FSOS

VLAN Configuration

Contents

1. VLAN Configuration....1
1.1 VLAN Overview....1
1.1.1 Vlan Configuration....2
1.1.2 Interface Default vlan ID....2
1.1.3 Interface Type....2
1.1.4 VLAN Attributes Based on Hybrid Interface....4
1.1.5 VLAN Attributes Based on Trunk Interface....4
1.1.6 Configure port priority....5
1.1.7 Ingress Filtering....5
1.1.8 Configure Types of Interface acceptable-frame....6
1.1.9 Configuration Example....6
1.2 MAC-Based VLAN Configuration....10
1.2.1 Overview for MAC-Based VLAN....10
1.2.2 Configure MAC-Based VLAN....10
1.2.3 Configuration Example for MAC-Based VLAN....11
1.3 Protocol-Based VLAN Configuration....13
1.3.1 Overview for Protocol-Based VLAN....13
1.3.2 Configure Protocol-Based VLAN....13
1.3.4 Example for Protocol-Based VLAN....14
1.4 IP-subnet VLAN....15
1.4.1 Overview for IP Subnet-Based VLAN....15
1.4.2 Configure IP Subnet-Based VLAN....15
1.4.3 Configuration Example....16

1. VLAN Configuration

1.1 VLAN Overview

Virtual Local Area Network (VLAN) is the technology which realizing virtual work group through segmenting the LAN devices into every network segment logically but not segmenting the LAN devices into every network segment physically. IEEE issued the IEEE 802.1Q in 1999, which was intended to standardize VLAN implementation solutions.

Network managers can logically segment the physical LAN into different broadcast domains via VLAN technology. Each VLAN contains a group of computer workstation with the same demands. The workstations of a VLAN do not have to belong to the same physical LAN segment. With VLAN technology, the broadcast and unicast traffic within a VLAN will not be forwarded to other VLANs. Therefore, it is very helpful in traffic controlling, saving device investment, simplifying network management and improving security. The following are VLAN features:

Compared with the traditional Ethernet, VLAN enjoys the following advantages.

helpful in traffic controlling

In traditional network, mass broadcast data will be sent to all network devices directly regardless of whether it is necessary or not, leading to network jitter consequently. However, VLAN supports to configure the necessary communication device in each VLAN so as to reduce broadcast and then improve network efficiency.

providing higher security

Device can only communicate with another device under the condition that both of them belongs to the same VLAN. For example, it must be under the help of router device if the VLAN device of Research and Development Department needs to connect with the VLAN device of Product Department. In this way, these two departments cannot communicate directly so as to improve system security function.

reducing network configuration workload

VLAN can be used to group specific hosts. When the physical position of a host changes within the range of the VLAN, you need not change its network configuration.

1.1.1 Vlan Configuration

Operation	Command	Remarks
Enter global configuration mode	configure terminal	-
Create/ delete vlan	(no) vlan *vlan-list*	
Add vlan interface	switchport ethernet ***port-number***	
Specify vlan description	description *string*	

1.1.2 Interface Default vlan ID

Interface default vlan is also called pvid. When receiving a untagged packet, system will add a tag to the packet in which the VLAN ID is the default VLAN ID.

Configure interface default vlan ID

Operation	Command	Remarks
Enter port configuration mode	interface ethernet ***port-number***	-
Configure interface pvid	switchport default vlan ***vlan-id***	optional
Restore default pvid	no switchport default vlan	pvid=1 by default.
Display interface detailed configuration	show interface ethernet ***port-number***	optional
Display interface brief configuration	show interface brief ethernet [***port-number***]	optional

1.1.3 Interface Type

Interface type can be divided into three types according to the different process modes the interface performs on tag label:

Access interface: the interface only belongs to one vlan, and it usually is used to connect the terminal device.

Trunk: the interface can be able to receive and forward multiple vlans. When the message is forwarded, the default vlan message will not carry the tag whereas the other vlan will carry the tag, and the tag is applied to the switch interface.

Hybrid interface: the interface can be able to receive and forward multiple vlans, and it allows multiple vlans to carry the tag or not carry the tag.

<table>
<tr><td rowspan="2">interface type</td><td colspan="2">Processing on receiving message</td><td rowspan="2">Processing on forwarding message</td></tr>
<tr><td>Untag</td><td>Tag</td></tr>
<tr><td>Access</td><td rowspan="3">Receive it and add a tag with VID being equal to PVID.</td><td rowspan="3">If VID of the packet is equal to the port permitted VID, receive it; if VID is different, discard it.</td><td>Strip the Tag and transmit the packet as the VID of the packet is equal to the port permitted VID</td></tr>
<tr><td>Hybrid</td><td>If VID of the packet is equal to the port permitted untag VID, remove the tag and transmit it; If VID of the packet is equal to the port permitted tag VID, keep the tag and transmit it.</td></tr>
<tr><td>Trunk</td><td>If VID of the packet is equal to the port permitted VID, keep the tag and transmit it.</td></tr>
</table>

Configure interface vlan mode

Operation	Command	Remarks
Enter port configuration mode	interface ethernet ***port-number***	-
Configure interface vlan mode	switchport mode **{ access | hybrid | trunk }**	Optional; Hybrid by default.

1.1.4 VLAN Attributes Based on Hybrid Interface

Enter port configuration mode	interface ethernet ***port-number***	-
Configure interface vlan mode	switchport mode **hybrid**	Optional; Hybrid by default
Allow the specified vlan to pass this hybrid port	switchport hybrid {tagged | untagged} vlan { *vlan-list* | *all* }	"tagged attribute" means that the vlan packet carries tag; "untagged attribute" means that the vlan packet does not carry tag;
Does not allow the specified vlan to pass this hybrid port	no switchport hybrid vlan *vlan-list*	

1.1.5 VLAN Attributes Based on Trunk Interface

Enter port configuration mode	interface ethernet ***port-number***	-
Configure interface vlan mode	switchport mode trunk	Optional; Hybrid by default;
Allow the specified vlan to pass this trunk port	switchport trunk allowed vlan { *vlan-list* | *all* }	
Do not allow the specified vlan to pass this trunk port	no switchport trunk allowed vlan { *vlan-list* | *all* }	

1.1.6 Configure port priority

When switch receives a untagged packet, system will add a vlan tag to the packet in which the vid value in the tag is the PVID value and the priority value is the interface priority value.

Configure the interface priority

Operation	Command	Remarks
Enter port configuration mode	interface ethernet ***port-number***	-
Configure port priority	priority ***value***	optional
Restore default priority	no priority	optional 0 by default
Display interface detailed configuration	show interface ethernet ***port-number***	optional
Display interface brief configuration	show interface brief ethernet [***port-number***]	optional

1.1.7 Ingress Filtering

By default, interface will check whether the receiving packet belongs to the vlan member, if it is, the interface will perform the forward processing or it will discard the packet. This process is called ingress filtering. Switch will enable this function by default and this function is allowed to be disabled.

Ingress Filtering

Operation	Command	Remarks
Enter port configuration mode	interface ethernet ***port-number***	-
Configure ingress filtering	[no] ingress filtering	optional Enabled by default
Display the configuration information	show ingress [interface ***port-number***]	optional

1.1.8 Configure Types of Interface acceptable-frame

By default, no matter tag packet or untag packet the switch receives, it allows modifying the packets to be the type that the interface can be received.

Configure Types of Interface acceptable-frame

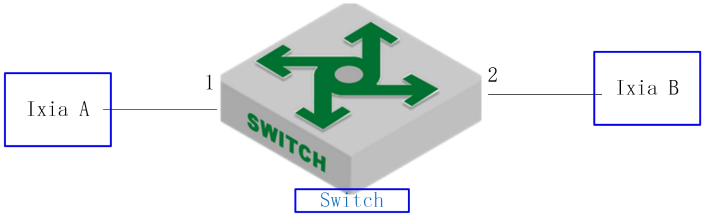
Operation	Command	Remarks
Enter port configuration mode	interface ethernet ***port-number***	-
Configure interface priority	ingress acceptable-frame { **all** | **tagged** }	"all" means it can receive the tag packets and untag packets; "tagged" means it can only receive the tag packets.
Display the configuration information	show ingress [interface ***port-number***]	optional

1.1.9 Configuration Example

Example 1

1.Network requirements

Create vlan 100, including member 1and 2, 1 is access port and 2 is trunk port.



sketch map of interface default vlan

2.Configuration steps

create vlan 100, and then add member 1 and member 2；

Switch(config)#vlan 100

Switch(config-if-vlan)#switchport ethernet 0/0/1 ethernet 0/0/2

modify the vlan mode of port 1 and port 2, and then configure the pvid.
Switch(config)#interface ethernet 0/0/1
Switch(config-if-ethernet-0/0/1)#switchport mode access
Switch(config-if-ethernet-0/0/1)#switchport default vlan 100
Switch(config-if-ethernet-0/0/1)#interface ethernet 0/0/2
Switch(config-if-ethernet-0/0/2)#switchport mode trunk
Switch(config-if-ethernet-0/0/2)#switchport default vlan 100
Switch(config-if-ethernet-0/0/2)#exit

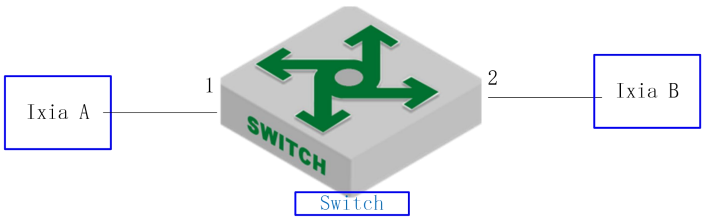
3.Result validation
display the information of port 1 and port 2
Switch(config)#show interface brief ethernet 0/0/1 ethernet 0/0/2

Port	Desc	Link	shutdn	Speed	Pri	PVID	Mode	TagVlan	UtVlan
e0/0/1		up	false	auto-f100	0	100	acc		100
e0/0/2		up	false	auto-f100	0	100	trk		100

Total entries: 2 .

Example 2

1.Network requirements
Configure port 1 to be access mode; configure port 2 to be trunk mode.



sketch map of interface vlan mode

2.Configuration steps
configure port 1 to be access mode;
Switch(config)#interface ethernet 0/0/1
Switch(config-if-ethernet-0/0/1)#switchport mode access

configure port 2 to be trunk mode;
Switch(config-if-ethernet-0/0/1)#interface ethernet 0/0/2
Switch(config-if-ethernet-0/0/2)#switchport mode trunk
Switch(config-if-ethernet-0/0/2)#exit

3.Result validation

display the information of port 1 and port 2:
Switch(config)#show interface brief ethernet 0/0/1 ethernet 0/0/2

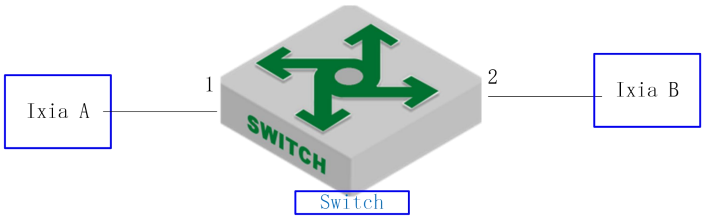
Port	Desc	Link	shutdn	Speed	Pri	PVID	Mode	TagVlan	UtVlan
e0/0/1		up	false	auto-f100	0	1	acc		1
e0/0/2		up	false	auto-f100	0	1	trk		1

Total entries: 2 .

Example 3

1.Network requirements

Create vlan 500, including member 1 and member 2; port 1 and port 2 are hybrid; configure the vlan 500 with tag in egress.



Tag attributes in hybrid egress

2.Configuration steps

configure vlan 500 and add member 1 and member 2;
Switch(config)#vlan 500
Switch(config-if-vlan)#switchport ethernet 0/0/1 ethernet 0/0/2
Switch(config-if-vlan)#show vlan 500
show VLAN information
VLAN ID : 500
VLAN status : static
VLAN member : e0/0/1-e0/0/2.
Static tagged ports :
Static untagged Ports : e0/0/1-e0/0/2.
Dynamic tagged ports :
Total entries: 1 vlan.#

configure vlan 100 with tag in egress of port 1 and port 2;
Switch(config-if-vlan)#interface range ethernet 0/0/1 ethernet 0/0/2
Switch(config-if-range)#switchport hybrid tagged vlan 500

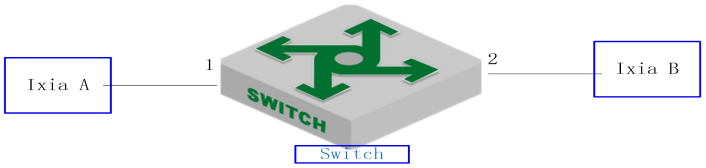
Switch(config-if-range)#show vlan 500
show VLAN information
VLAN ID : 500
VLAN status : static
VLAN member : e0/0/1-e0/0/2.
Static tagged ports : e0/0/1-e0/0/2.
Static untagged Ports :
Dynamic tagged ports :
Total entries: 1 vlan.

3.Result validation
(1) tester A forwards the unknown packet of vlan =500, ixia B can be able to receive the packet of vlan =500 with tag.

Example 4

1.Network requirements

Create vlan 100 and then add member 1 and member 2 ; create vlan 200 and then add member 1 and member 2.



sketch map of adding the port to vlan

2.Configuration steps

create vlan 100 and then add member 1and member 2
Switch(config)#vlan 100
Switch(config-if-vlan)#switchport ethernet 0/0/1 ethernet 0/0/2
Switch(config-if-vlan)#show vlan 100
show VLAN information
VLAN ID : 100
VLAN status : static
VLAN member : e0/0/1-e0/0/2.
Static tagged ports :
Static untagged Ports : e0/0/1-e0/0/2.
Dynamic tagged ports :

create vlan 200 and then add member 1and member 2

```
Switch(config)#vlan 200
Switch(config-if-vlan)#exit
Switch(config-if-range)#interface range ethernet 0/0/1 ethernet 0/0/2
Switch(config-if-range)#switchport hybrid untagged vlan 200
Switch(config-if-range)#show vlan 200
show VLAN information
VLAN ID                    : 200
VLAN status                : static
VLAN member                : e0/0/1-e0/0/2.
Static tagged ports        :
Static untagged Ports      : e0/0/1-e0/0/2.
Dynamic tagged ports       :
Total entries: 1 vlan.
```

1.2 MAC-Based VLAN Configuration

1.2.1 Overview for MAC-Based VLAN

As noted earlier, a single port in the campus network has multiple services, and each service belongs to different VLANs. So the flexible configuration of VLAN under the switch port to identify different services has become a key issue of the campus network management.

In order to solve the above-mentioned problems, the MAC-based VLAN is proposed. MAC (Media Access Control) address is burnt on a Network Interface Card (NIC), also known as the hardware address. It's composed of 48 bits long (6 bytes), 16 hex digits.

MAC-based VLAN is another way to distinguish VLAN that tag of VLAN is added to packet according to the source MAC address. This is often in combination with security technologies (such as 802.1X) to achieve the purpose of the terminal's safety and flexible access.

1.2.2 Configure MAC-Based VLAN

Users should bind the terminal MAC address with VLAN via the command line, and the device will generate a corresponding MAC VLAN table.

Configure MAC-Based VLAN

Operation	Command	Remarks
Enter global configuration mode	**configure terminal**	-
Configure static	**vlan-mac-table** *mac-address vid priority*	required

vlan-mac table		
Delete vlan-mac table	**no vlan-mac-table [***mac-address***]**	optional
Display vlan-mac table	**show vlan-mac-table[***mac-address***]**	any mode

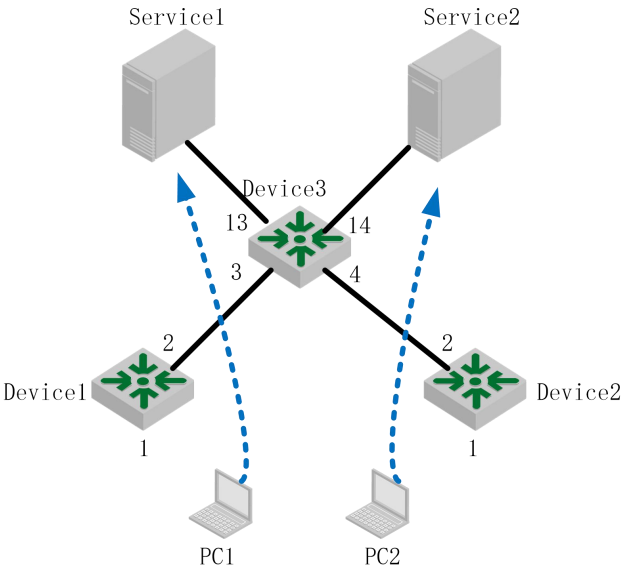
1.2.3 Configuration Example for MAC-Based VLAN

1. Application request

As shown below, port 1 of Device1 and Device2 connects to two meeting rooms respectively; PC1 and PC2 are the laptops which will be used during the meeting.

PC1 and PC2 respectively belong to two departments, and these two departments are isolated by VLAN 100 and VLAN 200. The requirement is that no matter these two laptops are used in which meeting room; they can only access the servers of their own departments, which are server 1 and server 2. The Mac address of PC1 is 00:00:00:00:11:22 and the Mac address of PC2 is 00:00:00:00:11:33.

Network diagram is as follows:



Network diagram for MAC-Based VLAN

2. Configuration steps

(1) Configuration of Device1

create VLAN 100 and VLAN 200, and then configure the port 2 to be trunk port to allow the packet of VLAN 100 and VLAN 200 to pass through.

```
Switch>enable
Switch#configure terminal
Switch(config)#
Switch(config)#vlan 100,200
Switch(config-if-vlan)#exit
Switch(config)#interface ethernet 0/0/2
Switch(config-if-ethernet-0/0/2)#switchport mode trunk
Switch(config-if-ethernet-0/0/2)#switchport trunk allowed vlan 100,200
```

configure port 1 to be hybrid port, and remove the vlan tag when it forwards the packet of VLAN100 and VLAN200.

```
Switch(config)#interface ethernet 0/0/1
Switch(config-if-ethernet-0/0/1)#switchport mode hybrid
Switch(config-if-ethernet-0/0/1)#switchport hybrid untagged vlan 100,200
```

create the MAC address of PC1 associates with VLAN100, create the MAC address of PC2 associates with VLAN200, enable MAC-VLAN function.

```
Switch(config)#vlan-mac-table 00:00:00:00:11:22    100    0
Switch(config)#vlan-mac-table 00:00:00:00:11:33    200    0
```

(2) Configuration of Device2

The configuration of device 2 is totally same as the configuration of device 1, so that won't be covered again here.

Configuration of Device3

create vlan 100 and vlan 200, and then add port 3 and port 4 to these two vlan.

```
Switch(config)#vlan 100,200
Switch(config-if-vlan)#switchport ethernet 0/0/3 ethernet 0/0/4
```

configure port 13 and port 14 to be trunk port to allow the packet of VLAN 100 and VLAN 200 to pass through.

```
Switch(config)#interface range ethernet 0/0/13 ethernet 0/0/14
Switch(config-if-range)#switchport mode trunk
Switch(config-if-range)#switchport trunk allowed vlan 100,200
```

3. Result validation

No matter these two laptops are used in which meeting rooms, they can only access the servers of their own departments

1.3 Protocol-Based VLAN Configuration

1.3.1 Overview for Protocol-Based VLAN

Protocol-based VLAN: the packet distributes different VLAN ID according to the receiving protocol types and encapsulation formats. "Protocol types + encapsulation formats" is also called model agreement. One protocol vlan can be able to bind multiple model agreements. Different model agreements can be distinguished by the vlan-protocol table index. Agreement template is referenced to the port, and then you can modify the packet vlan according to the model agreements.

Untagged packet processing (no vlan tag):

1. If the packet protocol types and encapsulation formats are conform to the model agreements, it will be tagged with the protocol vlan-id.
2. If the packet protocol types and encapsulation formats are not conforming to the model agreements, it will be tagged with the port default VLAN ID.

Tagged packet processing (has vlan tag):

1. If the packet protocol types and encapsulation formats are conform to the model agreements, the outer vlan information will be modified to be the protocol vlan-id.
2. If the packet protocol types and encapsulation formats are not conform to the model agreements, the processing mode will be the same as the port-based vlan.

This feature is mainly applied to bind the service type with VLAN, providing convenient management and maintenance.

There are two types' configuration modes of protocol-based VLAN. Please choose the suitable one according to the equipment type.

1.3.2 Configure Protocol-Based VLAN

Configure Protocol-Based VLAN

Operation	Command	Remarks
Enter global configuration mode	**configure terminal**	-
Configure protocol model	**vlan-protocol frametype {8023-llc-snap|8023-llc|ethernet2}** *ethertype* **interface ethernet** *device/slot/port vlan-id*	required
Delete protocol model	**no vlan-protocol [frametype {8023-llc-snap|8023-llc|ethernet2}** *ethertype* **interface**	optional

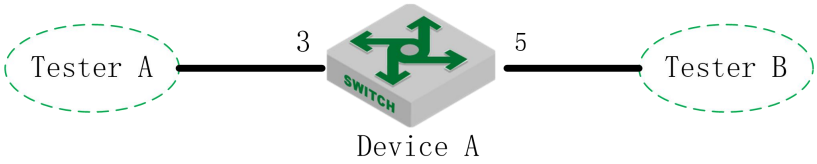
	ethernet *device/slot/port* **]**	
Display the configuration of protocol model	**show vlan-protocol [frametype {8023-llc-snap|8023-llc|ethernet2}** *ethertype* **interface ethernet** *device/slot/port***]**	any mode

1.3.4 Example for Protocol-Based VLAN

1. Network requirements

Create vlan 10, and then configure the protocol model, the model index value is 1, protocol type is 0x0800, with ethernetv2 encapsulation.
It requires the encapsulated IP data flow of ethernetv2 from port 3 add the tag of vlan 10.

Network diagram is as follows:



Network diagram for Protocol-Based VLAN

2. Configuration steps

create protocol vlan 10 and then add it to all ports.
switch(config)#vlan 10
switch(config-if-vlan)#switchport all
Add VLAN port successfully.

configure vlan 10 of port 5 to be tag attribute transmission.
switch(config)#interface ethernet 0/0/5
switch(config-if-ethernet-0/0/5)#switchport hybrid tagged vlan 10
switch(config-if-ethernet-0/0/5)#exit

create protocol model, protocol type to be 0x0800 with ethernetv2 encapsulation
switch(config)#vlan-protocol table index 1 ethertype 0800 protocol ethernetv2

configure the ingress enables the vlan protocol function firstly. Next, bind protocol template index and configure protocol vlan10.

```
switch(config)#interface ethernet 0/0/3
switch(config-if-ethernet-0/0/3)#vlan-protocol
switch(config-if-ethernet-0/0/3)#vlan-protocol table index 1 vlan    10
```

3． Result display and verification:

```
switch(config)#show vlan-protocol table
index    ethertype    protocol
1          0x0800         EthernetV2
switch(config)#show vlan-protocol interface ethernet 0/0/3
e0/0/3: : enable
global protocol-vlan table index 1 vlan 10
```

result: all the ethernetv2 IP data flow entering from port 3 should add vlan 10 tag before transmitting.

1.4 IP-subnet VLAN

1.4.1 Overview for IP Subnet-Based VLAN

IP subnet-based vlan is divided according to packet source IP address and subnet mask. After device received packets from the interface, it will confirm the packets belonging to which VLAN and then automatically divide these packets to specified VLAN to transmit.

This feature is mainly used for the specified IP address or network segment message transmission in the specified VLAN. Currently, our company S5300 BCM series, S5330 BCM series and S6300 - BCM possess this function. Please refer to the corresponding products for more details.

1.4.2 Configure IP Subnet-Based VLAN

IP Subnet-Based VLAN

Operation	Command	Remarks
Enter global configuration mode	**configure terminal**	-
Enable (disable) the VLAN based on IP subnet	**[no]vlan-subnet precede**	required
Configure the table of the VLAN based on IP subnet	**ip-subnet-vlan** *ipaddress mask vlan-id priority*	required

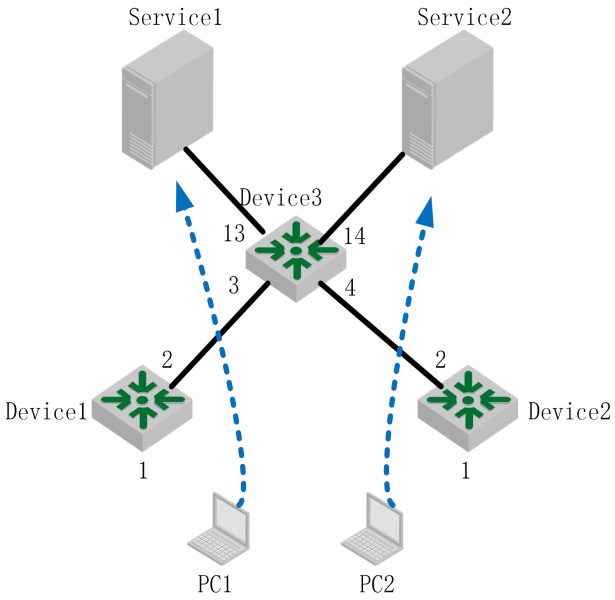
Delete IP subnet table	**no ip-subnet-vlan** *ipaddress mask*	optional
Display IP subnet table	**show ip-subnet-vlan [***ipaddress*| *mask***]**	any mode

1.4.3 Configuration Example

1.Network requirements

An enterprise network allocates IP subnet according to service type. The requirement is that different subnet users adopt different transmission paths to access upstream server.

As shown below:



Network diagram of IP Subnet-Based VLAN

The packets of device1 include data, IPTV, voice and so on. Their IP addresses are different from each other. Configure the IP Subnet-Based VLAN in device 1. After received the service packets, device will automatically divide these packet to specified VLAN according to different source IP. Moreover, device will forward these packets to the upper server.

2. Configuration steps

create VLAN and it should include the interfaces.
Switch(config)#vlan 100,200,300
Switch(config-if-vlan)#switchport ethernet 0/0/1 ethernet 0/0/2 ethernet 0/0/3

enable the vlan based on IP subnet, and then configure the table of IP subnet
Switch(config)#vlan-subnet precede
Switch(config)#ip-subnet-vlan 192.168.1.1 255.255.255.0 100 0

Switch(config)#ip-subnet-vlan 192.168.1.2 255.255.255.0 200 0
Switch(config)#ip-subnet-vlan 192.168.1.3 255.255.255.0 300 0
Switch(config)#
note: please ensure the uplink interface vlan100、vlan200、vlan300 with the tag.

3. Result validation
Switch(config)#show run garp
![GARP]
vlan-subnet precede
ip-subnet-vlan 192.168.1.1 255.255.255.0 100 0
ip-subnet-vlan 192.168.1.2 255.255.255.0 200 0
ip-subnet-vlan 192.168.1.3 255.255.255.0 300 0
Upon testing, the service message can only be transmitted to the specified server.