ZYXEL

www.zyxel.com

Switch Series

ES 3500 Series

GS 1920 Series / 2210 Series / 3700 Series

XGS 2210 Series / 3700 Series / 4500 Series

XS 1920-12 / 3700-24/ 3900-48

Firmware Version 4.00~4.30
Edition 1, 9/2016

Troubleshooting Guide

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

1 How to Troubleshoot Switch Related Issues

This document describes the necessary process for troubleshooting Zyxel Switch related issues.

STEP 1: Information Gathering

Start by gathering basic and general information. This is necessary for the following reasons:

- Attempt to locally reproduce issue.
- Gain perspective over customer's network architecture.
- Quickly identify devices.

You can verify which information is relevant for troubleshooting by reviewing "***Basic information***".

STEP 2: Identifying the Symptom

Analyze the problem that your customer is experiencing. Avoid using subjective responses. Rely on objective responses.

Example of **subjective** responses:

- The <*device*> stopped working sometimes.
- <*Device*> crashes all the time.
- All devices cannot access the Internet.

Example of **objective** responses:

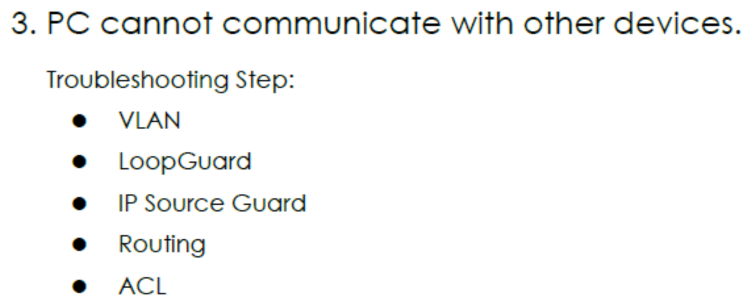
- <Device> undergoes **unexpected reboot** sometimes.
- Console CLI does not show any output.
- **Bob's laptop** cannot access the Internet.

Once you can clearly identify the symptom and the affected devices, refer to "***Symptom of Troubleshooting***" and locate the symptom that best matches customer's description.

STEP 3: Following the Troubleshooting Guides

Each symptoms will have a list of corresponding Troubleshooting Steps that you will need to look through.

Example:



3. PC cannot communicate with other devices.

Troubleshooting Step:

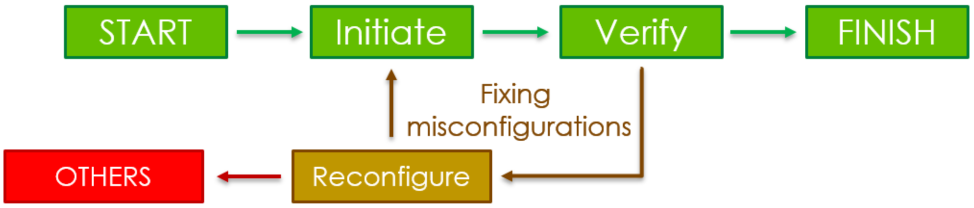
- VLAN
- LoopGuard
- IP Source Guard
- Routing
- ACL

If customer encounters symptom involving "*PC cannot communicate with other devices*", they will start the troubleshooting process by reviewing the following order:

- ***Troubleshooting of VLAN***
- ***Troubleshooting of Loop***
- ***Troubleshooting of IP Source Guard***
- ***Troubleshooting of Routing***
- ***Troubleshooting of ACL***

STEP 4: The Troubleshooting Process

Most of the Troubleshooting guide follows the common schema:



START: refers to where the troubleshooting process begins.

Initiate: refers to how the symptom is triggered.

Verify: indicates whether the issue is resolved or not.

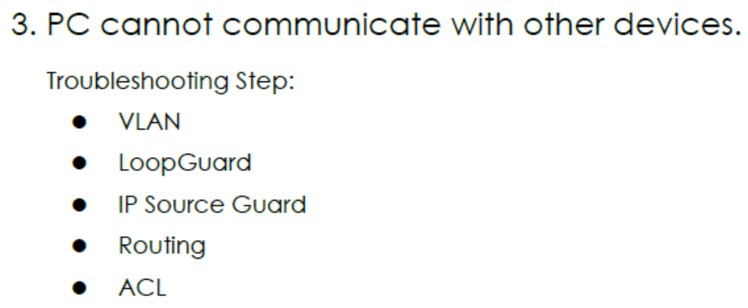
FINISH: is achieved when symptom related to this feature has either been resolved, or never encountered in the first place. Reaching this process will usually inform you to proceed to the next troubleshooting guide/agenda.

Reconfigure: refers to the common possible misconfigurations that may cause the observable symptoms.

OTHERS: this is achieved when symptom is caused by software malfunction or inter-operability issues between other devices. You will ultimately end-up in this section when all possible reconfigurations fails to pass the **Verify** stage. The **OTHERS** section will be occasionally updated as CSO continues to find new and unique problems.

If you end-up in the **OTHERS** section but cannot proceed further, then kindly consult with Zyxel's CSO.

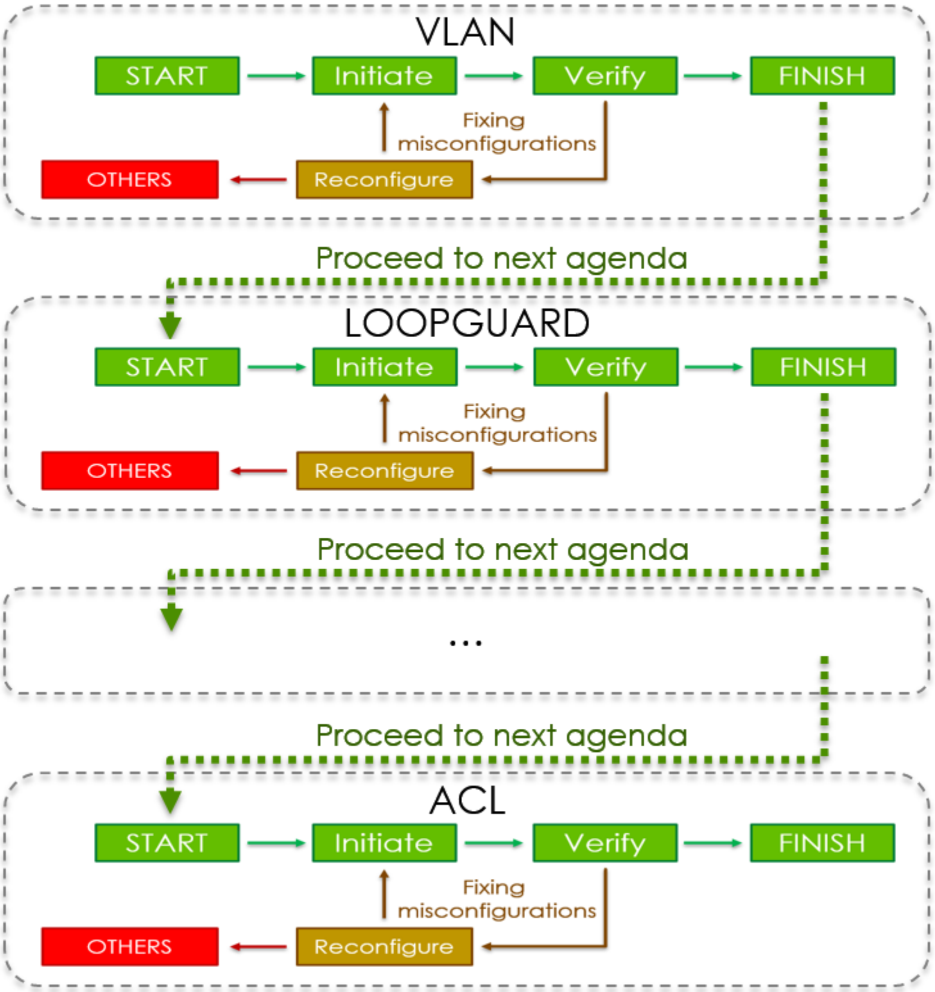
Example:



3. PC cannot communicate with other devices.

Troubleshooting Step:

- VLAN
- LoopGuard
- IP Source Guard
- Routing
- ACL


VLAN
START
Initiate
Verify
FINISH
Fixing misconfigurations
OTHERS
Reconfigure
Proceed to next agenda
LOOPGUARD
START
Initiate
Verify
FINISH
Fixing misconfigurations
OTHERS
Reconfigure
Proceed to next agenda
...
Proceed to next agenda
ACL
START
Initiate
Verify
FINISH
Fixing misconfigurations
OTHERS
Reconfigure

2 Symptom of Troubleshooting

Following are some common issue symptom report from customer, according to the symptoms of these problems, you can follow the below step and it will help you speed up to identify the cause of the problem.

1. Switch randomly crash.

   Troubleshooting Step:

   - Crash

2. Abnormal Status with PWR, SYS, ALM LED

   Troubleshooting Step:

   - HW Monitor

3. PC cannot communicate with other devices.

   Troubleshooting Step:

   - VLAN
   - LoopGuard
   - IP Source Guard
   - Routing
   - ACL

4. Client cannot get ip address from DHCP Server

   Troubleshooting Step:

   - VLAN
   - LoopGuard
   - IP Source Guard
   - DHCP Server
   - DHCP Relay
   - ACL

5. Administrator cannot manage the switches.

   Troubleshooting Step:

   - VLAN
   - Management
   - DHCP Relay
   - ACL

6. CCTV cannot watch Channel, LAG, Delay, Mosaics or Freeze.

   Troubleshooting Step:

   - VLAN
   - Multicast Troubleshooting.
   - L2 IGMP Snooping
   - L3 IGMP Routing
   - MVR

7. IP phone or IP Camera cannot be power on by PoE Switch.

   Troubleshooting Step:

   - PoE Troubleshooting Guide.

3 Basic Information

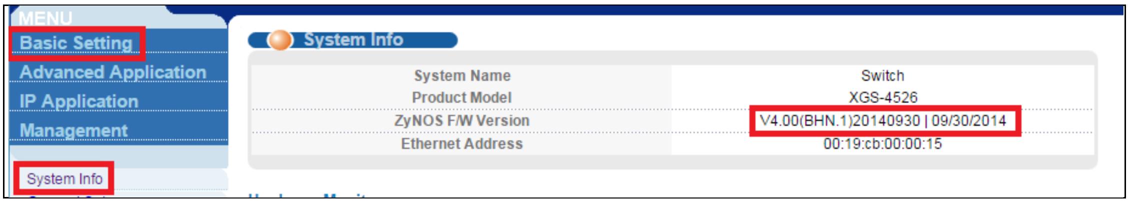
If switch happen some problem, following are some general information may need to confirm first:

- Firmware Version
- Configuration
- Tech-Support Logs
- Network Topology

3.1 Check Firmware Version

1. WebGUI:

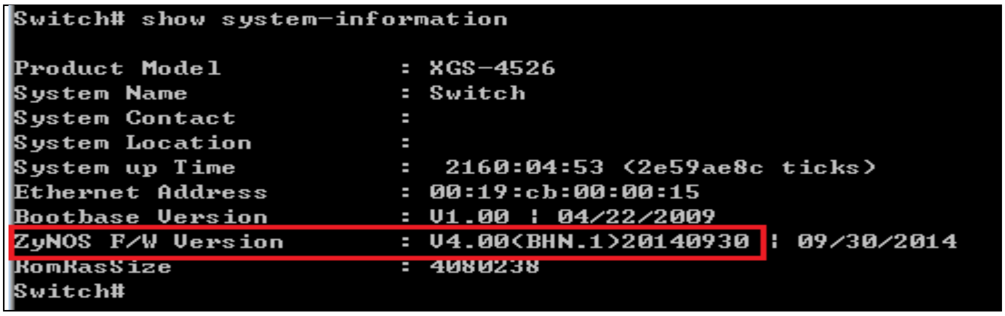
Figure 1 Basic Setting > System Info



System Name	Switch
Product Model	XGS-4526
ZyNOS F/W Version	V4.00(BHN.1)20140930 | 09/30/2014
Ethernet Address	00:19:cb:00:00:15

2. CLI:

Figure 2 Enter CLI command “show system-information”.

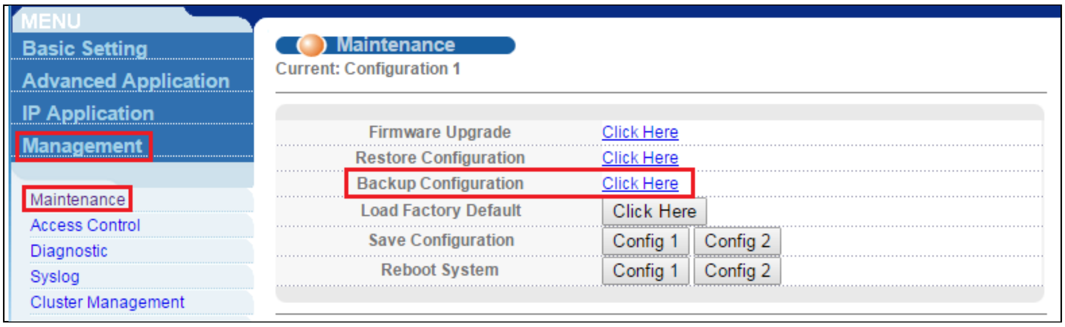


```
Switch# show system-information

Product Model                  : XGS-4526
System Name                    : Switch
System Contact                 :
System Location                :
System up Time                 :  2160:04:53 (2e59ae8c ticks)
Ethernet Address               : 00:19:cb:00:00:15
Bootbase Version               : V1.00 | 04/22/2009
ZyNOS F/W Version              : V4.00(BHN.1)20140930 | 09/30/2014
RomRasSize                     : 4080238
Switch#
```

3.2 Configuration

1. WebGUI:

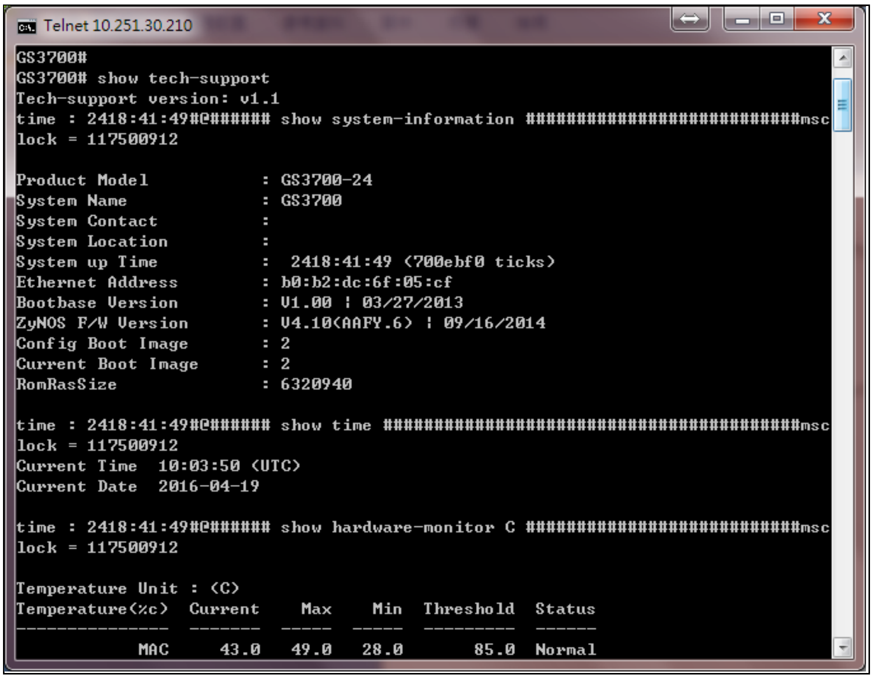
Figure 3 Management > Maintenance > Backup Configuration



3.3 Tech-Support Logs

1. CLI:

Figure 4 Enter CLI command "show tech-support".



```
GS3700#
GS3700# show tech-support
Tech-support version: v1.1
time : 2418:41:49#@###### show system-information ###########################msc
lock = 117500912

Product Model           : GS3700-24
System Name             : GS3700
System Contact          :
System Location         :
System up Time          :  2418:41:49 (700ebf0 ticks)
Ethernet Address        : b0:b2:dc:6f:05:cf
Bootbase Version        : V1.00 | 03/27/2013
ZyNOS F/W Version       : V4.10(AAFY.6) | 09/16/2014
Config Boot Image       : 2
Current Boot Image      : 2
RomRasSize              : 6320940

time : 2418:41:49#@###### show time #########################################msc
lock = 117500912
Current Time  10:03:50 (UTC)
Current Date  2016-04-19

time : 2418:41:49#@###### show hardware-monitor C ###########################msc
lock = 117500912

Temperature Unit : (C)
Temperature(%c)  Current    Max    Min  Threshold  Status
---------------  -------  -----  -----  ---------  ------
            MAC     43.0   49.0   28.0       85.0  Normal
```

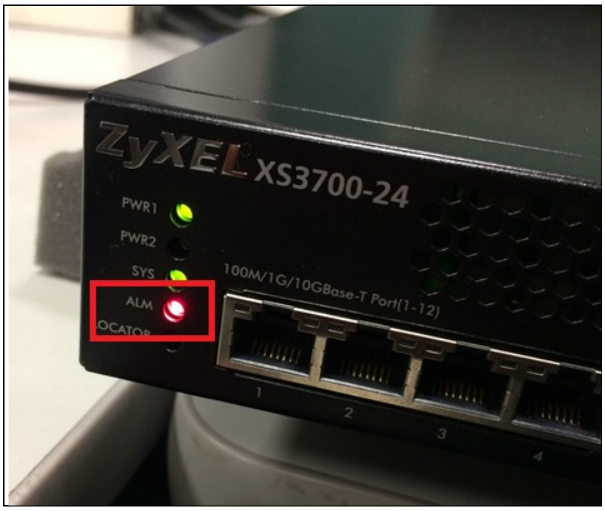
3.4 Topology

In order to speed up to understand the issue how to happen, the topology information is important for troubleshooting.

4 Hardware Monitor Status

4.1 Check ALM LED

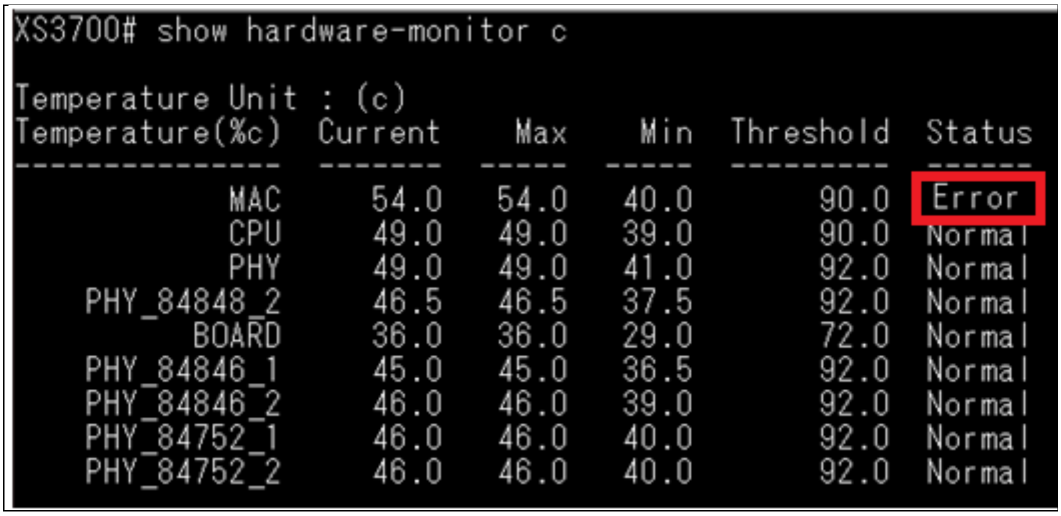
Figure 1 ALM LED On



4.2 Temperature Error

1. CLI:

Figure 2 Enter CLI command "Show hardware-monitor C".



```
XS3700# show hardware-monitor c

Temperature Unit : (c)
Temperature(%c)  Current    Max    Min   Threshold  Status
---------------  -------  -----  -----  ----------  ------
            MAC     54.0   54.0   40.0        90.0  Error
            CPU     49.0   49.0   39.0        90.0  Normal
            PHY     49.0   49.0   41.0        92.0  Normal
     PHY_84848_2    46.5   46.5   37.5        92.0  Normal
          BOARD     36.0   36.0   29.0        72.0  Normal
     PHY_84846_1    45.0   45.0   36.5        92.0  Normal
     PHY_84846_2    46.0   46.0   39.0        92.0  Normal
     PHY_84752_1    46.0   46.0   40.0        92.0  Normal
     PHY_84752_2    46.0   46.0   40.0        92.0  Normal
```

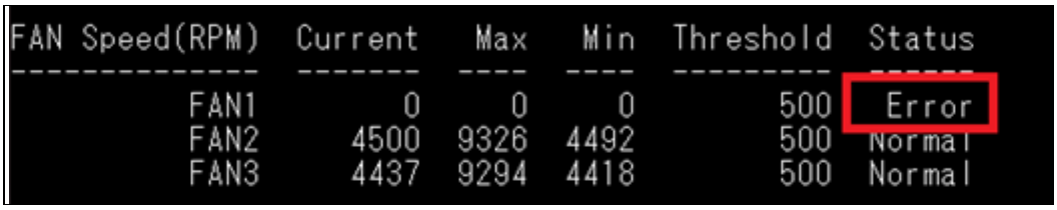
Note:

If MAC/CPU/PHY temperature status is error, the hardware may have some problem. Please send the device to RMA.

4.3 FAN Error

1. CLI:

Figure 3 Enter CLI command "Show hardware-monitor C".



```
FAN Speed(RPM)  Current   Max   Min   Threshold  Status
--------------  -------  ----  ----  ---------  ------
          FAN1        0     0     0        500   Error
          FAN2     4500  9326  4492        500  Normal
          FAN3     4437  9294  4418        500  Normal
```

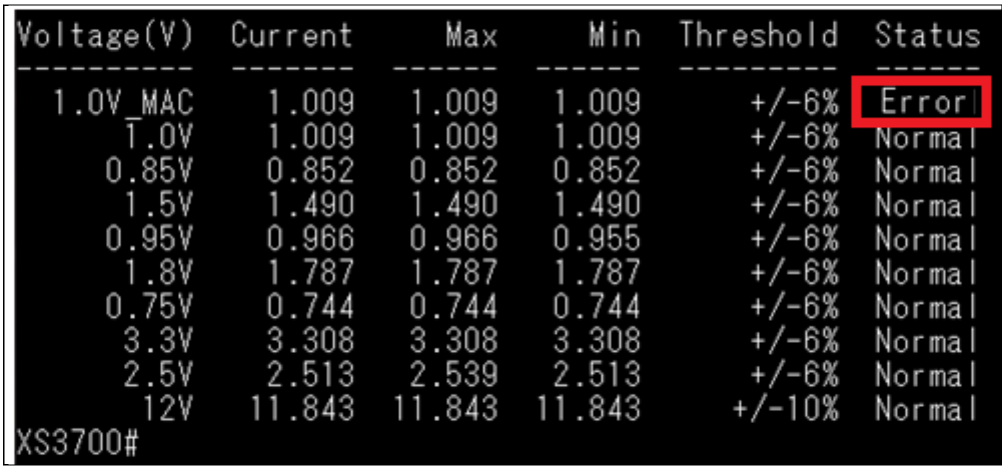
Note:

If FAN status is error, you can try to replace the FAN model to recovery it, if the problem cannot resolve, please send to the device to RMA.

4.4 Voltage Error

1. CLI:

Figure 4 Enter CLI command "Show hardware-monitor C".



```
Voltage(V)  Current     Max     Min  Threshold  Status
----------  -------  ------  ------  ---------  ------
  1.0V_MAC    1.009   1.009   1.009      +/-6%   Error
      1.0V    1.009   1.009   1.009      +/-6%  Normal
     0.85V    0.852   0.852   0.852      +/-6%  Normal
      1.5V    1.490   1.490   1.490      +/-6%  Normal
     0.95V    0.966   0.966   0.955      +/-6%  Normal
      1.8V    1.787   1.787   1.787      +/-6%  Normal
     0.75V    0.744   0.744   0.744      +/-6%  Normal
      3.3V    3.308   3.308   3.308      +/-6%  Normal
      2.5V    2.513   2.539   2.513      +/-6%  Normal
       12V   11.843  11.843  11.843     +/-10%  Normal
XS3700#
```

Note:

If Voltage status is error, the problem may relate power supply or power source.

Suggestion:

- Using a UPS connect to the switch and monitor a while, if the problem can resolve, the root cause may relate customer's environment.
- If problem cannot resolve by connection UPS, the root cause may relate power supply, please send the switch to RMA.

4.5 Switch cannot bootup successfully?

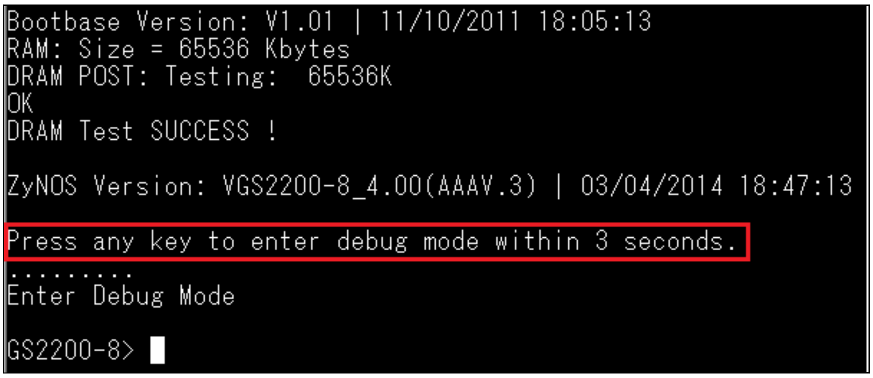
1. Use console to connect the switch and check all baudrate which is able to display information or not.
   - Baudrate 38400, 19200, 9600, 57600, 115200

Note:

If all baudrate has no any response, please send the switch to RMA.

2. If switch has responses, please verify below steps:
3. Open the terminal software (Need tosupport XModem function. e.g: Teraturn)
4. Reboot the switch and enter into debug mode.

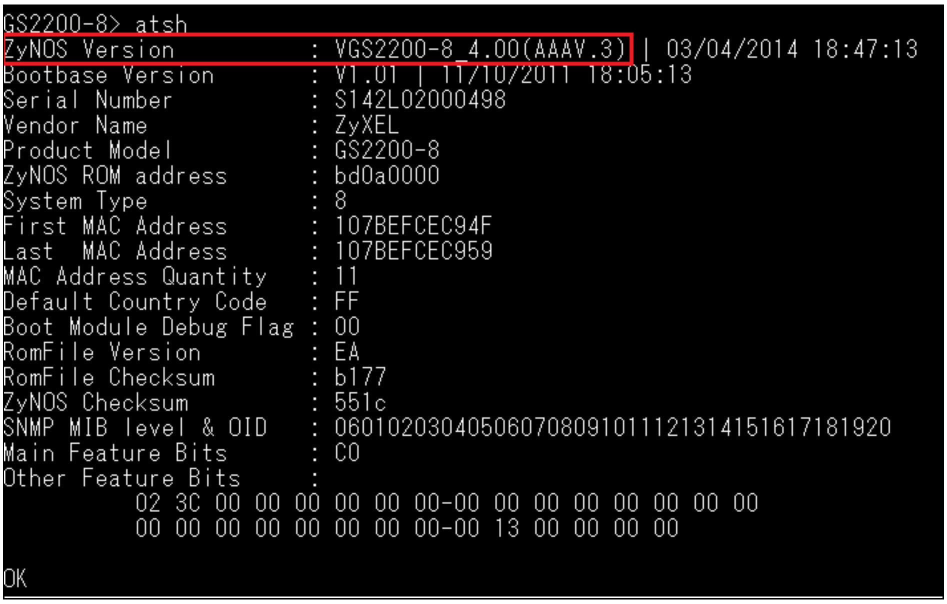
Figure 5 Enter debug mode



```
Bootbase Version: V1.01 | 11/10/2011 18:05:13
RAM: Size = 65536 Kbytes
DRAM POST: Testing:  65536K
OK
DRAM Test SUCCESS !

ZyNOS Version: VGS2200-8_4.00(AAAV.3) | 03/04/2014 18:47:13

Press any key to enter debug mode within 3 seconds.
.........
Enter Debug Mode

GS2200-8>
```

5. Check the Firmware version.

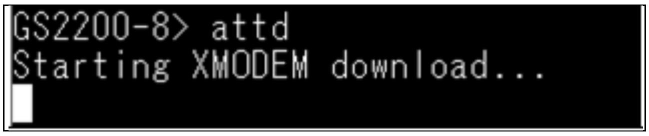
Figure 6 Enter CLI command "atsh".



```
GS2200-8> atsh
ZyNOS Version          : VGS2200-8_4.00(AAAV.3) | 03/04/2014 18:47:13
Bootbase Version       : V1.01 | 11/10/2011 18:05:13
Serial Number          : S142L02000498
Vendor Name            : ZyXEL
Product Model          : GS2200-8
ZyNOS ROM address      : bd0a0000
System Type            : 8
First MAC Address      : 107BEFCEC94F
Last  MAC Address      : 107BEFCEC959
MAC Address Quantity   : 11
Default Country Code   : FF
Boot Module Debug Flag : 00
RomFile Version        : EA
RomFile Checksum       : b177
ZyNOS Checksum         : 551c
SNMP MIB level & OID   : 060102030405060708091011121314151617181920
Main Feature Bits      : C0
Other Feature Bits     :
          02 3C 00 00 00 00 00 00-00 00 00 00 00 00 00 00
          00 00 00 00 00 00 00 00-00 13 00 00 00 00

OK
```

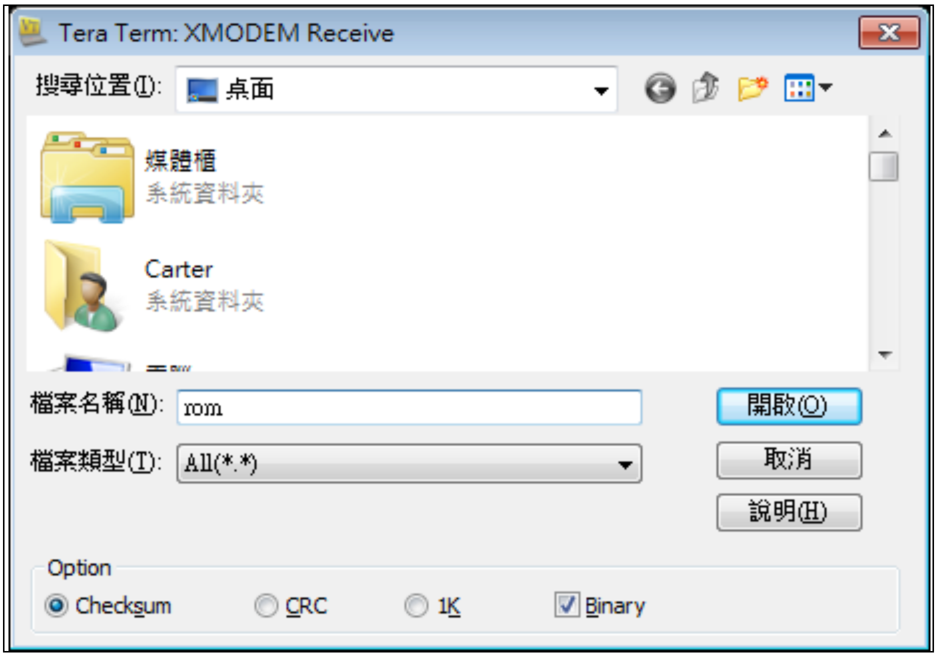
6. Download Rom File

Figure 7 Enter CLI command “attd”.



```
GS2200-8> attd
Starting XMODEM download...
```

Figure 8 Save Rom file.



Tera Term: XMODEM Receive

搜尋位置(I): 桌面

檔案名稱(N): rom

檔案類型(T): All(*.*)

Option

● Checksum ○ CRC ○ 1K ☑ Binary

7. Report to HQ CSO

Provide the rom file, firmware version and crash logs to HQ.

5 Switch Auto-Reboot, Crash

5.1 How to check switch is whether auto-reboot?

1. Login to the switch via Console/Telnet/SSH.
2. Enter CLI command "**Show Logging**".

- **Switch Crash**
  - system: System warm start
  - system: System has reset without management command
- **Reload Config**
  - system: System warm start
  - system: System has reset due to a management command
- **Boot Config**
  - system: System cold start
  - system: System has reset due to a management command
- **Reboot by un-plug power cable**
  - system: System cold start
  - system: System has reset without management command

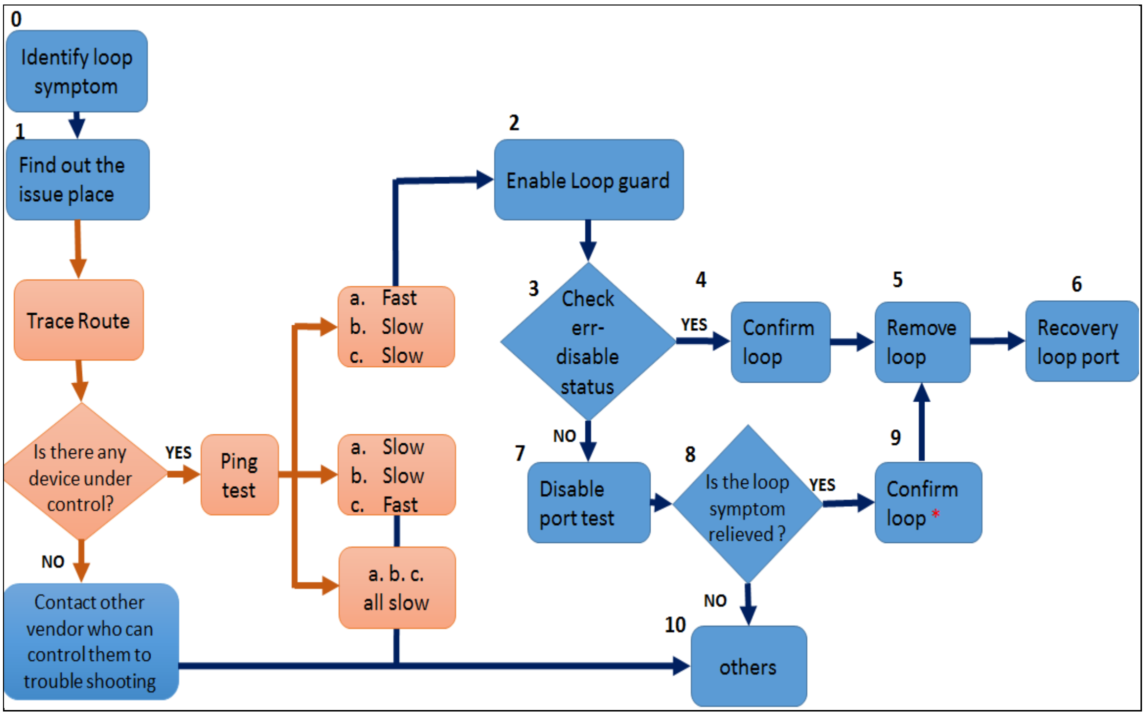
If user found switch Crash logs, please provide the following information to HQ CSO.

- Basic information (Page No.6)
- Switch Crash Frequency
- If possible, use console connect to switch and capture the crash log when issue happen.
- What's the device connect to the switch?
- Is there any server polling to the switch regularly?
- Before device crash occurs, have modified or changed on the switch?
- How many devices met this problem?

6 Troubleshooting for Loop

Flowchart:

Figure 1



6.1 Identify loop symptom

When loop happened, it is possible to find the following scenario:

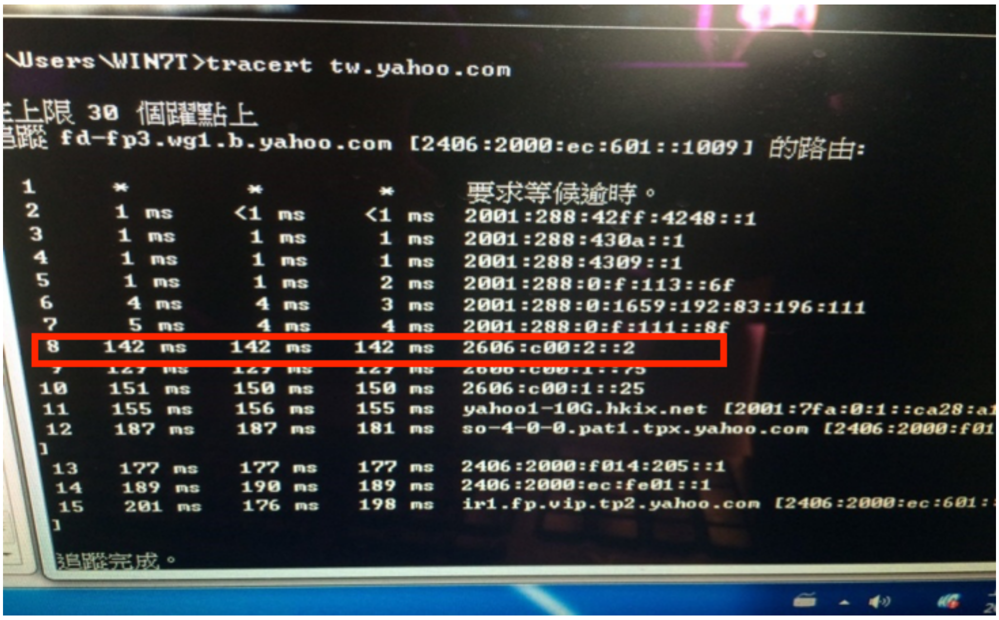
- The traffic becomes slower than before.
- The traffic is not stable. The client always gets lost.
- The LED of port is keep flashing fast.

To find out the slowest node in the topology. If it is under control, please start trouble shooting form here; if it is not, please contact another vendor.

6.2 Find out the issue place

1. Use "tracert" command to find out the place where the most possible loop is.

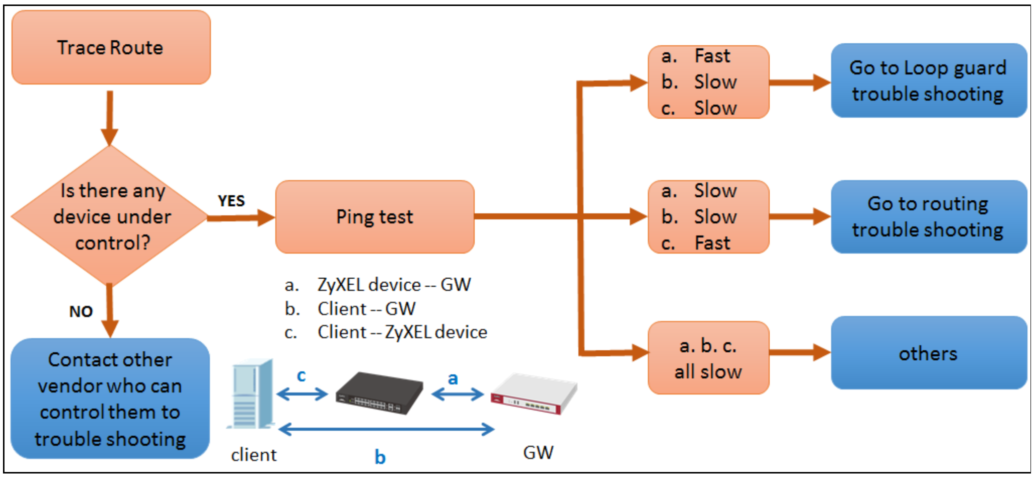
Figure 2



```
\Users\WIN7T>tracert tw.yahoo.com

上限 30 個躍點上
追蹤 fd-fp3.wg1.b.yahoo.com [2406:2000:ec:601::1009] 的路由:

  1     *        *        *     要求等候逾時。
  2     1 ms    <1 ms    <1 ms  2001:288:42ff:4248::1
  3     1 ms     1 ms     1 ms  2001:288:430a::1
  4     1 ms     1 ms     1 ms  2001:288:4309::1
  5     1 ms     1 ms     2 ms  2001:288:0:f:113::6f
  6     4 ms     4 ms     3 ms  2001:288:0:1659:192:83:196:111
  7     5 ms     4 ms     4 ms  2001:288:0:f:111::8f
  8   142 ms   142 ms   142 ms  2606:c00:2::2
  9   127 ms   127 ms   127 ms  2606:c00:1::75
 10   151 ms   150 ms   150 ms  2606:c00:1::25
 11   155 ms   156 ms   155 ms  yahoo1-10G.hkix.net [2001:7fa:0:1::ca28:a
 12   187 ms   187 ms   181 ms  so-4-0-0.pat1.tpx.yahoo.com [2406:2000:f01
]
 13   177 ms   177 ms   177 ms  2406:2000:f014:205::1
 14   189 ms   190 ms   189 ms  2406:2000:ec:fe01::1
 15   201 ms   176 ms   198 ms  ir1.fp.vip.tp2.yahoo.com [2406:2000:ec:601:
]

追蹤完成。
```

For example, in the above, form client tracert to Yahoo, you can notice that it get slower from no.8 node. And then to verify the area under no.8 can be controlled or not. If yes, do the ping test to verify where the issue is.

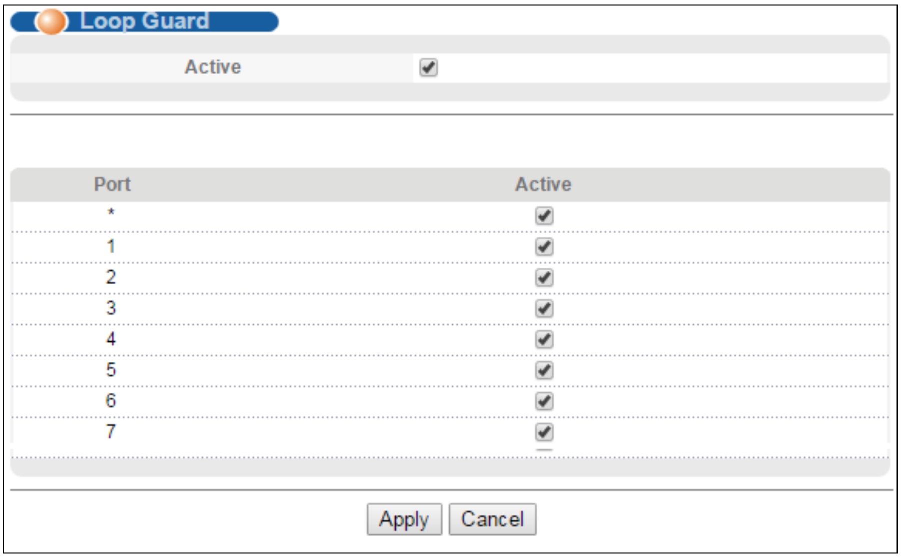
Figure 3


Trace Route
Is there any device under control?
YES
NO
Ping test
Contact other vendor who can control them to trouble shooting
a. ZyXEL device -- GW
b. Client -- GW
c. Client -- ZyXEL device
c
a
b
client
GW
a. Fast
b. Slow
c. Slow
a. Slow
b. Slow
c. Fast
a. b. c. all slow
Go to Loop guard trouble shooting
Go to routing trouble shooting
others

6.3 Enable Loop Guard

1. WebGUI:

Figure 4 Advanced Application>Loop Guard



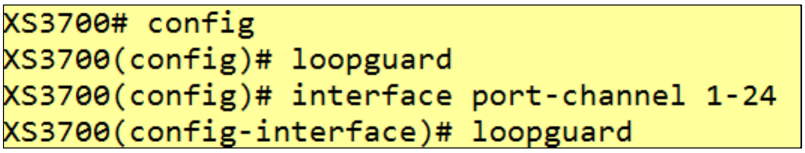
Loop Guard

Active ☑

Port	Active
*	☑
1	☑
2	☑
3	☑
4	☑
5	☑
6	☑
7	☑

2. CLI:

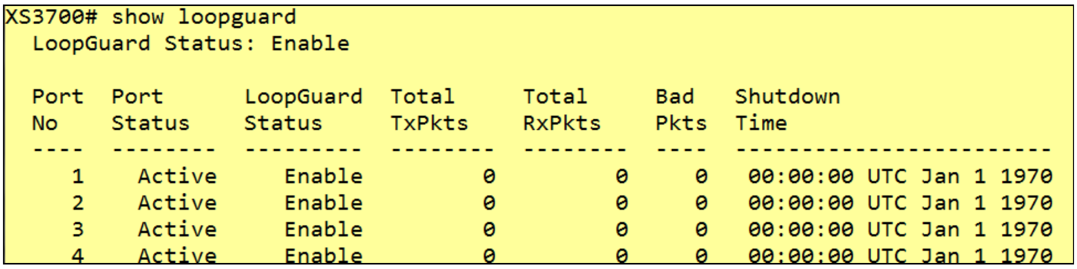
Figure 5



```
XS3700# config
XS3700(config)# loopguard
XS3700(config)# interface port-channel 1-24
XS3700(config-interface)# loopguard
```

3. Check Loop Guard status.

Figure 6 Enter CLI command "show loopguard"



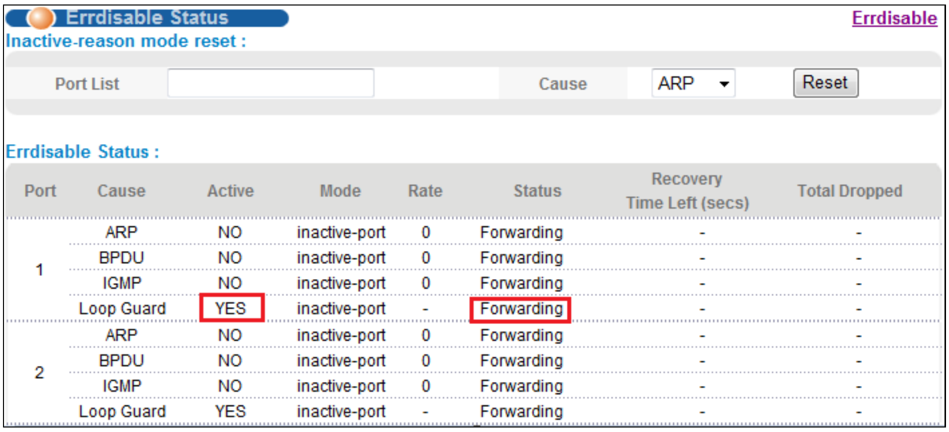
```
XS3700# show loopguard
  LoopGuard Status: Enable

  Port  Port      LoopGuard  Total     Total     Bad   Shutdown
  No    Status    Status     TxPkts    RxPkts    Pkts  Time
  ----  --------  ---------  --------  --------  ----  ------------------------
     1    Active     Enable         0         0     0   00:00:00 UTC Jan  1 1970
     2    Active     Enable         0         0     0   00:00:00 UTC Jan  1 1970
     3    Active     Enable         0         0     0   00:00:00 UTC Jan  1 1970
     4    Active     Enable         0         0     0   00:00:00 UTC Jan  1 1970
```

6.4 Check Err-Disable status

1. WebGUI:

- If switch didn't detect loop, you can see the status of Loop Guard is "Forwarding".

Figure 1 Advanced Application > Errdisable > Errdisable Status



Inactive-reason mode reset :

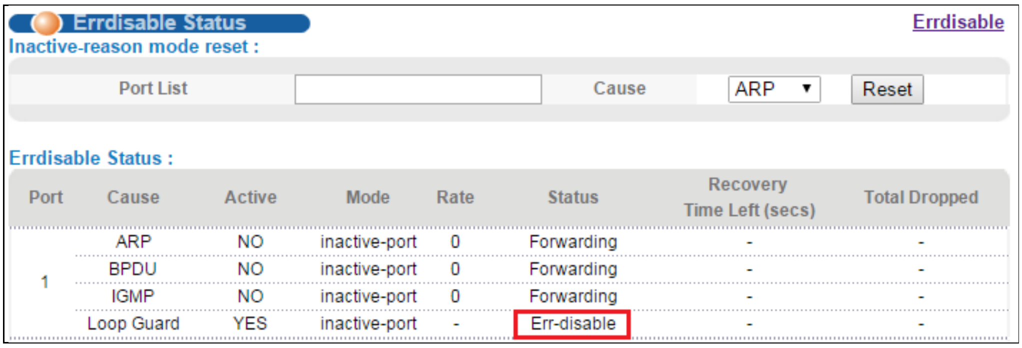
Port List | Cause ARP | Reset

Errdisable Status :

Port	Cause	Active	Mode	Rate	Status	Recovery Time Left (secs)	Total Dropped
1	ARP	NO	inactive-port	0	Forwarding	-	-
	BPDU	NO	inactive-port	0	Forwarding	-	-
	IGMP	NO	inactive-port	0	Forwarding	-	-
	Loop Guard	YES	inactive-port	-	Forwarding	-	-
2	ARP	NO	inactive-port	0	Forwarding	-	-
	BPDU	NO	inactive-port	0	Forwarding	-	-
	IGMP	NO	inactive-port	0	Forwarding	-	-
	Loop Guard	YES	inactive-port	-	Forwarding	-	-

- If switch detect loop, the status of Loop Guard is "Err-disable".

Figure 2 Advanced Application > Errdisable > Errdisable Status



Inactive-reason mode reset :

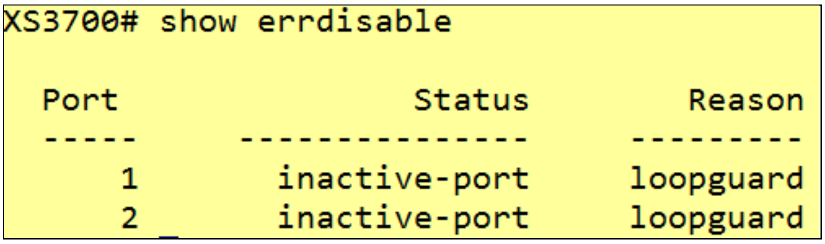
Port List | Cause ARP | Reset

Errdisable Status :

Port	Cause	Active	Mode	Rate	Status	Recovery Time Left (secs)	Total Dropped
1	ARP	NO	inactive-port	0	Forwarding	-	-
	BPDU	NO	inactive-port	0	Forwarding	-	-
	IGMP	NO	inactive-port	0	Forwarding	-	-
	Loop Guard	YES	inactive-port	-	Err-disable	-	-

2. CLI:

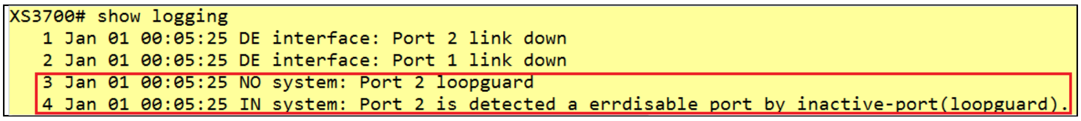
Figure 3 Enter CLI command "show errdisable"



```
XS3700# show errdisable

 Port                Status          Reason
 -----          ---------------     ---------
     1             inactive-port    loopguard
     2             inactive-port    loopguard
```

3. Loopguard event also record in system logs.

Figure 4 Enter CLI command "show logging"



```
XS3700# show logging
   1 Jan 01 00:05:25 DE interface: Port 2 link down
   2 Jan 01 00:05:25 DE interface: Port 1 link down
   3 Jan 01 00:05:25 NO system: Port 2 loopguard
   4 Jan 01 00:05:25 IN system: Port 2 is detected a errdisable port by inactive-port(loopguard).
```

6.5 Confirm Loop

We suggest that to enable Loop guard one by one from the core switch to the end switch in topology. So that we can find where is loop.

6.6 Remove Loop

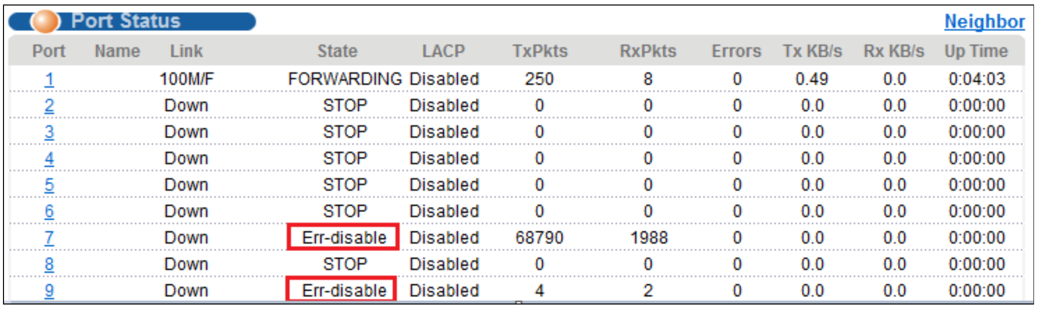
Un-plug cable from Err-Disable port.

6.7 Recovery Loop Port

1. If the port detect loop, the port status will become to "Err-disable".

   WebGUI:

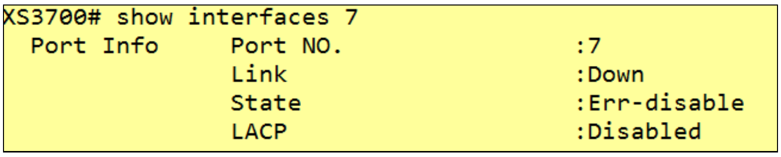
Figure 5 Advanced Application > Errdisable > Errdisable Status



Port	Name	Link	State	LACP	TxPkts	RxPkts	Errors	Tx KB/s	Rx KB/s	Up Time
1		100M/F	FORWARDING	Disabled	250	8	0	0.49	0.0	0:04:03
2		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
3		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
4		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
5		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
6		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
7		Down	Err-disable	Disabled	68790	1988	0	0.0	0.0	0:00:00
8		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
9		Down	Err-disable	Disabled	4	2	0	0.0	0.0	0:00:00

CLI:

Figure 6 Enter CLI command "show interface Port-ID"

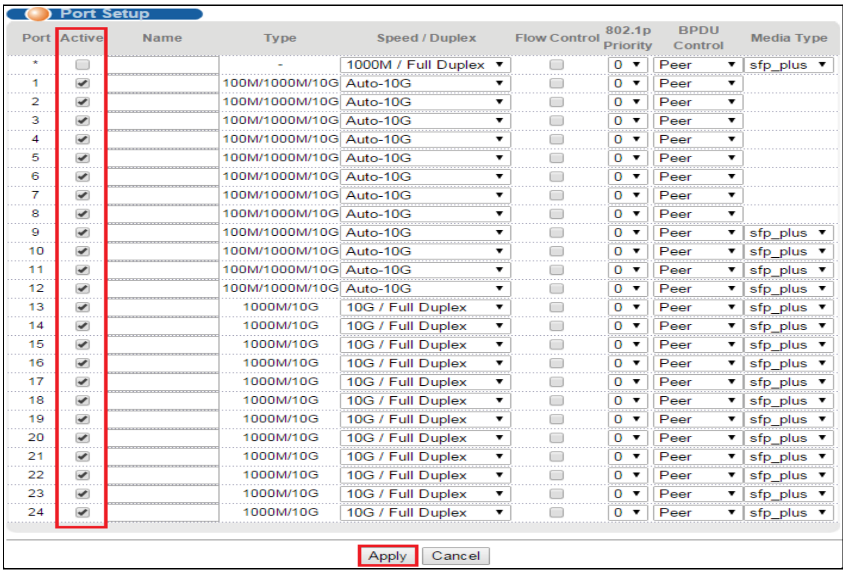


```
XS3700# show interfaces 7
  Port Info      Port NO.                 :7
                 Link                     :Down
                 State                    :Err-disable
                 LACP                     :Disabled
```

2. To recovery the port, it has to be disabled and enabled.

   WebGUI:

Figure 7 Basic Setting > Port Setup

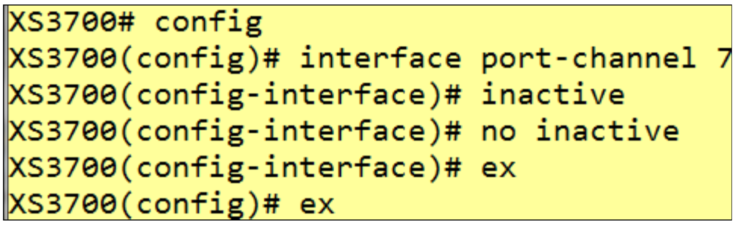


Port Setup

Port	Active	Name	Type	Speed / Duplex	Flow Control	802.1p Priority	BPDU Control	Media Type
*	□		-	1000M / Full Duplex	□	0	Peer	sfp_plus
1	☑		100M/1000M/10G	Auto-10G	□	0	Peer	
2	☑		100M/1000M/10G	Auto-10G	□	0	Peer	
3	☑		100M/1000M/10G	Auto-10G	□	0	Peer	
4	☑		100M/1000M/10G	Auto-10G	□	0	Peer	
5	☑		100M/1000M/10G	Auto-10G	□	0	Peer	
6	☑		100M/1000M/10G	Auto-10G	□	0	Peer	
7	☑		100M/1000M/10G	Auto-10G	□	0	Peer	
8	☑		100M/1000M/10G	Auto-10G	□	0	Peer	
9	☑		100M/1000M/10G	Auto-10G	□	0	Peer	sfp_plus
10	☑		100M/1000M/10G	Auto-10G	□	0	Peer	sfp_plus
11	☑		100M/1000M/10G	Auto-10G	□	0	Peer	sfp_plus
12	☑		100M/1000M/10G	Auto-10G	□	0	Peer	sfp_plus
13	☑		1000M/10G	10G / Full Duplex	□	0	Peer	sfp_plus
14	☑		1000M/10G	10G / Full Duplex	□	0	Peer	sfp_plus
15	☑		1000M/10G	10G / Full Duplex	□	0	Peer	sfp_plus
16	☑		1000M/10G	10G / Full Duplex	□	0	Peer	sfp_plus
17	☑		1000M/10G	10G / Full Duplex	□	0	Peer	sfp_plus
18	☑		1000M/10G	10G / Full Duplex	□	0	Peer	sfp_plus
19	☑		1000M/10G	10G / Full Duplex	□	0	Peer	sfp_plus
20	☑		1000M/10G	10G / Full Duplex	□	0	Peer	sfp_plus
21	☑		1000M/10G	10G / Full Duplex	□	0	Peer	sfp_plus
22	☑		1000M/10G	10G / Full Duplex	□	0	Peer	sfp_plus
23	☑		1000M/10G	10G / Full Duplex	□	0	Peer	sfp_plus
24	☑		1000M/10G	10G / Full Duplex	□	0	Peer	sfp_plus

CLI:

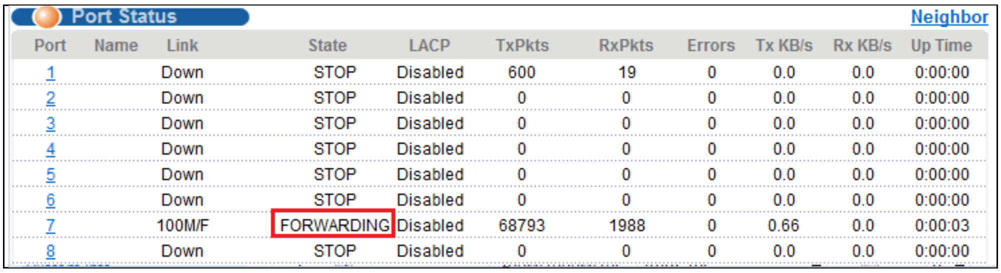
Figure 8



```
XS3700# config
XS3700(config)# interface port-channel 7
XS3700(config-interface)# inactive
XS3700(config-interface)# no inactive
XS3700(config-interface)# ex
XS3700(config)# ex
```

3. Repeat the above configuration twice. The first time disables the port active, the second time enables it. And the port is recovery to forwarding.

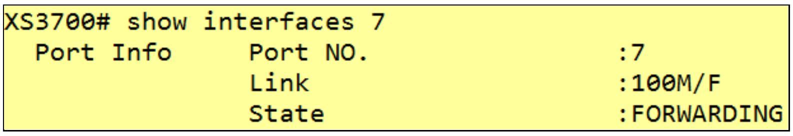
Figure 9



Port Status

Port	Name	Link	State	LACP	TxPkts	RxPkts	Errors	Tx KB/s	Rx KB/s	Up Time
1		Down	STOP	Disabled	600	19	0	0.0	0.0	0:00:00
2		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
3		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
4		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
5		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
6		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
7		100M/F	FORWARDING	Disabled	68793	1988	0	0.66	0.0	0:00:03
8		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00

Figure 10 Enter CLI command "show interface Port-ID"

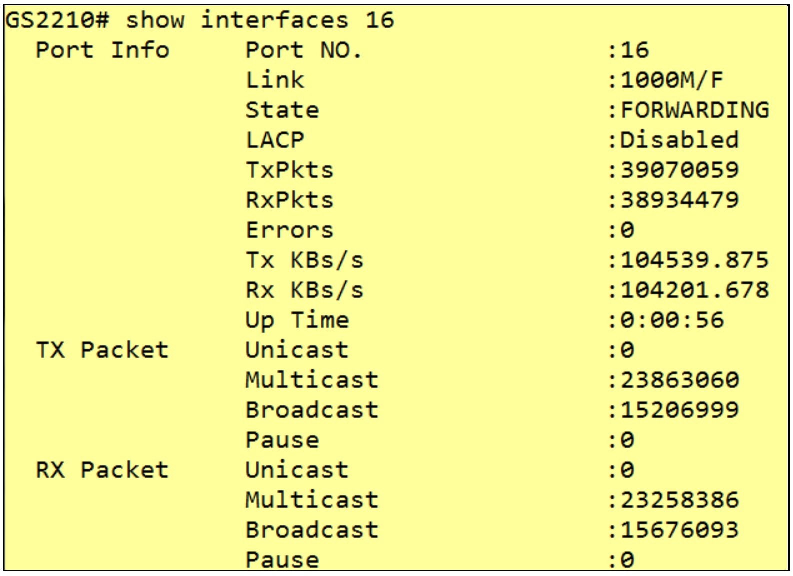


```
XS3700# show interfaces 7
  Port Info      Port NO.                   :7
                 Link                       :100M/F
                 State                      :FORWARDING
```

6.8 Disable Port Test

1. To check the port counters first. To compare their number of the RX (Multicast) packets. The largest one has the highest possibility of Loop.

Figure 11 Enter CLI command "show interface Port-ID"

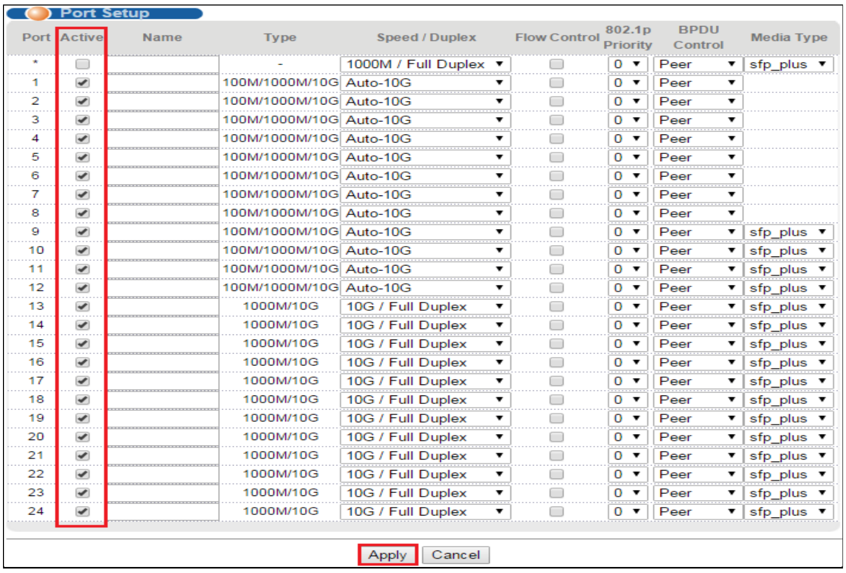


```
GS2210# show interfaces 16
  Port Info      Port NO.                :16
                 Link                    :1000M/F
                 State                   :FORWARDING
                 LACP                    :Disabled
                 TxPkts                  :39070059
                 RxPkts                  :38934479
                 Errors                  :0
                 Tx KBs/s                :104539.875
                 Rx KBs/s                :104201.678
                 Up Time                 :0:00:56
  TX Packet      Unicast                 :0
                 Multicast               :23863060
                 Broadcast               :15206999
                 Pause                   :0
  RX Packet      Unicast                 :0
                 Multicast               :23258386
                 Broadcast               :15676093
                 Pause                   :0
```

2. Disable ports one by one to relieve loop.

WebGUI:

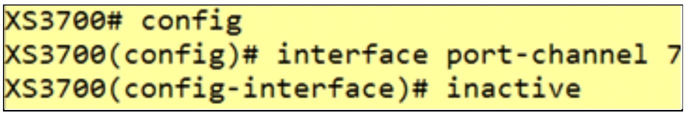
Figure 12 Basic Setting > Port Setup



Port	Active	Name	Type	Speed / Duplex	Flow Control	802.1p Priority	BPDU Control	Media Type
*	□		-	1000M / Full Duplex	□	0	Peer	sfp_plus
1	☑		100M/1000M/10G	Auto-10G	□	0	Peer	
2	☑		100M/1000M/10G	Auto-10G	□	0	Peer	
3	☑		100M/1000M/10G	Auto-10G	□	0	Peer	
4	☑		100M/1000M/10G	Auto-10G	□	0	Peer	
5	☑		100M/1000M/10G	Auto-10G	□	0	Peer	
6	☑		100M/1000M/10G	Auto-10G	□	0	Peer	
7	☑		100M/1000M/10G	Auto-10G	□	0	Peer	
8	☑		100M/1000M/10G	Auto-10G	□	0	Peer	
9	☑		100M/1000M/10G	Auto-10G	□	0	Peer	sfp_plus
10	☑		100M/1000M/10G	Auto-10G	□	0	Peer	sfp_plus
11	☑		100M/1000M/10G	Auto-10G	□	0	Peer	sfp_plus
12	☑		100M/1000M/10G	Auto-10G	□	0	Peer	sfp_plus
13	☑		1000M/10G	10G / Full Duplex	□	0	Peer	sfp_plus
14	☑		1000M/10G	10G / Full Duplex	□	0	Peer	sfp_plus
15	☑		1000M/10G	10G / Full Duplex	□	0	Peer	sfp_plus
16	☑		1000M/10G	10G / Full Duplex	□	0	Peer	sfp_plus
17	☑		1000M/10G	10G / Full Duplex	□	0	Peer	sfp_plus
18	☑		1000M/10G	10G / Full Duplex	□	0	Peer	sfp_plus
19	☑		1000M/10G	10G / Full Duplex	□	0	Peer	sfp_plus
20	☑		1000M/10G	10G / Full Duplex	□	0	Peer	sfp_plus
21	☑		1000M/10G	10G / Full Duplex	□	0	Peer	sfp_plus
22	☑		1000M/10G	10G / Full Duplex	□	0	Peer	sfp_plus
23	☑		1000M/10G	10G / Full Duplex	□	0	Peer	sfp_plus
24	☑		1000M/10G	10G / Full Duplex	□	0	Peer	sfp_plus

CLI:

Figure 13



```
XS3700# config
XS3700(config)# interface port-channel 7
XS3700(config-interface)# inactive
```

6.9 Is the loop symptom relieved?

6.10 Confirm loop *

If the loop symptom relieved when the port is disable, we can know the port has loop.

Why the port has loop, but loop guard doesn't active?

A: Zyxel loop guard feature is use the loop-guard packet to discover where the loop is. It is a multicast packet. But some features (ex. Unknown packet drop) will drop the loop-guard packet. If there are any clients (devices) which have those feature. The loop-guard will not be active. So that we suggest that the loop guard should be enabled in the end device.

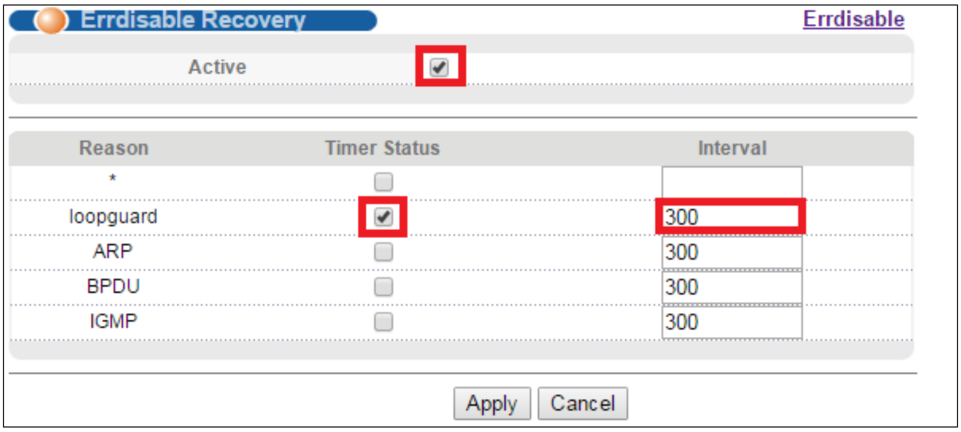
6.11 Others

1. There is no loop we can find in the topology, please go to the next process of trouble shooting.

6.12 How to setup Loop Guard auto-recovery

1. WebGUI

Figure 14 Advanced Application > Errdisable > Errdisable Recovery



Errdisable Recovery

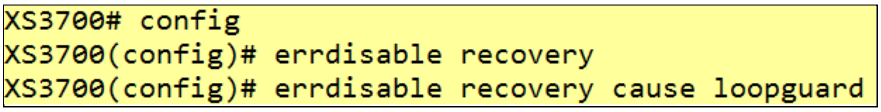
Errdisable

Active ☑

Reason	Timer Status	Interval
*	□	
loopguard	☑	300
ARP	□	300
BPDU	□	300
IGMP	□	300

2. CLI: (config)# errdisable recovery cause loopguard interval <seconds>

Figure 15



```
XS3700# config
XS3700(config)# errdisable recovery
XS3700(config)# errdisable recovery cause loopguard
```

3. Verifying the err-disable recovery

Figure 16 Enter CLI command “show errdisable recovery”

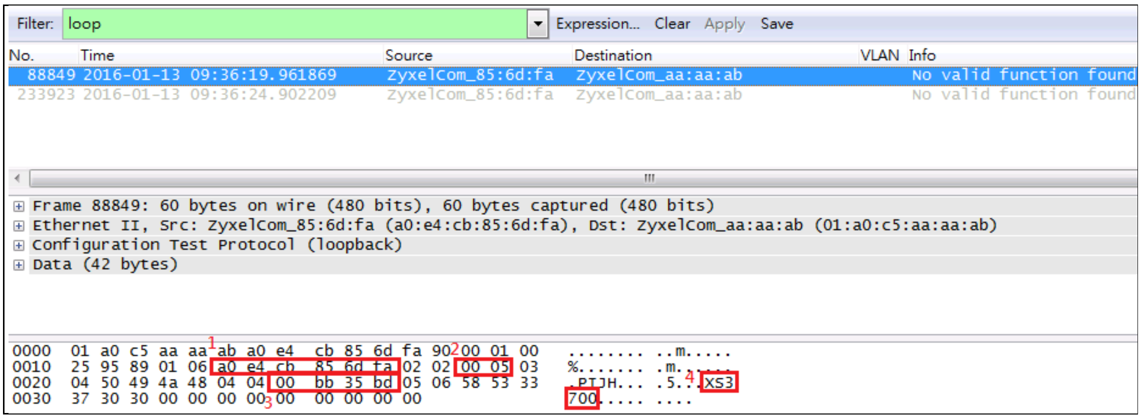
```
XS3700# show errdisable recovery
  Errdisable Recovery Status:Enable

  Reason            Timer Status        Time
  ----------        ------------        -------
   loopguard              Enable          300
         ARP             Disable          300
        BPDU             Disable          300
        IGMP             Disable          300

  Interfaces that will be enabled at the next timeout:

  Interface     Reason         Time left(sec)     Mode
  ---------     ----------     --------------     ---------------
          9      loopguard                239       inactive-port
```

Note:

The default recovery time is 300s. If time’s up and loop has removed, the feature will auto recovery the port.

4. Loop Guard Packet

Figure 17

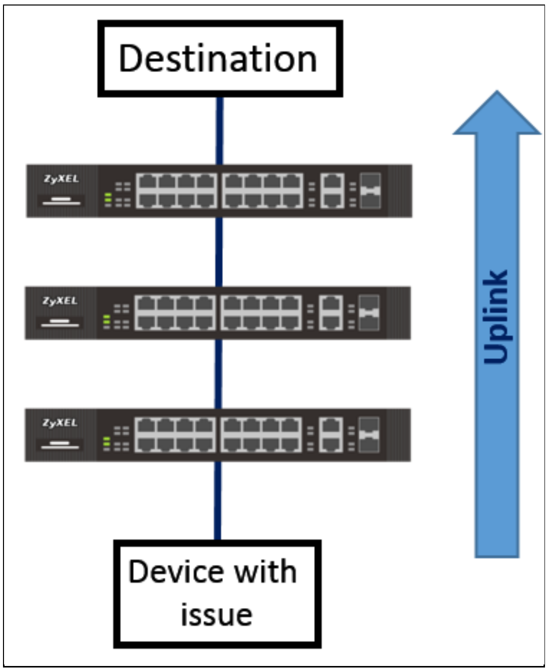


```
No.    Time                        Source               Destination          VLAN  Info
 88849 2016-01-13 09:36:19.961869  ZyxelCom_85:6d:fa   ZyxelCom_aa:aa:ab           No valid function found
233923 2016-01-13 09:36:24.902209  ZyxelCom_85:6d:fa   ZyxelCom_aa:aa:ab           No valid function found

⊞ Frame 88849: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
⊞ Ethernet II, Src: ZyxelCom_85:6d:fa (a0:e4:cb:85:6d:fa), Dst: ZyxelCom_aa:aa:ab (01:a0:c5:aa:aa:ab)
⊞ Configuration Test Protocol (loopback)
⊞ Data (42 bytes)

0000  01 a0 c5 aa aa ab a0 e4  cb 85 6d fa 90 00 01 00   ........ ..m.....
0010  25 95 89 01 06 a0 e4 cb  85 6d fa 02 02 00 05 03   %....... .m......
0020  04 50 49 4a 48 04 04 00  bb 35 bd 05 06 58 53 33   .PIJH... .5...XS3
0030  37 30 30 00 00 00 00 00  00 00 00 00               700..... ....
```

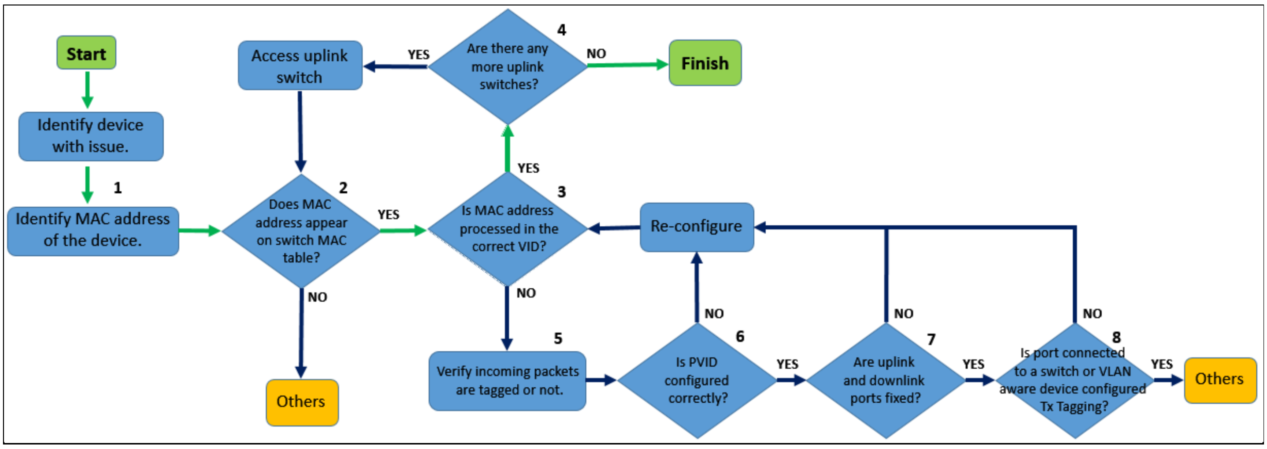
- The MAC of sender
- The port number of the sender. It starts from 0x0000. That’s 0x0000 stands for logic port 1, and 0x000f stands for logic port 16.
- This is the timestamp that the sender set when the preparing the packet. The unit is in seconds. With this field insert, the probe is different each time. The receiving can also have the information that the delay time and loop lasting time. Of course, to easy debug, we can have a debug flag to switch off this field.
- This is the model name of the sender. Like ES-3124. This is a string like host name.

7 Troubleshooting for VLAN

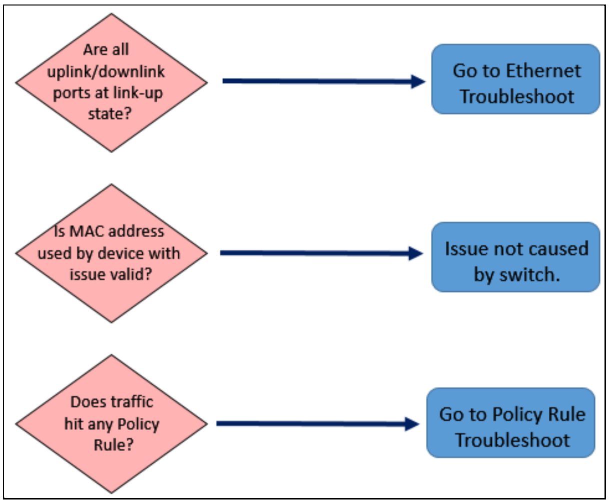
Illustration:

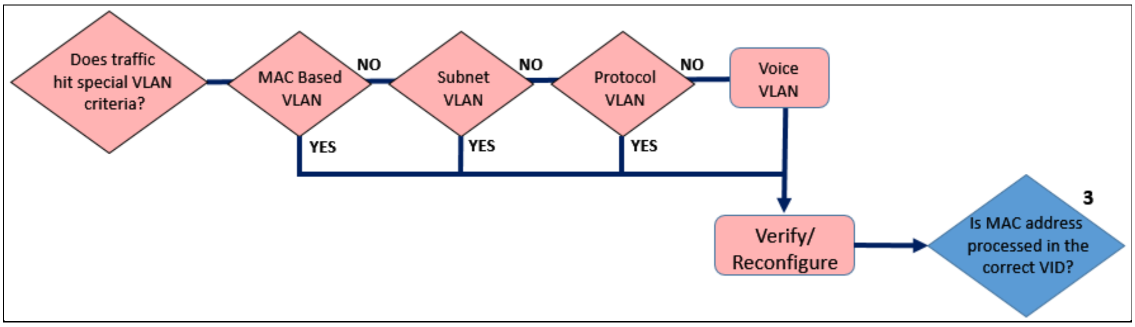


Flowchart:


Start
Identify device with issue.
1
Identify MAC address of the device.
Access uplink switch
2
Does MAC address appear on switch MAC table?
YES
NO
Others
3
Is MAC address processed in the correct VID?
YES
NO
4
Are there any more uplink switches?
YES
NO
Finish
5
Verify incoming packets are tagged or not.
Re-configure
6
Is PVID configured correctly?
NO
YES
7
Are uplink and downlink ports fixed?
NO
YES
8
Is port connected to a switch or VLAN aware device configured Tx Tagging?
NO
YES
Others

OTHERS:

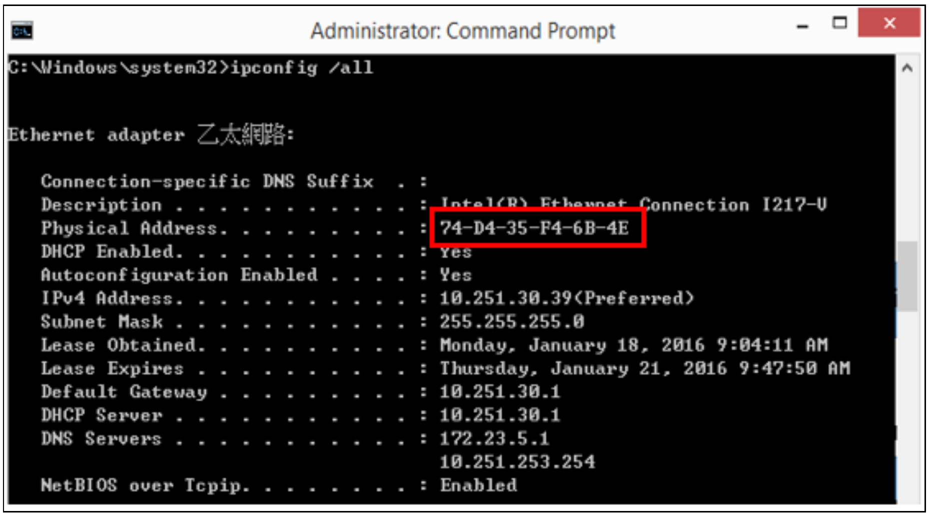

Are all uplink/downlink ports at link-up state?
Go to Ethernet Troubleshoot
Is MAC address used by device with issue valid?
Issue not caused by switch.
Does traffic hit any Policy Rule?
Go to Policy Rule Troubleshoot


Does traffic hit special VLAN criteria?
MAC Based VLAN
NO
Subnet VLAN
NO
Protocol VLAN
NO
Voice VLAN
YES
YES
YES
Verify/ Reconfigure
3
Is MAC address processed in the correct VID?

7.1 Identify and verify the MAC address of the interface of the device with issue.

Example using Windows OS, identifying MAC address of Local Area Connection

Figure 1



Administrator: Command Prompt

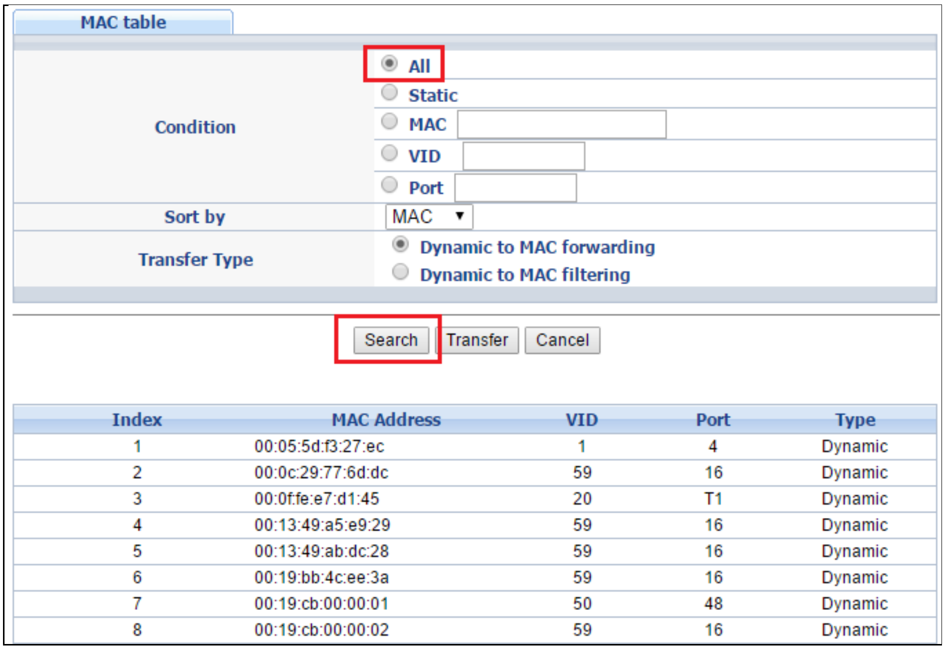
```
C:\Windows\system32>ipconfig /all


Ethernet adapter 乙太網路:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Ethernet Connection I217-V
   Physical Address. . . . . . . . . : 74-D4-35-F4-6B-4E
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 10.251.30.39(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Monday, January 18, 2016 9:04:11 AM
   Lease Expires . . . . . . . . . . : Thursday, January 21, 2016 9:47:50 AM
   Default Gateway . . . . . . . . . : 10.251.30.1
   DHCP Server . . . . . . . . . . . : 10.251.30.1
   DNS Servers . . . . . . . . . . . : 172.23.5.1
                                       10.251.253.254
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

After verifying MAC address, **go to step 2**.

7.2 Access the uplink Zyxel switch. Does the MAC address of the device with issue appear on the MAC address table of the Zyxel switch?

WebGUI:

Figure 2 Management > MAC Table



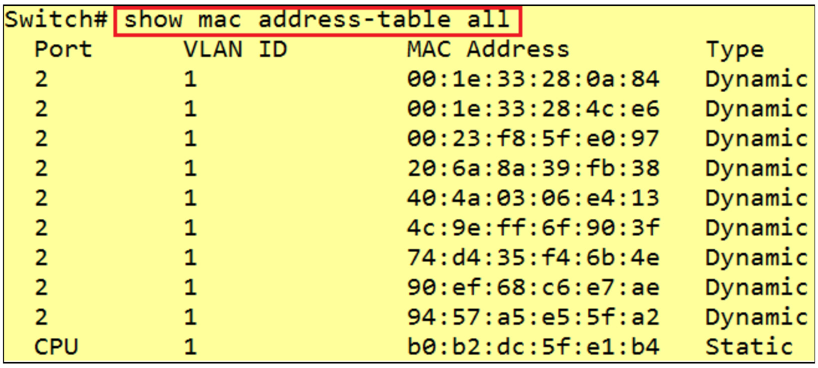
MAC table

Condition	● All ○ Static ○ MAC ○ VID ○ Port
Sort by	MAC
Transfer Type	● Dynamic to MAC forwarding ○ Dynamic to MAC filtering

Index	MAC Address	VID	Port	Type
1	00:05:5d:f3:27:ec	1	4	Dynamic
2	00:0c:29:77:6d:dc	59	16	Dynamic
3	00:0f:fe:e7:d1:45	20	T1	Dynamic
4	00:13:49:a5:e9:29	59	16	Dynamic
5	00:13:49:ab:dc:28	59	16	Dynamic
6	00:19:bb:4c:ee:3a	59	16	Dynamic
7	00:19:cb:00:00:01	50	48	Dynamic
8	00:19:cb:00:00:02	59	16	Dynamic

Using CLI:

Figure 3 Enter CLI command "show mac address-table all"



```
Switch# show mac address-table all
  Port        VLAN ID         MAC Address          Type
  2           1               00:1e:33:28:0a:84    Dynamic
  2           1               00:1e:33:28:4c:e6    Dynamic
  2           1               00:23:f8:5f:e0:97    Dynamic
  2           1               20:6a:8a:39:fb:38    Dynamic
  2           1               40:4a:03:06:e4:13    Dynamic
  2           1               4c:9e:ff:6f:90:3f    Dynamic
  2           1               74:d4:35:f4:6b:4e    Dynamic
  2           1               90:ef:68:c6:e7:ae    Dynamic
  2           1               94:57:a5:e5:5f:a2    Dynamic
  CPU         1               b0:b2:dc:5f:e1:b4    Static
```

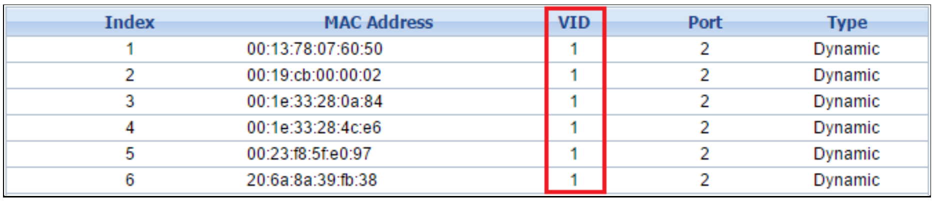
If MAC address of the device does appear, **go to step 3**.

If MAC address of the device does not appear, **go to <OTHERS>**

7.3 Is the MAC address of the device with issue being processed on the correct VID?

WebGUI:

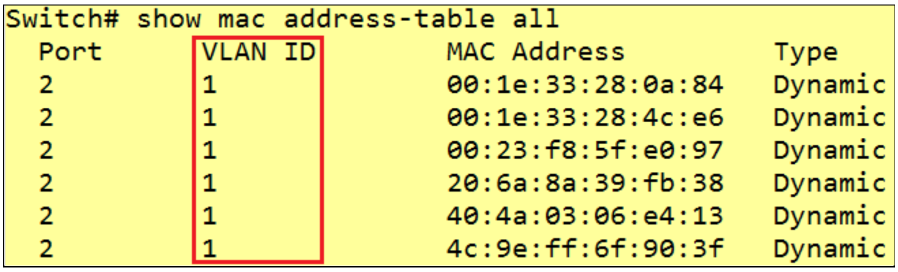
Figure 4 Management > MAC Table



Index	MAC Address	VID	Port	Type
1	00:13:78:07:60:50	1	2	Dynamic
2	00:19:cb:00:00:02	1	2	Dynamic
3	00:1e:33:28:0a:84	1	2	Dynamic
4	00:1e:33:28:4c:e6	1	2	Dynamic
5	00:23:f8:5f:e0:97	1	2	Dynamic
6	20:6a:8a:39:fb:38	1	2	Dynamic

CLI:

Figure 5 Enter CLI command "show mac address-table all"



```
Switch# show mac address-table all
  Port        VLAN ID         MAC Address          Type
  2           1               00:1e:33:28:0a:84    Dynamic
  2           1               00:1e:33:28:4c:e6    Dynamic
  2           1               00:23:f8:5f:e0:97    Dynamic
  2           1               20:6a:8a:39:fb:38    Dynamic
  2           1               40:4a:03:06:e4:13    Dynamic
  2           1               4c:9e:ff:6f:90:3f    Dynamic
```

If MAC address of the device is processed in the correct VID, **go to step 4**.

If MAC address of the device is not processed in the correct VID, **go to step 5**.

7.4 Are there any more Zyxel switches between this switch and destination?

If there are switches, access the next uplink switch and **repeat step 2.**

If there are no switches, proceed to **next agenda**.

7.5 Verify whether *device with issue*’s incoming packets are tagged or not.

This usually means that if the MAC address of the device is not processed in the configured PVID, then packets are most likely already tagged when reaching this Zyxel switch or another feature has forced the packet to be process in a different VID.

Most end devices usually sends untagged packets up the network. Devices like IP phones, Access Points, and neighboring switches, on the other hand, have the possibility of sending tagged packets.

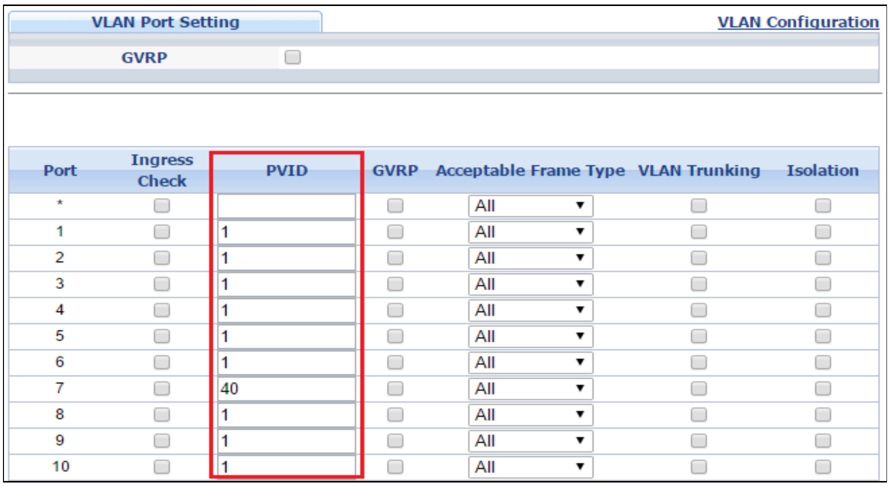
After verifying whether packets are tagged or untagged, **go to step 6**.

7.6 Is the PVID configured correctly?

The PVID decides which VLAN an untagged packet will be processed in. You can disregard PVID configurations if the downlink device has already tagged the *device with issue*’s packets correctly.

WebGUI:

Figure 6 Advance Application>VLAN>VLAN Configuration>VLAN Port Setup

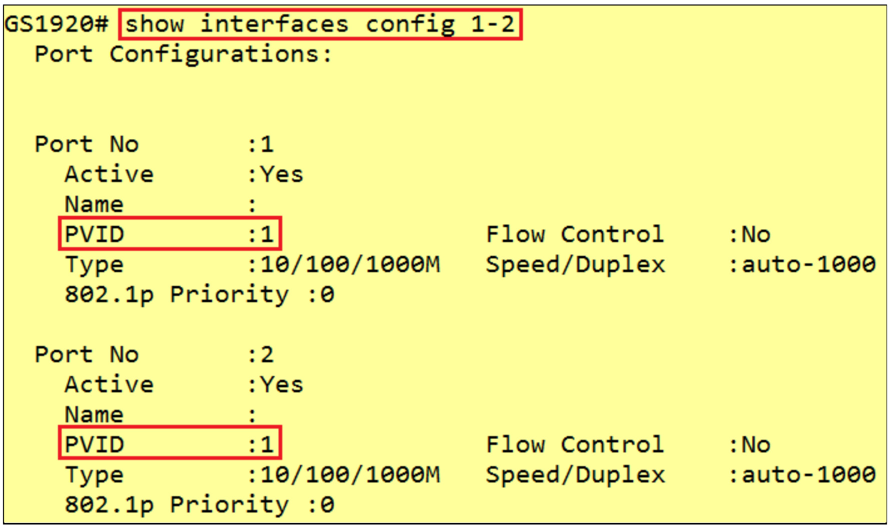


GVRP □

Port	Ingress Check	PVID	GVRP	Acceptable Frame Type	VLAN Trunking	Isolation
*	□		□	All	□	□
1	□	1	□	All	□	□
2	□	1	□	All	□	□
3	□	1	□	All	□	□
4	□	1	□	All	□	□
5	□	1	□	All	□	□
6	□	1	□	All	□	□
7	□	40	□	All	□	□
8	□	1	□	All	□	□
9	□	1	□	All	□	□
10	□	1	□	All	□	□

CLI:

Figure 7 Enter CLI command "show interface config Port-ID"



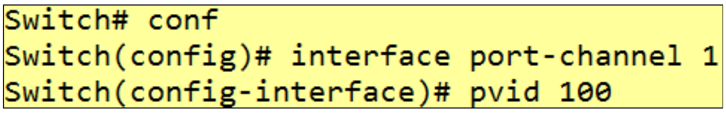
```
GS1920# show interfaces config 1-2
  Port Configurations:


  Port No        :1
    Active       :Yes
    Name         :
    PVID         :1                Flow Control     :No
    Type         :10/100/1000M     Speed/Duplex     :auto-1000
    802.1p Priority :0

  Port No        :2
    Active       :Yes
    Name         :
    PVID         :1                Flow Control     :No
    Type         :10/100/1000M     Speed/Duplex     :auto-1000
    802.1p Priority :0
```

If PVID configuration is correct, go to **step 7**.

If PVID configuration is not correct, reconfigure and return to **step 3**.

Example using CLI:

Figure 8



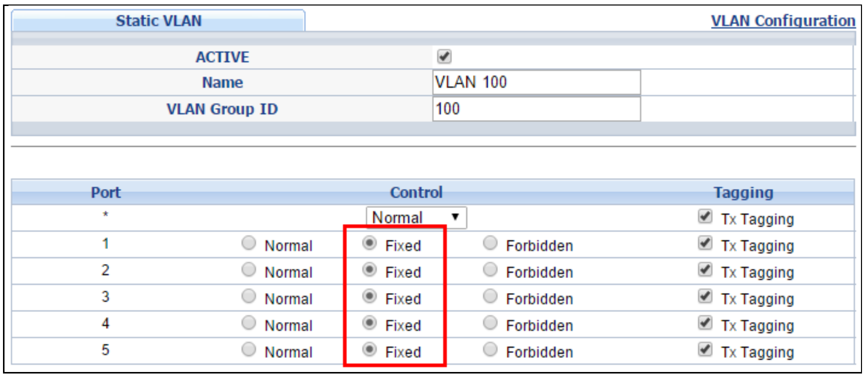
```
Switch# conf
Switch(config)# interface port-channel 1
Switch(config-interface)# pvid 100
```

7.7 Are the uplink and downlink ports fixed?

Packets can only be sent out ports that are fixed within the processed VLAN. Make sure that the port heading to the *destination* is "fixed". You will also need to fix the port going back to the *device with issue* as well to complete the communication.

Using Web GUI:

Figure 9 Advance Application > VLAN > VLAN Configuration > Static VLAN



Static VLAN

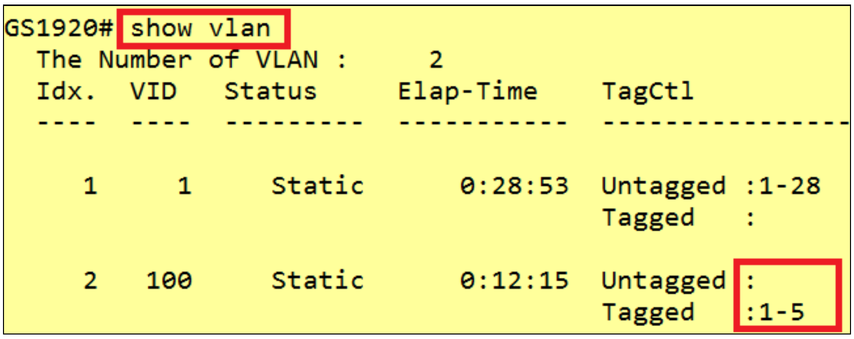
VLAN Configuration

ACTIVE	☑
Name	VLAN 100
VLAN Group ID	100

Port	Control			Tagging
*		Normal ▾		☑ Tx Tagging
1	○ Normal	● Fixed	○ Forbidden	☑ Tx Tagging
2	○ Normal	● Fixed	○ Forbidden	☑ Tx Tagging
3	○ Normal	● Fixed	○ Forbidden	☑ Tx Tagging
4	○ Normal	● Fixed	○ Forbidden	☑ Tx Tagging
5	○ Normal	● Fixed	○ Forbidden	☑ Tx Tagging

Using CLI:

Figure 10



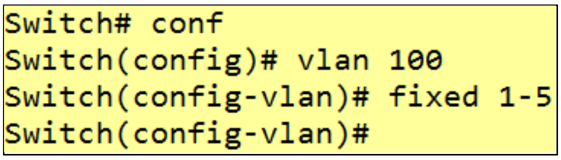
```
GS1920# show vlan
  The Number of VLAN :     2
  Idx.  VID   Status     Elap-Time    TagCtl
  ----  ----  ---------  -----------  ----------------

     1     1     Static      0:28:53  Untagged :1-28
                                      Tagged   :

     2   100     Static      0:12:15  Untagged :
                                      Tagged   :1-5
```

If a port on VLAN configuration is correct, go to **step 8**.

If ports on VLAN configuration are not correct, reconfigure and return to **step 3**.

Example using CLI:

Figure 11



```
Switch# conf
Switch(config)# vlan 100
Switch(config-vlan)# fixed 1-5
Switch(config-vlan)#
```

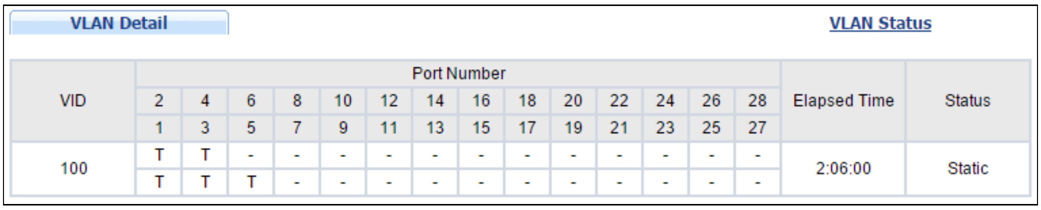
7.8 Is the egress rule configured correctly?

The egress rule indicates whether the packet going out the port should be "tagged" or "untagged". A port should generally be sending out untagged packets if the port is directly connected to an end station

(PC, laptops, printers, etc.). However, if the port is connected to a neighboring switch, or a device that has a virtual VLAN interface (IP phones, servers, routers, etc.), then the port must send tagged packets.

Using Web GUI:

Figure 12 Advance Application > VLAN > Index



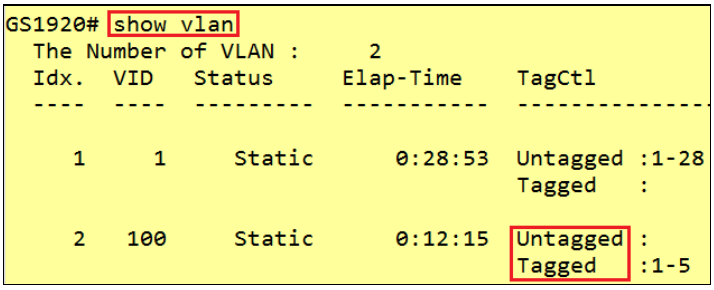
VLAN Detail VLAN Status

VID	Port Number														Elapsed Time	Status
	2	4	6	8	10	12	14	16	18	20	22	24	26	28		
	1	3	5	7	9	11	13	15	17	19	21	23	25	27		
100	T	T	-	-	-	-	-	-	-	-	-	-	-	-	2:06:00	Static
	T	T	T	-	-	-	-	-	-	-	-	-	-	-		

*Ports that are sending out tagged packets for this VLAN is labelled "T".

Using CLI:

Figure 13 Enter CLI command "show vlan"



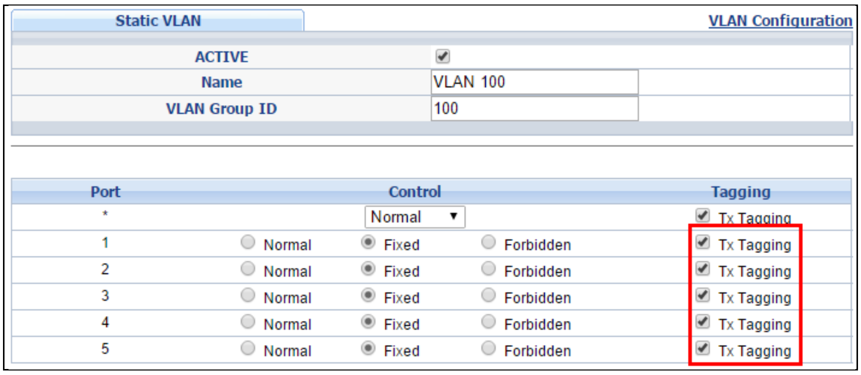
```
GS1920# show vlan
  The Number of VLAN :     2
  Idx.  VID   Status      Elap-Time    TagCtl
  ----  ----  ---------   -----------  ---------------

     1     1     Static       0:28:53  Untagged :1-28
                                       Tagged   :

     2   100     Static       0:12:15  Untagged :
                                       Tagged   :1-5
```

If a port on VLAN configuration is correct, go to **<OTHERS>**.

If a port on VLAN configuration is not correct, reconfigure and return to **step 3**.

Example using Web GUI:

Figure 14 Advance Application > VLAN > Static VLAN



Static VLAN | VLAN Configuration

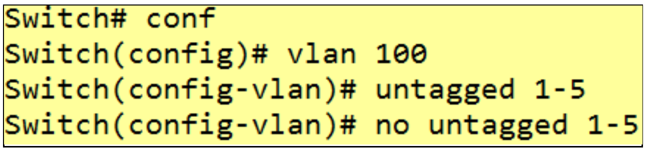
ACTIVE	☑
Name	VLAN 100
VLAN Group ID	100

Port	Control			Tagging
*	Normal ▾			☑ Tx Tagging
1	○ Normal	● Fixed	○ Forbidden	☑ Tx Tagging
2	○ Normal	● Fixed	○ Forbidden	☑ Tx Tagging
3	○ Normal	● Fixed	○ Forbidden	☑ Tx Tagging
4	○ Normal	● Fixed	○ Forbidden	☑ Tx Tagging
5	○ Normal	● Fixed	○ Forbidden	☑ Tx Tagging

*Check "Tx Tagging" if the port needs to send out tagged packets.

Example using CLI:

Figure 15



```
Switch# conf
Switch(config)# vlan 100
Switch(config-vlan)# untagged 1-5
Switch(config-vlan)# no untagged 1-5
```

*Check "Tx Tagging" if the port needs to send out tagged packets.

7.9 OTHERS:

1. Are all the physical ports at link-up status?

   Ensure all links are at link-up status. Resolve any Ethernet issues. **Move to Ethernet Troubleshooting**.

2. Is the MAC address of the *device with issue* a valid unicast MAC address?

   Only unicast MAC addresses are listed on the Zyxel switch's MAC address table.

   Examples of unicast MAC addresses:

   - 0**1**00.AAAA.BBBB
   - 2**3**01.1234.1234
   - A**9**21.FFFF.FFFF

   Where the second hex digit is either **1,3,5,7,9,B,D**, or **F**.

If the device with issue is using an invalid MAC address, **issue is not caused by the ZXEL switch**.

3. Does traffic between *device with issue* and *destination* hit any Policy Rule classifiers?

   If a policy applies to this traffic, move to **Policy Rule Troubleshooting**.

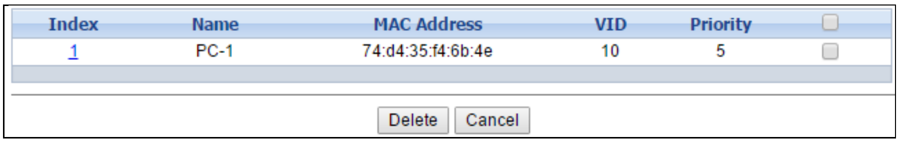
4. Does traffic between *device with issue* and *destination* hit any special VLAN criteria?

   If traffic should hit **MAC Based VLAN** criteria,

   - Verify device with issue's MAC address matches the MAC address field.
   - Verify MAC Based VLAN sends traffic to the destination's VLAN.

   Using Web GUI:

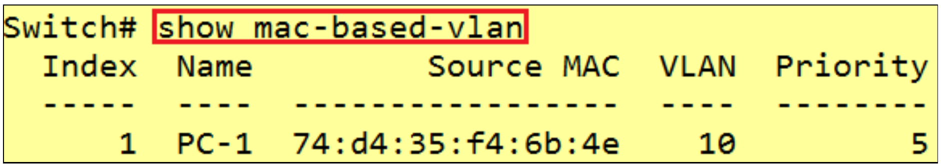
Figure 16 Advance Application > VLAN > VLAN Configuration > MAC Based VLAN Setup



Index	Name	MAC Address	VID	Priority	□
1	PC-1	74:d4:35:f4:6b:4e	10	5	□

Using CLI:

Figure 17 Enter CLI command "show mac-based-vlan"



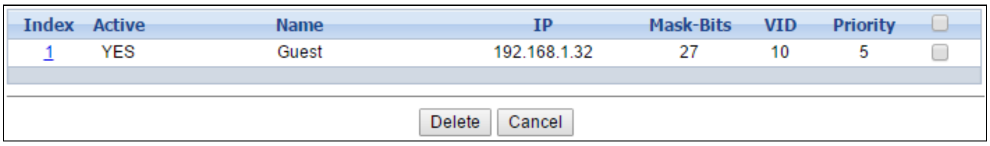
```
Switch# show mac-based-vlan
  Index  Name          Source MAC  VLAN  Priority
  -----  ----  -----------------  ----  --------
      1  PC-1  74:d4:35:f4:6b:4e    10         5
```

If traffic should hit **Subnet Based VLAN** criteria,

- Verify that *device with issue*'s IP address hits the IP address range.
- Verify that IP address range is sent to the *destination*'s VLAN.

Using Web GUI:

Figure 18 Advance Application > VLAN > VLAN Configuration > Subnet Based VLAN Setup

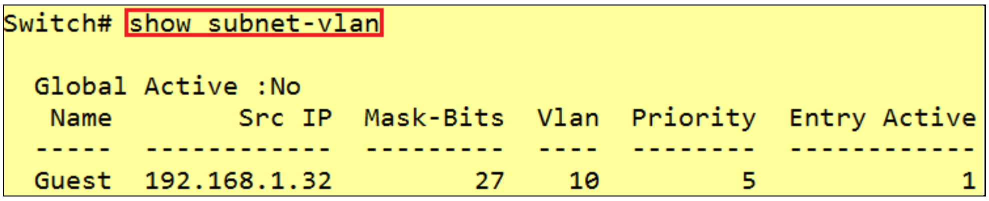


Index	Active	Name	IP	Mask-Bits	VID	Priority	□
1	YES	Guest	192.168.1.32	27	10	5	□

*This example ensures that IP address 192.168.1.32~192.168.1.63 is processed in VLAN 10.

Using CLI:

Figure 19 Enter CLI command "show subnet-vlan"



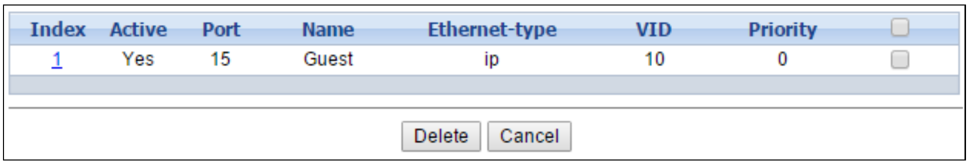
```
Switch# show subnet-vlan

  Global Active :No
   Name        Src IP   Mask-Bits  Vlan  Priority  Entry Active
  -----  ------------  ---------  ----  --------  ------------
  Guest  192.168.1.32         27    10         5             1
```

If traffic should hit **Protocol Based VLAN** criteria,

- Verify that device with issue's IP address hits the correct protocol.
- Verify that device with issue is connected under the correct port.
- Verify that protocol traffic is sent to the destination's VLAN.

Using Web GUI:

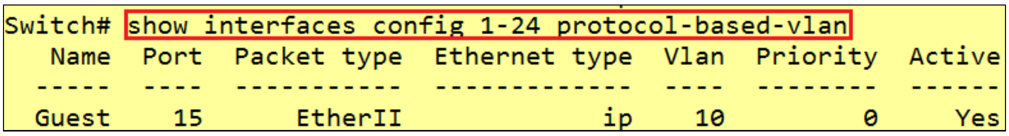
Figure 20 Advance Application > VLAN > VLAN Configuration > Protocol Based VLAN Setup



Index	Active	Port	Name	Ethernet-type	VID	Priority	□
1	Yes	15	Guest	ip	10	0	□

Using CLI:

Figure 21 Enter CLI command "show interface config Port-ID protocol-based-vlan"



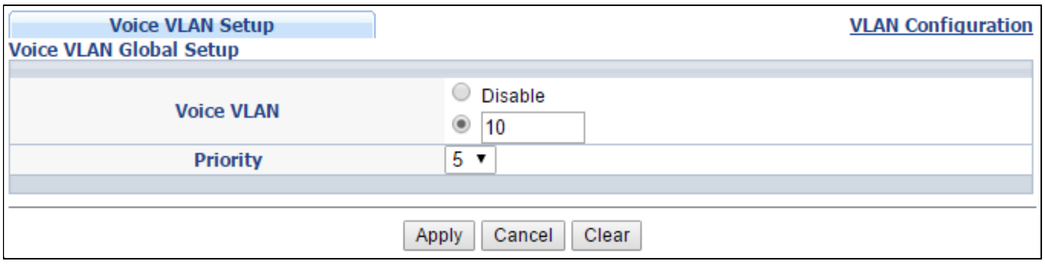
```
Switch# show interfaces config 1-24 protocol-based-vlan
   Name  Port  Packet type  Ethernet type  Vlan  Priority  Active
  -----  ----  -----------  -------------  ----  --------  ------
  Guest    15      EtherII             ip    10         0     Yes
```

If traffic should hit **Voice VLAN** criteria,

- Verify that Voice VLAN is enabled.
- Verify that traffic is sent to the destination's VLAN.

Using Web GUI:

Figure 22 Advance Application > VLAN > VLAN Configuration > Voice VLAN Setup

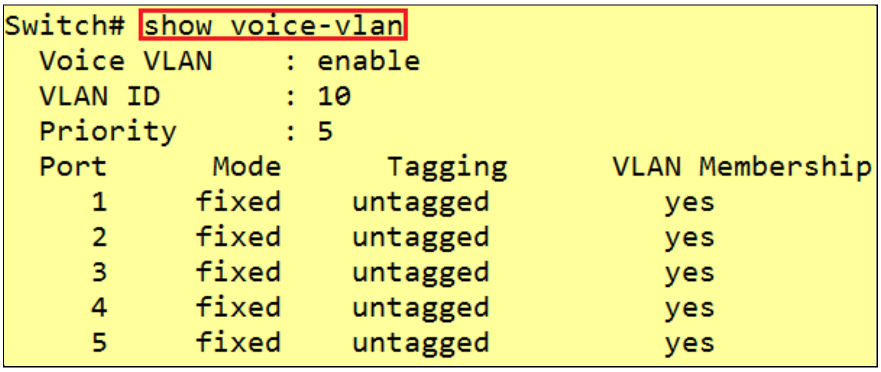


Voice VLAN Global Setup

Voice VLAN	○ Disable ● 10
Priority	5 ▼

Using CLI:

Figure 23 Enter CLI command "show voice-vlan"

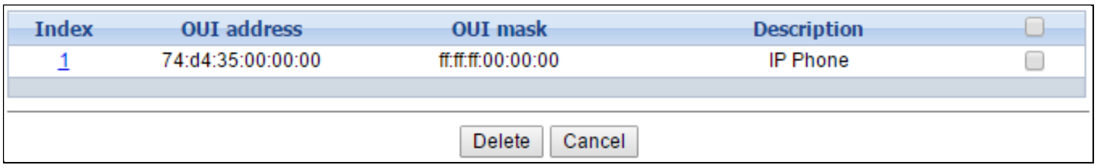


```
Switch# show voice-vlan
  Voice VLAN     : enable
  VLAN ID        : 10
  Priority       : 5
  Port       Mode      Tagging      VLAN Membership
     1      fixed     untagged          yes
     2      fixed     untagged          yes
     3      fixed     untagged          yes
     4      fixed     untagged          yes
     5      fixed     untagged          yes
```

- Verify that device with issue's MAC address hits the OUI address.
- Verify that the OUI mask is configured according to the correct format.

Using Web GUI:

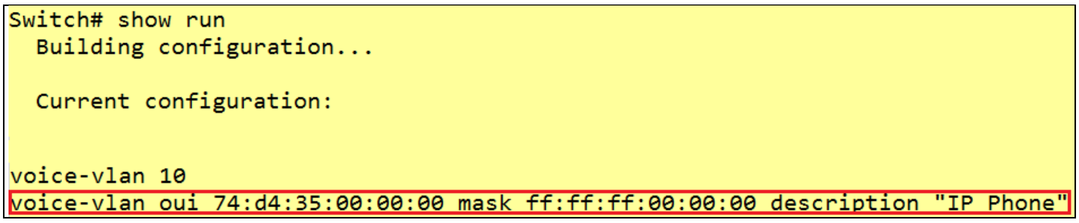
Figure 24 Advance Application > VLAN > VLAN Configuration > Voice VLAN Setup



Index	OUI address	OUI mask	Description	□
1	74:d4:35:00:00:00	ff:ff:ff:00:00:00	IP Phone	□

Using CLI:

Figure 25

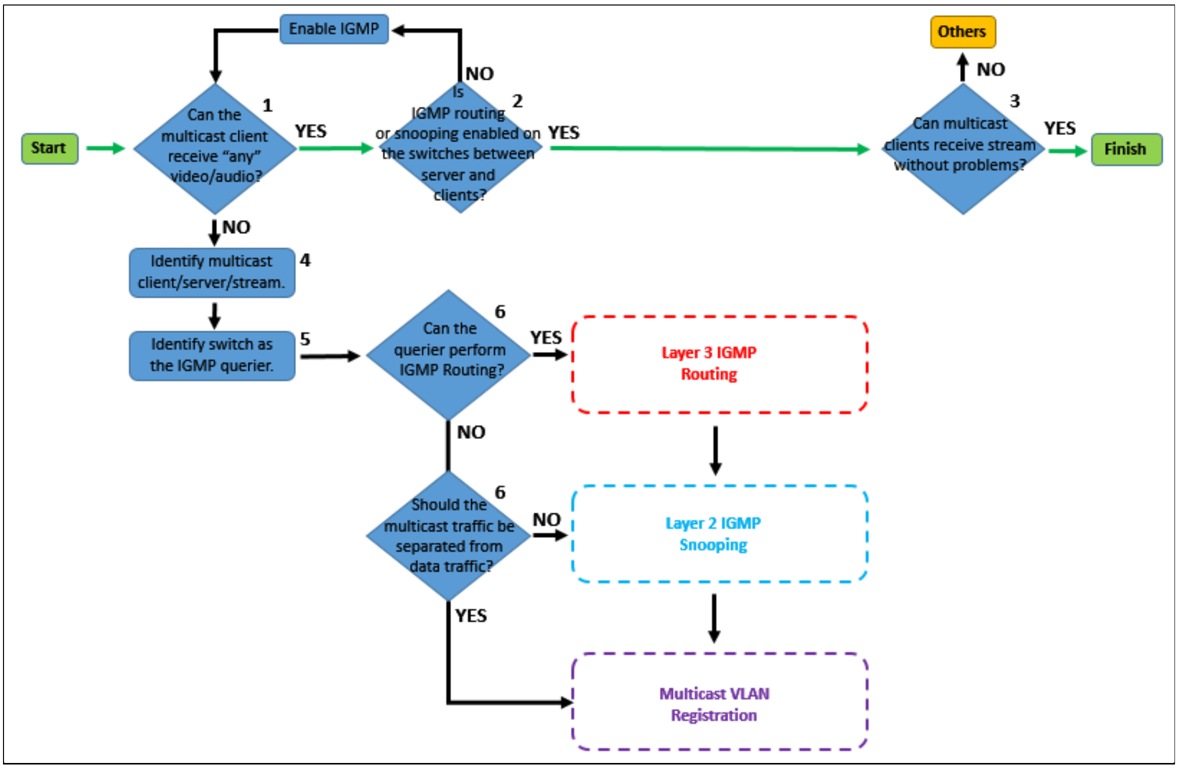


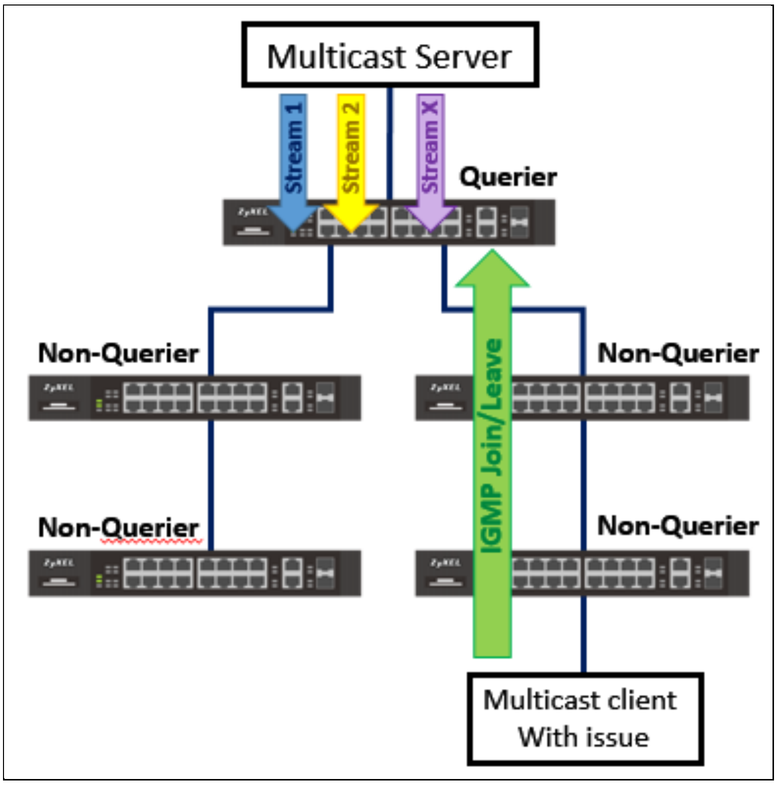
```
Switch# show run
  Building configuration...

  Current configuration:


voice-vlan 10
voice-vlan oui 74:d4:35:00:00:00 mask ff:ff:ff:00:00:00 description "IP Phone"
```

After verifying and reconfiguring the special VLAN criteria, go back to **step 3**.

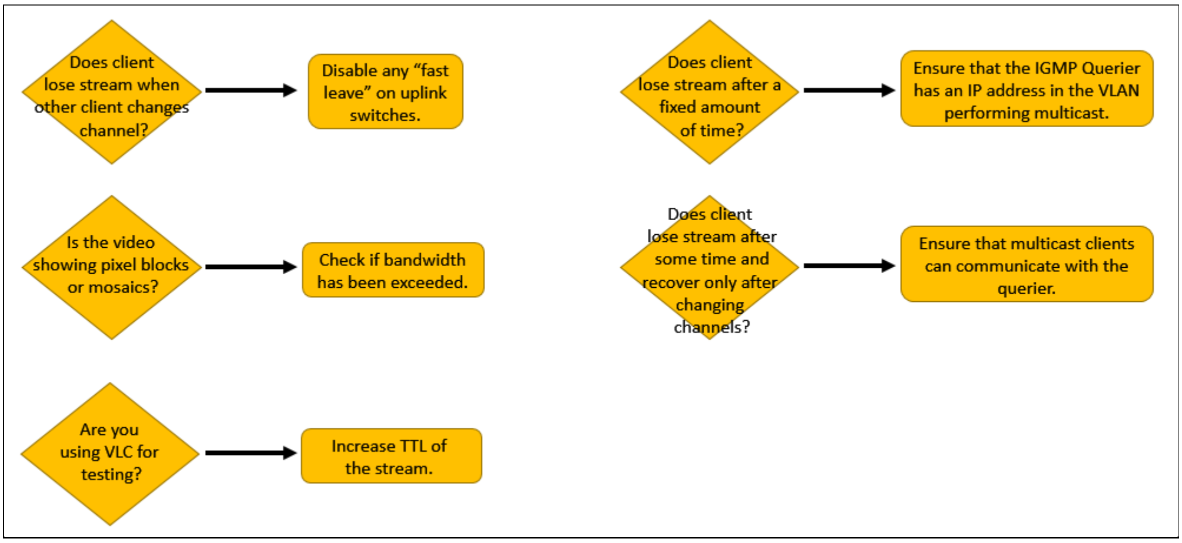
8 Troubleshooting for Multicast

Flowchart:


Enable IGMP
Others
Start
1
Can the multicast client receive "any" video/audio?
YES
NO
2
Is IGMP routing or snooping enabled on the switches between server and clients?
YES
NO
3
Can multicast clients receive stream without problems?
YES
NO
Finish
4
Identify multicast client/server/stream.
5
Identify switch as the IGMP querier.
6
Can the querier perform IGMP Routing?
YES
NO
Layer 3 IGMP Routing
6
Should the multicast traffic be separated from data traffic?
NO
YES
Layer 2 IGMP Snooping
Multicast VLAN Registration


Multicast Server
Stream 1
Stream 2
Stream X
Querier
Non-Querier
Non-Querier
Non-Querier
Non-Querier
IGMP Join/Leave
Multicast client
With issue

OTHERS:


Does client lose stream when other client changes channel?
Disable any "fast leave" on uplink switches.
Is the video showing pixel blocks or mosaics?
Check if bandwidth has been exceeded.
Are you using VLC for testing?
Increase TTL of the stream.
Does client lose stream after a fixed amount of time?
Ensure that the IGMP Querier has an IP address in the VLAN performing multicast.
Does client lose stream after some time and recover only after changing channels?
Ensure that multicast clients can communicate with the querier.

8.1 Can the multicast client with issue receive "any" video or audio?

There is a difference between clients receiving no stream and clients receiving poor stream.

Figure 1 Good Stream

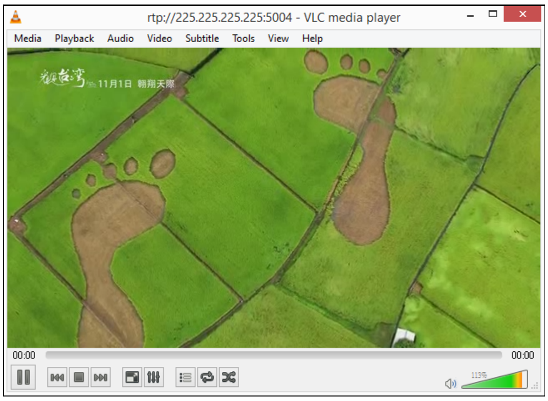
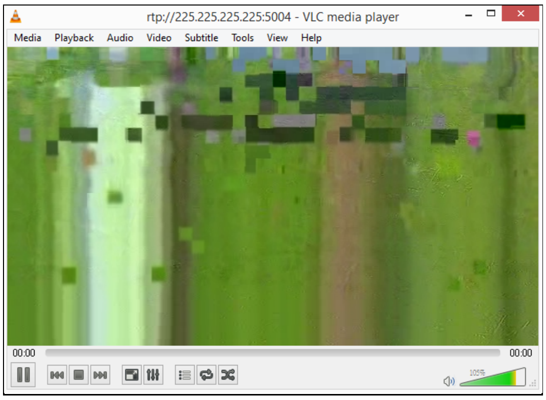


Figure 2 Poor stream (mosaic and blur)


rtp://225.225.225.225:5004 - VLC media player
Media Playback Audio Video Subtitle Tools View Help
00:00
00:00

When a multicast client receives no stream, two things may occur:

- Screen remains dark and no video nor audio.
- Image remains frozen right before joining/leaving a different multicast stream

If the multicast client receives stream but with poor quality, **go to step 2**.

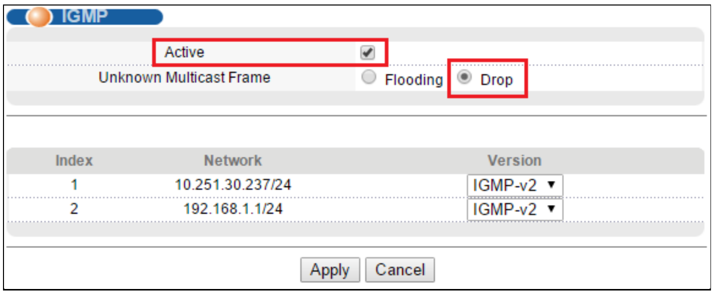
If the multicast client does not receive any stream from any multicast address, **go to step 4**.

8.2 Is IGMP routing or snooping enabled with "unknown multicast frames: drop" on the switches between server and clients?

An IPTV service can still function even without IGMP enabled. The purpose of IGMP is actually to optimize bandwidth within the network by preventing unwanted multicast flooding.

Using Web GUI:

Figure 3 IP Application > IGMP

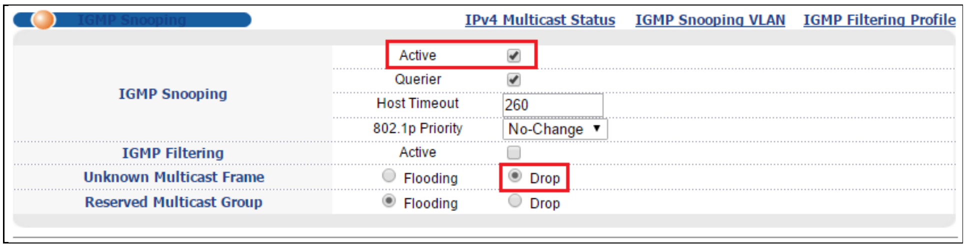


Active ☑

Unknown Multicast Frame ○ Flooding ● Drop

Index	Network	Version
1	10.251.30.237/24	IGMP-v2 ▼
2	192.168.1.1/24	IGMP-v2 ▼

Figure 4 Advance Application > Multicast > IPv4 Multicast > IGMP Snooping



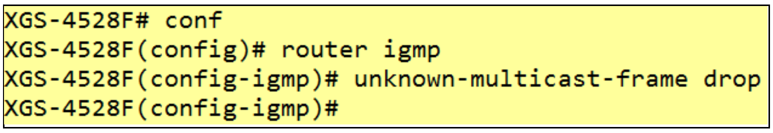
IGMP Snooping

IPv4 Multicast Status IGMP Snooping VLAN IGMP Filtering Profile

IGMP Snooping	Active	☑
	Querier	☑
	Host Timeout	260
	802.1p Priority	No-Change ▾
IGMP Filtering	Active	□
Unknown Multicast Frame	○ Flooding	● Drop
Reserved Multicast Group	● Flooding	○ Drop

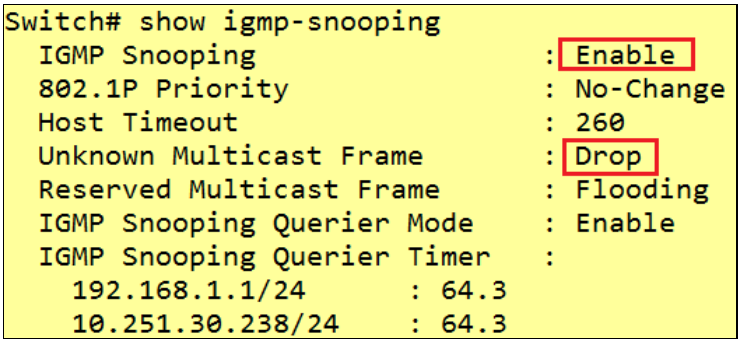
Using CLI:

Figure 5 Layer 3 IGMP Routing



```
XGS-4528F# conf
XGS-4528F(config)# router igmp
XGS-4528F(config-igmp)# unknown-multicast-frame drop
XGS-4528F(config-igmp)#
```

Figure 6 Layer 2 IGMP Snooping



```
Switch# show igmp-snooping
  IGMP Snooping                   : Enable
  802.1P Priority                 : No-Change
  Host Timeout                    : 260
  Unknown Multicast Frame         : Drop
  Reserved Multicast Frame        : Flooding
  IGMP Snooping Querier Mode      : Enable
  IGMP Snooping Querier Timer     :
    192.168.1.1/24       : 64.3
    10.251.30.238/24     : 64.3
```

If IGMP "unknown multicast frame: drop" is not enabled on the switches between server clients, reconfigure the switches and **repeat step 1**.

If IGMP "unknown multicast frame: drop" is already enabled, **go to step 3**.

8.3 Can multicast clients receive stream without problems?

Verify this by watching the video and switching channels on the set-top box.

If video quality is still poor or clients lose stream at irregular intervals, **go to <OTHERS>**. If no issues occur, proceed to the **next agenda**.

8.4 Identify the multicast clients, multicast servers, and multicast stream with issue.

There are three main factors to consider when dealing with multicast:

a. Which multicast clients are affected?

b. Where is the multicast server located? Server should be directly connected to the IGMP querier.

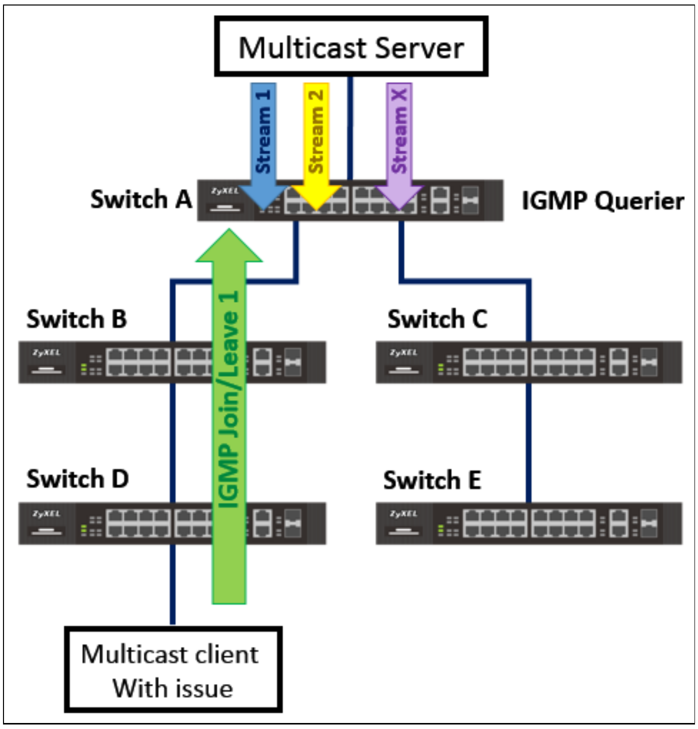
c. Which multicast addresses being streamed have this issue?

Once you have confirmed these three information, **go to step 5**.

8.5 Identify which switch is the IGMP querier.

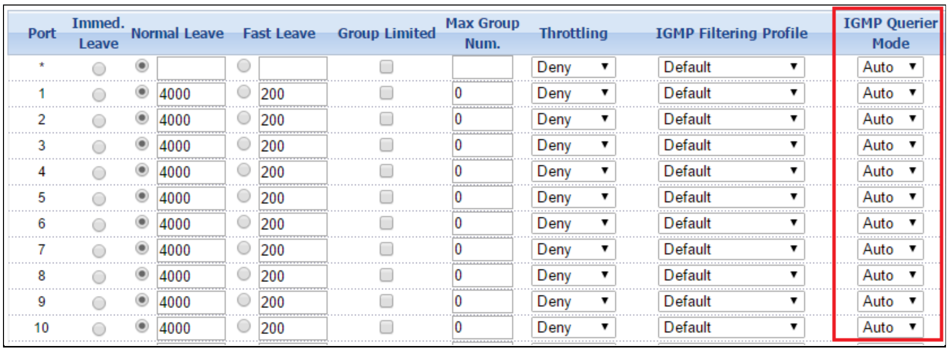
In this example, Switch A is the IGMP querier because the multicast server sends the multicast stream directly to Switch A.

Figure 7



If all switch in between server and client are using the defult IGMP querier port mode "auto", then we can disregard Switch C and Switch E. The IGMP Join/Leave of the **multicast client with issue** will travel across

Figure 8 Switch B and Switch D only.



Port	Immed. Leave	Normal Leave	Fast Leave	Group Limited	Max Group Num.	Throttling	IGMP Filtering Profile	IGMP Querier Mode
*	○	●	○	□		Deny	Default	Auto
1	○	● 4000	○ 200	□	0	Deny	Default	Auto
2	○	● 4000	○ 200	□	0	Deny	Default	Auto
3	○	● 4000	○ 200	□	0	Deny	Default	Auto
4	○	● 4000	○ 200	□	0	Deny	Default	Auto
5	○	● 4000	○ 200	□	0	Deny	Default	Auto
6	○	● 4000	○ 200	□	0	Deny	Default	Auto
7	○	● 4000	○ 200	□	0	Deny	Default	Auto
8	○	● 4000	○ 200	□	0	Deny	Default	Auto
9	○	● 4000	○ 200	□	0	Deny	Default	Auto
10	○	● 4000	○ 200	□	0	Deny	Default	Auto

*IGMP Querier Mode: Auto allows non-queriers to forward join/leave request towards direction of the querier.

Once you have determined the path of the IGMP join/leave requests, **go to step 6**.

8.6 Can the querier or Zyxel switch directly connected to the multicast server perform Layer 3 IGMP Routing?

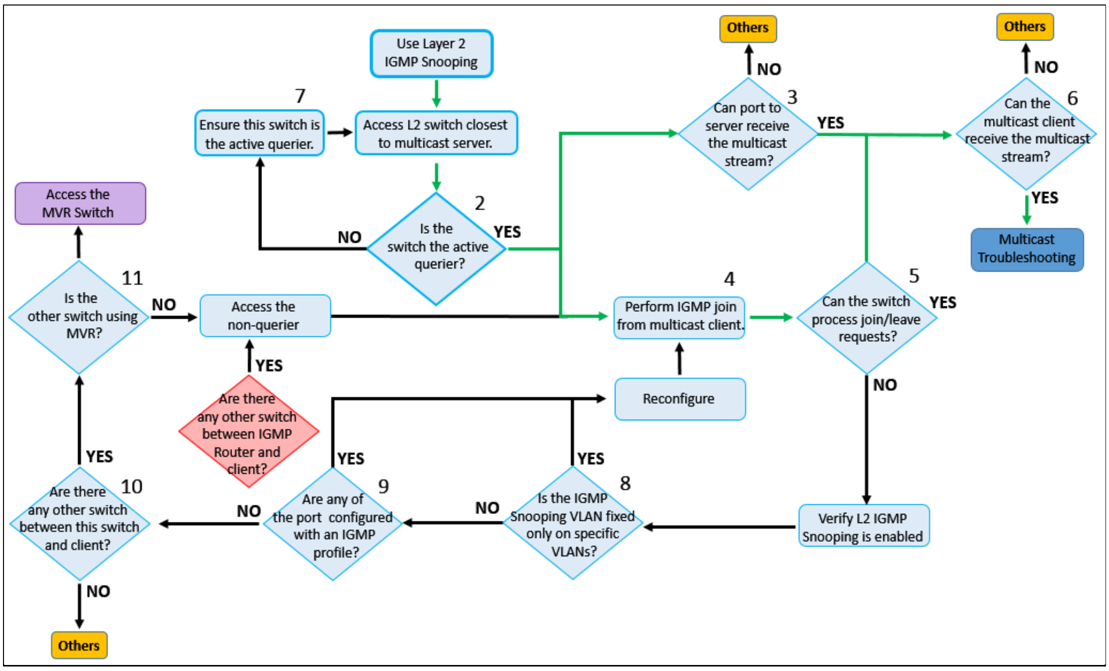
Layer 3 IGMP Routing and Layer 2 IGMP Snooping have very different configurations available. If the querier is also the gateway of the local clients, then use Layer 3 IGMP Routing.

If the querier is using Layer 3 IGMP Routing, proceed to the Layer 3 IGMP Routing section.

If the querier is not capable of using Layer 3 IGMP Routing, proceed to the Layer 2 IGMP Snooping section.

9 Troubleshooting for Layer 2 IGMP Snooping

Flowchart:


Use Layer 2 IGMP Snooping
7
Ensure this switch is the active querier.
Access L2 switch closest to multicast server.
2
Is the switch the active querier?
NO
YES
Others
NO
3
Can port to server receive the multicast stream?
YES
Others
NO
6
Can the multicast client receive the multicast stream?
YES
Multicast Troubleshooting
Access the MVR Switch
11
Is the other switch using MVR?
NO
Access the non-querier
YES
Are there any other switch between IGMP Router and client?
4
Perform IGMP join from multicast client.
5
Can the switch process join/leave requests?
YES
NO
Reconfigure
YES
YES
10
Are there any other switch between this switch and client?
NO
9
Are any of the port configured with an IGMP profile?
NO
8
Is the IGMP Snooping VLAN fixed only on specific VLANs?
Verify L2 IGMP Snooping is enabled
YES
NO
Others

9.1 Access the switch using Layer 2 IGMP Snooping closest to the multicast server.

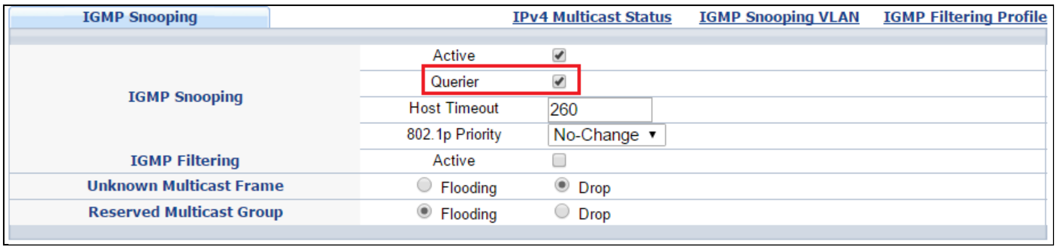
9.2 Is the switch the active querier?

By default, querier is disabled on the Zyxel switch using IGMP Snooping. There are two things that needs to be verified in check whether or not the switch is the active querier.

1. IGMP querier mode is globally enabled.

   Using Web GUI:

Figure 9 Advance Application > Multicast > IPv4 Multicast > IGMP Snooping

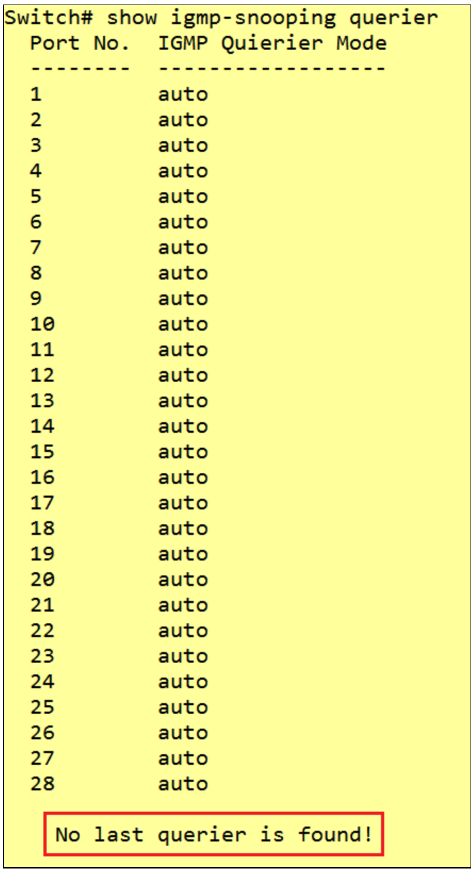


IGMP Snooping	Active	☑
	Querier	☑
	Host Timeout	260
	802.1p Priority	No-Change ▾
IGMP Filtering	Active	□
Unknown Multicast Frame	○ Flooding	● Drop
Reserved Multicast Group	● Flooding	○ Drop

2. The CLI shows a "No last querier is found".

   Using CLI:

Figure 10 Enter CLI command "show igmp-snooping querier"



```
Switch# show igmp-snooping querier
  Port No.  IGMP Quierier Mode
  --------  -----------------
  1         auto
  2         auto
  3         auto
  4         auto
  5         auto
  6         auto
  7         auto
  8         auto
  9         auto
  10        auto
  11        auto
  12        auto
  13        auto
  14        auto
  15        auto
  16        auto
  17        auto
  18        auto
  19        auto
  20        auto
  21        auto
  22        auto
  23        auto
  24        auto
  25        auto
  26        auto
  27        auto
  28        auto

    No last querier is found!
```

*The "No last querier is found" only means that there are no other active IGMP queriers in the network. This does not indicate whether this device is the active IGMP querier.

If both indicates that the switch is the active querier, **go to step 3**.

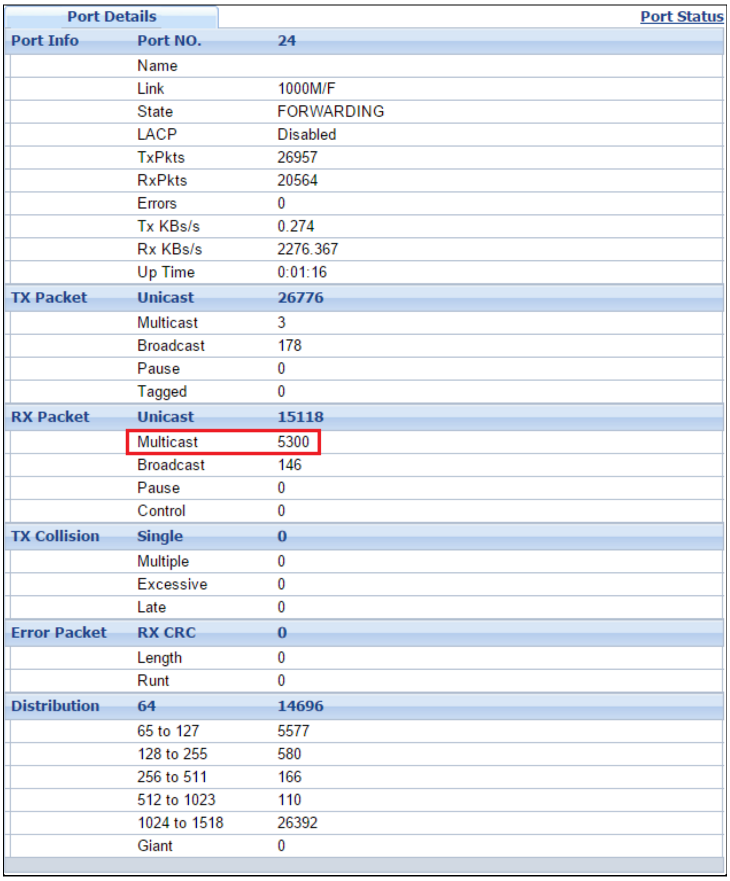
If both does not indicate that the switch is the active querier, **go to step 8**.

9.3 Can the Zyxel switch receive the multicast stream?

You can verify whether the switch is receiving multicast frames by looking at the **port counters**. Locate the port of the switch in the direction of the **multicast server**. Afterwards, check the port counters for *received multicast packets*. Check the port counters again after a few seconds. A consistent increase of received multicast packets is an indication that the port is receiving multicast streams.

Using Web GUI:

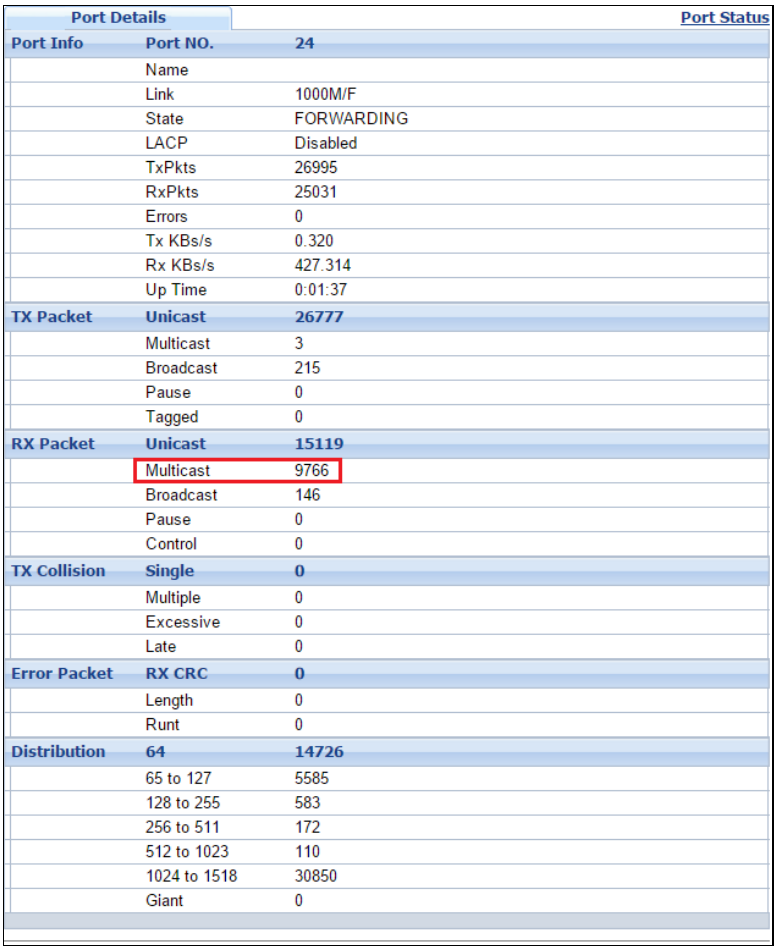
Figure 11 Status (Homepage) > Port Status > Port <*number*>



Port Details | Port Status

Port Info	**Port NO.**	**24**
	Name	
	Link	1000M/F
	State	FORWARDING
	LACP	Disabled
	TxPkts	26957
	RxPkts	20564
	Errors	0
	Tx KBs/s	0.274
	Rx KBs/s	2276.367
	Up Time	0:01:16
TX Packet	**Unicast**	**26776**
	Multicast	3
	Broadcast	178
	Pause	0
	Tagged	0
RX Packet	**Unicast**	**15118**
	Multicast	5300
	Broadcast	146
	Pause	0
	Control	0
TX Collision	**Single**	**0**
	Multiple	0
	Excessive	0
	Late	0
Error Packet	**RX CRC**	**0**
	Length	0
	Runt	0
Distribution	**64**	**14696**
	65 to 127	5577
	128 to 255	580
	256 to 511	166
	512 to 1023	110
	1024 to 1518	26392
	Giant	0

Figure 12

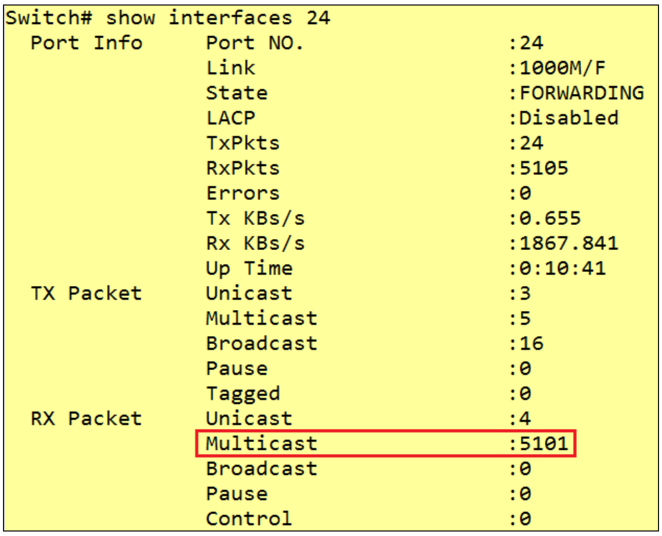


Port Details | Port Status

Port Info	**Port NO.**	**24**
	Name	
	Link	1000M/F
	State	FORWARDING
	LACP	Disabled
	TxPkts	26995
	RxPkts	25031
	Errors	0
	Tx KBs/s	0.320
	Rx KBs/s	427.314
	Up Time	0:01:37
TX Packet	**Unicast**	**26777**
	Multicast	3
	Broadcast	215
	Pause	0
	Tagged	0
RX Packet	**Unicast**	**15119**
	Multicast	9766
	Broadcast	146
	Pause	0
	Control	0
TX Collision	**Single**	**0**
	Multiple	0
	Excessive	0
	Late	0
Error Packet	**RX CRC**	**0**
	Length	0
	Runt	0
Distribution	**64**	**14726**
	65 to 127	5585
	128 to 255	583
	256 to 511	172
	512 to 1023	110
	1024 to 1518	30850
	Giant	0

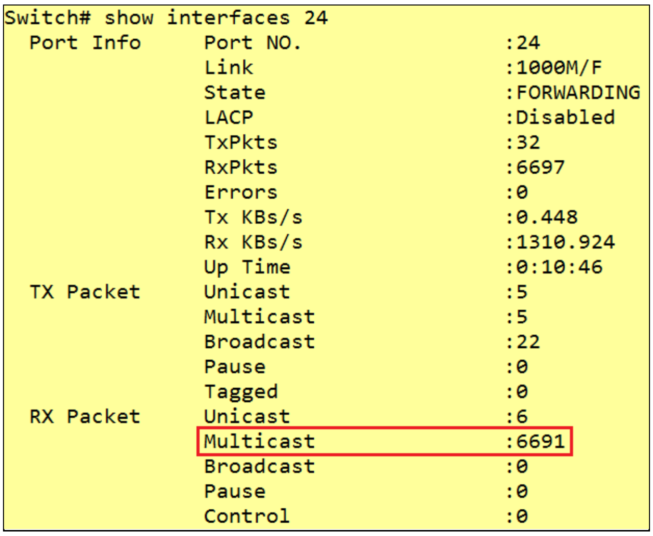
Using CLI:

Figure 13 Enter CLI command “show interface Port-ID”



```
Switch# show interfaces 24
  Port Info      Port NO.                :24
                 Link                    :1000M/F
                 State                   :FORWARDING
                 LACP                    :Disabled
                 TxPkts                  :24
                 RxPkts                  :5105
                 Errors                  :0
                 Tx KBs/s                :0.655
                 Rx KBs/s                :1867.841
                 Up Time                 :0:10:41
  TX Packet      Unicast                 :3
                 Multicast               :5
                 Broadcast               :16
                 Pause                   :0
                 Tagged                  :0
  RX Packet      Unicast                 :4
                 Multicast               :5101
                 Broadcast               :0
                 Pause                   :0
                 Control                 :0
```

Figure 14



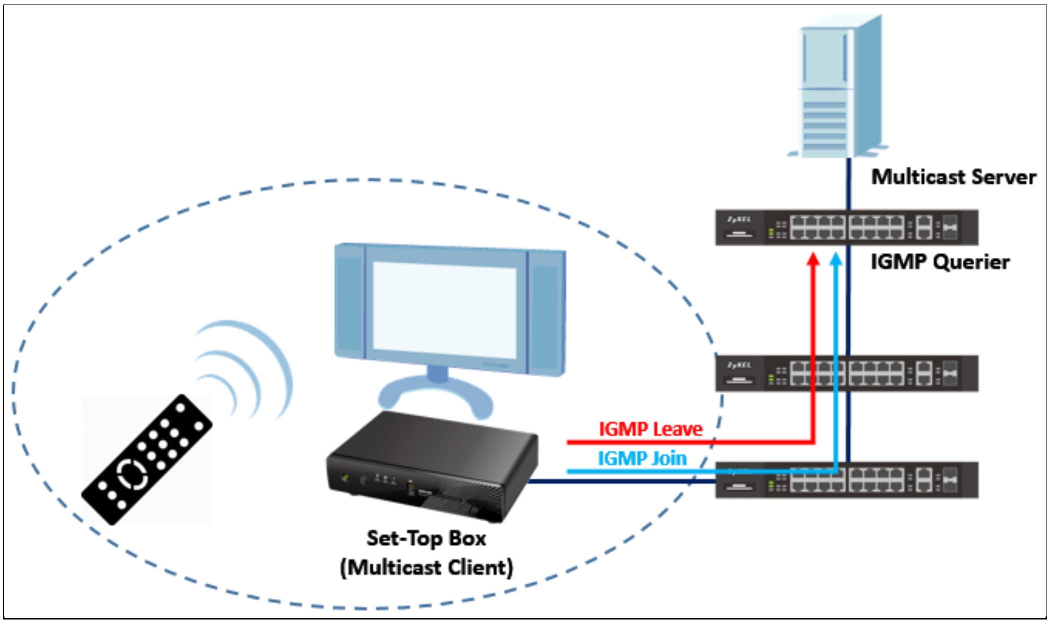
```
Switch# show interfaces 24
  Port Info      Port NO.                :24
                 Link                    :1000M/F
                 State                   :FORWARDING
                 LACP                    :Disabled
                 TxPkts                  :32
                 RxPkts                  :6697
                 Errors                  :0
                 Tx KBs/s                :0.448
                 Rx KBs/s                :1310.924
                 Up Time                 :0:10:46
  TX Packet      Unicast                 :5
                 Multicast               :5
                 Broadcast               :22
                 Pause                   :0
                 Tagged                  :0
  RX Packet      Unicast                 :6
                 Multicast               :6691
                 Broadcast               :0
                 Pause                   :0
                 Control                 :0
```

*This shows the difference in port counters, from left to right, in the span of a few seconds.

If the switch can receive the multicast stream, **go to step 4**.

If the switch cannot receive the multicast stream, **go to<OTHERS>**.

9.4 Perform an IGMP Join/Leave from the multicast client.



* Figure shows what occurs when a channel is changed through an IPTV's point of view.

Access the **multicast client** with issue (usually the set-top box of an IPTV), and start changing IPTV from one channel to **the channel with the multicast issue** (if any). Every time a channel changes, the set-top box sends an IGMP Join for the new channel as well an IGMP Leave for the old channel.

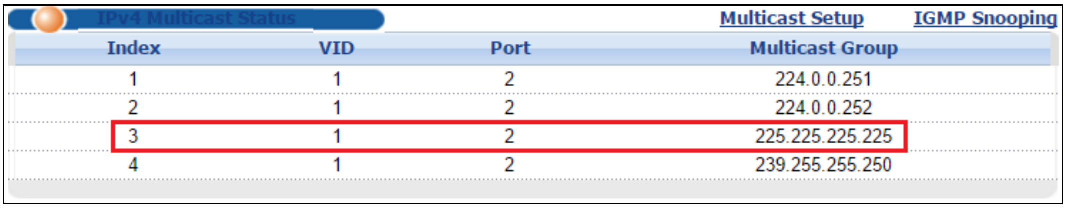
After performing an IGMP Join/Leave, proceed to **step 5**.

9.5 Did the Zyxel switch receive the IGMP Join/Leave from the multicast client?

After you perform the **IGMP join/leave**, the multicast address should appear in the multicast table. The appearance of the multicast address indicates that the switch can successfully receive the **IGMP join/leave**.

Using Web GUI:

Figure 15 Advance Application > Multicast



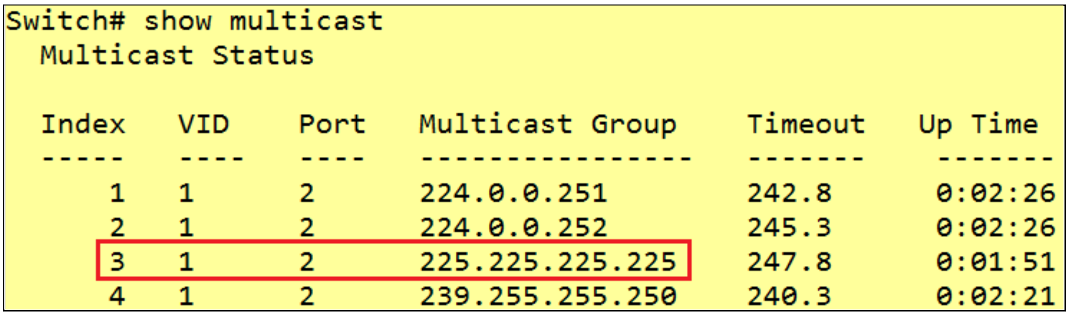
IPv4 Multicast Status

Multicast Setup IGMP Snooping

Index	VID	Port	Multicast Group
1	1	2	224.0.0.251
2	1	2	224.0.0.252
3	1	2	225.225.225.225
4	1	2	239.255.255.250

Using CLI:

Figure 16 Enter CLI command "show multicast"



```
Switch# show multicast
  Multicast Status

  Index    VID     Port    Multicast Group     Timeout    Up Time
  -----    ----    ----    ---------------     -------    -------
      1    1       2       224.0.0.251         242.8      0:02:26
      2    1       2       224.0.0.252         245.3      0:02:26
      3    1       2       225.225.225.225     247.8      0:01:51
      4    1       2       239.255.255.250     240.3      0:02:21
```

If the switch can receive the IGMP Join/Leave, proceed to **step 6**.

If the switch cannot receive the IGMP Join/Leave, ensure that IGMP snooping is enabled and go to **step 9**.

9.6 Can the multicast client receive the multicast stream?

If both **multicast stream** and **IGMP join/leave** reaches this switch, then the multicast client with issue should most likely be able to watch the channel through the IPTV.

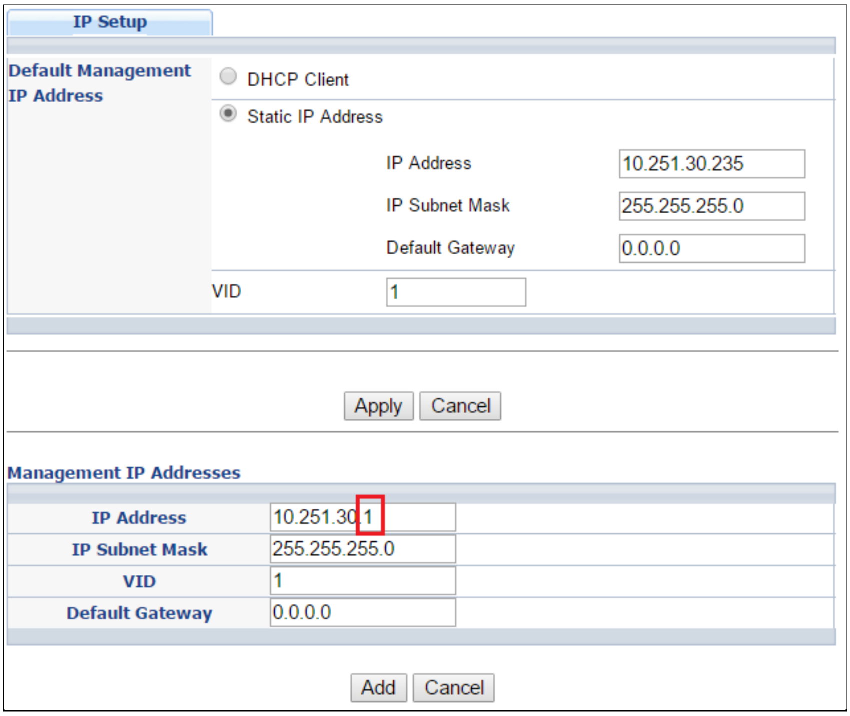
If the multicast client can now receive the multicast stream, **repeat the Multicast Troubleshooting section**.
If the multicast client still can receive the multicast stream, **go to<OTHERS>**.

9.7 Ensure that the Zyxel switch using Layer 2 IGMP Snooping is the active querier.

When two devices have querier mode enabled, the device with the **lower IP address** will assume the role of the active querier. In this case, we can configure the interface IP address of the IGMP querier to the lowest possible IP address in the network.

Using Web GUI:

Figure 17 Basic Setting > IP Setup



IP Setup

Default Management IP Address

○ DHCP Client
● Static IP Address

IP Address	10.251.30.235
IP Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
VID	1

Apply Cancel

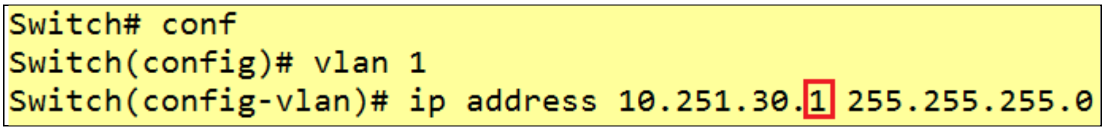
Management IP Addresses

IP Address	10.251.30.1
IP Subnet Mask	255.255.255.0
VID	1
Default Gateway	0.0.0.0

Add Cancel

Using CLI:

Figure 18



```
Switch# conf
Switch(config)# vlan 1
Switch(config-vlan)# ip address 10.251.30.1 255.255.255.0
```

In this example, the network in VLAN 1 is 10.251.30.0/24. Configuring the IP address to 10.251.30.1 will ensure that this device will be the active querier in VLAN 1.

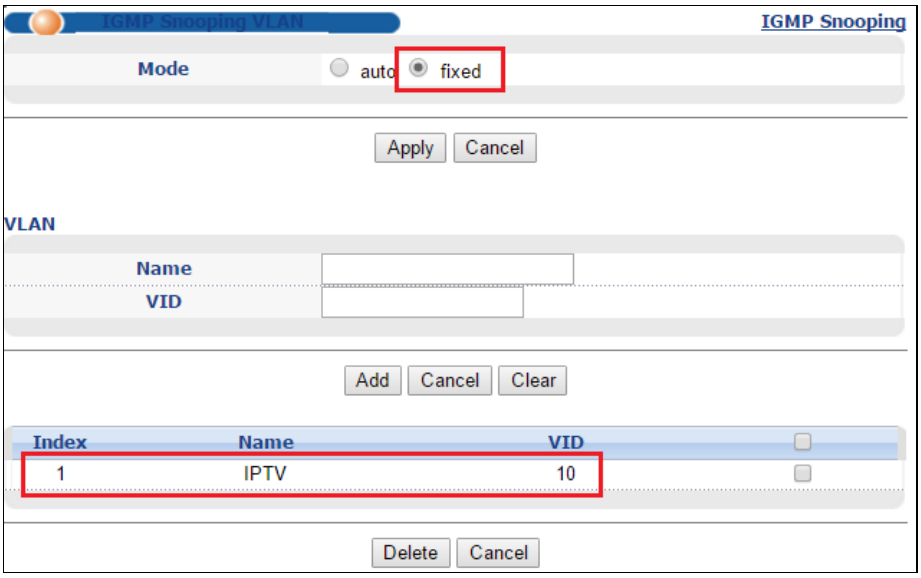
After reconfiguring the IP address of the IGMP querier's interface, **repeat step 2**.

9.8 Is the IGMP Snooping VLAN fixed only on specific VLANs?

By default, IGMP join/leave are processed in all VLAN. If the **IGMP snooping VLAN** is configured as "**Fixed**", this means that only IGMP join/leave from the configured IGMP snooping VLAN lists are processed. In this case, either reconfigure the mode to "**Auto**", or configure the VLAN where multicast clients are being processed.

Using Web GUI:

Figure 19 Advance Application > Multicast > IPv4 Multicast > IGMP Snooping > IGMP Snooping VLAN

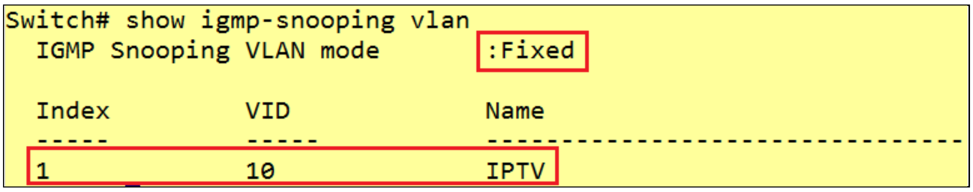


Mode ○ auto ● fixed

Index	Name	VID	□
1	IPTV	10	□

Using CLI:

Figure 20 Enter CLI command “show igmp-snooping vlan”



```
Switch# show igmp-snooping vlan
  IGMP Snooping VLAN mode        :Fixed

  Index          VID             Name
  -----          -----           --------------------------------
  1              10              IPTV
```

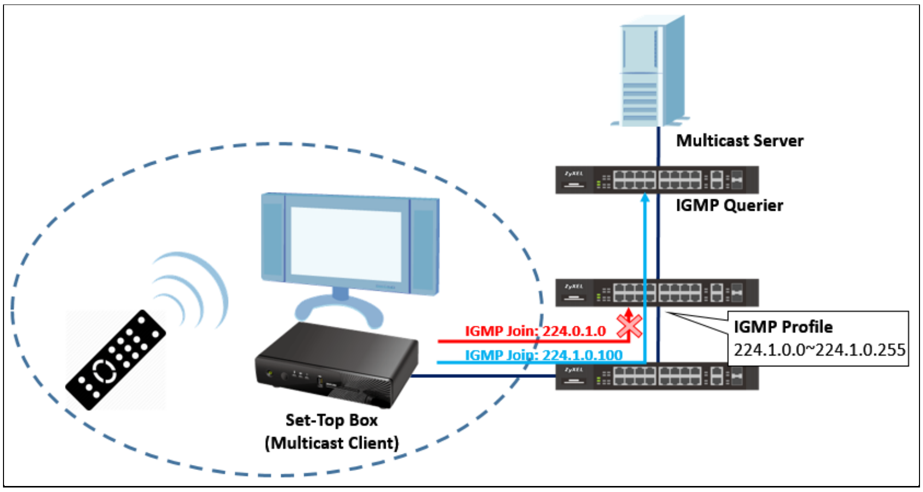
If the switch is either using “Auto” or “Fixed” with the configured VLAN, proceed to **step 9**.

If the switch has “Fixed” configured but did not configure the VLAN of multicast clients, reconfigure and **repeat step 4**.

9.9 Are any of the port configured with an IGMP filtering profile?

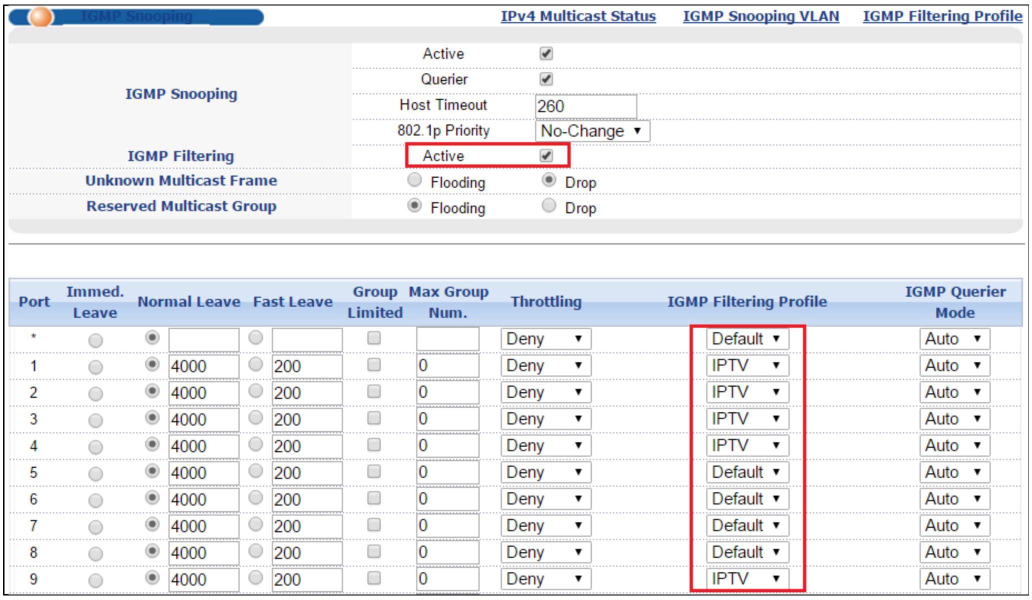
By default, **IGMP filtering** is disabled. If the switch has IGMP filtering **enabled** and is not using the **default filtering profile**, make sure that the ports are using an IGMP filtering profile whose **range** matches the **multicast addresses clients with issue** will need.

Figure 21



Using Web GUI:

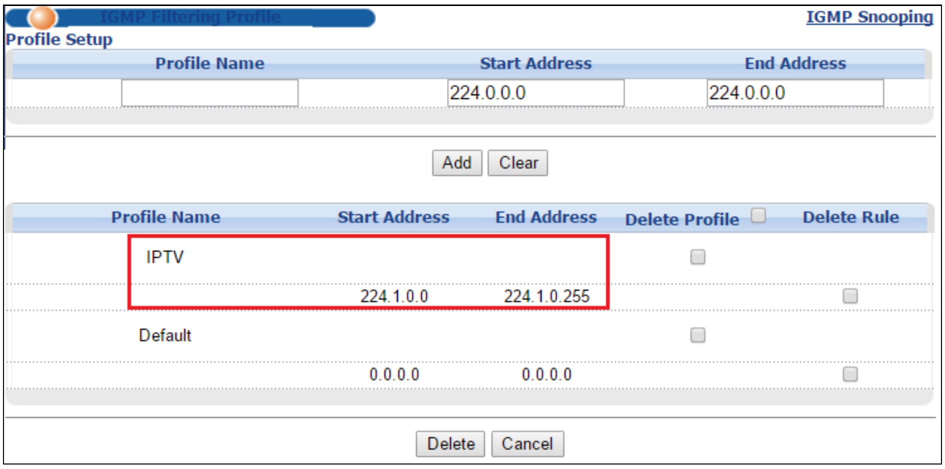
Figure 22 Advance Application > Multicast > IPv4 Multicast > IGMP Snooping



IGMP Snooping	Active	☑
	Querier	☑
	Host Timeout	260
	802.1p Priority	No-Change ▾
IGMP Filtering	Active	☑
Unknown Multicast Frame	○ Flooding	● Drop
Reserved Multicast Group	● Flooding	○ Drop

Port	Immed. Leave	Normal Leave	Fast Leave	Group Limited	Max Group Num.	Throttling	IGMP Filtering Profile	IGMP Querier Mode
*	○	●	○	□		Deny ▾	Default ▾	Auto ▾
1	○	● 4000	○ 200	□	0	Deny ▾	IPTV ▾	Auto ▾
2	○	● 4000	○ 200	□	0	Deny ▾	IPTV ▾	Auto ▾
3	○	● 4000	○ 200	□	0	Deny ▾	IPTV ▾	Auto ▾
4	○	● 4000	○ 200	□	0	Deny ▾	IPTV ▾	Auto ▾
5	○	● 4000	○ 200	□	0	Deny ▾	Default ▾	Auto ▾
6	○	● 4000	○ 200	□	0	Deny ▾	Default ▾	Auto ▾
7	○	● 4000	○ 200	□	0	Deny ▾	Default ▾	Auto ▾
8	○	● 4000	○ 200	□	0	Deny ▾	Default ▾	Auto ▾
9	○	● 4000	○ 200	□	0	Deny ▾	IPTV ▾	Auto ▾

Figure 23 Advance Application > Multicast > IPv4 Multicast > IGMP Snooping > IGMP Filtering Profile



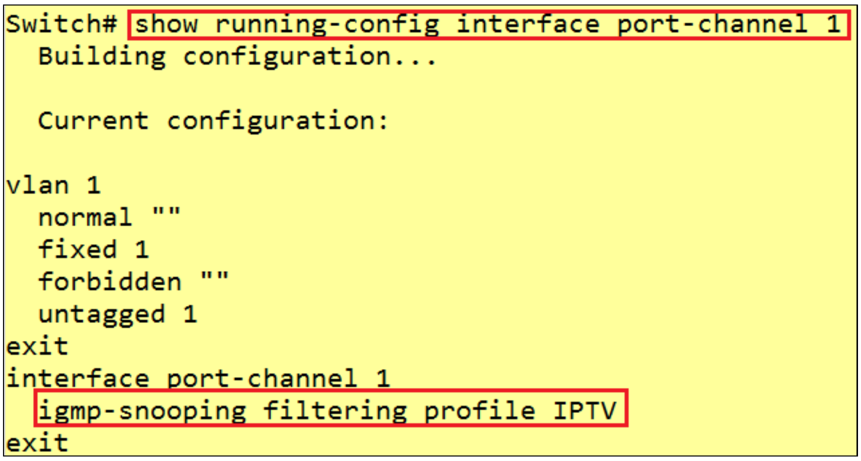
Profile Setup

Profile Name	Start Address	End Address
	224.0.0.0	224.0.0.0

Profile Name	Start Address	End Address	Delete Profile □	Delete Rule
IPTV			□	
	224.1.0.0	224.1.0.255		□
Default			□	
	0.0.0.0	0.0.0.0		□

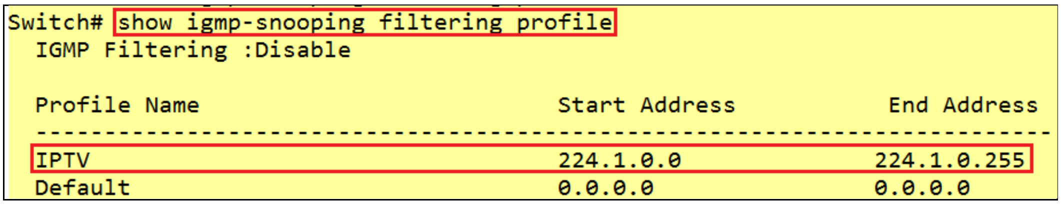
Using CLI:

Figure 24



```
Switch# show running-config interface port-channel 1
  Building configuration...

  Current configuration:

vlan 1
  normal ""
  fixed 1
  forbidden ""
  untagged 1
exit
interface port-channel 1
  igmp-snooping filtering profile IPTV
exit
```

Figure 25



```
Switch# show igmp-snooping filtering profile
  IGMP Filtering :Disable

  Profile Name                          Start Address           End Address
  ---------------------------------------------------------------------------
  IPTV                                  224.1.0.0               224.1.0.255
  Default                               0.0.0.0                 0.0.0.0
```

If the port is configured with a correct IGMP profile, proceed to **step 10**.

If the port is not configured with a correct IGMP profile, reconfigured and repeat **step 4**.

9.10 Are there any other switch between this switch and the multicast client with issue?

If there is a switch between this switch and the multicast client with issue, proceed to **step 11**.

If there are no switch between this switch and the multicast client with issue, **go to <OTHERS>**.

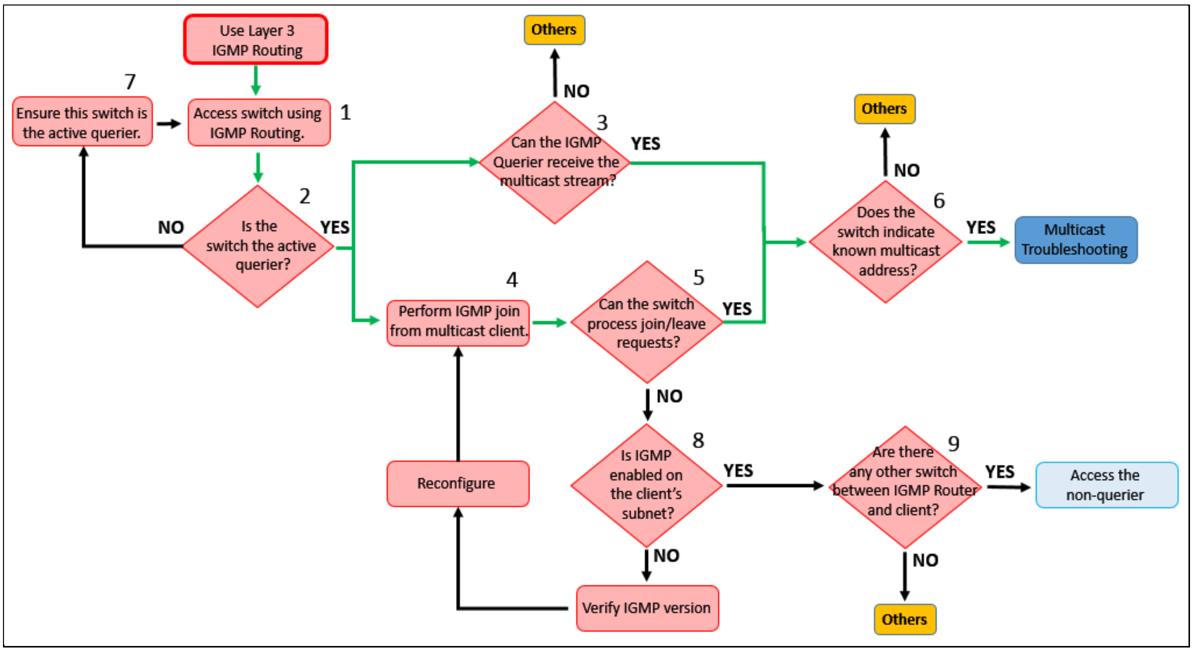
9.11 Does the other switch require MVR?

Multicast VLAN Registration (MVR) is a solution that allows multicast streaming between multicast clients and servers not sharing the same VLAN for a **pure layer 2** type application.

If the other switch does not require MVR, access the next switch and **repeat step 3**. If the other switch requires MVR, access the MVR switch and **go to step 8 of the MVR section**.

10 Troubleshooting for L3 IGMP Routing

Flowchart:


Use Layer 3 IGMP Routing
7
Ensure this switch is the active querier.
Access switch using IGMP Routing.
1
2
NO
Is the switch the active querier?
YES
Others
NO
3
Can the IGMP Querier receive the multicast stream?
YES
4
Perform IGMP join from multicast client.
5
Can the switch process join/leave requests?
YES
NO
Others
NO
6
Does the switch indicate known multicast address?
YES
Multicast Troubleshooting
8
Is IGMP enabled on the client's subnet?
YES
NO
Reconfigure
Verify IGMP version
9
Are there any other switch between IGMP Router and client?
YES
Access the non-querier
NO
Others

10.1 Access the switch using Layer 3 IGMP Routing.

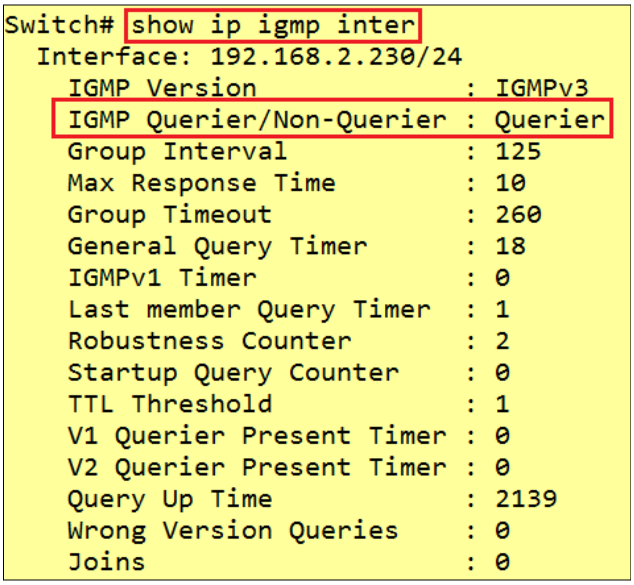
10.2 Is the switch the active querier?

By default, querier is enabled on the Zyxel switch using IGMP Routing. However, this switch can disable its querier role if another switch in the network also has IGMP routing enabled.

Enter CLI through console or TELNET to verify whether the switch is the active querier or not.

Using CLI:

Figure 26



```
Switch# show ip igmp inter
  Interface: 192.168.2.230/24
    IGMP Version                 : IGMPv3
    IGMP Querier/Non-Querier : Querier
    Group Interval               : 125
    Max Response Time            : 10
    Group Timeout                : 260
    General Query Timer          : 18
    IGMPv1 Timer                 : 0
    Last member Query Timer      : 1
    Robustness Counter           : 2
    Startup Query Counter        : 0
    TTL Threshold                : 1
    V1 Querier Present Timer : 0
    V2 Querier Present Timer : 0
    Query Up Time                : 2139
    Wrong Version Queries        : 0
    Joins                        : 0
```

*The switch will display "**Querier**" if this device is the active querier.

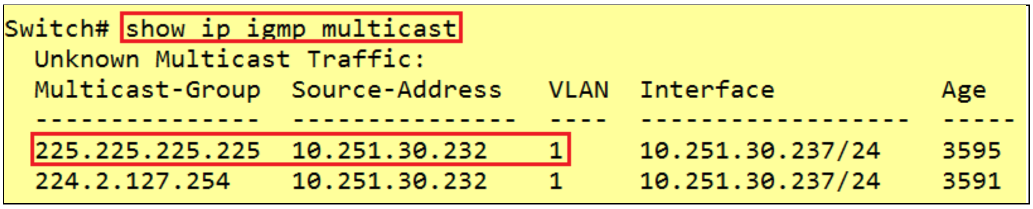
If the switch is the active querier, **go to step 3**.

If the switch is not the active querier, **go to step 7**.

10.3 Can the IGMP Querier receive the multicast stream?

You can confirm whether or not the IGMP Routing querier is receiving the multicast stream only by CLI.

Figure 27



```
Switch# show ip igmp multicast
  Unknown Multicast Traffic:
  Multicast-Group   Source-Address    VLAN  Interface           Age
  ---------------   ---------------   ----  ------------------  -----
  225.225.225.225   10.251.30.232      1    10.251.30.237/24    3595
  224.2.127.254     10.251.30.232      1    10.251.30.237/24    3591
```

*The figure indicates that the Zyxel switch is receiving multicast stream "225.225.225.225" on VLAN 1 from **multicast client** with IP address 10.251.30.232.

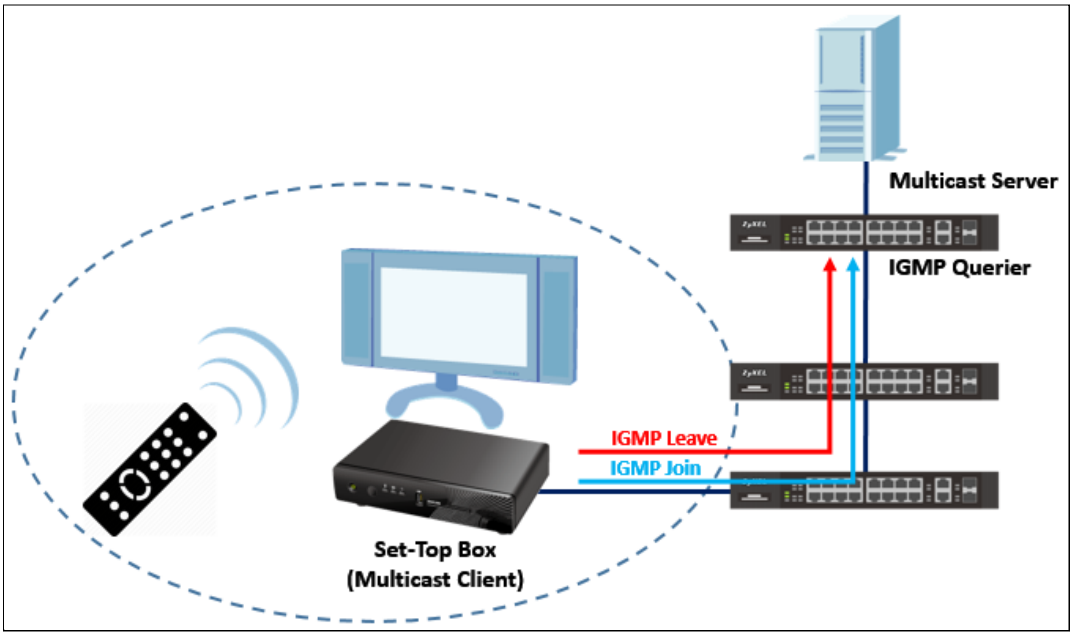
If the switch can receive the multicast stream, **go to step 4**.

If the switch cannot receive the multicast stream, **go to<OTHERS>**.

10.4 Perform an IGMP Join/Leave from the multicast client.

Access the **multicast client** with issue (usually the set-top box of an IPTV), and start changing IPTV from one channel to **the channel with the multicast issue** (if any). Every time a channel changes, the set-top box sends an IGMP Join for the new channel as well an IGMP Leave for the old channel.

Figure 28



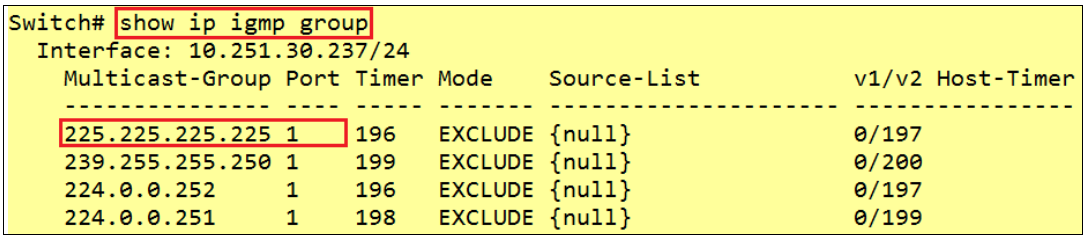
* Figure shows what occurs when a channel is changed through an IPTV's point of view.

After performing an IGMP Join/Leave, proceed to **step 5**.

10.5 Did the Zyxel switch receive the IGMP Join/Leave from the multicast client?

Access CLI to verify whether or not the Zyxel switch receives the **IGMP Join/Leave**.

Figure 29



```
Switch# show ip igmp group
  Interface: 10.251.30.237/24
    Multicast-Group Port Timer Mode    Source-List           v1/v2 Host-Timer
    --------------- ---- ----- ------- --------------------- ----------------
    225.225.225.225 1    196   EXCLUDE {null}                0/197
    239.255.255.250 1    199   EXCLUDE {null}                0/200
    224.0.0.252     1    196   EXCLUDE {null}                0/197
    224.0.0.251     1    198   EXCLUDE {null}                0/199
```

*The **multicast group address** will appear in the table if the switch receives the **IGMP Join**. Likewise, the **multicast group address** will disappear from the table if the switch receives the **IGMP Leave**.

If the switch can receive the IGMP Join/Leave, proceed to **step 6**.
If the switch cannot receive the IGMP Join/Leave, **go to step 8**.

10.6 Does the Zyxel switch indicate the known multicast group?

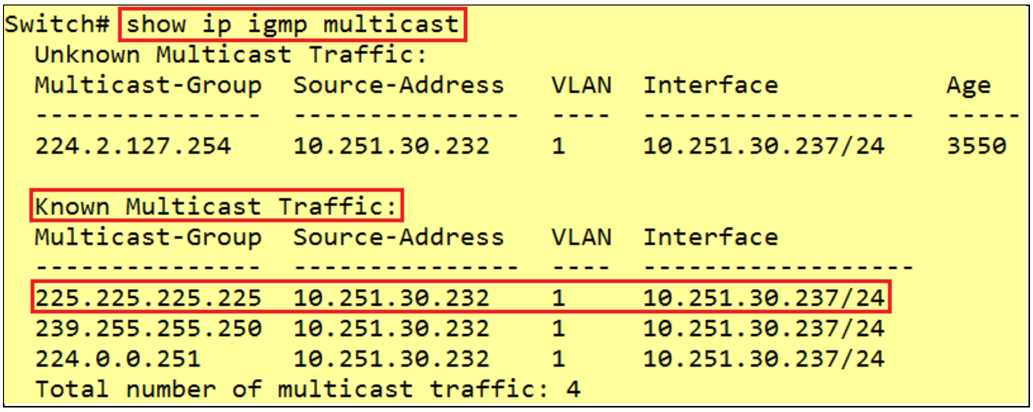
The **Zyxel switch using L3 IGMP Routing** will only start sending **multicast stream** when two conditions are met:

a. The L3 IGMP Router is receiving a **multicast stream** from any interface.

b. The L3 IGMP Router received the **IGMP Join** for the same **multicast stream** it receives.

When the two conditions are met, this stream will now be called a "**known multicast traffic**". You can access the CLI of the Zyxel switch to verify which multicast addresses are currently known.

Figure 30



```
Switch# show ip igmp multicast
  Unknown Multicast Traffic:
  Multicast-Group  Source-Address   VLAN  Interface           Age
  ---------------  ---------------  ----  ------------------  -----
  224.2.127.254    10.251.30.232    1     10.251.30.237/24    3550

  Known Multicast Traffic:
  Multicast-Group  Source-Address   VLAN  Interface
  ---------------  ---------------  ----  ------------------
  225.225.225.225  10.251.30.232    1     10.251.30.237/24
  239.255.255.250  10.251.30.232    1     10.251.30.237/24
  224.0.0.251      10.251.30.232    1     10.251.30.237/24
  Total number of multicast traffic: 4
```

*Figure shows that the switch has **known multicast traffic** 225.225.225.225.

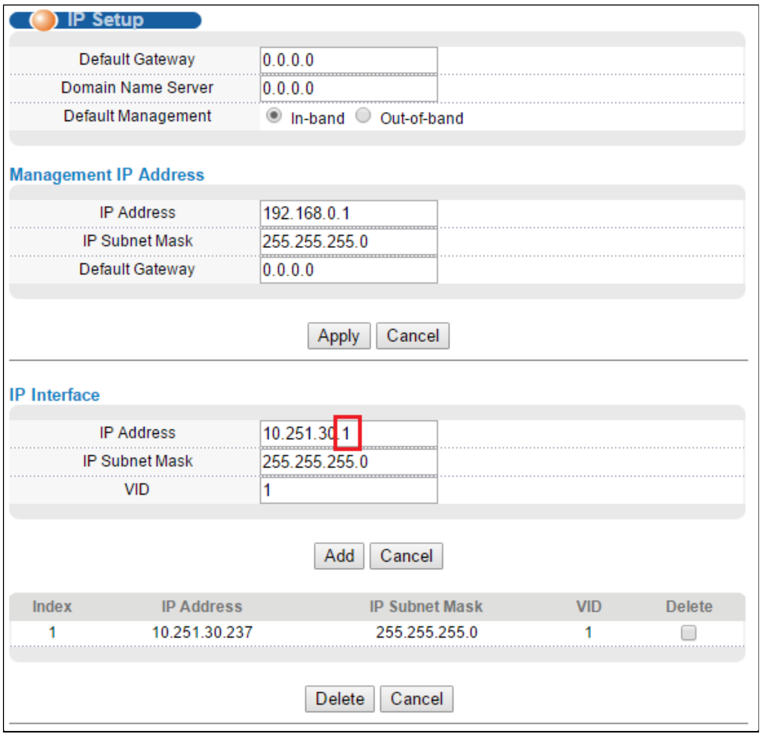
If the L3 IGMP Router now has the known multicast traffic for the multicast address with issue, **repeat the Multicast Troubleshooting section**.

10.7 Ensure that the Zyxel switch using Layer 3 IGMP Routing is the active querier.

When two devices have querier mode enabled, the device with the **lower IP address** will assume the role of the active querier. In this case, we can configure the interface IP address of the IGMP querier to the lowest possible IP address in the network.

Using Web GUI:

Figure 31 Basic Setting > IP Setup



IP Setup

Default Gateway	0.0.0.0
Domain Name Server	0.0.0.0
Default Management	● In-band ○ Out-of-band

Management IP Address

IP Address	192.168.0.1
IP Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0

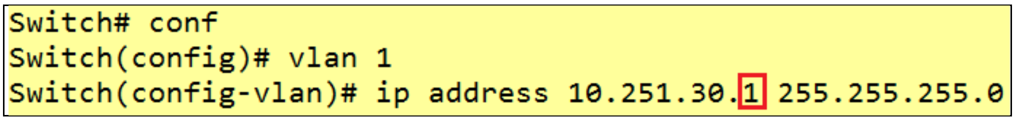
IP Interface

IP Address	10.251.30.1
IP Subnet Mask	255.255.255.0
VID	1

Index	IP Address	IP Subnet Mask	VID	Delete
1	10.251.30.237	255.255.255.0	1	□

Using CLI:

Figure 32



```
Switch# conf
Switch(config)# vlan 1
Switch(config-vlan)# ip address 10.251.30.1 255.255.255.0
```

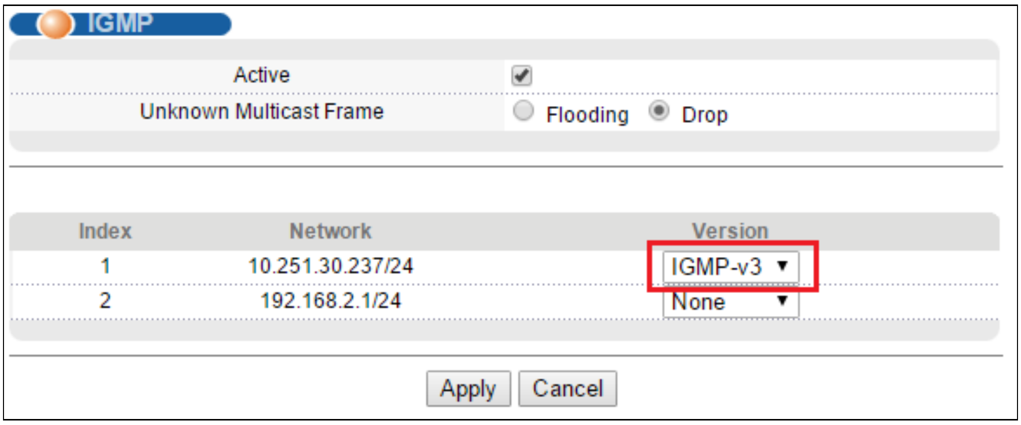
In this example, the network in VLAN 1 is 10.251.30.0/24. Configuring the IP address to 10.251.30.1 will ensure that this device will be the active querier in VLAN 1.

After reconfiguring the IP address of the IGMP querier's interface, **repeat step 1**.

10.8 Is Layer 3 IGMP Routing enabled on the multicast client's subnet?

Using Web GUI:

Figure 33 IP Application > IGMP

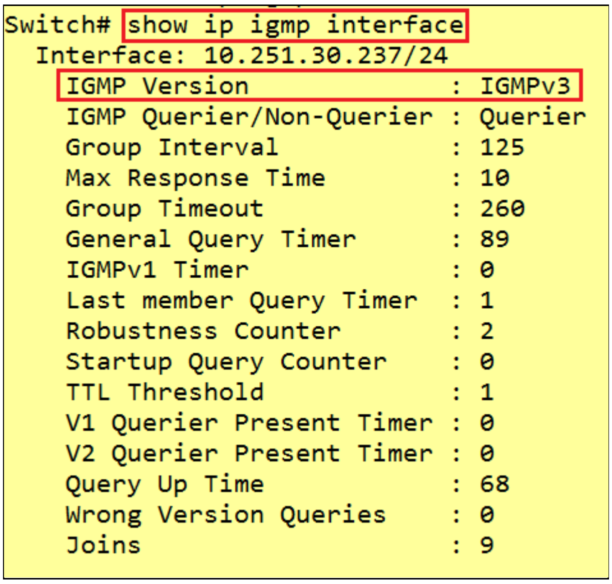


Active	☑
Unknown Multicast Frame	○ Flooding ● Drop

Index	Network	Version
1	10.251.30.237/24	IGMP-v3
2	192.168.2.1/24	None

Using CLI:

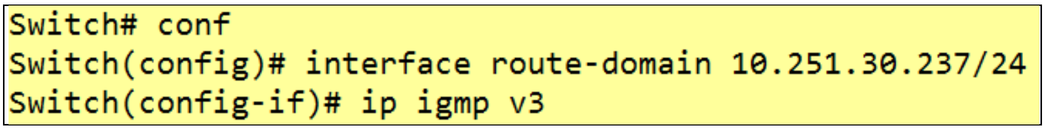
Figure 34



```
Switch# show ip igmp interface
  Interface: 10.251.30.237/24
    IGMP Version                 : IGMPv3
    IGMP Querier/Non-Querier : Querier
    Group Interval               : 125
    Max Response Time            : 10
    Group Timeout                : 260
    General Query Timer          : 89
    IGMPv1 Timer                 : 0
    Last member Query Timer  : 1
    Robustness Counter           : 2
    Startup Query Counter        : 0
    TTL Threshold                : 1
    V1 Querier Present Timer : 0
    V2 Querier Present Timer : 0
    Query Up Time                : 68
    Wrong Version Queries        : 0
    Joins                        : 9
```

Configure using CLI:

Figure 35



```
Switch# conf
Switch(config)# interface route-domain 10.251.30.237/24
Switch(config-if)# ip igmp v3
```

If IGMP is not enabled in the multicast client's network, the Layer 3 IGMP Router will not stream video on that network.

If the interface or network of the multicast client does not have IGMP enabled, **reconfigure and repeat step 4**.

If the interface or network of the multicast client has IGMP enabled already, **go to step 9**.

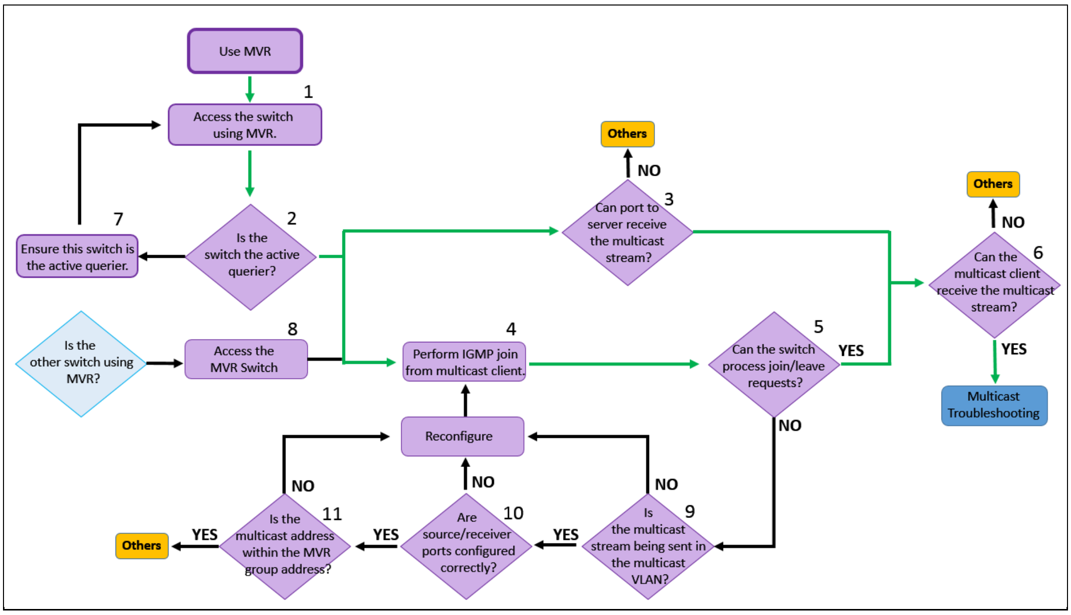
10.9 Are there any other switch between the IGMP querier and the multicast client?

If there are other switches between the IGMP querier and the multicast client, access the Layer 2 non-querier switch and **move on to step 3 of the Layer 2 IGMP Snooping Troubleshooting section**.

If there are no other switches between the IGMP querier and the multicast client, **go to <OTHERS>**.

11 Troubleshooting for Multicast VLAN Registration

Flowchart:


Use MVR
1
Access the switch using MVR.
2
Is the switch the active querier?
7
Ensure this switch is the active querier.
Others
NO
3
Can port to server receive the multicast stream?
Others
NO
6
Can the multicast client receive the multicast stream?
YES
Multicast Troubleshooting
8
Is the other switch using MVR?
Access the MVR Switch
4
Perform IGMP join from multicast client.
5
Can the switch process join/leave requests?
YES
NO
Reconfigure
NO
NO
NO
11
Is the multicast address within the MVR group address?
YES
Others
10
Are source/receiver ports configured correctly?
YES
9
Is the multicast stream being sent in the multicast VLAN?
YES

11.1 Access the switch using MVR.

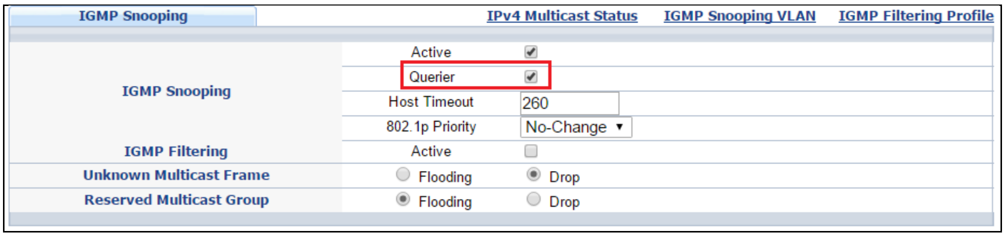
11.2 Is the switch the active querier?

By default, querier is disabled on the Zyxel switch using IGMP Snooping. There are two things that needs to be verified to check whether or not the switch is the active querier.

11.3 IGMP querier mode is globally enabled.

Using Web GUI:

Figure 1 Advance Application > Multicast > IPv4 Multicast > IGMP Snooping



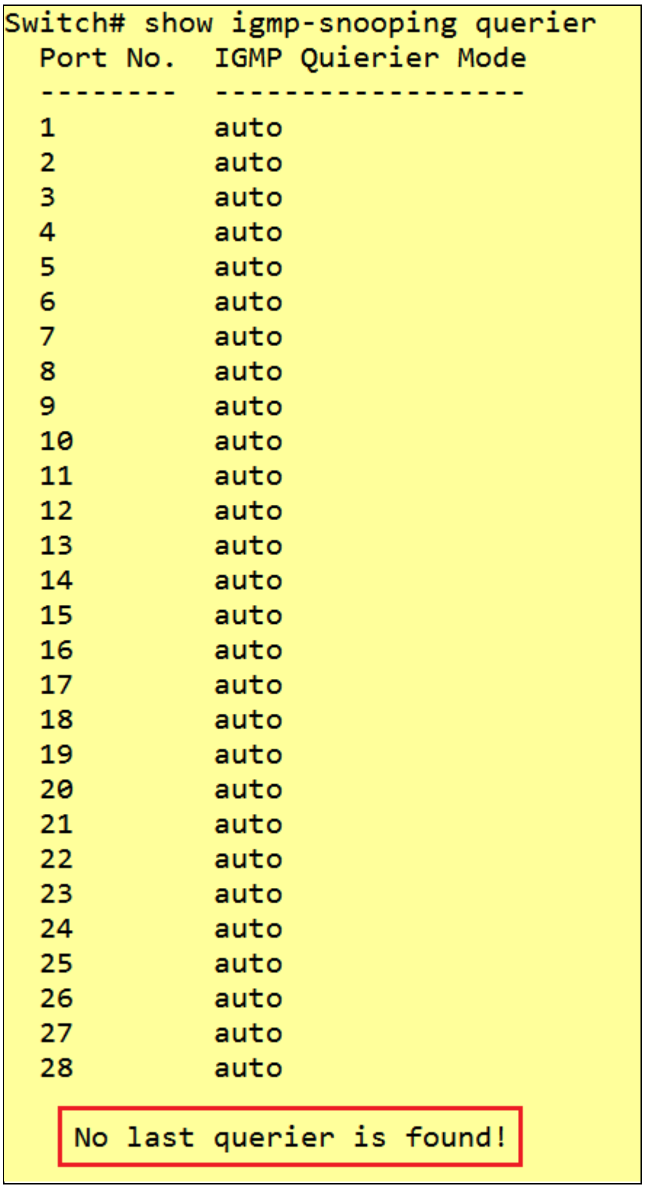
IGMP Snooping | IPv4 Multicast Status | IGMP Snooping VLAN | IGMP Filtering Profile

IGMP Snooping	Active	☑
	Querier	☑
	Host Timeout	260
	802.1p Priority	No-Change ▾
IGMP Filtering	Active	☐
Unknown Multicast Frame	○ Flooding	● Drop
Reserved Multicast Group	● Flooding	○ Drop

11.4 The CLI shows a "No last querier is found".

Using CLI:

Figure 2



```
Switch# show igmp-snooping querier
  Port No.   IGMP Quierier Mode
  --------   ------------------
  1          auto
  2          auto
  3          auto
  4          auto
  5          auto
  6          auto
  7          auto
  8          auto
  9          auto
  10         auto
  11         auto
  12         auto
  13         auto
  14         auto
  15         auto
  16         auto
  17         auto
  18         auto
  19         auto
  20         auto
  21         auto
  22         auto
  23         auto
  24         auto
  25         auto
  26         auto
  27         auto
  28         auto

    No last querier is found!
```

*The "No last querier is found" only means that there are no other active IGMP queriers in the network. This does not indicate whether this device is the active IGMP querier.

If both indicates that the switch is the active querier, **go to step 3**.

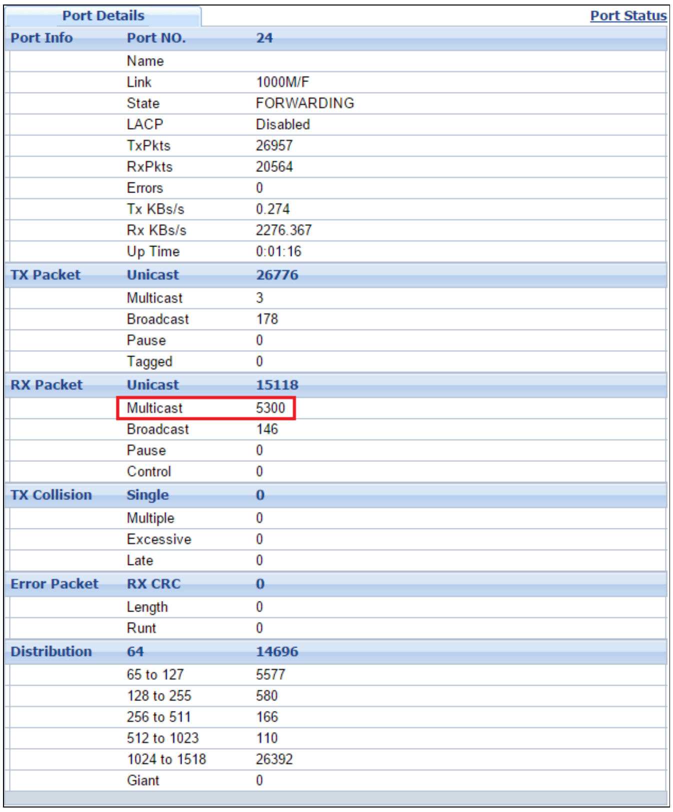
If both does not indicate that the switch is the active querier, **go to step 8**.

11.5 Can the Zyxel switch receive the multicast stream?

You can verify whether the switch is receiving multicast frames by looking at the **port counters**. Locate the port of the switch in the direction of the **multicast server**. Afterwards, check the port counters for *received multicast packets*. Check the port counters again after a few seconds. A consistent increase of received multicast packets is an indication that the port is receiving multicast streams.

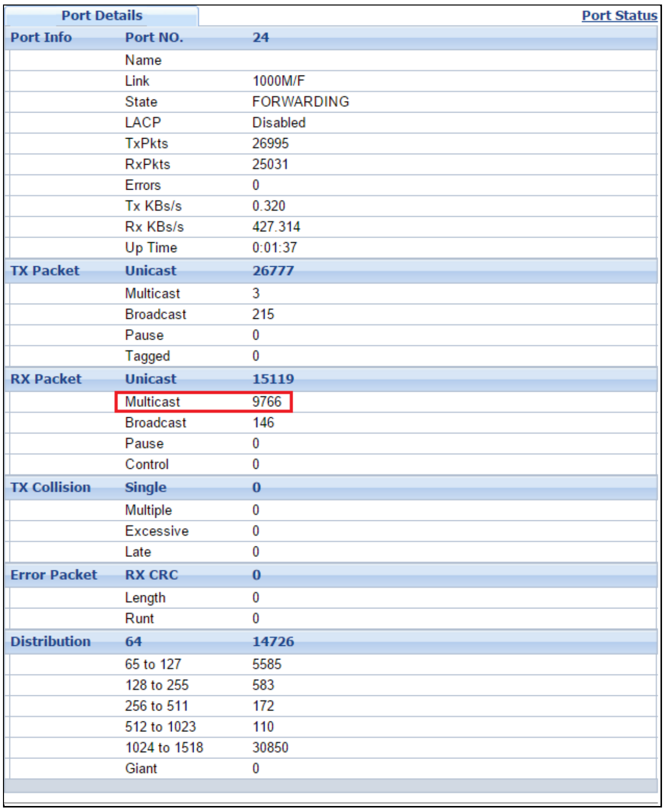
Using Web GUI:

Figure 3 Status (Homepage) > Port Status > Port <*number*>



Port Info	**Port NO.**	**24**
	Name	
	Link	1000M/F
	State	FORWARDING
	LACP	Disabled
	TxPkts	26957
	RxPkts	20564
	Errors	0
	Tx KBs/s	0.274
	Rx KBs/s	2276.367
	Up Time	0:01:16
TX Packet	**Unicast**	**26776**
	Multicast	3
	Broadcast	178
	Pause	0
	Tagged	0
RX Packet	**Unicast**	**15118**
	Multicast	5300
	Broadcast	146
	Pause	0
	Control	0
TX Collision	**Single**	**0**
	Multiple	0
	Excessive	0
	Late	0
Error Packet	**RX CRC**	**0**
	Length	0
	Runt	0
Distribution	**64**	**14696**
	65 to 127	5577
	128 to 255	580
	256 to 511	166
	512 to 1023	110
	1024 to 1518	26392
	Giant	0

Figure 4

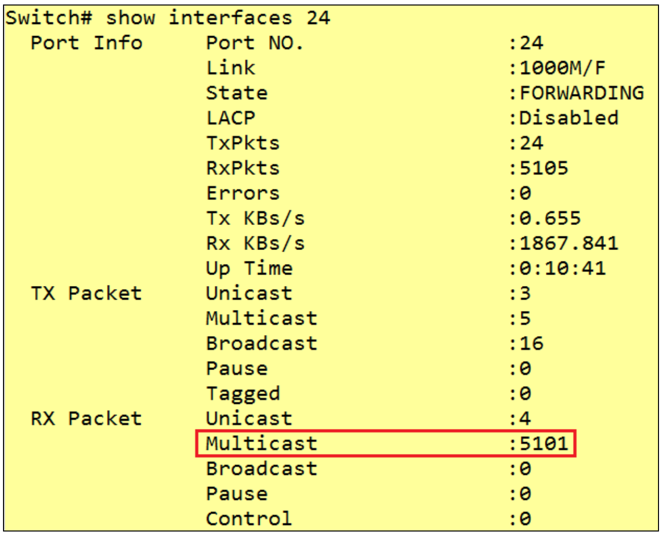


Port Details Port Status

Port Info	Port NO.	24
	Name	
	Link	1000M/F
	State	FORWARDING
	LACP	Disabled
	TxPkts	26995
	RxPkts	25031
	Errors	0
	Tx KBs/s	0.320
	Rx KBs/s	427.314
	Up Time	0:01:37
TX Packet	**Unicast**	**26777**
	Multicast	3
	Broadcast	215
	Pause	0
	Tagged	0
RX Packet	**Unicast**	**15119**
	Multicast	9766
	Broadcast	146
	Pause	0
	Control	0
TX Collision	**Single**	**0**
	Multiple	0
	Excessive	0
	Late	0
Error Packet	**RX CRC**	**0**
	Length	0
	Runt	0
Distribution	**64**	**14726**
	65 to 127	5585
	128 to 255	583
	256 to 511	172
	512 to 1023	110
	1024 to 1518	30850
	Giant	0

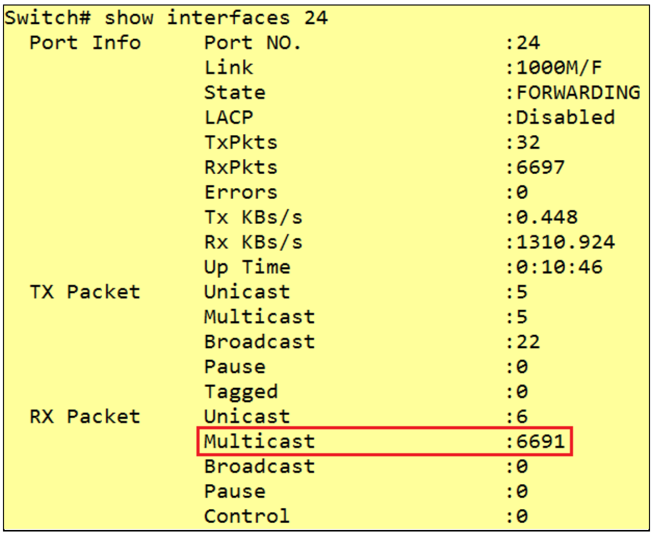
Using CLI:

Figure 5



```
Switch# show interfaces 24
  Port Info      Port NO.                :24
                 Link                    :1000M/F
                 State                   :FORWARDING
                 LACP                    :Disabled
                 TxPkts                  :24
                 RxPkts                  :5105
                 Errors                  :0
                 Tx KBs/s                :0.655
                 Rx KBs/s                :1867.841
                 Up Time                 :0:10:41
  TX Packet      Unicast                 :3
                 Multicast               :5
                 Broadcast               :16
                 Pause                   :0
                 Tagged                  :0
  RX Packet      Unicast                 :4
                 Multicast               :5101
                 Broadcast               :0
                 Pause                   :0
                 Control                 :0
```

Figure 6



```
Switch# show interfaces 24
  Port Info      Port NO.                :24
                 Link                    :1000M/F
                 State                   :FORWARDING
                 LACP                    :Disabled
                 TxPkts                  :32
                 RxPkts                  :6697
                 Errors                  :0
                 Tx KBs/s                :0.448
                 Rx KBs/s                :1310.924
                 Up Time                 :0:10:46
  TX Packet      Unicast                 :5
                 Multicast               :5
                 Broadcast               :22
                 Pause                   :0
                 Tagged                  :0
  RX Packet      Unicast                 :6
                 Multicast               :6691
                 Broadcast               :0
                 Pause                   :0
                 Control                 :0
```

*This shows the difference in port counters, from left to right, in the span of a few seconds.

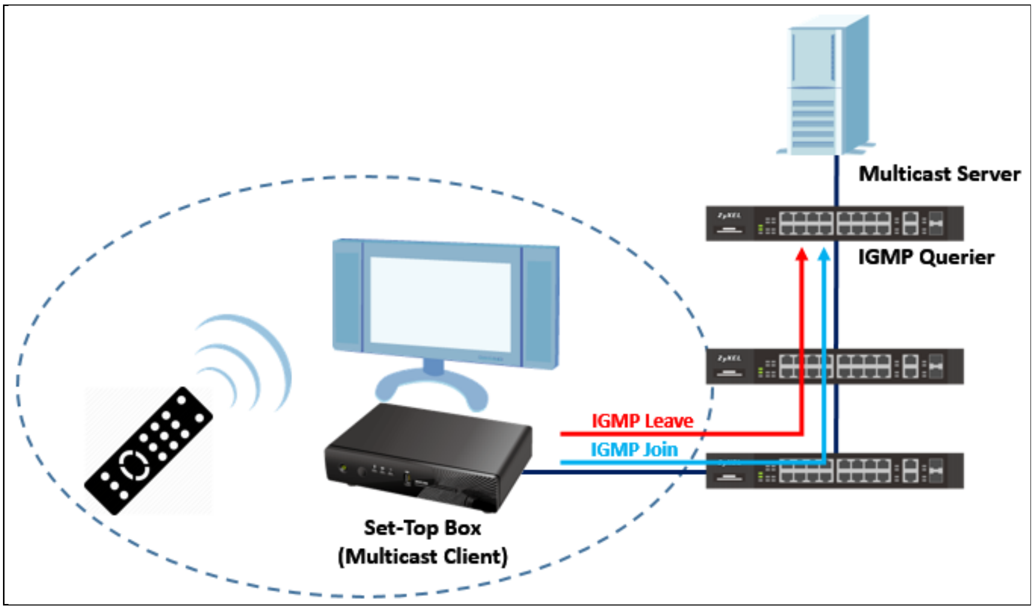
If the switch can receive the multicast stream, **go to step 4**.

If the switch cannot receive the multicast stream, **go to<OTHERS>**.

11.6 Perform an IGMP Join/Leave from the multicast client.

Access the **multicast client** with issue (usually the set-top box of an IPTV), and start changing IPTV from one channel to **the channel with the multicast issue** (if any). Every time a channel changes, the set-top box sends an IGMP Join for the new channel as well an IGMP Leave for the old channel.

Figure 7



* Figure shows what occurs when a channel is changed through an IPTV's point of view.

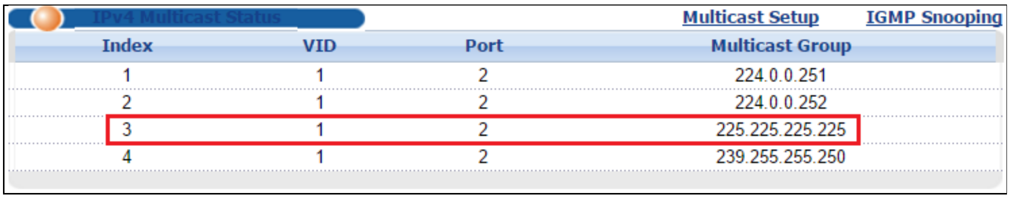
After performing an IGMP Join/Leave, **proceed to step 5**.

11.7 Did the Zyxel switch receive the IGMP Join/Leave from the multicast client?

After you perform the **IGMP join/leave**, the multicast address should appear in the multicast table. The appearance of the multicast address indicates that the switch can successfully receive the **IGMP join/leave**. For the case of MVR, the multicast group address must have VID in the **Multicast VLAN ID**.

Using Web GUI:

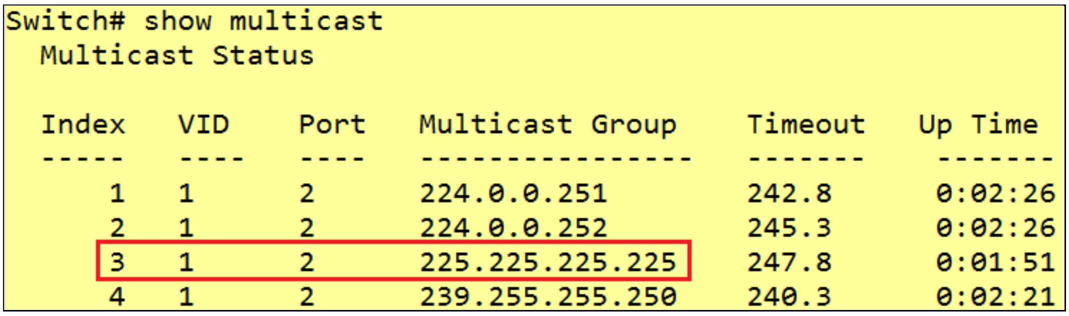
Figure 8 Advance Application > Multicast



Index	VID	Port	Multicast Group
1	1	2	224.0.0.251
2	1	2	224.0.0.252
3	1	2	225.225.225.225
4	1	2	239.255.255.250

Using CLI:

Figure 9



```
Switch# show multicast
 Multicast Status

 Index   VID    Port    Multicast Group      Timeout    Up Time
 -----   ----   ----    ----------------     -------    -------
     1   1      2       224.0.0.251          242.8      0:02:26
     2   1      2       224.0.0.252          245.3      0:02:26
     3   1      2       225.225.225.225      247.8      0:01:51
     4   1      2       239.255.255.250      240.3      0:02:21
```

If the switch can receive the IGMP Join/Leave in the Multicast VLAN ID, **proceed to step 6**.

If the switch cannot receive the IGMP Join/Leave, **go to step 10**.

11.8 Can the multicast client receive the multicast stream?

If both **multicast stream** and **IGMP join/leave** reaches this switch, then the multicast client with issue should most likely be able to watch the channel through the IPTV.

If the multicast client can now receive the multicast stream, **repeat the Multicast Troubleshooting section**.

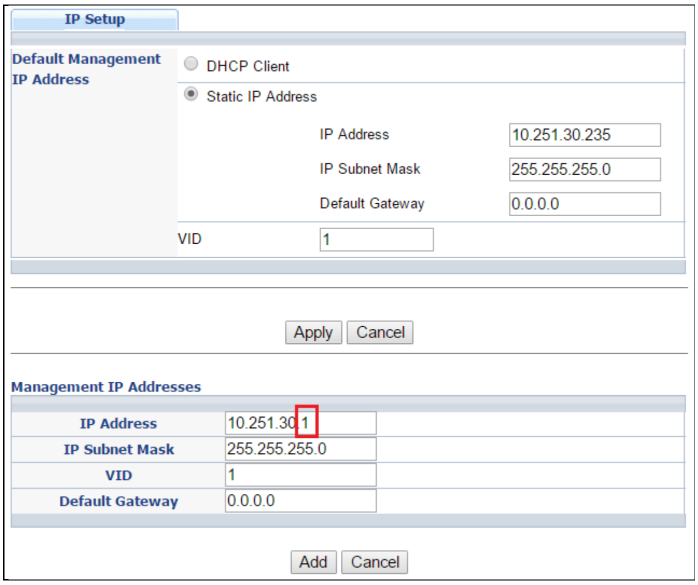
If the multicast client still can receive the multicast stream, **go to<OTHERS>**.

11.9 Ensure that the Zyxel switch using MVR is the active querier.

When two devices have querier mode enabled, the device with the **lower IP address** will assume the role of the active querier. In this case, we can configure the interface IP address of the IGMP querier to the lowest possible IP address in the network.

Using Web GUI:

Figure 10 Basic Setting > IP Setup



Default Management IP Address

○ DHCP Client

● Static IP Address

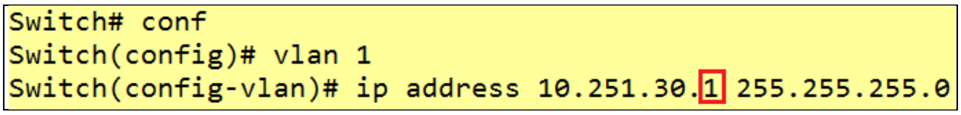
IP Address	10.251.30.235
IP Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
VID	1

Management IP Addresses

IP Address	10.251.30.1
IP Subnet Mask	255.255.255.0
VID	1
Default Gateway	0.0.0.0

Using CLI:

Figure 11



```
Switch# conf
Switch(config)# vlan 1
Switch(config-vlan)# ip address 10.251.30.1 255.255.255.0
```

In this example, the network in VLAN 1 is 10.251.30.0/24. Configuring the IP address to 10.251.30.1 will ensure that this device will be the active querier in VLAN 1.

After reconfiguring the IP address of the IGMP querier's interface, **repeat step 2**.

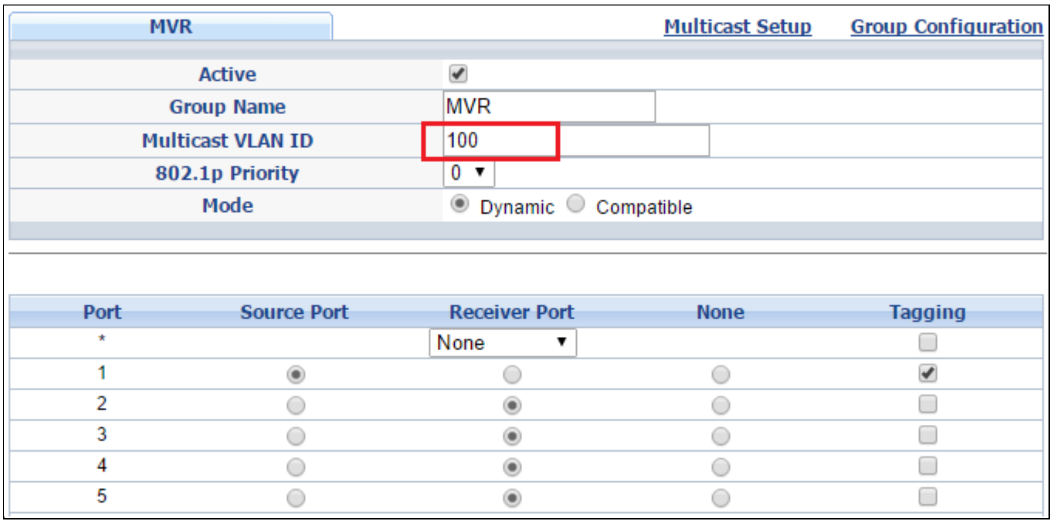
Access the Zyxel switch using MVR. **Go to step 3**.

11.10 Is the multicast stream being sent in the multicast VLAN ID?

Make sure that the Multicast VLAN ID matches the multicast stream's VLAN. If the multicast stream does not contain any VLAN tags, then multicast stream will be processed through this port's PVID.

Using Web GUI:

Figure 12 Advance Application > Multicast > MVR

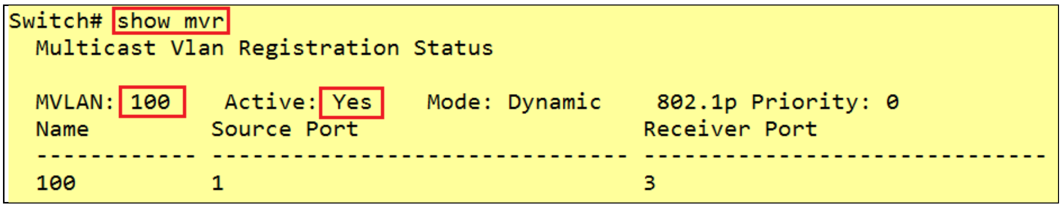


Active	☑
Group Name	MVR
Multicast VLAN ID	100
802.1p Priority	0 ▼
Mode	● Dynamic ○ Compatible

Port	Source Port	Receiver Port	None	Tagging
*		None ▼		□
1	●	○	○	☑
2	○	●	○	□
3	○	●	○	□
4	○	●	○	□
5	○	●	○	□

Using CLI:

Figure 13



```
Switch# show mvr
  Multicast Vlan Registration Status

  MVLAN: 100   Active: Yes   Mode: Dynamic    802.1p Priority: 0
  Name         Source Port                     Receiver Port
  ------------ ------------------------------- ------------------------------
  100          1                               3
```

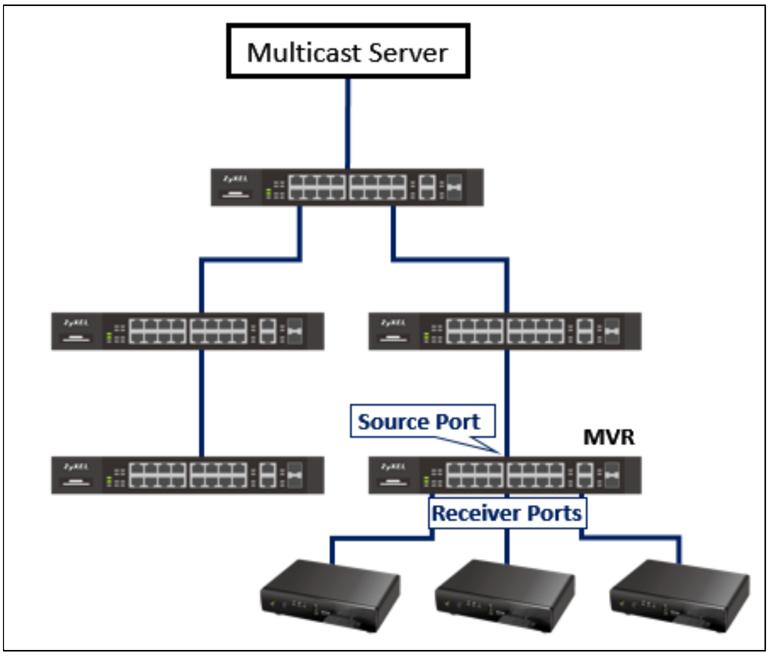
If the switch's Multicast VLAN ID matches the multicast stream's VLAN, **go to step 10**.

If the switch's Multicast VLAN ID does not match the multicast stream's VLAN, **reconfigure and repeat step 3**.

11.11 Are the MVR source and receiver ports configured correctly?

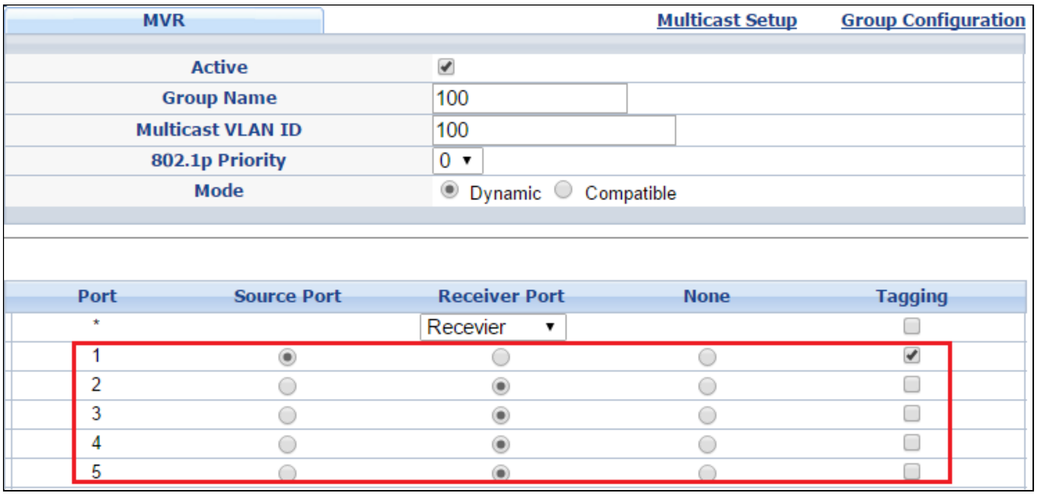
Make sure that the port towards the server is a **source port**, while ports to subscribers or multicast clients are **receiver ports**. You will need to use tagging if the path to the querier is through a specific VLAN.

Figure 14



Using Web GUI:

Figure 15 Advance Application > Multicast > MVR

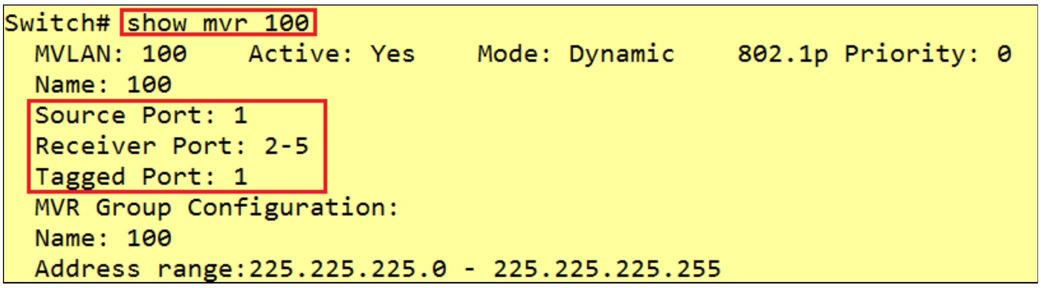


Active	☑
Group Name	100
Multicast VLAN ID	100
802.1p Priority	0 ▼
Mode	● Dynamic ○ Compatible

Port	Source Port	Receiver Port	None	Tagging
*		Recevier ▼		□
1	●	○	○	☑
2	○	●	○	□
3	○	●	○	□
4	○	●	○	□
5	○	●	○	□

Using CLI:

Figure 16



```
Switch# show mvr 100
  MVLAN: 100     Active: Yes     Mode: Dynamic     802.1p Priority: 0
  Name: 100
  Source Port: 1
  Receiver Port: 2-5
  Tagged Port: 1
  MVR Group Configuration:
  Name: 100
  Address range:225.225.225.0 - 225.225.225.255
```

If the MVR ports are configured correctly, **go to step 11**.

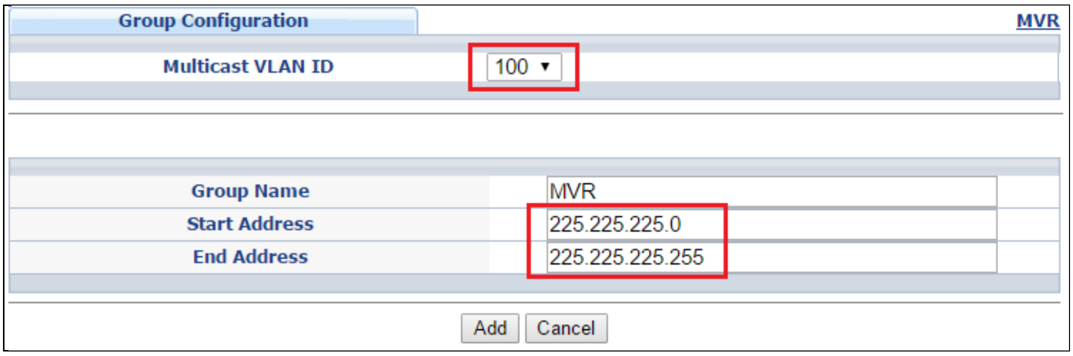
If the MVR ports are not configured correctly, **reconfigure and repeat step 3**.

11.12 Is the multicast stream within the MVR group address range?

The **MVR group address range** allows the **IGMP join/leave** for this specific address range from **multicast clients** to be forwarded across the **Multicast VLAN ID**. If the IGMP join/leave is not within the MVR group address range, then these will be forwarded across the PVID instead.

Using Web GUI:

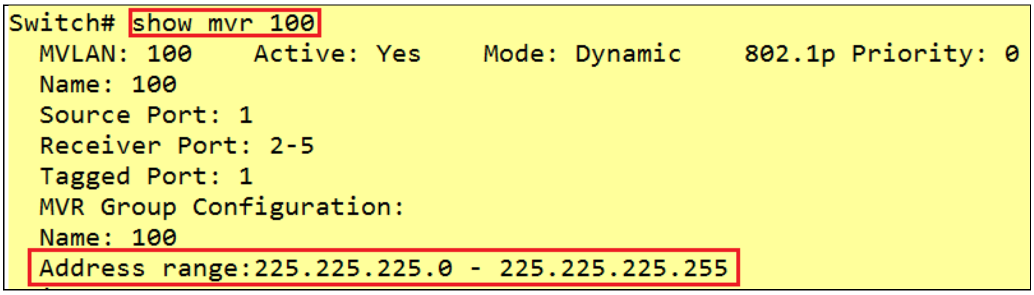
Figure 17 Advance Application > Multicast > MVR > Group Configuration



Multicast VLAN ID	100 ▾
Group Name	MVR
Start Address	225.225.225.0
End Address	225.225.225.255

Using CLI:

Figure 18



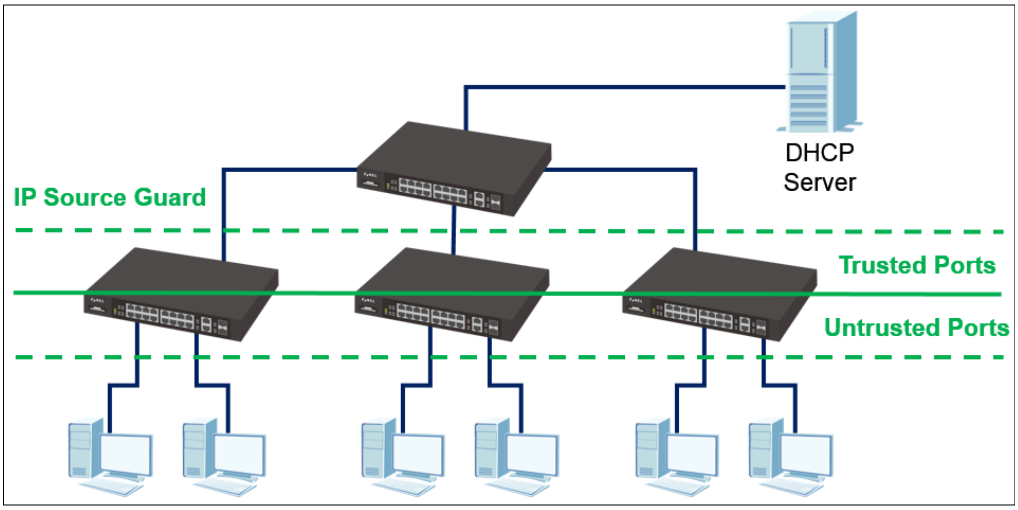
```
Switch# show mvr 100
  MVLAN: 100     Active: Yes     Mode: Dynamic     802.1p Priority: 0
  Name: 100
  Source Port: 1
  Receiver Port: 2-5
  Tagged Port: 1
  MVR Group Configuration:
  Name: 100
  Address range:225.225.225.0 - 225.225.225.255
```

If the multicast stream's address is within the MVR address range, **go to <OTHERS>**.

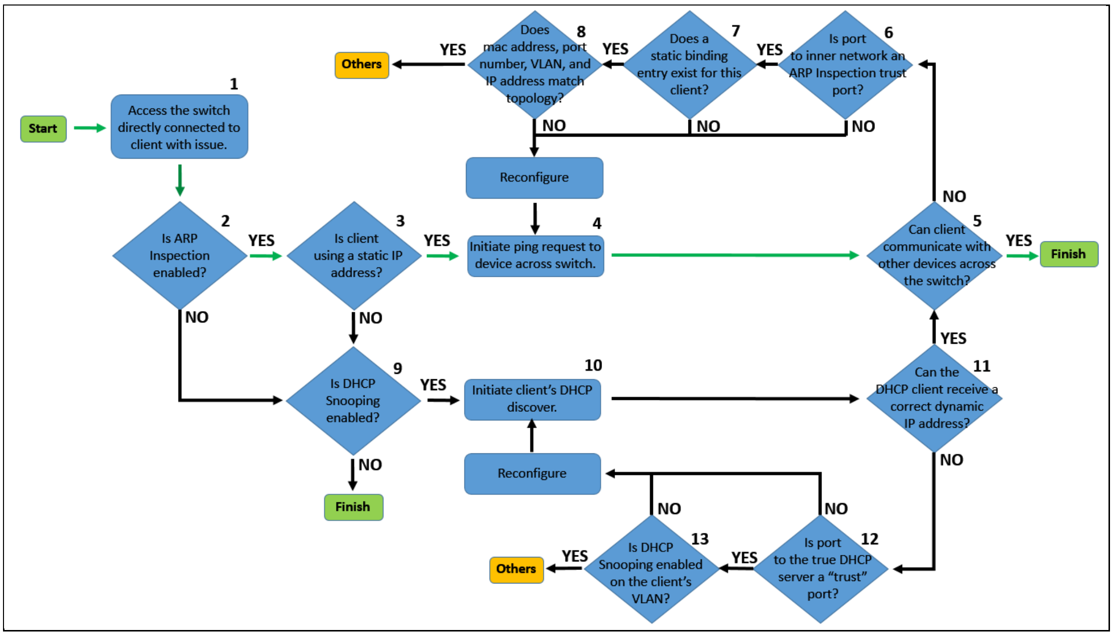
If the multicast stream's address is not within the MVR address range, **reconfigure and repeat step 3**.

12 Troubleshooting for IP Source Guard

Illustration:



Flowchart:


Start
1
Access the switch directly connected to client with issue.
2
Is ARP Inspection enabled?
YES
NO
3
Is client using a static IP address?
YES
NO
4
Initiate ping request to device across switch.
5
Can client communicate with other devices across the switch?
YES
Finish
NO
6
Is port to inner network an ARP Inspection trust port?
YES
NO
7
Does a static binding entry exist for this client?
YES
NO
8
Does mac address, port number, VLAN, and IP address match topology?
YES
Others
NO
Reconfigure
9
Is DHCP Snooping enabled?
YES
NO
Finish
10
Initiate client's DHCP discover.
11
Can the DHCP client receive a correct dynamic IP address?
YES
NO
12
Is port to the true DHCP server a "trust" port?
YES
NO
13
Is DHCP Snooping enabled on the client's VLAN?
YES
Others
NO
Reconfigure

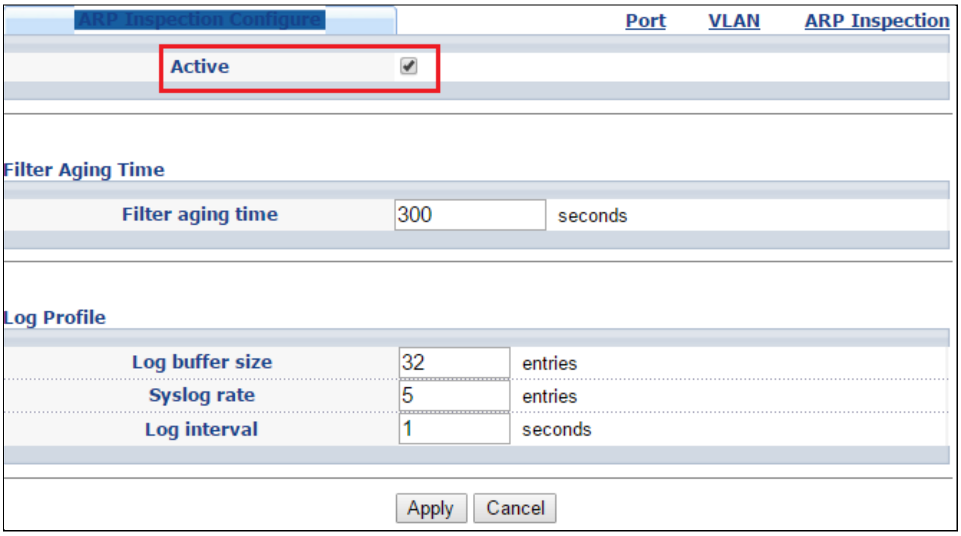
OTHERS:

12.1 Access the switch directly connected to the client with issue.

12.2 Is ARP Inspection enabled on the Switch?

Using Web GUI:

Figure 1 Advance Application > IP Source Guard > IP Source Guard Setup > ARP Inspection> Configure



ARP Inspection Configure

Active ☑

Filter Aging Time

Filter aging time 300 seconds

Log Profile

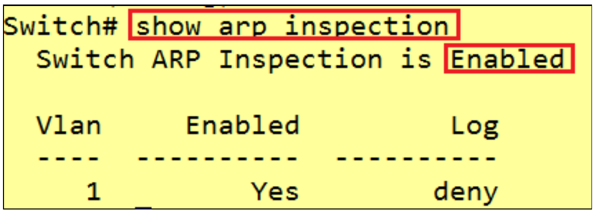
Log buffer size 32 entries

Syslog rate 5 entries

Log interval 1 seconds

Using CLI:

Figure 2



```
Switch# show arp inspection
  Switch ARP Inspection is Enabled

  Vlan      Enabled          Log
  ----   ----------   ----------
     1          Yes         deny
```

If ARP Inspection is enabled, **go to step 3**.

If ARP Inspection is not enabled, **go to step 9**.

12.3 Is the client with issue using a static IP address?

If the client with issue is using a static IP address, **go to step 4**.

If the client with issue is using a dynamic IP address, **go to step 9**.

12.4 Initiate a ping request from client with issue to destination with issue.

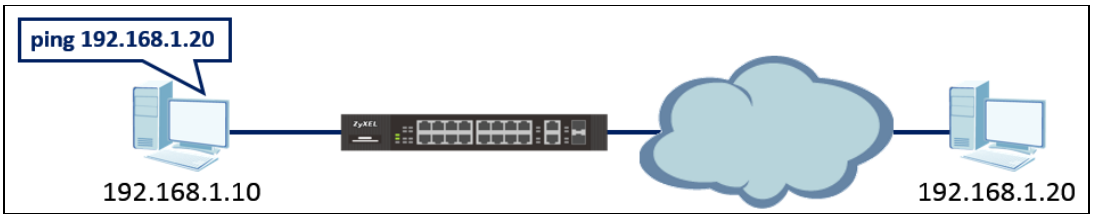
The *destination with issue* could be one of the following:

Device in the same LAN: ping the device's IP address.

Device in a different LAN: ping the device's IP address.

Internet: ping Goggle's public DNS server "8.8.8.8".

Figure 3



Afterwards, **proceed to step 5**.

12.5 Can the client with issue communicate with devices across the Zyxel switch?

If ping from client with issue to destination with issue is successful, **proceed to the next agenda**.

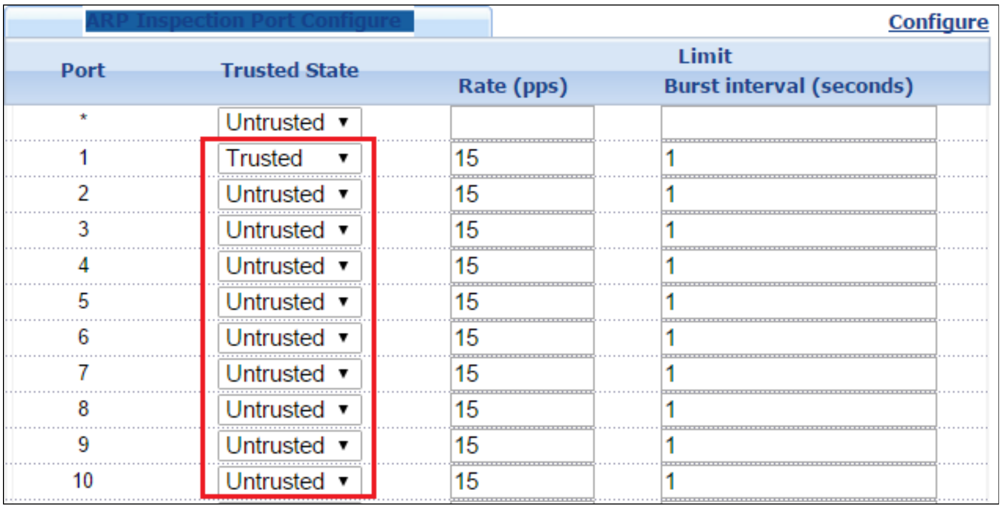
If ping from client with issue to destination with issue is not successful, **go to step 6**.

12.6 Is the port to the inner network configured as an ARP Inspection “trust” port?

The inner network’s port should be configured as a trust port. This is because there are locally resources such as severs or gateways which are classified as trusted devices managed by the administrators. If the inner network is configured as an untrusted port, then any local resources that uses static IP addresses will not be able to communicate with other devices.

Using Web GUI:

Figure 4 Advance Application > IP Source Guard > IP Source Guard Setup > ARP Inspection> Configure > Port



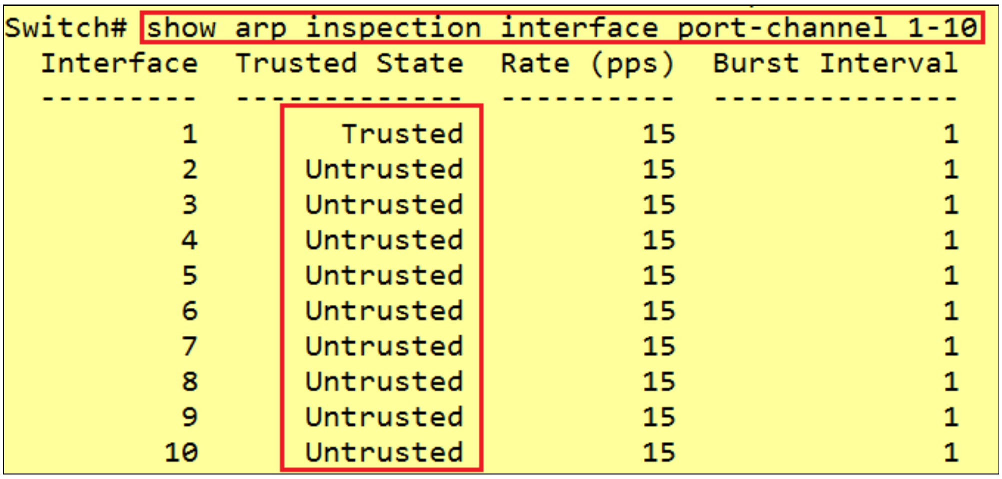
ARP Inspection Port Configure

Configure

Port	Trusted State	Limit	
		Rate (pps)	Burst interval (seconds)
*	Untrusted ▼		
1	Trusted ▼	15	1
2	Untrusted ▼	15	1
3	Untrusted ▼	15	1
4	Untrusted ▼	15	1
5	Untrusted ▼	15	1
6	Untrusted ▼	15	1
7	Untrusted ▼	15	1
8	Untrusted ▼	15	1
9	Untrusted ▼	15	1
10	Untrusted ▼	15	1

Using CLI:

Figure 5

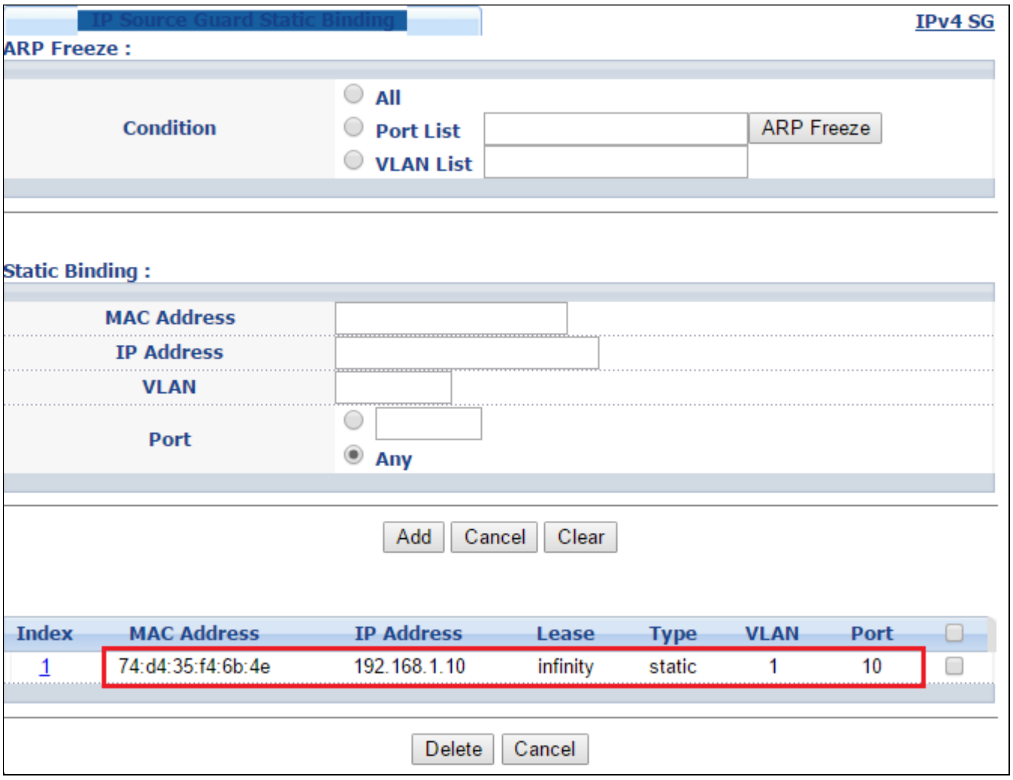


```
Switch# show arp inspection interface port-channel 1-10
  Interface  Trusted State  Rate (pps)  Burst Interval
  ---------  -------------  ----------  --------------
          1        Trusted          15               1
          2      Untrusted          15               1
          3      Untrusted          15               1
          4      Untrusted          15               1
          5      Untrusted          15               1
          6      Untrusted          15               1
          7      Untrusted          15               1
          8      Untrusted          15               1
          9      Untrusted          15               1
         10      Untrusted          15               1
```

12.7 Does a static binding entry exist for this client?

Using Web GUI:

Figure 6 Advance Application > IP Source Guard > IP Source Guard Setup > Static Binding



ARP Freeze :

Condition: ○ All ○ Port List ○ VLAN List

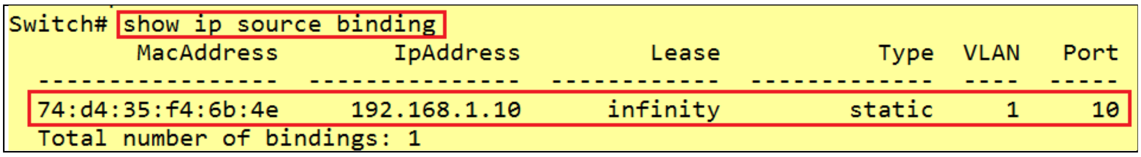
Static Binding :

MAC Address	
IP Address	
VLAN	
Port	○ ● Any

Index	MAC Address	IP Address	Lease	Type	VLAN	Port	□
1	74:d4:35:f4:6b:4e	192.168.1.10	infinity	static	1	10	□

Using CLI:

Figure 7



```
Switch# show ip source binding
          MacAddress            IpAddress             Lease               Type   VLAN    Port
  -----------------   ---------------   ------------   -------------   ----   -----
  74:d4:35:f4:6b:4e      192.168.1.10         infinity            static      1      10
  Total number of bindings: 1
```

If a static binding entry exists for this client already, **go to step 8**.

If a static binding entry does not exist for this client yet, **create an entry for the client with issue and repeat step 4**.

12.8 Does the static binding entry match all of the client's information?

The IP source binding will only allow a client to forward traffic while ARP Inspection is enabled when all the following matches:

- Source MAC address of the client
- Source IP address of the client
- The VLAN client's traffic will pass through
- The physical port on the switch where client's traffic is coming from.

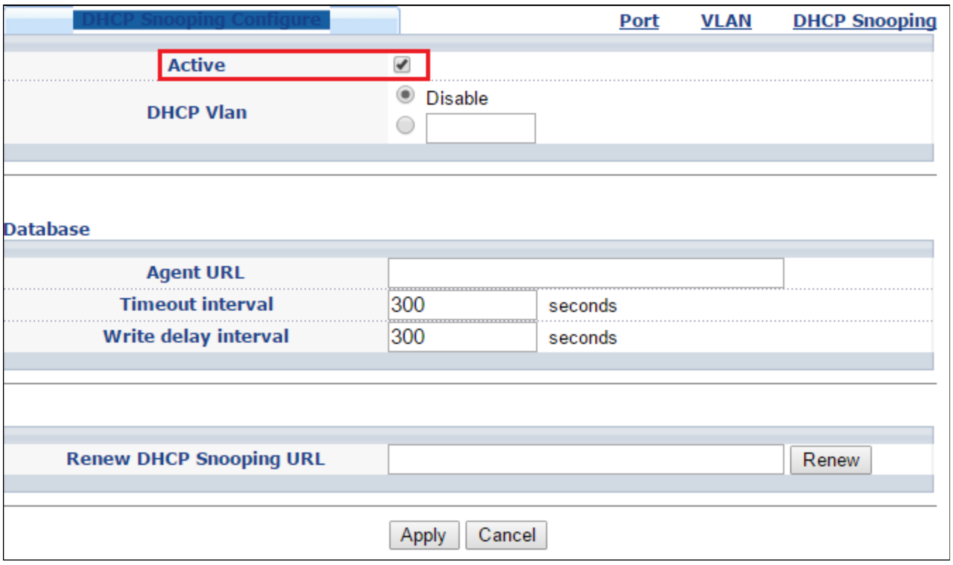
If all four matches should match client's information, **go to <OTHERS>**.

If all four matches did not match client's information, **reconfigure and repeat step 4**.

12.9 Is DHCP Snooping enabled on the Zyxel switch?

Using Web GUI:

Figure 8 Advance Application > IP Source Guard > IP Source Guard Setup > DHCP Snooping > Configure



DHCP Snooping Configure | Port | VLAN | DHCP Snooping

Active ☑

DHCP Vlan ● Disable ○

Database

Agent URL

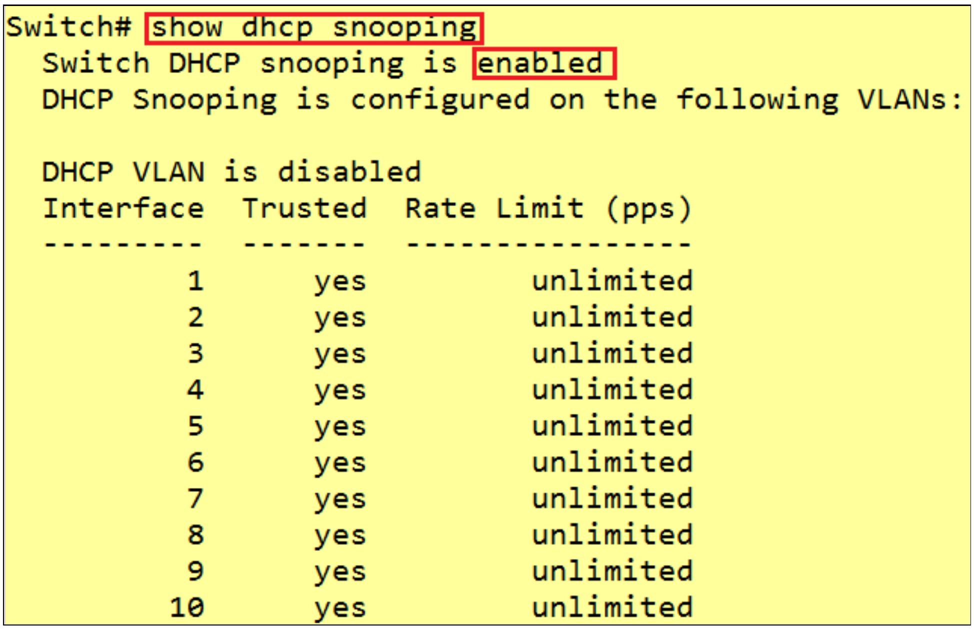
Timeout interval 300 seconds

Write delay interval 300 seconds

Renew DHCP Snooping URL

Using CLI:

Figure 9



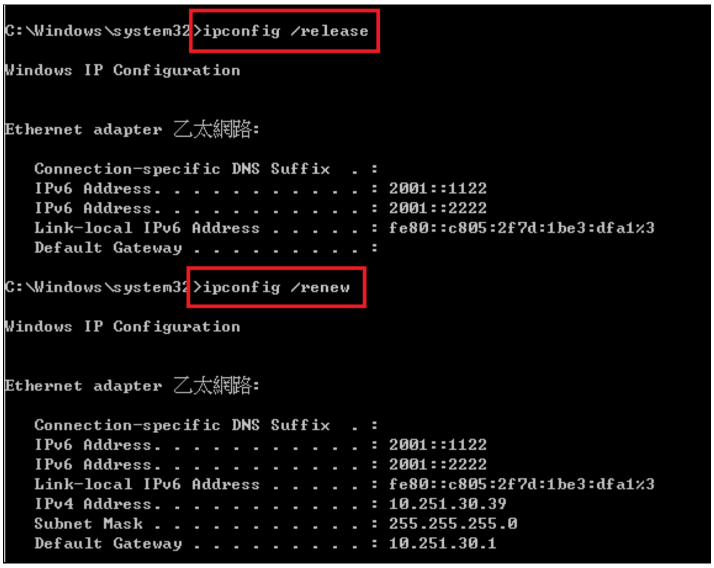
```
Switch# show dhcp snooping
  Switch DHCP snooping is enabled
  DHCP Snooping is configured on the following VLANs:

  DHCP VLAN is disabled
  Interface  Trusted  Rate Limit (pps)
  ---------  -------  ----------------
          1      yes         unlimited
          2      yes         unlimited
          3      yes         unlimited
          4      yes         unlimited
          5      yes         unlimited
          6      yes         unlimited
          7      yes         unlimited
          8      yes         unlimited
          9      yes         unlimited
         10      yes         unlimited
```

If DHCP Snooping is enabled, **go to step 10**.

If DHCP Snooping is disabled, **proceed to the next agenda**.

12.10 Initiate a DHCP-discover on client with issue.

Figure 10

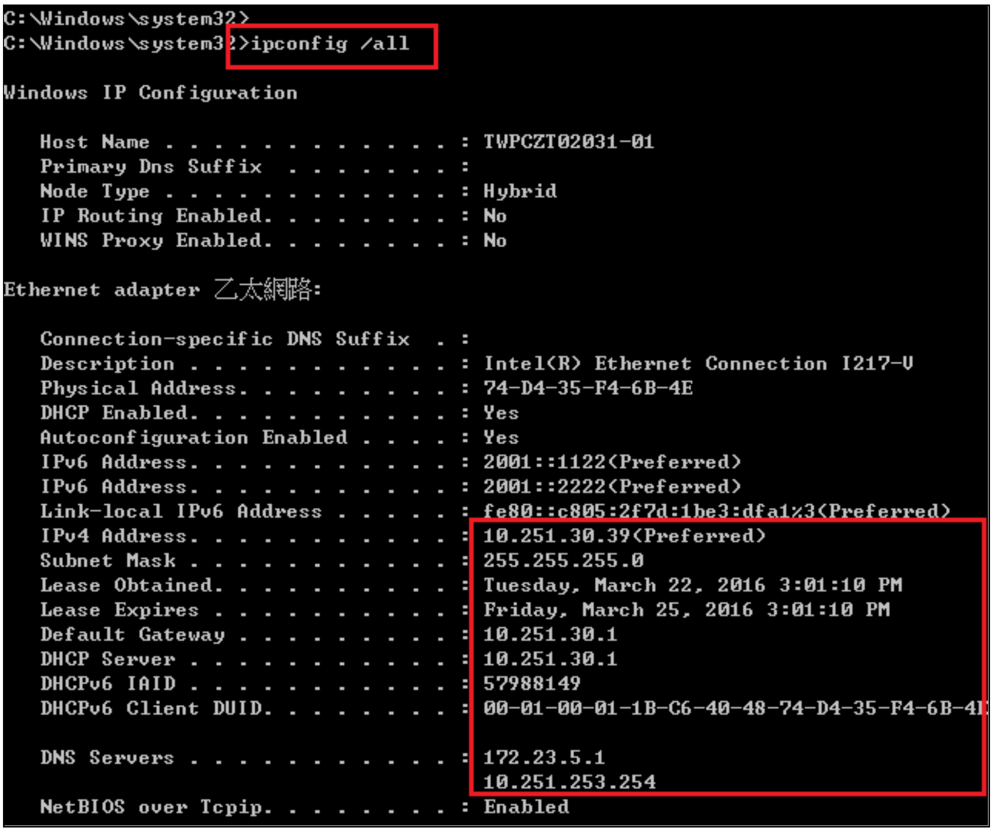


```
C:\Windows\system32>ipconfig /release

Windows IP Configuration


Ethernet adapter 乙太網路:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001::1122
   IPv6 Address. . . . . . . . . . . : 2001::2222
   Link-local IPv6 Address . . . . . : fe80::c805:2f7d:1be3:dfa1%3
   Default Gateway . . . . . . . . . :

C:\Windows\system32>ipconfig /renew

Windows IP Configuration


Ethernet adapter 乙太網路:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001::1122
   IPv6 Address. . . . . . . . . . . : 2001::2222
   Link-local IPv6 Address . . . . . : fe80::c805:2f7d:1be3:dfa1%3
   IPv4 Address. . . . . . . . . . . : 10.251.30.39
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.251.30.1
```

Afterwards, **proceed to step 11**.

12.11 Can the DHCP client receive a correct dynamic IP address?

Figure 11



```
C:\Windows\system32>
C:\Windows\system32>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : TWPCZT02031-01
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter 乙太網路:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Ethernet Connection I217-V
   Physical Address. . . . . . . . . : 74-D4-35-F4-6B-4E
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2001::1122(Preferred)
   IPv6 Address. . . . . . . . . . . : 2001::2222(Preferred)
   Link-local IPv6 Address . . . . . : fe80::c805:2f7d:1be3:dfa1%3(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.251.30.39(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Tuesday, March 22, 2016 3:01:10 PM
   Lease Expires . . . . . . . . . . : Friday, March 25, 2016 3:01:10 PM
   Default Gateway . . . . . . . . . : 10.251.30.1
   DHCP Server . . . . . . . . . . . : 10.251.30.1
   DHCPv6 IAID . . . . . . . . . . . : 57988149
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1B-C6-40-48-74-D4-35-F4-6B-4

   DNS Servers . . . . . . . . . . . : 172.23.5.1
                                       10.251.253.254
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

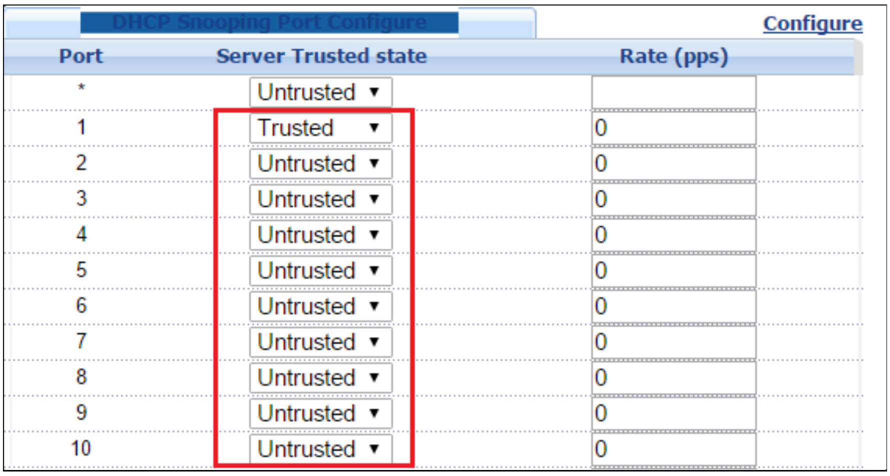
If the dynamic IP configurations are all correct, **go to step 5**.

If there are no dynamic IP configurations or configurations are incorrect, **go to step 12**.

12.12 Is the port to the true DHCP server a “trusted” port?

Using Web GUI:

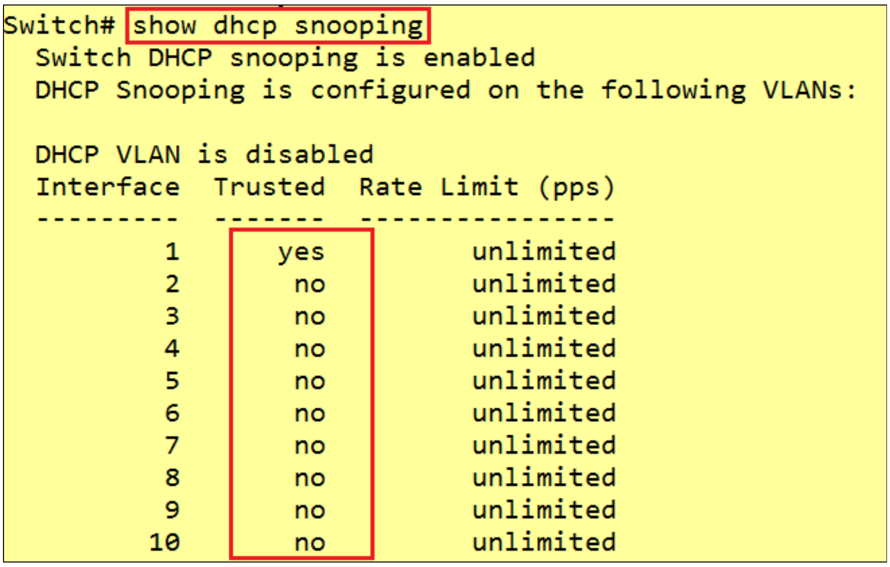
Figure 12 Advance Application > IP Source Guard > IP Source Guard Setup > DHCP Snooping > Configure > Port



Port	Server Trusted state	Rate (pps)
*	Untrusted ▾	
1	Trusted ▾	0
2	Untrusted ▾	0
3	Untrusted ▾	0
4	Untrusted ▾	0
5	Untrusted ▾	0
6	Untrusted ▾	0
7	Untrusted ▾	0
8	Untrusted ▾	0
9	Untrusted ▾	0
10	Untrusted ▾	0

Using CLI:

Figure 13



```
Switch# show dhcp snooping
  Switch DHCP snooping is enabled
  DHCP Snooping is configured on the following VLANs:

  DHCP VLAN is disabled
  Interface  Trusted  Rate Limit (pps)
  ---------  -------  ----------------
          1      yes         unlimited
          2       no         unlimited
          3       no         unlimited
          4       no         unlimited
          5       no         unlimited
          6       no         unlimited
          7       no         unlimited
          8       no         unlimited
          9       no         unlimited
         10       no         unlimited
```

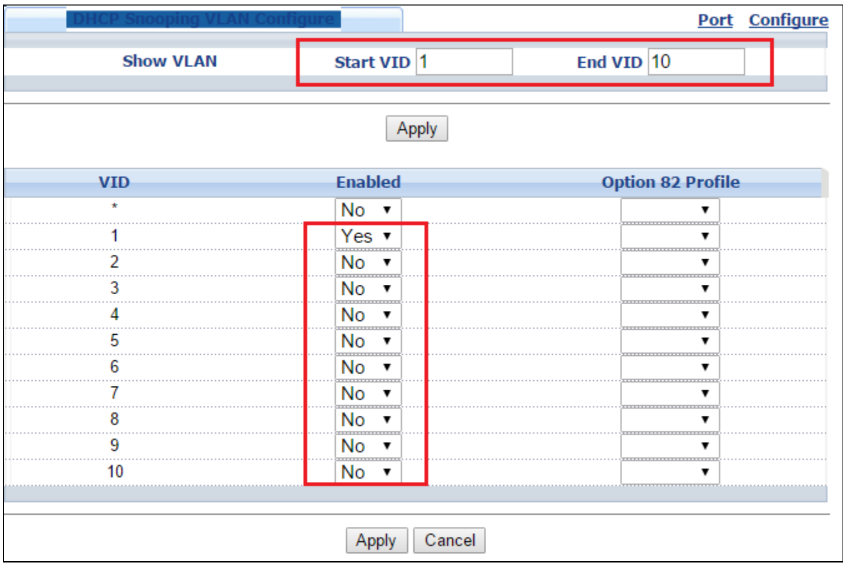
If only the port to the true DHCP server is a “trusted” port, **go to step 13**.

If the port to the true DHCP server is not a “trusted” port, make sure only the port to the true DHCP server is a “trusted” port and **repeat step 10**.

12.13 13. Is DHCP Snooping enabled on the client's VLAN?

Using Web GUI:

Figure 14 Advance Application > IP Source Guard > IP Source Guard Setup > DHCP Snooping > Configure > VLAN



DHCP Snooping VLAN Configure   Port Configure

Show VLAN   Start VID 1   End VID 10

Apply

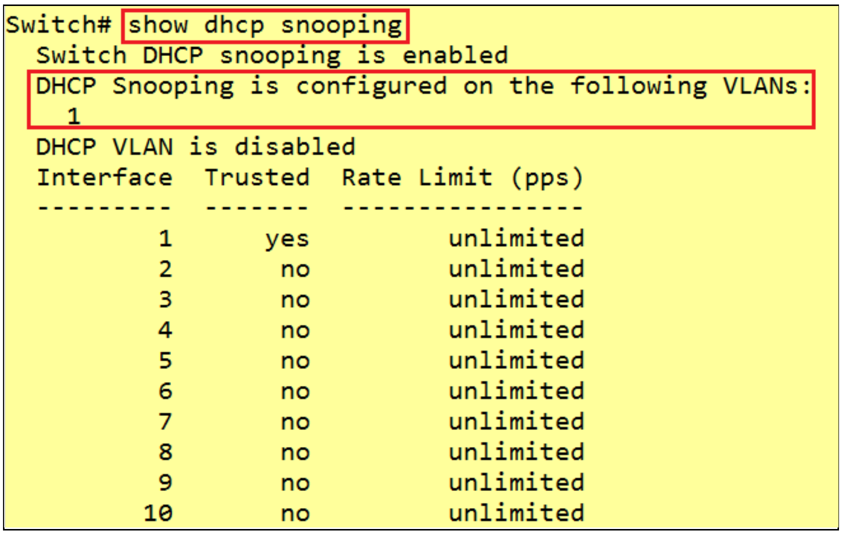
VID	Enabled	Option 82 Profile
*	No	
1	Yes	
2	No	
3	No	
4	No	
5	No	
6	No	
7	No	
8	No	
9	No	
10	No	

Apply Cancel

*You must first indicate the star and end VID in order to view the VID list.

Using CLI:

Figure 15



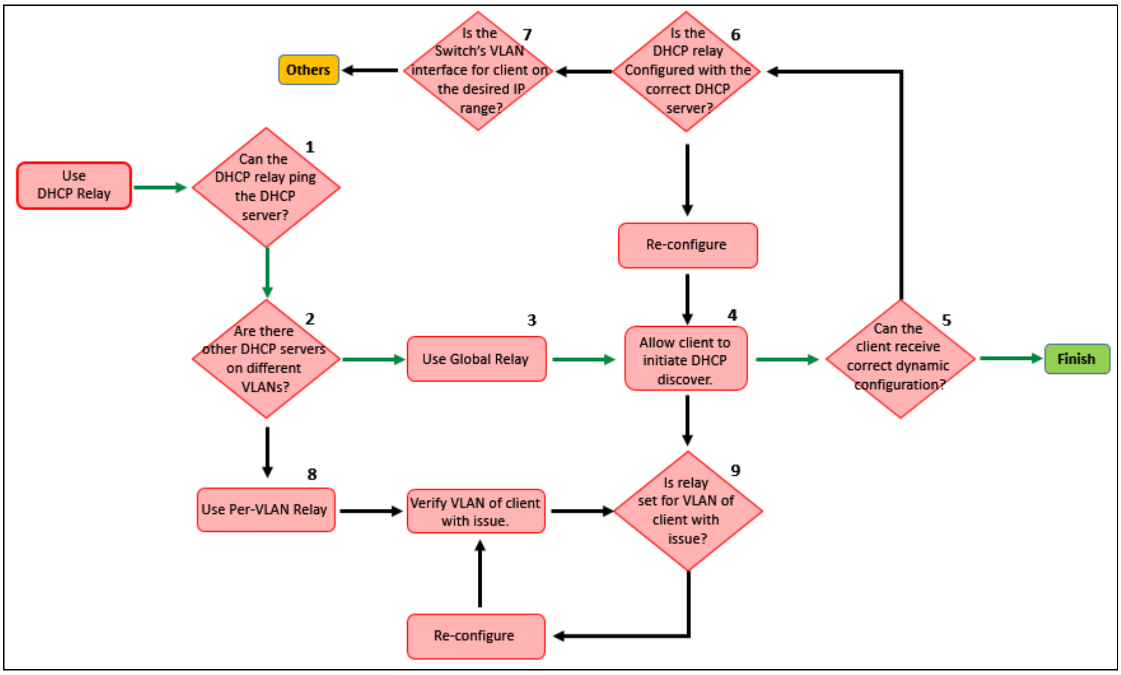
```
Switch# show dhcp snooping
  Switch DHCP snooping is enabled
  DHCP Snooping is configured on the following VLANs:
    1
  DHCP VLAN is disabled
  Interface  Trusted  Rate Limit (pps)
  ---------  -------  ----------------
          1      yes         unlimited
          2       no         unlimited
          3       no         unlimited
          4       no         unlimited
          5       no         unlimited
          6       no         unlimited
          7       no         unlimited
          8       no         unlimited
          9       no         unlimited
         10       no         unlimited
```

If DHCP Snooping is already enabled on the client with issue's VLAN, **go to <OTHERS>**.

If DHCP Snooping is not yet enabled on the client with issue's VLAN, **reconfigure and repeat step 10**.

13 Troubleshooting for DHCP Relay

Flowchart:


Use DHCP Relay
1
Can the DHCP relay ping the DHCP server?
2
Are there other DHCP servers on different VLANs?
3
Use Global Relay
4
Allow client to initiate DHCP discover.
5
Can the client receive correct dynamic configuration?
Finish
6
Is the DHCP relay Configured with the correct DHCP server?
Re-configure
7
Is the Switch's VLAN interface for client on the desired IP range?
Others
8
Use Per-VLAN Relay
Verify VLAN of client with issue.
9
Is relay set for VLAN of client with issue?
Re-configure

OTHERS:

13.1 Can the switch performing DHCP relay ping the DHCP server?

If the DHCP relay can ping the DHCP server, **go to step 2**.

If the DHCP relay cannot ping the DHCP server, **go to <OTHERS>**.

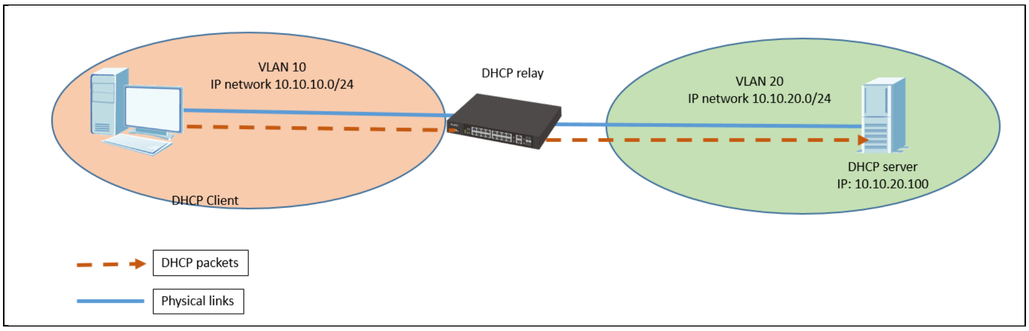
13.2 Are there other DHCP servers on different VLANs?

When clients and DHCP server are on different IP networks, there are two choices for DHCP Relays.

DHCP Smart Relay illustration:

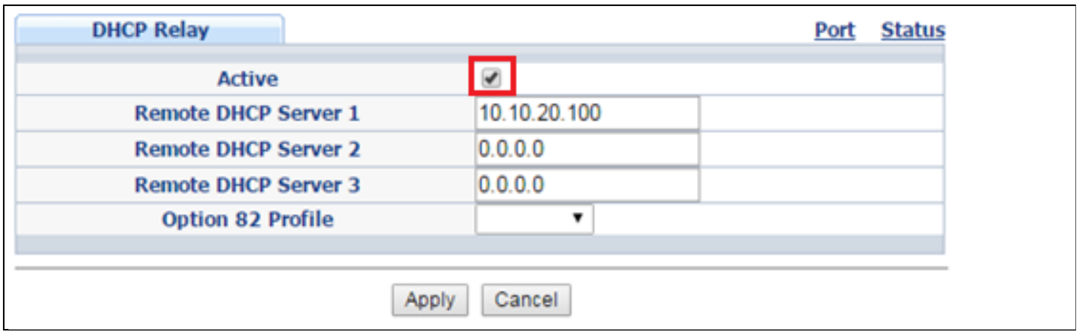
When there is only one DHCP server in the network, you can enabled DHCP Smart relay to send client DHCP packet to the DHCP Server.

Figure 1



Using Web GUI:

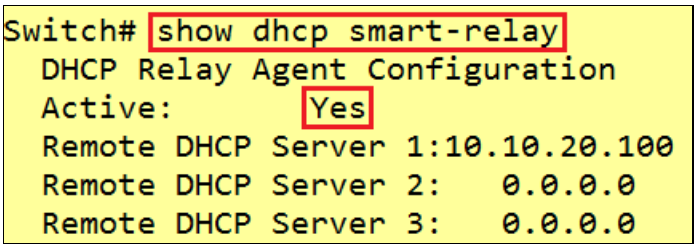
Figure 2 IP Application > DHCP > DHCPv4 > Global



Active	☑
Remote DHCP Server 1	10.10.20.100
Remote DHCP Server 2	0.0.0.0
Remote DHCP Server 3	0.0.0.0
Option 82 Profile	▾

Using CLI:

Figure 3

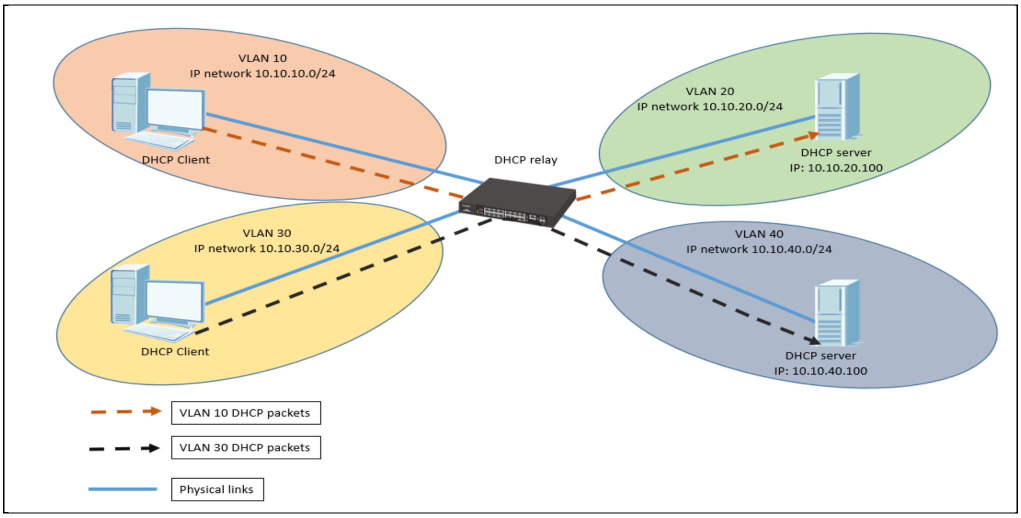


```
Switch# show dhcp smart-relay
  DHCP Relay Agent Configuration
  Active:          Yes
  Remote DHCP Server 1:10.10.20.100
  Remote DHCP Server 2:    0.0.0.0
  Remote DHCP Server 3:    0.0.0.0
```

DHCP Per-VLAN Relay illustration:

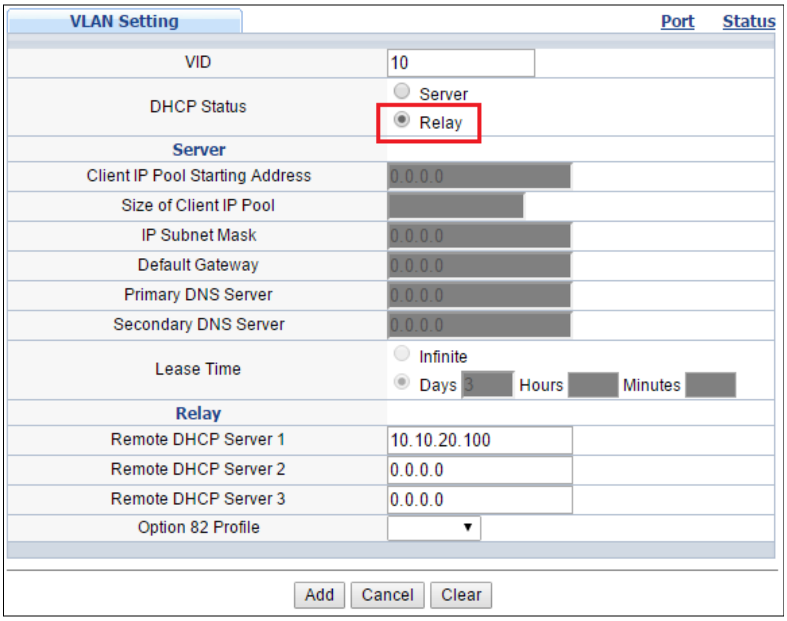
For a larger enterprise network deployment, more than one DHCP server may exist on different LAN segments while clients on specific VLANs need to acquire configurations from specific DHCP servers.

Figure 4



Using Web GUI:

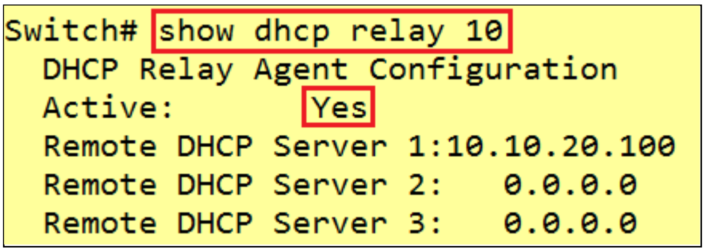
Figure 5 IP Application > DHCP > DHCPv4 > VLAN



VID	10
DHCP Status	○ Server ● Relay
Server	
Client IP Pool Starting Address	0.0.0.0
Size of Client IP Pool	
IP Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0
Lease Time	○ Infinite ● Days 3 Hours Minutes
Relay	
Remote DHCP Server 1	10.10.20.100
Remote DHCP Server 2	0.0.0.0
Remote DHCP Server 3	0.0.0.0
Option 82 Profile	▾

Using CLI:

Figure 6



```
Switch# show dhcp relay 10
  DHCP Relay Agent Configuration
  Active:          Yes
  Remote DHCP Server 1:10.10.20.100
  Remote DHCP Server 2:    0.0.0.0
  Remote DHCP Server 3:    0.0.0.0
```

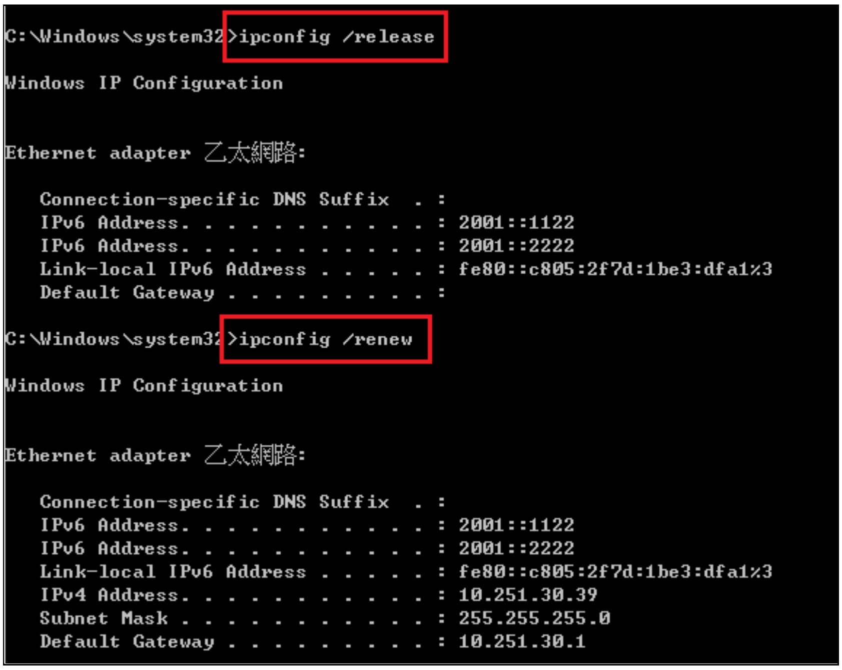
If customer has DHCP servers on only one VLAN, **configure DHCP Smart Relay and go to step 3**.

If customer has DHCP servers on different VLANs, **configure per-VLAN DHCP Relay and go to step 9**.

13.3 Allow client to initiate a DHCP discover.

Operating systems like Microsoft Windows can manually initiate a DHCP discover in the Windows command line.

Figure 7



```
C:\Windows\system32>ipconfig /release

Windows IP Configuration


Ethernet adapter 乙太網路:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001::1122
   IPv6 Address. . . . . . . . . . . : 2001::2222
   Link-local IPv6 Address . . . . . : fe80::c805:2f7d:1be3:dfa1%3
   Default Gateway . . . . . . . . . :

C:\Windows\system32>ipconfig /renew

Windows IP Configuration


Ethernet adapter 乙太網路:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001::1122
   IPv6 Address. . . . . . . . . . . : 2001::2222
   Link-local IPv6 Address . . . . . : fe80::c805:2f7d:1be3:dfa1%3
   IPv4 Address. . . . . . . . . . . : 10.251.30.39
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.251.30.1
```

Afterwards, **proceed to step 4**.

13.4 Can the client with issue receive the correct dynamic configurations?

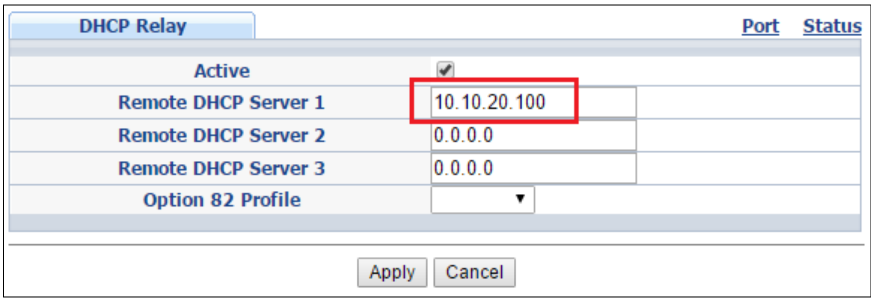
If the client receives the correct dynamic configuration, **proceed to the next agenda**.

If the client does not receive the correct dynamic configuration, **go to step 5**.

13.5 Is the DHCP relay configured with the correct DHCP server address?

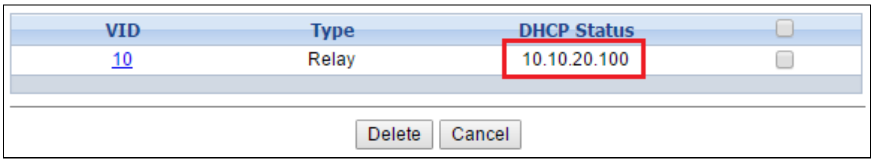
Using Web GUI:

Figure 8 IP Application > DHCP > DHCPv4 > Global



Active	☑
Remote DHCP Server 1	10.10.20.100
Remote DHCP Server 2	0.0.0.0
Remote DHCP Server 3	0.0.0.0
Option 82 Profile	▾

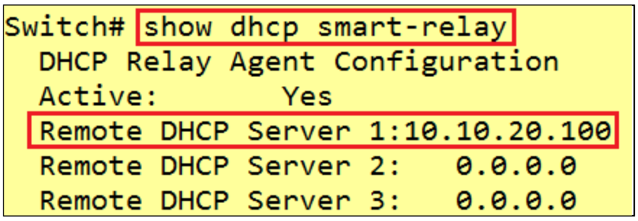
Figure 9 IP Application > DHCP > DHCPv4 > VLAN



VID	Type	DHCP Status	□
10	Relay	10.10.20.100	□

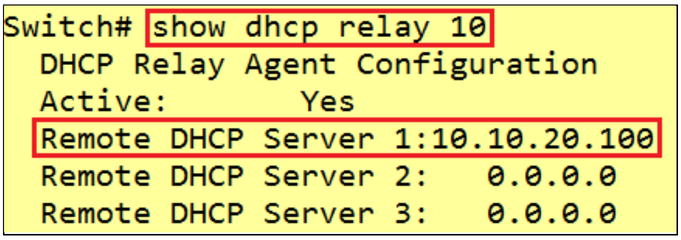
Using CLI:

Figure 10 DHCP Smart Relay



```
Switch# show dhcp smart-relay
  DHCP Relay Agent Configuration
  Active:         Yes
  Remote DHCP Server 1:10.10.20.100
  Remote DHCP Server 2:    0.0.0.0
  Remote DHCP Server 3:    0.0.0.0
```

Figure 11 Per-VLAN Relay



```
Switch# show dhcp relay 10
  DHCP Relay Agent Configuration
  Active:        Yes
  Remote DHCP Server 1:10.10.20.100
  Remote DHCP Server 2:    0.0.0.0
  Remote DHCP Server 3:    0.0.0.0
```

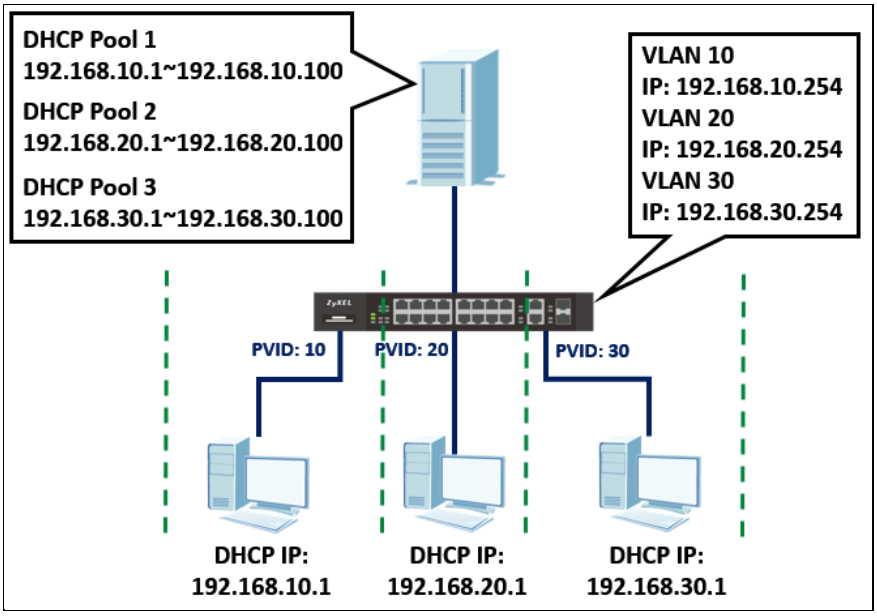
If the relay is configured with the correct remote DHCP server address, **go to step 6**.

If the relay is not configured with the correct remote DHCP server address, **re-configure and repeat step 3**.

13.6 Is the switch’s VLAN interface for client using the correct IP subnet?

The DHCP server will provide its dynamic configuration based on the DHCP relay’s VLAN interface towards the DHCP client. This means that if a client sends a DHCP discover to the DHCP relay on VLAN 10, the DHCP relay sends this request to the DHCP server using its VLAN 10 IP address. The DHCP server then matches the VLAN 10 IP address into its local pool to determine which dynamic configuration for clients to use.

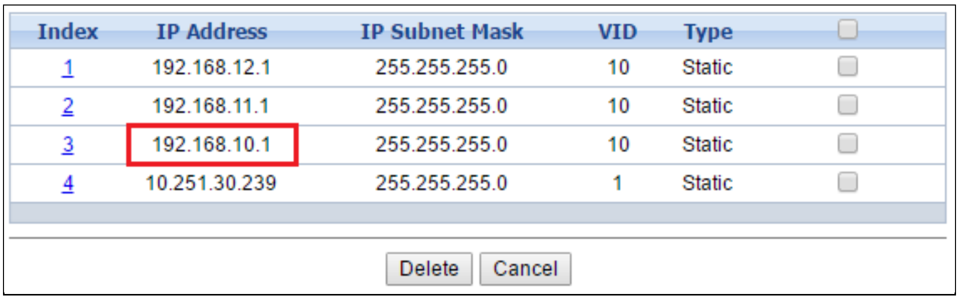
Figure 16



In the event that the VLAN interface has multiple IP addresses, the DHCP server will provide dynamic configurations for the lowest IP address.

Using Web GUI:

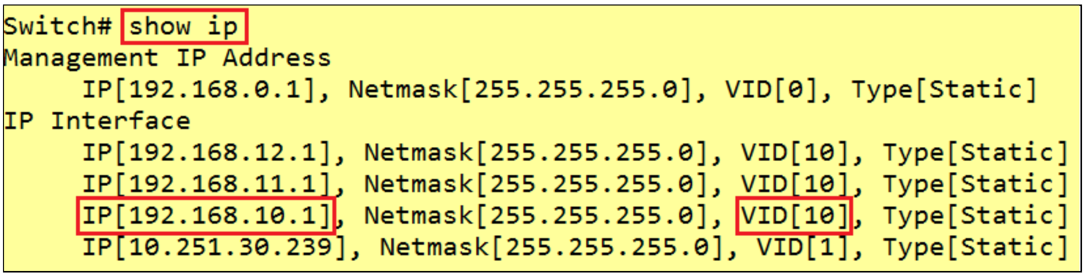
Figure 17 Basic Settings > IP Setup



Index	IP Address	IP Subnet Mask	VID	Type	☐
1	192.168.12.1	255.255.255.0	10	Static	☐
2	192.168.11.1	255.255.255.0	10	Static	☐
3	192.168.10.1	255.255.255.0	10	Static	☐
4	10.251.30.239	255.255.255.0	1	Static	☐

Using CLI:

Figure 18



```
Switch# show ip
Management IP Address
     IP[192.168.0.1], Netmask[255.255.255.0], VID[0], Type[Static]
IP Interface
     IP[192.168.12.1], Netmask[255.255.255.0], VID[10], Type[Static]
     IP[192.168.11.1], Netmask[255.255.255.0], VID[10], Type[Static]
     IP[192.168.10.1], Netmask[255.255.255.0], VID[10], Type[Static]
     IP[10.251.30.239], Netmask[255.255.255.0], VID[1], Type[Static]
```

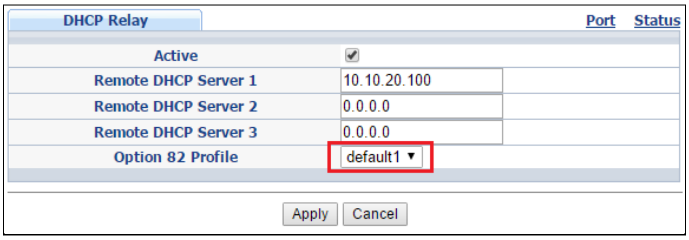
If the VLAN's IP interface is configured correctly, **go to step 7**.

If the VLAN's IP interface is not configured correctly, **reconfigure and repeat step 3**.

13.7 Is the DHCP relay's option 82 configured correctly?

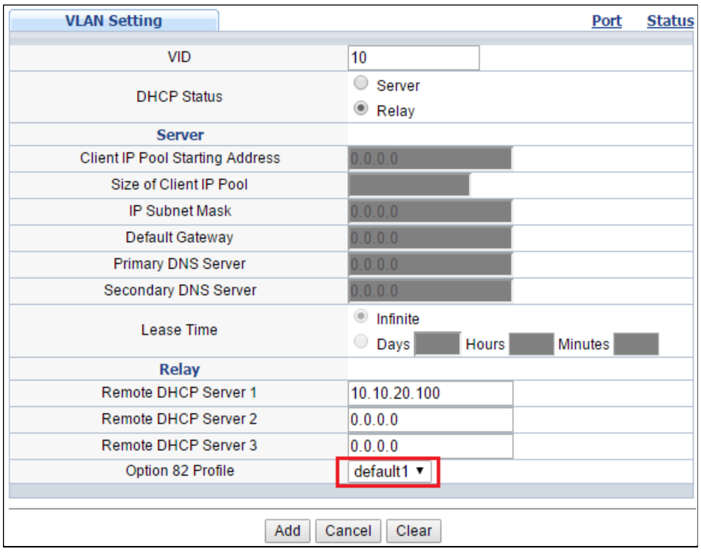
If DHCP Relay option 82 profile is used, check the circuit-ID in the DHCP server. For example, option profile default 1(Slot-port, VLAN), the relay agent adds option 82 circuit-id in DHCP packets and forward this to the DHCP Server, then the DHCP server received the packet, it will check the option 82 and assign IP address.

Figure 19 DHCP Smart Relay Option 82



Active	☑
Remote DHCP Server 1	10.10.20.100
Remote DHCP Server 2	0.0.0.0
Remote DHCP Server 3	0.0.0.0
Option 82 Profile	default1 ▾

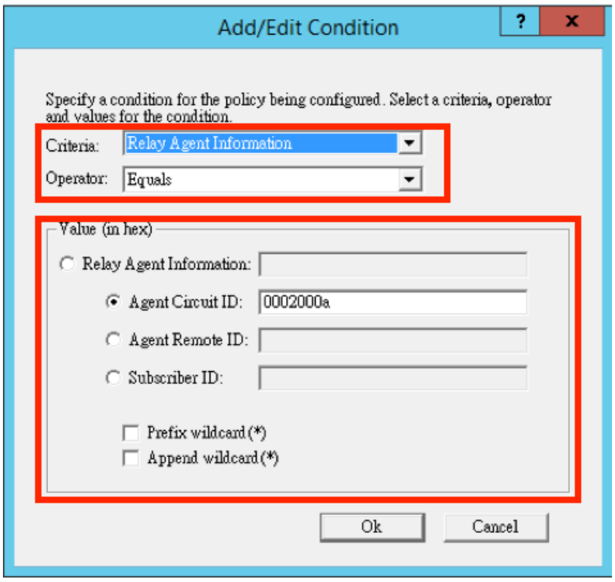
Figure 20 Per-VLAN Relay Option 82



VID	10
DHCP Status	○ Server ● Relay
Server	
Client IP Pool Starting Address	0.0.0.0
Size of Client IP Pool	
IP Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0
Lease Time	● Infinite ○ Days Hours Minutes
Relay	
Remote DHCP Server 1	10.10.20.100
Remote DHCP Server 2	0.0.0.0
Remote DHCP Server 3	0.0.0.0
Option 82 Profile	default1 ▾

For Windows OS, check the IP Pool policy. Below is a configuration example; 0002000a, "00" stands for slot-id, "02 stands for port number on relay agent and "000a" is the VLAN ID.

Figure 21



Specify a condition for the policy being configured. Select a criteria, operator and values for the condition.

Criteria: Relay Agent Information

Operator: Equals

Value (in hex)

○ Relay Agent Information:

● Agent Circuit ID: 0002000a

○ Agent Remote ID:

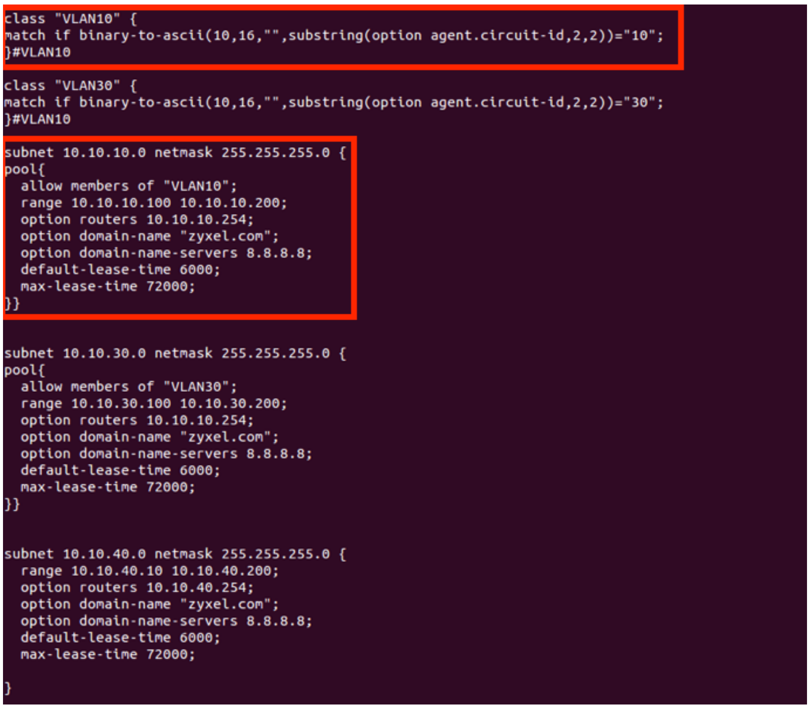
○ Subscriber ID:

□ Prefix wildcard (*)

□ Append wildcard (*)

For Ubuntu, create the rule to assign IP address, below is an example circuit-id of dhcpd.conf;

Figure 22



```
class "VLAN10" {
match if binary-to-ascii(10,16,"",substring(option agent.circuit-id,2,2))="10";
}#VLAN10

class "VLAN30" {
match if binary-to-ascii(10,16,"",substring(option agent.circuit-id,2,2))="30";
}#VLAN10

subnet 10.10.10.0 netmask 255.255.255.0 {
pool{
  allow members of "VLAN10";
  range 10.10.10.100 10.10.10.200;
  option routers 10.10.10.254;
  option domain-name "zyxel.com";
  option domain-name-servers 8.8.8.8;
  default-lease-time 6000;
  max-lease-time 72000;
}}


subnet 10.10.30.0 netmask 255.255.255.0 {
pool{
  allow members of "VLAN30";
  range 10.10.30.100 10.10.30.200;
  option routers 10.10.10.254;
  option domain-name "zyxel.com";
  option domain-name-servers 8.8.8.8;
  default-lease-time 6000;
  max-lease-time 72000;
}}


subnet 10.10.40.0 netmask 255.255.255.0 {
  range 10.10.40.10 10.10.40.200;
  option routers 10.10.40.254;
  option domain-name "zyxel.com";
  option domain-name-servers 8.8.8.8;
  default-lease-time 6000;
  max-lease-time 72000;

}
```

If option 82 is configured correctly, **go to <OTHERS>**.

If option 82 is not configured correctly, **reconfigure and repeat step 3**

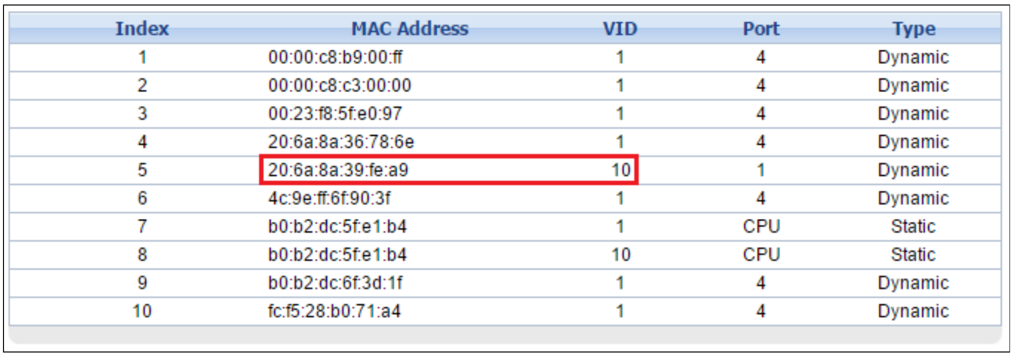
13.8 Verify which VLAN the client with issue belongs.

You can verify this by checking the MAC address table.

Below is an example on how to determine which VLAN client "*20:6a:8a:39:fe:a9*" is being processed in.

Using Web GUI:

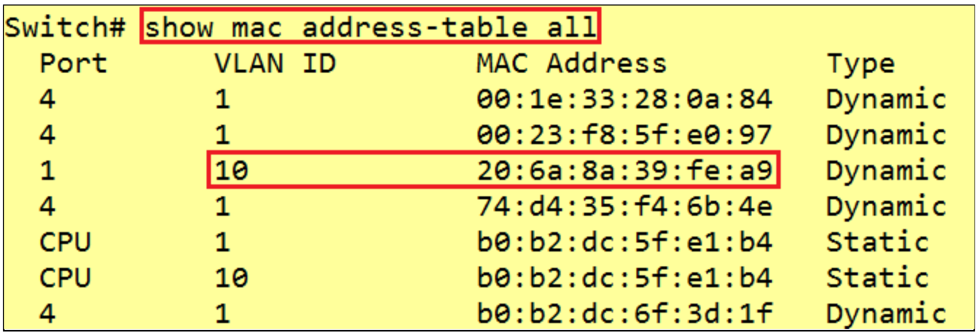
Figure 23 Management > MAC Table



Index	MAC Address	VID	Port	Type
1	00:00:c8:b9:00:ff	1	4	Dynamic
2	00:00:c8:c3:00:00	1	4	Dynamic
3	00:23:f8:5f:e0:97	1	4	Dynamic
4	20:6a:8a:36:78:6e	1	4	Dynamic
5	20:6a:8a:39:fe:a9	10	1	Dynamic
6	4c:9e:ff:6f:90:3f	1	4	Dynamic
7	b0:b2:dc:5f:e1:b4	1	CPU	Static
8	b0:b2:dc:5f:e1:b4	10	CPU	Static
9	b0:b2:dc:6f:3d:1f	1	4	Dynamic
10	fc:f5:28:b0:71:a4	1	4	Dynamic

Using CLI:

Figure 24



```
Switch# show mac address-table all
  Port        VLAN ID        MAC Address        Type
  4           1              00:1e:33:28:0a:84  Dynamic
  4           1              00:23:f8:5f:e0:97  Dynamic
  1           10             20:6a:8a:39:fe:a9  Dynamic
  4           1              74:d4:35:f4:6b:4e  Dynamic
  CPU         1              b0:b2:dc:5f:e1:b4  Static
  CPU         10             b0:b2:dc:5f:e1:b4  Static
  4           1              b0:b2:dc:6f:3d:1f  Dynamic
```

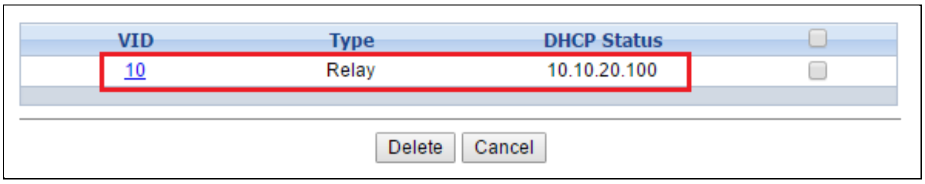
After verifying client's VLAN, **go to step 9**.

13.9 Is the DHCP relay set for the VLAN of the client with issue?

Make sure that the per-VLAN DHCP relay is configured on the correct VLAN of the client with issue

Using Web GUI:

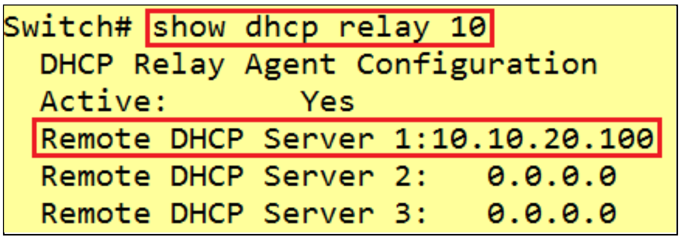
Figure 25 IP Application > DHCP > DHCPv4 > VLAN



VID	Type	DHCP Status	□
10	Relay	10.10.20.100	□

Using CLI:

Figure 26



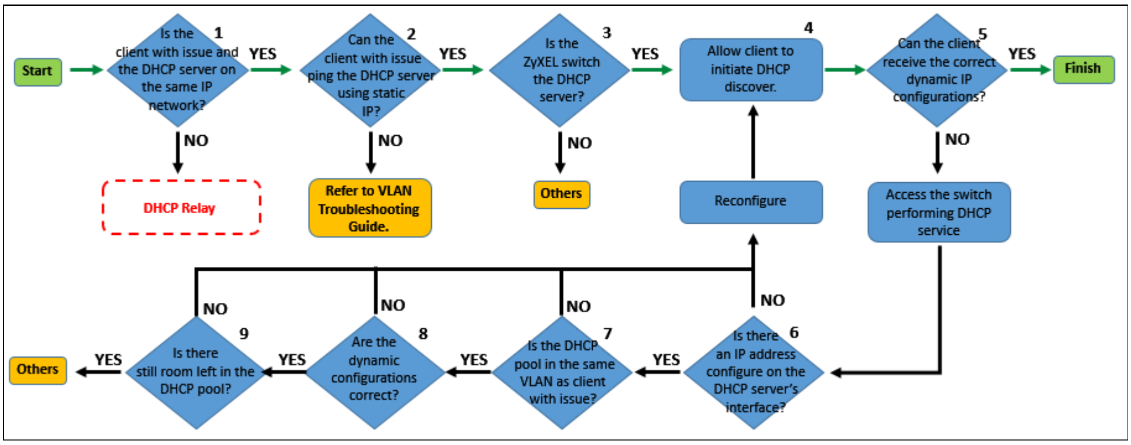
```
Switch# show dhcp relay 10
  DHCP Relay Agent Configuration
  Active:          Yes
  Remote DHCP Server 1:10.10.20.100
  Remote DHCP Server 2:    0.0.0.0
  Remote DHCP Server 3:    0.0.0.0
```

If the VLAN is configured correctly, **proceed to step 4**.

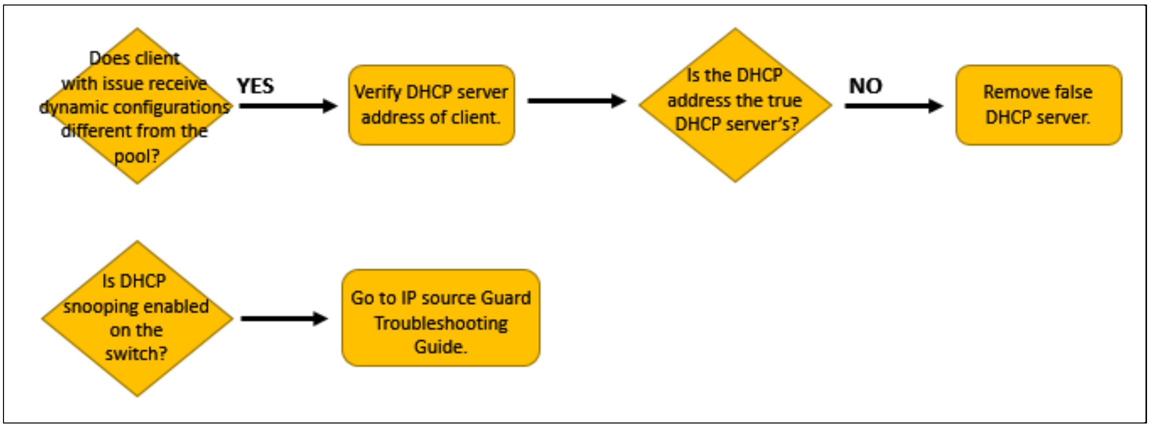
If the VLAN is not configured correctly, **reconfigure and repeat step 8**.

14 Troubleshooting for DHCP Server

Flowchart:


Start
1
Is the client with issue and the DHCP server on the same IP network?
YES
NO
DHCP Relay
2
Can the client with issue ping the DHCP server using static IP?
YES
NO
Refer to VLAN Troubleshooting Guide.
3
Is the ZyXEL switch the DHCP server?
YES
NO
Others
4
Allow client to initiate DHCP discover.
Reconfigure
5
Can the client receive the correct dynamic IP configurations?
YES
Finish
NO
Access the switch performing DHCP service
6
Is there an IP address configure on the DHCP server's interface?
NO
YES
7
Is the DHCP pool in the same VLAN as client with issue?
NO
YES
8
Are the dynamic configurations correct?
NO
YES
9
Is there still room left in the DHCP pool?
NO
YES
Others

OTHERS:


Does client with issue receive dynamic configurations different from the pool?
YES
Verify DHCP server address of client.
Is the DHCP address the true DHCP server's?
NO
Remove false DHCP server.
Is DHCP snooping enabled on the switch?
Go to IP source Guard Troubleshooting Guide.

14.1 Is the client with issue and DHCP server on the same IP network?

If the client and server are on the same IP network, **go to step 2**.

If the client and server are not on the same IP network, **proceed to the DHCP Relay Troubleshooting Guide**.

14.2 Can the client with issue ping the DHCP server's interface using a static IP configuration?

If the client with issue can ping the DHCP server, **go to step 3**.

If the client with issue cannot ping the DHCP server, **proceed to the VLAN Troubleshooting Guide**.

14.3 Is the Zyxel switch the DHCP server?

Figure 1 Switch is the local DHCP server

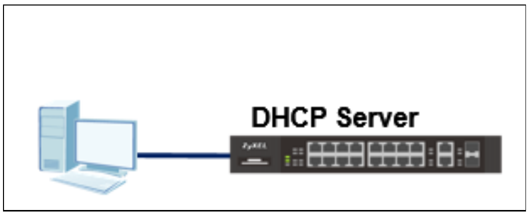
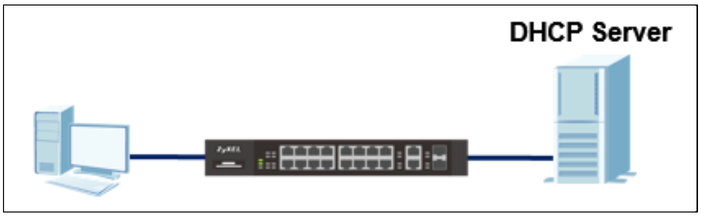


Figure 2 Network uses an external DHCP server

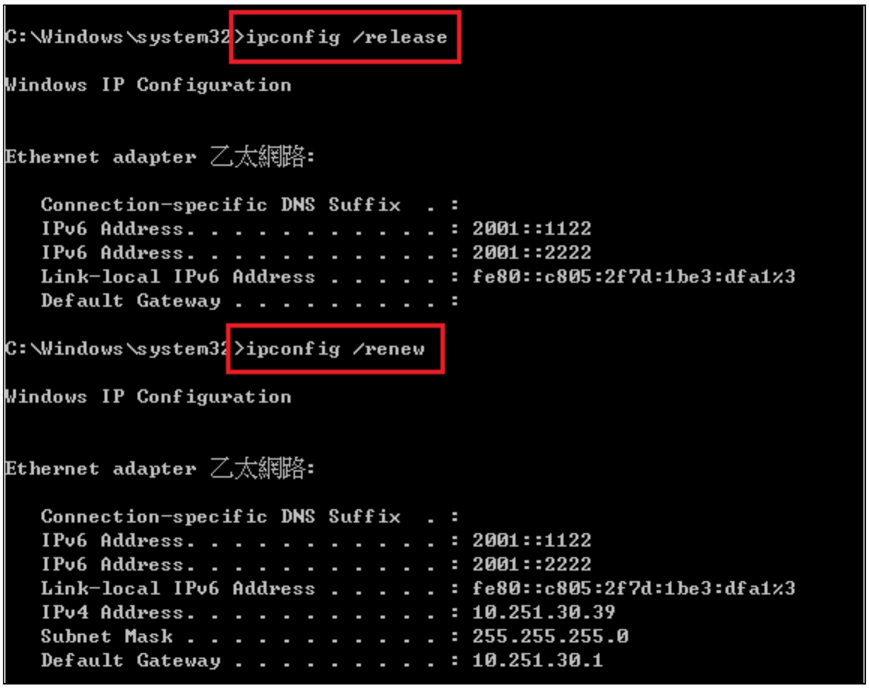


If the Zyxel switch is the DHCP server, **go to step 4**.

If the Zyxel switch is not the DHCP server, **go to <OTHERS>**.

14.4 Allow client with issue to initiate a DHCP discover.

Figure 3

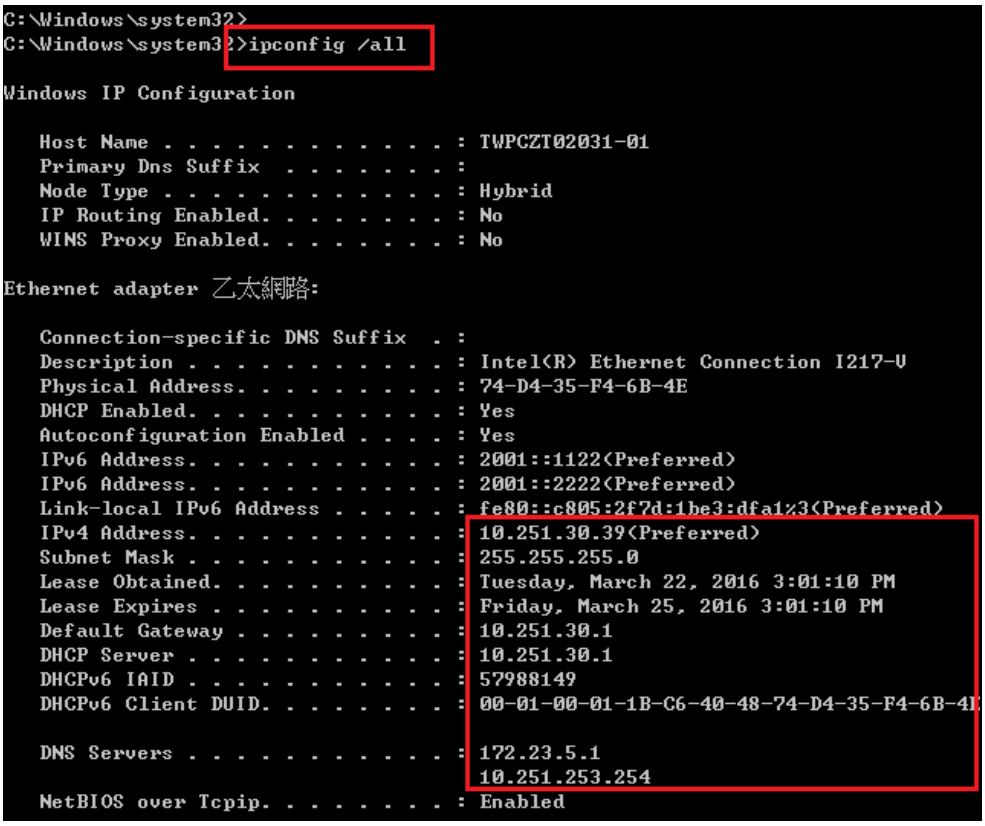


```
C:\Windows\system32>ipconfig /release

Windows IP Configuration


Ethernet adapter 乙太網路:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001::1122
   IPv6 Address. . . . . . . . . . . : 2001::2222
   Link-local IPv6 Address . . . . . : fe80::c805:2f7d:1be3:dfa1%3
   Default Gateway . . . . . . . . . :

C:\Windows\system32>ipconfig /renew

Windows IP Configuration


Ethernet adapter 乙太網路:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001::1122
   IPv6 Address. . . . . . . . . . . : 2001::2222
   Link-local IPv6 Address . . . . . : fe80::c805:2f7d:1be3:dfa1%3
   IPv4 Address. . . . . . . . . . . : 10.251.30.39
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.251.30.1
```

Afterwards, **proceed to step 5**.

14.5 Can the DHCP client receive a correct dynamic IP address?

Figure 4



```
C:\Windows\system32>
C:\Windows\system32>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : TWPCZT02031-01
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter 乙太網路:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Ethernet Connection I217-V
   Physical Address. . . . . . . . . : 74-D4-35-F4-6B-4E
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2001::1122(Preferred)
   IPv6 Address. . . . . . . . . . . : 2001::2222(Preferred)
   Link-local IPv6 Address . . . . . : fe80::c805:2f7d:1be3:dfa1%3(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.251.30.39(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Tuesday, March 22, 2016 3:01:10 PM
   Lease Expires . . . . . . . . . . : Friday, March 25, 2016 3:01:10 PM
   Default Gateway . . . . . . . . . : 10.251.30.1
   DHCP Server . . . . . . . . . . . : 10.251.30.1
   DHCPv6 IAID . . . . . . . . . . . : 57988149
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1B-C6-40-48-74-D4-35-F4-6B-4E

   DNS Servers . . . . . . . . . . . : 172.23.5.1
                                       10.251.253.254
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

If the dynamic IP configurations are all correct, **proceed to the next agenda**.

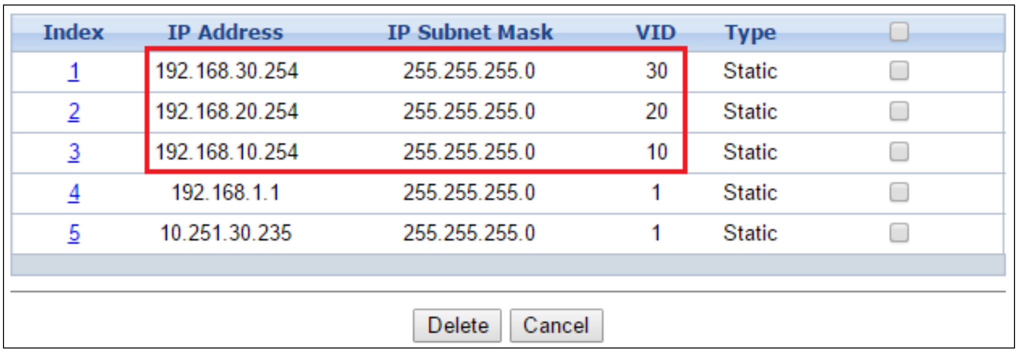
If there are no dynamic IP configurations or configurations are incorrect, access the switch performing DHCP service and **go to step 6**.

14.6 Is there an IP address configured on the DHCP server's interface?

You cannot configure a DHCP pool if the VLAN for the DHCP service has no IP address configured.

Using Web GUI:

Figure 5 Basic Setting > IP Setup

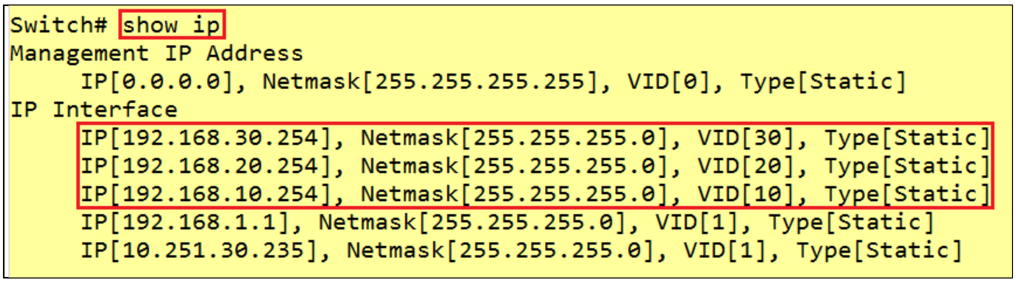


Index	IP Address	IP Subnet Mask	VID	Type	□
1	192.168.30.254	255.255.255.0	30	Static	□
2	192.168.20.254	255.255.255.0	20	Static	□
3	192.168.10.254	255.255.255.0	10	Static	□
4	192.168.1.1	255.255.255.0	1	Static	□
5	10.251.30.235	255.255.255.0	1	Static	□

In this example, VLAN 10, 20, and 30 will be used for DHCP service.

Using CLI:

Figure 6



```
Switch# show ip
Management IP Address
     IP[0.0.0.0], Netmask[255.255.255.255], VID[0], Type[Static]
IP Interface
     IP[192.168.30.254], Netmask[255.255.255.0], VID[30], Type[Static]
     IP[192.168.20.254], Netmask[255.255.255.0], VID[20], Type[Static]
     IP[192.168.10.254], Netmask[255.255.255.0], VID[10], Type[Static]
     IP[192.168.1.1], Netmask[255.255.255.0], VID[1], Type[Static]
     IP[10.251.30.235], Netmask[255.255.255.0], VID[1], Type[Static]
```

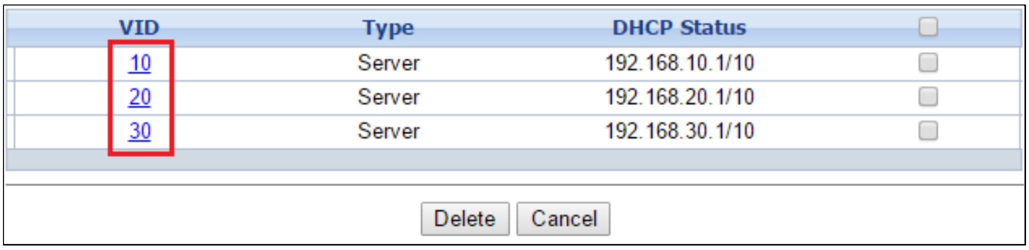
If the DHCP server's interfaces have been configured with an IP address, **go to step 7**.

If the DHCP server's interfaces have not yet been configured with an IP address, **reconfigure and repeat step 4**.

14.7 Is the DHCP pool in the same VLAN as the client with issue?

Using Web GUI:

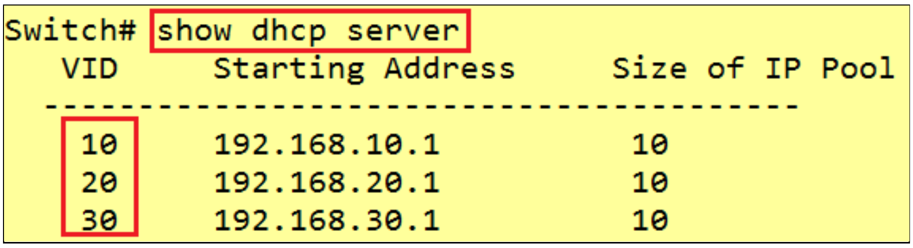
Figure 7 IP Setting > DHCP > DHCPv4 > VLAN



VID	Type	DHCP Status	□
10	Server	192.168.10.1/10	□
20	Server	192.168.20.1/10	□
30	Server	192.168.30.1/10	□

Using Web GUI:

Figure 8



```
Switch# show dhcp server
   VID       Starting Address      Size of IP Pool
  ----------------------------------------
    10       192.168.10.1           10
    20       192.168.20.1           10
    30       192.168.30.1           10
```

If a DHCP pool exist for the client with issues VLAN, **go to step 8**.

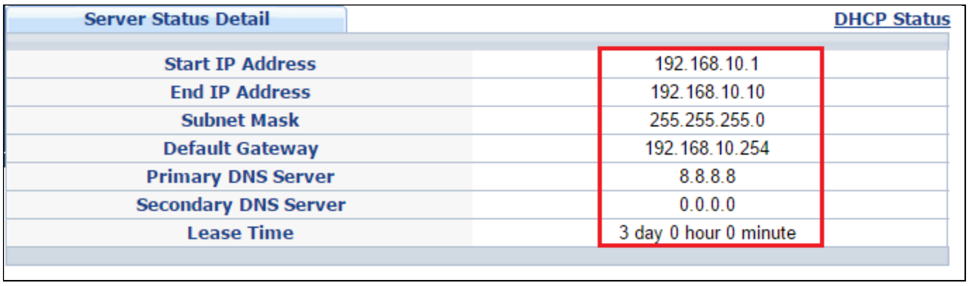
If a DHCP pool does not exist for the client with issues VLAN, **reconfigure and repeat step 4**.

14.8 Is the configured DHCP pool configured correctly?

For clients to successfully access the internet, **the IP address, subnet mask, default gateway, and at least a primary DNS server** must be configured correctly.

Using Web GUI:

Figure 9 IP Setting > DHCP > DHCPv4 > "Index"

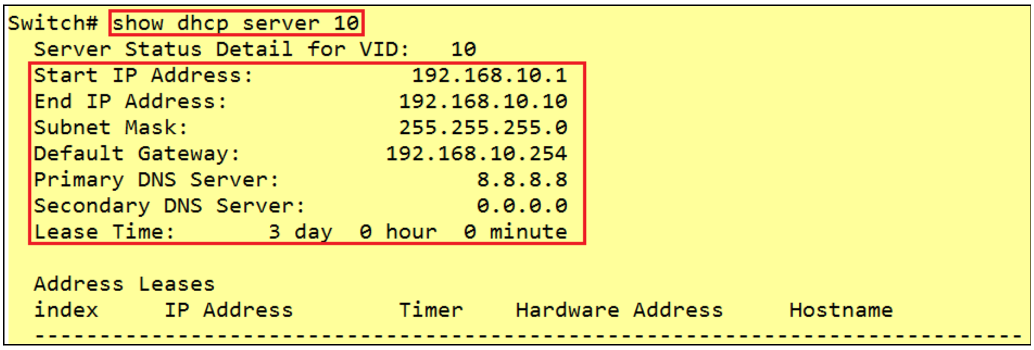


Server Status Detail　　DHCP Status

Start IP Address	192.168.10.1
End IP Address	192.168.10.10
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.254
Primary DNS Server	8.8.8.8
Secondary DNS Server	0.0.0.0
Lease Time	3 day 0 hour 0 minute

Using CLI:

Figure 10



```
Switch# show dhcp server 10
  Server Status Detail for VID:   10
  Start IP Address:            192.168.10.1
  End IP Address:             192.168.10.10
  Subnet Mask:                255.255.255.0
  Default Gateway:           192.168.10.254
  Primary DNS Server:               8.8.8.8
  Secondary DNS Server:             0.0.0.0
  Lease Time:          3 day  0 hour  0 minute

  Address Leases
  index      IP Address        Timer    Hardware Address     Hostname
  ---------------------------------------------------------------------------
```

If the configured DHCP pool is correct, **go to step 9**.

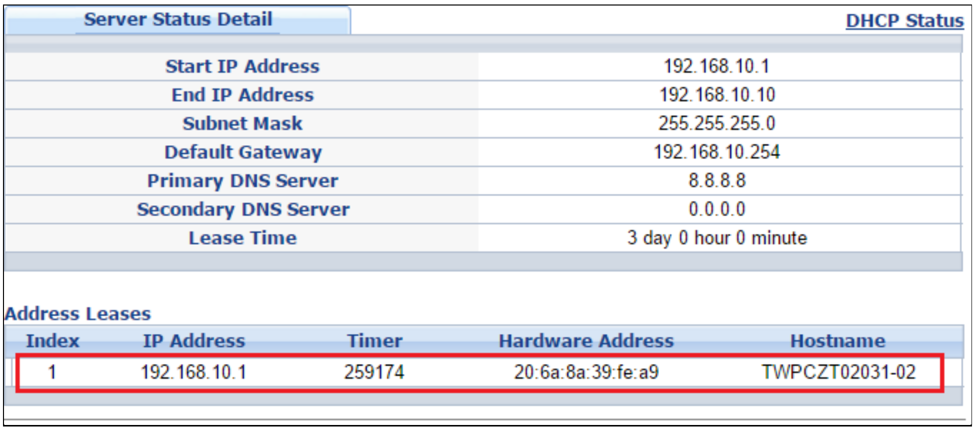
If the configured DHCP pool is incorrect, **reconfigure and repeat step 4**.

14.9 Is there still room left in the DHCP pool?

The **size of client IP pool** in the DHCP configuration limits the number of how many clients can successfully request a dynamic configuration from the DHCP server. Once the limit has been reached, the DHCP server will no longer send out DHCP offers.

Using Web GUI:

Figure 11 IP Setting > DHCP > DHCPv4 > "Index"



Start IP Address	192.168.10.1
End IP Address	192.168.10.10
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.254
Primary DNS Server	8.8.8.8
Secondary DNS Server	0.0.0.0
Lease Time	3 day 0 hour 0 minute

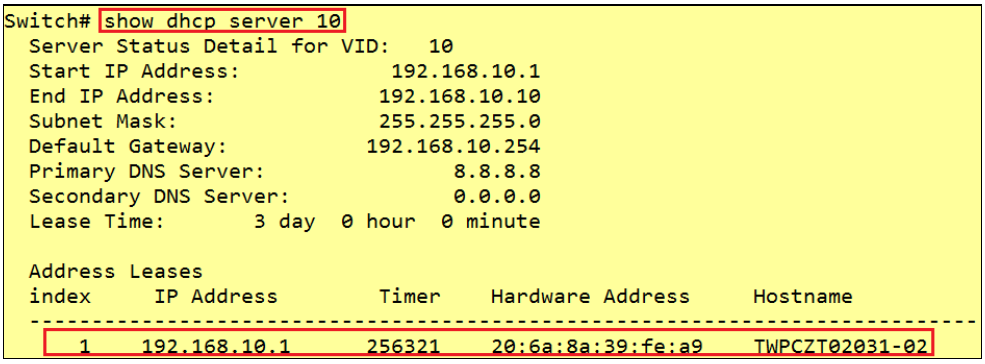
Address Leases

Index	IP Address	Timer	Hardware Address	Hostname
1	192.168.10.1	259174	20:6a:8a:39:fe:a9	TWPCZT02031-02

Check the index number to verify how many clients are currently using the DHCP pool.

Using CLI:

Figure 12



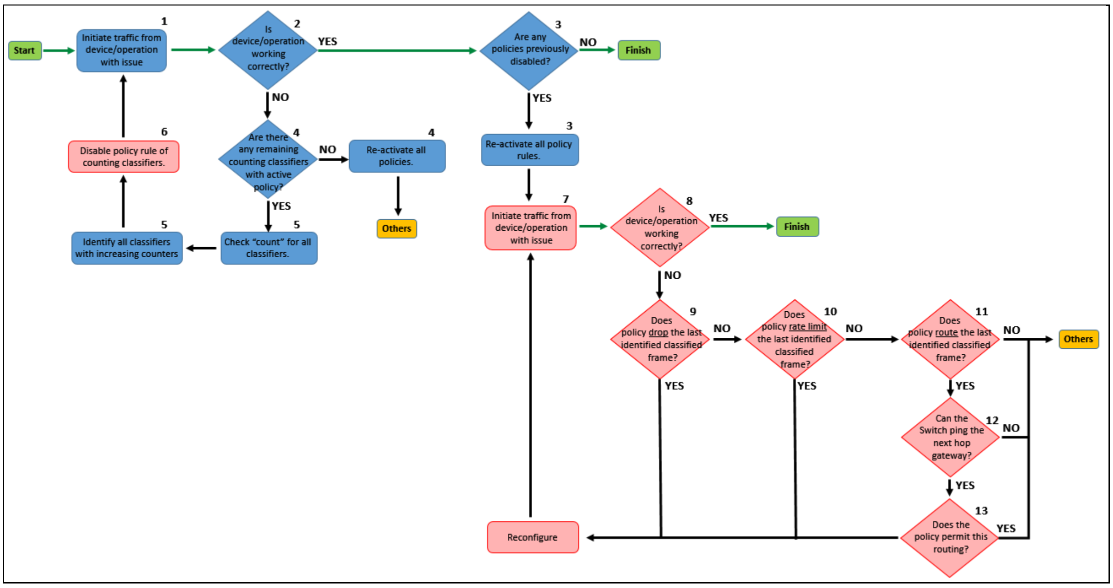
```
Switch# show dhcp server 10
  Server Status Detail for VID:   10
  Start IP Address:           192.168.10.1
  End IP Address:            192.168.10.10
  Subnet Mask:               255.255.255.0
  Default Gateway:          192.168.10.254
  Primary DNS Server:              8.8.8.8
  Secondary DNS Server:            0.0.0.0
  Lease Time:        3 day  0 hour  0 minute

  Address Leases
  index     IP Address        Timer    Hardware Address     Hostname
  ----------------------------------------------------------------------------
      1     192.168.10.1      256321   20:6a:8a:39:fe:a9    TWPCZT02031-02
```

If the number of DHCP entries do not exceed the pool size, **go to <OTHERS>**.

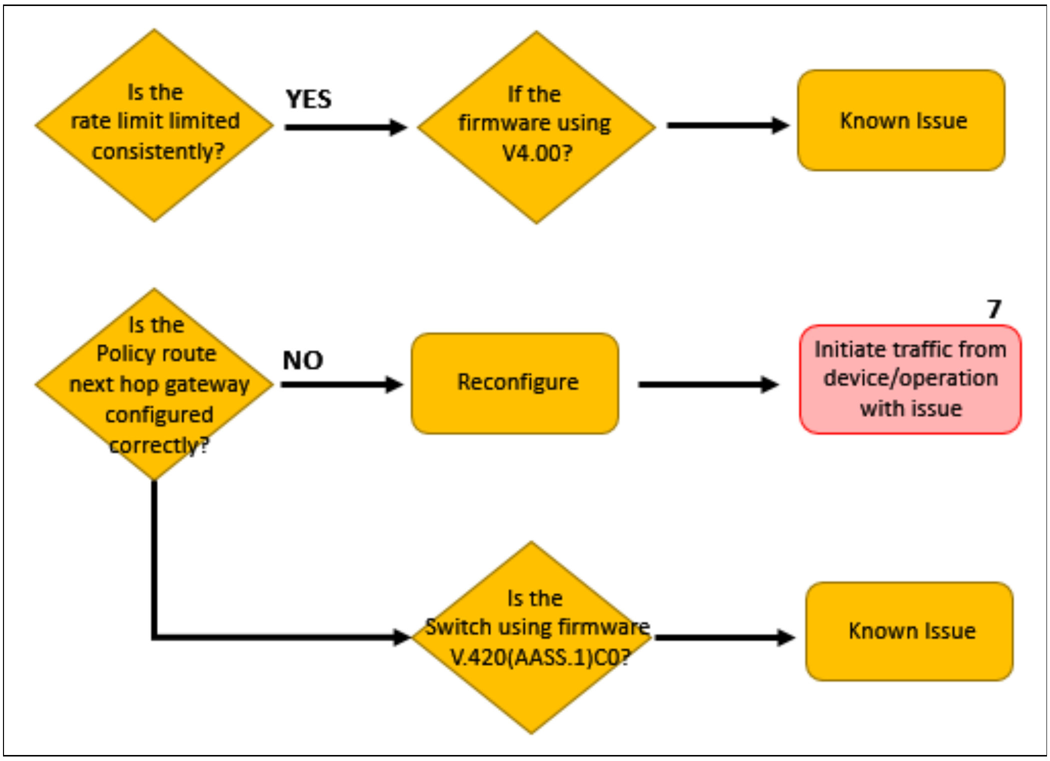
If the number of DHCP entries exceed the pool size, increase the pool size or create another VLAN for excess clients. **Repeat step 4 afterwards**.

15 Troubleshooting for ACL

Flowchart:

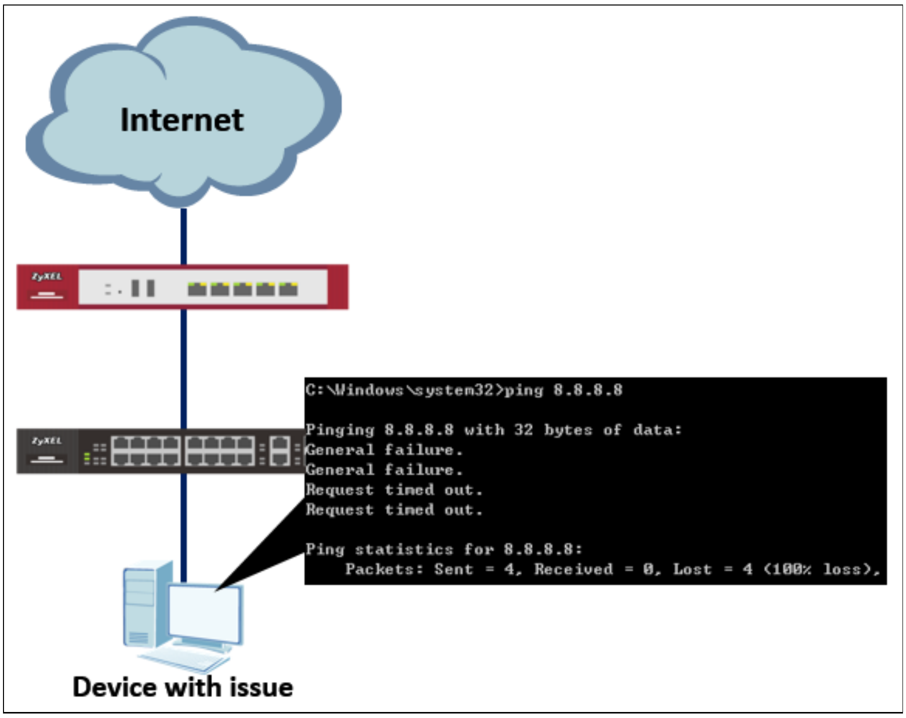

Start
1
Initiate traffic from device/operation with issue
2
Is device/operation working correctly?
YES
NO
3
Are any policies previously disabled?
NO
Finish
YES
3
Re-activate all policy rules.
4
Are there any remaining counting classifiers with active policy?
NO
4
Re-activate all policies.
Others
YES
5
Check "count" for all classifiers.
5
Identify all classifiers with increasing counters
6
Disable policy rule of counting classifiers.
7
Initiate traffic from device/operation with issue
8
Is device/operation working correctly?
YES
Finish
NO
9
Does policy drop the last identified classified frame?
NO
YES
10
Does policy rate limit the last identified classified frame?
NO
YES
11
Does policy route the last identified classified frame?
NO
Others
YES
12
Can the Switch ping the next hop gateway?
NO
YES
13
Does the policy permit this routing?
YES
Reconfigure

OTHERS:


Is the rate limit limited consistently?
YES
If the firmware using V4.00?
Known Issue
Is the Policy route next hop gateway configured correctly?
NO
Reconfigure
7
Initiate traffic from device/operation with issue
Is the Switch using firmware V.420(AASS.1)C0?
Known Issue

15.1 Initiate traffic from device or operation with issue

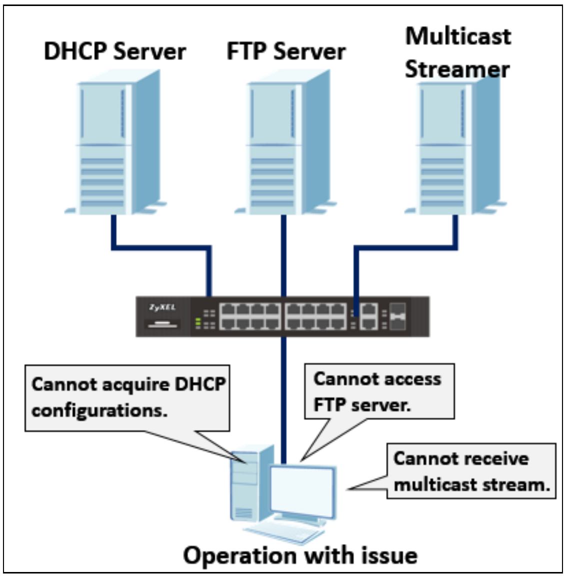
Figure 1



```
C:\Windows\system32>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
General failure.
General failure.
Request timed out.
Request timed out.

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Device with issue may refer to a specific device or a set of device that is not operating as intended

Figure 2


DHCP Server
FTP Server
Multicast Streamer
ZyXEL
Cannot acquire DHCP configurations.
Cannot access FTP server.
Cannot receive multicast stream.
Operation with issue

Operation with issue refers to the specific network service or operation.

15.2 Is the device or operation working accordingly?

If the device or operation is working accordingly, **go to step 3**.

If the device or operation does not work accordingly, **go to step 4**.

15.3 Are any policies previously disabled?

If any policies were disabled on step 5, **reactivate these policies and go to step 7**.

If there were no disabled policies from step 5, **proceed to the next agenda**.

15.4 Are there any remaining counting classifiers with policies still active?

Counting classifiers are the classifiers whose counters were rising in **step 5**.

If there are still active policies among the counted classifiers, **go to step 5**.

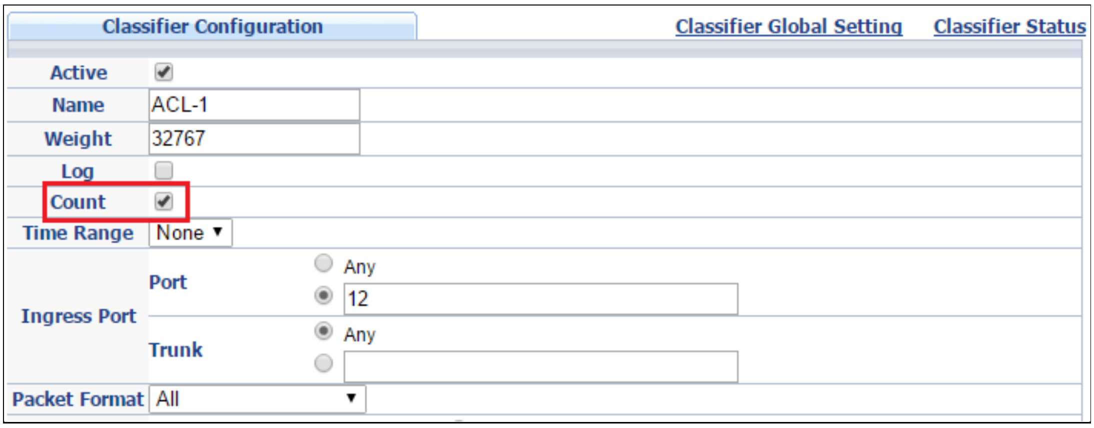
If there are no more active policies, **reactivate all policies and proceed to <OTHERS>**.

15.5 Identify the policies that are affecting traffic.

Select each configured classifiers and check "Log". This will allow the switch to count the real time number of packets affected by this classifier. This will help narrow down which classifier may have affected or interrupted service.

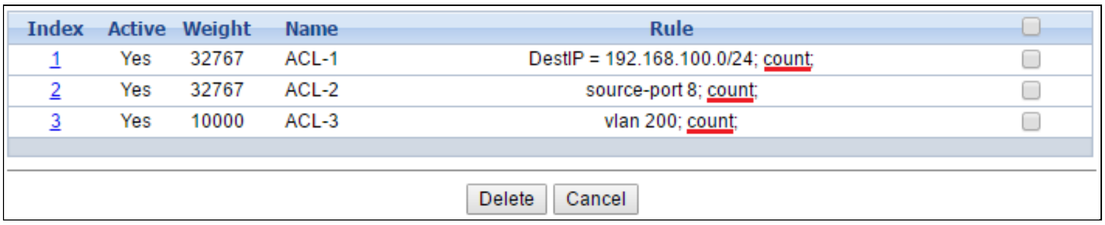
Using Web GUI:

Figure 3 Advance Application > Classifier > Classifier Configuration



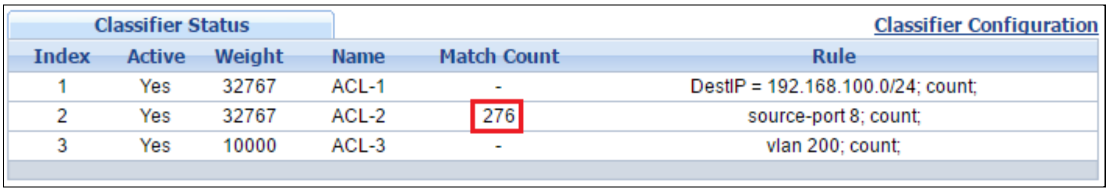
Active	☑		
Name	ACL-1		
Weight	32767		
Log	□		
Count	☑		
Time Range	None ▾		
Ingress Port	Port	○	Any
		●	12
	Trunk	●	Any
		○	
Packet Format	All ▾		

Figure 4



Index	Active	Weight	Name	Rule	□
1	Yes	32767	ACL-1	DestIP = 192.168.100.0/24; count;	□
2	Yes	32767	ACL-2	source-port 8; count;	□
3	Yes	10000	ACL-3	vlan 200; count;	□

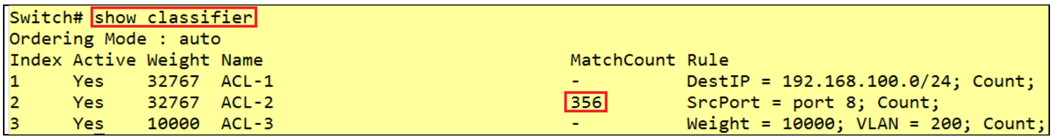
Figure 5 Advance Application > Classifier



Index	Active	Weight	Name	Match Count	Rule
1	Yes	32767	ACL-1	-	DestIP = 192.168.100.0/24; count;
2	Yes	32767	ACL-2	276	source-port 8; count;
3	Yes	10000	ACL-3	-	vlan 200; count;

Using CLI:

Figure 6



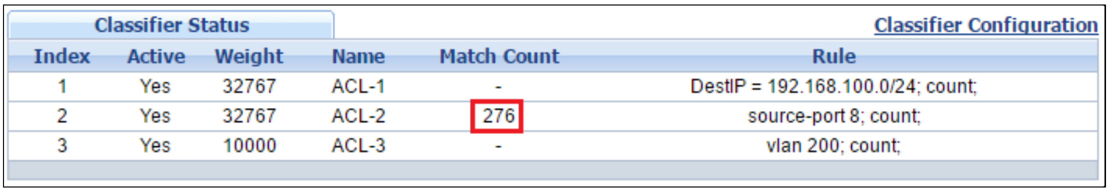
```
Switch# show classifier
Ordering Mode : auto
Index Active Weight Name                                 MatchCount Rule
1     Yes    32767  ACL-1                                -          DestIP = 192.168.100.0/24; Count;
2     Yes    32767  ACL-2                                356        SrcPort = port 8; Count;
3     Yes    10000  ACL-3                                -          Weight = 10000; VLAN = 200; Count;
```

After identifying the counting classifier, **proceed to step 6**.

15.6 Disable the policy rule or policy route of counting classifiers.

Example:

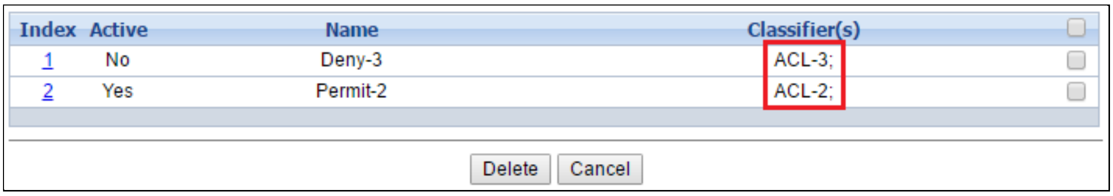
Figure 7 Advance Application > Classifier



Index	Active	Weight	Name	Match Count	Rule
1	Yes	32767	ACL-1	-	DestIP = 192.168.100.0/24; count;
2	Yes	32767	ACL-2	276	source-port 8; count;
3	Yes	10000	ACL-3	-	vlan 200; count;

*Classifier shows raising counter on "ACL-2".

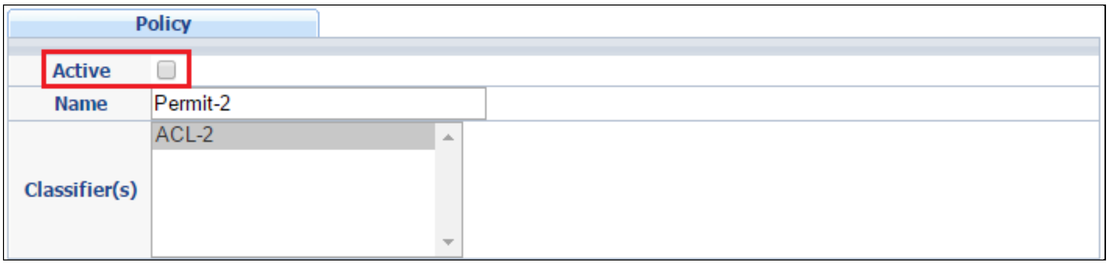
Figure 8 Advance Application > Policy Rule



Index	Active	Name	Classifier(s)	☐
1	No	Deny-3	ACL-3;	☐
2	Yes	Permit-2	ACL-2;	☐

*Classifier is bound to Policy "Permit-2".

Figure 9 Advance Application > Policy Rule



Active	☐
Name	Permit-2
Classifier(s)	ACL-2

*Uncheck the "Active" box of this policy.

After disabling a policy rule or policy route, **repeat step 1**.

15.7 Initiate traffic from device or operation with issue.

After initiating traffic, **go to step 8**.

15.8 Is the device or operation working accordingly?

If the device or operation is working accordingly, **proceed to the next agenda**.

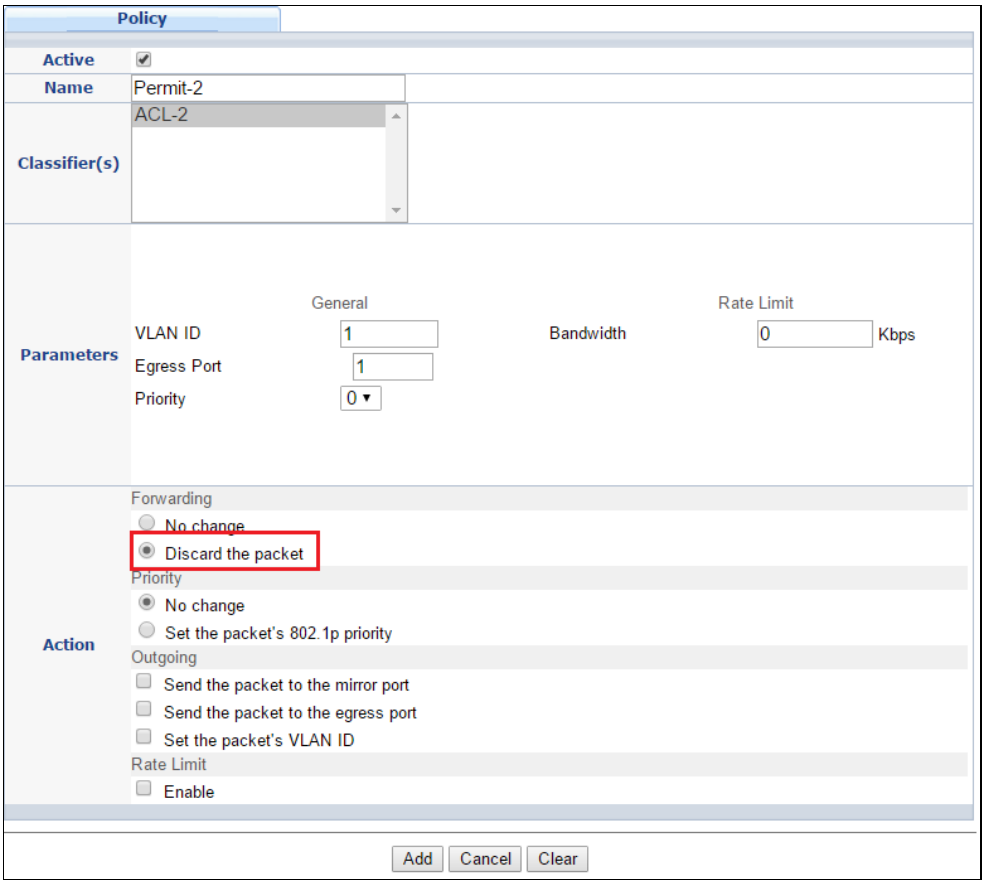
If the device or operation does not work accordingly, **go to step 9**.

15.9 Does the policy drop the last identified classified frame?

Verify the action of the last inactive policy rule or route. If action involves "Discard the packet", the classified frames are prevented from forwarding.

Using Web GUI:

Figure 10 Advance Application > Policy Rule



Policy

Active: ☑

Name: Permit-2

Classifier(s): ACL-2

Parameters

General

VLAN ID: 1

Egress Port: 1

Priority: 0

Rate Limit

Bandwidth: 0 Kbps

Action

Forwarding

○ No change

● Discard the packet

Priority

● No change

○ Set the packet's 802.1p priority

Outgoing

□ Send the packet to the mirror port

□ Send the packet to the egress port

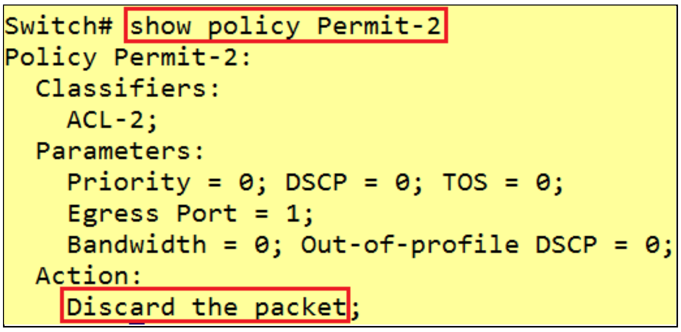
□ Set the packet's VLAN ID

Rate Limit

□ Enable

Using CLI:

Figure 11



```
Switch# show policy Permit-2
Policy Permit-2:
  Classifiers:
    ACL-2;
  Parameters:
    Priority = 0; DSCP = 0; TOS = 0;
    Egress Port = 1;
    Bandwidth = 0; Out-of-profile DSCP = 0;
  Action:
    Discard the packet;
```

If policy action is to "Discard the packet", **reconfigure forwarding to "No change" and go to step 7**.

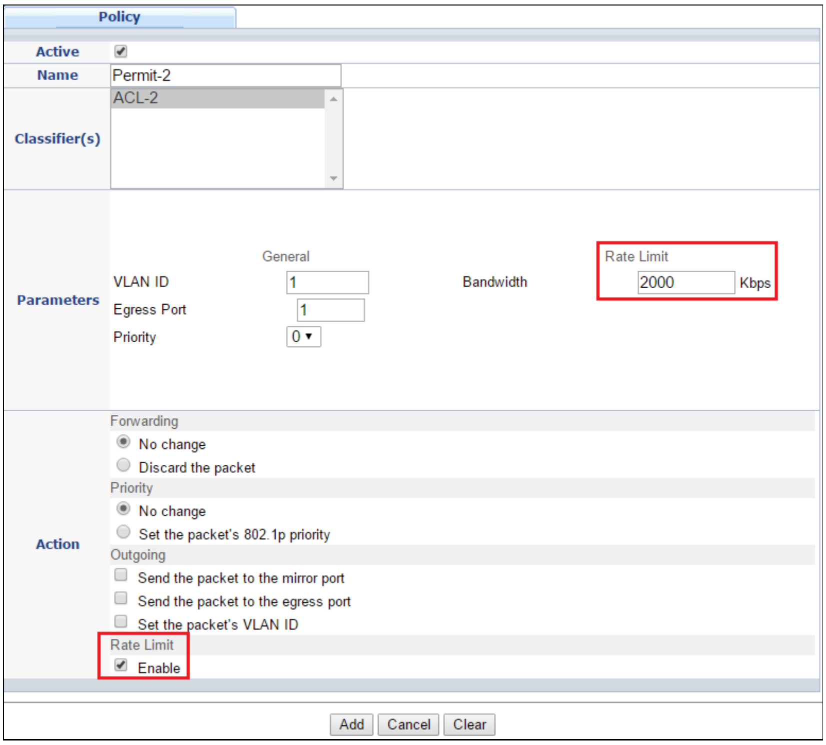
If policy action is not to "Discard the packet"," **go to step 10**.

15.10 Does the policy rate limit the last identified classified frame?

Verify the action of the last inactive policy rule or route. If action involves "Rate Limit", the classified frames are undergoing bandwidth limitation.

Using Web GUI:

Figure 12 Advance Application > Policy Rule

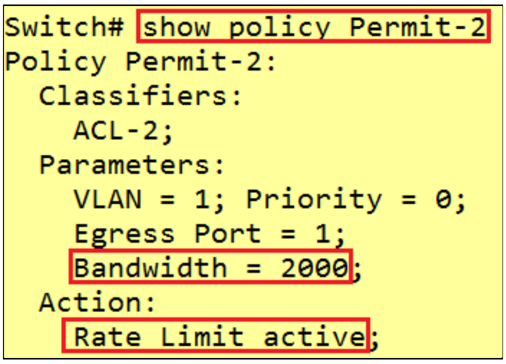


Policy

Active	☑
Name	Permit-2
Classifier(s)	ACL-2
Parameters	General VLAN ID 1 Egress Port 1 Priority 0 ▾ Bandwidth Rate Limit 2000 Kbps
Action	Forwarding ● No change ○ Discard the packet Priority ● No change ○ Set the packet's 802.1p priority Outgoing □ Send the packet to the mirror port □ Send the packet to the egress port □ Set the packet's VLAN ID Rate Limit ☑ Enable

Using CLI:

Figure 13



```
Switch# show policy Permit-2
Policy Permit-2:
  Classifiers:
    ACL-2;
  Parameters:
    VLAN = 1; Priority = 0;
    Egress Port = 1;
    Bandwidth = 2000;
  Action:
    Rate Limit active;
```

If policy action is to "Rate limit", increase the bandwidth value and **go to step 7**.

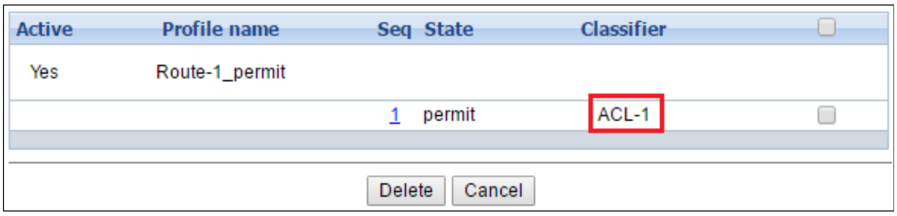
If policy action is not to "Rate Limit"," **go to step 11**.

15.11 Does the policy route the last identified classified frame?

Verify the action of the last inactive policy rule or route.

Using Web GUI:

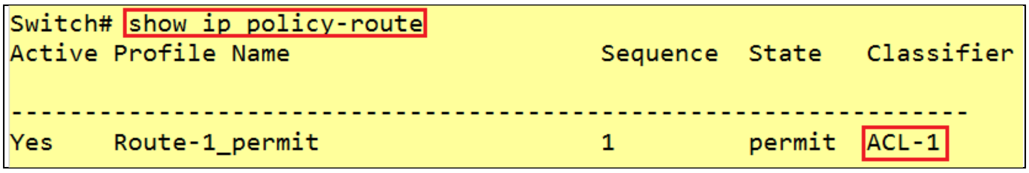
Figure 14 IP Application > Policy Route > Rule Configuration



Active	Profile name	Seq	State	Classifier	□
Yes	Route-1_permit				
		1	permit	ACL-1	□

Using CLI:

Figure 15



```
Switch# show ip policy-route
Active Profile Name                        Sequence  State   Classifier

-----------------------------------------------------------------
Yes    Route-1_permit                      1         permit  ACL-1
```

If policy action is to route traffic, **go to step 12**.

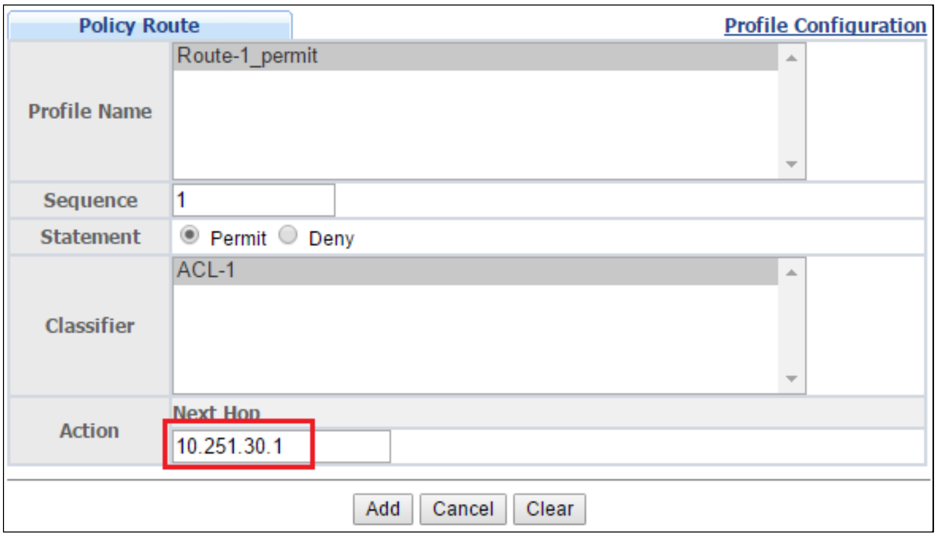
If policy action is not to route traffic, **go to <OTHERS>**.

15.12 Can the Zyxel switch ping the next hop gateway?

Policy route ensures that the classifier with Layer 3 criteria is routed to a specific next hop gateway. Policy Routes supersedes static routing. Verify the configured next hop gateway of the counting classifier and have the switch ping this gateway.

Using Web GUI:

Figure 16 IP Application > Policy Route > Rule Configuration

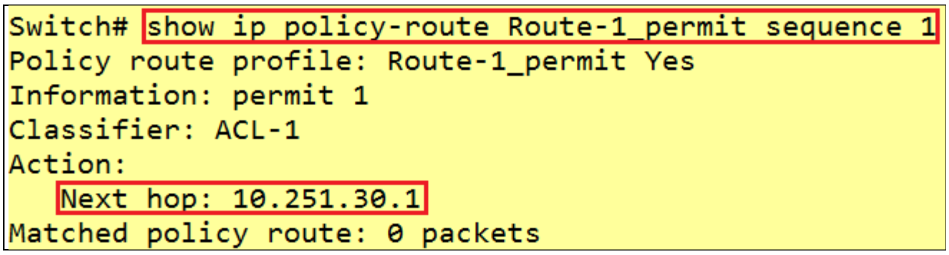


Profile Name	Route-1_permit
Sequence	1
Statement	● Permit ○ Deny
Classifier	ACL-1
Action	Next Hop 10.251.30.1

The policy route configuration can be viewed by clicking on the sequence number.

Using CLI:

Figure 17



```
Switch# show ip policy-route Route-1_permit sequence 1
Policy route profile: Route-1_permit Yes
Information: permit 1
Classifier: ACL-1
Action:
   Next hop: 10.251.30.1
Matched policy route: 0 packets
```

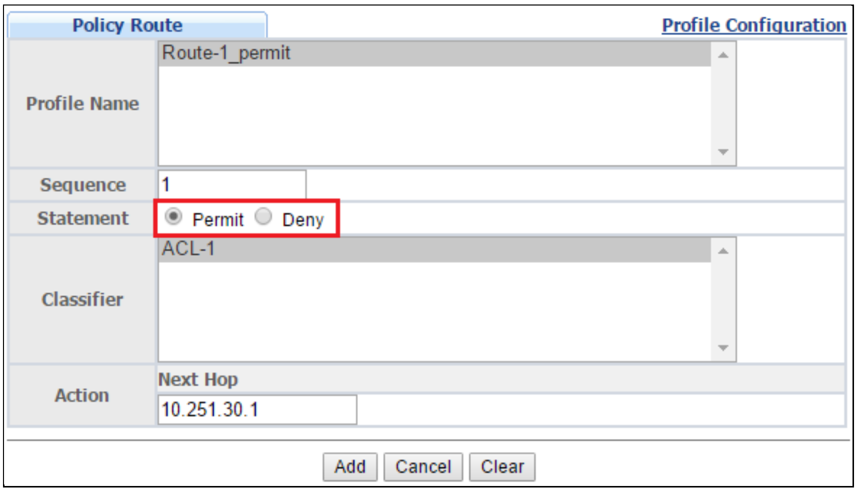
If the switch can ping the next hop gateway, **go to step 13**.

If the switch cannot ping the next hop gateway, **go to <OTHERS>**.

15.13 Does the policy permit this routing?

Using Web GUI:

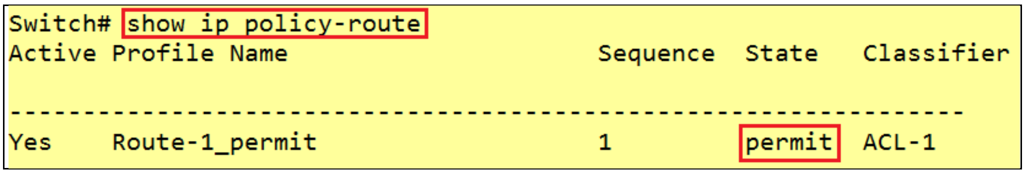
Figure 18 IP Application > Policy Route > Rule Configuration



Profile Name	Route-1_permit
Sequence	1
Statement	● Permit ○ Deny
Classifier	ACL-1
Action	Next Hop 10.251.30.1

Using CLI:

Figure 19



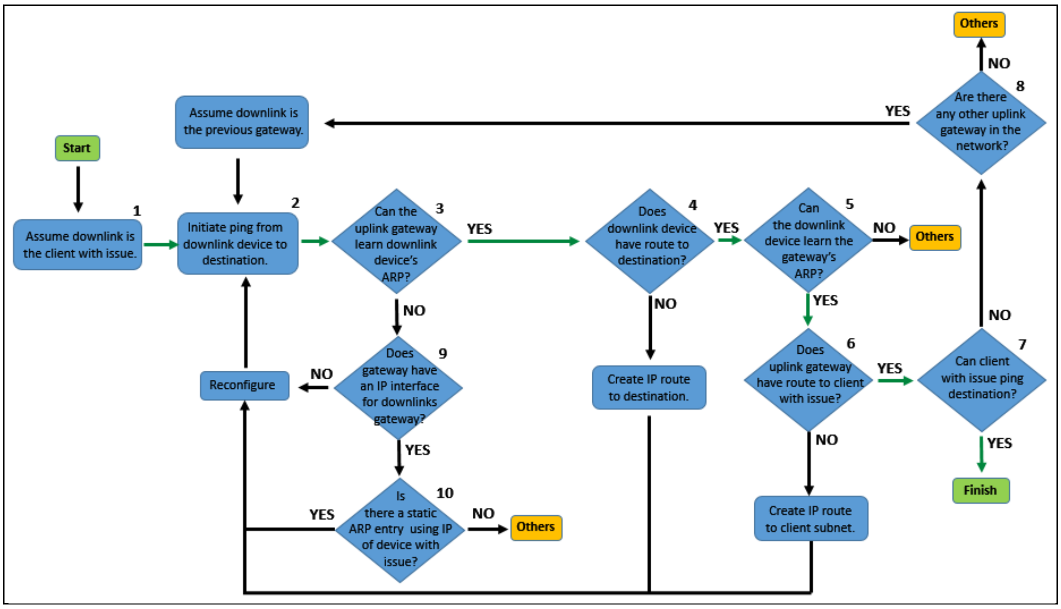
```
Switch# show ip policy-route
Active Profile Name                          Sequence  State   Classifier

-------------------------------------------------------------------
Yes    Route-1_permit                        1         permit  ACL-1
```

If the policy route state is permitted, **go to <OTHERS>**.

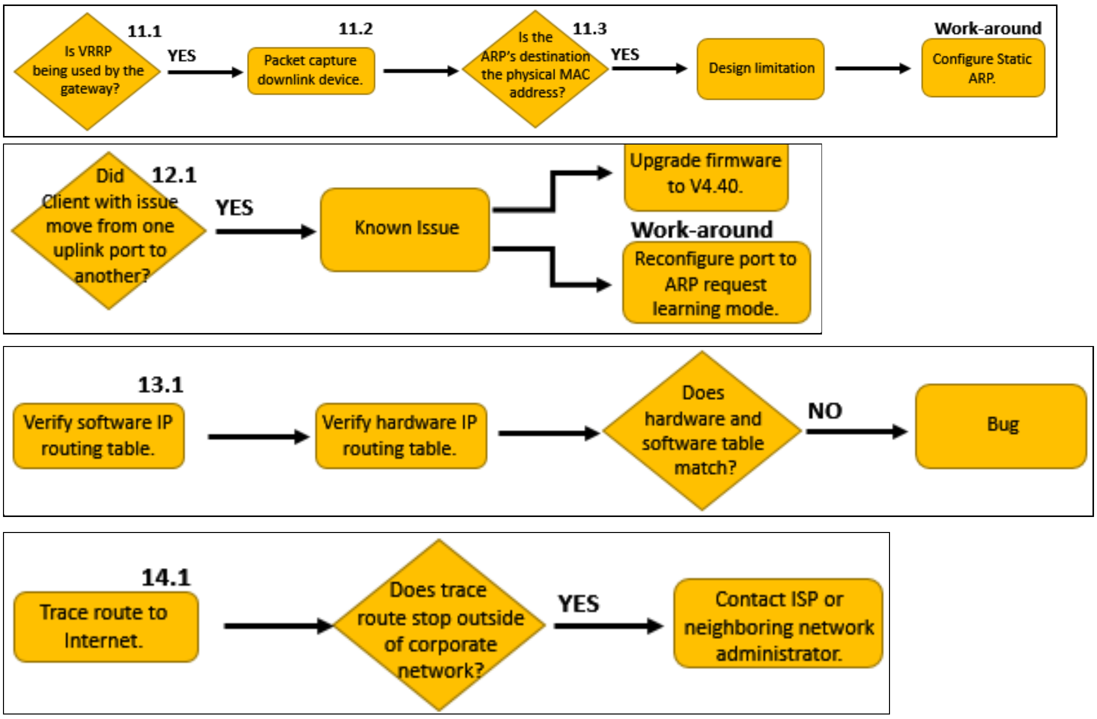
If the policy route state is denied, change state to “permit” and **repeat step 7**.

16 Troubleshooting for Routing

Flowchart:


Others
NO
8
Are there any other uplink gateway in the network?
YES
Assume downlink is the previous gateway.
Start
1
Assume downlink is the client with issue.
2
Initiate ping from downlink device to destination.
3
Can the uplink gateway learn downlink device's ARP?
YES
4
Does downlink device have route to destination?
YES
5
Can the downlink device learn the gateway's ARP?
NO
Others
NO
YES
NO
9
Does gateway have an IP interface for downlinks gateway?
NO
Reconfigure
NO
Create IP route to destination.
6
Does uplink gateway have route to client with issue?
YES
7
Can client with issue ping destination?
NO
YES
Finish
YES
10
Is there a static ARP entry using IP of device with issue?
YES
NO
Others
Create IP route to client subnet.

OTHERS:


11.1
Is VRRP being used by the gateway?
YES
11.2
Packet capture downlink device.
11.3
Is the ARP's destination the physical MAC address?
YES
Design limitation
Work-around
Configure Static ARP.
12.1
Did Client with issue move from one uplink port to another?
YES
Known Issue
Upgrade firmware to V4.40.
Work-around
Reconfigure port to ARP request learning mode.
13.1
Verify software IP routing table.
Verify hardware IP routing table.
Does hardware and software table match?
NO
Bug
14.1
Trace route to Internet.
Does trace route stop outside of corporate network?
YES
Contact ISP or neighboring network administrator.

16.1 Access the client with issue.

For now, the client with issue will be considered as the **downlink device**.

Afterwards, **move on to step 2**.

16.2 Initiate a ping test from downlink device to destination with issue.

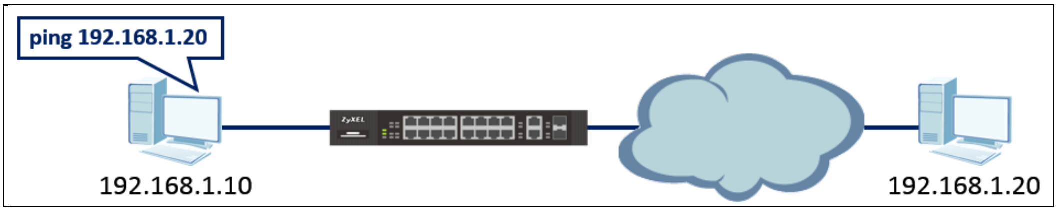
The *destination with issue* could be one of the following:

Device in the same LAN: ping the device's IP address.

Device in a different LAN: ping the device's IP address.

Internet: ping Goggle's public DNS server "8.8.8.8".

Figure 1



After performing the ping test, **go to step 3**.

16.3 Can the uplink gateway learn the downlink device's ARP?

The uplink gateway refers to the next hop gateway of the downlink device with respect to your destination. You can check the ARP table to verify that the downlink device's traffic can reach the uplink gateway. Also verify that the **Port, VLAN, IP address, and MAC address** matches the downlink device's information.

Port refers to where the downlink device's ARP packets should come from.

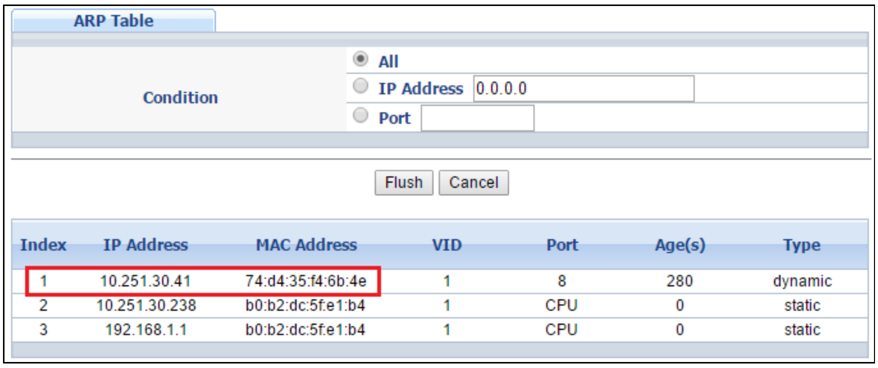
VLAN refers to which VLAN the downlink device's ARP packets are processed by the switch. This is the PVID if the ARP packets received by the switch are untagged.

IP Address refers to the IP address of the downlink device.

MAC Address refers to the hardware or Ethernet address of the downlink device.

Using Web GUI:

Figure 2 Management > ARP Table



ARP Table

Condition

● All

○ IP Address 0.0.0.0

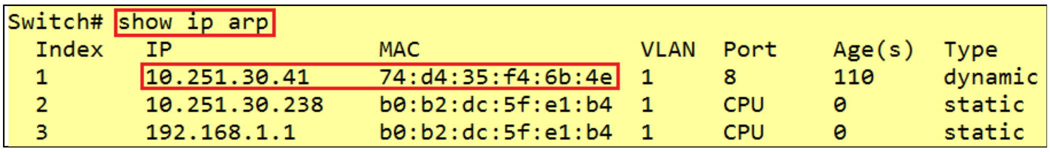
○ Port

Flush Cancel

Index	IP Address	MAC Address	VID	Port	Age(s)	Type
1	10.251.30.41	74:d4:35:f4:6b:4e	1	8	280	dynamic
2	10.251.30.238	b0:b2:dc:5f:e1:b4	1	CPU	0	static
3	192.168.1.1	b0:b2:dc:5f:e1:b4	1	CPU	0	static

Using CLI:

Figure 3



```
Switch# show ip arp
  Index    IP              MAC                VLAN  Port    Age(s)  Type
  1        10.251.30.41    74:d4:35:f4:6b:4e  1     8       110     dynamic
  2        10.251.30.238   b0:b2:dc:5f:e1:b4  1     CPU     0       static
  3        192.168.1.1     b0:b2:dc:5f:e1:b4  1     CPU     0       static
```

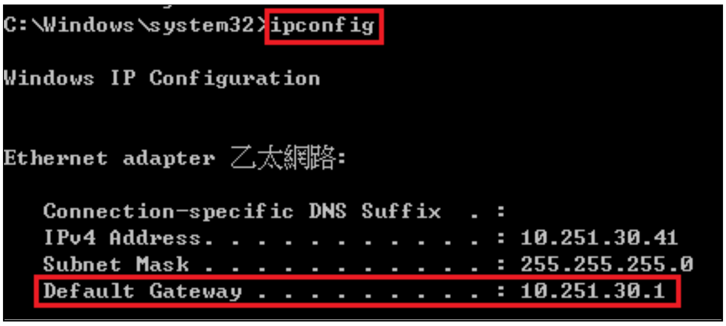
If the uplink gateway can correctly learn the downlink device’s ARP entry, **go to step 4**.

If the uplink gateway cannot correctly learn the downlink device’s ARP entry, **go to step 9**.

16.4 Does downlink device have route to destination?

If downlink device is a PC, all packets destined for a different network is sent to the default gateway.

Figure 4

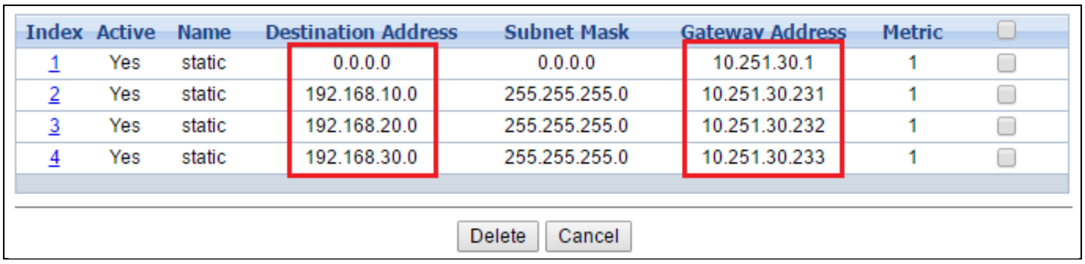


```
C:\Windows\system32>ipconfig

Windows IP Configuration


Ethernet adapter 乙太網路:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 10.251.30.41
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.251.30.1
```

If downlink device is another Zyxel switch, verify whether a route exists for your destination address with the correct gateway. In this example, any packet destined for network "192.168.10.0"

Using Web GUI:

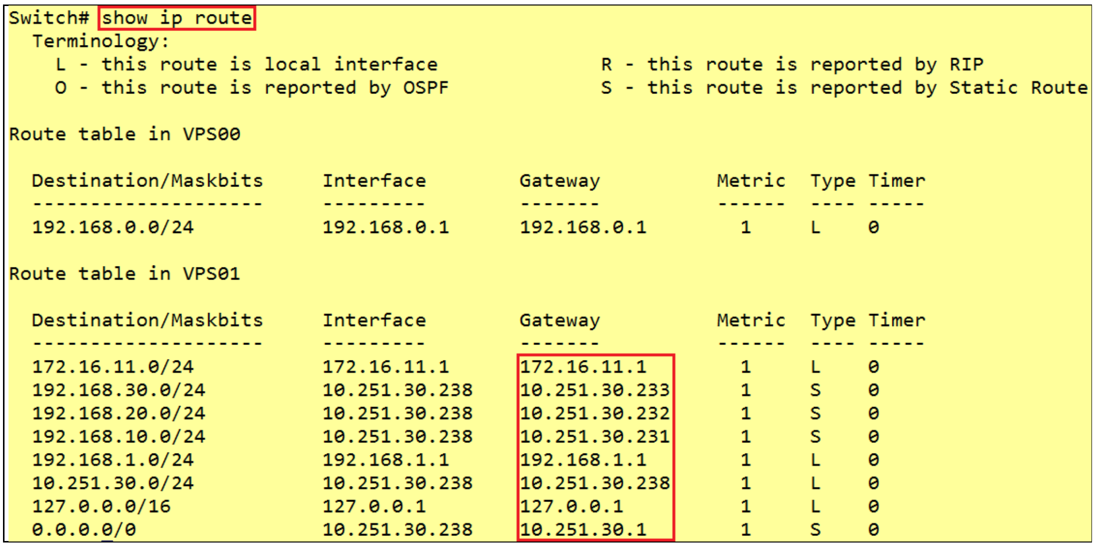
Figure 5 IP Application > Static Routing > IPv4 Static Route



Index	Active	Name	Destination Address	Subnet Mask	Gateway Address	Metric	☐
1	Yes	static	0.0.0.0	0.0.0.0	10.251.30.1	1	☐
2	Yes	static	192.168.10.0	255.255.255.0	10.251.30.231	1	☐
3	Yes	static	192.168.20.0	255.255.255.0	10.251.30.232	1	☐
4	Yes	static	192.168.30.0	255.255.255.0	10.251.30.233	1	☐

Using CLI:

Figure 6



```
Switch# show ip route
  Terminology:
    L - this route is local interface             R - this route is reported by RIP
    O - this route is reported by OSPF            S - this route is reported by Static Route

Route table in VPS00

  Destination/Maskbits      Interface        Gateway          Metric  Type Timer
  --------------------      ---------        -------          ------  ---- -----
  192.168.0.0/24            192.168.0.1      192.168.0.1        1      L    0

Route table in VPS01

  Destination/Maskbits      Interface        Gateway          Metric  Type Timer
  --------------------      ---------        -------          ------  ---- -----
  172.16.11.0/24            172.16.11.1      172.16.11.1        1      L    0
  192.168.30.0/24           10.251.30.238    10.251.30.233      1      S    0
  192.168.20.0/24           10.251.30.238    10.251.30.232      1      S    0
  192.168.10.0/24           10.251.30.238    10.251.30.231      1      S    0
  192.168.1.0/24            192.168.1.1      192.168.1.1        1      L    0
  10.251.30.0/24            10.251.30.238    10.251.30.238      1      L    0
  127.0.0.0/16              127.0.0.1        127.0.0.1          1      L    0
  0.0.0.0/0                 10.251.30.238    10.251.30.1        1      S    0
```

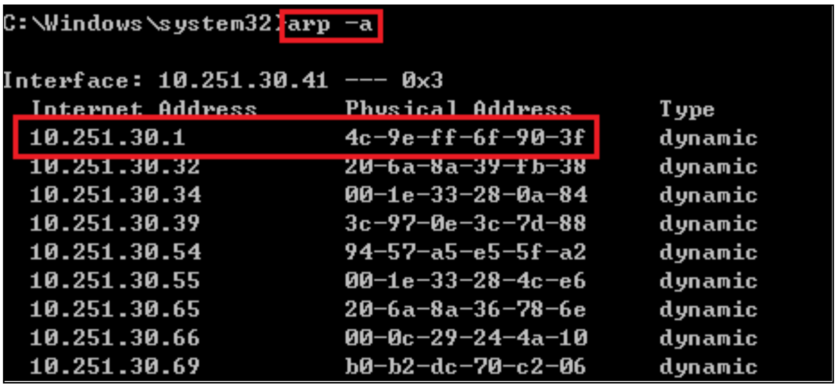
If there is a routing entry for destination address, **then go to step 5.**

If there is no routing entry for destination address, **then add static route and repeat step 2**.

16.5 Can the downlink device learn the uplink gateway's ARP?

You can check the ARP table to verify that the uplink gateway's traffic can reach the downlink device. Also verify that the IP address and MAC address matches the downlink device's information in case of spoofing attacks.
If downlink device is an end device:

Figure 7



```
C:\Windows\system32>arp -a

Interface: 10.251.30.41 --- 0x3
  Internet Address      Physical Address      Type
  10.251.30.1           4c-9e-ff-6f-90-3f     dynamic
  10.251.30.32          20-6a-8a-39-fb-38     dynamic
  10.251.30.34          00-1e-33-28-0a-84     dynamic
  10.251.30.39          3c-97-0e-3c-7d-88     dynamic
  10.251.30.54          94-57-a5-e5-5f-a2     dynamic
  10.251.30.55          00-1e-33-28-4c-e6     dynamic
  10.251.30.65          20-6a-8a-36-78-6e     dynamic
  10.251.30.66          00-0c-29-24-4a-10     dynamic
  10.251.30.69          b0-b2-dc-70-c2-06     dynamic
```

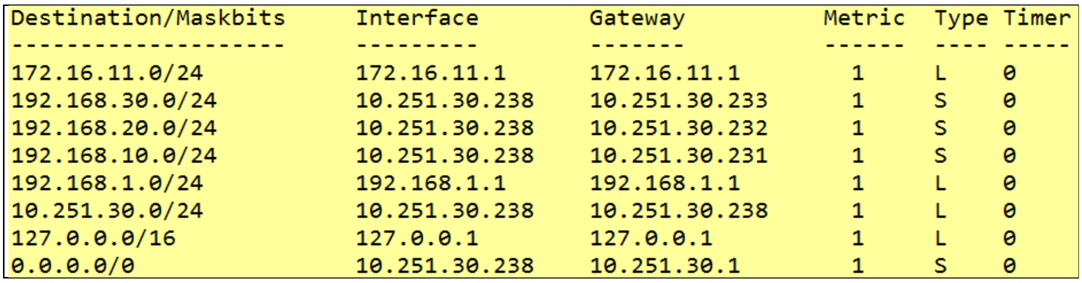
If the downlink device can correctly learn the uplink gateway's ARP entry, **go to step 6**.

If the downlink device cannot correctly learn the uplink gateway's ARP entry, **go to <OTHERS>**.

16.6 Does the uplink gateway have route to network of client with issue?

Similar to Step 4, this time, verify whether the uplink gateway knows how to route traffic back to client. This means that if the client with issue is in network "192.168.10.0", the uplink gateway must have a destination address for network "192.168.10.0". Note that the Web GUI of static routes do not display local interface. So if a Zyxel switch locally has an IP interface in network "192.168.10.0", this will not be displayed. For a more accurate routing table, use CLI instead.

Figure 8



```
Destination/Maskbits      Interface         Gateway           Metric  Type Timer
--------------------      ---------         -------           ------  ---- -----
172.16.11.0/24            172.16.11.1       172.16.11.1         1      L     0
192.168.30.0/24           10.251.30.238     10.251.30.233       1      S     0
192.168.20.0/24           10.251.30.238     10.251.30.232       1      S     0
192.168.10.0/24           10.251.30.238     10.251.30.231       1      S     0
192.168.1.0/24            192.168.1.1       192.168.1.1         1      L     0
10.251.30.0/24            10.251.30.238     10.251.30.238       1      L     0
127.0.0.0/16              127.0.0.1         127.0.0.1           1      L     0
0.0.0.0/0                 10.251.30.238     10.251.30.1         1      S     0
```

Type "L" refers to local interfaces. This indicates that the switch locally has an IP interface for this destination address. While type "S" refers to static routes. This indicates that the destination network is not directly connected to this switch and network is mostly likely across another gateway.

If the uplink gateway has route to network of client with issue, **go to step 7**.

If the uplink gateway does not have route to network of client with issue, **add static route to network of client with issue and repeat step 2**.

16.7 Can the client with issue communicate with destination with issue?

If ping from client with issue to destination with issue is successful, **proceed to the next agenda**.

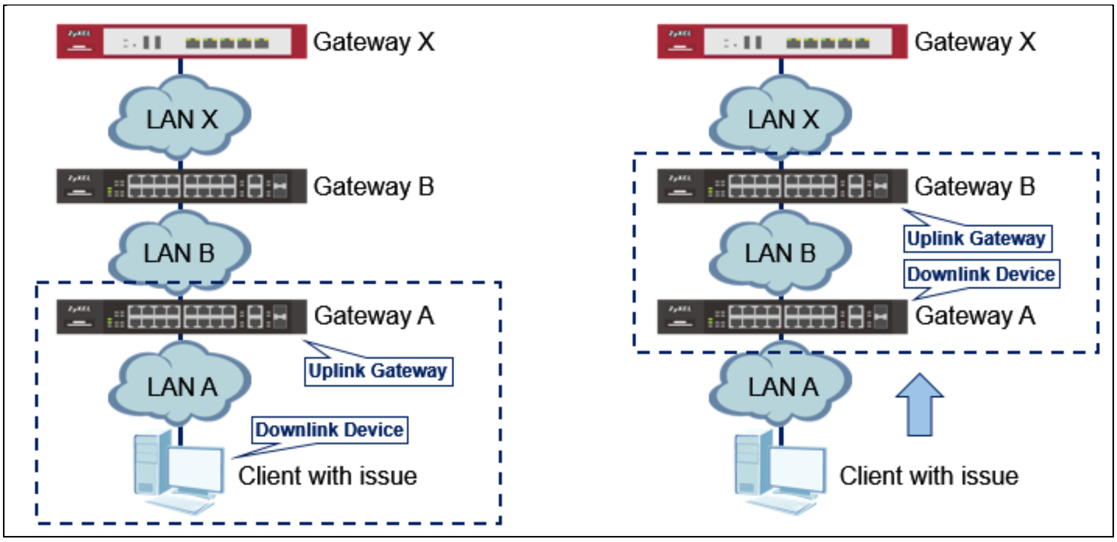
If ping from client with issue to destination with issue is not successful, **go to step 8**.

16.8 Are there any other uplink gateways in your corporate network?

We now need to troubleshoot the next neighboring network and uplink gateway. From the illustration below, we started at **LAN A**, now we will move on to **LAN B** with a different set of downlink device and uplink gateway. The downlink device for **LAN B** will be the previous uplink gateway in **LAN A**. Once done with LAN B, move on to LAN C and so on.

This process ends when the uplink gateway is managed by a different organization, such as, Internet Service Providers.

Figure 9



*Before *After

If there are other uplink gateways in the corporate network, move on to the next set of downlink and uplink devices and **repeat step 2**.

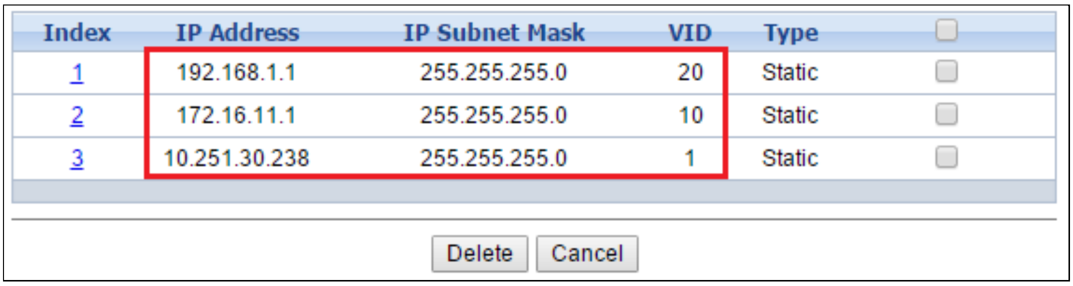
If there are no other uplink gateways in the corporate network, **proceed to <OTHERS>**.

16.9 Does gateway have an IP interface for downlink devices?

The gateway's IP address and VLAN must match the default or next hop gateway address of downlink devices.

Using Web GUI:

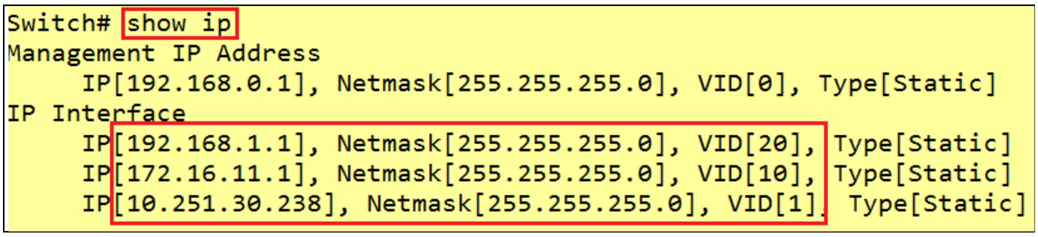
Figure 10 IP Application > Static Routing > IPv4 Static Route



Index	IP Address	IP Subnet Mask	VID	Type	□
1	192.168.1.1	255.255.255.0	20	Static	□
2	172.16.11.1	255.255.255.0	10	Static	□
3	10.251.30.238	255.255.255.0	1	Static	□

Using CLI:

Figure 11



```
Switch# show ip
Management IP Address
     IP[192.168.0.1], Netmask[255.255.255.0], VID[0], Type[Static]
IP Interface
     IP[192.168.1.1], Netmask[255.255.255.0], VID[20], Type[Static]
     IP[172.16.11.1], Netmask[255.255.255.0], VID[10], Type[Static]
     IP[10.251.30.238], Netmask[255.255.255.0], VID[1], Type[Static]
```

If the uplink gateway has the correct IP address in the correct VLAN, **go to step 10**.

If the uplink gateway does not have the correct IP address in the correct VLAN, reconfigure and **repeat step 2**.

16.10 Is there a static ARP entry using the IP of the downlink device or uplink gateway?

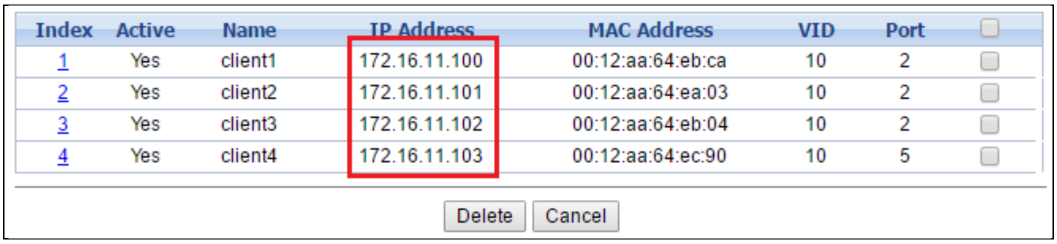
Static ARP prevents the learning of ARP entries for another MAC address or port. If the switch cannot update its ARP table for this IP address, then packets are sent to a wrong destination causing failed communication.

If the switch does not have any static ARP for the downlink or uplink devices, **go to step 11**.

If the switch has an incorrect static ARP entry for the downlink or uplink devices, reconfigure and **repeat step 2**.

Using Web GUI:

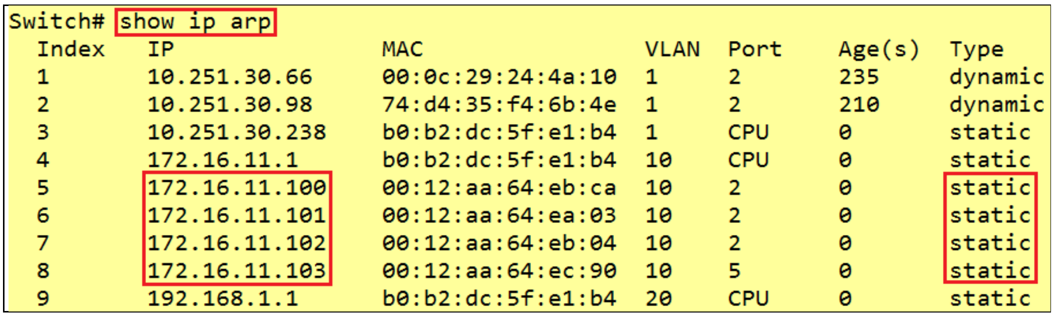
Figure 12 IP Application > ARP Setup > Static ARP



Index	Active	Name	IP Address	MAC Address	VID	Port	☐
1	Yes	client1	172.16.11.100	00:12:aa:64:eb:ca	10	2	☐
2	Yes	client2	172.16.11.101	00:12:aa:64:ea:03	10	2	☐
3	Yes	client3	172.16.11.102	00:12:aa:64:eb:04	10	2	☐
4	Yes	client4	172.16.11.103	00:12:aa:64:ec:90	10	5	☐

Using CLI:

Figure 13



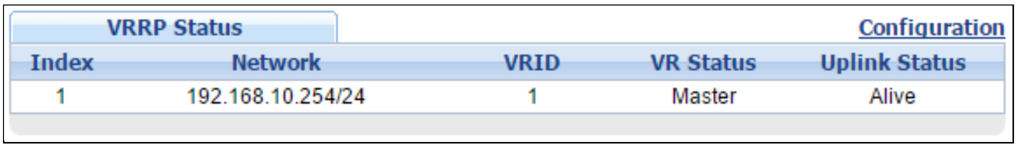
```
Switch# show ip arp
  Index    IP              MAC                VLAN  Port    Age(s)  Type
  1        10.251.30.66    00:0c:29:24:4a:10  1     2       235     dynamic
  2        10.251.30.98    74:d4:35:f4:6b:4e  1     2       210     dynamic
  3        10.251.30.238   b0:b2:dc:5f:e1:b4  1     CPU     0       static
  4        172.16.11.1     b0:b2:dc:5f:e1:b4  10    CPU     0       static
  5        172.16.11.100   00:12:aa:64:eb:ca  10    2       0       static
  6        172.16.11.101   00:12:aa:64:ea:03  10    2       0       static
  7        172.16.11.102   00:12:aa:64:eb:04  10    2       0       static
  8        172.16.11.103   00:12:aa:64:ec:90  10    5       0       static
  9        192.168.1.1     b0:b2:dc:5f:e1:b4  20    CPU     0       static
```

16.11 Is the downlink device's gateway the switch's VRRP IP address?

VRRP allows a switch to generate a virtual IP address for L3 gateway redundancy using a virtual MAC address. Verify whether a VRRP virtual interface is active on the **client with issue's** network.

Using Web GUI:

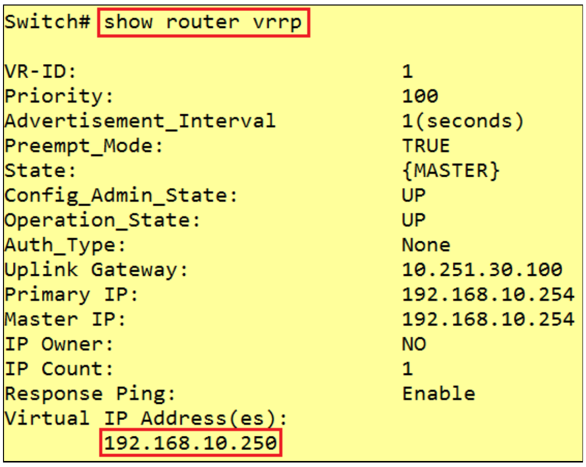
Figure 14 IP Application > VRRP



Index	Network	VRID	VR Status	Uplink Status
1	192.168.10.254/24	1	Master	Alive

Using CLI:

Figure 15



```
Switch# show router vrrp

VR-ID:                           1
Priority:                        100
Advertisement_Interval           1(seconds)
Preempt_Mode:                    TRUE
State:                           {MASTER}
Config_Admin_State:              UP
Operation_State:                 UP
Auth_Type:                       None
Uplink Gateway:                  10.251.30.100
Primary IP:                      192.168.10.254
Master IP:                       192.168.10.254
IP Owner:                        NO
IP Count:                        1
Response Ping:                   Enable
Virtual IP Address(es):
        192.168.10.250
```

If the switch has a virtual IP address for the client with issue's network, **proceed to step 12**.

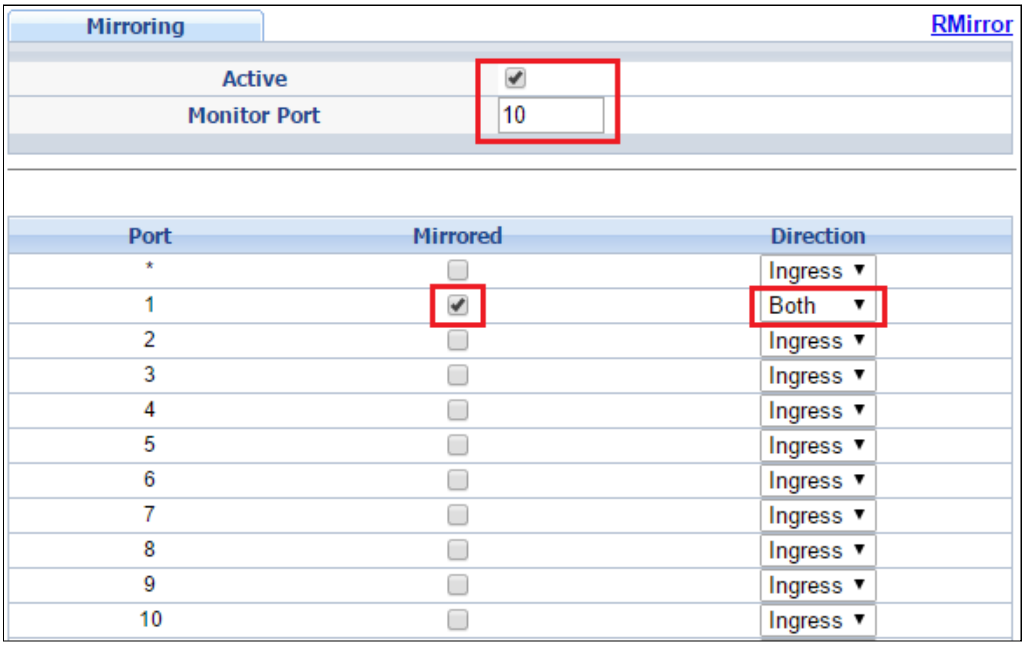
If the switch does not have a virtual IP address for the client with issue's network, **go to step 14**.

16.12 Mirror and capture the traffic of client with issue.

Access the switch **directly** connected to client with issue and mirror ingress and egress traffic on that port. Afterwards, have the client with issue ping the virtual IP address.

Using Web GUI:

Figure 16 Advance Application > Mirroring



Mirroring

RMirror

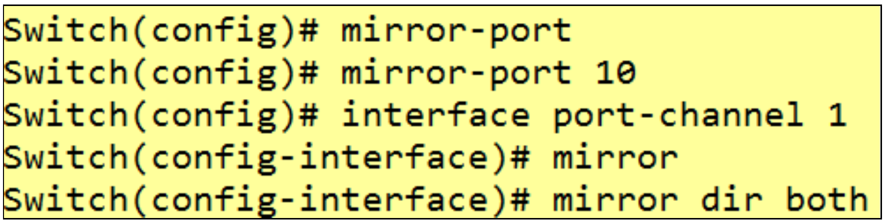
Active	☑
Monitor Port	10

Port	Mirrored	Direction
*	☐	Ingress
1	☑	Both
2	☐	Ingress
3	☐	Ingress
4	☐	Ingress
5	☐	Ingress
6	☐	Ingress
7	☐	Ingress
8	☐	Ingress
9	☐	Ingress
10	☐	Ingress

In this example, PC running Wireshark is connected to port 10 of this switch while client with issue is directly connected to port 1.

Using CLI:

Figure 17



```
Switch(config)# mirror-port
Switch(config)# mirror-port 10
Switch(config)# interface port-channel 1
Switch(config-interface)# mirror
Switch(config-interface)# mirror dir both
```

After capturing the client with issue's traffic, **proceed to step 13**.

16.13 Does the client with issue's ARP reply sent to the switch's physical MAC address?

Examine the packet capture of the client with issue's traffic. Locate the client with issue's ARP replies from the switch's ARP request. Verify whether the client with issue's ARP replies are sent to the switch physical MAC address instead of the VRRP's virtual MAC address.

If the client with issue sends ARP replies destined for the switch's physical address, **go to step 14**.

If the client with issue sends ARP replies destined for the switch's virtual address, this is a design limitation.

16.14 Did symptom only occur after client with issue move from one uplink port to another?

Uplink port refers to port of the Uplink Gateway which leads to the client with issue.

Figure 18 Above shows client did not change uplink port

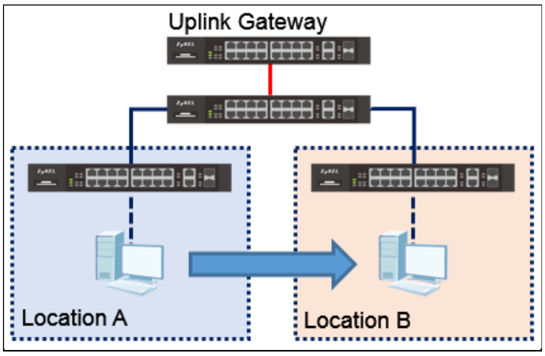
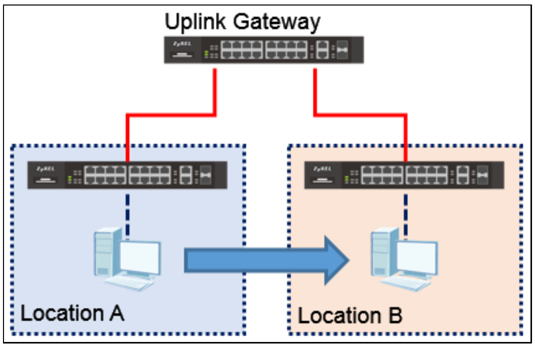


Figure 19 *Above shows client changed uplink port.*

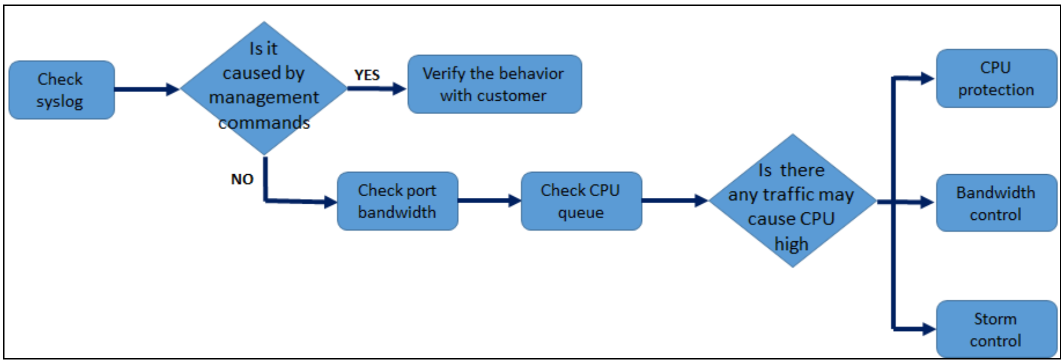


If the client moved from one uplink port to another, this is a known issue.

If the client did not move from one uplink port to another, **go to Others**.

17 Troubleshooting for CPU high

Flowchart:


Check syslog
Is it caused by management commands
YES
Verify the behavior with customer
NO
Check port bandwidth
Check CPU queue
Is there any traffic may cause CPU high
CPU protection
Bandwidth control
Storm control

17.1 Check syslog

a. Verify frequency.

b. Is there any special log before CPU high?

c. Abnormal attack

17.2 Is it caused by management commands?

Some commands will cause the CPU high

a. Save configuration (Write memory)

b. Collect tech-support log

c. Sflow

17.3 Check port bandwidth

switch# show interfaces <port id>

17.4 Check CPU queue

switch> bcm pw

17.5 Is there any traffic may cause CPU high?

a. A lot of IGMP request

b. ARP broadcast storms

c. Ethernet broadcast storms

d. SNMP polling

18 Troubleshooting for PoE

Before trouble shooting, you should know:

A. PD : Model info, Supported PoE standard and class, the number

B. PSE : Supported PoE standard, and the remaining power budget

Class	Current Range (mA)	Power Range (W)	**PSE Allocated Power by Class**
0	0-4	0.44-12.94	**15.4**
1	9-12	0.44-3.84	**4**
2	17-20	3.84-6.49	**7**
3	26-30	6.49-12.95	**15.4**
4	36-44	12.95-25.50	**30**

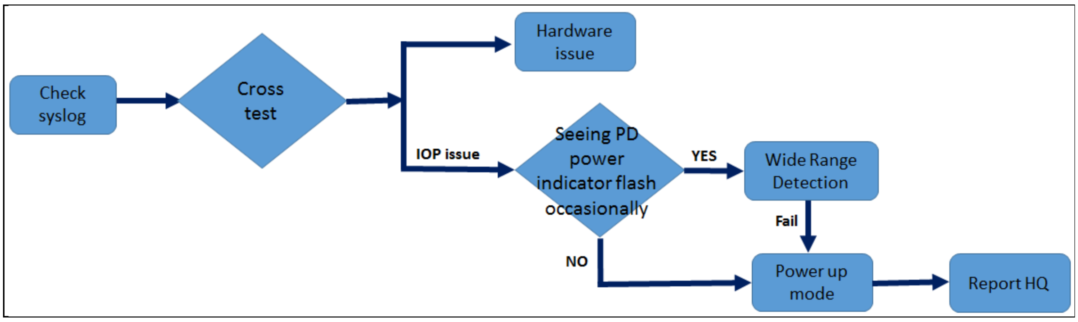
C. Cable: type and length

i. Make sure that the Ethernet cable length does not exceed 100 meters.

ii. If PD does not power-on, try swapping the Ethernet cable with a cable that has no issues powering-on different PDs.

D. Use the latest firmware for the Zyxel switch.

Flowchart:



18.1 Check syslog

a. PoE Overload Event: The PD requested more power than the configured max power on the specific port while in consumption mode.

b. PoE Power Management Event: The overall consumed power exceeded the total power budget.

➔ If the customer original uses classification mode, please try to use consumption mode. But it is possible some PD will be shut down when the

c. PoE Short-Circuit Event: The connected PD may be faulty. It could also mean that the PD is using an older standard and not 802.3af/at. You can try changing the "Power-Up" option to "Legacy" or "Pre-802.3at" in the PoE Setup page.

18.2 Cross test

Creating a table to list down which ports were able to power-on PD during the cross test:

Device	PD Model X (1)	PD Model X (2)	PD Model Y
Switch Model X (1)			
Switch Model X (2)			
Switch Model Y			

*During the cross test, Switch will only be connected to one PD at a time, and use the Consumption mode. Please test multi-port of the test switch to double confirm the test result.

Switch Model X (1): The reported switch with issue.

Switch Model X (2): A different switch but the same model as the reported switch. (Make sure it works well if possible.)

Switch Model Y: A different switch but of a different model (the newer series if possible).

PD Model X (1): The reported PD that has issue.

PD Model X (2): A different PD but same model as the reported PD.

PD Model Y: A different PD but of a different model (Zyxel PD model if possible).

<u>The test results' meaning:</u>

a. The reported PD has the hardware issue.

Device	PD Model X (1)	PD Model X (2)	PD Model Y
Switch Model X (1)	Fail	Success	Success
Switch Model X (2)	Fail	Success	Success
Switch Model Y	Fail	Success	Success

No ports among all switch could power-on PD Model X (1), while PD Model X (2) shows a different result.

b. The reported switch has the hardware issue

Device	PD Model X (1)	PD Model X (2)	PD Model Y
Switch Model X (1)	Fail	Fail	Fail
Switch Model X (2)	Success	Success	Success
Switch Model Y	Success	Success	Success

Please test every ports in Switch Model X (1) to further verify the hardware issue.

c. The interoperability issue.

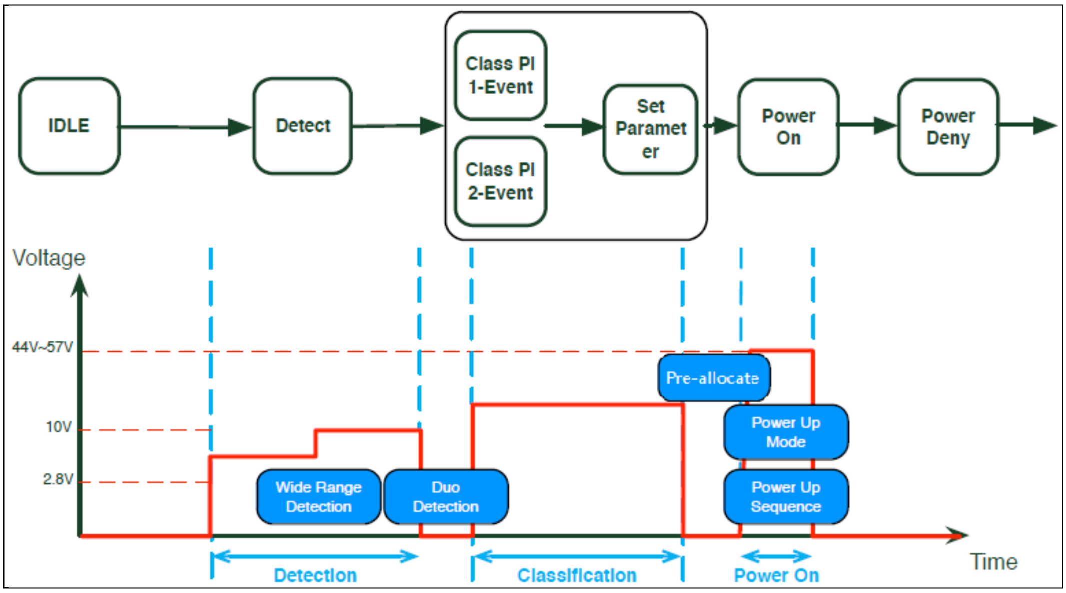
Device	PD Model X (1)	PD Model X (2)	PD Model Y
Switch Model X (1)	Fail	Fail	Success
Switch Model X (2)	Fail	Fail	Success
Switch Model Y	Success	Success	Success

Device	PD Model X (1)	PD Model X (2)	PD Model Y
Switch Model X (1)	Fail	Fail	Success
Switch Model X (2)	Fail	Fail	Success
Switch Model Y	Fail	Fail	Success

18.3 The interoperability issue.

It is the flow talking about when the PD connect to the PSE, how the PSE decides to power on it or not.

Figure 1



18.4 Wide Range Detection

During the detection in the flow, PSE will send a little power to detect the connected device is PD or not. The IEEE802.3 defined a detected range for PD. If the PD out of the range, the PSE will not recognize it is a "PD", and then the PSE decide not to supply it. The feature is a little to extend the detected range to let the PSE recognize it. If you can see PD power indicator flash occasionally, please try to use the feature.

- You can also try "Dual detection" to double check it.

18.5 Power-Up

This is Zyxel's solution for powering-on PDs with a current output outside the standard defined range. Each mode uses different criteria for power delivery. It is advised that if the power-on option what you used does not power-on your PD, try changing the power-on option in this order: **802.3at -> 802.3af -> Legacy -> Pre-802.3at**. If the PD is powered on via anyone mode in the above, it is the mode it should be.

18.6 Report HQ

If you want to request HQ for further examining the IOP issue, please also provide the following information:

A. PD : Model info, Supported PoE standard and class, the number

B. Cross test result

C. Business impact (Project info, customer background, the number of switch they have)

Other can help you :

- Power-up sequence delay

  If you have to power on many PD, they will possible to request switch at same time, and let the PoE abnormal failed. Please use the feature to let switch power on PDs one by one.