ZYXEL

www.zyxel.com

User Handbook

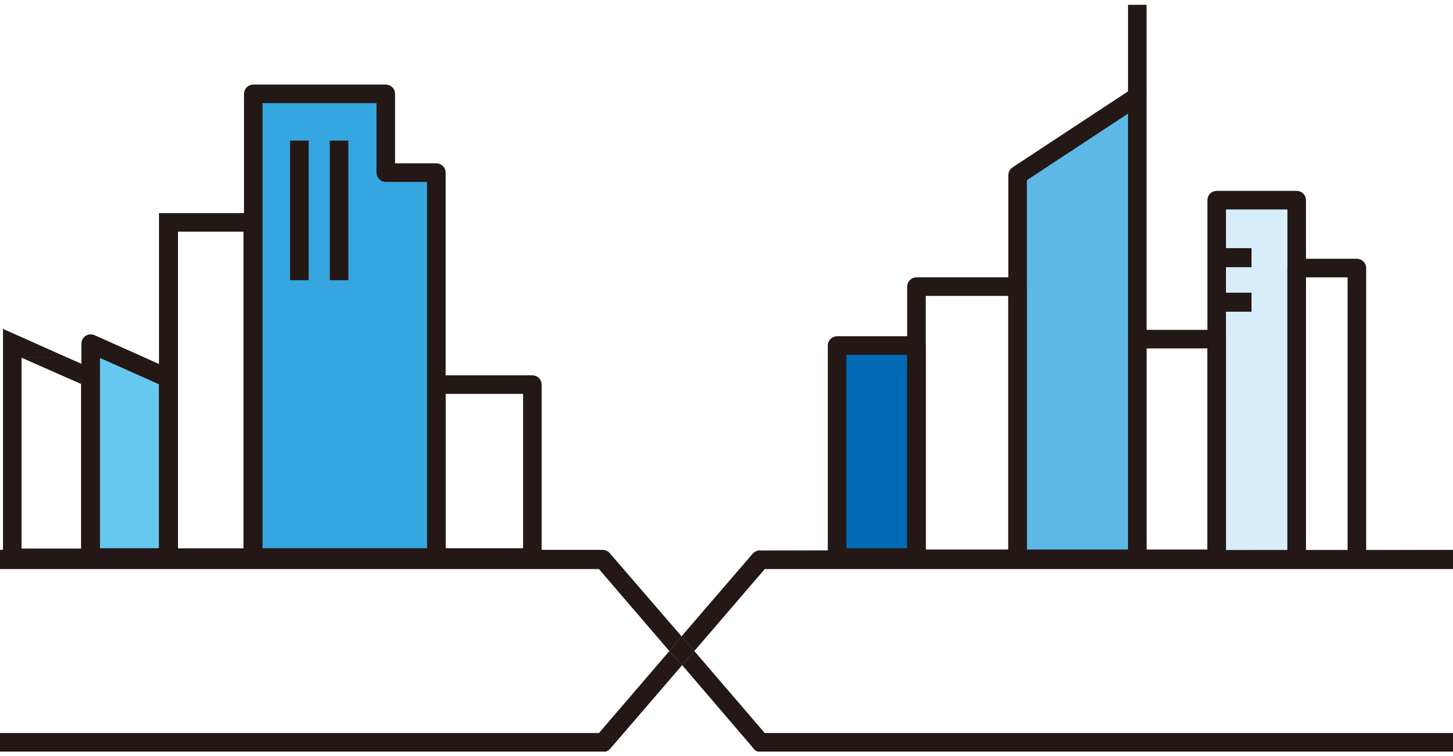
Switch Series

Zyxel GS1920 / GS2210 / XGS2210 / GS3700 / XGS3700 / XGS4600 / XS1920 / XS3700

Default Login Details

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

Version 1.0 Edition



This handbook is a series of tutorials that guides you through various applications of the Zyxel. The purpose of the handbook is to show you how to proceed through an application rather than explain the meaning of GUI features. For the latter, see the Related Information section.

Note: IP addresses, port numbers, and object names are just examples used in these tutorials, so you must replace them with the corresponding information from your own network environment when implementing a tutorial.

Bold text indicates the name of a GUI menu, field or field choice.

The handbook is for Zyxel Enterprise Switch series products. Not all products support all firmware features. Screenshots and graphics in this handbook may differ slightly from your product due to differences in your product firmware or your computer operating system. Every effort has been made to ensure that the information in this handbook is accurate at the time of writing.

Related Documentation

- User's Guide

  The User's Guide introduces the Zyxel Enterprise Switch series, describes the hardware and explains how to use the Web Configuration to configure the Zyxel Switch.

- CLI Reference Guide

  The CLI Reference Guide explains how to use the Command-Line Interface (CLI) to configure the Zyxel Switch.

Note: It is recommended you use the Web Configuration to configure the Zyxel Switch.

- More Information

  Go to **support.zyxel.com** to find other information on the Zyxel Switch.

Table Of Content

Configure the basic information on Switch

1.1 General Settings

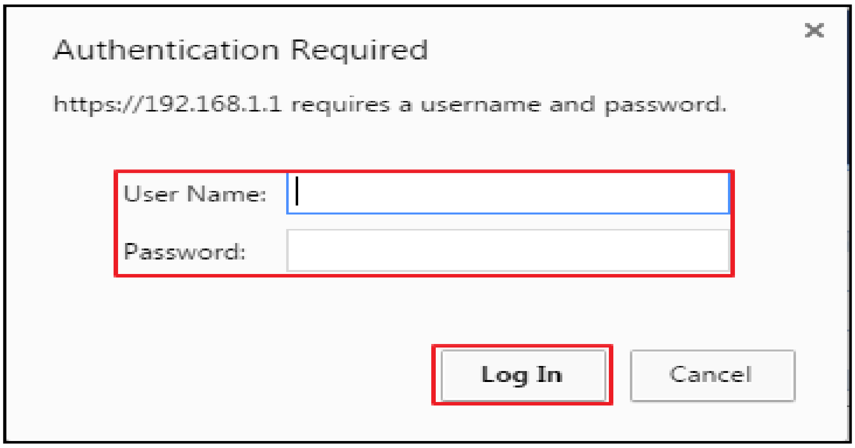
1.1.1 How to configure management IP address?

Overview

Management IP address provides to connect to the switch by using web browser to configure settings & save configuration of the entire switch.

1. Open a browser (IE, Chrome, Safari, Firefox, etc.…)
2. Go to website https://192.168.1.1 (default management IP address).
3. Default – (username: **admin**) (password: **1234**), **Log in**.

Figure 1



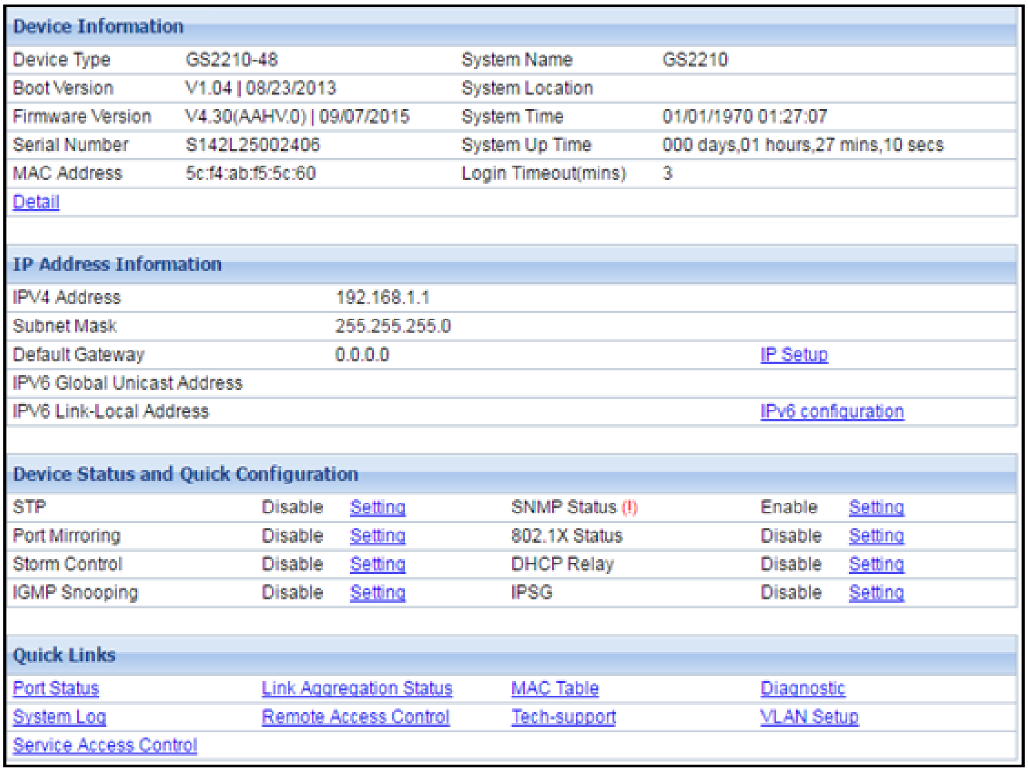
Authentication Required

https://192.168.1.1 requires a username and password.

User Name:

Password:

Figure 2 **Dashboard**



Device Information

Device Type	GS2210-48	System Name	GS2210
Boot Version	V1.04 | 08/23/2013	System Location	
Firmware Version	V4.30(AAHV.0) | 09/07/2015	System Time	01/01/1970 01:27:07
Serial Number	S142L25002406	System Up Time	000 days,01 hours,27 mins,10 secs
MAC Address	5c:f4:ab:f5:5c:60	Login Timeout(mins)	3
Detail			

IP Address Information

IPV4 Address	192.168.1.1	
Subnet Mask	255.255.255.0	
Default Gateway	0.0.0.0	IP Setup
IPV6 Global Unicast Address		
IPV6 Link-Local Address		IPv6 configuration

Device Status and Quick Configuration

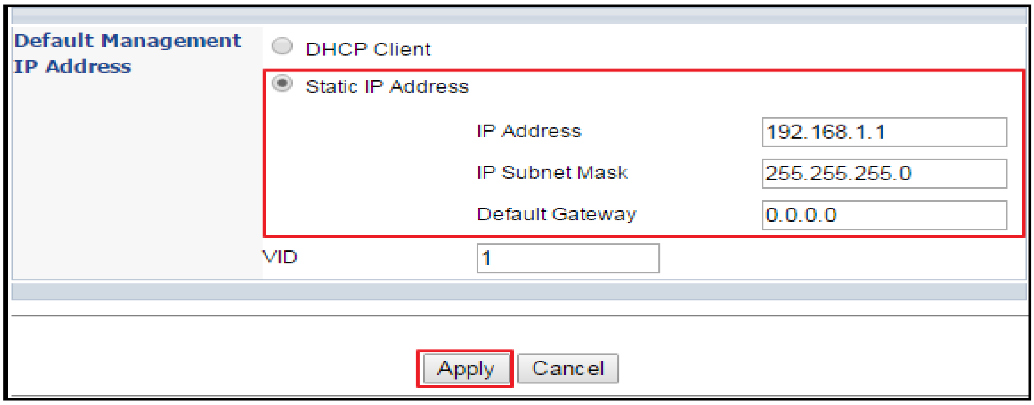
STP	Disable	Setting	SNMP Status (!)	Enable	Setting
Port Mirroring	Disable	Setting	802.1X Status	Disable	Setting
Storm Control	Disable	Setting	DHCP Relay	Disable	Setting
IGMP Snooping	Disable	Setting	IPSG	Disable	Setting

Quick Links

Port Status	Link Aggregation Status	MAC Table	Diagnostic
System Log	Remote Access Control	Tech-support	VLAN Setup
Service Access Control			

1. The highlight part, please enter the IP address & subnet mask of the switch. For example: (**192.168.1.2**, **255.255.255.0**). Then click **Apply** to save the configuration.

Figure 3 **Basic Setting > IP Setup**



Default Management IP Address

○ DHCP Client

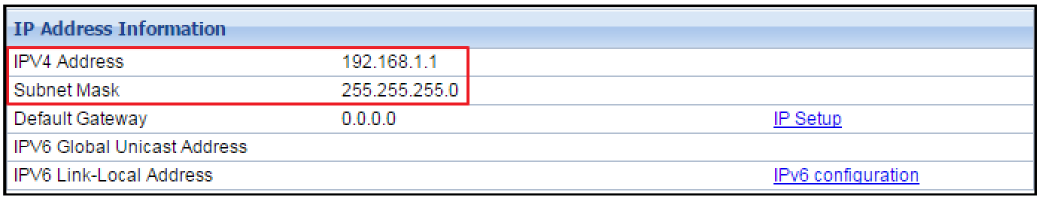
● Static IP Address

IP Address	192.168.1.1
IP Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
VID	1

Verify

1. In this screen is to check the **IP Address Information**.

Figure 4 **Quick Button > Status**



IP Address Information

IPV4 Address	192.168.1.1	
Subnet Mask	255.255.255.0	
Default Gateway	0.0.0.0	IP Setup
IPV6 Global Unicast Address		
IPV6 Link-Local Address		IPv6 configuration

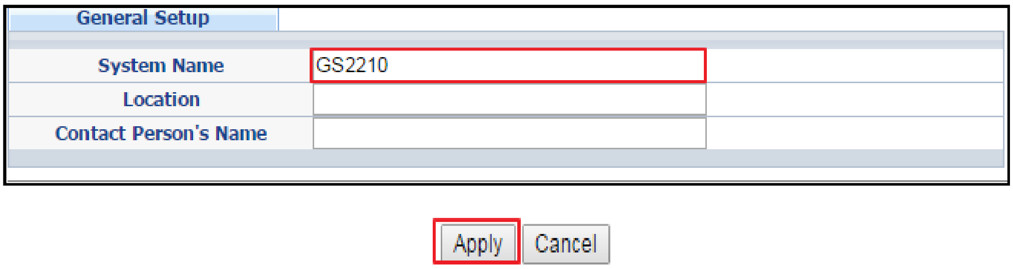
1.1.2 How to configure switch host name?

Overview

Configure the switch with hostname for identification purpose.

1. Enter a hostname for identification purpose of the switch, and then click **Apply** to save the configuration.

Figure 1 **Basic setting > General setup**



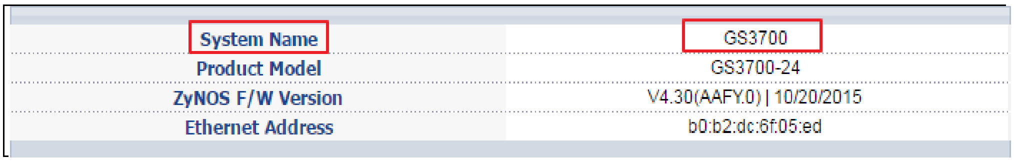
General Setup

System Name	GS2210
Location	
Contact Person's Name	

Verify

1. In the screen it will display the system status **Device information** > **System name.**

Figure 2 **Basic Setting > System Info.**



System Name	GS3700
Product Model	GS3700-24
ZyNOS F/W Version	V4.30(AAFY.0) | 10/20/2015
Ethernet Address	b0:b2:dc:6f:05:ed

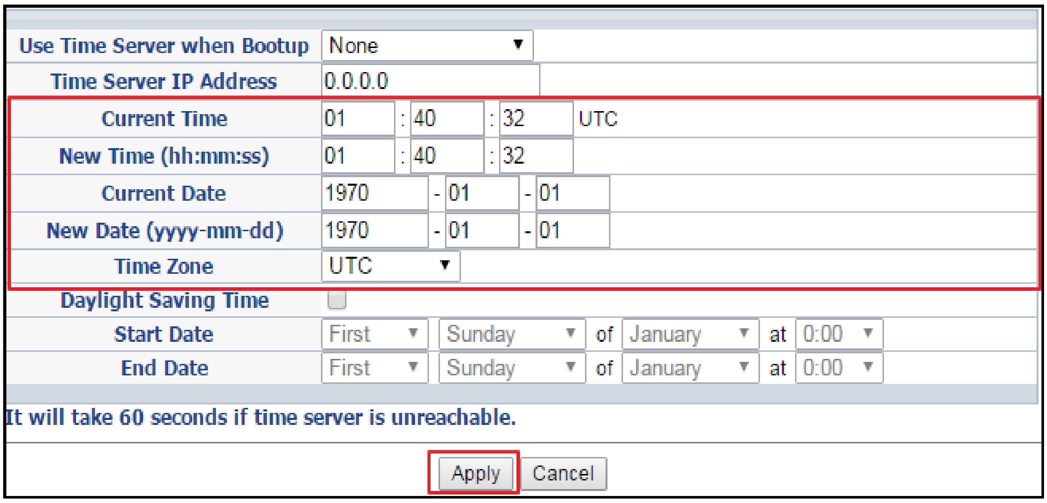
1.1.3 How to configure system time?

Overview

Set the system date and time for the switch.

1. First change the **New Date,** second change the **New Time**, and then click **Apply** to save the configuration.

Figure 1 **Basic Setting > General Setup**



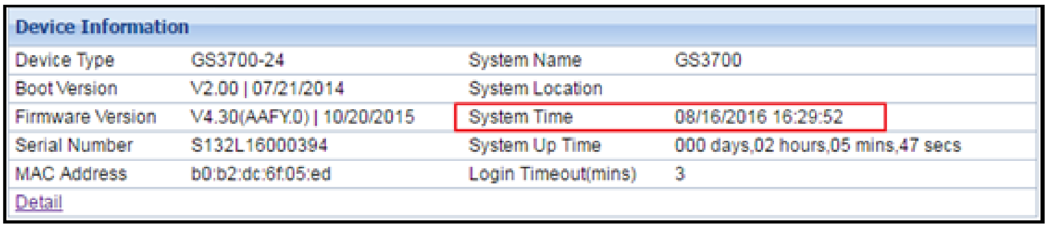
Use Time Server when Bootup	None ▼
Time Server IP Address	0.0.0.0
Current Time	01 : 40 : 32 UTC
New Time (hh:mm:ss)	01 : 40 : 32
Current Date	1970 - 01 - 01
New Date (yyyy-mm-dd)	1970 - 01 - 01
Time Zone	UTC ▼
Daylight Saving Time	□
Start Date	First ▼ Sunday ▼ of January ▼ at 0:00 ▼
End Date	First ▼ Sunday ▼ of January ▼ at 0:00 ▼

It will take 60 seconds if time server is unreachable.

Verify

1. In this screen is to check the **Device Information** > **System time**

Figure 2 **Quick Button > Status**



Device Information

Device Type	GS3700-24	System Name	GS3700
Boot Version	V2.00 | 07/21/2014	System Location	
Firmware Version	V4.30(AAFY.0) | 10/20/2015	System Time	08/16/2016 16:29:52
Serial Number	S132L16000394	System Up Time	000 days,02 hours,05 mins,47 secs
MAC Address	b0:b2:dc:6f:05:ed	Login Timeout(mins)	3

Maintain Devices and Network

2.1 Firmware

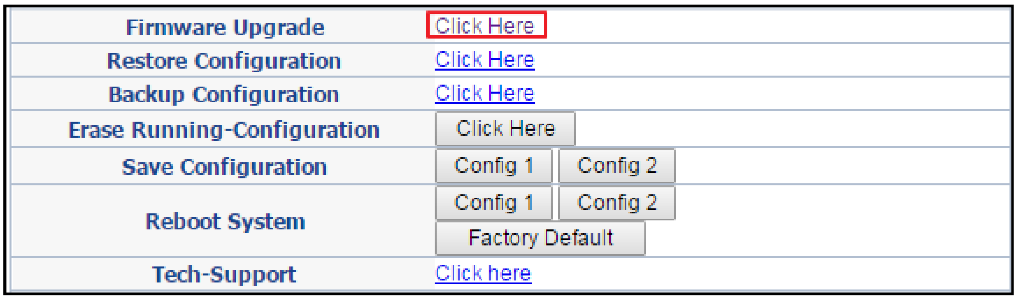
2.1.1 How to upgrade firmware from GUI?

Overview

The switch can be maintained by upgrading it to the latest new firmware version. **But make sure you have downloaded (and unzipped) the correct model firmware and version to your computer before uploading to the device, uploading the wrong model firmware may damage your device.**

1. Select **Firmware Upgrade.**

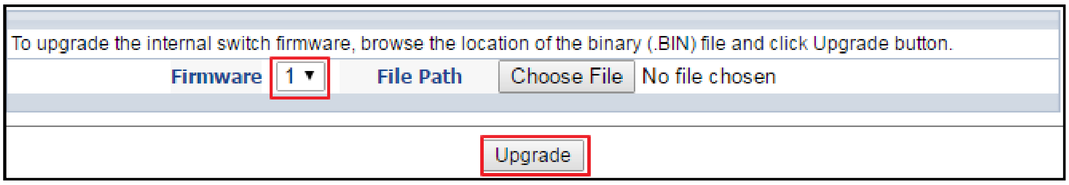
Figure 1 **Management > Maintenance > Firmware Upgrade**



Firmware Upgrade	Click Here
Restore Configuration	Click Here
Backup Configuration	Click Here
Erase Running-Configuration	Click Here
Save Configuration	Config 1 Config 2
Reboot System	Config 1 Config 2 Factory Default
Tech-Support	Click here

2. To upgrade firmware image, users can select to upload firmware image to image **1 or 2** and click upgrade to activate the process. Firmware upgrades are only applied after a reboot. To reboot, go to **Management > Maintenance > Reboot System** and select which configuration will switch use when it restart.

Figure 2 **Management > Maintenance > Firmware Upgrade**

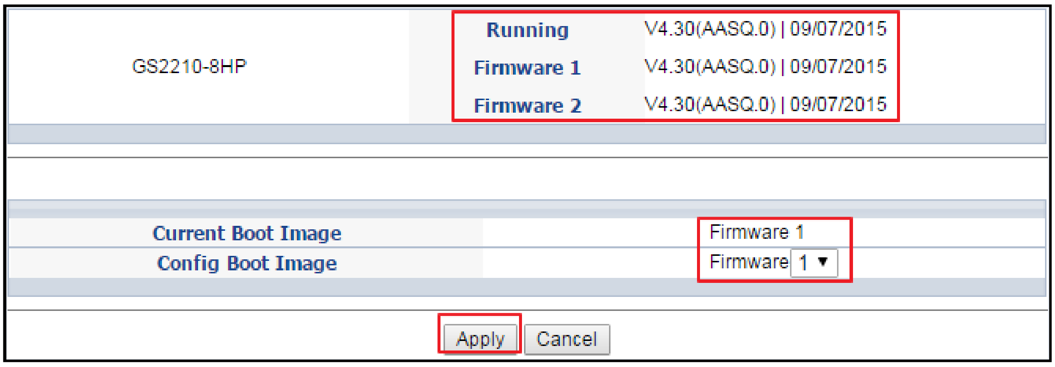


To upgrade the internal switch firmware, browse the location of the binary (.BIN) file and click Upgrade button.

Firmware: 1 ▾ File Path: Choose File No file chosen

3. Users can select which **boot image 1 or 2** to use. Then click **Apply** to save the settings into the memory of the switch. The saved settings will take effect when the switch reboot.

Figure 3 **Management > Maintenance > Firmware Upgrade**



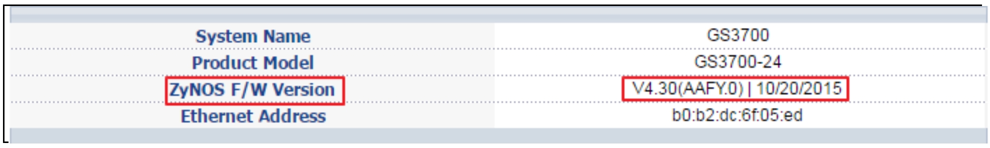
GS2210-8HP	Running	V4.30(AASQ.0) | 09/07/2015
	Firmware 1	V4.30(AASQ.0) | 09/07/2015
	Firmware 2	V4.30(AASQ.0) | 09/07/2015

Current Boot Image	Firmware 1
Config Boot Image	Firmware 1 ▾

Verify

1. In this screen to check **Device Information >Firmware Version**

Figure 4 **Basic Setting > System Info.**



System Name	GS3700
Product Model	GS3700-24
ZyNOS F/W Version	V4.30(AAFY.0) | 10/20/2015
Ethernet Address	b0:b2:dc:6f:05:ed

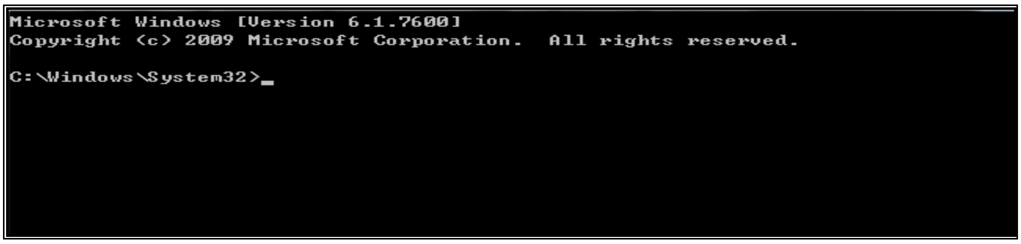
2.1.2 How to upgrade firmware from FTP?

Overview

Upgrade firmware by using File Transfer Protocol (FTP).

1. On the operating system open the **Command Processor** (**CMD**).

Figure 1 **PC > Start > All Programs > Accessories > Command Prompt**

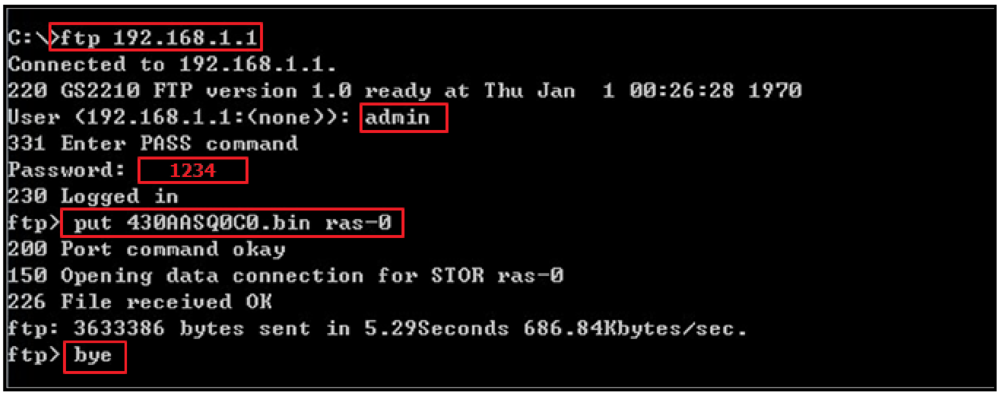


```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\System32>_
```

2. Use a FTP client to access the switch>**ftp (switch IP address)**>**Enter username & password**> **put** 430XXXX0C0.bin **ras-0**. Ras-0: firmware image 1. Ras-1: firmware image 2. Ras: only for Switch model series with only single image.

Note: The firmware image (.bin file) should be in the same directory of the cmd command page.

Figure 2

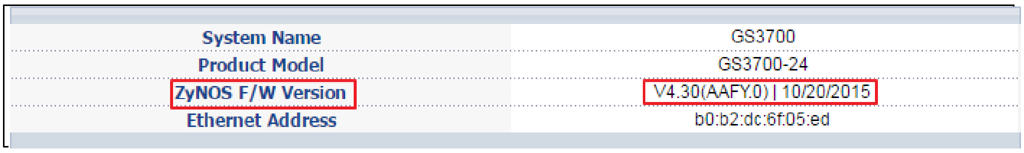


```
C:\>ftp 192.168.1.1
Connected to 192.168.1.1.
220 GS2210 FTP version 1.0 ready at Thu Jan  1 00:26:28 1970
User (192.168.1.1:(none)): admin
331 Enter PASS command
Password:  1234
230 Logged in
ftp> put 430AASQ0C0.bin ras-0
200 Port command okay
150 Opening data connection for STOR ras-0
226 File received OK
ftp: 3633386 bytes sent in 5.29Seconds 686.84Kbytes/sec.
ftp> bye
```

Verify

1. Go to website https://192.168.1.1, click the quick button **(Status)**. Check in the **Device Information** >**Firmware Version**

Figure 3 **Basic Setting > System Info.**



System Name	GS3700
Product Model	GS3700-24
ZyNOS F/W Version	V4.30(AAFY.0) | 10/20/2015
Ethernet Address	b0:b2:dc:6f:05:ed

2.2 Reset

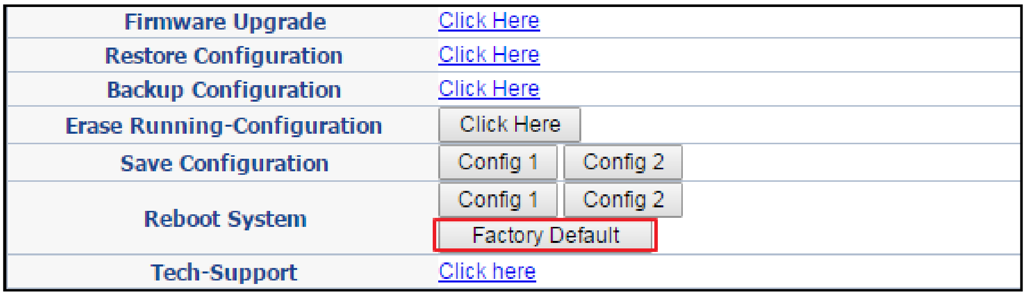
2.2.1 How to reset switch?

Overview

Reset the switch to its default settings.

1. In this page click the **Factory default** Icon, the switch will reset back to default settings. Then wait for the switch to restart.

Figure 1 **Management > Maintenance**



Firmware Upgrade	Click Here
Restore Configuration	Click Here
Backup Configuration	Click Here
Erase Running-Configuration	Click Here
Save Configuration	Config 1 Config 2
Reboot System	Config 1 Config 2 Factory Default
Tech-Support	Click here

Verify

1. Go to website https://192.168.1.1, the entire switch configuration will be gone and set to default configuration.

NOTE: Each Zyxel switch products has a different **Reset** web page settings & hardware reset button, please kindly reference the User guides.

3.1 Virtual Local Area Network

Overview

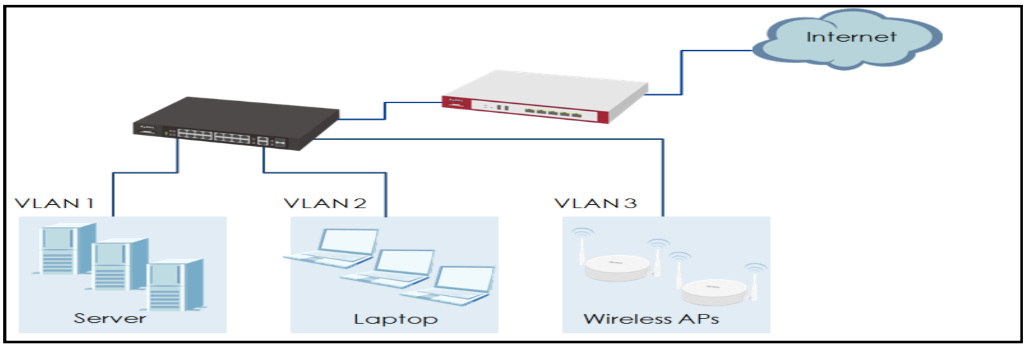
VLAN is a group of end stations with a common set of requirements; Independent of their physical location, floods traffic only to the ports belongs to that VLAN.

- VLAN characteristic:
  - ◆ A broadcast domain.
  - ◆ Logical network. (Subnet).
  - ◆ An independent LAN network.

- Benefits of VLAN:
  - ◆ Simple management.
  - ◆ Increase performance.
  - ◆ Flexible network segmentation.
  - ◆ Enhance network security.
  - ◆ Reduce costs.

VLAN topology:

Figure 1



Note: In the scenario it configured with 3 VLANs, divided into VLAN1 (server), VLAN2 (laptop) & VLAN3 (wireless APs). Different VLAN group can't communicate with other VLAN, unless it goes through a router.

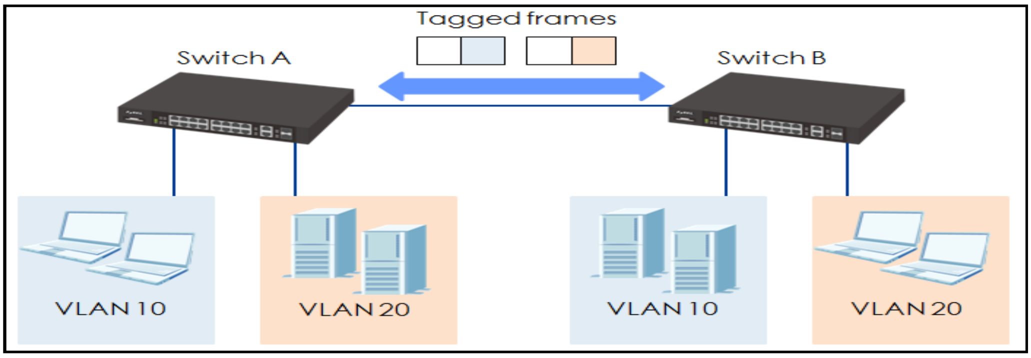
3.1.1 How to configure Static VLAN on the switch?

Overview

Static VLAN is the widest used VLAN in real application. It can cross multiple switches. It does add s 4 bytes to be tagged frame into its normal MTU.

Static VLAN topology,

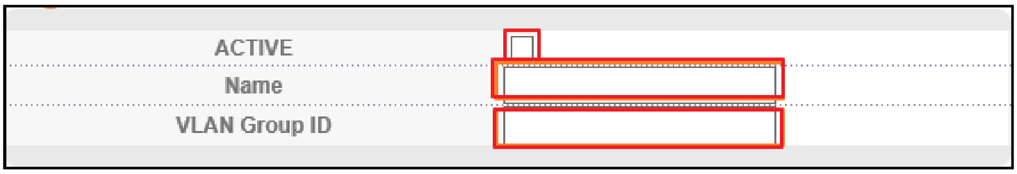
Figure 1



Note: In the scenario, both switch is configured with VLAN10/20, in order to let the same VLAN to communicate is to tag the frames with a VID number.

1. Check the **Active** to activate the VLAN settings. Enter a descriptive name for VLAN group for identification purpose and enter the valid VLAN ID for this static entry.

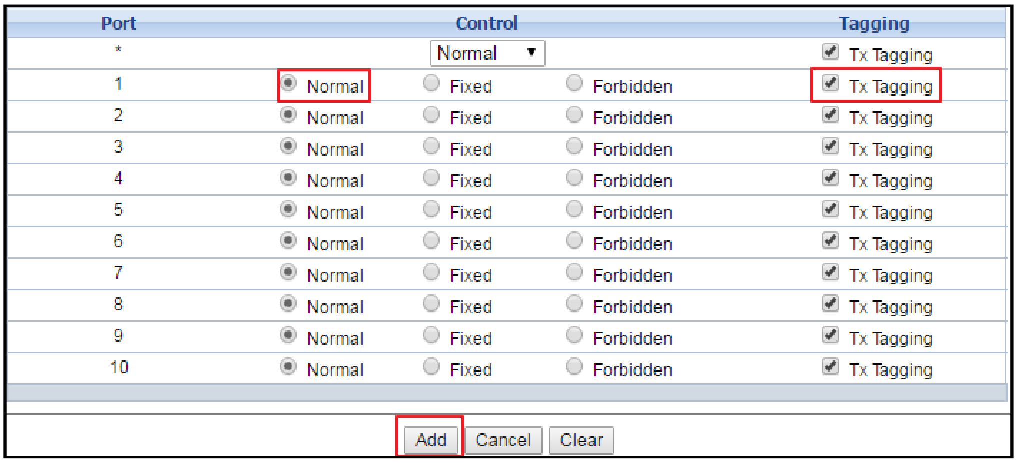
Figure 2 **Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup**



ACTIVE	□
Name	
VLAN Group ID	

2. Choose which control to be configured, **Normal**: for the port to dynamically join this VLAN group using GVRP. **Fixed**: to be permanent member of this VLAN group. **Forbidden**: prohibit the port from joining this VLAN group. Check the **tagging** to tag all outgoing frames with this VLAN group ID, then click **Add**.

Figure 3 **Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup**

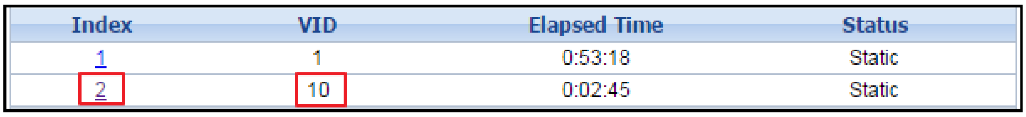


Port	Control			Tagging
*	Normal ▾			☑ Tx Tagging
1	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
2	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
3	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
4	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
5	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
6	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
7	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
8	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
9	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
10	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging

Verify

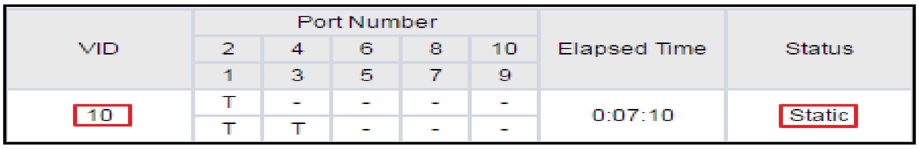
1. Check the VLAN status in the **Index** table, it will display the VLAN that been configured. Example: (**Figure 4**) User configured **VID 10**, to check the status, click **Index no. 2**, then it will display the configuration of the **VID 10** as it show in (**Figure 5**).

Figure 4 **Advanced Application > VLAN**



Index	VID	Elapsed Time	Status
1	1	0:53:18	Static
2	10	0:02:45	Static

Figure 5 **Advanced Application > VLAN > Index**



VID	Port Number					Elapsed Time	Status
	2	4	6	8	10		
	1	3	5	7	9		
10	T	-	-	-	-	0:07:10	Static
	T	T	-	-	-		

3.1.2 How to configure Subnet Base VLAN on the switch?

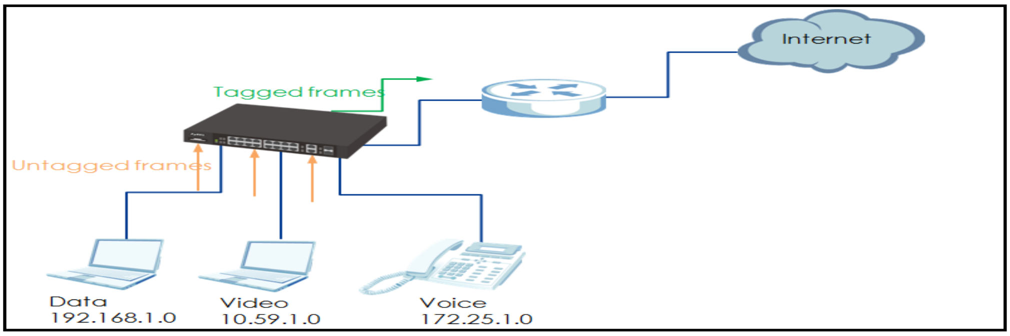
Overview

Subnet based VLANs allow to group traffic into logical VLANs based on the source IP subnet you specify.

Note: Subnet based VLAN applies to un-tagged packets and is applicable only when you use IEEE 802.1Q tagged VLAN.

Subnet based VLAN topology,

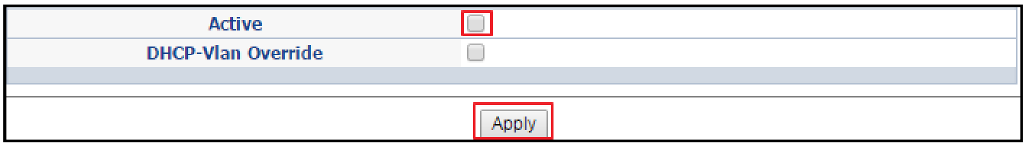
Figure 1



Note: In the scenario, switch is configured with a three specify IP source subnet. It divided with Data (192.168.1.0), Video (10.59.1.0) & Voice (172.25.1.0). With this feature if the switch receives an IP address of 192.168.1.1, the device will know that the traffic is Data traffic.

1. Check the **Active** box to activate the subnet-based VLAN, and then click **Apply**.

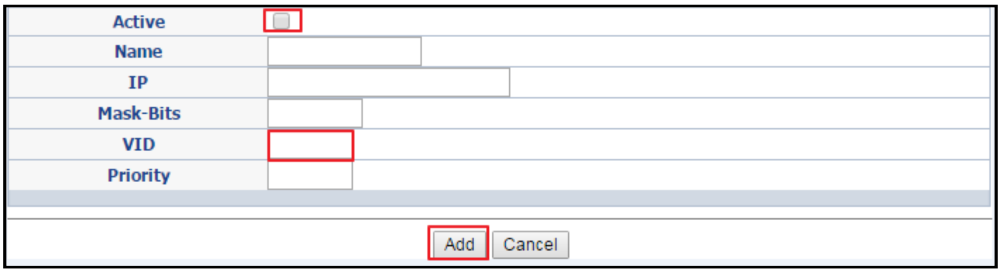
Figure 2 **Advanced Application > VLAN > VLAN Configuration > Subnet-based VLAN**



Active	□
DHCP-Vlan Override	□

2. Check the **Active** box to activate the features and **IP**, **Mask-bits** & **VID** should be filled. Click **Add** to save the configuration. For more details click the **HELP** icon at the quick button.

Figure 3 **Advanced Application > VLAN > VLAN Configuration > Subnet-based VLAN**

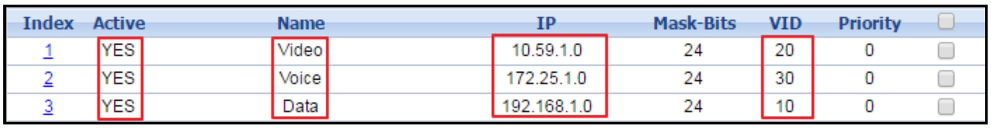


Active	☐
Name	
IP	
Mask-Bits	
VID	
Priority	

Verify:

1. Click the **Index** number to check & edit the settings.

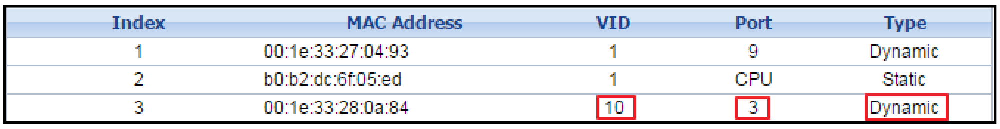
Figure 4 **Advanced Application > VLAN > VLAN Configuration > Subnet-based VLAN**



Index	Active	Name	IP	Mask-Bits	VID	Priority	☐
1	YES	Video	10.59.1.0	24	20	0	☐
2	YES	Voice	172.25.1.0	24	30	0	☐
3	YES	Data	192.168.1.0	24	10	0	☐

2. The device Mac Address should be listed inside the MAC table with a specified VID group number configured by client.

Figure 5 **Management > MAC Table**



Index	MAC Address	VID	Port	Type
1	00:1e:33:27:04:93	1	9	Dynamic
2	b0:b2:dc:6f:05:ed	1	CPU	Static
3	00:1e:33:28:0a:84	10	3	Dynamic

3.1.3 How to configure Protocol Base VLAN on the switch?

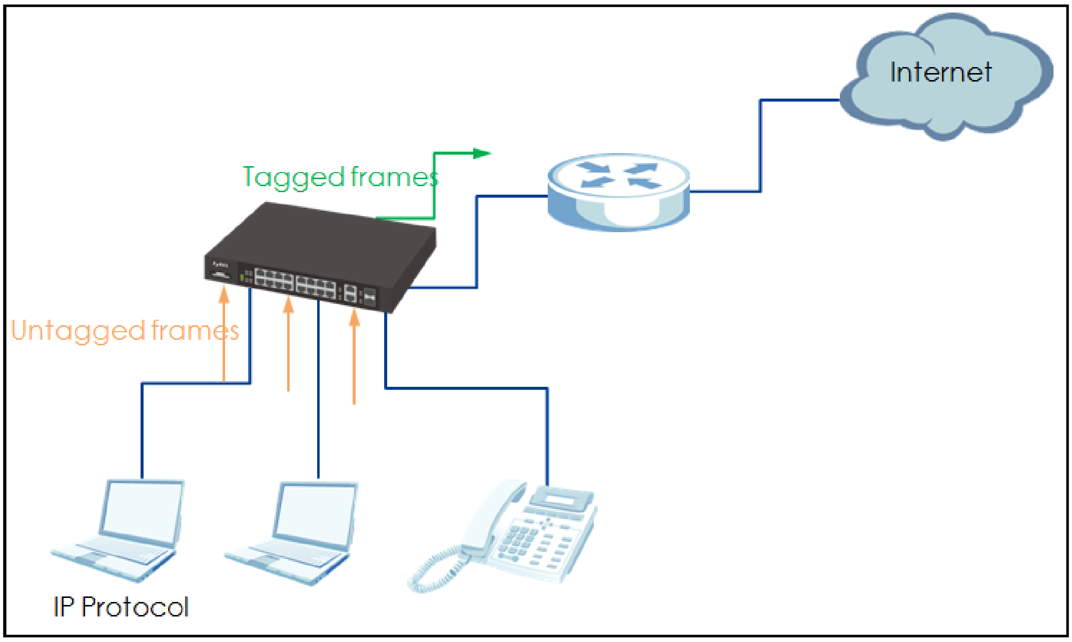
Overview

Protocol-based VLANs allow you to group traffic into logical VLANs based on the protocol you specify. Allow users to classify source traffic by specific protocols.

Notes: Protocol-based VLAN applies to un-tagged packets and is applicable only when you use IEEE 802.1Q tagged VLAN.

Protocol Base VLAN topology:

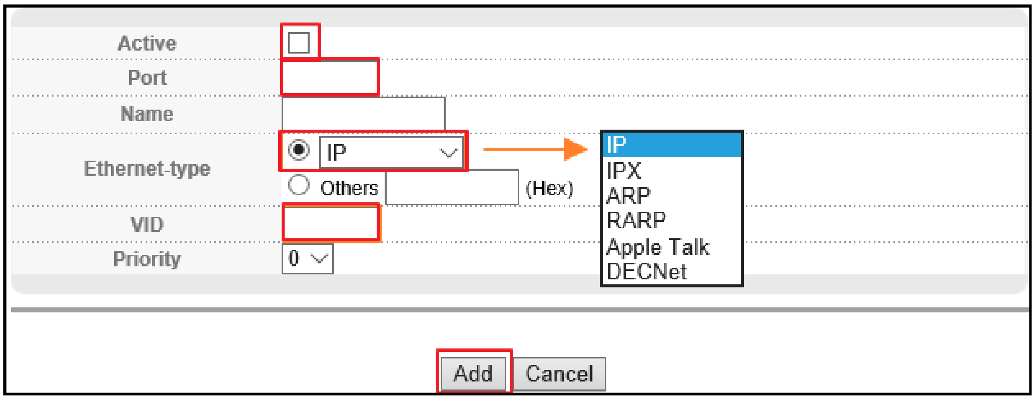
Figure 1



Note: In the scenario, the switch is configured and specify based on the protocol.

1. Check the **Active** box to activate the features. Choose which **Ethernet-type** to configure. Fill in the **VID** number that has been created on the static VLAN. Then click **Add** to save the configuration.

Figure 2 **Advanced Application > VLAN > VLAN Configuration > Protocol-based VLAN**

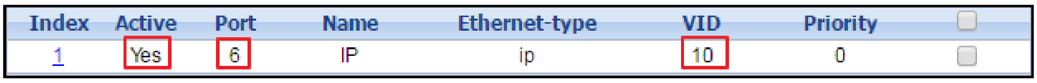


Active	☐
Port	
Name	
Ethernet-type	● IP ○ Others (Hex)
VID	
Priority	0

Verify

1. Click the **Index** number to check & edit the configuration.

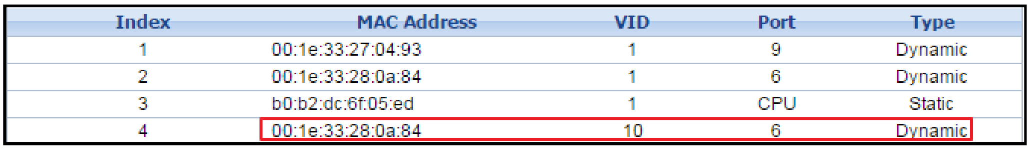
Figure 3 **Advanced Application > VLAN > VLAN Configuration > Protocol-based VLAN**



Index	Active	Port	Name	Ethernet-type	VID	Priority	☐
1	Yes	6	IP	ip	10	0	☐

2. The MAC Address of the device should be listed in the MAC table with the specified VID group number configured by client.

Figure 4 **Management > MAC Table**



Index	MAC Address	VID	Port	Type
1	00:1e:33:27:04:93	1	9	Dynamic
2	00:1e:33:28:0a:84	1	6	Dynamic
3	b0:b2:dc:6f:05:ed	1	CPU	Static
4	00:1e:33:28:0a:84	10	6	Dynamic

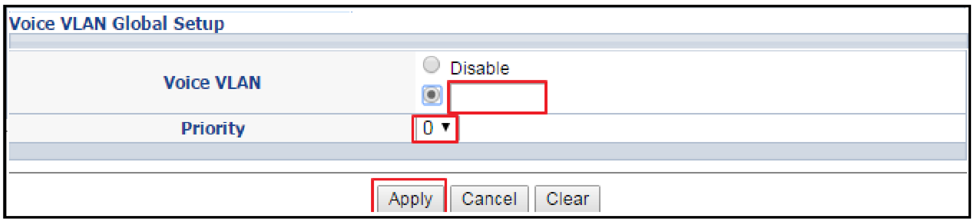
3.1.4 How to configure Voice VLAN on the switch?

Overview

Voice VLAN ensures that the sound quality of an IP phone is preserved from deteriorating when the data traffic on the Switch ports is high which enables the separation of voice and data traffic coming onto the Switch port.

1. Click the Voice VLAN radio button if you want to enable the Voice VLAN feature and enter a valid VLAN ID number that is associated with the voice VLAN. Then click **Apply** to save the configuration.

Figure 1 **Advanced Application > VLAN > VLAN Configuration >Voice VLAN**

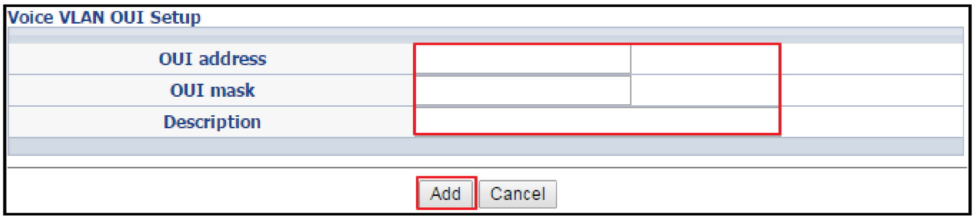


Voice VLAN Global Setup

Voice VLAN	○ Disable ●
Priority	0 ▾

2. Setting up voice VLAN OUI, fill in the three options. Then click **Add** to apply the setup. For more specific details click the **HELP** icon on the upper right corner of the page.

Figure 2 **Advanced Application > VLAN > VLAN Configuration >Voice VLAN**



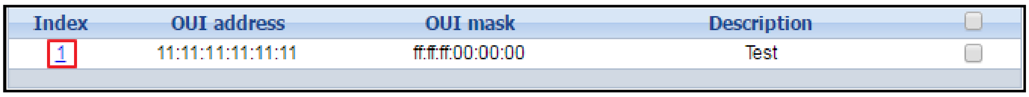
Voice VLAN OUI Setup

OUI address	
OUI mask	
Description	

Verify

1. Click the **Index** number to check & edit the configuration.

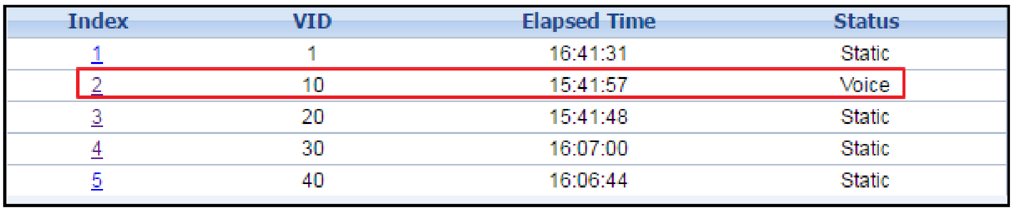
Figure 3 **Advanced Application > VLAN > VLAN Configuration >Voice VLAN**



Index	OUI address	OUI mask	Description	□
1	11:11:11:11:11:11	ff:ff:ff:00:00:00	Test	□

2. Display the VID number & the status VLAN.

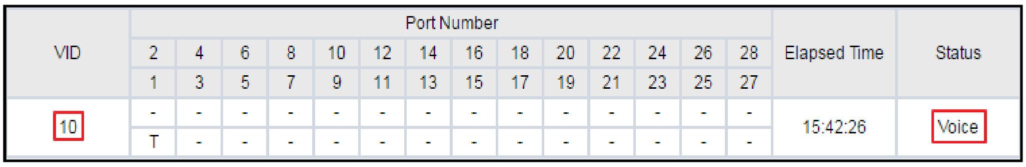
Figure 4 **Advanced Application > VLAN**



Index	VID	Elapsed Time	Status
1	1	16:41:31	Static
2	10	15:41:57	Voice
3	20	15:41:48	Static
4	30	16:07:00	Static
5	40	16:06:44	Static

3. To confirm the port number belongs to which VID & VLAN.

Figure 5 **Advanced Application > VLAN > Index 2**



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		
10	-	-	-	-	-	-	-	-	-	-	-	-	-	-	15:42:26	Voice
	T	-	-	-	-	-	-	-	-	-	-	-	-	-		

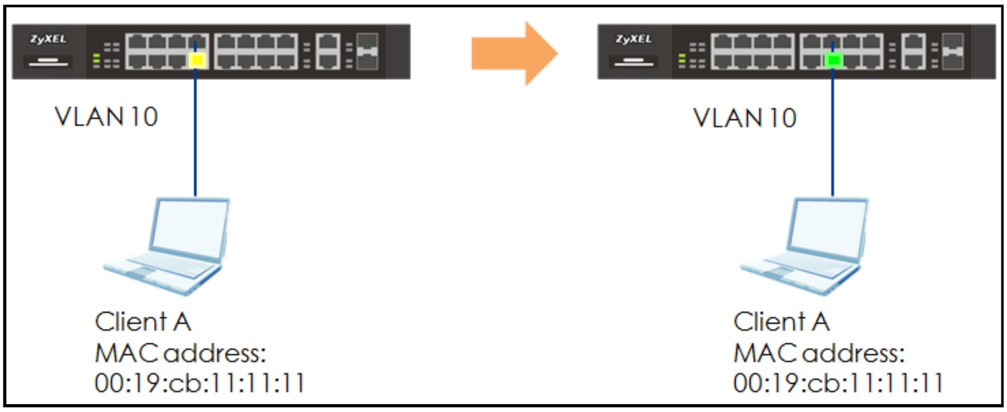
3.1.5 How to configure MAC Base VLAN on the switch?

Overview

MAC-based VLAN feature assigns incoming untagged packets to a VLAN and classifies the traffic based on the source MAC address of the packet. A feature that decides the VLAN for forwarding an untagged frame based on the source MAC address of the frame.

MAC Base VLAN topology:

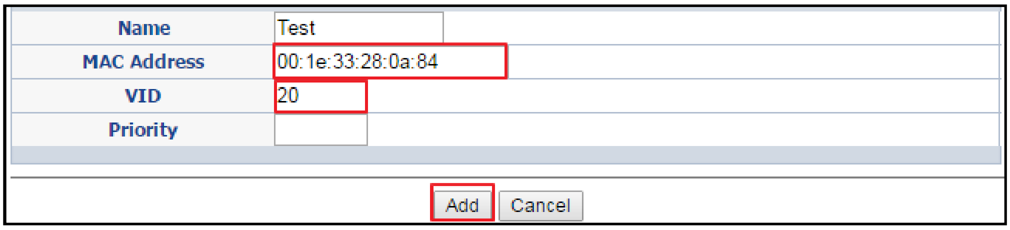
Figure 1



Note: In the scenario, the switch port is configured with the specific device (Client A) VID & MAC address.

1. Fill in the exact MAC address of the device and enter which VID group number to be configured then click **Add** to run the features.

Figure 2 **Advanced Application > VLAN > VLAN Configuration > MAC-based VLAN**

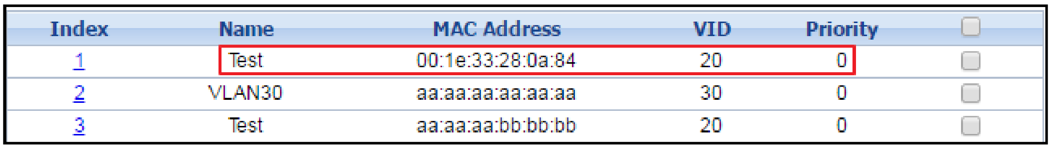


Name	Test
MAC Address	00:1e:33:28:0a:84
VID	20
Priority	

Verify

1. It display the MAC based VLAN configuration. Click the **Index** number to change the configuration.

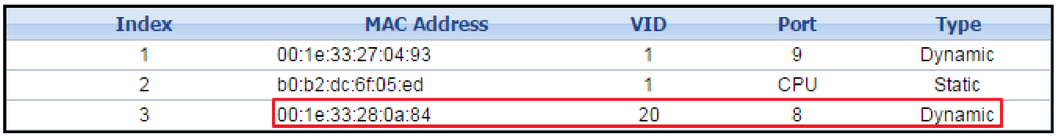
Figure 3 **Advanced Application > VLAN > VLAN Configuration > MAC-based VLAN**



Index	Name	MAC Address	VID	Priority	□
1	Test	00:1e:33:28:0a:84	20	0	□
2	VLAN30	aa:aa:aa:aa:aa:aa	30	0	□
3	Test	aa:aa:aa:bb:bb:bb	20	0	□

2. The device MAC address should be seen in the MAC table.

Figure 4 **Management > MAC Table**



Index	MAC Address	VID	Port	Type
1	00:1e:33:27:04:93	1	9	Dynamic
2	b0:b2:dc:6f:05:ed	1	CPU	Static
3	00:1e:33:28:0a:84	20	8	Dynamic

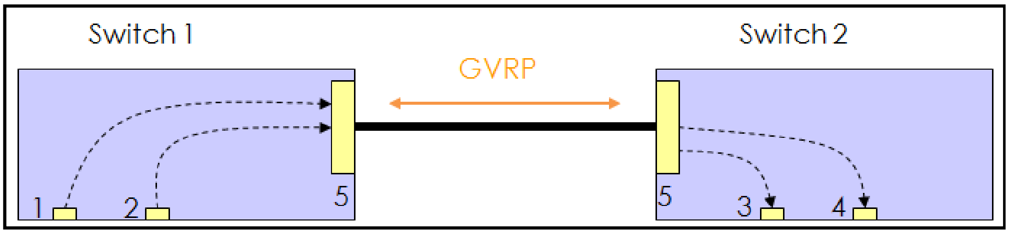
3.1.6 How to configure GVRP on the switch?

Overview

GVRP a protocol dynamically exchange VLAN configuration information with other devices.

GVRP topology:

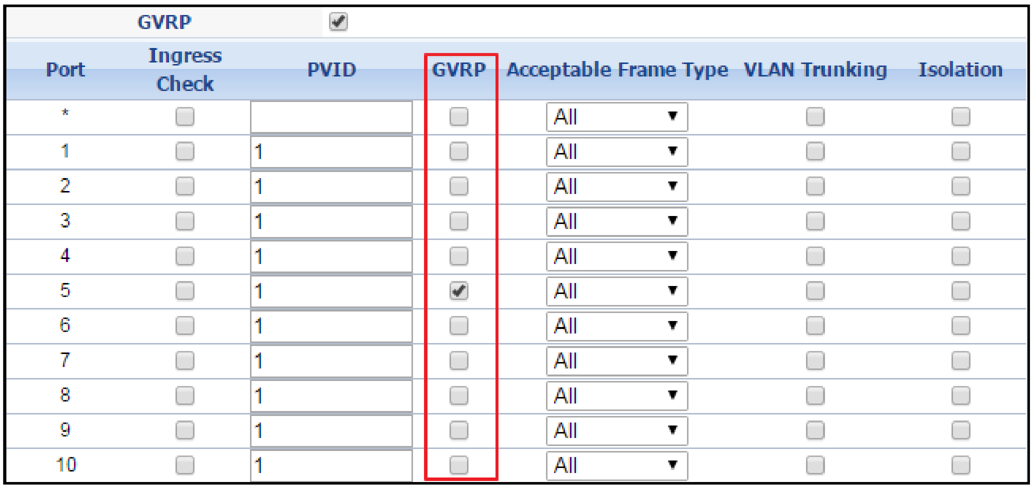
Figure 1



Note: In the scenario both switch port number 5 are enable with GVRP features, so that the switch 1 will learn the switch 2 VLAN configuration dynamically, same with switch 2 it will learn the VLAN configuration of switch 1 dynamically.

1. Check the GVRP box to activate the features and select which port should be process with GVRP features. Then click **Apply** to activate the features.

Figure 2 **ADVANCED APPLICATION > VLAN > VLAN CONFIGURATION > VLAN PORT SETUP**



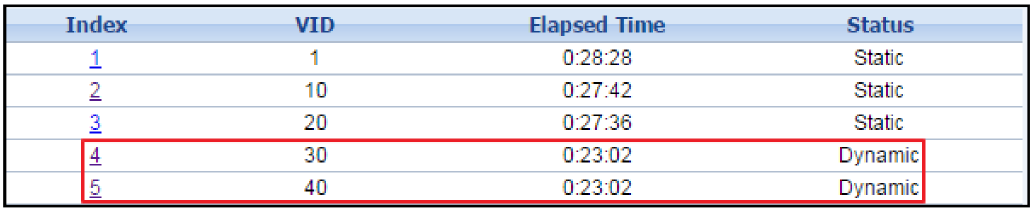
GVRP ☑

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	□	1	□	All ▾	□	□
8	□	1	□	All ▾	□	□
9	□	1	□	All ▾	□	□
10	□	1	□	All ▾	□	□

Verify

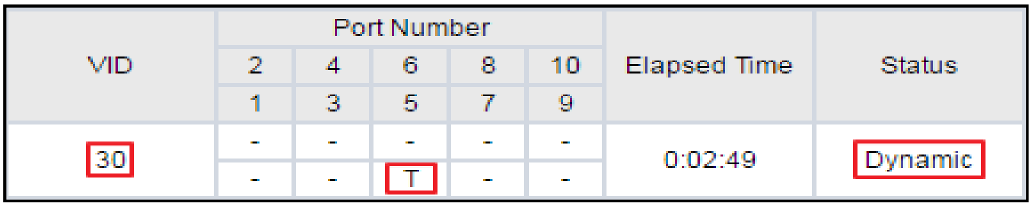
1. Check in the **Index** table, it will appear a dynamic VLAN configuration, belongs to the other device configured with GVRP. Click the **Index** number to display the VLAN table.

Figure 3 **(Switch 1) Advanced Application > VLAN**



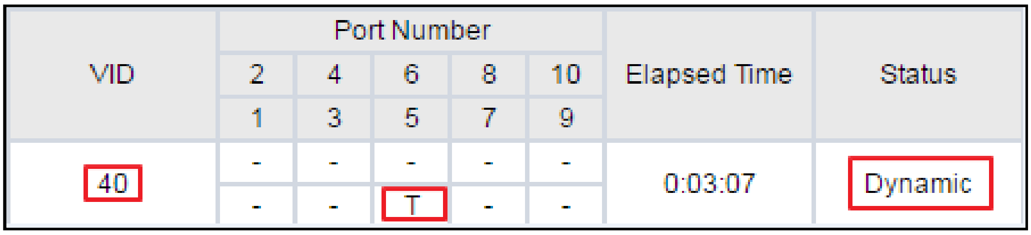
Index	VID	Elapsed Time	Status
1	1	0:28:28	Static
2	10	0:27:42	Static
3	20	0:27:36	Static
4	30	0:23:02	Dynamic
5	40	0:23:02	Dynamic

Figure 4 **(Switch 1)**



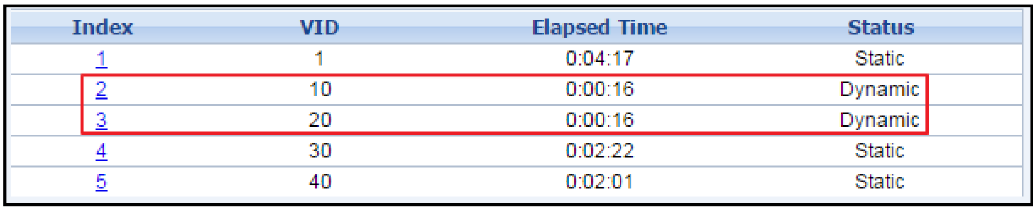
VID	Port Number					Elapsed Time	Status
	2	4	6	8	10		
	1	3	5	7	9		
30	-	-	-	-	-	0:02:49	Dynamic
	-	-	T	-	-		

Figure 5 **(Switch 1)**



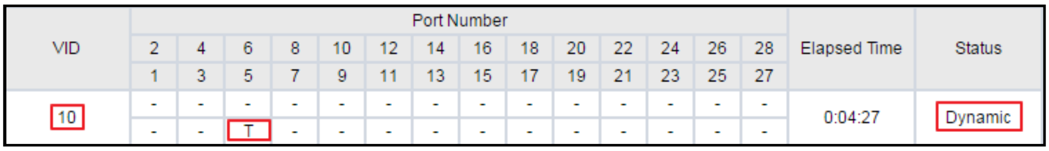
VID	Port Number					Elapsed Time	Status
	2	4	6	8	10		
	1	3	5	7	9		
40	-	-	-	-	-	0:03:07	Dynamic
	-	-	T	-	-		

Figure 6 **(Switch 2) Advanced Application > VLAN**



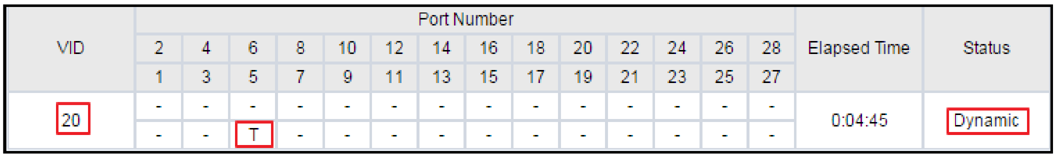
Index	VID	Elapsed Time	Status
1	1	0:04:17	Static
2	10	0:00:16	Dynamic
3	20	0:00:16	Dynamic
4	30	0:02:22	Static
5	40	0:02:01	Static

Figure 7 **(Switch 2)**



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		
10	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0:04:27	Dynamic
	-	-	T	-	-	-	-	-	-	-	-	-	-	-		

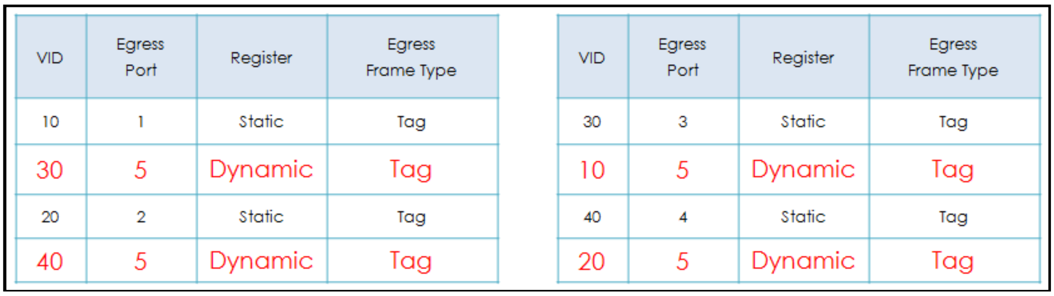
Figure 8 **(Switch 2)**



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		
20	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0:04:45	Dynamic
	-	-	T	-	-	-	-	-	-	-	-	-	-	-		

Result:

Figure 9



VID	Egress Port	Register	Egress Frame Type
10	1	Static	Tag
30	5	Dynamic	Tag
20	2	Static	Tag
40	5	Dynamic	Tag

VID	Egress Port	Register	Egress Frame Type
30	3	Static	Tag
10	5	Dynamic	Tag
40	4	Static	Tag
20	5	Dynamic	Tag

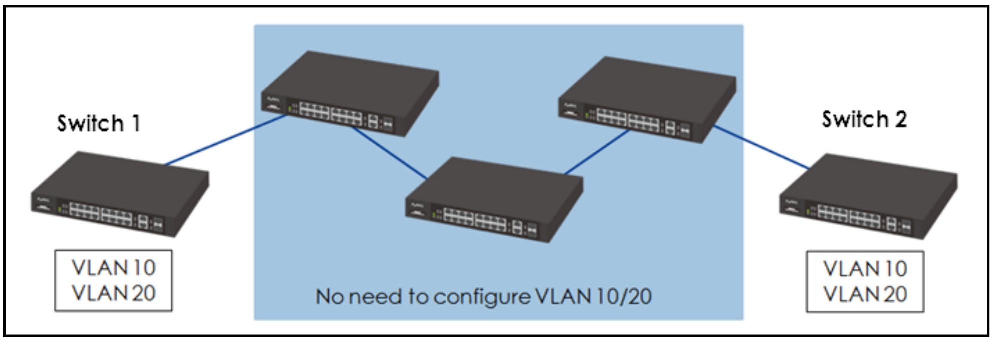
3.1.7 How to configure VLAN Trunking on the switch?

Overview

VLAN trunking, allow an unknown VLAN groups frame pass through a port. Communicate with end device without the same VLAN configuration on the switch.

VLAN trunking topology:

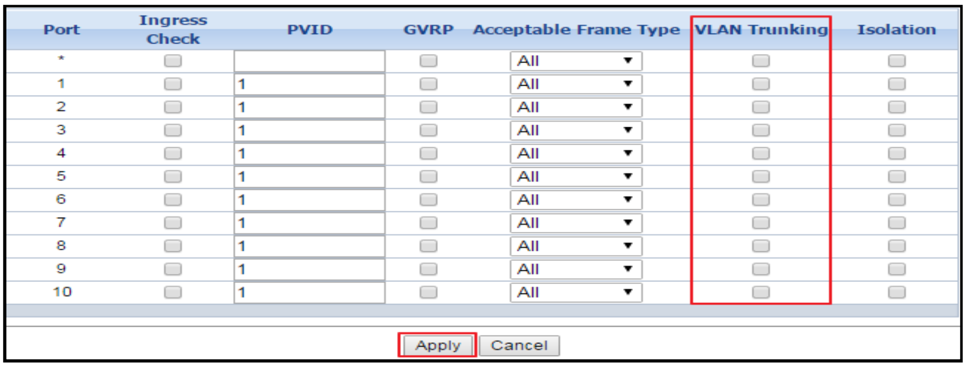
Figure 1



Note: In the scenario the task is to let switch 1 VLAN10/20 communicate with switch 2 VLAN 10/20, but the highlight part 3 switch in the center are not configured with the same VLAN. So we need to activate the VLAN trunking in the 3 switch to reach the goal.

1. Select a port connected to the other switch to allow frames belonging to unknown VLAN groups to pass through the Switch. Then click **Apply** to activate the features.

Figure 2 **Advanced Application > VLAN > VLAN Configuration > VLAN Port Setup**

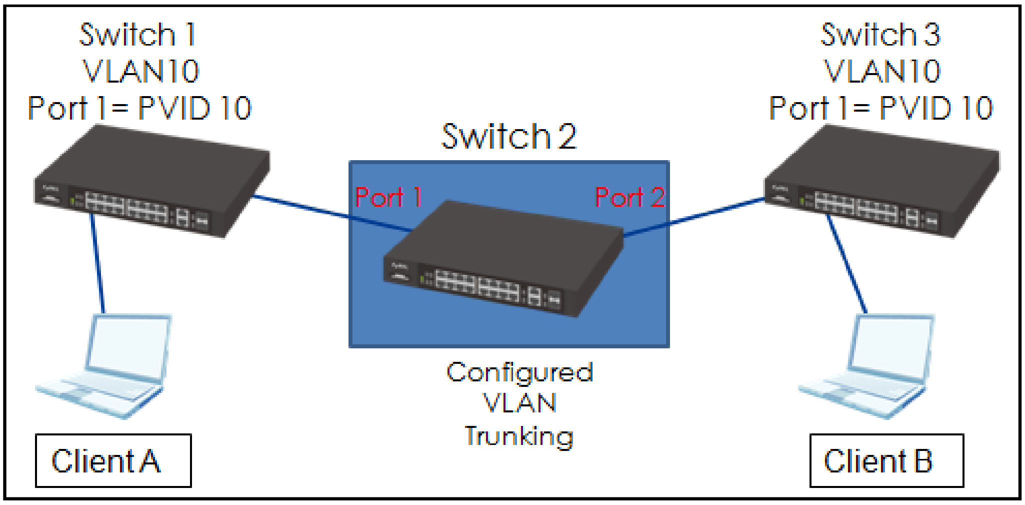


Port	Ingress Check	PVID	GVRP	Acceptable Frame Type	VLAN Trunking	Isolation
*	☐		☐	All	☐	☐
1	☐	1	☐	All	☐	☐
2	☐	1	☐	All	☐	☐
3	☐	1	☐	All	☐	☐
4	☐	1	☐	All	☐	☐
5	☐	1	☐	All	☐	☐
6	☐	1	☐	All	☐	☐
7	☐	1	☐	All	☐	☐
8	☐	1	☐	All	☐	☐
9	☐	1	☐	All	☐	☐
10	☐	1	☐	All	☐	☐

Verify

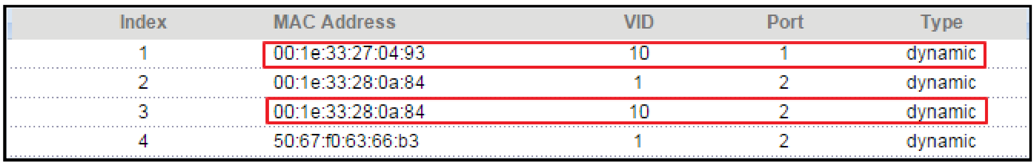
1. Switch 1 VLAN10 can ping switch 3 VLAN10.

Figure 3 Topology



2. Switch 2 will have the device MAC address & VID in the **MAC Table**.

Figure 4 **Management > MAC Table**



Index	MAC Address	VID	Port	Type
1	00:1e:33:27:04:93	10	1	dynamic
2	00:1e:33:28:0a:84	1	2	dynamic
3	00:1e:33:28:0a:84	10	2	dynamic
4	50:67:f0:63:66:b3	1	2	dynamic

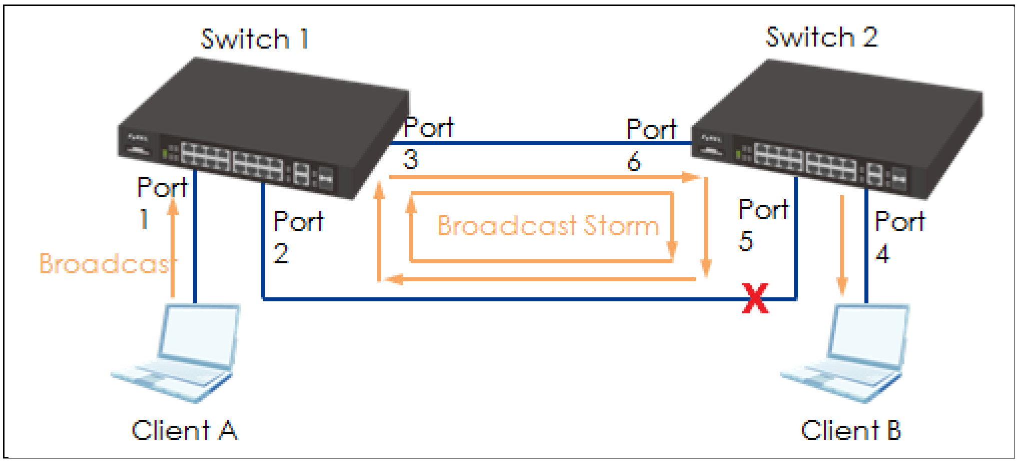
4.1 STP (Spanning Tree Protocol)

Overview

Blocks a certain ports and there is only one active path for each network segment. It's a loop avoidance mechanism, a protocol used to solve problems that are caused redundant topology like broadcast storm, multiple frame transmission & MAC database instability.

STP topology,

Figure 1



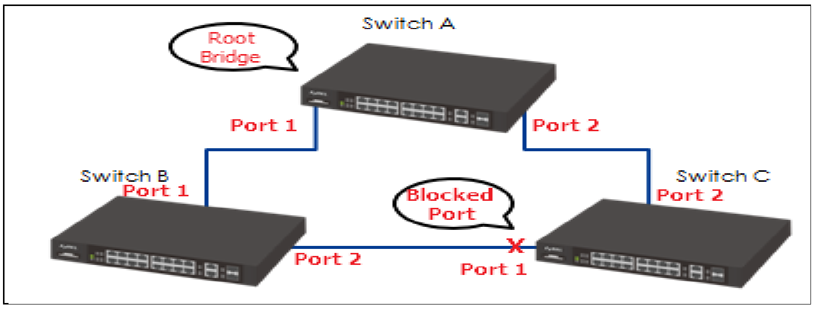
Note: In the scenario both switch are configured with STP features. Assume switch 1 is the root bridge and the switch 2 port 5 is the blocked port. STP can't prevent a broadcast storm to happen and provide redundancy for a loop topology.

4.1.1 How to configure RSTP on the switch?

Overview

The Switch uses IEEE 802.1w RSTP (Rapid Spanning Tree Protocol) that allows faster convergence of the spanning tree than STP. In RSTP, there are additional port roles; alternate port & backup port, and the port states are discarding, learning, and forwarding.

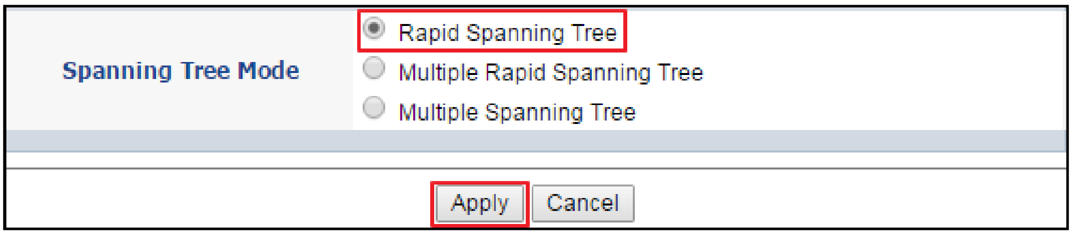
Topology:



Note: In the scenario all switch have been configured with RSTP features the elected root bridge is switch A with a lowest bridge priority and switch C port 1 is the blocked port.

1. Select **Rapid Spanning Tree** then click **Apply** to run feature.

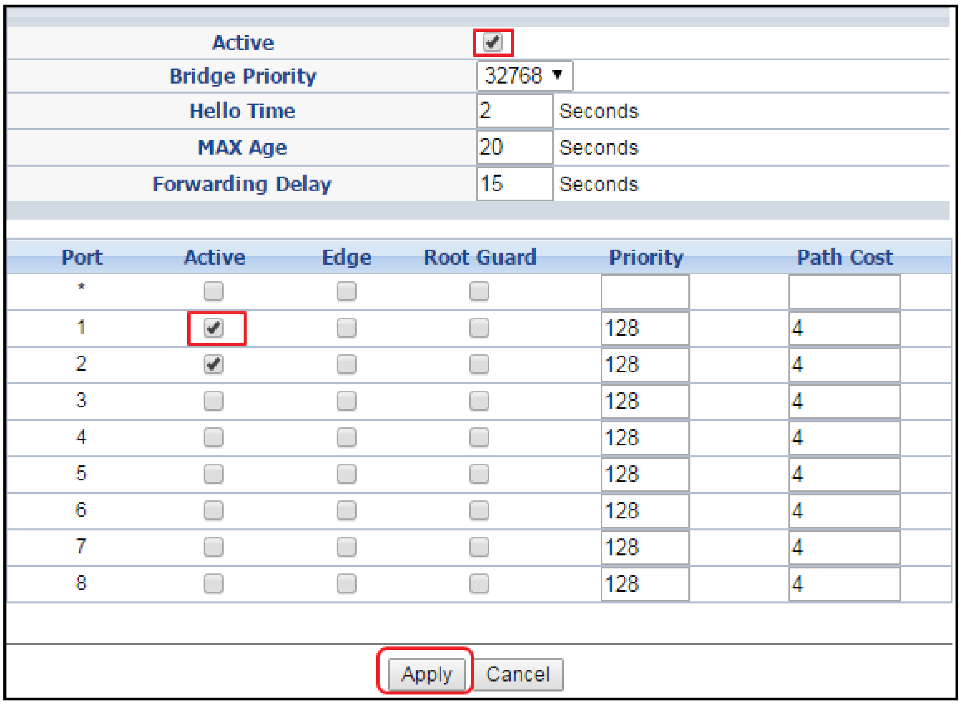
Figure 1 **Advanced Application > Spanning Tree Protocol > Configuration**



Spanning Tree Mode: ● Rapid Spanning Tree ○ Multiple Rapid Spanning Tree ○ Multiple Spanning Tree

2. Select and check which port should be activate with RSTP and click **Apply** to save the configuration. For more specific information please kindly click the **HELP** button.

Figure 2 **Advanced Application > Spanning Tree Protocol > RSTP**



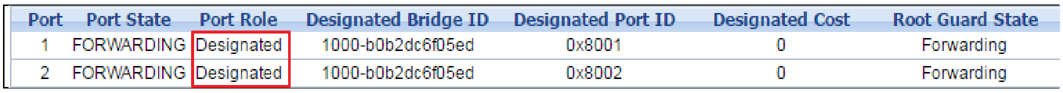
Active	☑	
Bridge Priority	32768 ▼	
Hello Time	2	Seconds
MAX Age	20	Seconds
Forwarding Delay	15	Seconds

Port	Active	Edge	Root Guard	Priority	Path Cost
*	□	□	□		
1	☑	□	□	128	4
2	☑	□	□	128	4
3	□	□	□	128	4
4	□	□	□	128	4
5	□	□	□	128	4
6	□	□	□	128	4
7	□	□	□	128	4
8	□	□	□	128	4

Verify

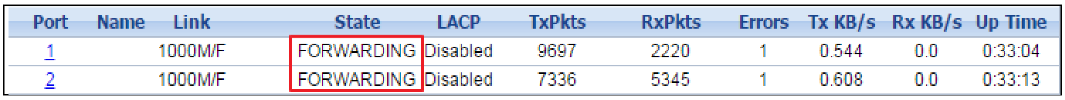
1. **Figure 3, Figure 4 & Figure 5,** In this screen display the RSTP process and port status.

Figure 3, (Switch A) **Advanced Application > Spanning Tree Protocol**



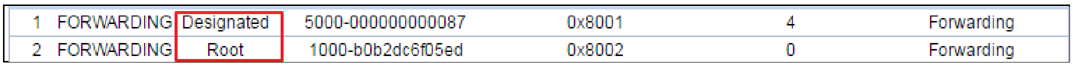
Port	Port State	Port Role	Designated Bridge ID	Designated Port ID	Designated Cost	Root Guard State
1	FORWARDING	Designated	1000-b0b2dc6f05ed	0x8001	0	Forwarding
2	FORWARDING	Designated	1000-b0b2dc6f05ed	0x8002	0	Forwarding

Management > Port Status



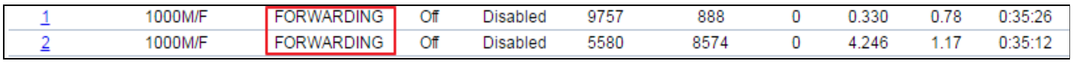
Port	Name	Link	State	LACP	TxPkts	RxPkts	Errors	Tx KB/s	Rx KB/s	Up Time
1		1000M/F	FORWARDING	Disabled	9697	2220	1	0.544	0.0	0:33:04
2		1000M/F	FORWARDING	Disabled	7336	5345	1	0.608	0.0	0:33:13

Figure 4, (Switch B) **Advanced Application > Spanning Tree Protocol**



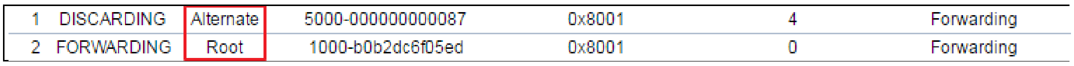
1	FORWARDING	Designated	5000-000000000087	0x8001	4	Forwarding
2	FORWARDING	Root	1000-b0b2dc6f05ed	0x8002	0	Forwarding

Management > Port Status



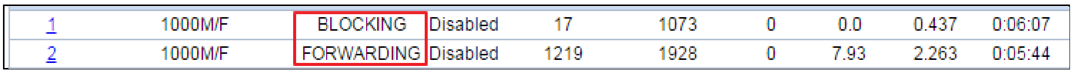
1	1000M/F	FORWARDING	Off	Disabled	9757	888	0	0.330	0.78	0:35:26
2	1000M/F	FORWARDING	Off	Disabled	5580	8574	0	4.246	1.17	0:35:12

Figure 5, (Switch C) **Advanced Application > Spanning Tree Protocol**



1	DISCARDING	Alternate	5000-000000000087	0x8001	4	Forwarding
2	FORWARDING	Root	1000-b0b2dc6f05ed	0x8001	0	Forwarding

Management > Port Status



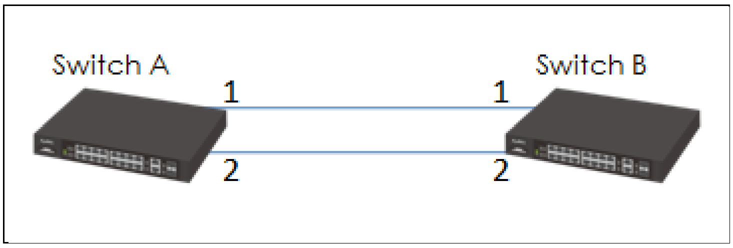
1	1000M/F	BLOCKING	Disabled	17	1073	0	0.0	0.437	0:06:07
2	1000M/F	FORWARDING	Disabled	1219	1928	0	7.93	2.263	0:05:44

4.1.2 How to configure MSTP on the switch?

Overview

Multiple spanning-tree (MSTP), allows frames assigned to different VLANs to follow separate paths & provides multiple forwarding paths for data traffic and enables load balancing.

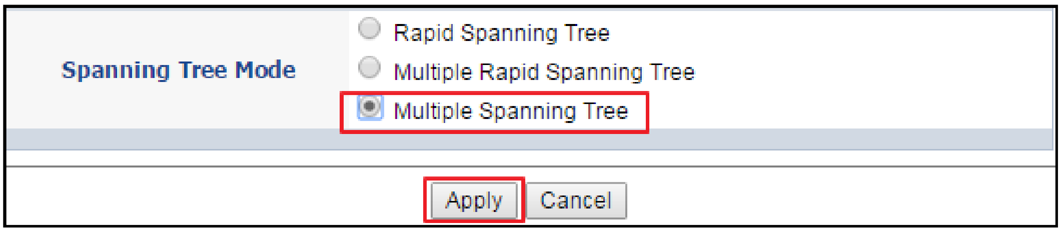
Topology:



Note: In the scenario both switches are configured with MSTP, configured with the same region & revision number. VLAN 1is mapped to instance 1. The port 1 is been configured to be the primary link & port 2 is the secondary link (blocked port).

1. Select **multiple spanning tree** then click **Apply** to save configuration.

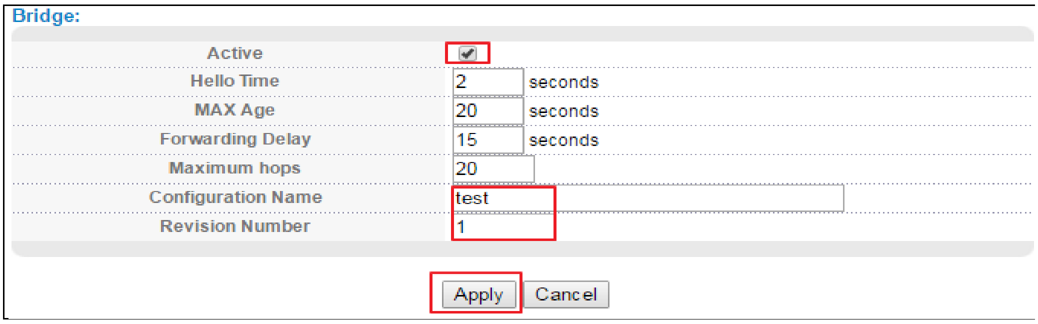
Figure 1 **Advanced Application > Spanning-Tree Protocol > Configuration**



Spanning Tree Mode: ○ Rapid Spanning Tree ○ Multiple Rapid Spanning Tree ● Multiple Spanning Tree

2. Check the **Active** box and click **Apply** to save the configuration & activate the feature. Switch in the same region should have the same **Configuration name & Revision number**. Please kindly use the **HELP** icon for more specific information.

Figure 2, **Advanced Application > Spanning-Tree Protocol > MSTP**

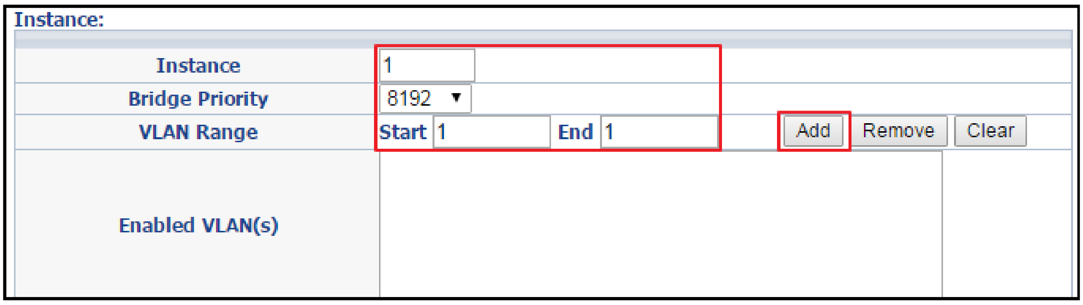


Bridge:

Active	☑
Hello Time	2 seconds
MAX Age	20 seconds
Forwarding Delay	15 seconds
Maximum hops	20
Configuration Name	test
Revision Number	1

3. In this screen is to configure MSTI use to identify this MST instance on the Switch (numbers 0-15). Set the priority of the Switch for the specific spanning tree instance, the lower priority will be the root bridge. VLAN range to configure which VLAN to be mapped in the MSTI.

Figure 3, **Advanced Application > Spanning-Tree Protocol > MSTP**

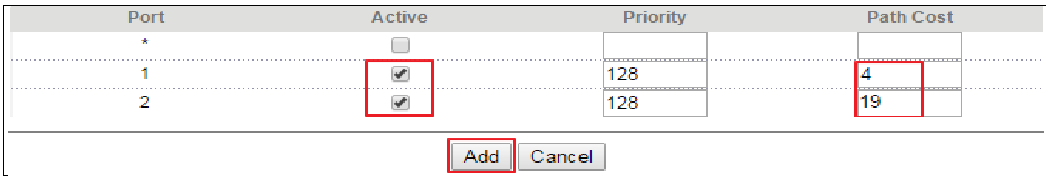


Instance:

Instance	1
Bridge Priority	8192
VLAN Range	Start 1 End 1
Enabled VLAN(s)	

4. select which port to be add in MSTI, configure the priority to decide which port should be disabled when one port or more forms a loop in a switch the higher the priority value will be disabled first. Path cost is the cost of transmitting. Click **Add** to save the configuration.

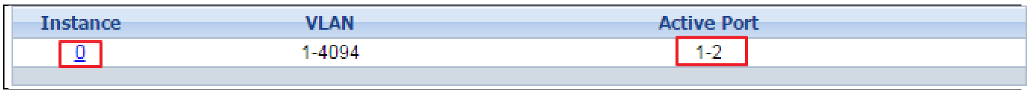
Figure 4, **Advanced Application > Spanning-Tree Protocol > MSTP**



Port	Active	Priority	Path Cost
*	□		
1	☑	128	4
2	☑	128	19

5. Click the **Instance 0** then configure which port should run STP features.

Figure 5, **Advanced Application > Spanning-Tree Protocol > MSTP**

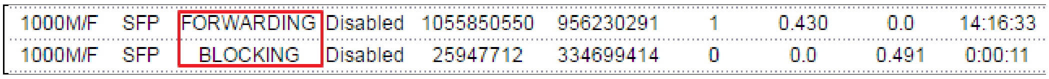


Instance	VLAN	Active Port
0	1-4094	1-2

Verify

1. Please click the **Status** icon on the upper right of the web page. It will display the MSTP port status of the switch.

Figure 6, **Status** (Quick Button)



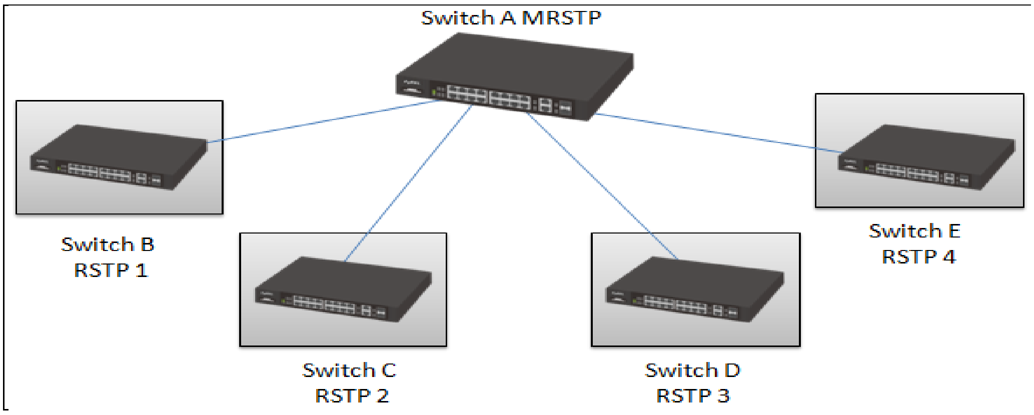
1000M/F	SFP	FORWARDING	Disabled	1055850550	956230291	1	0.430	0.0	14:16:33
1000M/F	SFP	BLOCKING	Disabled	25947712	334699414	0	0.0	0.491	0:00:11

4.1.3 How to configure MRSTP on the switch?

Overview

It's an extension to RSTP to provide multiple ring extensions in one switch. Each spanning tree operates independently with its own bridge information. Protect network for self-recovery when a link goes down

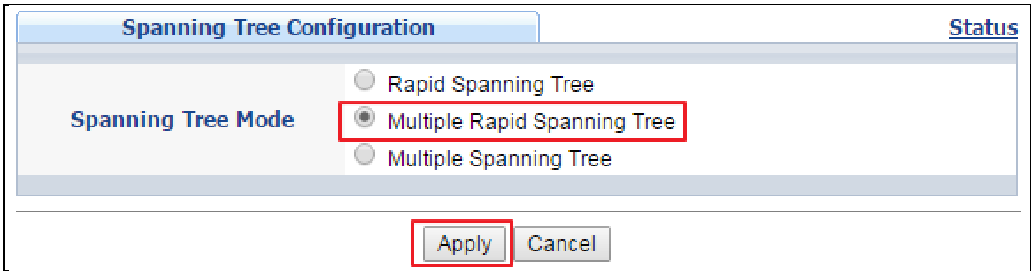
Topology:



Note: In the scenario, switch A is configured with MRSTP and connected with 4 different RTP divided & configured to tree 1,2,3,4.

1. Select multiple rapid spanning tree and click **Apply** to run MRSTP.

Figure 1, **Advanced Application > Spanning Tree Protocol > Configuration**

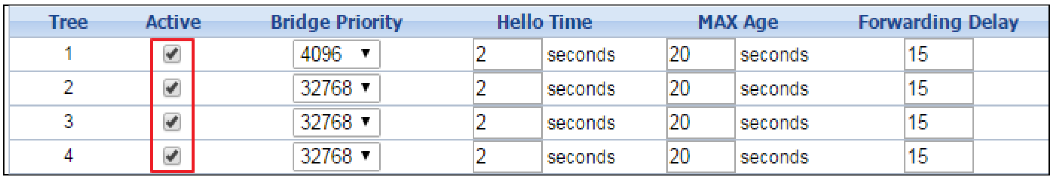

Spanning Tree Configuration

Status

Spanning Tree Mode
○ Rapid Spanning Tree
● Multiple Rapid Spanning Tree
○ Multiple Spanning Tree

2. The tree features are depend on the device and it's design, some of the device can only configured 2 tree. Select and check how many STP to be configured in MRSTP.

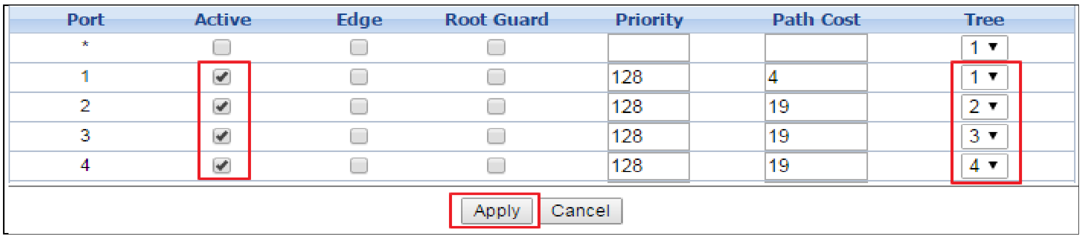
Figure 2,



Tree	Active	Bridge Priority	Hello Time	MAX Age	Forwarding Delay
1	☑	4096 ▾	2 seconds	20 seconds	15
2	☑	32768 ▾	2 seconds	20 seconds	15
3	☑	32768 ▾	2 seconds	20 seconds	15
4	☑	32768 ▾	2 seconds	20 seconds	15

3. Select and check which port to be configured and choose which STP **(Tree)** is it configured in Figure 2, then **Apply** to save the configuration.

Figure 3,

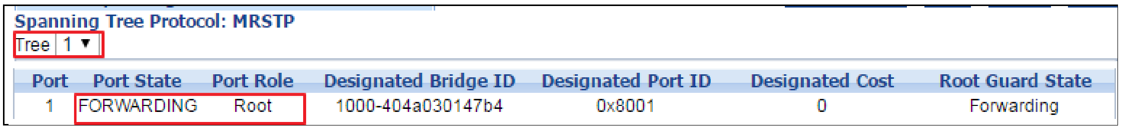


Port	Active	Edge	Root Guard	Priority	Path Cost	Tree
*	□	□	□			1 ▾
1	☑	□	□	128	4	1 ▾
2	☑	□	□	128	19	2 ▾
3	☑	□	□	128	19	3 ▾
4	☑	□	□	128	19	4 ▾

Verify

1. In this screen it will display the MRSTP status; user can change the **Tree** type to show each tree status.

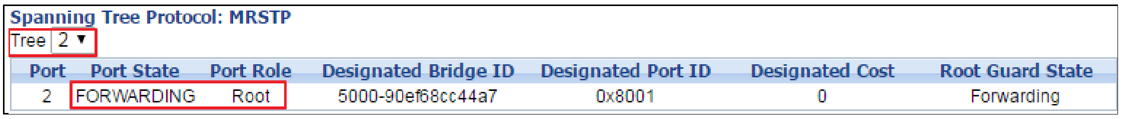
Figure 4, **Advanced Application > Spanning Tree Protocol**



Spanning Tree Protocol: MRSTP

Tree 1 ▼

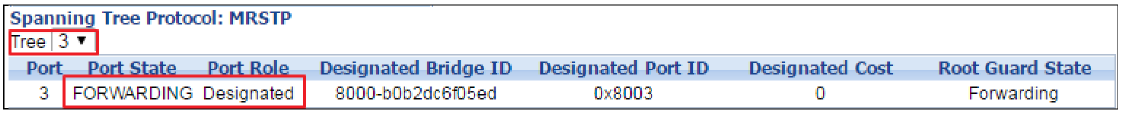
Port	Port State	Port Role	Designated Bridge ID	Designated Port ID	Designated Cost	Root Guard State
1	FORWARDING	Root	1000-404a030147b4	0x8001	0	Forwarding



Spanning Tree Protocol: MRSTP

Tree 2 ▼

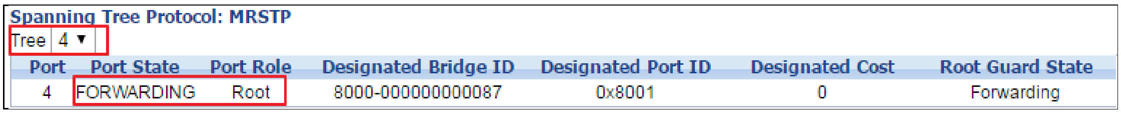
Port	Port State	Port Role	Designated Bridge ID	Designated Port ID	Designated Cost	Root Guard State
2	FORWARDING	Root	5000-90ef68cc44a7	0x8001	0	Forwarding



Spanning Tree Protocol: MRSTP

Tree 3 ▼

Port	Port State	Port Role	Designated Bridge ID	Designated Port ID	Designated Cost	Root Guard State
3	FORWARDING	Designated	8000-b0b2dc6f05ed	0x8003	0	Forwarding



Spanning Tree Protocol: MRSTP

Tree 4 ▼

Port	Port State	Port Role	Designated Bridge ID	Designated Port ID	Designated Cost	Root Guard State
4	FORWARDING	Root	8000-000000000087	0x8001	0	Forwarding

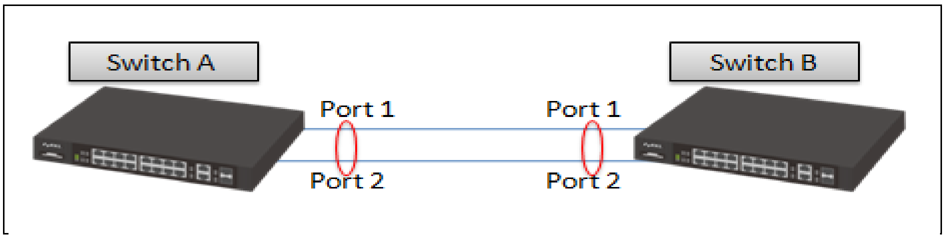
4.2 Link Aggregation

Overview

Link aggregation a feature to aggregate one or more Ethernet interfaces to form a logical point-to-point link, known as a LAG, virtual link, or bundle, provides degradation if failure occurs and increase availability. It provides network redundancy by load-balancing traffic across all available links. If one of the links fails, the system automatically load-balances traffic across all remaining links.

Link Aggregation topology,

Figure 1,



Note: Switch A port 1 & 2 are bundled to from a link aggregation same as switch B port 1 & 2 are configured with link aggregation also.

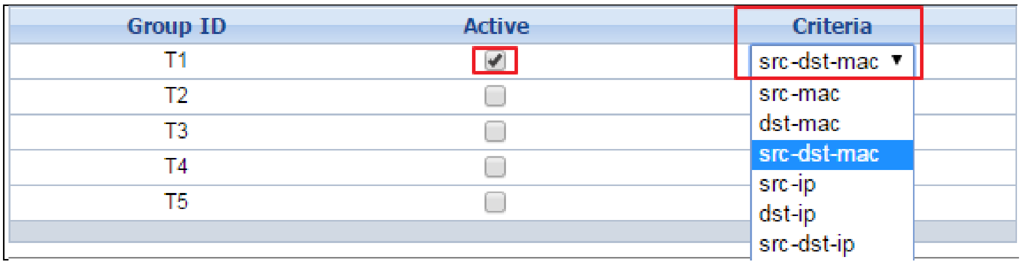
4.2.1 How to configure Static Trunk on the switch?

Overview

Static trunks are groups of two to eight ports that act as single virtual links. Static trunks are commonly used to improve network performance by increasing the available bandwidth between the switch and other network devices as well as to enhance the reliability of the connections between network devices.

1. In this screen activate trunk group **T1**, select the traffic distribution algorithm used by this group and select the ports that should belong to this group as shown in the figure below. Click **Apply** when you are done.

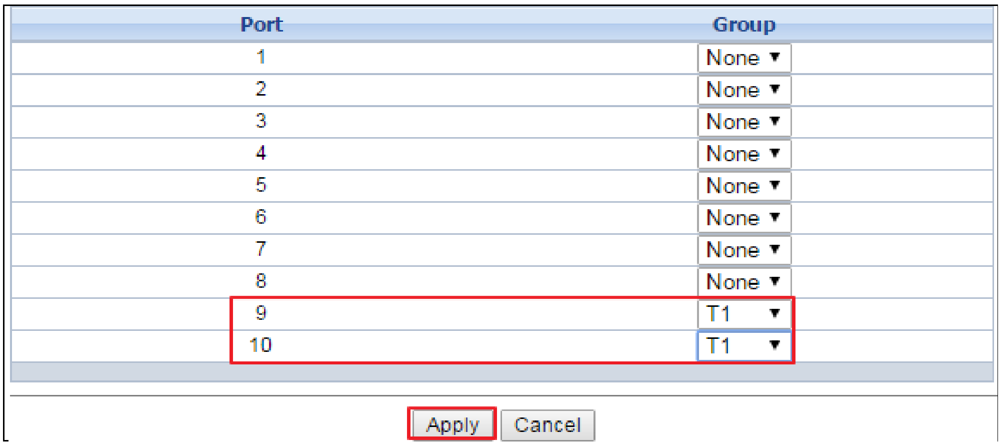
Figure 2, **Advanced Application > Link Aggregation > Link Aggregation Setting**



Group ID	Active	Criteria
T1	☑	src-dst-mac ▼
T2	☐	
T3	☐	
T4	☐	
T5	☐	

2. Select which port to be bundle then choose the right **Group ID** that configured in **step 1.**

Figure 3, **Advanced Application > Link Aggregation > Link Aggregation Setting**

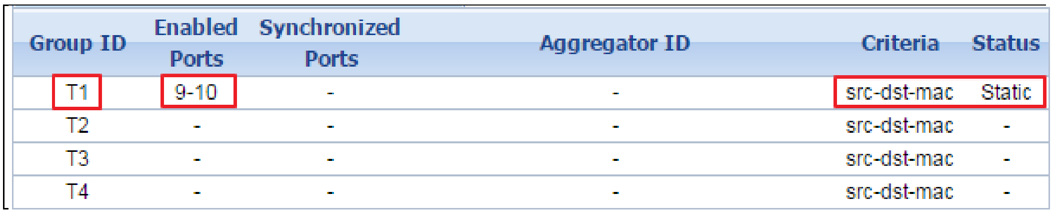


Port	Group
1	None ▾
2	None ▾
3	None ▾
4	None ▾
5	None ▾
6	None ▾
7	None ▾
8	None ▾
9	T1 ▾
10	T1 ▾

Verify

1. In this screen you can confirm the **Link Aggregation (static trunk)** configuration.

Figure 4, **Advanced Application > Link Aggregation**



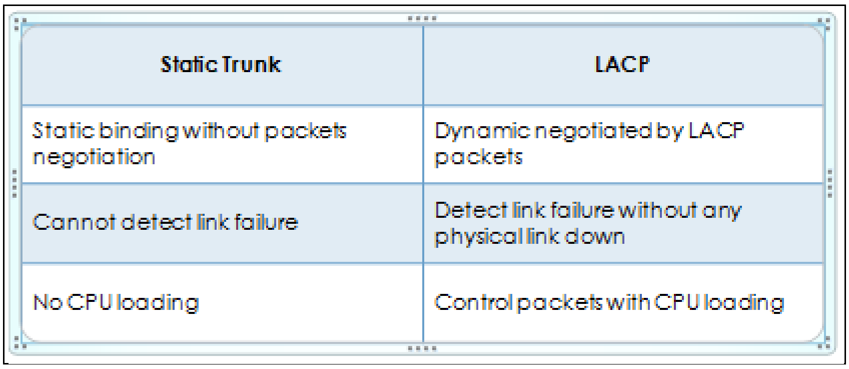
Group ID	Enabled Ports	Synchronized Ports	Aggregator ID	Criteria	Status
T1	9-10	-	-	src-dst-mac	Static
T2	-	-	-	src-dst-mac	-
T3	-	-	-	src-dst-mac	-
T4	-	-	-	src-dst-mac	-

4.2.2 How to configure LACP on the switch?

Overview

Link Aggregation Control Protocol (LACP) is part of an IEEE specification (802.3ad) that allows you to bundle several physical ports together to form a single logical channel. LACP allows a switch to load sharing & can detect failure even if not directly connect, or remove the link from the group

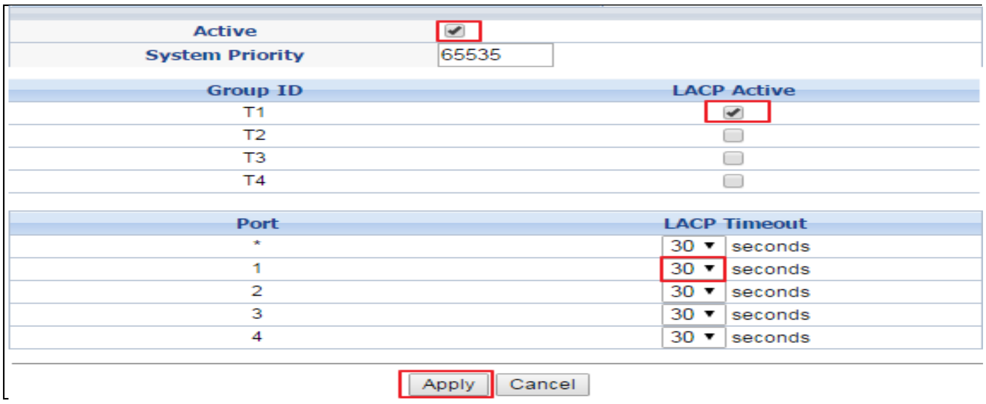
Figure 1, Difference between **static Trunk & LACP.**



Static Trunk	LACP
Static binding without packets negotiation	Dynamic negotiated by LACP packets
Cannot detect link failure	Detect link failure without any physical link down
No CPU loading	Control packets with CPU loading

1. Check **Active Box** to run LACP then choose & check the **Group ID** that been configured. **LACP Timeout** is the time interval between the individual port exchanges of LACP packets in order to check that the peer port in the trunk group is still up. Please use the **HELP** button for more information.

Figure 2, **Advanced Application > Link Aggregation > Link Aggregation Setting > LACP**



Active	☑
System Priority	65535

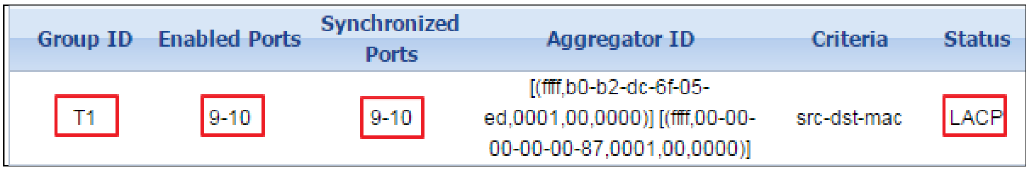
Group ID	LACP Active
T1	☑
T2	□
T3	□
T4	□

Port	LACP Timeout
*	30 seconds
1	30 seconds
2	30 seconds
3	30 seconds
4	30 seconds

Verify

1. In this screen user can check the **LACP** settings.

Figure 3, **Advanced Application > Link Aggregation**



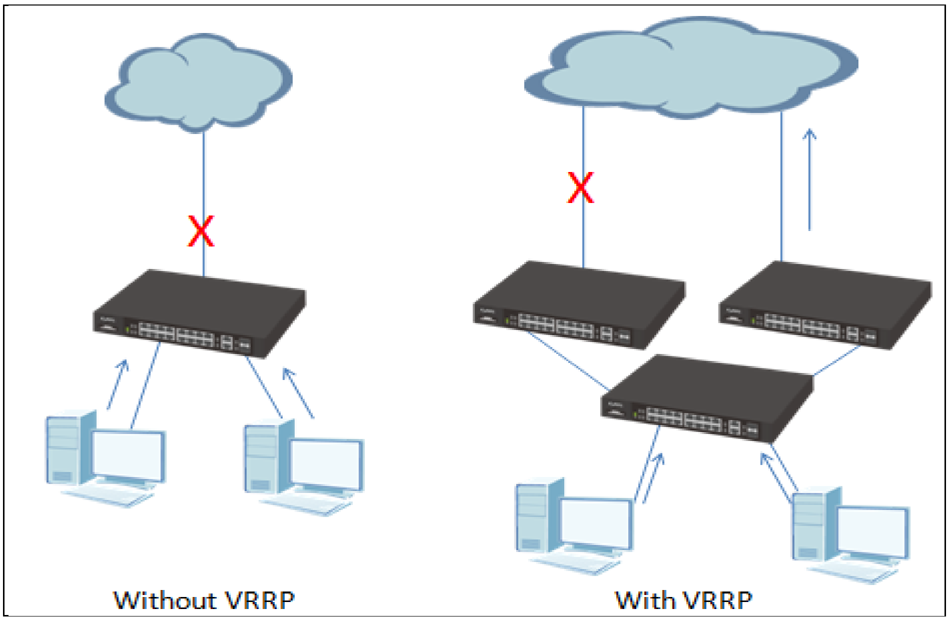
Group ID	Enabled Ports	Synchronized Ports	Aggregator ID	Criteria	Status
T1	9-10	9-10	[(ffff,b0-b2-dc-6f-05-ed,0001,00,0000)] [(ffff,00-00-00-00-00-87,0001,00,0000)]	src-dst-mac	LACP

4.3 VRRP (Layer 3)

Overview

Traditional network has one and only one gateway to put between internal network and external network. When the link of router has some trouble, the user can't access to internet anymore. But when we enable VRRP, if MASTER router fails, and the BACKUP router will take over, and ensure the traffic still go through.

VRRP topology,

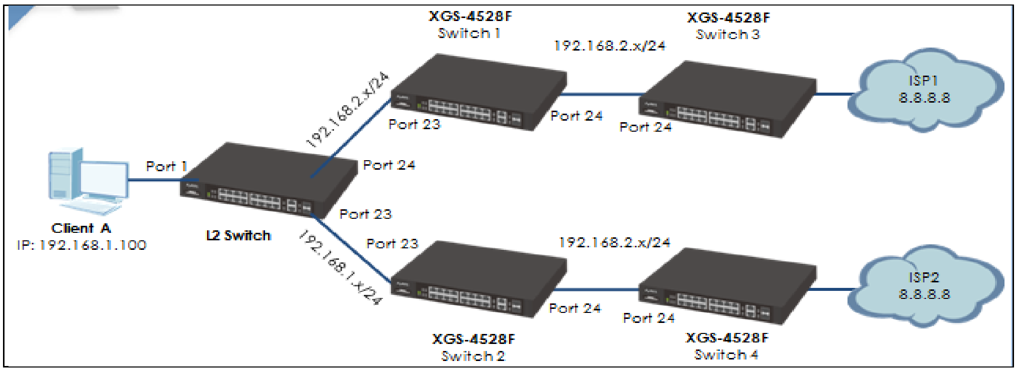


4.3.1 How to set VRRP on the switch?

Overview

Each host in a network is configured to send packets to a statically configured default gateway. The default gateway can become a single point of failure. Virtual Router Redundancy Protocol (VRRP), defined in RFC 2338, allows you to create redundant backup gateways to ensure that the default gateway of a host is always available.

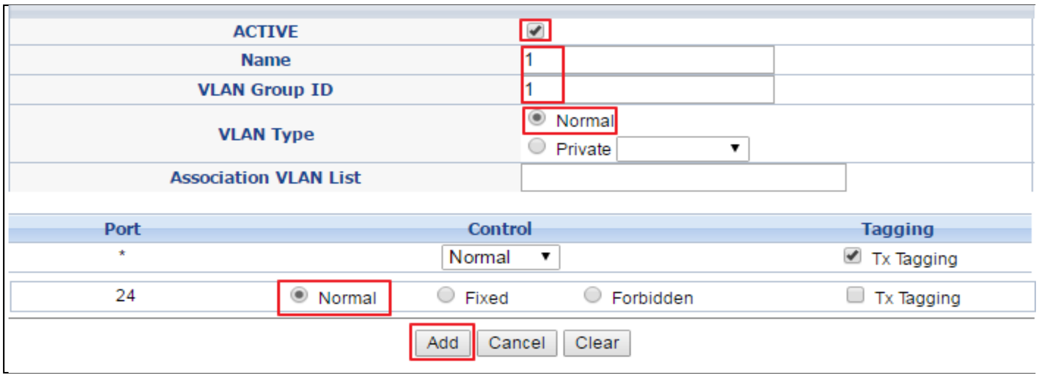
VRRP Topology,



Note: Both switches are configured with VRRP features, switch 1is set to be the master & switch 2is the backup. So that is switch A is down, switch 2(backup) will take over the master, there will be no traffic issue happen.

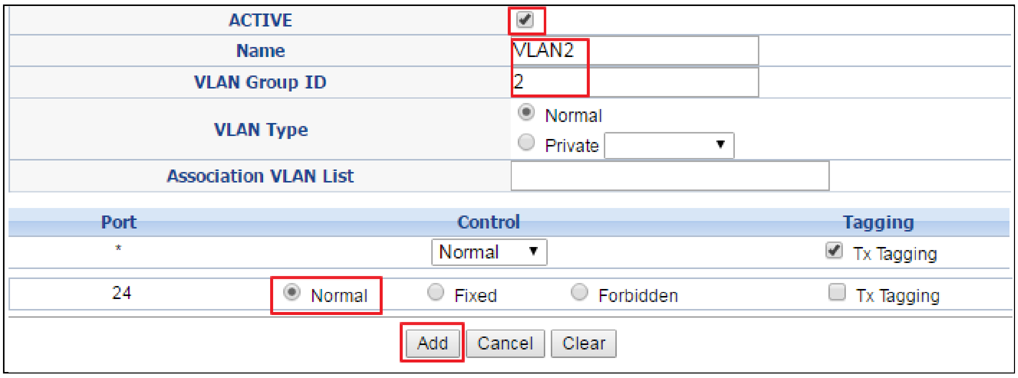
1. On switch 1 & 2, configures VLAN 1 & 2.

Figure1, **Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup**



ACTIVE	☑
Name	1
VLAN Group ID	1
VLAN Type	● Normal ○ Private ▼
Association VLAN List	

Port	Control			Tagging
*	Normal ▼			☑ Tx Tagging
24	● Normal	○ Fixed	○ Forbidden	□ Tx Tagging

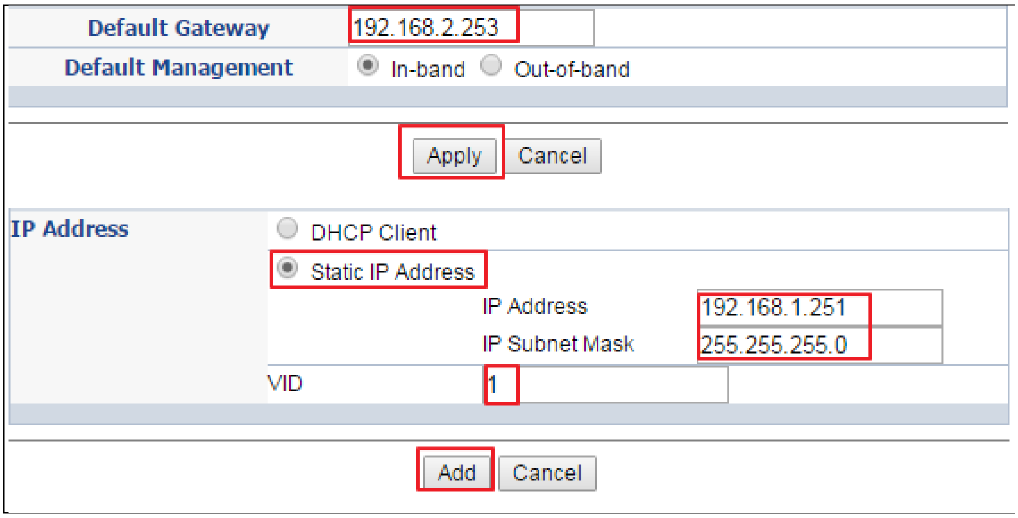


ACTIVE	☑
Name	VLAN2
VLAN Group ID	2
VLAN Type	● Normal ○ Private ▾
Association VLAN List	

Port	Control			Tagging
*	Normal ▾			☑ Tx Tagging
24	● Normal	○ Fixed	○ Forbidden	□ Tx Tagging

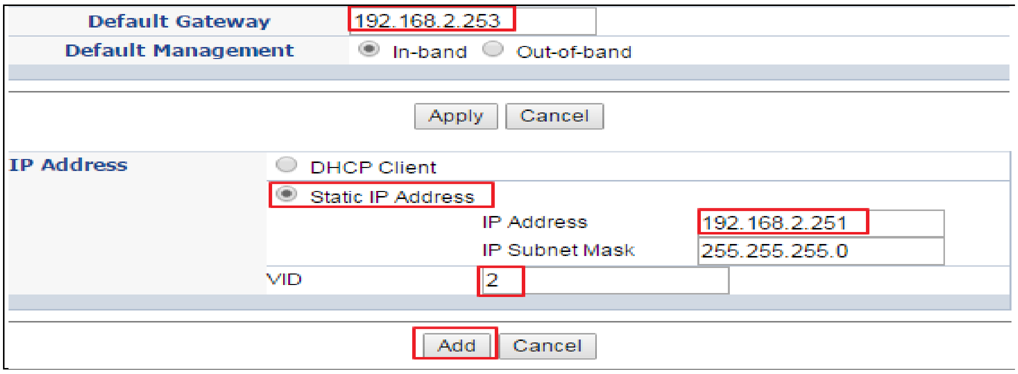
2. Configure IP interface & set default gateway for VLAN 1 & 2.

Figure 2, **Basic Setting > IP Setup >IP Configuration**



Default Gateway	192.168.2.253
Default Management	● In-band ○ Out-of-band

IP Address	○ DHCP Client	
	● Static IP Address	
	IP Address	192.168.1.251
	IP Subnet Mask	255.255.255.0
	VID	1

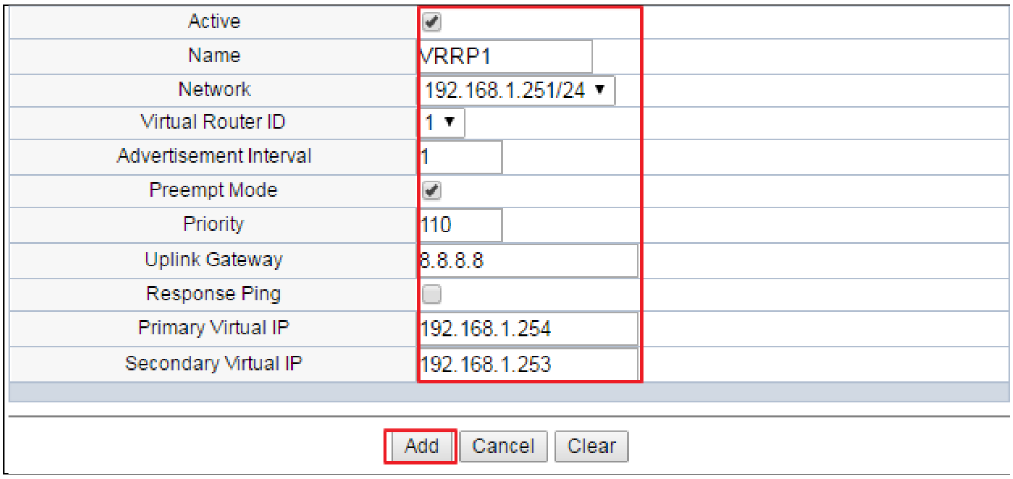


Default Gateway	192.168.2.253
Default Management	● In-band ○ Out-of-band

IP Address	○ DHCP Client	
	● Static IP Address	
	IP Address	192.168.2.251
	IP Subnet Mask	255.255.255.0
	VID	2

3. In this screen the highlight part is to configure & activate VRRP. Be sure to check **Active** to run VRRP features and **Preempt Mode** to let the switch choose the master. The **Virtual Router ID, Primary & Secondary Virtual IP** should have the same configure with the master & backup switch. For more specific information, please kindly use **HELP** icon.

Figure 3, **IP Application > VRRP > Configuration**

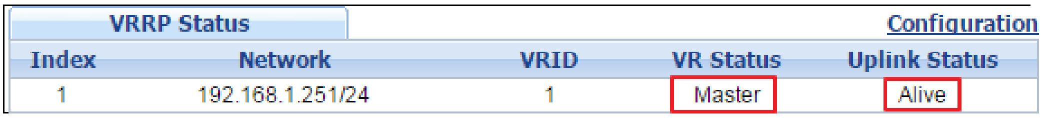


Active	☑
Name	VRRP1
Network	192.168.1.251/24 ▼
Virtual Router ID	1 ▼
Advertisement Interval	1
Preempt Mode	☑
Priority	110
Uplink Gateway	8.8.8.8
Response Ping	☐
Primary Virtual IP	192.168.1.254
Secondary Virtual IP	192.168.1.253

Verify

1. In this screen will display the VRRP status and will show the master switch.

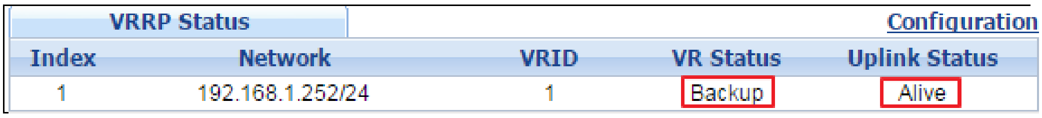
Figure 4, **Switch 1, IP Application > VRRP**



Index	Network	VRID	VR Status	Uplink Status
1	192.168.1.251/24	1	Master	Alive

2. In this screen will display the VRRP status and will show the backup switch.

Figure 5, **Switch 2, IP Application > VRRP**



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

5.1 IGMP Routing

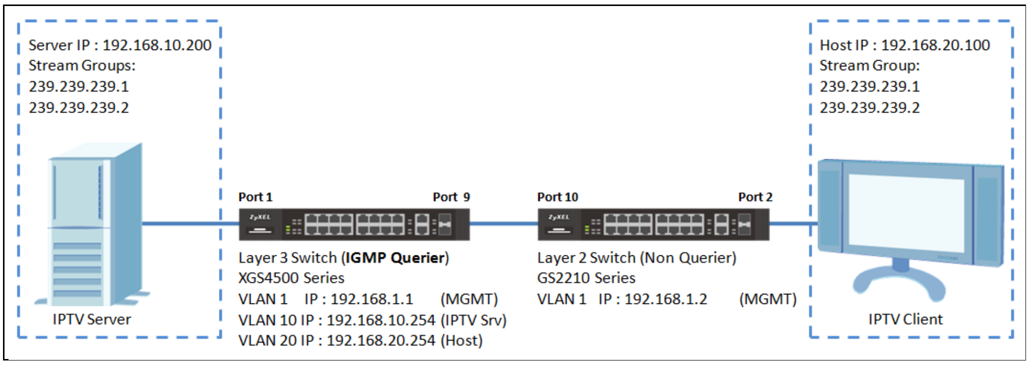
Overview

Use for routing multicast data within autonomous system, provides multicast forwarding capability to a layer 3 switch.

5.1.1 How to setup IPTV Layer3 environment?

The network administrator want to separator the stream server and host in difference VLANs to avoid the other packets to affect the stream quality. The example instructs how to implement the IPTV service on Layer 3 topology.

Figure, IPTV service on Layer3 environment.

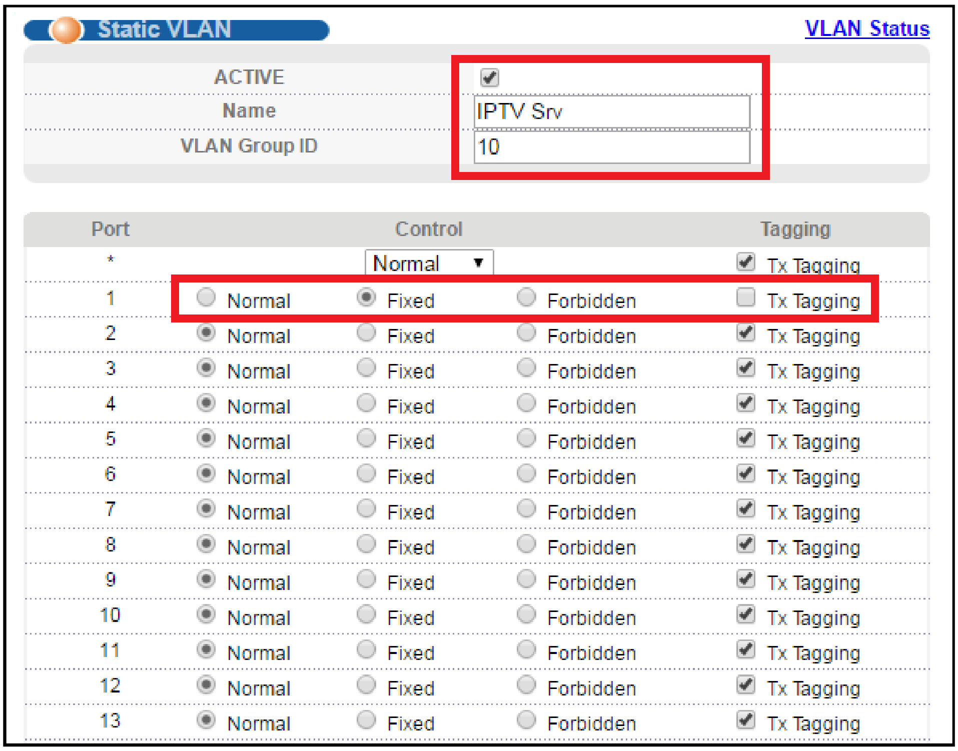

Server IP : 192.168.10.200
Stream Groups:
239.239.239.1
239.239.239.2
IPTV Server
Port 1
Port 9
Layer 3 Switch (IGMP Querier)
XGS4500 Series
VLAN 1 IP : 192.168.1.1 (MGMT)
VLAN 10 IP : 192.168.10.254 (IPTV Srv)
VLAN 20 IP : 192.168.20.254 (Host)
Port 10
Port 2
Layer 2 Switch (Non Querier)
GS2210 Series
VLAN 1 IP : 192.168.1.2 (MGMT)
Host IP : 192.168.20.100
Stream Group:
239.239.239.1
239.239.239.2
IPTV Client

Note: All network IP address and subnet masks are used as examples in this article.

Please replace them with your actual network IP address and subnet masks. This example was tested using XGS-4528F and GS2210-8

1. In the XGS-4528F, go to **Advanced Application > VLAN > Static VLAN**, to create VLAN 10 for IPTV Server and VLAN 20 for host. **Active** the VLAN 10 and type the **Name** and **VLAN Group ID** then select the **Fixed** and remove **TX Tagging** on Port 1. Click **Add**.

Figure 2 **Advanced Application > VLAN > Static VLAN**



Static VLAN

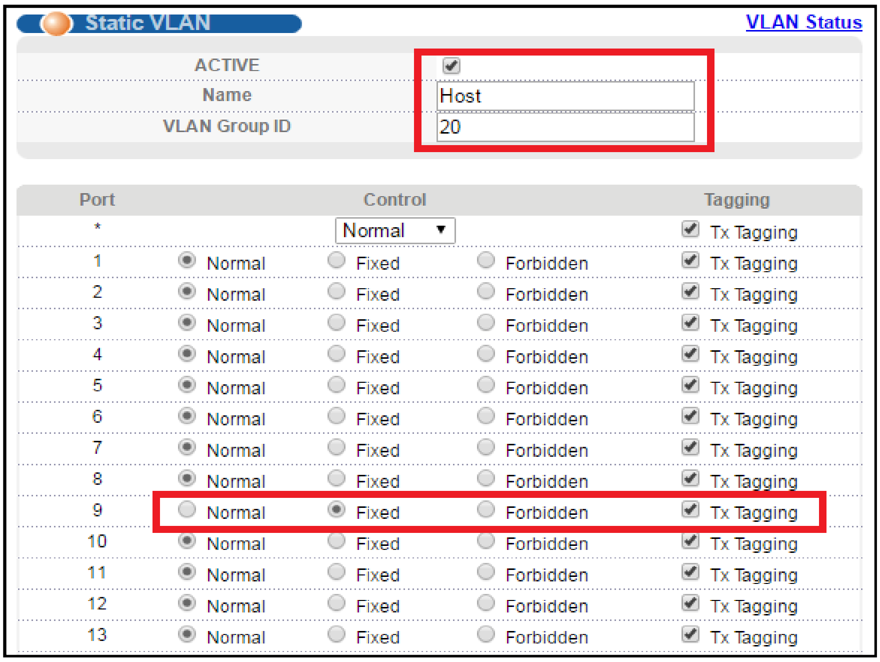
VLAN Status

ACTIVE	☑
Name	IPTV Srv
VLAN Group ID	10

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
6	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
7	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
8	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
9	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
10	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
11	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
12	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
13	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging

2. **Active** the VLAN 20 and type the **Name** and **VLAN Group ID** then select the **Fixed** on Port 9.Click **Add**.

Figure 3 **Advanced Application > VLAN > Static VLAN**



Static VLAN

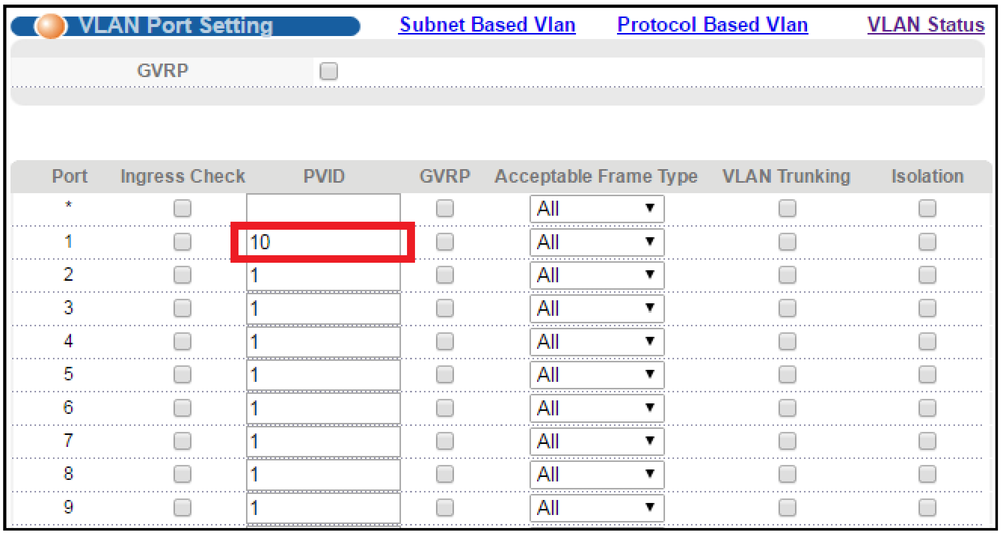
VLAN Status

ACTIVE	☑
Name	Host
VLAN Group ID	20

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
6	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
7	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
8	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
9	○ Normal	● Fixed	○ Forbidden	☑ Tx Tagging
10	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
11	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
12	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
13	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging

3. Go to **Advanced Application > VLAN > VLAN Port Setting**, to configure PVID 10 for Port 1. Click **Apply**.

Figure 4 **Advanced Application > VLAN > VLAN Port Setting**



VLAN Port Setting

Subnet Based Vlan

Protocol Based Vlan

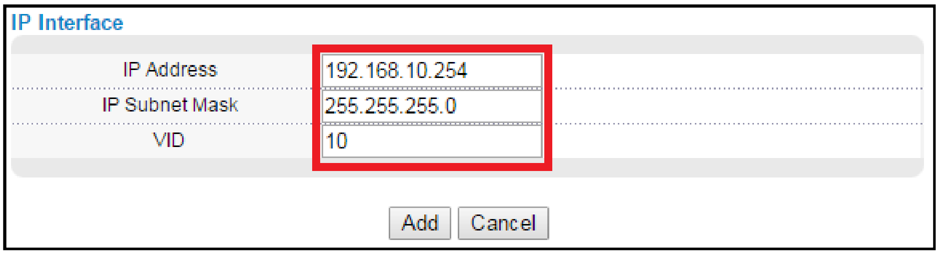
VLAN Status

GVRP □

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

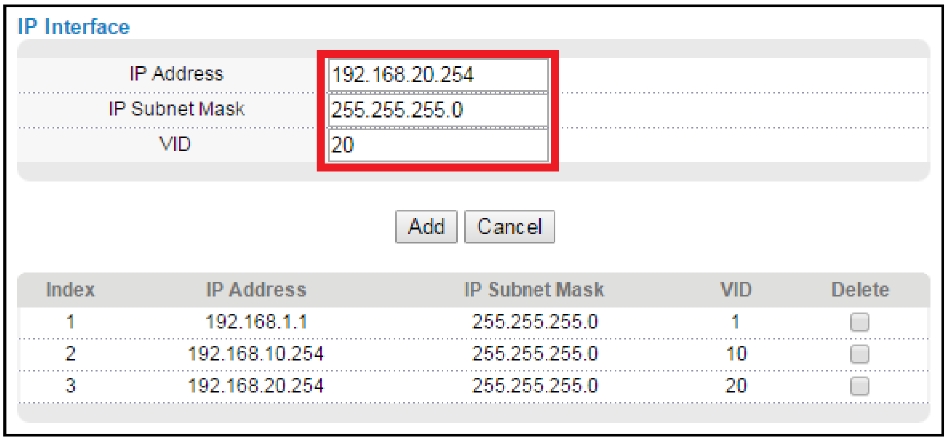
4. Go to **Basic Setting > IP Setup > IP Interface**, to create ip address for VLAN 10and VLAN 20.Click **Add**.

Figure 5 **Basic Setting > IP Setup > IP Interface**



IP Interface

IP Address	192.168.10.254
IP Subnet Mask	255.255.255.0
VID	10



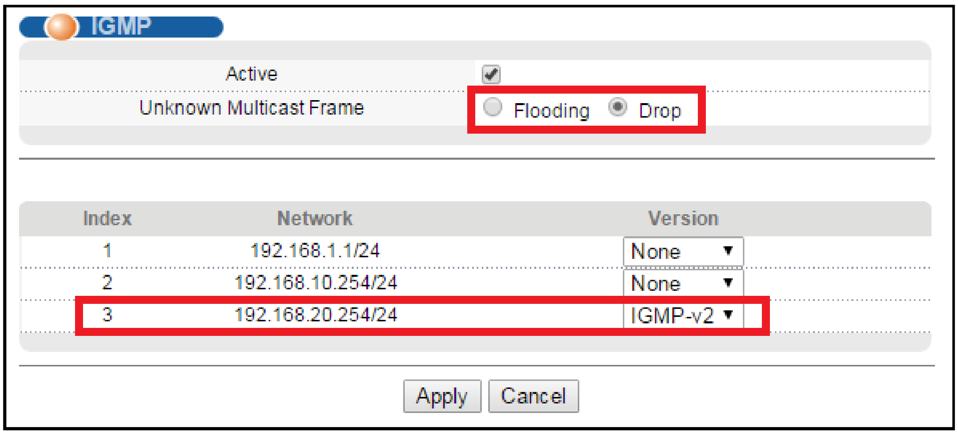
IP Interface

IP Address	192.168.20.254
IP Subnet Mask	255.255.255.0
VID	20

Index	IP Address	IP Subnet Mask	VID	Delete
1	192.168.1.1	255.255.255.0	1	□
2	192.168.10.254	255.255.255.0	10	□
3	192.168.20.254	255.255.255.0	20	□

5. Go to **IP Application > IGMP**, active the IGMP router and select the **Drop** for unknown Multicast Frame and enable the IGMP-v2 for VLAN 20 interface. **Unknown Multicast Frame Drop** is able to discard IGMP packets flooding to all ports. Switch will send the General-Query when user enables IGMP-Version on VLAN interface. Click **Apply**.

Figure 6 **IP Application > IGMP**



IGMP

Active ☑

Unknown Multicast Frame ○ Flooding ● Drop

Index	Network	Version
1	192.168.1.1/24	None
2	192.168.10.254/24	None
3	192.168.20.254/24	IGMP-v2

5.2 IGMP Snooping

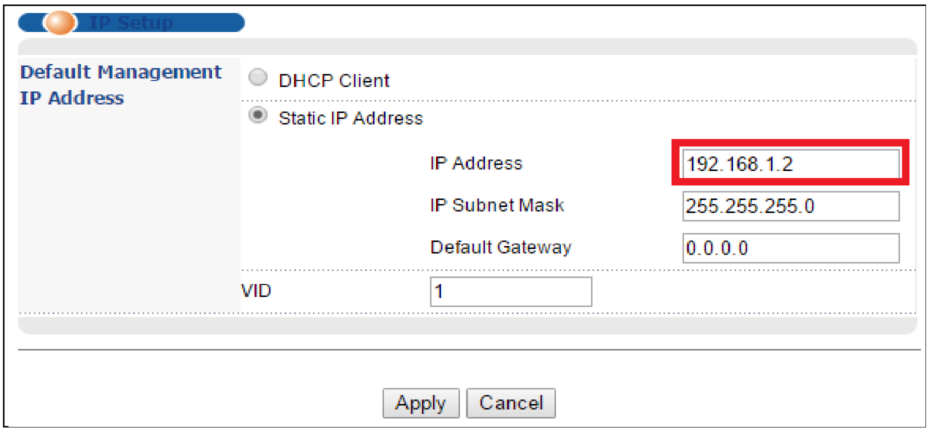
Overview

The switch can passively snoop on the IGMP packets transferred between IP multicast routers/switches and IP multicast host to learn the IP multicast group membership. It checks IGMP packets passing through it, picks out the group registration information, and configures multicasting accordingly. IGMP snooping allows the switch to learn multicast groups without you having to manually configure them.

5.2.1 How to setup IPTV Layer3 environment?

1. Go to Basic Setting > IP Setup, to change the management IP to192.168.1.2.Click Apply.

Figure 1, **Basic Setting > IP Setup**



IP Setup

Default Management IP Address

○ DHCP Client

● Static IP Address

IP Address: 192.168.1.2

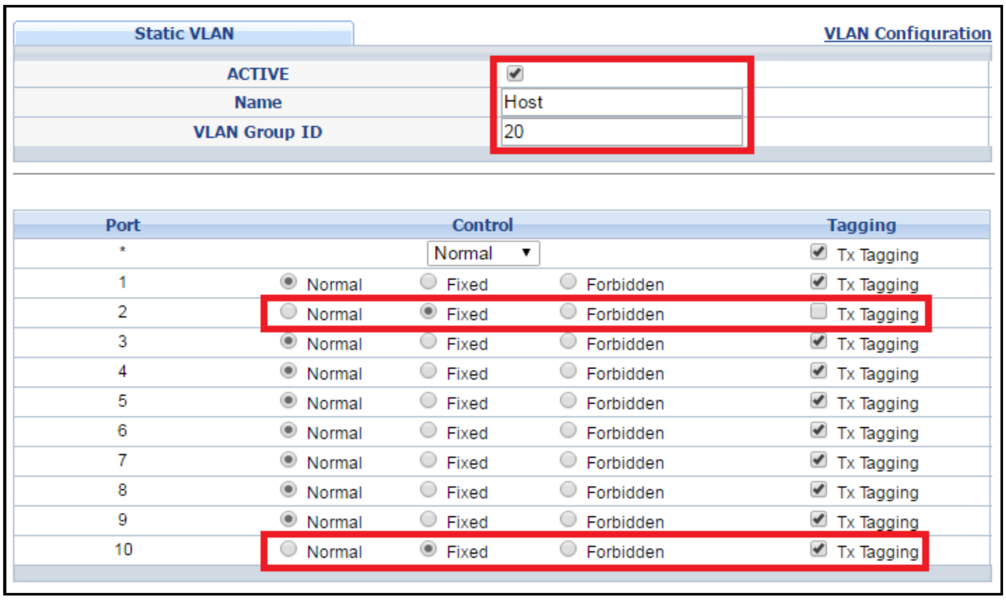
IP Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

VID: 1

2. Go to Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup, to create VLAN 20 for Host. Active the VLAN 20 and type the Name and VLAN Group ID then select the Fixed on Port 2 and Port 10 and remove TX Tagging on Port 2.Click Add.

Figure 2, **Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup**



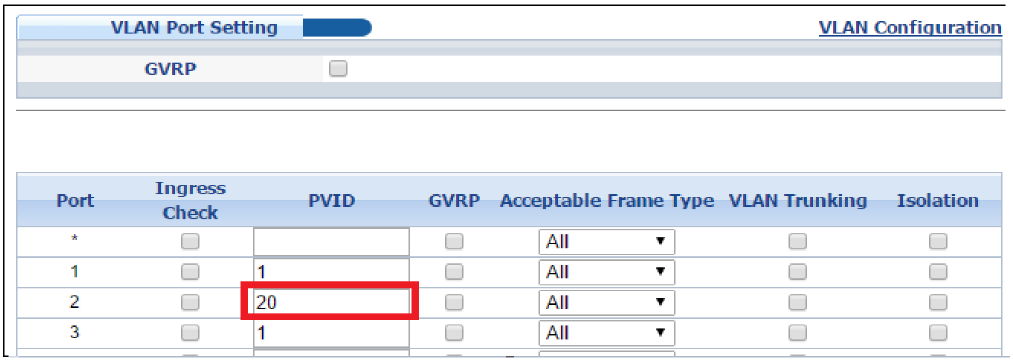
Static VLAN | VLAN Configuration

ACTIVE	☑
Name	Host
VLAN Group ID	20

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
6	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
7	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
8	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
9	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
10	○ Normal	● Fixed	○ Forbidden	☑ Tx Tagging

3. Go to Advanced Application > VLAN > VLAN Configuration> VLAN Port Setup, to configure PVID 20 for Port 2. Click Apply.

Figure 3, **Advanced Application > VLAN > VLAN Configuration> VLAN Port Setup**



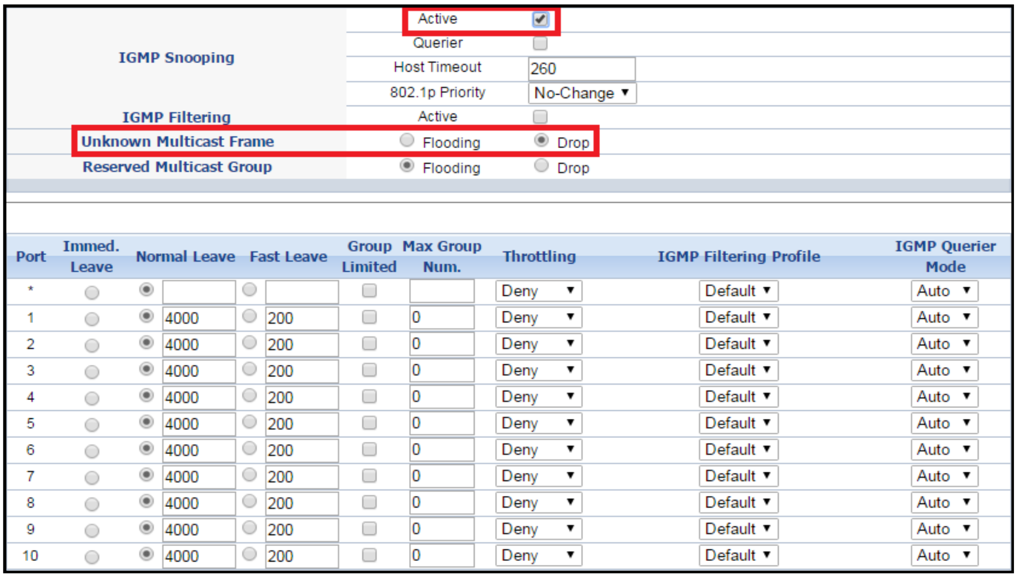
VLAN Port Setting | VLAN Configuration

GVRP □

Port	Ingress Check	PVID	GVRP	Acceptable Frame Type	VLAN Trunking	Isolation
*	□		□	All ▾	□	□
1	□	1	□	All ▾	□	□
2	□	20	□	All ▾	□	□
3	□	1	□	All ▾	□	□

4. Go to Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping, to set up IGMP-Snooping. Active the IGMP Snooping and choose the Unknown Multicast Frame to Drop. Click Apply.

Figure 4, **Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping**



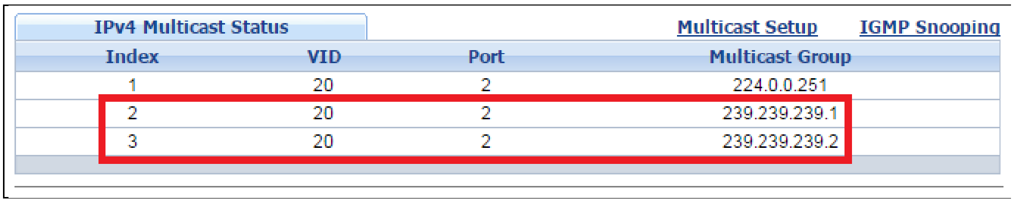
IGMP Snooping	Active	☑
	Querier	□
	Host Timeout	260
	802.1p Priority	No-Change ▾
IGMP Filtering	Active	□
Unknown Multicast Frame	○ Flooding	● Drop
Reserved Multicast Group	● Flooding	○ Drop

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 ▾	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 ▾

Verify

1. Client use VLC to send the IGMP-Join to group 239.239.239.1 or 239.239.239.2. Go to **Advanced Application > Multicast > IPv4 Multicast**, the group entry has recorded on IGMP-Snooping table.

Figure 5, **Advanced Application > Multicast > IPv4 Multicast**



Index	VID	Port	Multicast Group
1	20	2	224.0.0.251
2	20	2	239.239.239.1
3	20	2	239.239.239.2

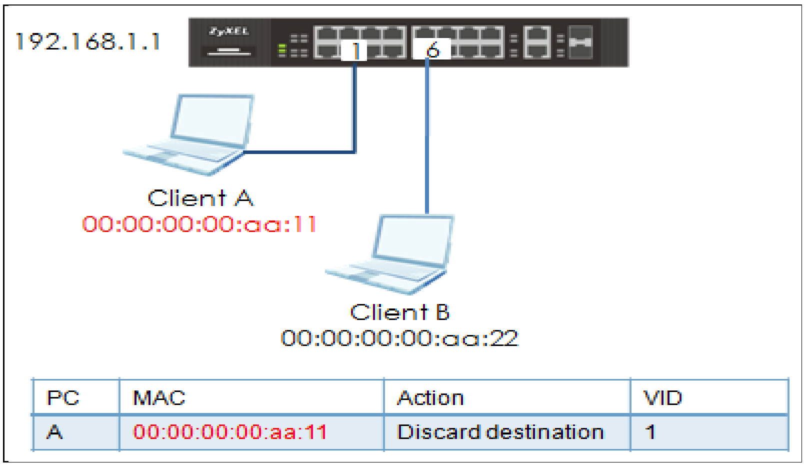
How to protect network?

6.1 MAC Filter

Overview

Filtering means sifting traffic going through the Switch based on the source and/or destination MAC addresses and VLAN group (ID).

Scenario,



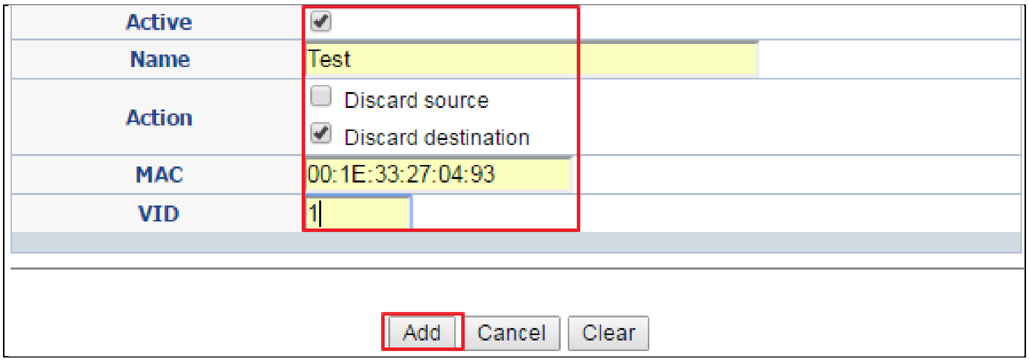
PC	MAC	Action	VID
A	00:00:00:00:aa:11	Discard destination	1

Note, in this scenario Client A has been configured witch MAC filtering an action of discard destination, it means that it drop the frames to the destination MAC address (specified in the **MAC** address). The Switch can still receive frames originating from the MAC address.

6.1.1 How to set MAC filter?

1. Check the **Active** box to activate filtering, select which action to be run. Input the specific MAC address of the device want to be configured and key in which VLAN ID then **Add** to save configuration.

Figure 1, **Advanced Application > Filtering**

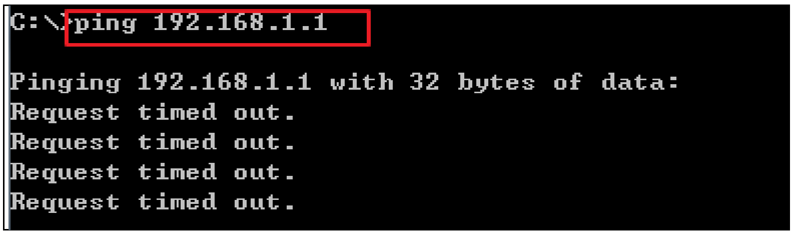


Active	☑
Name	Test
Action	□ Discard source ☑ Discard destination
MAC	00:1E:33:27:04:93
VID	1

Verify

1. Based on the scenario, client A should not be able to ping the switch (192.168.1.1) because the switch drops all frames to the destination MAC address..

Figure 2, **Windows Command Processor (CMD)**



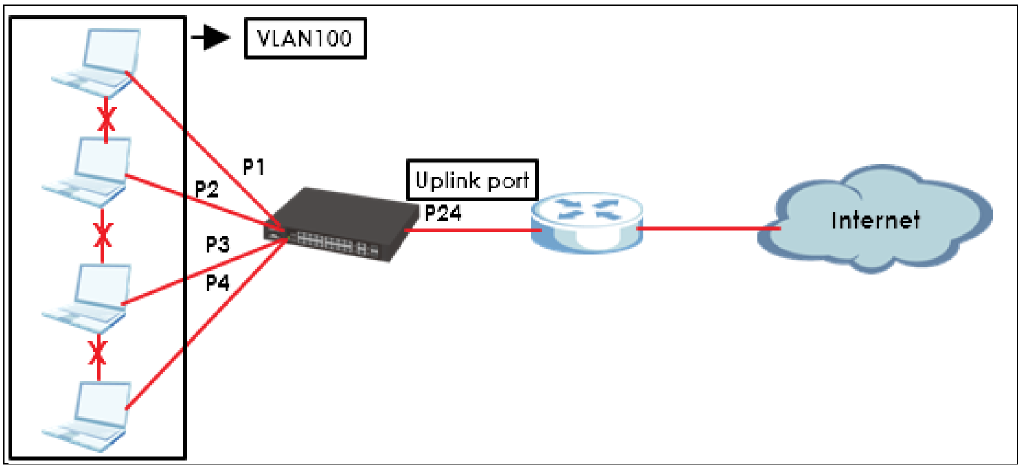
```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

6.2 Layer 2 isolation

Overview

This feature is to Block traffic communication between ports in the same VLAN, but it can communicate with the uplink port to access the internet.

Topology,

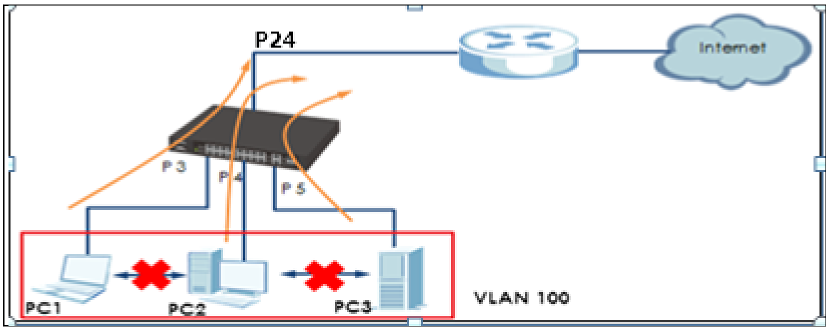


Note: Block all traffics within the same VLAN, but it can communicate with uplink port (port 24)

.

6.2.1 How to setup L2 isolation?

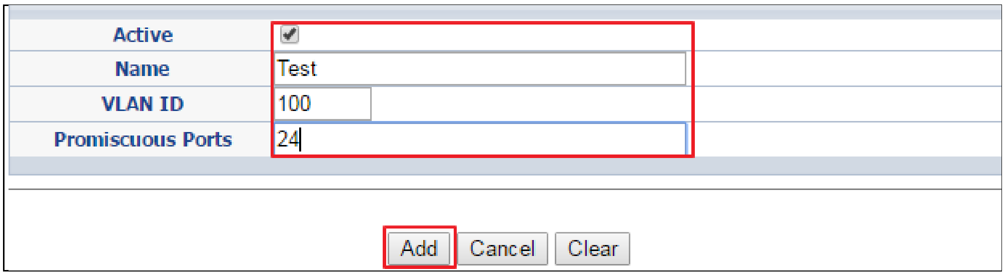
Topology,



Note, all in the same VLAN can't communicate with each other, but can communicate with uplink port.

1. In this screen, check **Active** to run features and specify which VLAN ID and input the uplink port then **add** to save configuration.

Figure 1, **Advanced Application > Private VLAN**

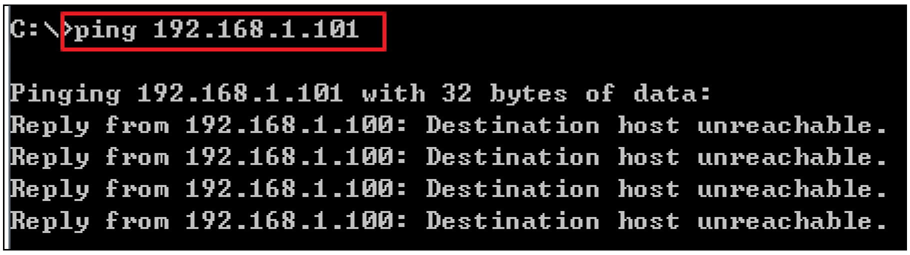


Active	☑
Name	Test
VLAN ID	100
Promiscuous Ports	24

Verify

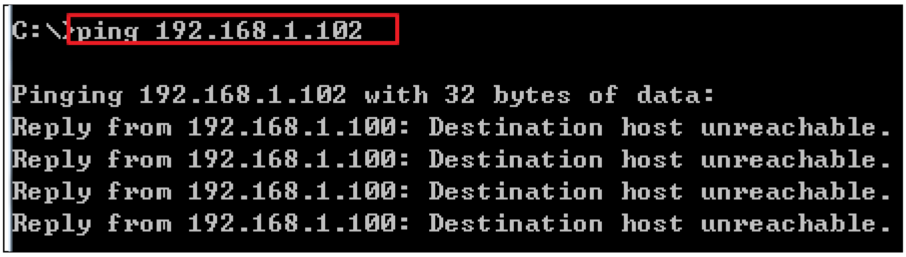
1. According to the scenario, VLAN 100 PC1, PC2 & PC3 can't communicate with each other, but they can communicate with Port 24 (uplink port) to access the internet.

PC1 can't ping PC2



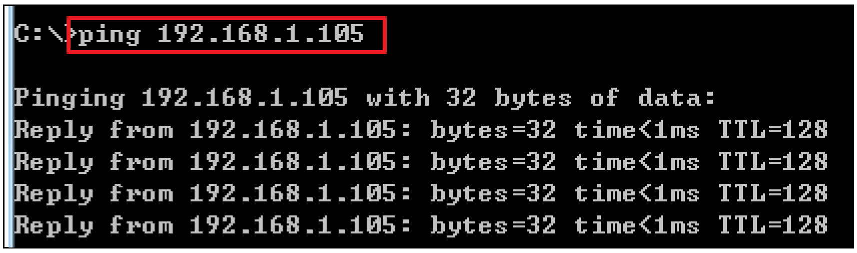
```
C:\>ping 192.168.1.101

Pinging 192.168.1.101 with 32 bytes of data:
Reply from 192.168.1.100: Destination host unreachable.
Reply from 192.168.1.100: Destination host unreachable.
Reply from 192.168.1.100: Destination host unreachable.
Reply from 192.168.1.100: Destination host unreachable.
```

PC1 can't ping PC3



```
C:\>ping 192.168.1.102

Pinging 192.168.1.102 with 32 bytes of data:
Reply from 192.168.1.100: Destination host unreachable.
Reply from 192.168.1.100: Destination host unreachable.
Reply from 192.168.1.100: Destination host unreachable.
Reply from 192.168.1.100: Destination host unreachable.
```

PC1 can ping uplink port 24.



```
C:\>ping 192.168.1.105

Pinging 192.168.1.105 with 32 bytes of data:
Reply from 192.168.1.105: bytes=32 time<1ms TTL=128
Reply from 192.168.1.105: bytes=32 time<1ms TTL=128
Reply from 192.168.1.105: bytes=32 time<1ms TTL=128
Reply from 192.168.1.105: bytes=32 time<1ms TTL=128
```

7.1 802.1x Authentication

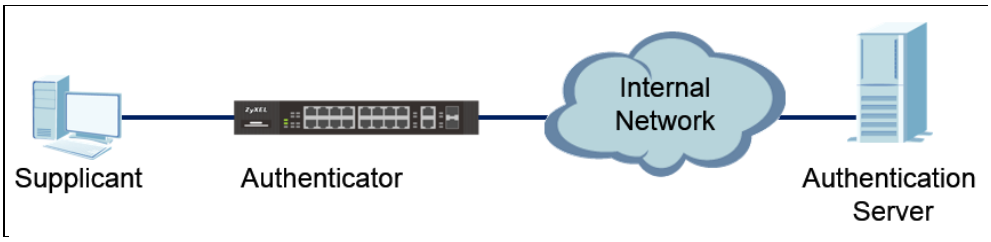
Overview

802.1 x authentications is a common security application which requires hosts to enter a username and password in order to be authenticated by an authentication server. The Zyxelenterprise switch models support 802.1x Port Authentication that forces hosts to submit valid user credentials before their traffic can be forwarded across the switch. Dynamic VLAN Assignment, a variation of Port Authentication, allows host traffic to be processed in VLANs based on the submitted user credentials regardless of the PVID. This document contains a step-by-step procedure on how to implement 802.1x Dynamic VLAN Assignment using the GS3700-24 and an authentication server which usesFreeRADIUS running on the Linux OS.

7.1.1 How to Implement 802.1X Port Authentication with Dynamic VLAN Assignment (Radius Server)

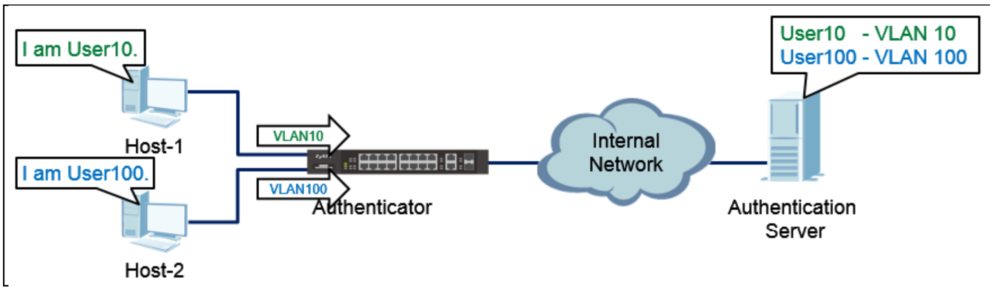
Scenario and Topology

Port Authentication:



Upon detection of a new client (supplicant), the port on the switch (authenticator) will be enabled and set to an "unauthorized" state. In this state, only the 802.1x traffic will be allowed; other traffic, such as DHCP or HTTP, will be blocked at the data link layer. The authenticator will send out EAP-requests identity to the supplicant. The supplicants will need to return an EAP-response packet that the authenticator forwards to the authentication server. The authenticating server can accept or reject the EAP-request; if it accepts the request, the authenticator will set the port as "authorized", which allow is forwarding across the switch.

Dynamic VLAN Assignment:

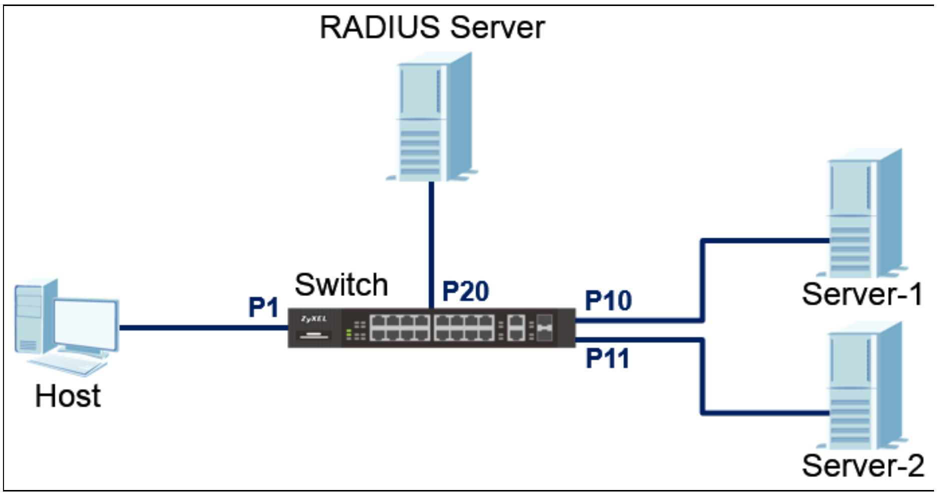


An authentication server informs the authenticator to process the host's traffic on specific VLANs. This can be done by adding the following attributes on the user profile:

Tunnel-Type = **VLAN**
Tunnel-Medium-Type = **IEEE-802**
Tunnel-Private-Group-ID = ***<VLAN ID>***

With Dynamic VLAN Assignment, administrators allow a more flexible network access to the users. Host-1 can access VLAN10 by submitting User10 credentials. Likewise, Host-2 can access VLAN20 by submitting User100 by submitting User100 credentials.

Scenario,



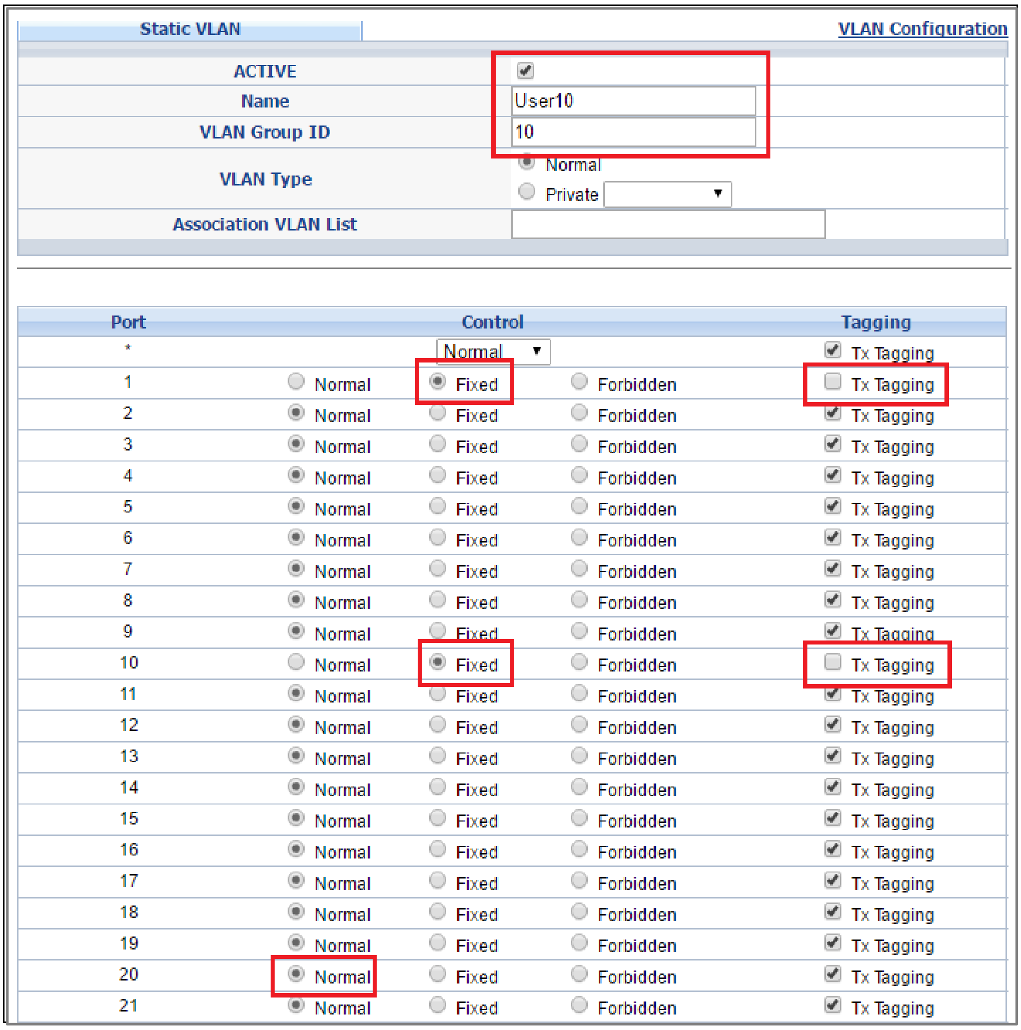
Objectives:

- Core Switch provides the dynamic IP configurations for Host.
- If Host enters the "VLAN10" user credentials, Host receives dynamic IP address for network 192.168.10.0.
- If Host enters the "VLAN20" user credentials, Host receives dynamic IP address for network 192.168.20.0.
- If Host enters an invalid credential, Host is not allowed to communicate across Core Switch.

- Only the “VLAN 10” users can access Server-1.
- Only the “VLAN 20” users can access Server-2.

1. Create VLAN 10 for Host and Server-1

Figure 1, **Advance Application > VLAN > VLAN Configuration > Static VLAN Setup**



Static VLAN

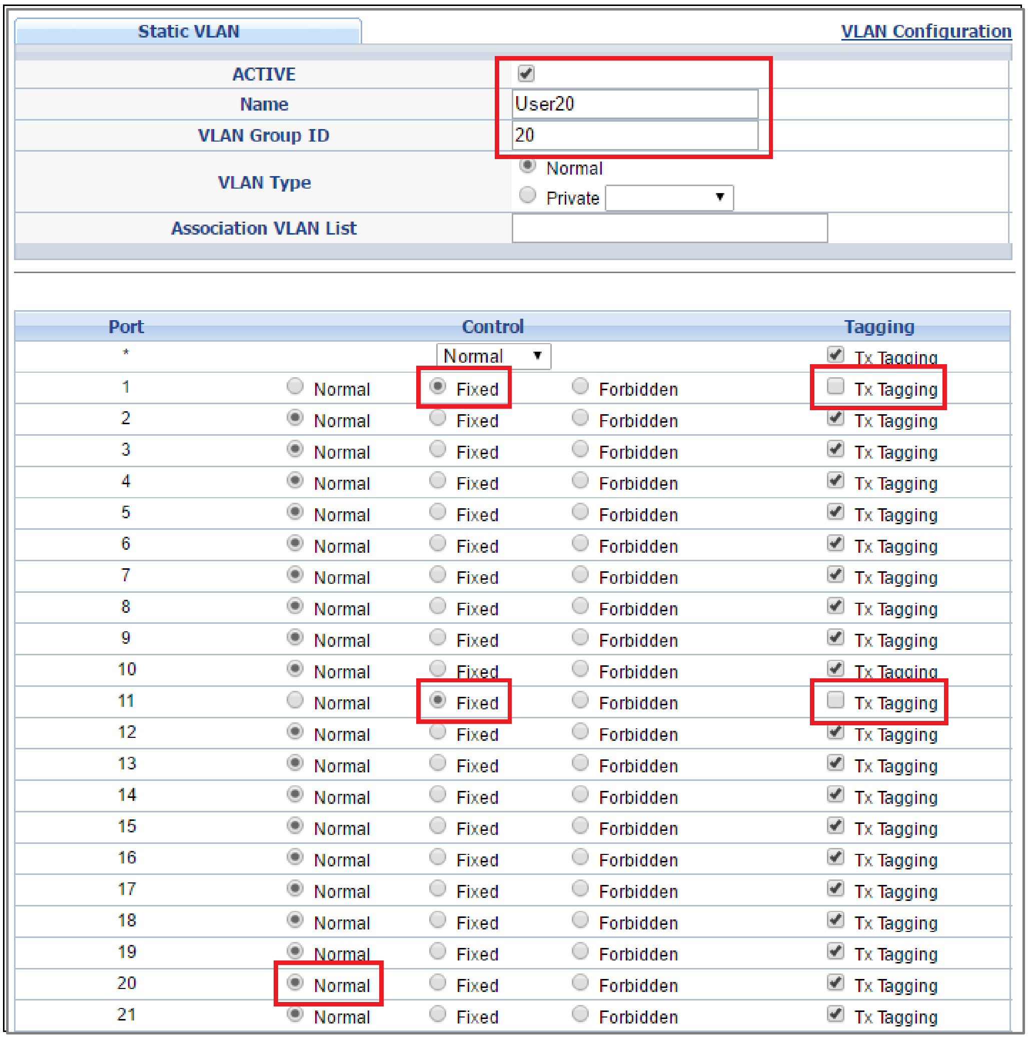
VLAN Configuration

ACTIVE	☑
Name	User10
VLAN Group ID	10
VLAN Type	● Normal ○ Private
Association VLAN List	

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
6	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
7	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
8	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
9	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
10	○ Normal	● Fixed	○ Forbidden	□ Tx Tagging
11	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
12	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
13	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
14	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
15	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
16	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
17	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
18	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
19	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
20	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
21	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging

2. Create VLAN 20 for Host and Server-2.

Figure 2, **Advance Application > VLAN > VLAN Configuration > Static VLAN Setup**



Static VLAN

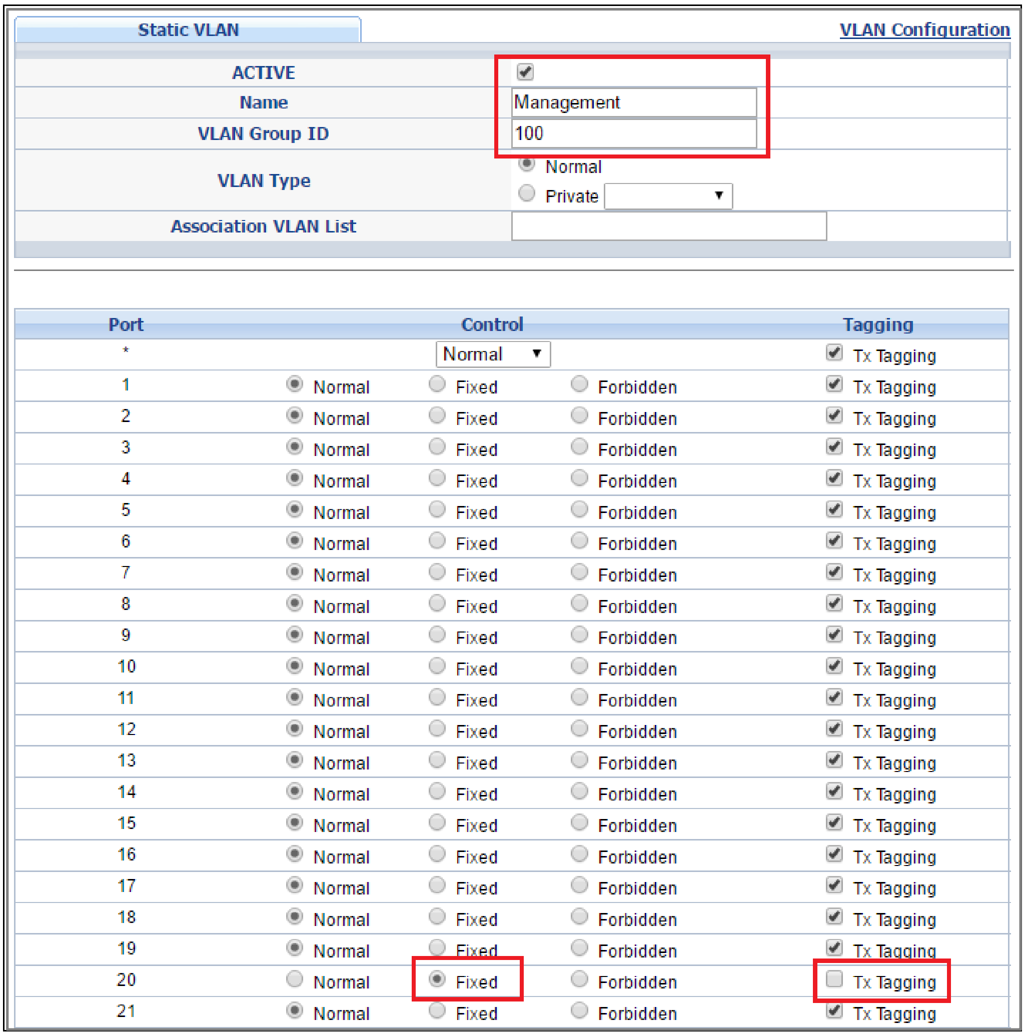
VLAN Configuration

ACTIVE	☑
Name	User20
VLAN Group ID	20
VLAN Type	● Normal ○ Private ▾
Association VLAN List	

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
6	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
7	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
8	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
9	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
10	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
11	○ Normal	● Fixed	○ Forbidden	□ Tx Tagging
12	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
13	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
14	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
15	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
16	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
17	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
18	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
19	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
20	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
21	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging

3. Create VLAN 100 for the RADIUS server and management purpose

Figure 3, **Advance Application > VLAN > VLAN Configuration > Static VLAN Setup**



Static VLAN

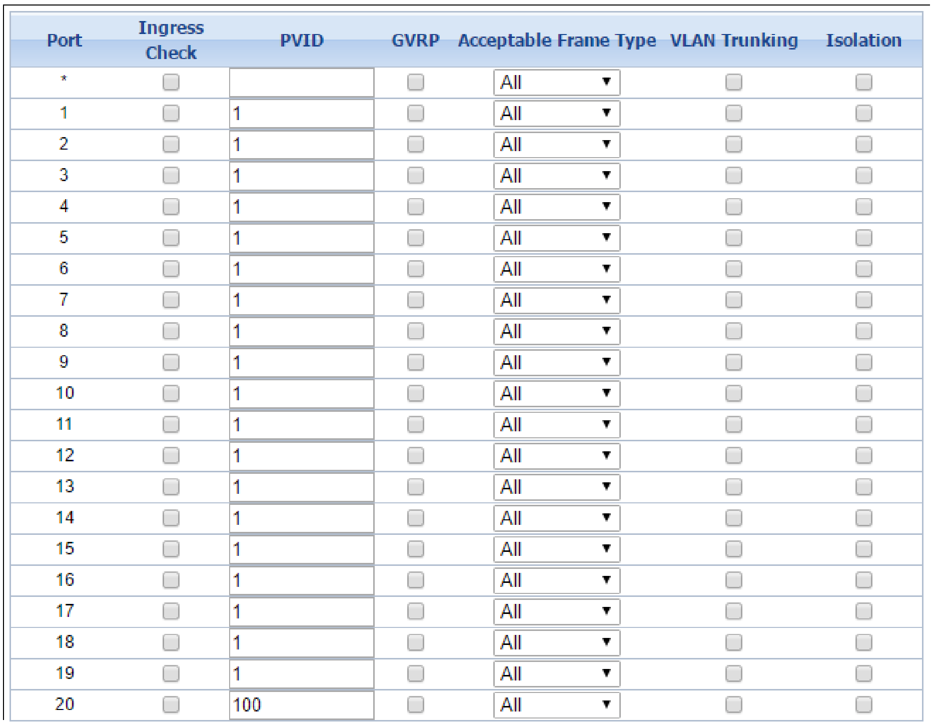
VLAN Configuration

ACTIVE	☑
Name	Management
VLAN Group ID	100
VLAN Type	● Normal ○ Private ▾
Association VLAN List	

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
6	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
7	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
8	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
9	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
10	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
11	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
12	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
13	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
14	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
15	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
16	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
17	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
18	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
19	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
20	○ Normal	● Fixed	○ Forbidden	□ Tx Tagging
21	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging

4. Configure the PVID of the port to the RADIUS server as management VLAN

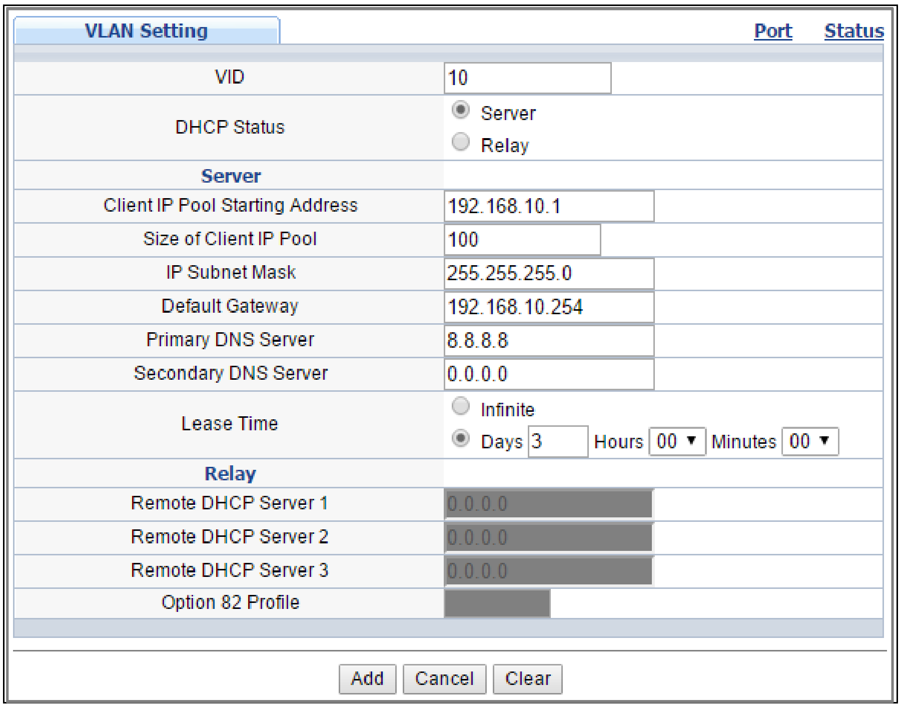
Figure 4, **Advance Application > VLAN > VLAN Configuration > VLAN Port Setup**



Port	Ingress Check	PVID	GVRP	Acceptable Frame Type	VLAN Trunking	Isolation
*	□		□	All ▼	□	□
1	□	1	□	All ▼	□	□
2	□	1	□	All ▼	□	□
3	□	1	□	All ▼	□	□
4	□	1	□	All ▼	□	□
5	□	1	□	All ▼	□	□
6	□	1	□	All ▼	□	□
7	□	1	□	All ▼	□	□
8	□	1	□	All ▼	□	□
9	□	1	□	All ▼	□	□
10	□	1	□	All ▼	□	□
11	□	1	□	All ▼	□	□
12	□	1	□	All ▼	□	□
13	□	1	□	All ▼	□	□
14	□	1	□	All ▼	□	□
15	□	1	□	All ▼	□	□
16	□	1	□	All ▼	□	□
17	□	1	□	All ▼	□	□
18	□	1	□	All ▼	□	□
19	□	1	□	All ▼	□	□
20	□	100	□	All ▼	□	□

5. Configure the DHCP service for VLAN 10 users

Figure 5, **IP Application > DHCP > DHCPv4 > VLAN**

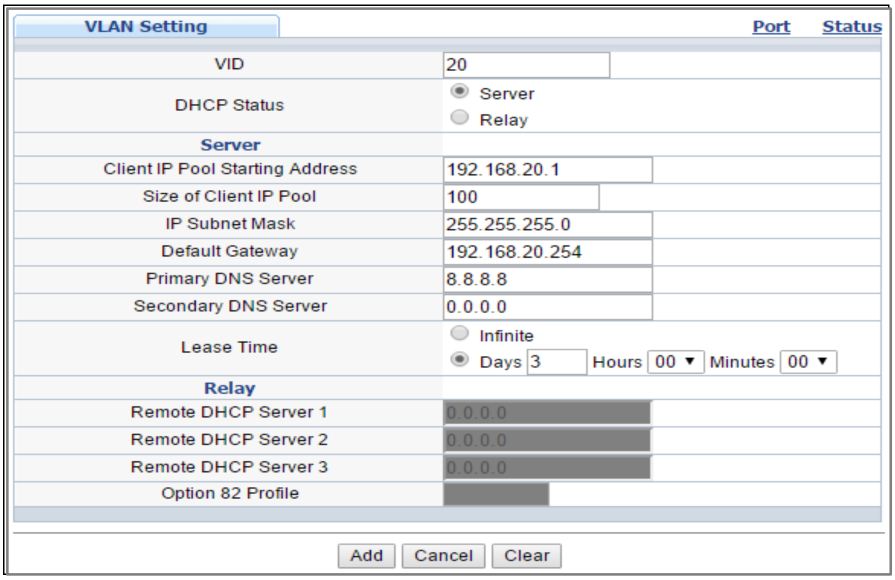


VLAN Setting | Port | Status

VID	10
DHCP Status	● Server ○ Relay
Server	
Client IP Pool Starting Address	192.168.10.1
Size of Client IP Pool	100
IP 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	○ Infinite ● Days 3 Hours 00 Minutes 00
Relay	
Remote DHCP Server 1	0.0.0.0
Remote DHCP Server 2	0.0.0.0
Remote DHCP Server 3	0.0.0.0
Option 82 Profile	

6. Configure the DHCP service for VLAN 20 user

Figure 6, **IP Application > DHCP > DHCPv4 > VLAN**

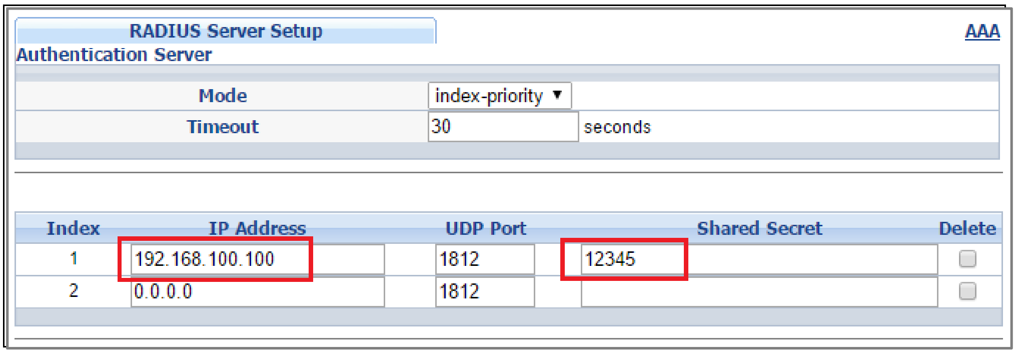


VLAN Setting | Port | Status

VID	20
DHCP Status	● Server ○ Relay
Server	
Client IP Pool Starting Address	192.168.20.1
Size of Client IP Pool	100
IP Subnet Mask	255.255.255.0
Default Gateway	192.168.20.254
Primary DNS Server	8.8.8.8
Secondary DNS Server	0.0.0.0
Lease Time	○ Infinite ● Days 3 Hours 00 Minutes 00
Relay	
Remote DHCP Server 1	0.0.0.0
Remote DHCP Server 2	0.0.0.0
Remote DHCP Server 3	0.0.0.0
Option 82 Profile	

7. Input the RADIUS server's IP address and set the shared secret as "12345"

Figure 7, **Advance Application > AAA > RADIUS Server Setup**



RADIUS Server Setup

AAA

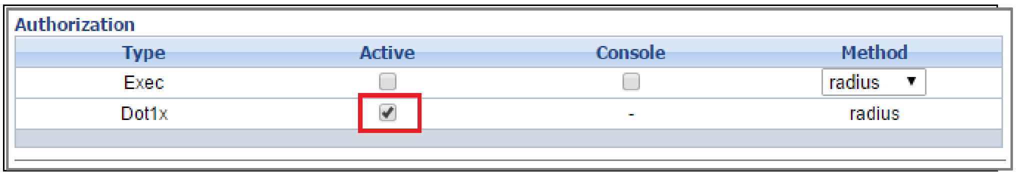
Authentication Server

Mode	index-priority ▾
Timeout	30 seconds

Index	IP Address	UDP Port	Shared Secret	Delete
1	192.168.100.100	1812	12345	□
2	0.0.0.0	1812		□

8. Check Dot1x under the Authorization section

Figure 8, **Advance Application > AAA > AAA Setup**

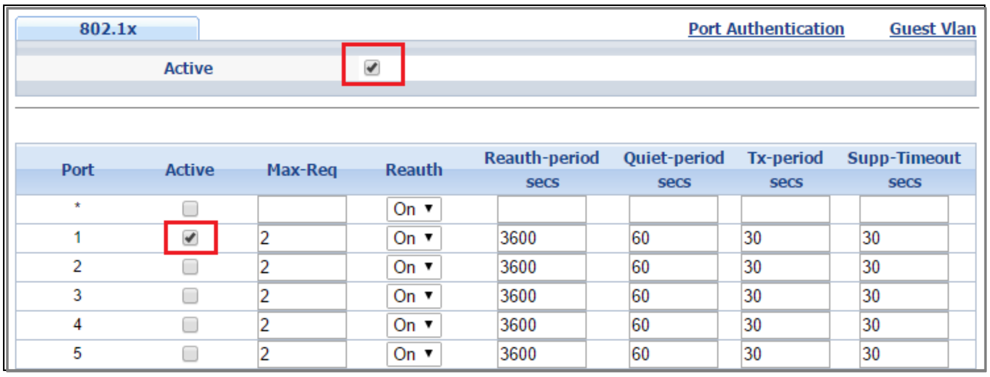


Authorization

Type	Active	Console	Method
Exec	□	□	radius ▾
Dot1x	☑	-	radius

9. Activate Port Authentication on the port connected to Host

Figure 9, **Advance Application > Port Authentication > 802.1x**



802.1x

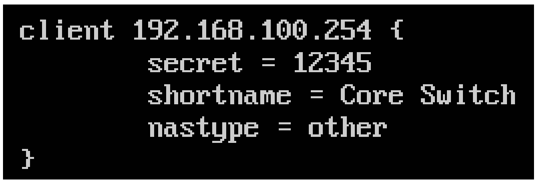
Port Authentication Guest Vlan

Active ☑

Port	Active	Max-Req	Reauth	Reauth-period secs	Quiet-period secs	Tx-period secs	Supp-Timeout secs
*	□		On ▾				
1	☑	2	On ▾	3600	60	30	30
2	□	2	On ▾	3600	60	30	30
3	□	2	On ▾	3600	60	30	30
4	□	2	On ▾	3600	60	30	30
5	□	2	On ▾	3600	60	30	30

10.Access the RADIUS server. Edit the Client profile located in **/etc/freeradius/clients.conf** for Core Switch

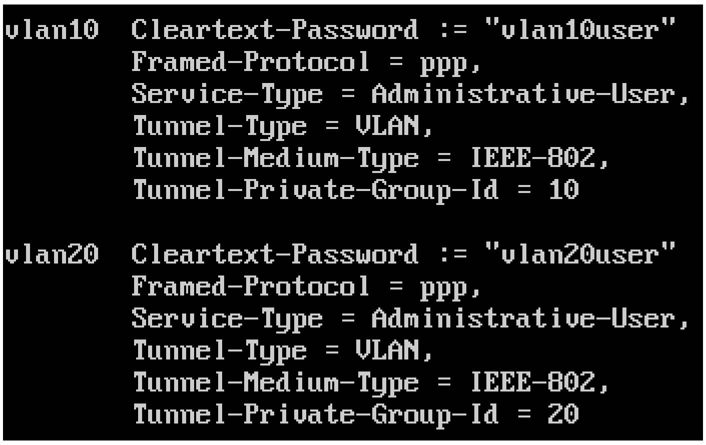
Figure 10, **/etc/freeradius/clients.conf**



```
client 192.168.100.254 {
        secret = 12345
        shortname = Core Switch
        nastype = other
}
```

11.Edit the User profile located in **/etc/freeradius/users** for Host credentials and attributes

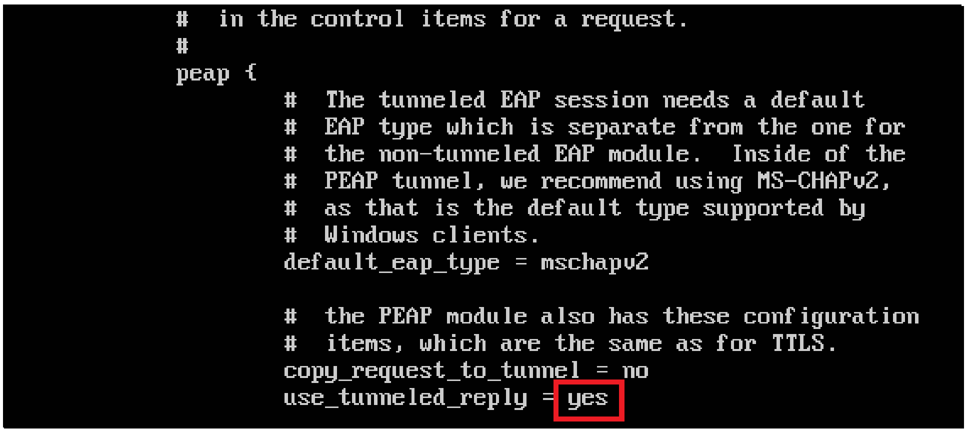
Figure 11, **/etc/freeradius/users**



```
vlan10  Cleartext-Password := "vlan10user"
        Framed-Protocol = ppp,
        Service-Type = Administrative-User,
        Tunnel-Type = VLAN,
        Tunnel-Medium-Type = IEEE-802,
        Tunnel-Private-Group-Id = 10

vlan20  Cleartext-Password := "vlan20user"
        Framed-Protocol = ppp,
        Service-Type = Administrative-User,
        Tunnel-Type = VLAN,
        Tunnel-Medium-Type = IEEE-802,
        Tunnel-Private-Group-Id = 20
```

12.Edit EAP profile located in **/etc/freeradius/eap.conf** to allow dynamic VLAN attributes

Figure 12, **/etc/freeradius/eap.conf**



```
                #  in the control items for a request.
                #
                peap {
                        #  The tunneled EAP session needs a default
                        #  EAP type which is separate from the one for
                        #  the non-tunneled EAP module.  Inside of the
                        #  PEAP tunnel, we recommend using MS-CHAPv2,
                        #  as that is the default type supported by
                        #  Windows clients.
                        default_eap_type = mschapv2

                        #  the PEAP module also has these configuration
                        #  items, which are the same as for TTLS.
                        copy_request_to_tunnel = no
                        use_tunneled_reply = yes
```

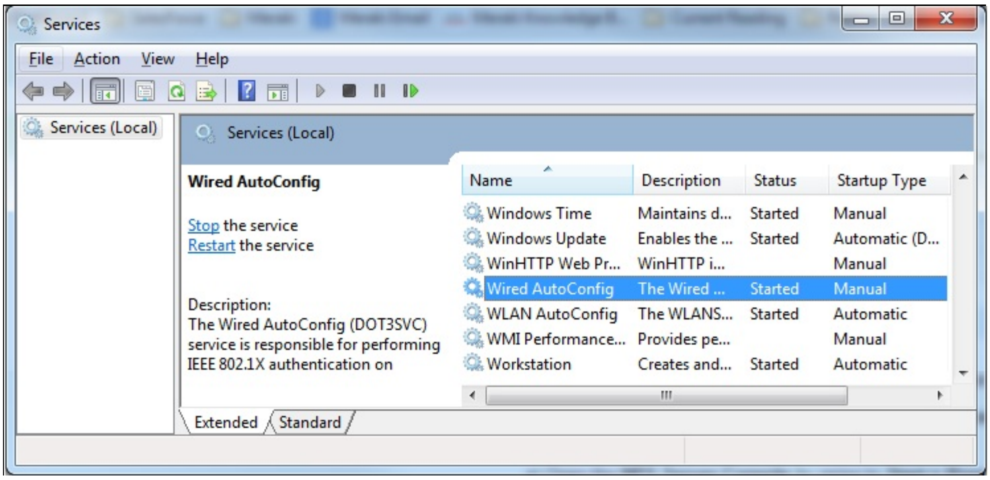
13.Restart the FreeRADIUS service to refresh the settings

Verification procedures

1. Access the Host PC.

2. Click the **Start button** and type **services.msc** into the search box.

3. In the Services window, locate the service named **Wired AutoConfig**.



Wired AutoConfig

Stop the service
Restart the service

Description:
The Wired AutoConfig (DOT3SVC) service is responsible for performing IEEE 802.1X authentication on

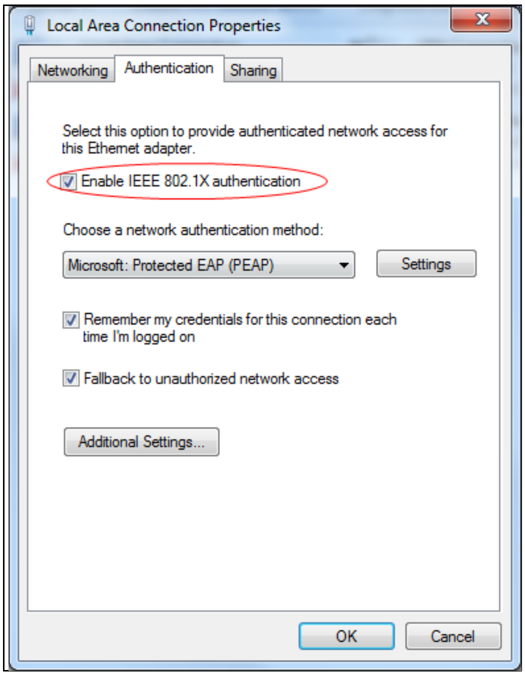
Name	Description	Status	Startup Type
Windows Time	Maintains d...	Started	Manual
Windows Update	Enables the ...	Started	Automatic (D...
WinHTTP Web Pr...	WinHTTP i...		Manual
Wired AutoConfig	The Wired ...	Started	Manual
WLAN AutoConfig	The WLANS...	Started	Automatic
WMI Performance...	Provides pe...		Manual
Workstation	Creates and...	Started	Automatic

4. Make sure the service status is “**Started**”.

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

6. Click on the Authentication tab and check “**Enable IEEE 802.1X authentication**”.

7. Choose the network authentication method **Microsoft: Protected EAP (PEAP)**.



Local Area Connection Properties

Networking | Authentication | Sharing

Select this option to provide authenticated network access for this Ethernet adapter.

☑ Enable IEEE 802.1X authentication

Choose a network authentication method:

Microsoft: Protected EAP (PEAP) | Settings

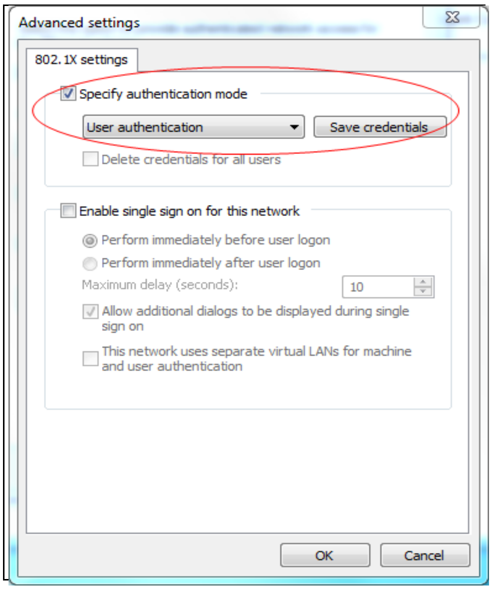
☑ Remember my credentials for this connection each time I'm logged on

☑ Fallback to unauthorized network access

Additional Settings...

OK | Cancel

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



Advanced settings

802.1X settings

☑ Specify authentication mode

User authentication | Save credentials

□ Delete credentials for all users

□ Enable single sign on for this network

● Perform immediately before user logon

○ Perform immediately after user logon

Maximum delay (seconds): 10

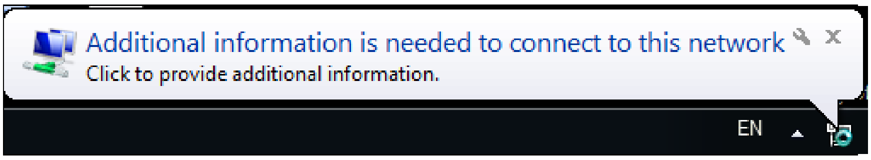
☑ Allow additional dialogs to be displayed during single sign on

□ This network uses separate virtual LANs for machine and user authentication

OK | Cancel

9. Make sure that the Host PC is using the **dynamic IP address configurations**.
10. Connect the Host PC to port 1 of the Core Switch.

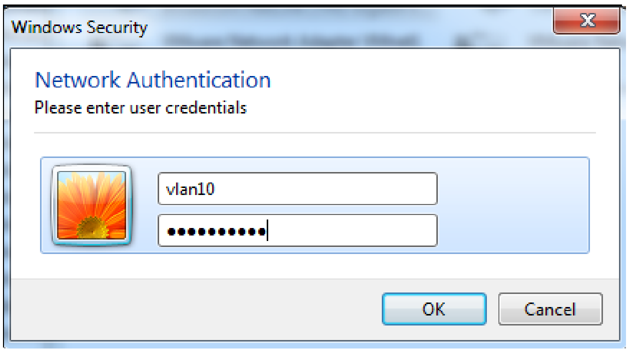
11. Host PC should show "**Additional information is needed to connect to this network.**"



Additional information is needed to connect to this network

Click to provide additional information.

12. Enter the username (**vlan10**) and password (**vlan10user**) which must be consistent with the RADIUS server's user profile settings.



Windows Security

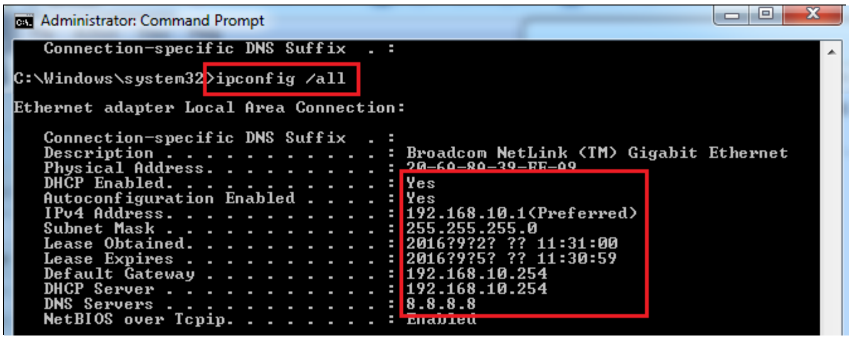
Network Authentication

Please enter user credentials

vlan10

••••••••••

13. Go to Windows command prompt and type "**ipconfig /all**". The IP address should be assigned to the VLAN 10 network (192.168.10.X).



Administrator: Command Prompt

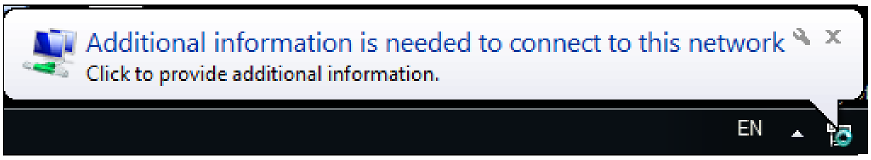
```
   Connection-specific DNS Suffix  . :

C:\Windows\system32>ipconfig /all

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Broadcom NetLink (TM) Gigabit Ethernet
   Physical Address. . . . . . . . . : 20-60-80-39-FE-09
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.10.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 2016?9?22? ?? 11:31:00
   Lease Expires . . . . . . . . . . : 2016?9?5? ?? 11:30:59
   Default Gateway . . . . . . . . . : 192.168.10.254
   DHCP Server . . . . . . . . . . . : 192.168.10.254
   DNS Servers . . . . . . . . . . . : 8.8.8.8
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

14. Host PC can ping **Server-1** connected to port 10 of Core Switch with the IP **192.168.10.100**.

15. Disconnect Host PC from port 1 of Core Switch.

16. Reconnect the Host PC to port 1 of the Core Switch.

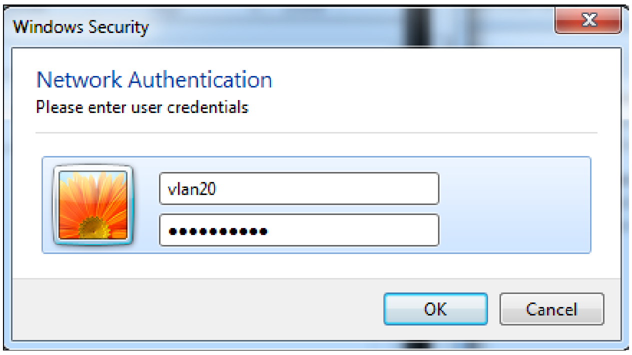
17. Host PC should show "**Additional information is needed to connect to this network**".



Additional information is needed to connect to this network

Click to provide additional information.

18. Enter the username (**vlan20**) and password (**vlan20user**) which must be consistent with the RADIUS server's user profile settings.



Windows Security

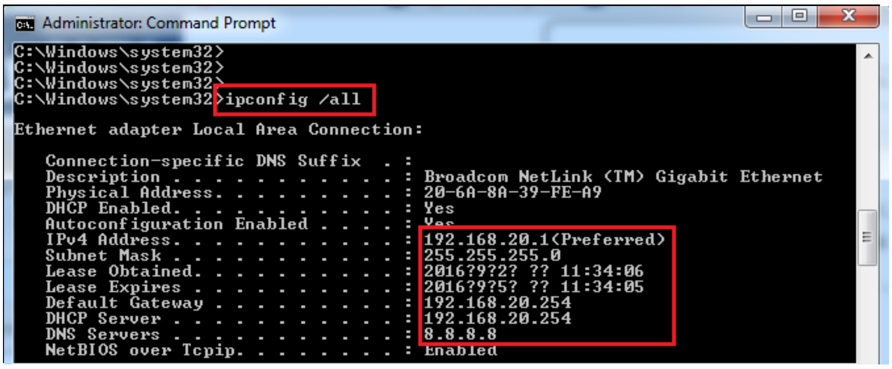
Network Authentication

Please enter user credentials

vlan20

••••••••••

19. Go to Windows command prompt and type "**ipconfig /all**". The IP address should be assigned to the VLAN 10 network (192.168.20.X).



Administrator: Command Prompt

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

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Broadcom NetLink (TM) Gigabit Ethernet
   Physical Address. . . . . . . . . : 20-6A-8A-39-FE-A9
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.20.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 2016?9?22? ?? 11:34:06
   Lease Expires . . . . . . . . . . : 2016?9?25? ?? 11:34:05
   Default Gateway . . . . . . . . . : 192.168.20.254
   DHCP Server . . . . . . . . . . . : 192.168.20.254
   DNS Servers . . . . . . . . . . . : 8.8.8.8
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

20. Host PC can ping **Server-2** connected to port 11 of Core Switch with the IP **192.168.20.100**.

Note: Only the Zyxel enterprise switch models can support Dynamic VLAN Assignment. Smart managed switches do not support the 802.1x attributes necessary for Dynamic VLAN Assignment

8.1 IP Source Guard

Overview

Use IPv4 and IPv6 source guard to filter unauthorized DHCP and ARP packets in your network. It uses a binding table to distinguish between authorized and unauthorized DHCP ARP packets in your network. A binding contains:

- MAC address
- VLAN ID
- IP address
- Port number

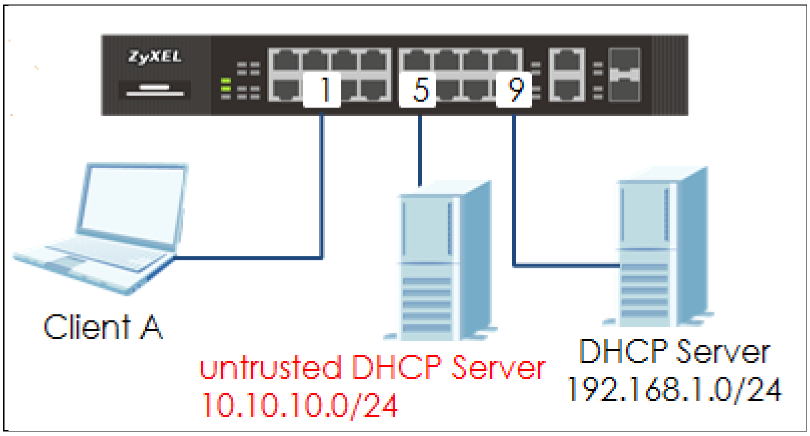
When switch receives a DHCP or ARP packets, it looks up the MAC address, VLAN ID, IP address & port number in the binding table. If there is binding, the switch forward the packet. If there is not, the switch discards the packet.

8.1.1 How to set DHCP snooping? (Dynamic)

Overview

DHCP snooping, you can configure the DHCP Server on a "Trusted Port" so that all clients can get the IP address from a trusted DHCP server. Also, all DHCP IP address assignments will be recorded into an internal table called the "Snooping Table". So if there is another DHCP server in the network, but located on an untrust port, all DHCP message will be discard.

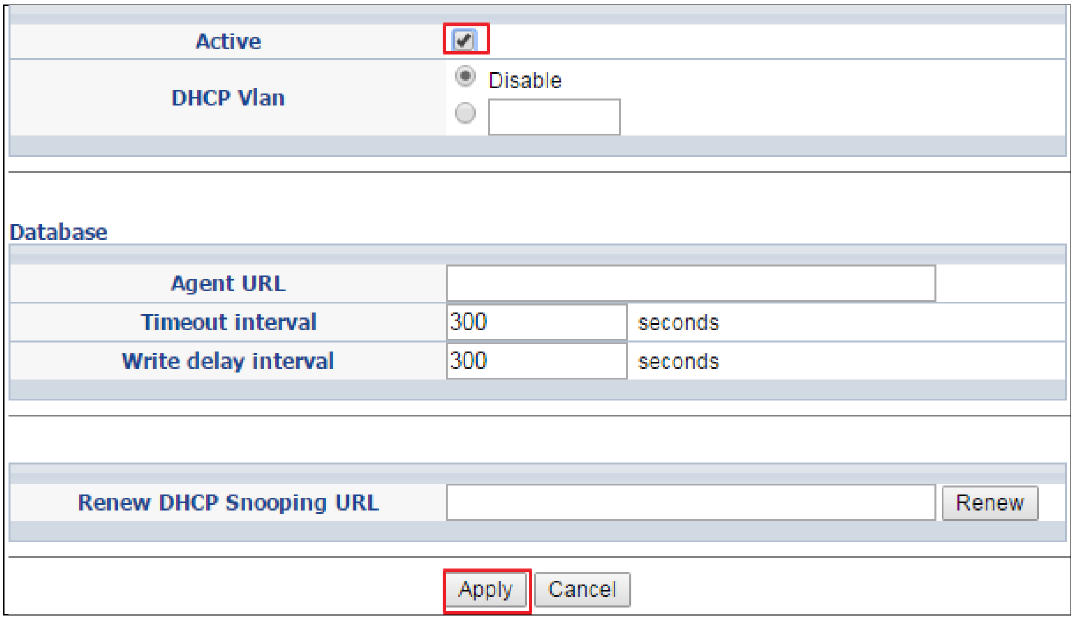
Topology,



Note: In the scenario the switch is configure with DHCP snooping trusted port 9, so that client A or other device can get an IP from the DHCP server. At the right side if the port is not been configured with trusted port (10.10.10.0/24) all DHCP packets will be discard and client A still gets IP with the DHCP server (192.168.1.0/24) trusted port.

1. In this screen check the **Active** box then click **Apply** to enable DHCP snooping features. For the following options, please use the **HELP** icon for more information.

Figure 1, **Advanced Application > IP Source Guard > DHCP Snooping > Configure**



Active	☑	
DHCP Vlan	● Disable ○	

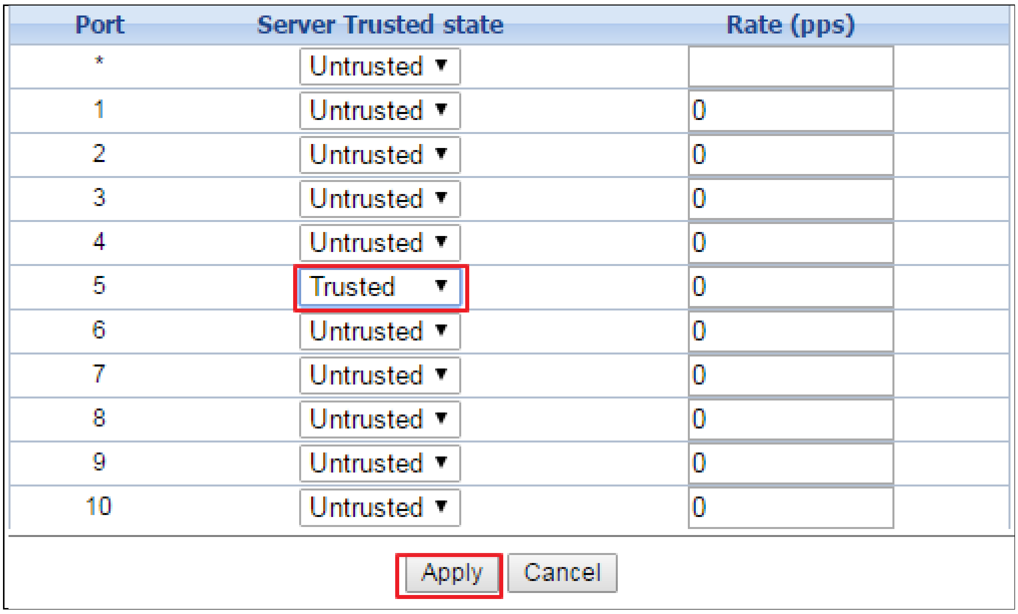
Database

Agent URL		
Timeout interval	300	seconds
Write delay interval	300	seconds

Renew DHCP Snooping URL		Renew

2. Select which port should be **Trusted** for the DHCP server or other switch and **Rate** specify the maximum number for DHCP packets (1-2048) that the Switch receives from each port each second.

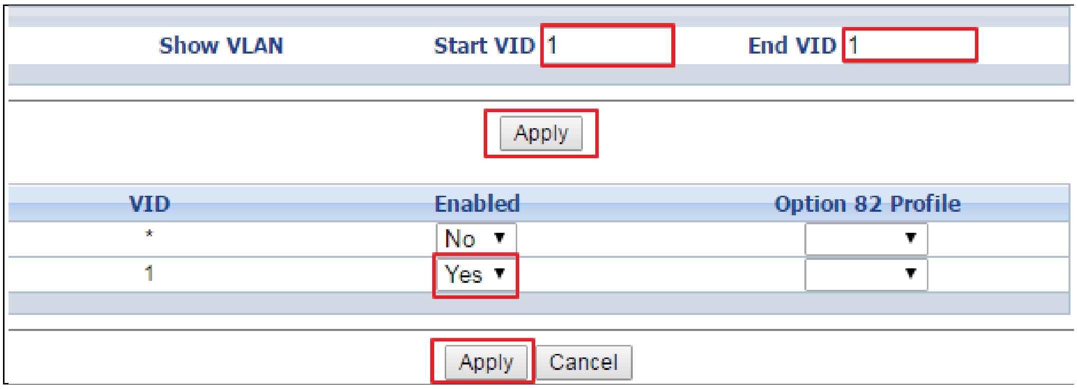
Figure 2, **Advanced Application > IP Source Guard > DHCP Snooping > Configure > Port**



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

3. Use this screen to enable DHCP snooping on each VLAN and to specify whether or not the Switch adds DHCP relay agent option 82 information to DHCP requests that the Switch relays to a DHCP server for each VLAN.

Figure 3, **Advanced Application > IP Source Guard > DHCP Snooping > Configure > VLAN**



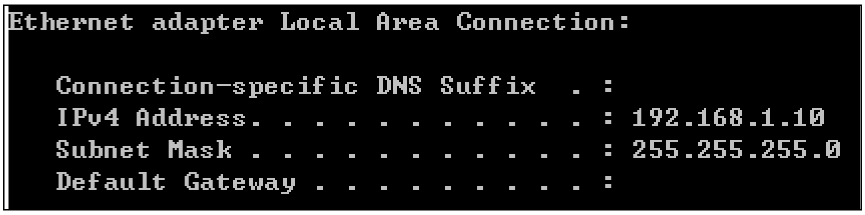
Show VLAN Start VID 1 End VID 1

VID	Enabled	Option 82 Profile
*	No ▼	▼
1	Yes ▼	▼

Verify

1. Based on the scenario client A should get an IP of 192.168.1.X/24.

Figure 4, **Run Windows Command Processor (CMD)**



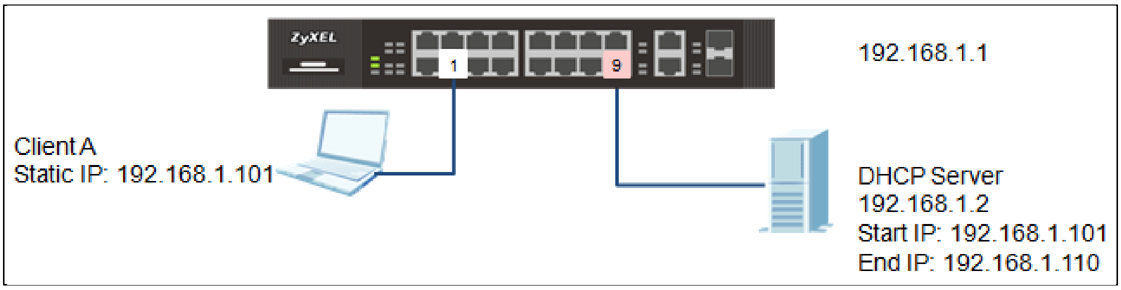
```
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.1.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
```

8.1.2 How to set static MAC binding? (Static)

Overview

Static MAC address is an address that has been manually entered in the MAC address table, Static MAC address does not age out. After setting up a static MAC address on a port it reduce the need for broadcasting.

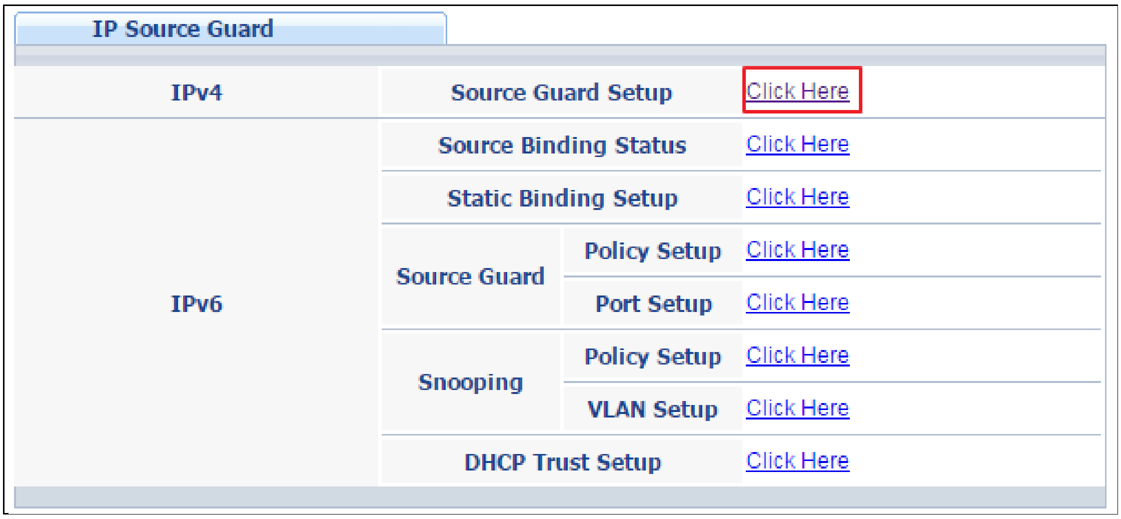
Topology,



Note: in the scenario switch port 1 has been configured static MAC binding with client A specific MAC address and given the port 1 an IP address of 192.168.1.101.

1. Enter **Source Guard Setup.**

Figure 1, **Advanced Application > IP Source Guard**

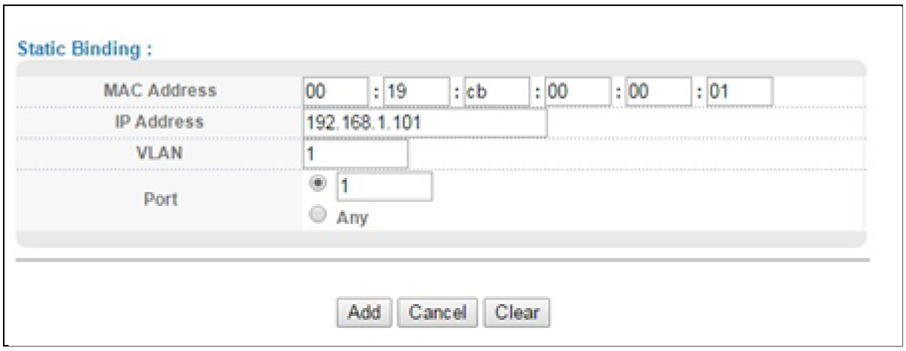


IP Source Guard

IPv4	Source Guard Setup		Click Here
IPv6	Source Binding Status		Click Here
	Static Binding Setup		Click Here
	Source Guard	Policy Setup	Click Here
		Port Setup	Click Here
	Snooping	Policy Setup	Click Here
		VLAN Setup	Click Here
	DHCP Trust Setup		Click Here

2. Input the specific MAC address of the device. User can specify the IP address, VLAN & port number.

Figure 2, **Advanced Application > IP Source Guard > Static Binding**



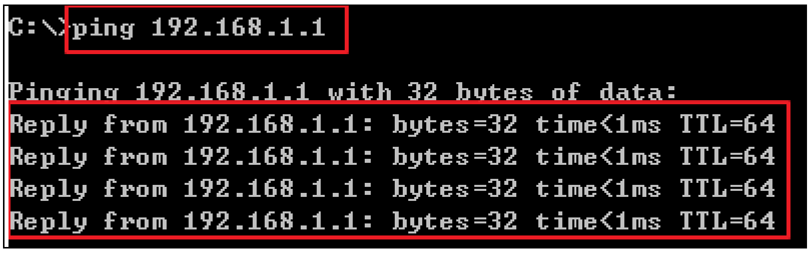
Static Binding :

MAC Address	00 : 19 : cb : 00 : 00 : 01
IP Address	192.168.1.101
VLAN	1
Port	● 1 ○ Any

Verify

1. Based on the scenario client A should be configured with an IP address of 192.168.1.101 and can ping the switch IP 192.168.1.1.

Figure 3, **Run Windows Command Processor**



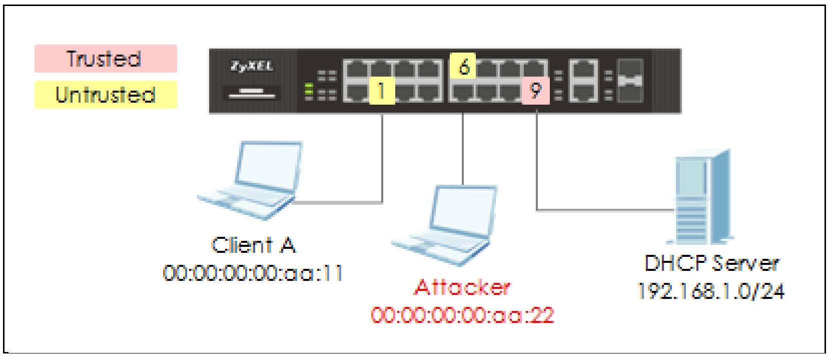
```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
```

8.1.3 How to set ARP inspection?

Overview

This feature prevent ARP spoofing from the network to secure L2 forwarding, it contains a DHCP snooping table which can match and check which IP address is allowed to access the network, if It's not the traffic will be blocked and classified to blacklist.

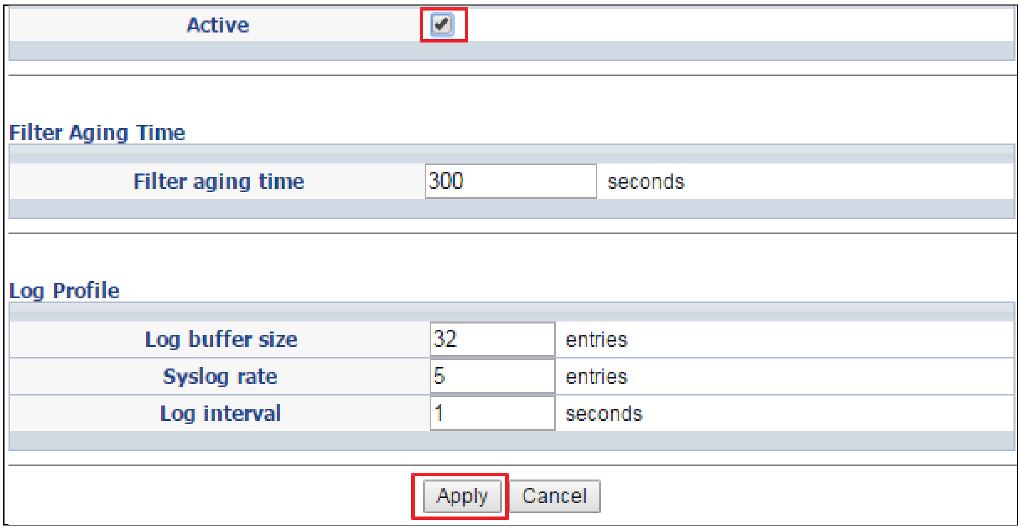
Topology,



Note: in this scenario assume that there's attacker want to join the network, but the switch is configured with ARP inspection so that it will detect and match the white list (DHCP snooping table) first, if the MAC address doesn't match the table it will be blocked and classified to blacklist.

1. Check the **Active** box and click the **Apply** to run the feature. Please kindly use the **HELP** button for more specific information.

Figure 1, **Advanced Application > IP Source Guard > Source Guard setup > ARP Inspection > Configure**



Active	☑

Filter Aging Time

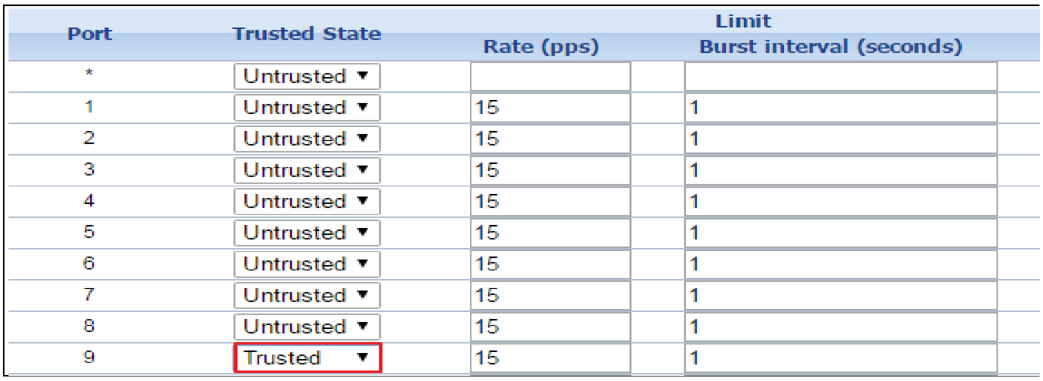
Filter aging time	300 seconds

Log Profile

Log buffer size	32 entries
Syslog rate	5 entries
Log interval	1 seconds

2. In this screen user can configure which device will be trust on this port. Ex: based on the scenario, port 9 was been configured as trusted port so that DHCP server can provide IP address to client within the whitelist-DHCP snooping and Static binding tables

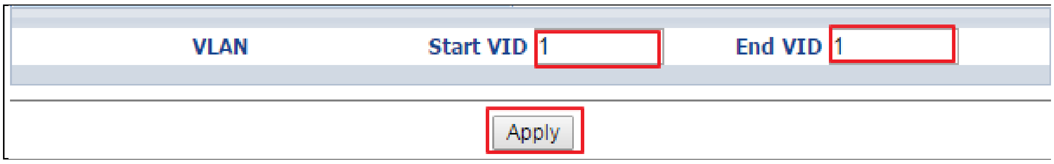
Figure 2, **Advanced Application > IP Source Guard > Source Guard setup > ARP Inspection > Configure > Port**



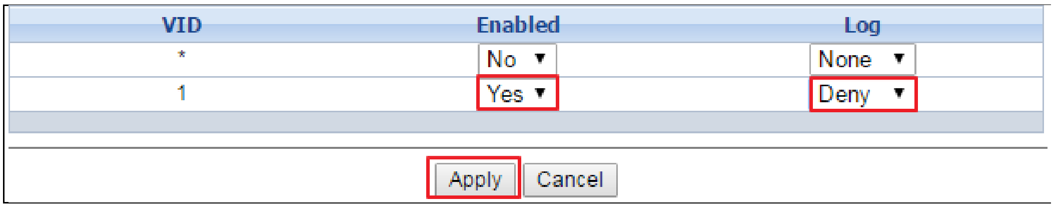
Port	Trusted State	Limit	
		Rate (pps)	Burst interval (seconds)
*	Untrusted		
1	Untrusted	15	1
2	Untrusted	15	1
3	Untrusted	15	1
4	Untrusted	15	1
5	Untrusted	15	1
6	Untrusted	15	1
7	Untrusted	15	1
8	Untrusted	15	1
9	Trusted	15	1

3. Use this screen to enable ARP inspection on each VLAN and to specify when the Switch generates log messages for receiving ARP packets from each VLAN.

Figure 3, **Advanced Application > IP Source Guard > Source Guard setup > ARP Inspection > Configure > VLAN**



VLAN	Start VID	End VID
	1	1

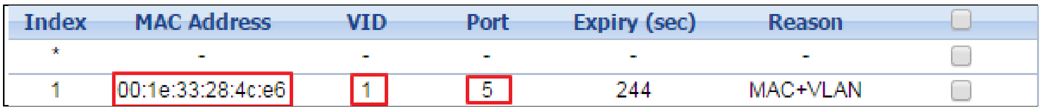


VID	Enabled	Log
*	No ▼	None ▼
1	Yes ▼	Deny ▼

Verify

1. Figure 4, in this screen it will display the unknown ARP blocked by the switch.

Figure 4, **Advanced Application > IP Source Guard > Source Guard setup > ARP Inspection**



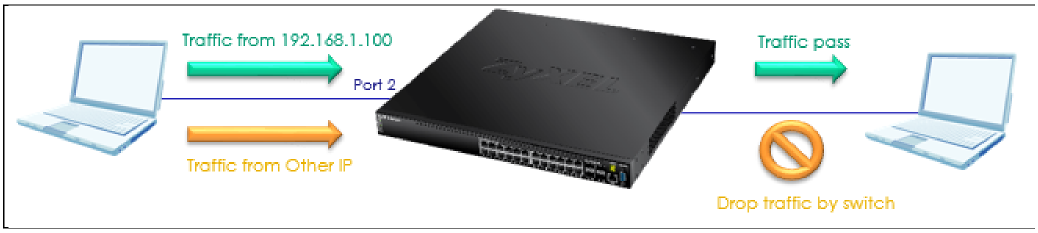
Index	MAC Address	VID	Port	Expiry (sec)	Reason	□
*	-	-	-	-	-	□
1	00:1e:33:28:4c:e6	1	5	244	MAC+VLAN	□

9.1 Access Control List (ACL)

Overview

ACL (Access Control List) is the name of a combination of Classifier and Policy Rule. A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming port number. For example, you can configure a classifier to select traffic from the same protocol port (such as Telnet) to form a flow. A policy rule ensures that a traffic flow gets the requested treatment in the network. Please be advised, that you must first configure a classifier in the Classifier screen before you configure a policy rule.

Scenario:



Goal:

Let all other traffic from port 2 will be dropped, but only traffic coming from port 2 with 192.168.1.100 will be forwarded. It has to define 3 ACL (classifier & policy rule) to achieve the purpose:

1. Drop all other traffic from port 2
2. Allow ARP to through port 2
3. Allow the traffic coming from port 2 with 192.168.1.100

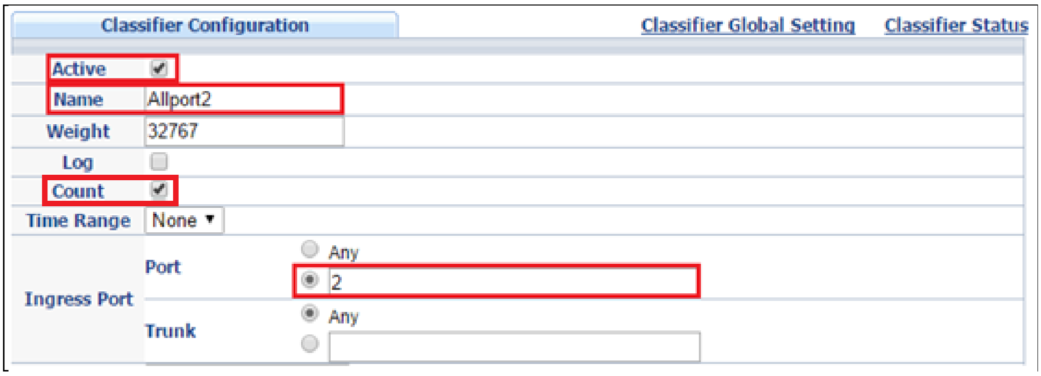
9.1.1 How to block host to access internet?

Overview

We define three rules. First, we define a classifier for the traffic that is coming from port 2 is the host and its source address 192.168.1.100; second, we specify a classifier for the traffic from port 2. Finally we specify a classifier for ARP.

1. Select **Active, set Name as "Allport2", select "Count"** and **Ingress port as 2,** then clicks **Add** to run feature.

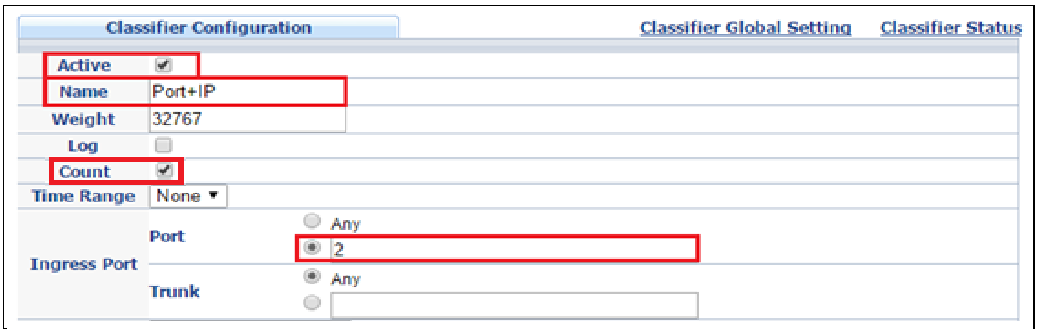
Figure 1 **Advanced Application > Classifier> Classifier Configuration**



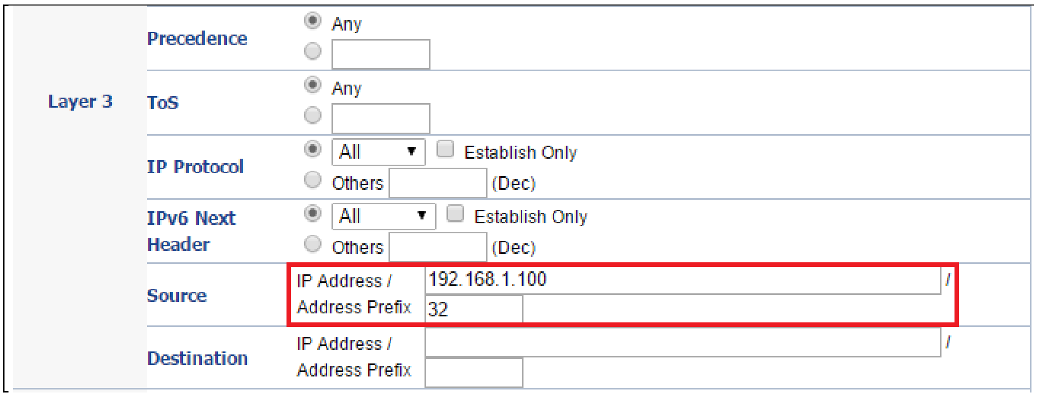
Active	☑	
Name	Allport2	
Weight	32767	
Log	□	
Count	☑	
Time Range	None ▾	
Ingress Port	Port	○ Any ● 2
	Trunk	● Any ○

2. Select **Active, set Name as “Port+IP”, Ingress port as 2, selects “Count”** and **Source IP as 192.168.1.100/32,** then click **Add** to run feature.

Figure 2 **Advanced Application > Classifier> Classifier Configuration**



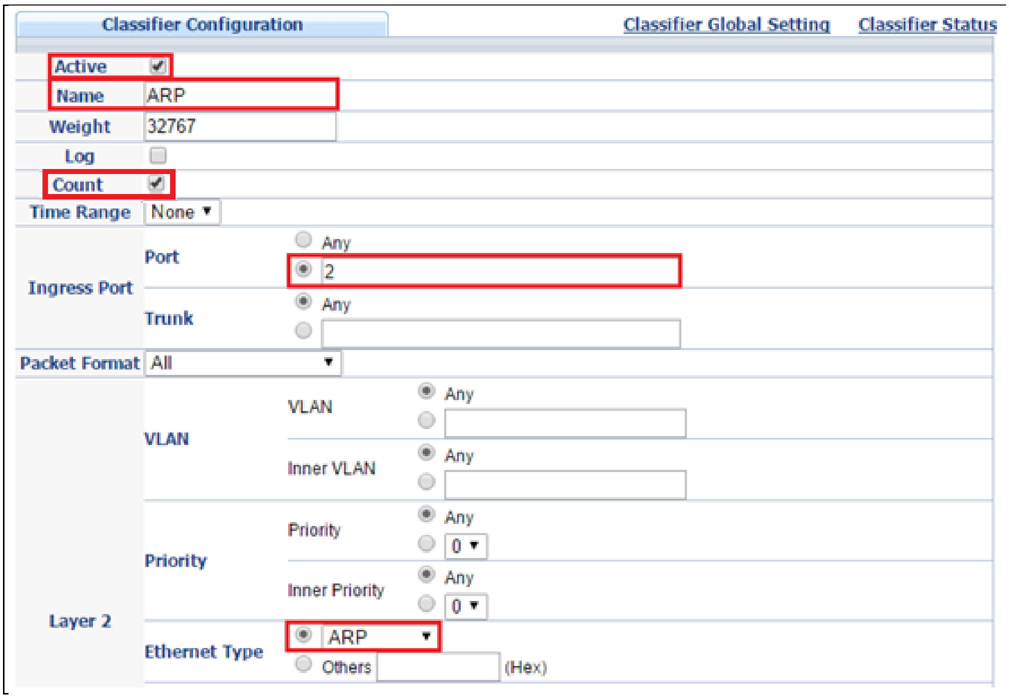
Active	☑	
Name	Port+IP	
Weight	32767	
Log	□	
Count	☑	
Time Range	None ▾	
Ingress Port	Port	○ Any ● 2
	Trunk	● Any ○



Layer 3	Precedence	● Any ○
	ToS	● Any ○
	IP Protocol	● All ▾ □ Establish Only ○ Others (Dec)
	IPv6 Next Header	● All ▾ □ Establish Only ○ Others (Dec)
	Source	IP Address / Address Prefix: 192.168.1.100 / 32
	Destination	IP Address / Address Prefix: /

3. Select **Active, set Name as “ARP”, Ingress port as 2, select “Count** “and **Ethernet Type as ARP,** then click **Add** to run feature.

Figure 3 **Advanced Application > Classifier> Classifier Configuration**



Active ☑

Name ARP

Weight 32767

Log □

Count ☑

Time Range None

Ingress Port — Port: ○ Any ● 2; Trunk: ● Any ○

Packet Format All

Layer 2 — VLAN: VLAN ● Any ○; Inner VLAN ● Any ○

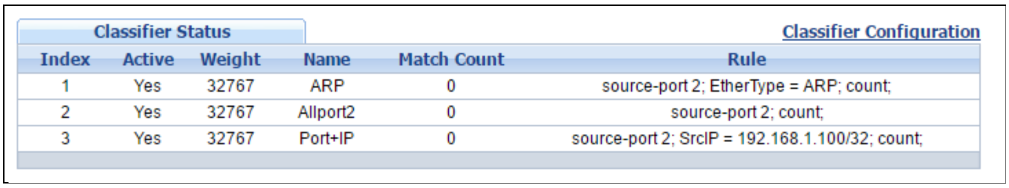
Priority: Priority ● Any ○ 0; Inner Priority ● Any ○ 0

Ethernet Type: ● ARP ○ Others (Hex)

Verify

1. In this screen display the classifiers status.

Figure 4, **Advanced Application > Classifier**



Index	Active	Weight	Name	Match Count	Rule
1	Yes	32767	ARP	0	source-port 2; EtherType = ARP; count;
2	Yes	32767	Allport2	0	source-port 2; count;
3	Yes	32767	Port+IP	0	source-port 2; SrcIP = 192.168.1.100/32; count;

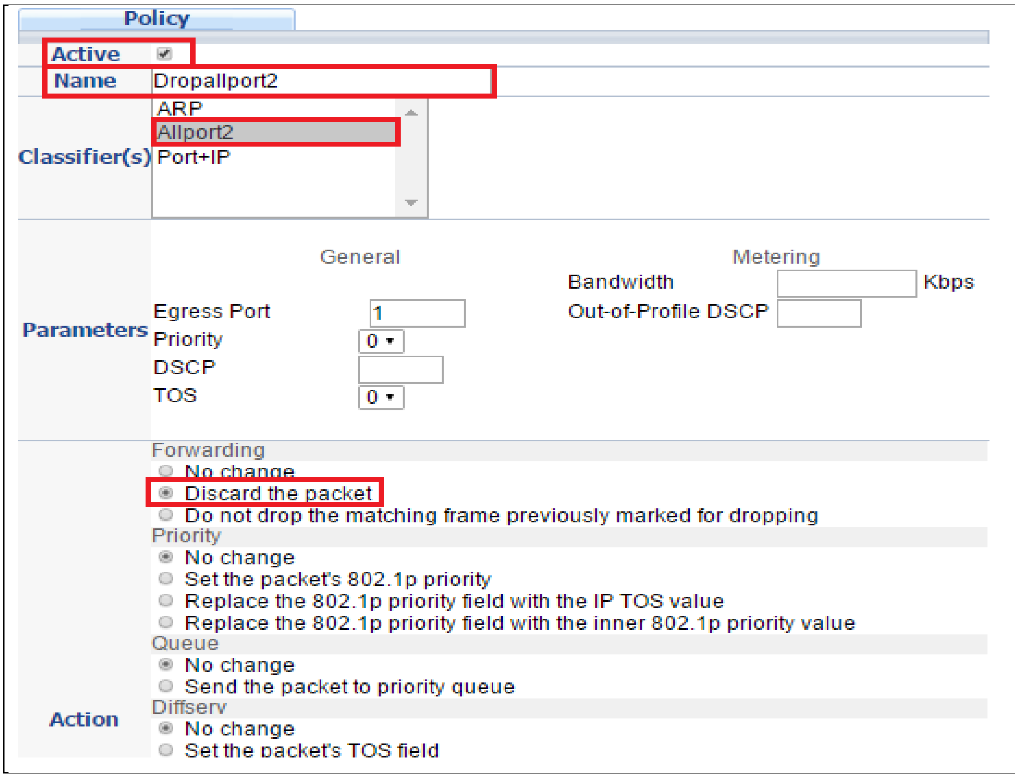
9.1.2 How to configure classifier on the switch?

Overview

After the classification, we need to define the policy rule to ensure that the traffic gets the deserved treatment in the network. Here, we also define three policy rules. The first policy rule is to forward (do not drop the matching frame previously marked for dropping) only the traffic from port 2 and with the ip address of 192.168.1.100. The second policy rule is to discard all the traffic from port 2 on first classifier; and we apply the second policy rule on second classifier. Moreover, do not forget to apply a policy rule (do not drop the matching frame previously marked for dropping) for our last classifier.

1. Select **Active, set Name as "Dropallport2", select classifier "Allport2"**and**select "Discard the packet" in Action,** then click **Add** to run feature

Figure 5 **Advanced Application >Policy Rule**



Policy

Active ☑

Name Dropallport2

Classifier(s)
ARP
Allport2
Port+IP

Parameters

General
Egress Port 1
Priority 0
DSCP
TOS 0

Metering
Bandwidth Kbps
Out-of-Profile DSCP

Action

Forwarding
○ No change
● Discard the packet
○ Do not drop the matching frame previously marked for dropping

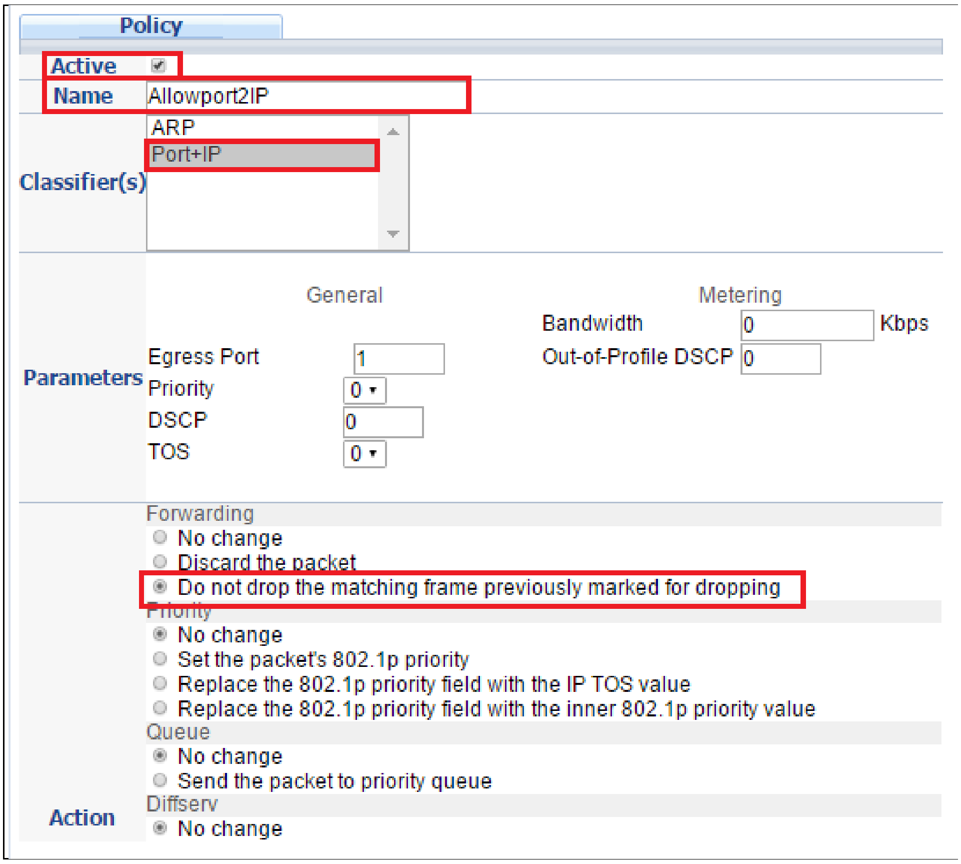
Priority
● No change
○ Set the packet's 802.1p priority
○ Replace the 802.1p priority field with the IP TOS value
○ Replace the 802.1p priority field with the inner 802.1p priority value

Queue
● No change
○ Send the packet to priority queue

Diffserv
● No change
○ Set the packet's TOS field

2. Select **Active, set Name as “Allowport2IP”, select classifier “Port+IP”** and **select “Do not drop the matching frame previously marked for dropping” in Action,** then click **Add** to run feature.

Figure 6 **Advanced Application > Policy Rule**



Policy

Active ☑

Name Allowport2IP

Classifier(s)
ARP
Port+IP

Parameters

General
Egress Port 1
Priority 0
DSCP 0
TOS 0

Metering
Bandwidth 0 Kbps
Out-of-Profile DSCP 0

Action

Forwarding
○ No change
○ Discard the packet
● Do not drop the matching frame previously marked for dropping

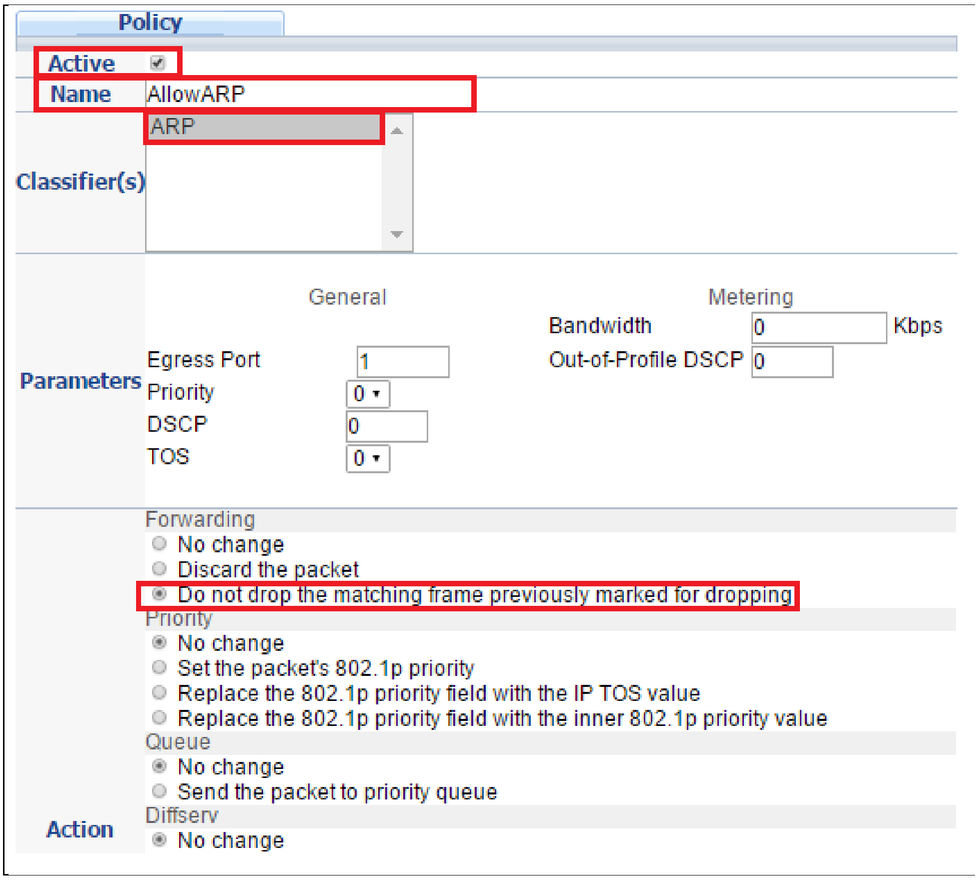
Priority
● No change
○ Set the packet's 802.1p priority
○ Replace the 802.1p priority field with the IP TOS value
○ Replace the 802.1p priority field with the inner 802.1p priority value

Queue
● No change
○ Send the packet to priority queue

Diffserv
● No change

3. Select **Active, set Name as "AllowARP", select classifier "ARP"** and **select "Do not drop the matching frame previously marked for dropping" in Action,** then click **Add** to run feature.

Figure 7 **Advanced Application > Policy Rule**



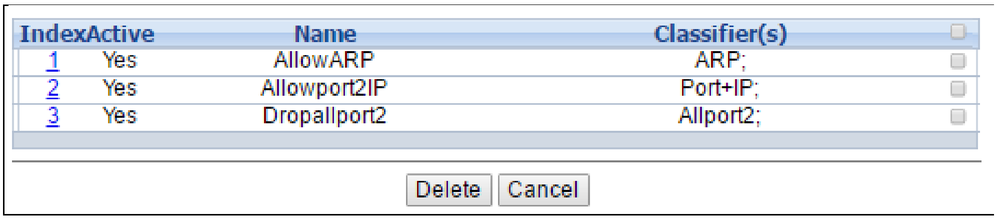
Policy

Active	☑
Name	AllowARP
Classifier(s)	ARP
Parameters	General: Egress Port: 1 Priority: 0 DSCP: 0 TOS: 0 Metering: Bandwidth: 0 Kbps Out-of-Profile DSCP: 0
Action	Forwarding ○ No change ○ Discard the packet ● Do not drop the matching frame previously marked for dropping Priority ● No change ○ Set the packet's 802.1p priority ○ Replace the 802.1p priority field with the IP TOS value ○ Replace the 802.1p priority field with the inner 802.1p priority value Queue ● No change ○ Send the packet to priority queue Diffserv ● No change

Verify

1. In this screen it will display the policy rule status.

Figure 8, **Advanced Application > Policy Rule**

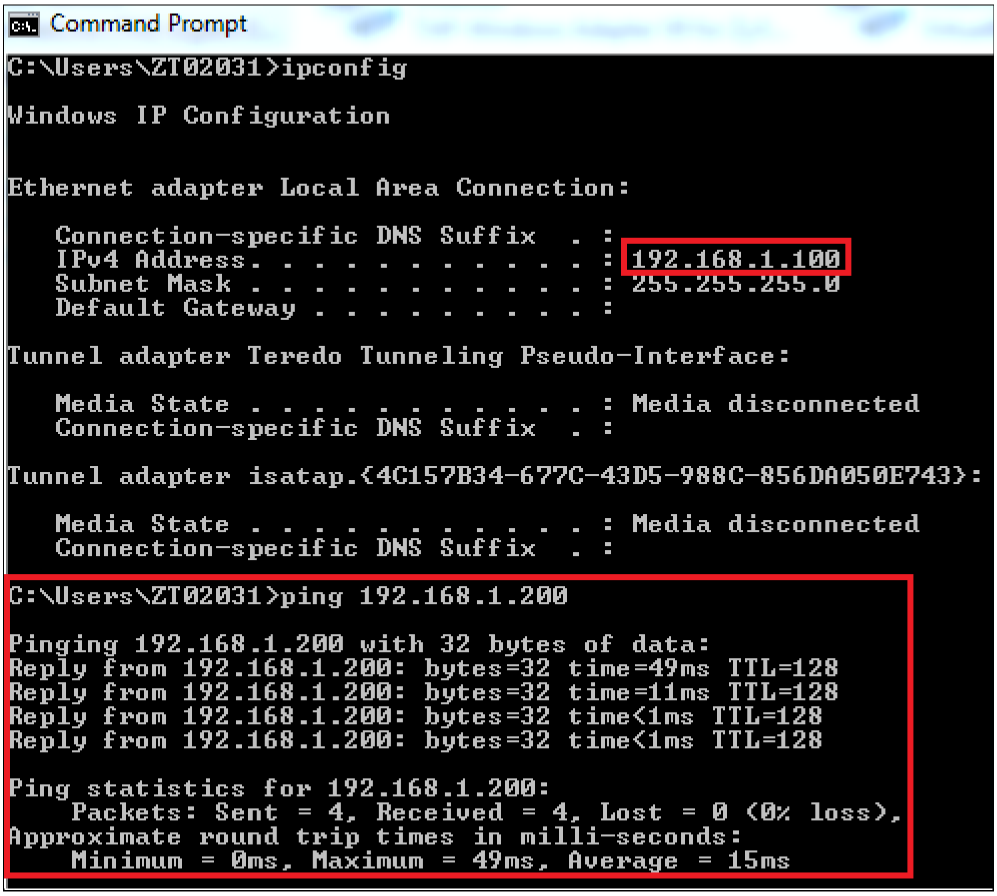


Index	Active	Name	Classifier(s)	□
1	Yes	AllowARP	ARP;	□
2	Yes	Allowport2IP	Port+IP;	□
3	Yes	Dropallport2	Allport2;	□

Verify

1. Connect a PC —A to the Switch on port2. Connect another PC —B to the Switch on port10 with IP 192.168.1.200. First set the IP of PC —A to 192.168.1.100. At this time, PC —A can ping PC —B.

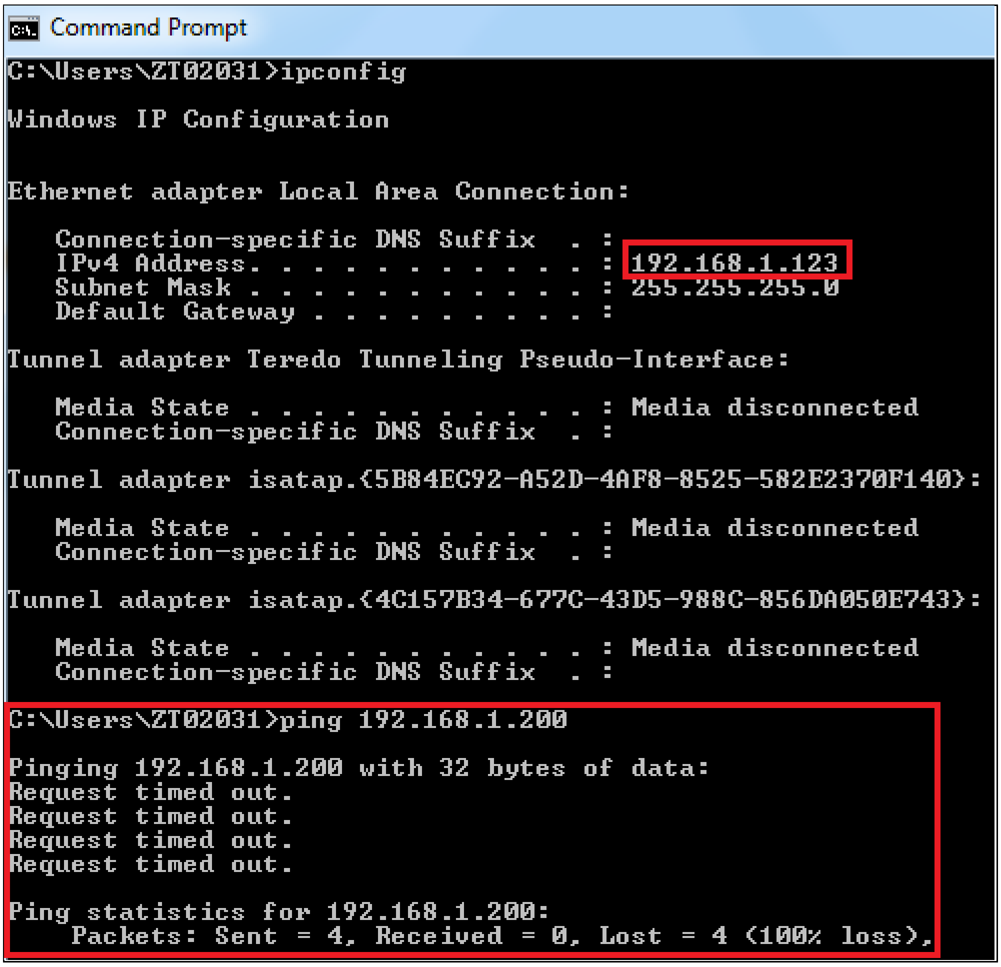
PC —A can ping PC —B



```
C:\Users\ZT02031>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.1.100
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Tunnel adapter Teredo Tunneling Pseudo-Interface:

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

Tunnel adapter isatap.{4C157B34-677C-43D5-988C-856DA050E743}:

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

C:\Users\ZT02031>ping 192.168.1.200

Pinging 192.168.1.200 with 32 bytes of data:
Reply from 192.168.1.200: bytes=32 time=49ms TTL=128
Reply from 192.168.1.200: bytes=32 time=11ms TTL=128
Reply from 192.168.1.200: bytes=32 time<1ms TTL=128
Reply from 192.168.1.200: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.200:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 49ms, Average = 15ms
```

2. However, if you set the IP of PC —A to another IP besides 192.168.1.100, it can no longer ping PC —B.

PC —A can no longer ping PC —B

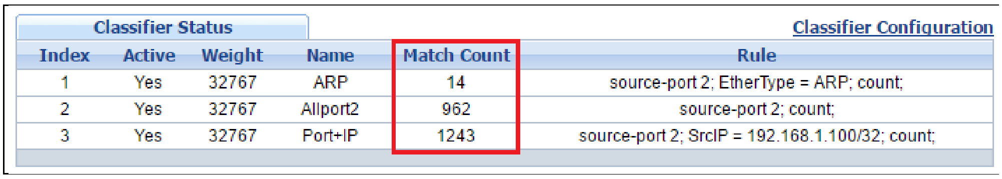


Command Prompt

```
C:\Users\ZT02031>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.1.123
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Tunnel adapter Teredo Tunneling Pseudo-Interface:

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

Tunnel adapter isatap.{5B84EC92-A52D-4AF8-8525-582E2370F140}:

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

Tunnel adapter isatap.{4C157B34-677C-43D5-988C-856DA050E743}:

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

C:\Users\ZT02031>ping 192.168.1.200

Pinging 192.168.1.200 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.200:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

3. You may also know how many packets match the classifiers in Match Count of Classifier Status.

Match Count of Classifier Status



Index	Active	Weight	Name	Match Count	Rule
1	Yes	32767	ARP	14	source-port 2; EtherType = ARP; count;
2	Yes	32767	Allport2	962	source-port 2; count;
3	Yes	32767	Port+IP	1243	source-port 2; SrcIP = 192.168.1.100/32; count;

10.1 Management

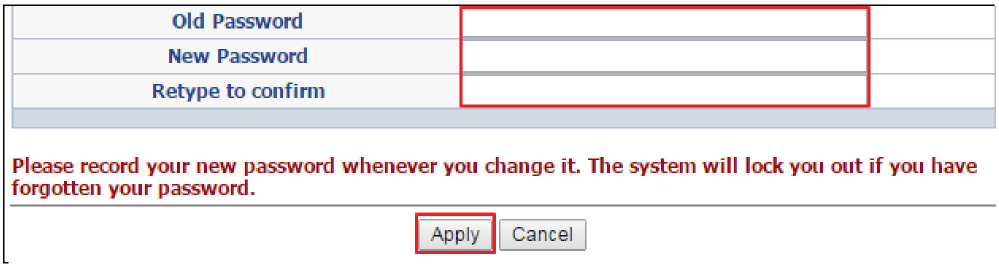
10.1.1 How to change password?

Overview

User can change the switch administrator password.

1. In this screen the highlight part is how the user change the password then clicks **Apply** to save the settings.

Figure 1, **Management > Access Control > Logins**



Old Password	
New Password	
Retype to confirm	

Please record your new password whenever you change it. The system will lock you out if you have forgotten your password.

Verify

1. Please logout the device, and then login again using the new password. It should let you access the WEB GUI website.

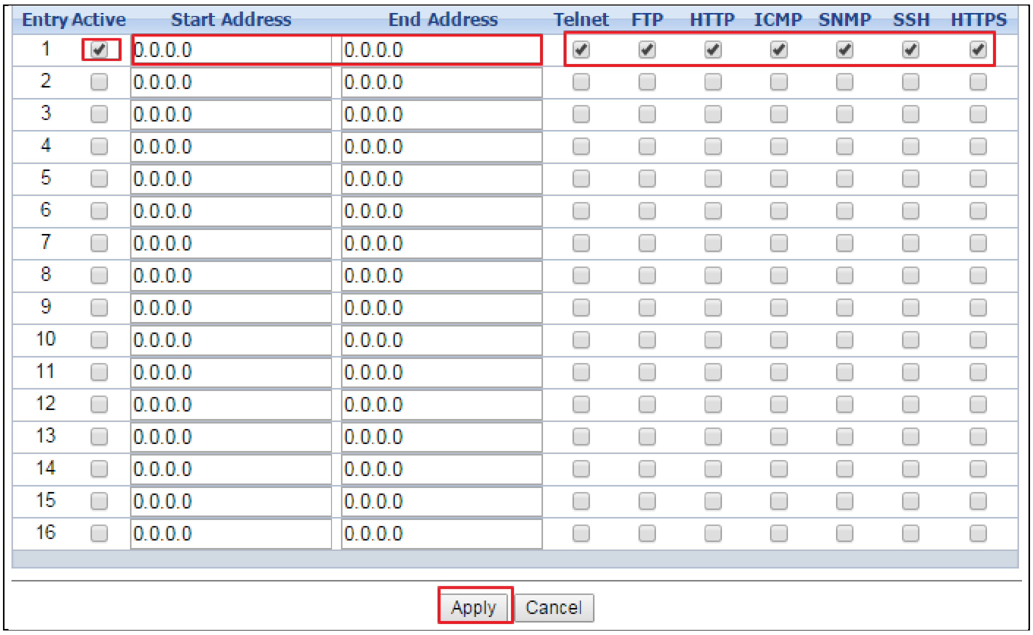
10.1.2 How to configure remote management service?

Overview

Remote management service is to specify a group of one or more “trusted computers” from which an administrator may use a service to manage the Switch.

1. Select and check how many entry want to be **Active.** User can configure the range of an IP address and configure which remote should be use to login to the device.

Figure 1, **Management > Access Control > Remote Management**

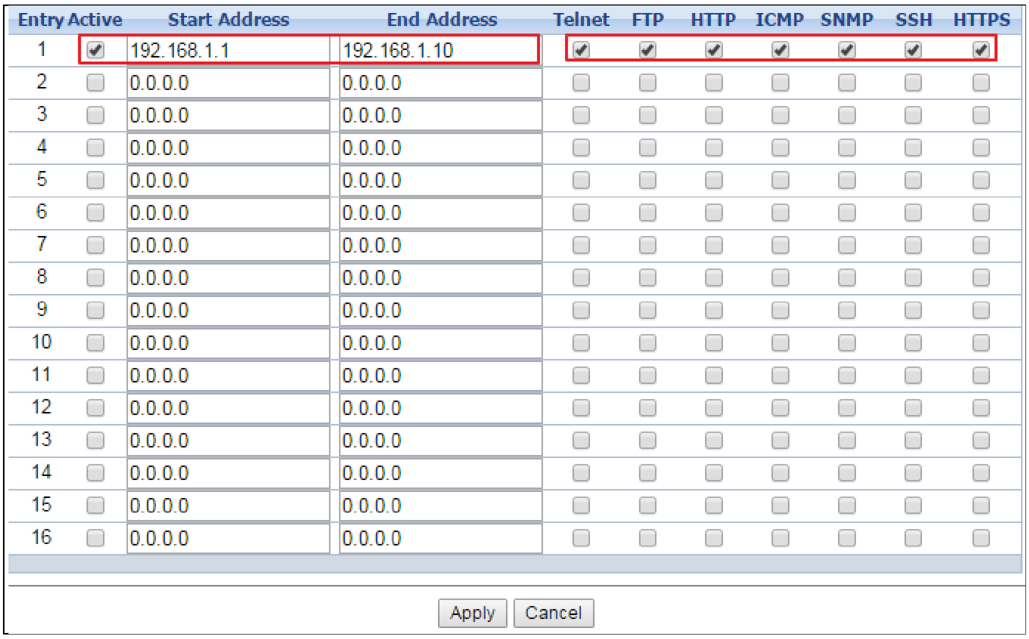


Entry	Active	Start Address	End Address	Telnet	FTP	HTTP	ICMP	SNMP	SSH	HTTPS
1	☑	0.0.0.0	0.0.0.0	☑	☑	☑	☑	☑	☑	☑
2	□	0.0.0.0	0.0.0.0	□	□	□	□	□	□	□
3	□	0.0.0.0	0.0.0.0	□	□	□	□	□	□	□
4	□	0.0.0.0	0.0.0.0	□	□	□	□	□	□	□
5	□	0.0.0.0	0.0.0.0	□	□	□	□	□	□	□
6	□	0.0.0.0	0.0.0.0	□	□	□	□	□	□	□
7	□	0.0.0.0	0.0.0.0	□	□	□	□	□	□	□
8	□	0.0.0.0	0.0.0.0	□	□	□	□	□	□	□
9	□	0.0.0.0	0.0.0.0	□	□	□	□	□	□	□
10	□	0.0.0.0	0.0.0.0	□	□	□	□	□	□	□
11	□	0.0.0.0	0.0.0.0	□	□	□	□	□	□	□
12	□	0.0.0.0	0.0.0.0	□	□	□	□	□	□	□
13	□	0.0.0.0	0.0.0.0	□	□	□	□	□	□	□
14	□	0.0.0.0	0.0.0.0	□	□	□	□	□	□	□
15	□	0.0.0.0	0.0.0.0	□	□	□	□	□	□	□
16	□	0.0.0.0	0.0.0.0	□	□	□	□	□	□	□

Verify

1. In this screen, user can check the remote management configuration.

Figure 2, **Management > Access Control > Remote Management**



Entry	Active	Start Address	End Address	Telnet	FTP	HTTP	ICMP	SNMP	SSH	HTTPS
1	☑	192.168.1.1	192.168.1.10	☑	☑	☑	☑	☑	☑	☑
2	□	0.0.0.0	0.0.0.0	□	□	□	□	□	□	□
3	□	0.0.0.0	0.0.0.0	□	□	□	□	□	□	□
4	□	0.0.0.0	0.0.0.0	□	□	□	□	□	□	□
5	□	0.0.0.0	0.0.0.0	□	□	□	□	□	□	□
6	□	0.0.0.0	0.0.0.0	□	□	□	□	□	□	□
7	□	0.0.0.0	0.0.0.0	□	□	□	□	□	□	□
8	□	0.0.0.0	0.0.0.0	□	□	□	□	□	□	□
9	□	0.0.0.0	0.0.0.0	□	□	□	□	□	□	□
10	□	0.0.0.0	0.0.0.0	□	□	□	□	□	□	□
11	□	0.0.0.0	0.0.0.0	□	□	□	□	□	□	□
12	□	0.0.0.0	0.0.0.0	□	□	□	□	□	□	□
13	□	0.0.0.0	0.0.0.0	□	□	□	□	□	□	□
14	□	0.0.0.0	0.0.0.0	□	□	□	□	□	□	□
15	□	0.0.0.0	0.0.0.0	□	□	□	□	□	□	□
16	□	0.0.0.0	0.0.0.0	□	□	□	□	□	□	□