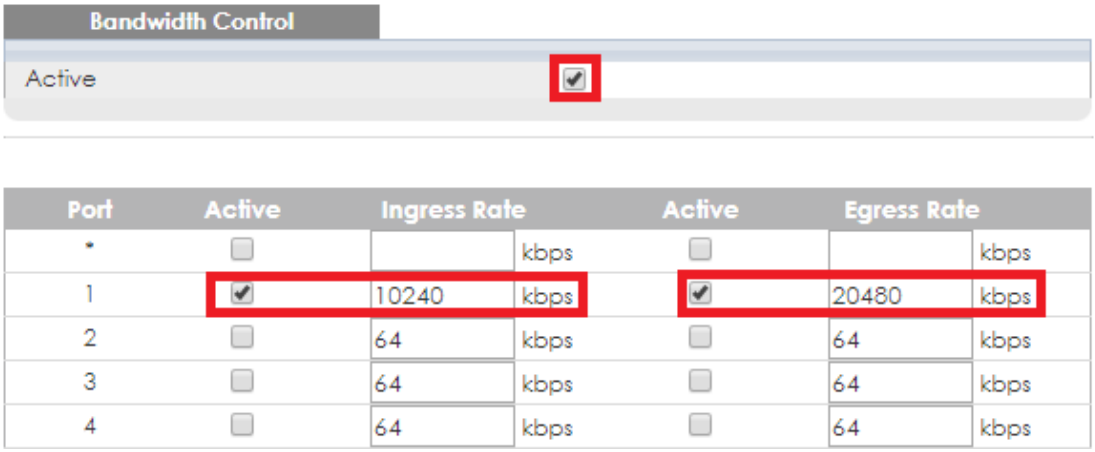


Figure 15 Configure bandwidth control to limit the traffic rate

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.

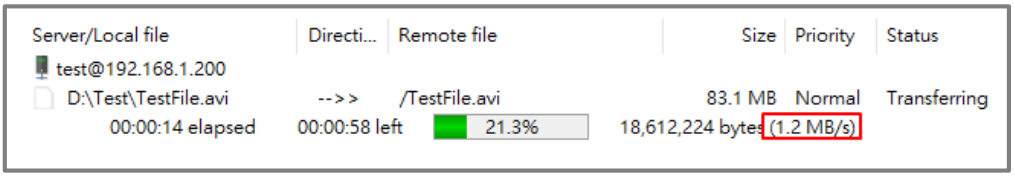
3.2.1 Configure Switch

1 Enter the web GUI. Go to **Menu > Advanced Application > Bandwidth Control**. Check the "**Active**" box. Key in the rate in **Ingress Rate** (PC **Upload rate**) = **10240 kbps** and **Egress Rate** (PC **Download rate**) = **20480 kbps**. Remember to check the port "**Active**" boxes as well. Click "**Apply**".

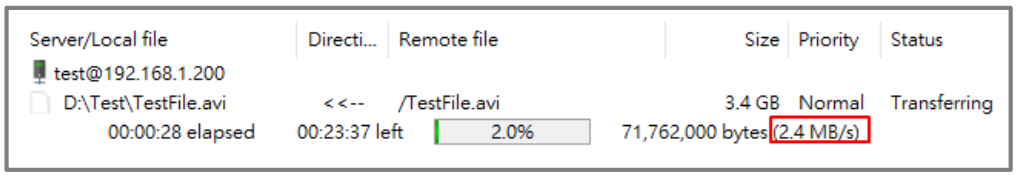


3.2.2 Test the Result

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



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



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 Snooping for multicast clients in the same LAN

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

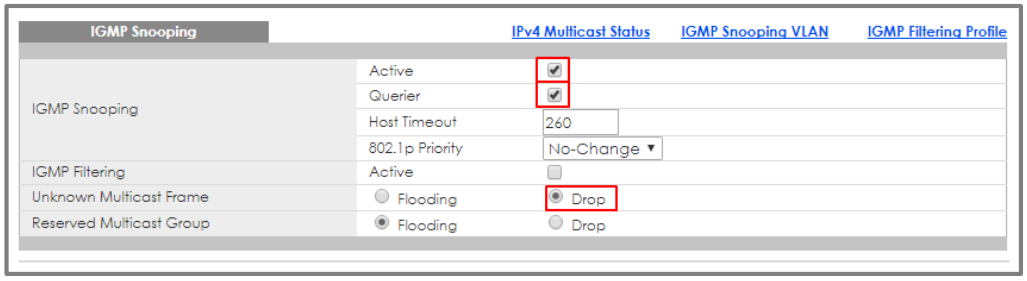
Figure 18 Configure IGMP Snooping for multicast clients in the same LAN

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.

4.2.1 Configure Switch

1 Configure the VLAN 10 on Switch. (Please refer to the topic: **2.1 How to configure the switch to separate traffic between departments**).

2 Configure the IGMP Snooping: Enter the web GUI and go to **Menu > Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping**. Check the "Active" box and select Unknown Multicast Frame as **Drop**. Check **Querier**. Click "Apply".

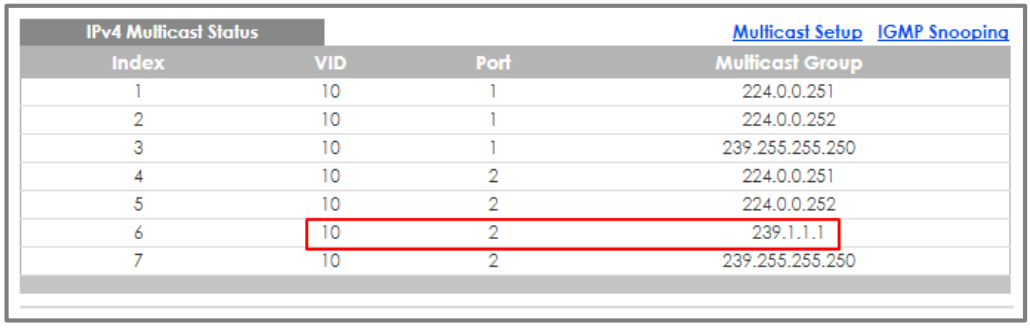


4.2.2 Test the Result

1 Play the stream on Media Server using Multicast IP address 239.1.1.1.

2 Have PC send an IGMP join message for 239.1.1.1.

3 Go to **Menu > Advanced Application > Multicast > IPv4 Multicast**. PC connected to port 2 joins Multicast Group-239.1.1.1.



Network Security

5.1 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.

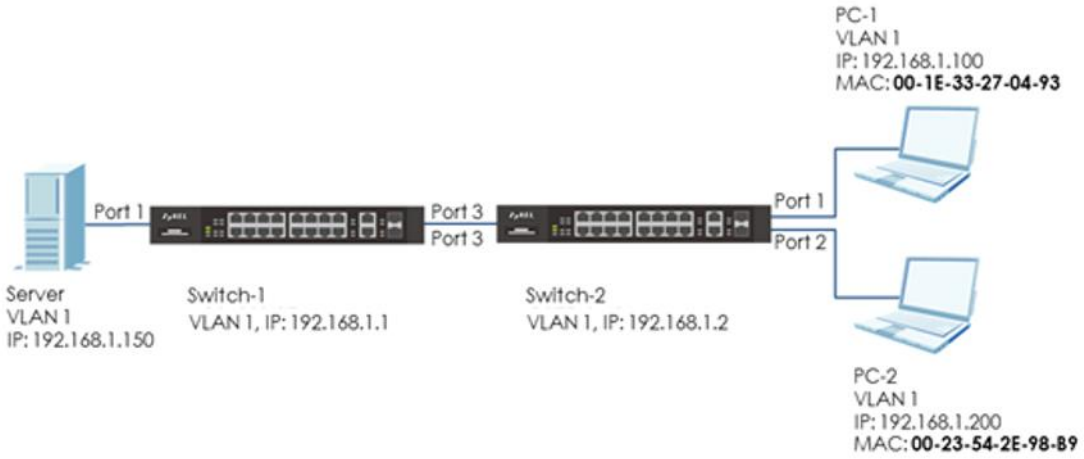
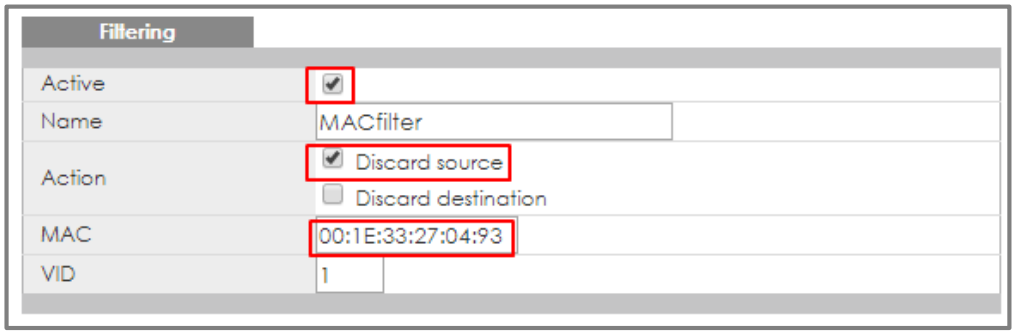


Figure 20 Configure MAC filter to block unwanted traffic

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.

5.1.1 Configure Switch-1

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



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

5.1.2 Test the Result

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

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

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

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

2 PC-2 can ping Server successfully.

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

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

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

5.1.3 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.

5.2 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.

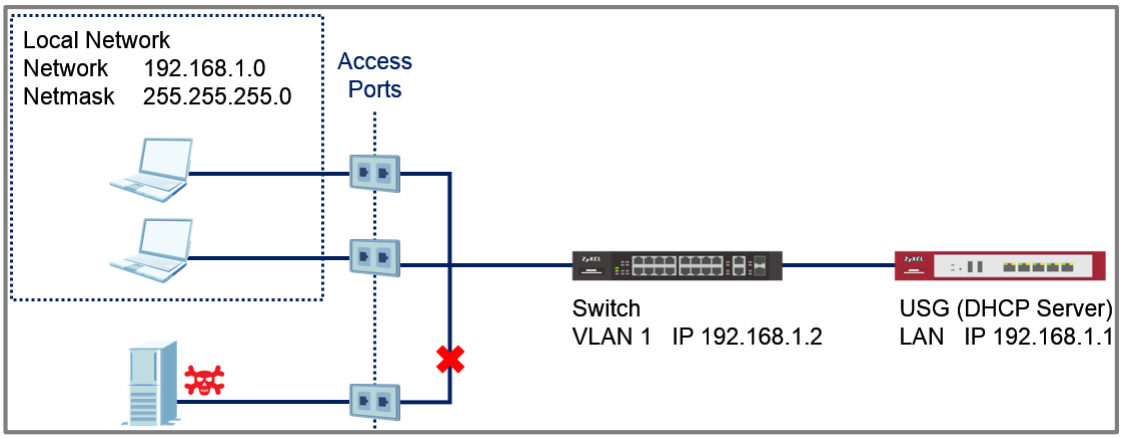


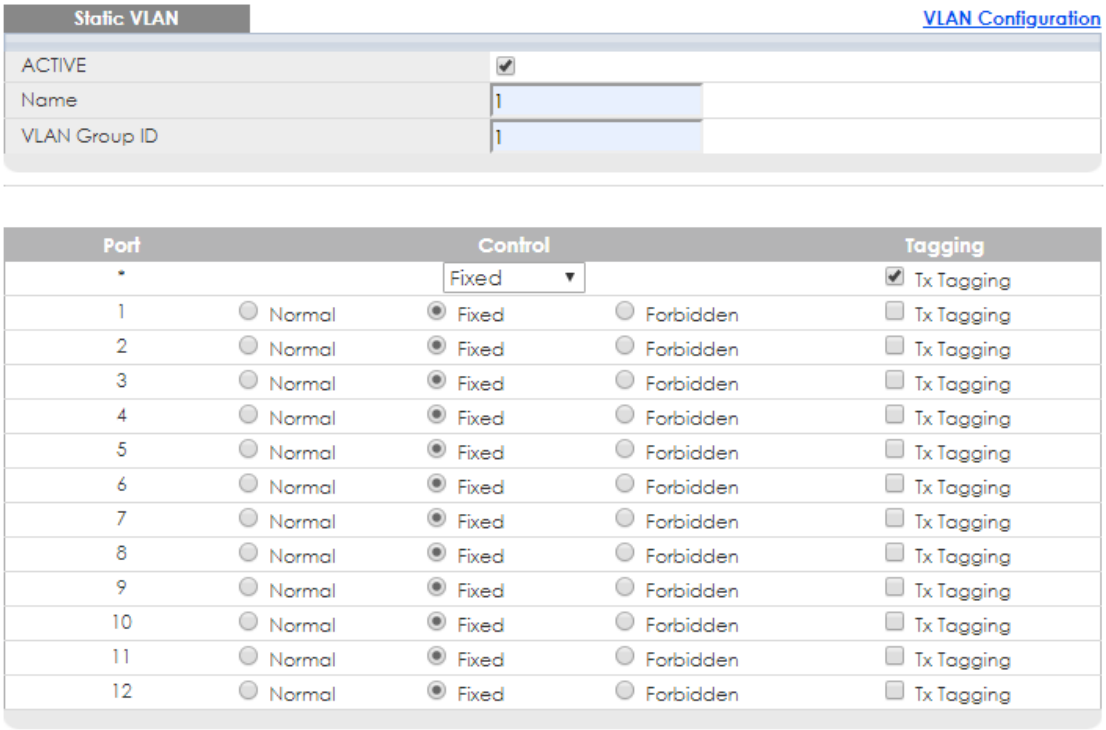
Figure 26 Fake DHCP Server Connected through Publicly Accessible Ports

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.

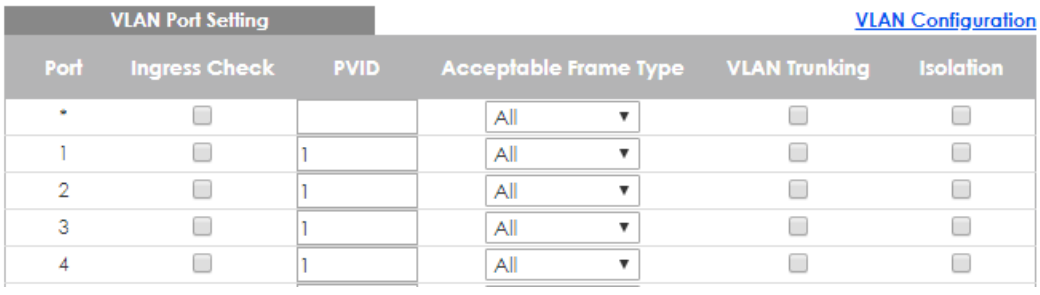
5.2.1 Configuration in the Switch

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

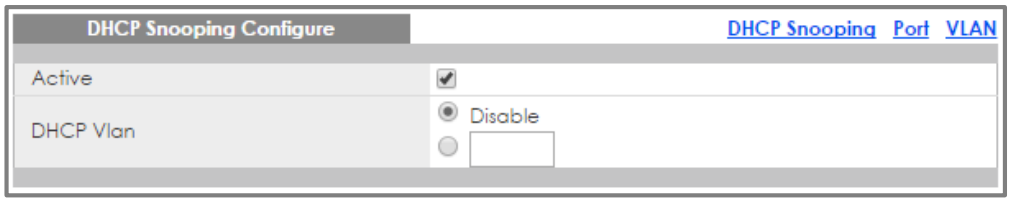
2 Go to **Advance Application > VLAN > VLAN Configuration > Static VLAN Setup**. For this example, all traffic entering access ports are sent to VLAN 1. VLAN 1 should be fixed and untagged for all access ports. Click **Add**.



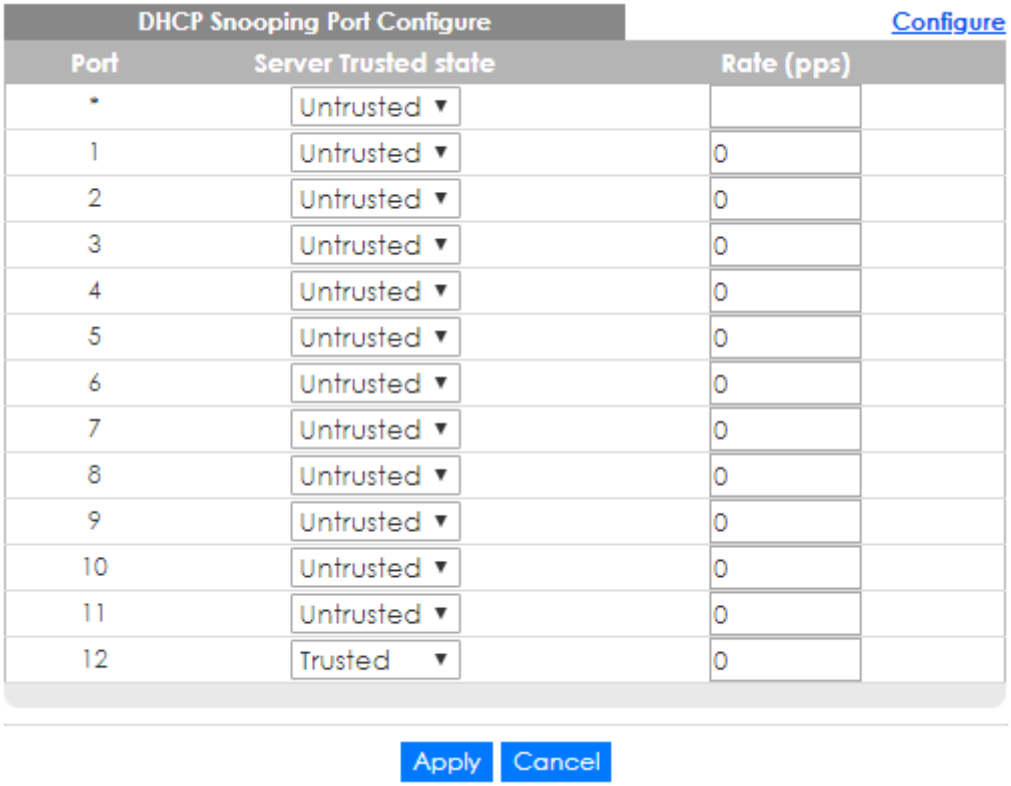
3 Go to **Advance Application > VLAN > VLAN Configuration > VLAN Port Setup**. Configure all access ports with PVID 1. Click **Apply**.



4 Go to **Advance Application > DHCP Snooping > Configure**. Check the Active box under DHCP Snooping Configure. Click **Apply**.

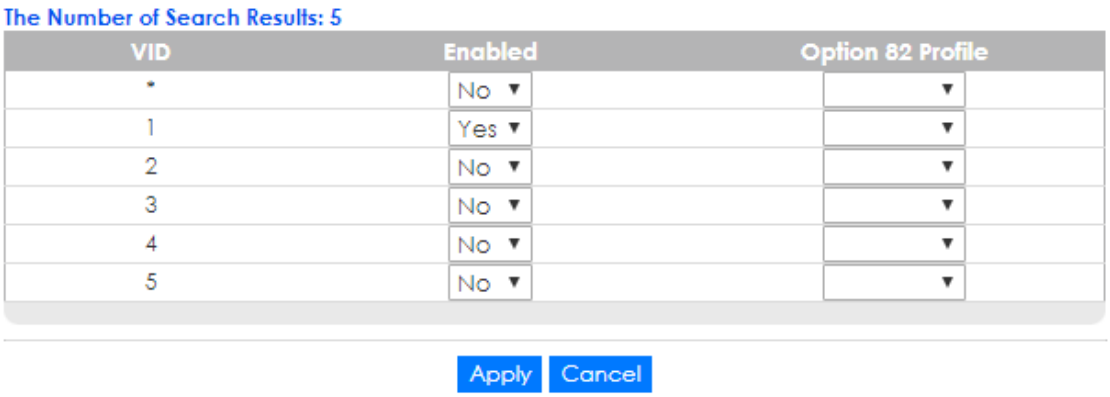


5 Go to **Advance Application > DHCP Snooping > Configure > Port**. Set all access ports as untrusted ports. Ports to the USG or other network components should be trusted ports. Click **Apply**.



6 Go to **Advance Application > DHCP Snooping > Configure > VLAN**. Input the VID and make sure that the PVID of the access ports are included in this range. Click **Apply**.

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



5.2.2 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.

5.2.3 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 > 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 > 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 > DHCP Snooping > Configure > Port**.
   b. Make sure that both redundant ports are trusted ports in **Advance Application > DHCP Snooping > Configure > Port** when using a ring topology.

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.

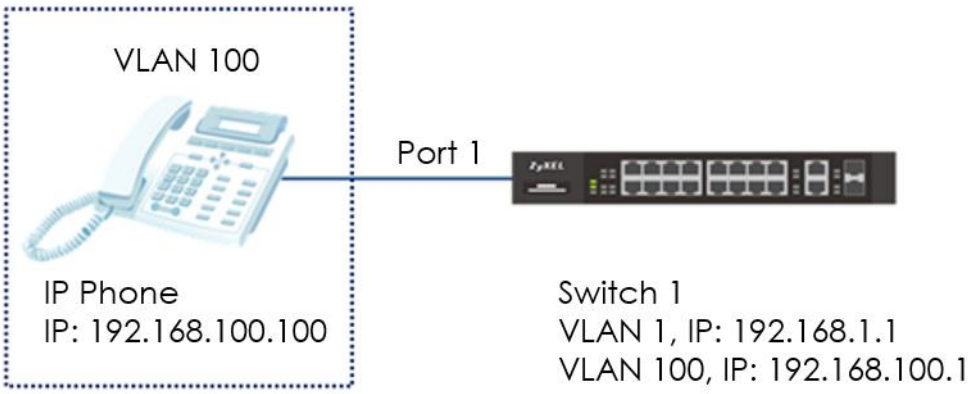


Figure 23 Configure LLDP-MED to assign an IP Phone's VLAN

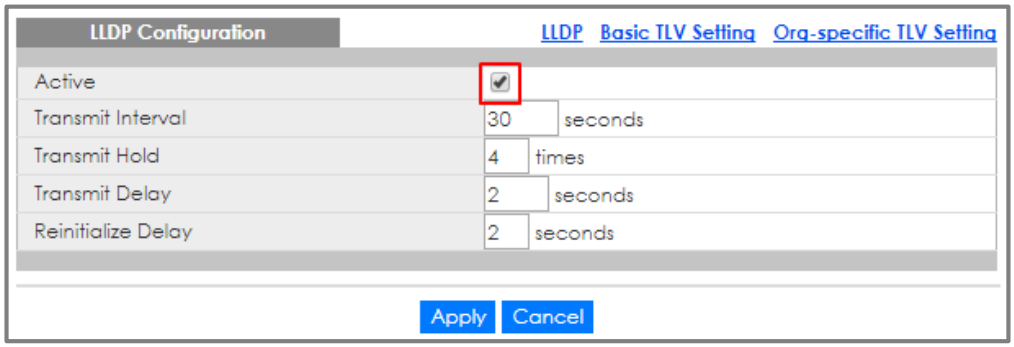
Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks.

6.1.1 Configure VLAN for IP Phone

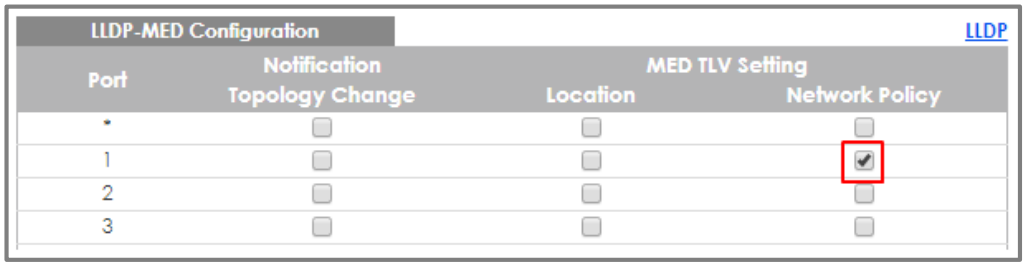
1 Configure VLAN 100 on Switch (Please refer to the topic: **2.1 How to configure the switch to separate traffic between departments**). VLAN 100 is created for the IP Phone.

6.1.2 Configure Switch

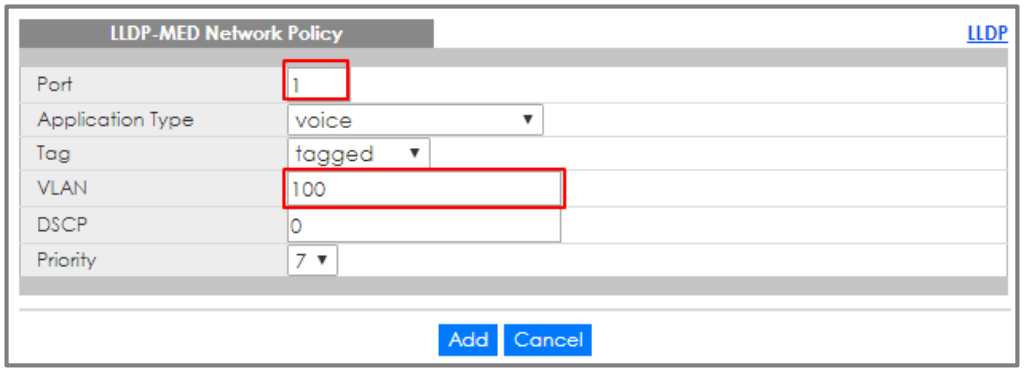
1 Enter the web GUI and go to **Menu > Advanced Application > LLDP > LLDP Configuration**. Make sure that the LLDP configuration is active.



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

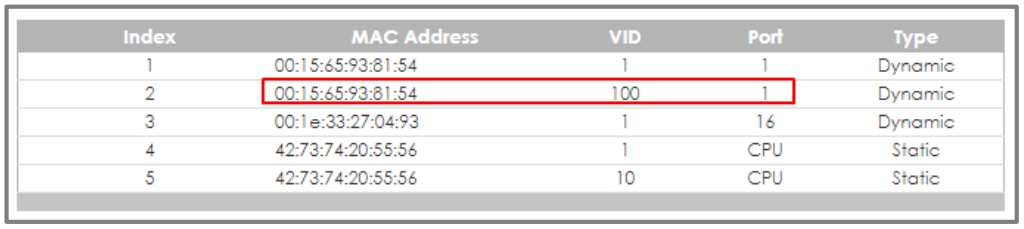


3 Enter the web GUI and go to **Menu > Advanced Application > LLDP > LLDP-MED Network Policy**. Key in the port number as 1 and the VLAN we want to assign the IP Phone to (VLAN 100) and leave DSCP as "0". We can also set the Priority. Click "Add".



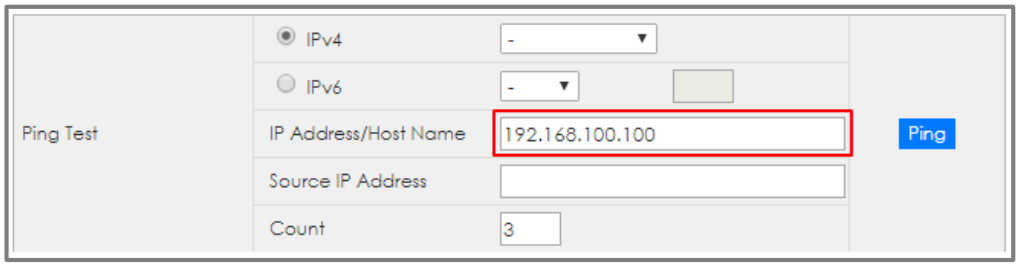
6.1.3 Test the Result

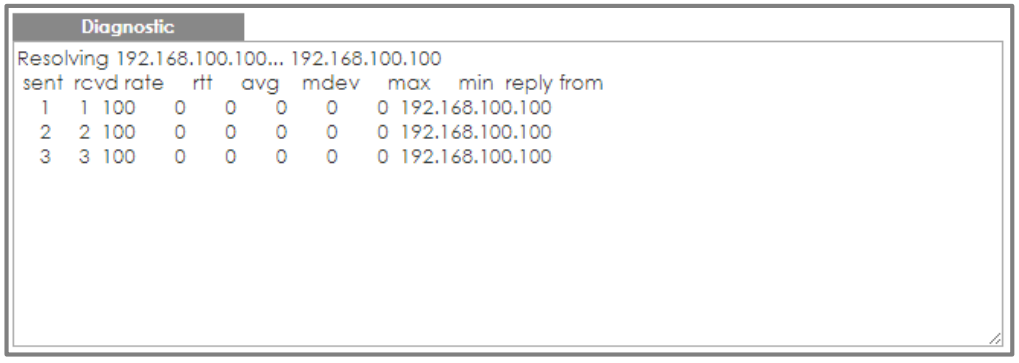
1 Go to **Menu > Management > MAC Table > Search.** Check the MAC table. The IP Phone's MAC address should be in VLAN 100.



Index	MAC Address	VID	Port	Type
1	00:15:65:93:81:54	1	1	Dynamic
2	00:15:65:93:81:54	100	1	Dynamic
3	00:1e:33:27:04:93	1	16	Dynamic
4	42:73:74:20:55:56	1	CPU	Static
5	42:73:74:20:55:56	10	CPU	Static

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





6.1.4 What Could Go Wrong

1 If the MAC address of the IP Phone is not assigned to the VLAN 100 successfully, please check if the IP Phone supports LLDP-MED. LLDP-MED must be enabled on the switch.

2 Since the IP Phone is assigned a VLAN ID via the function of the **Network Policy** in LLDP-MED, The voice traffic from the switch must be tagged backed to the IP Phone. Port 1 in VLAN 100 on the Switch should be **tagged out** (Check TX tagging) so that the Switch can ping the IP Phone successfully.

3 Since the IP Phone is assigned a VLAN ID via the function of the **Network Policy** in LLDP-MED, please make sure the IP Phone either supports LLDP-MED, or has LLDP-MED enabled.

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

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

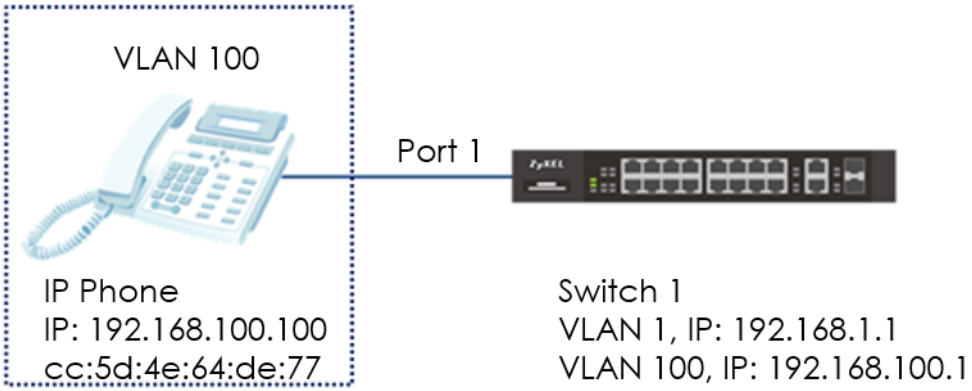


Figure 24 Configure Voice VLAN to separate VOIP traffic from data traffic

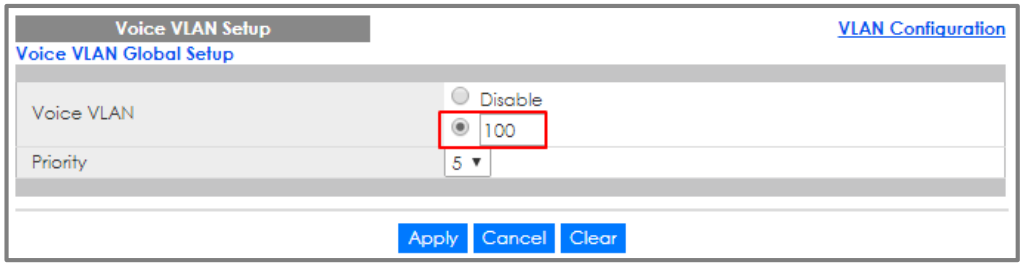
Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks.

6.2.1 Configure VLAN 100 for IP Phone

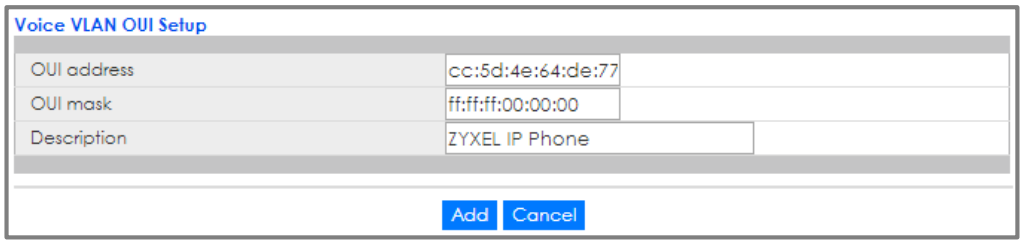
1 Configure VLAN 100 on Switch (Please refer to the topic: **2.1 How to configure the switch to separate traffic between departments**). VLAN 100 is created as the Voice VLAN for the IP Phone.

6.2.2 Configure Voice VLAN

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



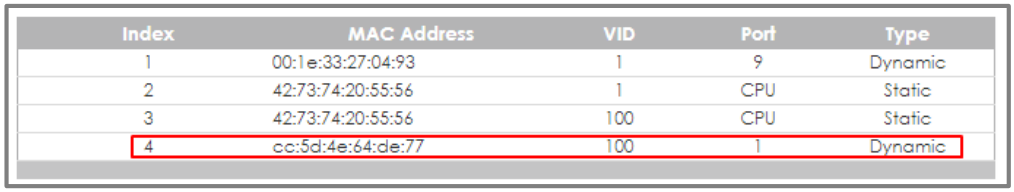
2 Configure the OUI Setup: Enter the web GUI and go to: **Menu > Advanced Application > VLAN > VLAN Configuration > Voice VLAN Setup**. Set the OUI address. (You can key in the MAC address.) In this example, it is cc:5d:4e:64:de:77. Set up the OUI mask as **ff:ff:ff**:00:00:00. Click "Add".



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

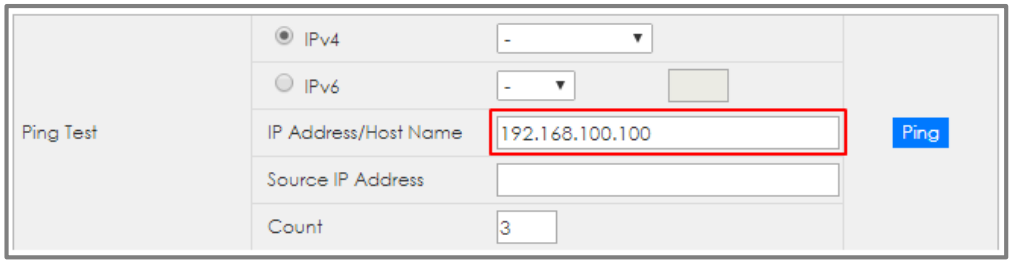
6.2.3 Test the Result

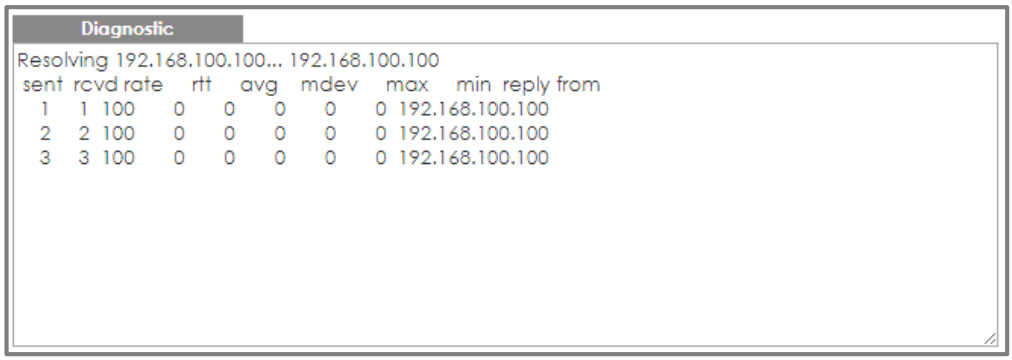
1 Go to **Menu > Management > MAC Table > Search.** Check the MAC address table. The IP Phone is assigned to VLAN 100.



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

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





6.2.4 What Could Go Wrong

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

2 Here are the expected behaviors of IP phones based on the different settings. If you find the behaviors of the IP Phone is not the same as your expectation, please refer below:

a. If the IP Phone is VLAN **enabled** and this VLAN is the same as **Voice VLAN**: The Switch will keep the Voice VLAN and assign the priority setting to the IP phone. The IP phone will only recognize the tagged traffic. In this case, port 1 in VLAN 100 on Switch should be set as **tagged out** (check the TX tagging box).

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

c. If the IP Phone is VLAN **disabled**: The Switch will assign the Voice VLAN and priority setting to the IP phone's VOIP traffic. This setting causes the IP Phone to only send and receive **untagged** traffic. In this case, port 1 in VLAN 100 on Switch should be set as **untagged out** (uncheck the TX tagging box).

6.3 How to configure the switch to improve Voice traffic quality

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

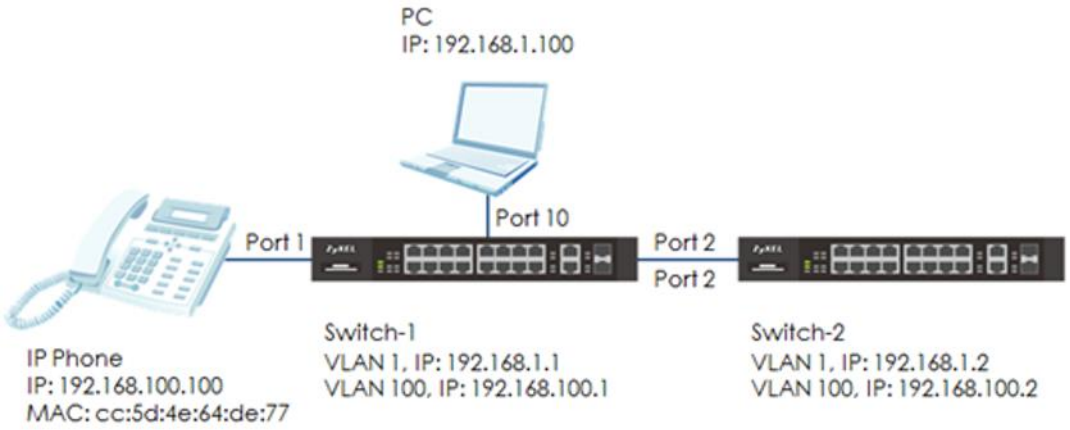


Figure 25 Configure Voice VLAN to separate VOIP traffic from data traffic

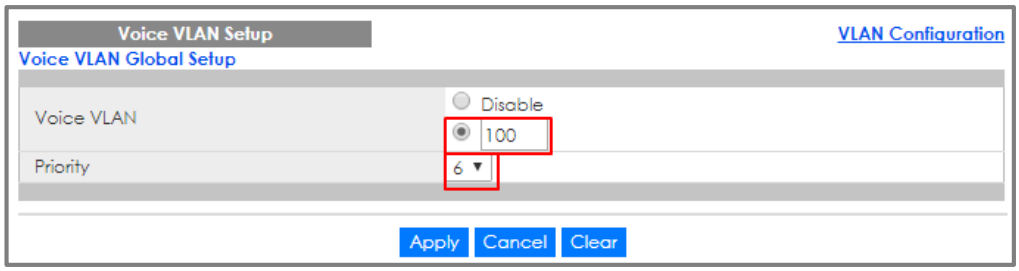
Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks.

6.3.1 Configure VLAN for voice traffic

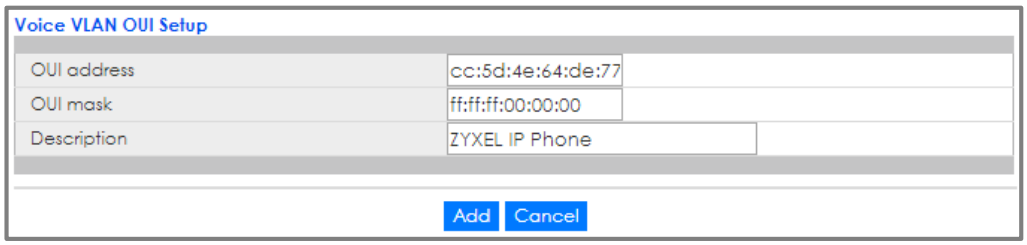
1 Configure VLAN 100 on Switch-1 and Switch-2. (Please refer to the topic: **2.1 How to configure the switch to separate traffic between departments**). VLAN 100 is created for the Voice VLAN. Make sure that devices in VLAN 100 can communicate across Switch-1 and Switch-2.

6.3.2 Configure Voice VLAN

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



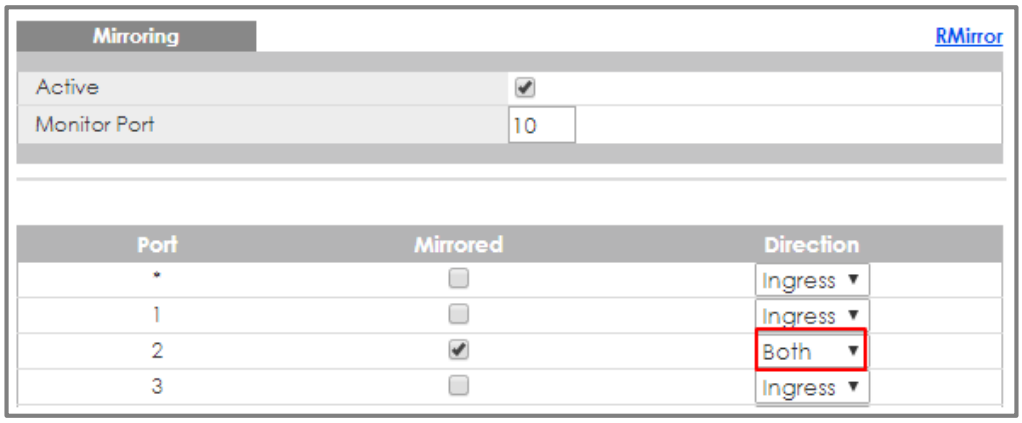
2 Configure the OUI Setup: Enter the web GUI and go to: **Menu > Advanced Application > VLAN > VLAN Configuration > Voice VLAN Setup**. Set the OUI address. (You can key in the MAC address.) In this example, it is cc:5d:4e:64:de:77. Set up the OUI mask as **ff:ff:ff**:00:00:00. Click "Add".



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

6.3.3 Configure Mirroring (For "Test the Result")

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

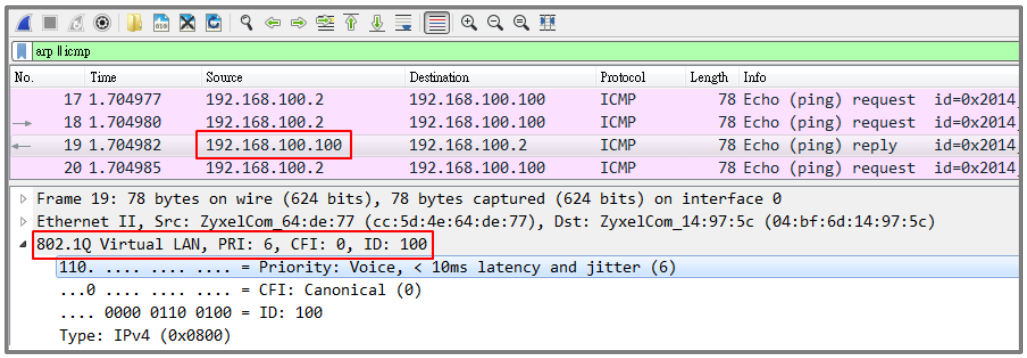


6.3.4 Test the Result

1 Connect the PC and Switch-1. Open **Wireshark** to monitor the packet. Filter "**arp || icmp**".

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

3 Check the packet from IP Phone (**192.168.100.100**) on Wireshark. The VLAN header should indicate the assigned Voice VLAN priority "6".



6.3.5 What Could Go Wrong

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

2 Here are the expected behaviors of IP phones based on the different settings. If you find the behaviors of the IP Phone is not the same as your expectation, please refer below:

a. If the IP Phone is VLAN **enabled** and this VLAN is the same as **Voice VLAN**: The Switch will keep the Voice VLAN and assign the priority setting to the IP phone. The IP phone will only recognize the tagged traffic. In this case, port 1 in VLAN 100 on Switch should be set as **tagged out** (check the TX tagging box).

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

c. If the IP Phone is VLAN **disabled**: The Switch will assign the Voice VLAN and priority setting to the IP phone's VOIP traffic. This setting causes the IP Phone to only send and receive **untagged** traffic. In this case, port 1 in VLAN 100 on Switch should be set as **untagged out** (uncheck the TX tagging box).

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

Surveillance Application

7.1 How to Apply Extended Range Mode on Zyxel Surveillance Switch

Traditionally, PoE switch delivers power and data within the distance of 100-meter limitation. If you want to deploy a power device for a longer distance, you have to add an extra PoE switch to extend the distance like the figure below (Figure.1). Therefore, you have to spend more money on it. Now, with the Zyxel surveillance switch GS1300/GS1350 series, you can fulfill the need to deploy your PD to a distant location and also reduce the expense.

If your PD is "**802.3af mode**" and is able to run with the "link speed **10 Mbps**", with the feature of extended range on Zyxel surveillance switch, you can simply deploy your power device with the distance at most 250 meters without extra PoE switch like the figure below (Figure. 2).

After enabling the extended range, the selected port on switch will enter forced 802.3at mode and the max power of output on the port will extend to 33 watts to compensate cable loss over long distance cabling. Furthermore, the link speed will be fixed to 10Mbps to guarantee data transmission over long distance operation. That's why the PD should be able to run with the link speed 10 Mbps.

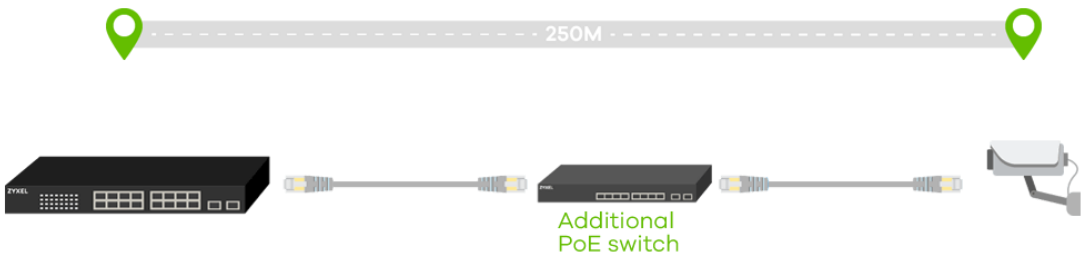


Figure 1

Figure 2

Below example will instruct the administrator on how to apply the extended range mode.

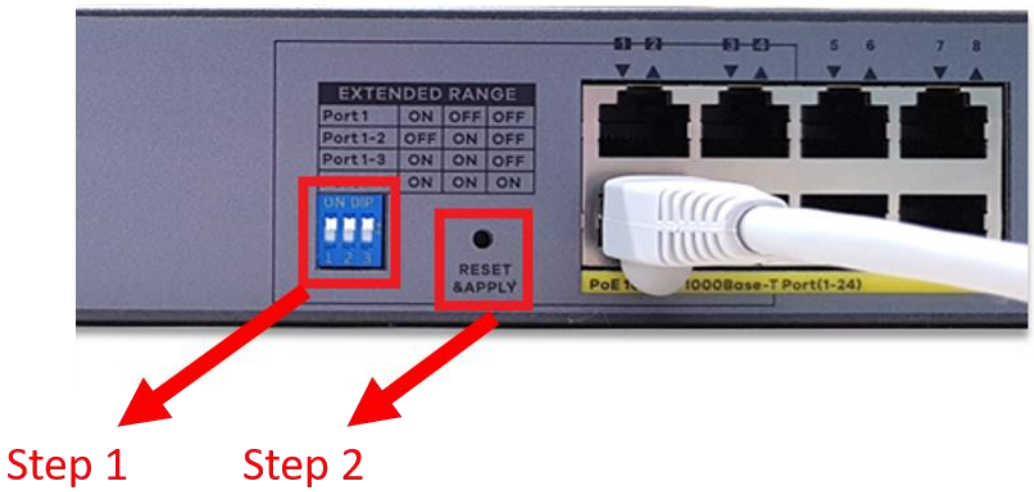
> Note:
> If PD can't link up at the distance of 250m, please try to shorten the distance to 200m or change a higher quality cable.

7.1.1 Configure Extended Range

GS1300 Series

1. Follow the instruction on the front panel and toggle the dip switches for the selected port.

2. Push the **RESET & APPLY** button to restart switch.

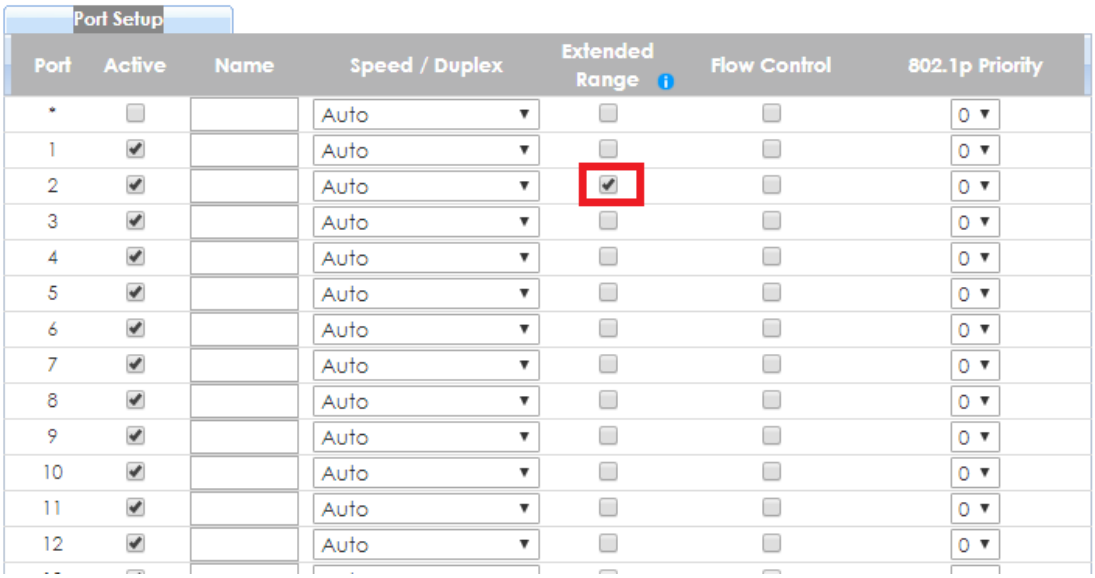


GS1350 Series

1. Access switch via Web GUI

2. Go to **Basic Setting > Port Setup**

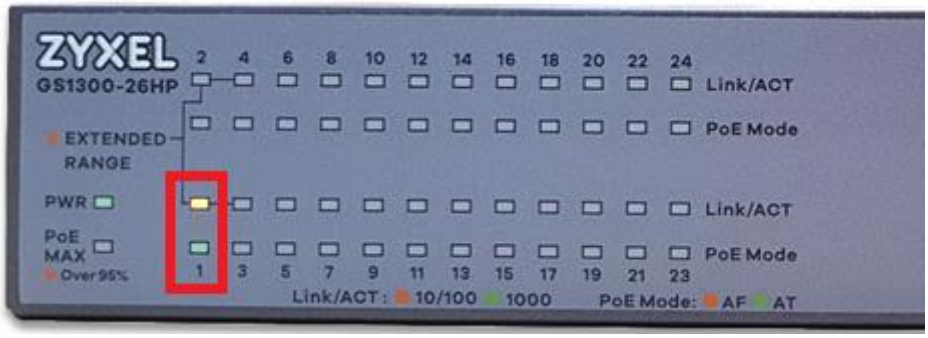
3. Select the port you would like to enable extended range



7.1.2 Test the result

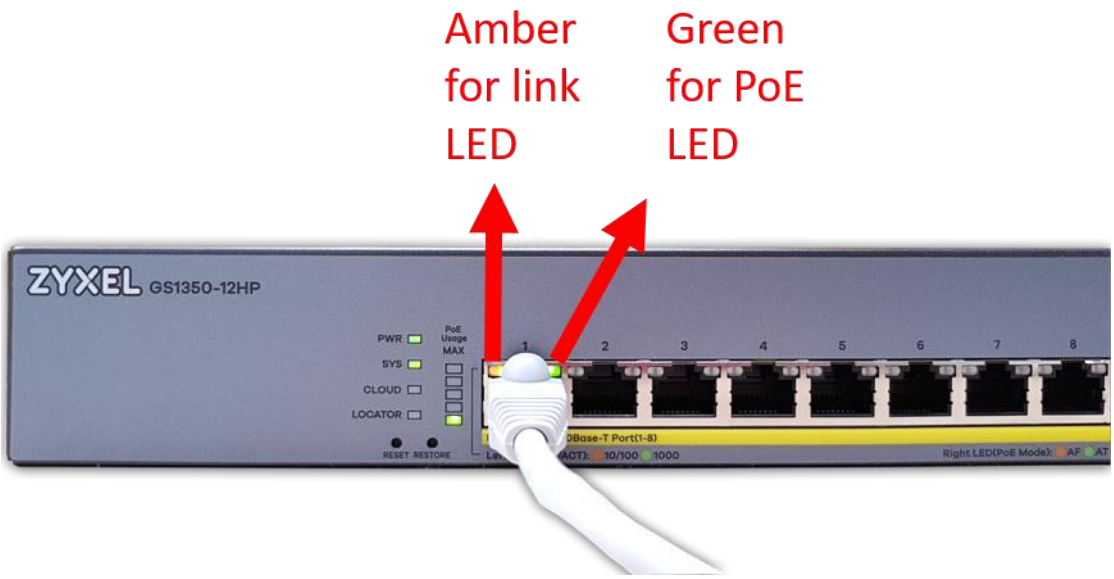
GS1300 Series

After enabling extended range successfully, the link LED will show "**amber**" for 10Mbps and the PoE LED will show "**green**" for 802.3at.



GS1350 Series

1. After enabling extended range successfully, the link LED will show "**amber**" for 10Mbps and the PoE LED will show "**green**" for 802.3at.



2. Check PoE status and you will find the Power-Up mode is fixed to 802.3at and the Max Power is 33 watts

PoE Status

PoE Time Range Setup | PoE Setup

PoE Mode	Consumption
Total Power (W)	375.0
Usage (%)	0
Consuming Power (W)	3.8
Allocated Power (W)	NA
Remaining Power (W)	371.2

Port	State	Class	PD Priority	Power-Up	Consuming Power (W)	Max Power (W)	Time-Range State
1	Enable	0	Low	802.3at	0.0	0.0	-
2	Enable	4	Low	802.3at	2.5	33.0	-
3	Enable	0	Low	802.3at	0.0	0.0	-
4	Enable	0	Low	802.3at	0.0	0.0	-
5	Enable	0	Low	802.3at	0.0	0.0	-
6	Enable	0	Low	802.3at	0.0	0.0	-
7	Enable	0	Low	802.3at	0.0	0.0	-
8	Enable	0	Low	802.3at	0.0	0.0	-
9	Enable	0	Low	802.3at	0.0	0.0	-
10	Enable	0	Low	802.3at	0.0	0.0	-

7.1.3 What May Go Wrong:

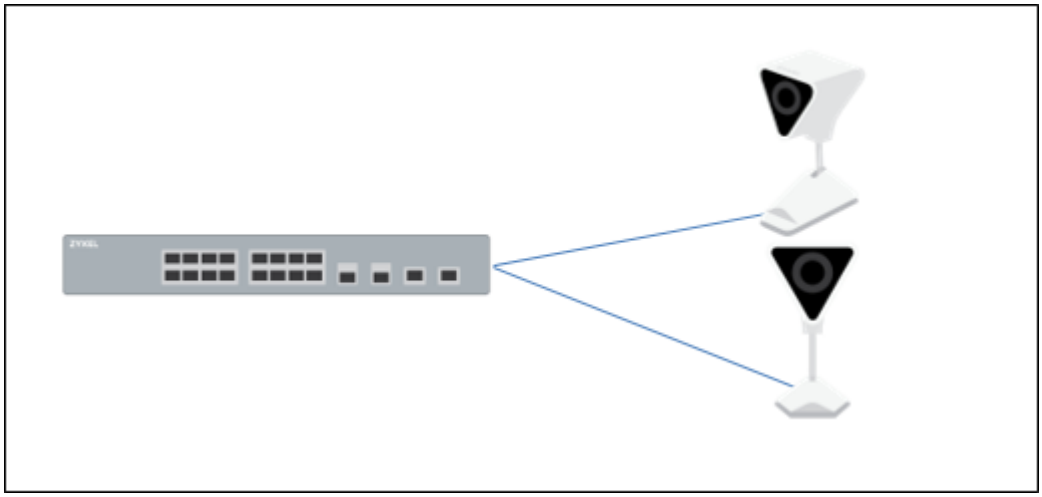
1. For GS1300 Series, after toggling the dip switches on the front panel, remember to push the reset & apply button. After pushing the button, the switch will restart and the feature of extended range will indeed be activated.

2. For GS1350 Series, we recommend users to enable the extended range first and then plug in the cable. Otherwise, users have to re-plug the cable or re-enable the PoE to activate extended range.

7.2 How to Configure the Switch to Implement Auto PD Recovery

The crash/hang on surveillance devices (ex: IP camera) can usually be recovered by just a reboot. Zyxel switch GS1350 series models support PoE feature "**Auto PD Recovery**" which offers a way to restart malfunctioning PDs from Zyxel Switch (PSE) to reduce service-down time by sending a field engineer to troubleshoot the live site. Additionally, this feature ensures the reliability of network by preventing situations where PDs are suddenly no longer working.

In the purpose of ensuring reliability of the network, below example will instruct administrator on how to configure the switch by using **Auto PD Recovery** to have an alternative & sufficient way to reset power supply of malfunctioning PDs.



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.
In order to access PDs efficiently to simulate the PD malfunction, the example was tested with WAC6502D-S and NWA1123-NI as PDs instead of common IP Cameras, and we use GS1350-6HP as the PoE Switch.

There are 2 options for **Auto PD Recovery** feature.

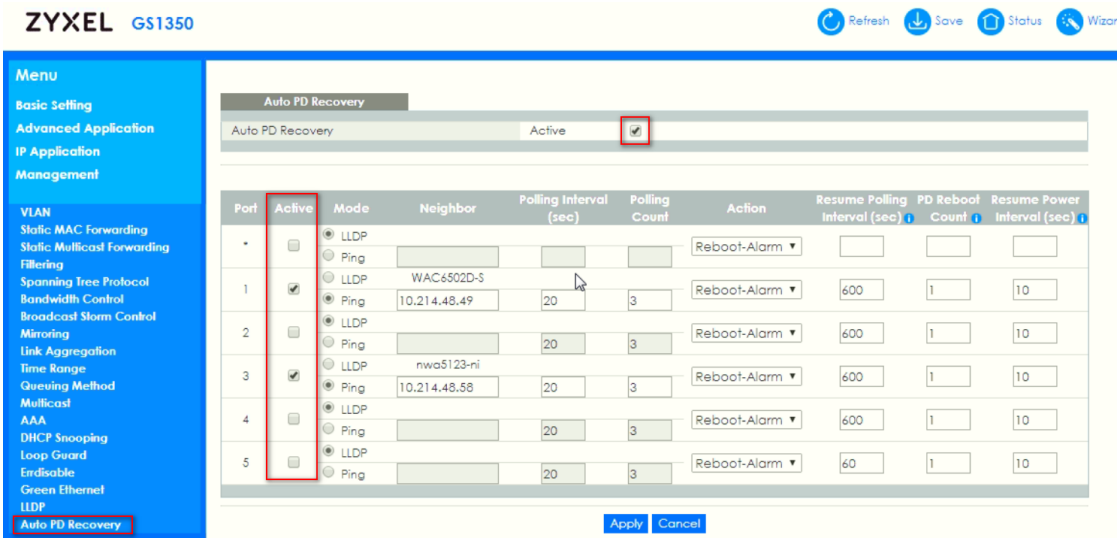
1.Ping mode: Detect the PD status by performing ping requests.
2.LLDP mode: Monitor LLDP packets from the PD.

Both modes detect PD status within a certain period of time (referred to as "**Resume Polling Interval**"). Once the configured criteria is reached, the switch will perform reboot-alarm action to the PD.
The number of times that the switch can make the PD reboot is also a configurable value (referred to as "**PD Reboot Count**"). If the times that the switch tries to reboot the PD reaches the value, the switch will no longer try rebooting the PD even if the polling count is reached.

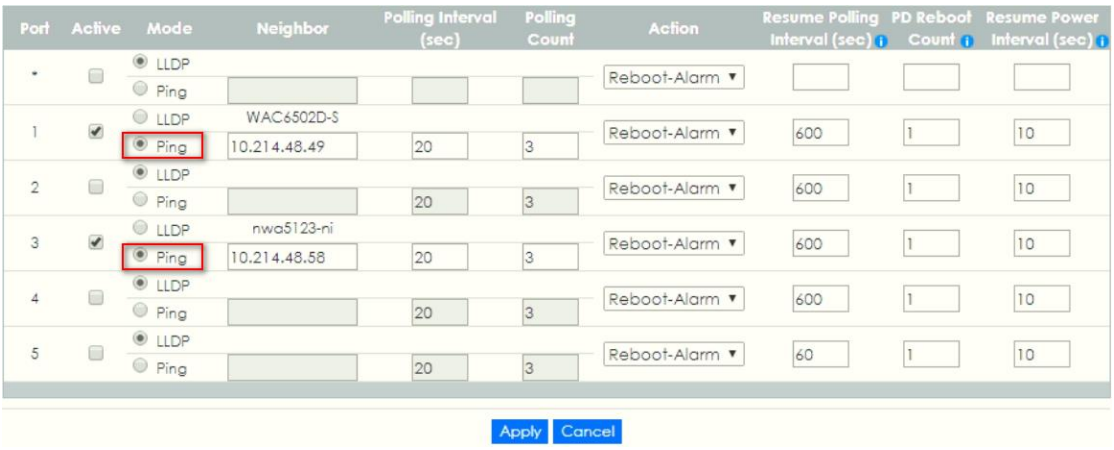
We will respectively use “Ping mode” & “LLDP mode” in the following examples.

7.2.1 Configuration in the Switch (Ping mode)

1. Access the web-GUI of the Switch.
2. Go to **Advanced Application > Auto PD Recovery**.
   Activate Auto PD Recovery and check the desired port(s).



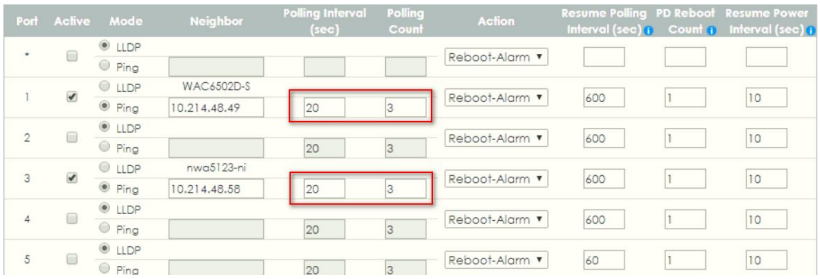
3. Select the mode as "Ping" and make sure the IP of the PD is correct.



Note:

The default setting about Polling Interval (20 secs) and Polling Count (3 times) will make switch detect the PD status by performing ping requests every 20 seconds.

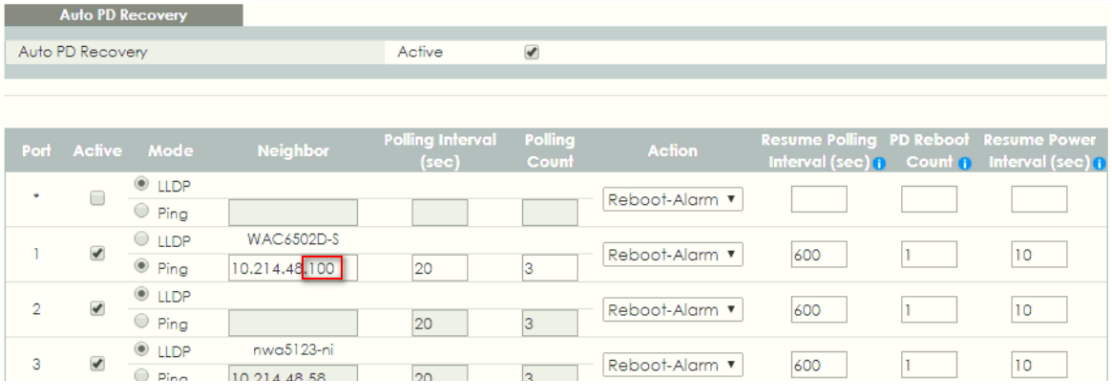
If there is no ping reply from the PD, polling count starts to count from 1. Once polling count is reached to 3 times, the switch will perform the reboot-alarm action to reboot the PD.



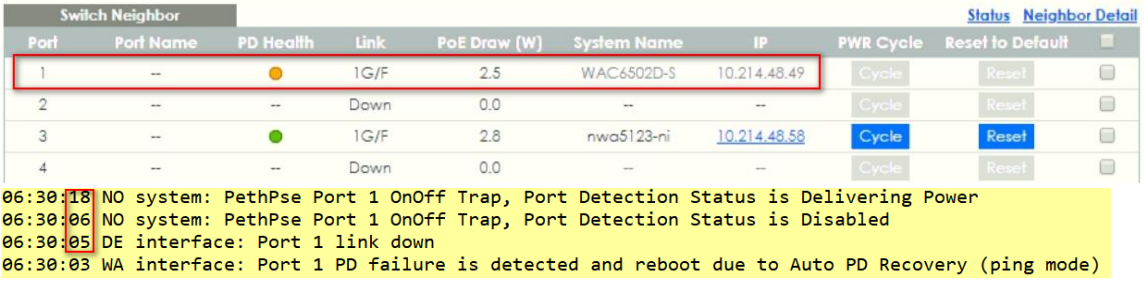
Port	Active	Mode	Neighbor	Polling Interval (sec)	Polling Count	Action	Resume Polling Interval (sec)	PD Reboot Count	Resume Power Interval (sec)
*	☐	LLDP / Ping				Reboot-Alarm			
1	☑	LLDP / Ping	WAC6502D-S / 10.214.48.49	20	3	Reboot-Alarm	600	1	10
2	☐	LLDP / Ping		20	3	Reboot-Alarm	600	1	10
3	☑	LLDP / Ping	nwa5123-ni / 10.214.48.58	20	3	Reboot-Alarm	600	1	10
4	☐	LLDP / Ping		20	3	Reboot-Alarm	600	1	10
5	☐	LLDP / Ping		20	3	Reboot-Alarm	60	1	10

7.2.2 Test the Result (Ping Mode)

1. Change the polling PD IP in **Auto PD Recovery** page to simulate the situation that the PD is not replying ping requests from the switch.



2. Once the **Polling Count** reached to 3 times, the switch will perform the reboot-alarm action to reboot the PD.
   In **Main Status > Neighbor**, the **PD Health** status will turn to yellow LED (means the PD is rebooting).
   When switch performs rebooting the PD (the connected port is detected as link-down on switch), the switch will start to again supply the power to the PD 10 seconds later (default value of **Resume Power Interval**).

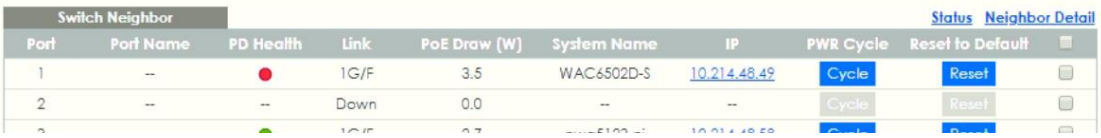


3. After the PD is powered on, the switch resumes to detect the PD status by performing ping requests after 600 seconds (default value of **Resume Polling Interval**).
4. The **Polling Count** will once again reach 3 times since there is still no response from the changed polling IP 10.214.48.100. However, the switch will no longer perform

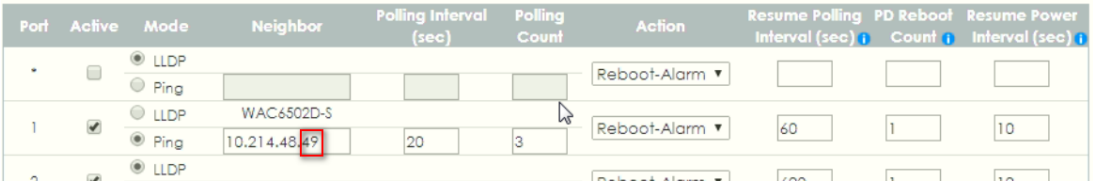
PD recovery process due to the **PD Reboot Count** Value (default: 1 time) is reached.

```
WA interface: Port 1 PD failure is detected. PD recovery process is
terminated as switch has reached the maximum PD reboot threshold (ping mode)
```

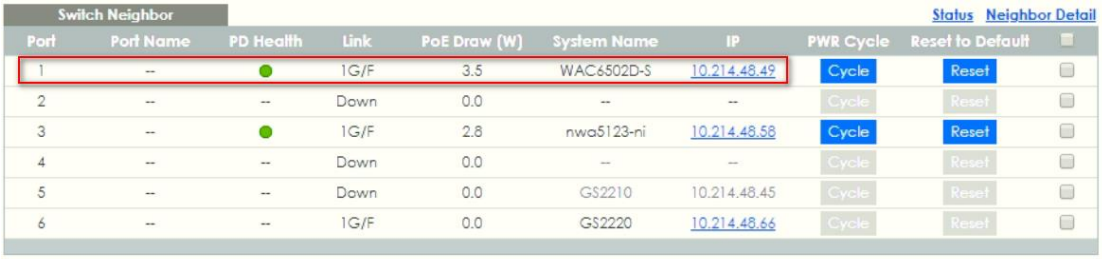
Meanwhile the detecting process (ping requests) keeps going, the **PD Health** status will become red LED (means the PD is considered dead).



5. Change back the correct ping IP of the PD in **Auto PD Recovery** page to simulate the situation that the PD is normally responding the ping requests.



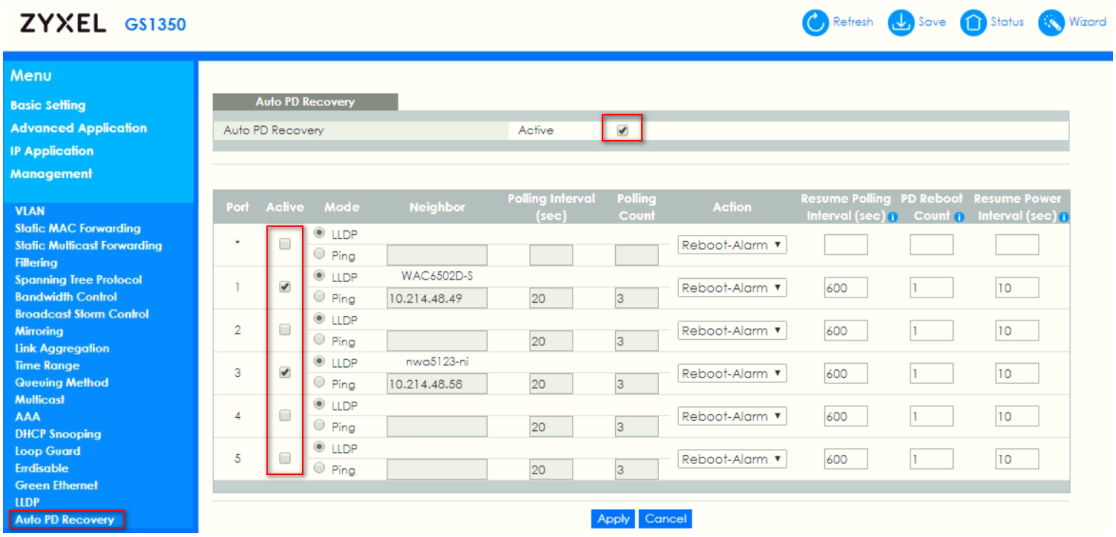
6. After the next successful detecting process, the **PD Health** status will turn to greed LED (means the PD is considered normal).



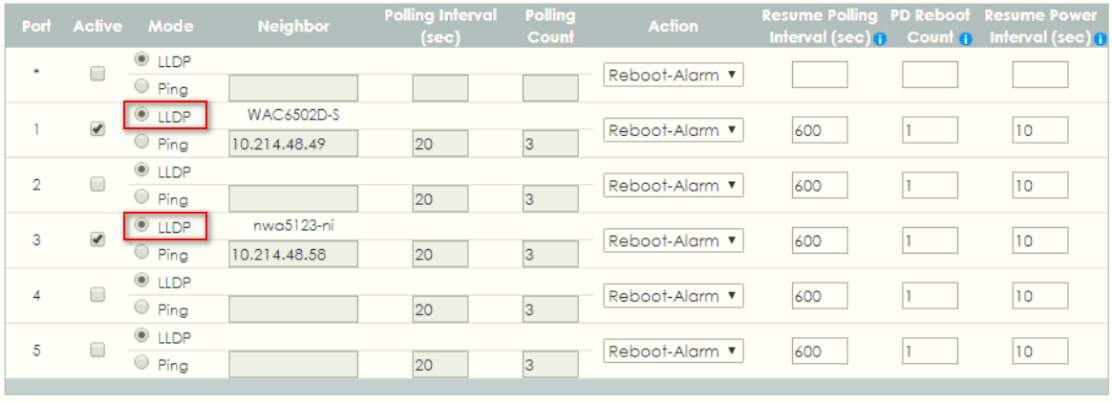
Note:
The **PD reboot count** will be reset in case of any modification of **Auto PD Recovery** is applied, or rebooting of the switch itself

7.2.3 Configuration in the Switch (LLDP mode)

1. Access the web GUI of the Switch.
2. Go to **Advanced Application > Auto PD Recovery**.
   Activate Auto PD Recovery and check the desired port(s).



3. Select the mode as "LLDP" (default mode).



Note:

In LLDP mode, switch monitors the PD status by checking incoming LLDP packets every 30 seconds (default value of transmit interval for LLDP feature) from the PD.

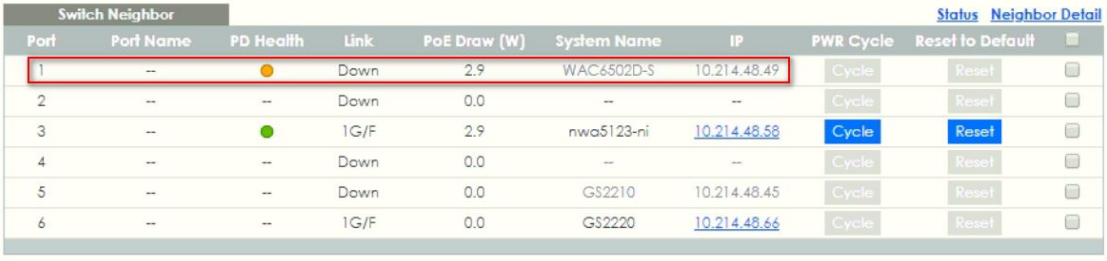
Likewise, switch sends out LLDP packets to the PD every 30 seconds to update the neighbor table on the PD.

Switch will check the LLDP table every 600 seconds (default value of **Resume Polling Interval**). If the PD entry disappears (default LLDP table aging time: 120 seconds) in switch's LLDP table, the switch will perform the reboot-alarm action (default action) to reboot the PD.

7.2.4 Test the Result (LLDP Mode)

1. Turn off LLDP feature of the PD to simulate the situation that PD is not responding LLDP anymore.

2. Once the PD entry disappears in switch's LLDP table, the switch will perform the reboot-alarm action to reboot the PD.
   In **Main Status > Neighbor**, the **PD Health** status will turn to yellow LED (means the PD is rebooting).
   When switch performs rebooting the PD (the connected port is detected as link-down on switch), the switch will start to again supply the power to the PD 10 seconds later (default value of **Resume Power Interval**).



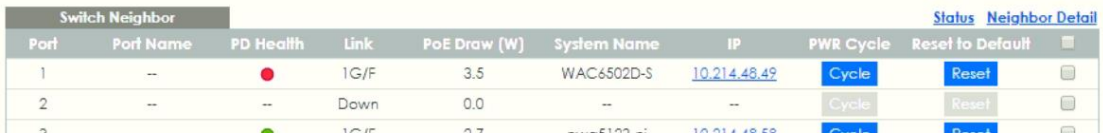

```
07:42:33 NO system: PethPse Port 1 OnOff Trap, Port Detection Status is Delivering Power
07:42:27 IN authentication: HTTP(s) user admin login [IP address = 10.214.48.43]
07:42:19 NO system: PethPse Port 1 OnOff Trap, Port Detection Status is Disabled
07:42:19 DE interface: Port 1 link down
07:42:17 WA interface: Port 1 PD failure is detected and reboot due to Auto PD Recovery (lldp mode)
```

3. After the PD is powered on, the switch resumes to detect the PD status by checking LLDP table after 600 seconds (default value of **Resume Polling Interval**).
4. The PD's LLDP info is still missing since the LLDP feature is turned off on the PD. However, the switch will no longer perform PD recovery process due to the **PD Reboot Count** Value (default: 1 time) is reached.

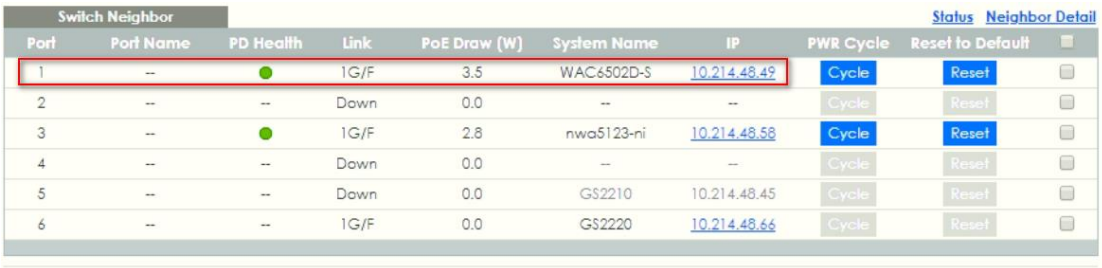
```
WA interface: Port 1 PD failure is detected. PD recovery process is
```

```
terminated as switch has reached the maximum PD reboot threshold (lldp mode)
```

5. Meanwhile the detecting process (checking LLDP table) keeps going, the **PD Health** status will become red LED (means the PD is considered dead).



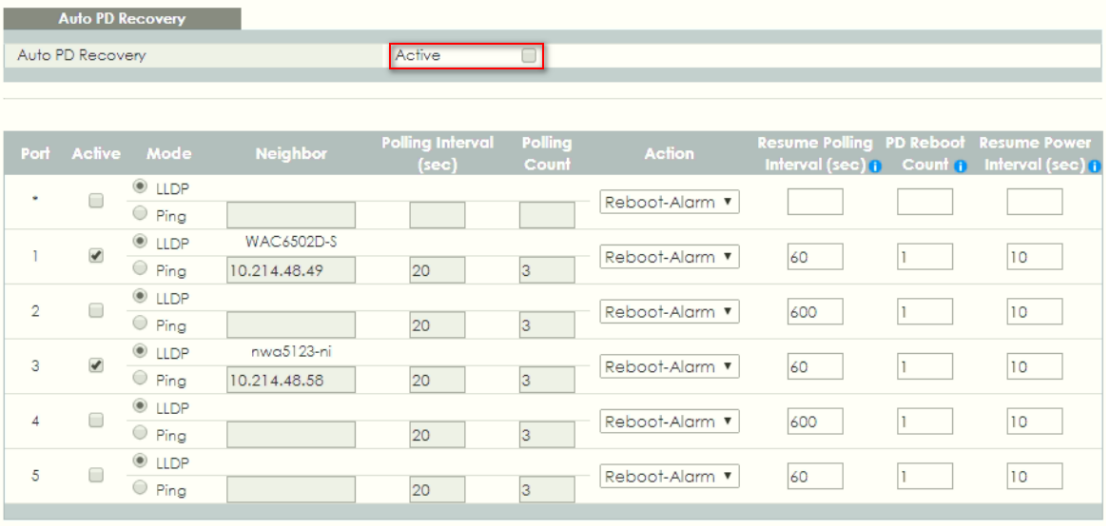
6. Recover the LLDP feature on the PD to simulate the situation that the PD can regularly exchange LLDP info with the switch.
7. After the next successful detecting process, the **PD Health** status will turn to greed LED (means the PD is considered normal).

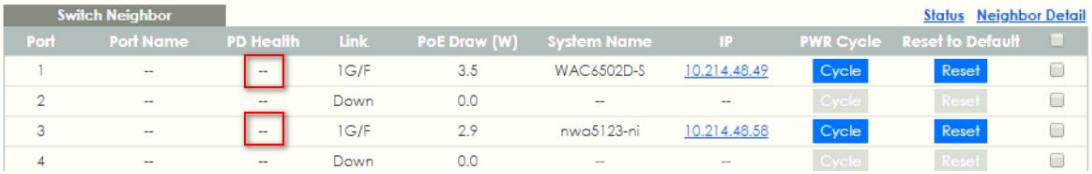


Note:
The **PD reboot count** will be reset in case of any modification of **Auto PD Recovery** is applied, or rebooting of the switch itself

7.2.5 What May Go Wrong

1. In **Main Status > Neighbor**, the **PD Health** will not display the status instantaneously after any enable/disable action was applied.





The status will be refreshed after the configured **Resume Polling Interval** (default: 600 secs), which means the detecting process is ongoing.