FSOS

Ethernet Configuration Guide

Contents

Figures

1 Configuring Interface

1.1 Overview

Ethernet interface operate in 10, 100 or 1000 Mbps speed and in full or half duplex mode. The configuration of speed or duplex at combo ports cannot be effective when combo port is working at optical mode.

1.2 Configuring Interface State

1.2.1 Configurations

Switch# configure terminal	Enter the Configure mode
Switch(config)# interface eth-0-1	Specify the interface (eth-0-1) to be configured and enter the Interface mode
Switch(config-if)# no shutdown	Make interface eth-0-1 UP
Switch(config-if)# interface eth-0-2	Specify the interface (eth-0-2) to be configured and enter the Interface mode
Switch(config-if)# shutdown	Shutdown interface eth-0-2
Switch(config)# end	Exit to exec mode
Switch# show interface status	Display interface state

1.2.2 Validation

Switch# show interface status

```
Port        Status      Duplex    Speed     Mode     Type
------------------------------------------------------------
eth-0-1     up          a-full    a-1000    access   1000BASE_T
eth-0-2     admin down  auto      auto      access   1000BASE_T
```

1.3 Configuring Interface Speed

1.3.1 Configurations

Switch# configure terminal	Enter the Configure mode
Switch(config)# interface eth-0-1	Specify the interface (eth-0-1) to be configured and enter the Interface mode
Switch(config-if)# speed 100	Set interface eth-0-1 speed to 100M
Switch(config-if)# no shutdown	Make interface eth-0-1 UP
Switch(config-if)# interface eth-0-2	Specify the interface (eth-0-2) to be configured and enter the Interface mode
Switch(config-if)# no shutdown	Make interface eth-0-2 UP
Switch(config-if)# speed 1000	Set interface eth-0-2 speed to 1000M
Switch(config-if)# interface eth-0-3	Specify the interface (eth-0-3) to be configured and enter the Interface mode
Switch(config-if)# no shutdown	Make interface eth-0-3 UP
Switch(config-if)# speed auto	Set interface eth-0-3 speed to auto negotiation
Switch(config)# end	Exit to exec mode
Switch# show interface status	Display interface speed

1.3.2 Validation

Switch# show interface status

```
Port        Status      Duplex    Speed     Mode     Type
------------------------------------------------------------
eth-0-1     up          a-full    100       access   1000BASE_T
eth-0-2     up          a-full    1000      access   1000BASE_T
eth-0-3     up          a-full    a-1000    access   1000BASE_T
```

1.4 Configuring Interface Duplex

1.4.1 Configurations

Switch# configure terminal	Enter the Configure mode
Switch(config)# interface eth-0-1	Specify the interface (eth-0-1) to be configured and enter the Interface mode
Switch(config-if)# no shutdown	Make interface eth-0-1 UP
Switch(config-if)# duplex full	Set interface eth-0-1 duplex to full

Switch(config-if)# interface eth-0-2	Specify the interface (eth-0-2) to be configured and enter the Interface mode.
Switch(config-if)# no shutdown	Make interface eth-0-2 UP
Switch(config-if)# duplex half	Set interface eth-0-2 duplex to half
Switch(config)# interface eth-0-3	Specify the interface (eth-0-3) to be configured and enter the Interface mode
Switch(config-if)# no shutdown	Make interface eth-0-3 UP
Switch(config-if)# duplex auto	Set interface eth-0-3 duplex to auto negotiation
Switch(config-if)# end	Exit to exec mode
Switch# show interface status	Display interface duplex

1.4.2 Validation

Switch# show interface status

```
Port        Status      Duplex    Speed     Mode     Type
-------------------------------------------------------------
eth-0-1     up          full      a-1000    access   1000BASE_T
eth-0-2     up          half      a-100     access   1000BASE_T
eth-0-3     up          a-full    a-1000    access   1000BASE_T
```

2 Configuring Layer3 Interfaces

2.1 Overview

3 types of Layer3 interface are supported:

- VLAN interfaces: You should configure VLAN interfaces for any VLANs for which you want to route traffic. VLAN interfaces are created when you enter a VLAN ID following the interface vlan global configuration command. To delete a VLAN interface, use the no interface vlan in global configuration command.
- Routed Ports: Ports are physical ports configured to be in Layer 3 mode by using the no switchport in interface configuration command.
- Layer 3 Link Aggregation Ports: Link Aggregation interfaces made up of routed ports.

A Layer 3 switch can have an IP address assigned to each routed port and VLAN interface. All Layer 3 interfaces require an IP address to route traffic. This section shows how to configure an interface as a Layer 3 interface and how to assign an IP address to an interface.

2.2 Configuring Routed Port

This chapter describes configuring routed port and using them. All physical interfaces can be configured as routed port by using the no switchport in interface configuration command. Follow these steps to configure a routed port.

2.2.1 Configurations

Switch# configure terminal	Enter the Configure mode
Switch(config)# interface eth-0-1	Specify the interface (eth-0-1) to be configured and enter the Interface mode
Switch(config-if)# no switchport	Configure on physical port only, change this port to Layer3 interface
Switch(config-if)# no shutdown	Enable this interface
Switch(config-if)# ip address 1.1.1.1/24	Configure IP address to 1.1.1.1/24
Switch(config-if)# end	Return to privileged EXEC mode
Switch# show ip interface brief	Verify the configuration

2.2.2 Validation

Switch# show ip interface brief

```
Interface              IP-Address      Status                Protocol
eth-0-1                 1.1.1.1         up                      up
Switch# show ip interface
Interface eth-0-1
  Interface current state: UP
  Internet address(es):
    1.1.1.1/24 broadcast 1.1.1.255
  Joined group address(es):
    224.0.0.1
  The maximum transmit unit is 1500 bytes
  ICMP error messages limited to one every 1000 milliseconds
  ICMP redirects are always sent
ICMP unreachables are always sent
  ICMP mask replies are always sent
  ARP timeout 01:00:00,  ARP retry interval 1s
  VRRP master of :  VRRP is not configured on this interface
```

2.3 Configuring VLAN Interfaces

This chapter describes configuring VLAN interfaces and using them. Several Virtual LAN (VLAN) interfaces can be configured on a single Ethernet interface. Once created, a VLAN interface functions the same as any physical interface, and it can be configured and displayed like any physical interface. Routing protocols, such as, RIP, OSPF and BGP can run across networks using VLAN interfaces.

2.3.1 Configurations

Switch# configure terminal	Enter the Configure mode
Switch(config)# vlan database	Enter VLAN database mode
Switch(config-vlan)# vlan 10	Create VLAN 10
Switch(config-vlan)# exit	Exit the VLAN database mode and enter the Configure mode
Switch(config)# interface eth-0-2	Specify the interface (eth-0-2) to be configured and enter the Interface mode
Switch(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode
Switch(config-if)# switchport trunk allowed vlan all	Enable all VLAN IDs on this port
Switch(config-if)# no shutdown	Enable the interface
Switch(config-if)# exit	Exit the Interface mode and enter the Configure mode
Switch(config)# interface vlan10	Specify the interface vlan10 to be configured and enter the Interface mode

Switch(config-if)# ip address 2.2.2.2/24	Configure IP address to 2.2.2.2/24
Switch(config-if)# end	Return to privileged EXEC mode
Switch# show ip interface brief	Verify the configuration

2.3.2 Validation

Switch# show ip interface brief

```
Interface              IP-Address      Status                Protocol
vlan10                 2.2.2.2         up                    up
```

Switch# show ip interface

```
Interface vlan10
  Interface current state: UP
  Internet address(es):
    2.2.2.2/24 broadcast 2.2.2.255
  Joined group address(es):
    224.0.0.1
  The maximum transmit unit is 1500 bytes
  ICMP error messages limited to one every 1000 milliseconds
  ICMP redirects are always sent
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are always sent
  ARP timeout 01:00:00,  ARP retry interval 1s
  VRRP master of :  VRRP is not configured on this interface
```

3 Configuring Interface Errdisable

3.1 Overview

Errdisable is a mechanism to protect the system through shutdown the abnormal interface. If an interface enters errdisable state, there are two ways to recovery it from errdisabled state. The first one is to enable errdisable recovery of this reason before errdisable detection; the interface will be recovered automatically after the configured time. But if errdisable occurred first, then errdisable recovery is enabled, the errdisable will not be recovered automatically. The secondary one is configuring “no shutdown” command on the errdisabled interface.

The flap of interface link state is a potential error caused by hardware or line problem. The administrator can also configure the detection conditions for interface link flap.

3.2 Configuring Errdisable Detection

Switch# configure terminal	Enter the Configure mode
Switch(config)# errdisable detect reason link-flap	Enable detect link flap errdisable
Switch(config)# end	Exit to exec mode
Switch# show errdisable detect	Display errdisable detect

Switch# show errdisable detect

```
ErrDisable Reason          Detection status
-----------------          ----------------
bpduguard                  Enabled
bpduloop                   Enabled
link-monitor-failure       Enabled
oam-remote-failure         Enabled
port-security              Enabled
link-flap                  Enabled
udld                       Enabled
fdb-loop                   Enabled
```

3.3 Configuring Errdisable Recovery

Switch# configure terminal	Enter the Configure mode
Switch(config)# errdisable recovery reason link-flap	Enable link flap errdisable recovery
Switch(config)# errdisable recovery interval 30	Set recovery interval
Switch(config)# end	Exit to exec mode
Switch# show errdisable recovery	Display errdisable recovery

Switch# show errdisable recovery

```
ErrDisable Reason          Timer Status
-----------------          --------------
bpduguard                  Disabled
bpduloop                   Disabled
link-monitor-failure       Disabled
oam-remote-failure         Disabled
port-security              Disabled
link-flap                  Enabled
udld                       Disabled
fdb-loop                   Disabled

Timer interval: 30 seconds
```

3.4 Configuring Errdisable Flap

Switch# configure terminal	Enter the Configure mode
Switch(config)# errdisable flap reason link-flap 20 60	Set link flap condition is 20 times in 60 seconds
Switch(config)# end	Exit to exec mode
Switch# show errdisable flap	Display errdisable flap

Switch# show errdisable flap

```
ErrDisable Reason          Flaps     Time (sec)
-----------------          ------    ----------
link-flap                  20        60
```

3.5 Checking Errdisable Status

Administrator can check the interface errdisable status though two commands.

Switch# show errdisable recovery	Display errdisable recovery

Switch# show interface status	Display interface status

If link flap errdisable is enabled recovery, the command will display the left time for recovery; otherwise, will display “unrecovery”.

Case 1: recovery errdisable

Switch# show errdisable recovery

```
ErrDisable Reason          Timer Status
-----------------          --------------
bpduguard                  Disabled
bpduloop                   Disabled
link-monitor-failure       Disabled
oam-remote-failure         Disabled
port-security              Disabled
link-flap                  Enabled
udld                       Disabled
fdb-loop                   Disabled

Timer interval: 30 seconds

Interfaces that will be enabled at the next timeout:
Interface Errdisable Reason Time Left(sec)
--------- ----------------- --------------
eth-0-3   link-flap         25
```

Case 2: unrecovery errdisable

Switch# show errdisable recovery

```
ErrDisable Reason          Timer Status
-----------------          --------------
bpduguard                  Disabled
bpduloop                   Disabled
link-monitor-failure       Disabled
oam-remote-failure         Disabled
port-security              Disabled
link-flap                  Disabled
udld                       Disabled
fdb-loop                   Disabled

Timer interval: 300 seconds
```

The interface status command will also display brief information to indicate interface errdisable state.

Switch# show interface status

```
Port       Status       Duplex    Speed     Mode     Type          Description
--------------------------------------------------------------------------------
eth-0-1    up           a-full    a-1000    TRUNK    1000BASE_SX
eth-0-2    down         auto      auto      TRUNK    Unknown
eth-0-3    errdisable   a-full    a-1000    TRUNK    1000BASE_SX
eth-0-4    down         auto      auto      ACCESS   Unknown
```

4 Configuring MAC Address Table

4.1 Overview

MAC address table contains address information for the switch to forward traffic between ports. The address table includes these types of address:

- Dynamic address: the source address learnt by the switch and will be aged after aging time if this address is not hit. We only support IVL learning mode.
- Static address: the source address manually added by administrators.

4.2 References

IEEE 802.1D

IEEE 802.1Q

4.3 Terminology

Following is a brief description of terms and concepts used to describe the MAC address table:

IVL: Independent VLAN Learning: for a given set of VLANs, if a given individual MAC Address is learned in one VLAN, it can't be used in forwarding decisions taken for that address relative to any other VLAN in the given set.

SVL: Shared VLAN Learning: for a given set of VLANs, if an individual MAC Address is learned in one VLAN, it can be used in forwarding decisions taken for that address relative to all other VLANs in the given set.

4.4 Configuring Address Aging Time

The aging time is not exact time. If aging time set to N, then the dynamic address will be aged after N~2N interval. The default aging time is 300 seconds.

4.4.1 Topology

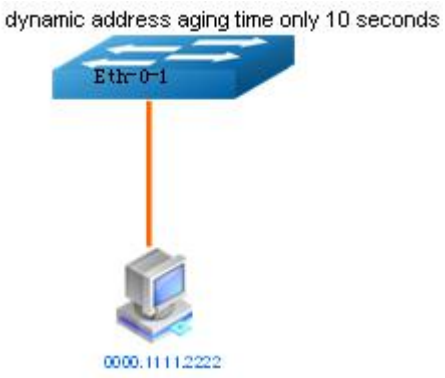

Figure 4-1 Address Aging Time

4.4.2 Configurations

Switch# configure terminal	Enter the Configure mode
Switch(config)# mac-address-table ageing-time 10	Set dynamic address aging time to 10 seconds
Switch(config)# end	Exit to EXEC mode
Switch# show mac address-table ageing-time	Display address aging time

4.4.3 Validation

Switch# show mac address-table ageing-time

```
MAC address table ageing time is 10 seconds
```

4.5 Configuring Static Unicast Address

Unicast address can be only bound to one port.

4.5.1 Topology

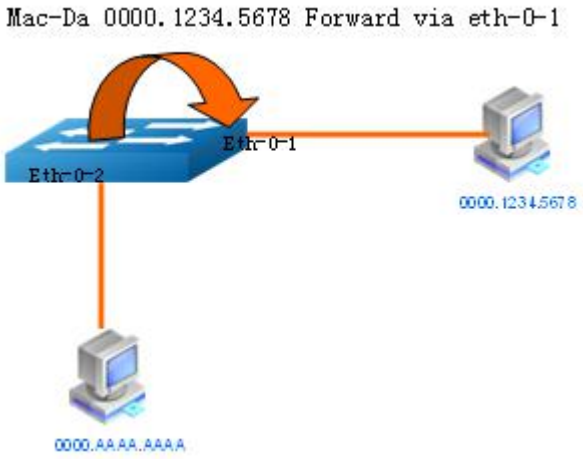

Figure 4-2 Static Unicast Address

4.5.2 Configurations

Switch# configure terminal	Enter the Configure mode
Switch(config)# mac-address-table 0000.1234.5678 forward eth-0-1 vlan 1	Add static unicast address
Switch(config)# end	Exit to EXEC mode
Switch# show mac address-table	Display MAC address table

4.5.3 Validation

Switch# show mac address-table

```
Mac Address Table
-------------------------------------------
(*) - Security Entry
Vlan    Mac Address       Type       Ports
----   --------------   --------   --------
1       0000.1234.5678   static     eth-0-1
```

4.6 Configuring Static Multicast Address

Multicast address can be bound to multi-port.

4.6.1 Topology

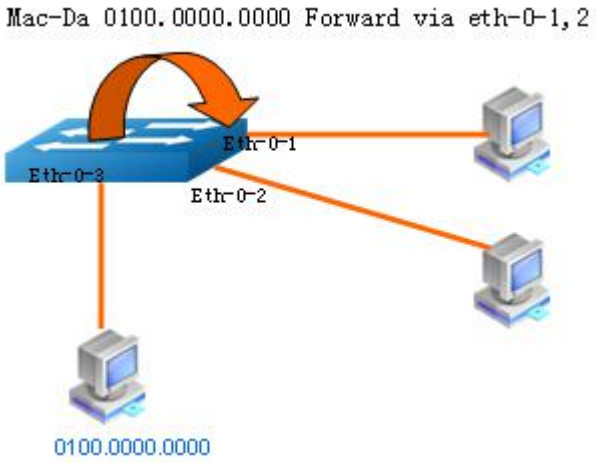

Figure 4-3 Static Multicast Address

4.6.2 Configurations

Switch# configure terminal	Enter the Configure mode
Switch(config)# mac-address-table 0100.0000.0000 forward eth-0-1 vlan 1	Add static multicast address to interface eth-0-1
Switch(config)# mac-address-table 0100.0000.0000 forward eth-0-2 vlan 1	Add static multicast address to interface eth-0-2
Switch(config)# end	Exit to EXEC mode
Switch# show mac address-table	Display MAC address table

4.6.3 Validation

Switch# show mac address-table

```
   Mac Address Table
-------------------------------------------
(*) - Security Entry
Vlan    Mac Address        Type         Ports
----   --------------    -------      -------
1      0100.0000.0000    static       eth-0-1
                                      eth-0-2
```

4.7 Configuring MAC Filter Address

MAC filter will discard these frames whose source or destination address is set to discard. The MAC filter has higher priority than MAC address.

4.7.1 Topology

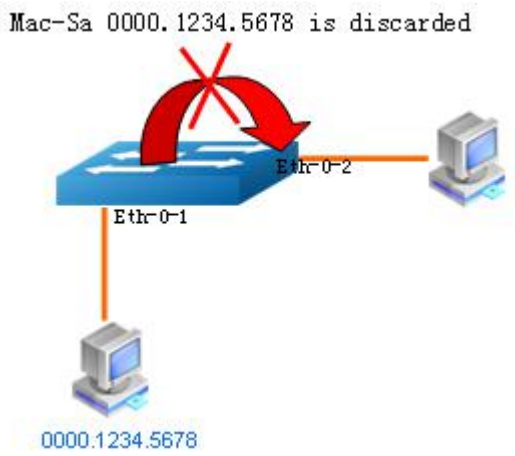

Figure 4-4 MAC filter

4.7.2 Configurations

Switch# configure terminal	Enter the Configure mode
Switch(config)# mac-address-table 0000.1234.5678 discard	Add unicast address to be discarded
Switch(config)# end	Exit to exec mode
Switch# show mac-filter address-table	Display MAC filter address table

4.7.3 Validation

Switch# show mac-filter address-table

```
    MAC Filter Address Table
---------------------------------
Current count          : 1
Max count              : 256
Left count             : 255
 Filter address list   :
---------------------------------
0000.1234.5678
```

5 Configuring VLAN

5.1 Overview

VLAN (Virtual Local Area Network) is a switched network that is logically segmented the network into different broadcast domain so that packets are only switched between ports that are designated for the same VLAN. Each VLAN is considered as a logical network, and packets send to stations that do not belong to the same VLAN must be forwarded through a router.

5.2 References

IEEE 802.1Q

5.3 Terminology

Following is a brief description of terms and concepts used to describe the VLAN:

VID: VLAN identifier

LAN: Local Area Network

VLAN: Virtual LAN

PVID: Port VID, the untagged or priority-tagged frames will be assigned with this VID

Tagged Frame:Tagged Frame is inserted with 4 Bytes VLAN Tag, show in the picture below:

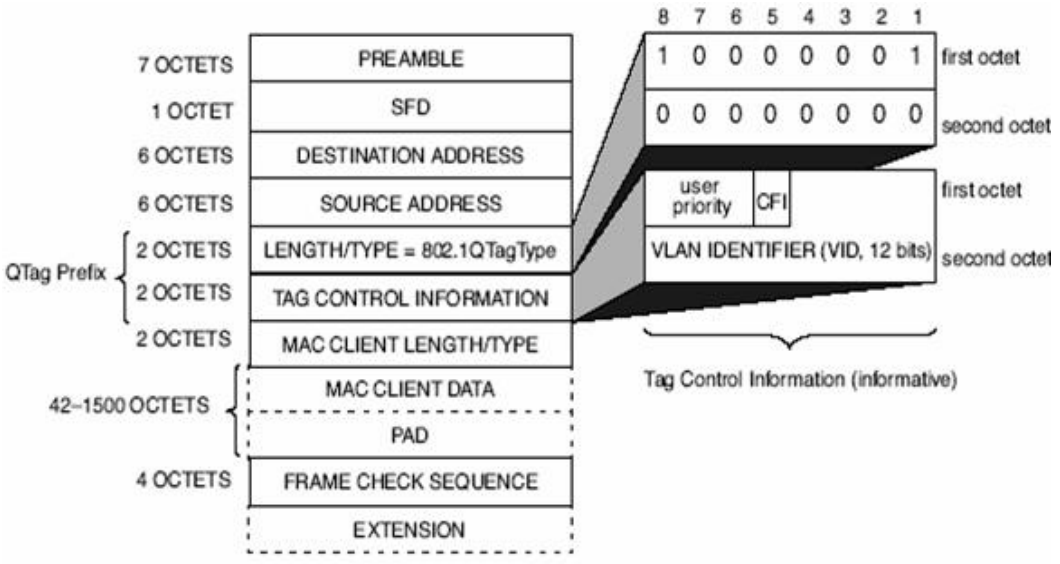

Figure 5-1 VLAN Tagged Frame

Trunk Link:Both tagged and untagged frames can be transmitted on this link. Trunk link allow for multiple VLANs to cross this link.

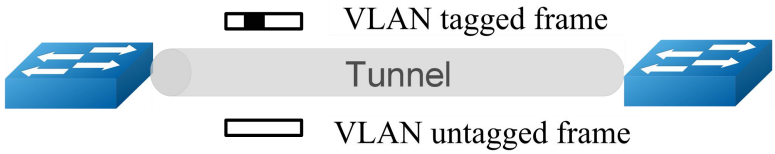

Figure 5-2 Trunk Link

Access Link:Only untagged frames can be transmitted on this link. Access link is at the edge of the network, where end stations attach.

Figure 5-3 Access Link

5.4 Configuring Access Port

Access port only receives untagged or priority-tagged frames, and transmits untagged frames.

5.4.1 Topology

Figure 5-4 Access Port

5.4.2 Configurations

Switch 1

Switch# configure terminal	Enter the Configure mode
Switch(config)# vlan database	Enter the VLAN database mode
Switch(config-vlan)# vlan 2	Create VLAN 2
Switch(config-vlan)# exit	Exit VLAN database mode
Switch(config)# interface eth-0-1	Enter the interface mode
Switch(config-if)# switchport mode access	Set the switching characteristics of this interface to access mode
Switch(config-if)# switchport access vlan 2	Enable VLAN port access by specifying VLAN ID 2 on this interface
Switch(config-if)# end	Exit to exec mode
Switch# show vlan brief	Display vlan's configurations
Switch# show interface switchport interface eth-0-1	Display interface's switch configurations

5.4.3 Validation

Switch# show interface switchport interface eth-0-1

```
Interface name          : eth-0-1
Switchport mode         : access
Ingress filter          : enable
Acceptable frame types  : vlan-untagged only
Default Vlan            : 2
Configured Vlans        :    2
```

Switch# show vlan brief

```
VLAN ID  Name            State    STP ID  DSCP    Member ports
                                                  (u)-Untagged, (t)-Tagged
```

```
======= ================ ======= ======= ======= ========================
1       default          ACTIVE  0       Disable eth-0-2(u) eth-0-3(u)
                                                 eth-0-4(u) eth-0-5(u)
                                                 eth-0-6(u) eth-0-7(u)
                                                 eth-0-8(u) eth-0-9(u)
                                                 eth-0-10(u) eth-0-11(u)
                                                 eth-0-12(u) eth-0-13(u)
                                                 eth-0-14(u) eth-0-15(u)
                                                 eth-0-16(u) eth-0-17(u)
                                                 eth-0-18(u) eth-0-19(u)
                                                 eth-0-20(u) eth-0-21(u)
                                                 eth-0-22(u) eth-0-23(u)
2       VLAN0002         ACTIVE  0       Disable eth-0-1(u)
```

5.5 Configuring Trunk Port

Trunk port receives tagged, untagged, and priority-tagged frames, and transmits both untagged and tagged frames. If trunk port receives an untagged frame, this frame will be assigned to the VLAN of the trunk port's PVID; if a frame send out from the trunk port and the frame's VID is equal to the trunk port's PVID, this frame will be send out without VLAN tag.

5.5.1 Topology

Figure 5-5 Trunk Port

5.5.2 Configurations

Switch 1

Switch# configure terminal	Enter the Configure mode
Switch(config)# vlan database	Enter the VLAN database mode
Switch(config-vlan)# vlan 10,20	Create VLAN 10,20
Switch(config-vlan)# exit	Exit VLAN database mode
Switch(config)# interface eth-0-1	Enter the interface mode
Switch(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode
Switch(config-if)# switchport trunk allowed vlan all	Set this trunk allow all VLANs on this interface

Switch(config-if)# switchport trunk native vlan 10	Set this trunk port's PVID to 10
Switch(config-if)# exit	Exit the interface mode
Switch(config)# interface eth-0-2	Enter the interface mode
Switch(config-if)# switchport mode access	Set the switching characteristics of this interface to access mode
Switch(config-if)# switchport access vlan 10	Enable VLAN port access by specifying VLAN ID 10 on this interface
Switch(config-if)# end	Exit to exec mode
Switch# show vlan brief	Display vlan's configurations
Switch# show interface switchport	Display interface's switch configurations

Switch 2

Switch# configure terminal	Enter the Configure mode
Switch(config)# vlan database	Enter the VLAN database mode
Switch(config-vlan)# vlan 10,20	Create VLAN 10,20
Switch(config-vlan)# exit	Exit VLAN database mode
Switch(config)# interface eth-0-1	Enter the interface mode
Switch(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode
Switch(config-if)# switchport trunk allowed vlan all	Set this trunk port allow all VLANs on this interface
Switch(config-if)# switchport trunk native vlan 10	Set this trunk port's PVID to 10
Switch(config-if)# exit	Exit the interface mode
Switch(config)# interface eth-0-2	Enter the interface mode
Switch(config-if)# switchport mode access	Set the switching characteristics of this interface to access mode
Switch(config-if)# switchport access vlan 10	Enable VLAN port access by specifying VLAN ID 10 on this interface
Switch(config-if)# end	Exit to exec mode
Switch# show vlan brief	Display vlan's configurations
Switch# show interface switchport	Display interface's switch configurations

5.5.3 Validation

Switch 1

Switch# show interface switchport

```
Interface name           : eth-0-1
Switchport mode          : trunk
Ingress filter           : enable
Acceptable frame types   : all
Default Vlan             : 10
Configured Vlans         :    1   10   20
Interface name           : eth-0-2
Switchport mode          : access
Ingress filter           : enable
Acceptable frame types   : vlan-untagged only
Default Vlan             : 10
Configured Vlans         :   10
```

Switch# show vlan brief

```
VLAN ID  Name            State   STP ID  DSCP    Member ports
                                                 (u)-Untagged, (t)-Tagged
======= ================ ======= ======= ======= ========================
1        default          ACTIVE  0       Disable eth-0-1(t) eth-0-3(u)
                                                 eth-0-4(u) eth-0-5(u)
                                                 eth-0-6(u) eth-0-7(u)
                                                 eth-0-8(u) eth-0-9(u)
                                                 eth-0-10(u) eth-0-11(u)
                                                 eth-0-12(u) eth-0-13(u)
                                                 eth-0-14(u) eth-0-15(u)
                                                 eth-0-16(u) eth-0-17(u)
                                                 eth-0-18(u) eth-0-19(u)
                                                 eth-0-20(u) eth-0-21(u)
                                                 eth-0-22(u) eth-0-23(u)
10       VLAN0010         ACTIVE  0       Disable eth-0-1(t) eth-0-2(u)
20       VLAN0020         ACTIVE  0       Disable eth-0-1(t)
```

Switch 2

Switch# show interface switchport

```
Interface name           : eth-0-1
Switchport mode          : trunk
Ingress filter           : enable
Acceptable frame types   : all
Default Vlan             : 10
Configured Vlans         :    1   10   20
Interface name           : eth-0-2
Switchport mode          : access
Ingress filter           : enable
Acceptable frame types   : vlan-untagged only
Default Vlan             : 10
Configured Vlans         :   10
```

Switch# show vlan brief

```
VLAN ID  Name            State   STP ID  DSCP    Member ports
                                                 (u)-Untagged, (t)-Tagged
======= ================ ======= ======= ======= ========================
1        default          ACTIVE  0       Disable eth-0-1(t) eth-0-3(u)
                                                 eth-0-4(u) eth-0-5(u)
                                                 eth-0-6(u) eth-0-7(u)
                                                 eth-0-8(u) eth-0-9(u)
                                                 eth-0-10(u) eth-0-11(u)
                                                 eth-0-12(u) eth-0-13(u)
                                                 eth-0-14(u) eth-0-15(u)
                                                 eth-0-16(u) eth-0-17(u)
                                                 eth-0-18(u) eth-0-19(u)
                                                 eth-0-20(u) eth-0-21(u)
                                                 eth-0-22(u) eth-0-23(u)
10       VLAN0010         ACTIVE  0       Disable eth-0-1(t) eth-0-2(u)
20       VLAN0020         ACTIVE  0       Disable eth-0-1(t)
```

6 Configuring Voice VLAN

6.1 Overview

The voice VLAN feature enables ports to carry IP voice traffic from an IP phone. When the switch is connected to an IP Phone, the IP Phone sends voice traffic and voice traffic's COS values is set to 5 by default.

6.2 Configurations

Switch#configure terminal	Enter the Configure mode
Switch(config)# qos enable	Enable QOS
Switch(config)# vlan database	Enter the VLAN database mode
Switch(config-vlan)# vlan 2	Create VLAN 2
Switch(config-vlan)# exit	Exit VLAN database mode
Switch(config)# voice vlan 2	Set VLAN 2 as VOICE VLAN
Switch(config)# voice vlan mac-address 0055.0000.0000 ffff.ff00.0000 description test	Add an OUI entry for VOICE VLAN
Switch(config)# interface eth-0-1	Enter the interface mode
Switch(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode
Switch(config-if)# switchport trunk allowed vlan all	Set this trunk allow all VLANs on this interface
Switch(config-if)# voice vlan enable	Enable VLOICE VLAN on eth-0-1
Switch(config-if)# interface eth-0-2	Enter the interface mode
Switch(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode
Switch(config-if)# switchport trunk allowed vlan all	Set this trunk allow all VLANs on this interface
Switch(config-if)# replace cos	Replace the COS (enabled by default)

6.3 Validation

Send packet to eth-0-1, the format of the packet send.

```
        0x0000:  0000 0a02 0001 0055 0000 0011 8100 0002  ........k.......
        0x0010:  0800 aadd aadd aadd aadd aadd aadd aadd  ................
        0x0020:  aadd aadd aadd aadd aadd aadd aadd aadd  ................
        0x0030:  aadd aadd aadd aadd aadd aadd            ............
```

Receive packet from eth-0-2,the format of the packet received.

```
        0x0000:  0000 0a02 0001 0055 0000 0011 8100 a002  ........k.......
        0x0010:  0800 aadd aadd aadd aadd aadd aadd aadd  ................
        0x0020:  aadd aadd aadd aadd aadd aadd aadd aadd  ................
        0x0030:  aadd aadd aadd aadd aadd aadd            ............
```

In packet which received on eth-0-2, the COS is replace as **a**.

7 Configuring VLAN Classification

7.1 Overview

VLAN classification is used to define specific rules for directing packets to selected VLANs based on protocol or subnet criteria. Sets of rules can be grouped (one group per interface).

VLAN classification rules have 3 types: mac based, ip based and protocol based. MAC based vlan classification rule will classify packets to specified VLAN according to the source MAC address of incoming packets; IP based vlan classification rule will classify packets according to the source IP address of incoming packets; And protocol based vlan classification rule will classify packets according to the layer3 type of incoming packets. The following layer3 types can be supported: ARP, IP(v4), MPLS, Mcast MPLS, PPPoE, RARP.

Different types of vlan classification rules can be added to same vlan classification group. VLAN classification group can only be applied on switchport. Only one type of vlan classification rules can take effect on one switchport.

7.2 Topology

In this configuration example, three VLAN classifier rules are created:

- Rule 1 is mac based rule, it will classify the packets with MACSA 2222.2222.2222 to vlan 5;
- Rule 2 is ip based rule, it will classify the packets sourced from subnet 1.1.1.1/24 to vlan 5;
- Rule 3 is protocol based rule, it will classify all arp packets to vlan 5.

Add rule 1, rule2, rule3 to group 31. Then apply group 31 to 3 interfaces: eth-0-1, eth-0-2, eth-0-3. These 3 interfaces have different vlan classification type. Eth-0-1 is configured to ip based vlan class, this means only ip based rules can take effect on this interface. Eth-0-2 is configured to mac based vlan class, this means only mac based rules can take effect on this interface. Eth-0-3 is configured to protocol based vlan class, this means only protocol based rules can take effect on this interface.

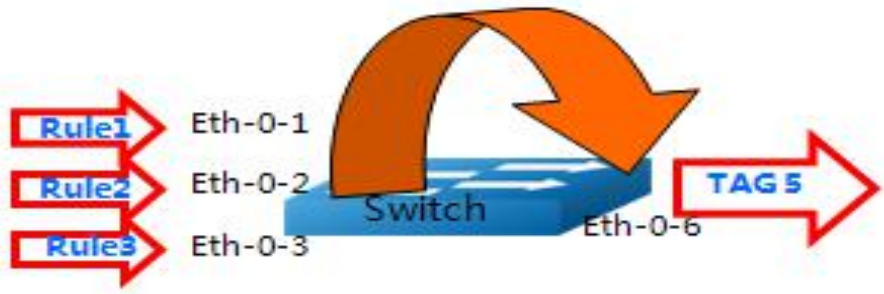

Figure 7-1 VLAN classification Topology

7.3 Configuration

VLANCLASS details

"**show vlan classifier group**" command displays all vlan classification groups, "**show vlan classifier rule**" command displays all vlan classification rules.

Switch# configure terminal	Enter the Configure mode
Switch(config)# vlan database	Enter the VLAN configuration mode
Switch(config-vlan)# vlan 5	Enable vlan5
Switch(config-vlan)# vlan 6	Enable vlan6
Switch(config-vlan)# exit	Exit the vlan configuration mode
Switch(config)# vlan classifier rule 1 mac 2222.2222.2222 vlan 5	Create a mac-based VLAN classifier rule. This rule will class all packets with source MAC 2222.2222.2222 to vlan 5
Switch(config)# vlan classifier rule 2 ip 1.1.1.1/24 vlan 5	Create a subnet-based VLAN classifier rule. This rule will classify all packets with source IP address in the subnet 1.1.1.1/24 to vlan 5
Switch(config)# vlan classifier rule 3 protocol arp vlan 5	Create a protocol-based VLAN classifier rule. This rule will classify all arp packets to vlan 5
Switch(config)# vlan classifier group 31 add rule 1	Create a vlan classifier group 31 and add rule 1 to this group
Switch(config)# vlan classifier group 31 add rule 2	Add rule 2 to group 31
Switch(config)# vlan classifier group 31 add rule 3	Add rule 3 to group 31
Switch(config-if)# end	Return to privileged EXEC mode

Interface details

"**show vlan classifier interface group**" command displays all vlan classification on interface.

Switch# configure terminal	Enter configuration mode
Switch(config)# interface eth-0-1	Enter the interface mode
Switch(config-if)# switchport access vlan 6	Assign PVID 6 to port eth-0-1
Switch(config-if)# switchport access allowed vlan add 5	Allow port eth-0-1 to be memberport of VLAN 5 and receive packets from VLAN 5
Switch(config-if)# vlan classifier activate 31 based ip	Apply group 31 on this port, and set this port's vlan class type to ip-based. Only ip-based vlan class rules in group 31 can take effect on this port
Switch(config-if)# exit	Exit the interface mode
Switch(config)# interface eth-0-2	Enter the interface mode
Switch(config-if)# switchport access vlan 6	Assign PVID6 to port eth-0-2
Switch(config-if)# switchport access allowed vlan add 5	Allow port eth-0-2 to be memberport of VLAN 5 and receive packets from VLAN 5
Switch(config-if)# vlan classifier activate 31 based mac	Apply group 31 on this port, and set this port's vlan class type to mac-based. Only mac-based vlan class rules in group 31 can take effect on this port
Switch(config-if)# exit	Exit the interface mode
Switch(config)# interface eth-0-3	Enter the interface mode
Switch(config-if)# switchport access vlan 6	Assign PVID6 to port eth-0-3
Switch(config-if)# switchport access allowed vlan add 5	Allow port eth-0-3 to be memberport of VLAN 5 and receive packets from VLAN 5
Switch(config-if)# vlan classifier activate 31 based protocol	Apply group 31 on this port and set this port's vlan class type to protocol-based. Only protocol-based vlan class rules in group 1 can take effect on this port
Switch(config-if)# exit	Exit the interface mode
Switch(config)# interface eth-0-6	Enter the interface mode
Switch(config-if)# switchport access vlan 6	Assign PVID6 to port eth-0-6
Switch(config-if)# exit	Exit the interface mode

7.4 Validation

Step 1 Verify the VLAN classifier rules.

Switch# show vlan classifier rule

```
vlan classifier rule 1 mac 2222.2222.2222 vlan 5
vlan classifier rule 2 ip 1.1.1.1/24 vlan 5
vlan classifier rule 3 protocol arp vlan 5
```

Step 2 Verify the VLAN classifier group.

Switch# show vlan classifier group

```
vlan classifier group 31 add rule 1
vlan classifier group 31 add rule 2
vlan classifier group 31 add rule 3
```

Step 3 Verify the VLAN classifier interface.

Switch# show vlan classifier interface group

```
vlan classifier group 31 on interface eth-0-2, based mac
vlan classifier group 31 on interface eth-0-1, based ip
vlan classifier group 31 on interface eth-0-3, based protocol
```

8 Configuring VLAN Maping

8.1 Configuring VLAN Translation

8.1.1 Overview

Service-provider business customers often have specific requirements for VLAN IDs and the number of VLANs to be supported. The VLAN required by different customers in the same service-provider network might overlap, and traffic of customers through the infrastructure might be mixed. Assigning different VIDs to each customer to mapping their own's would bring the traffic from different customers separate.

Using the VLAN translation feature, service providers can use a series of VLANs to support customers who have their own VLANs. Customer VLAN IDs are translated, and traffic from different customers is segregated within the service-provider infrastructure, even when they appear to be on the same VLAN.

8.1.2 Topology

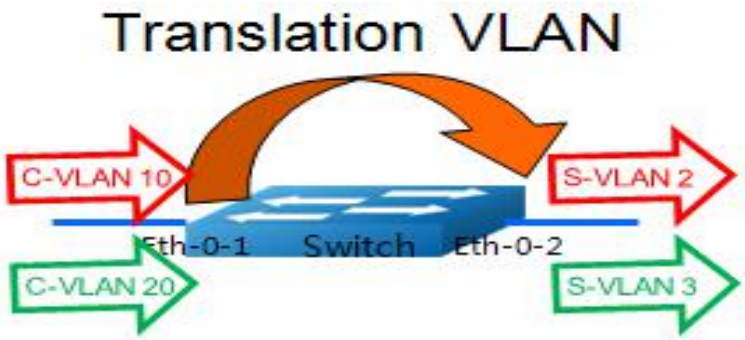

Figure 8-1 VLAN translation

8.1.3 Configuration

Switch# configure terminal	Enter the Configure mode
Switch(config)# vlan database	Enter the VLAN configure mode
Switch(config-vlan)# vlan 2,3	Create VLAN 2,3; These vlans are s-vlan

Switch(config)# ethernet evc evc_c1	Create EVC evc_c1
Switch(config-evc)# dot1q mapped-vlan 2	Set mapped-vlan id to vlan id 2
Switch(config)# ethernet evc evc_c2	Create EVC evc_c2
Switch(config-evc)# dot1q mapped-vlan 3	Set mapped-vlan id to vlan id 3
Switch(config)# vlan mapping table vm	Create vlan mapping table vm
Switch(config-vlan-mapping)# raw-vlan 10 evc evc_c1	Add vlan-mapping entry to vlan mapping table, this entry will map raw packet vlan 10 to processed vlan 2. All incoming packet with vlan id 10 will be translate to vlan 2
Switch(config-vlan-mapping)# raw-vlan 20 evc evc_c2	Add vlan-mapping entry to vlan mapping table, this entry will map raw packet vlan 20 to processed vlan 3. All incoming packet with vlan id 20 will be translate to vlan 3
Switch(config)# interface eth-0-1	Specify the interface (eth-0-1) to be configure and enter the Interface mode
Switch(config-if)# switchport mode trunk	Configure interface to trunk port
Switch(config-if)# switchport trunk vlan-translation	Configure trunk interface to vlan-translation mode
Switch(config-if)# switchport trunk vlan-translation mapping table vm	Apply vlan mapping table vm on current port. The vlan mapping entry in this mapping table will be applied on this port automatically
Switch(config-if)# switchport trunk allowed vlan add 2,3	Add this port to vlan 2,3
Switch(config-if)# interface eth-0-2	Specify the interface (eth-0-2)to be configured and enter the Interface mode
Switch(config-if)# switchport mode trunk	Configure interface to trunk port. This port is used as uplink port
Switch(config-if)# switchport trunk allowed vlan add 2,3	Add this port to vlan 2,3
Switch(config-if)# end	Exit the Interface mode and enter the Exec mode
Switch# show interface switchport interface eth-0-1	Verify the configuration
Switch# show vlan mapping table	Verify vlan mapping table configuration

8.1.4 Validation

This example shows how to configure a switchport to vlan-translation port. You can use show the configuration on the switchport.

Switch# show interface switchport interface eth-0-1

```
Interface name          : eth-0-1
 Switchport mode        : trunk
 VLAN traslation        : enable
 VLAN mapping table     : vm
 Ingress filter         : enable
 Acceptable frame types  : all
 Default Vlan           : 1
 Configured Vlans       : 1    2    3
```

Switch# show vlan mapping table

```
Table Name         EVC Name           Mapped VLAN Raw VLAN
 ================ ================  =========== ======================
vm                 evc_c1            2           10
                   evc_c2            3           20
```

8.2 Configuring 802.1q Tunneling

8.2.1 Overview

802.1Q tunneling expands VLAN space by using a VLAN-in-VLAN hierarchy and tagging the tagged packets, and the maximal VLAN number can reach 4096 × 4096 . Using the 802.1Q tunneling feature, service providers can use a single VLAN to support clients which have multiple VLANs. The ISP usually builds a VLAN model to monitor whole VLAN of backbone network by using GARP or GVRP and accelerate network convergence speed by using STP.

Using 802.1Q tunneling as initial solution is right at first, but it can cause expansibility problem as clients increased. Some clients hope to bring their own VLAN ID which will face two problems. Firstly, the first client's VLAN tag may clash with the other clients. Secondly, the usable tags may be severely limited for the service-provider. The core network will have limits on the 4096 numbers VLAN, if the clients are permitted to use their respective VLAN ID by their own manner.

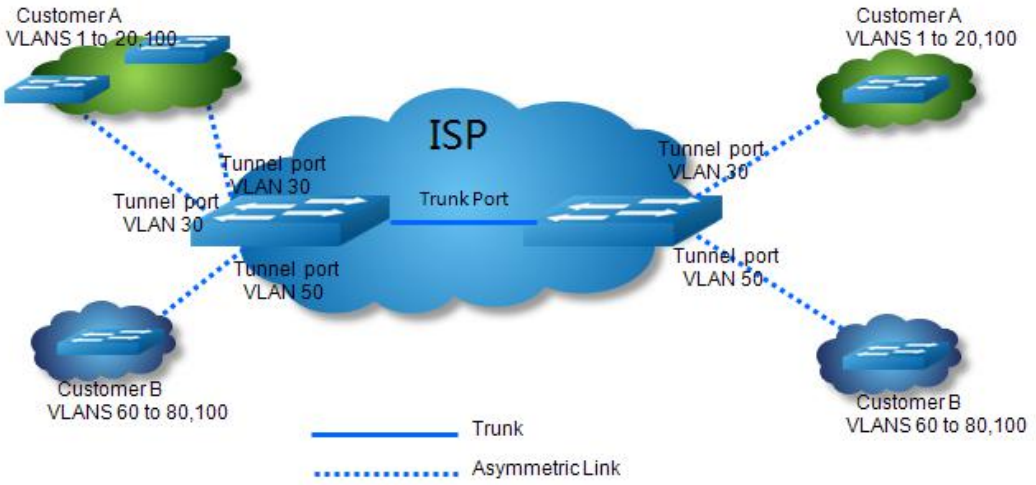

Figure 8-2 802.1Q tunnel

Using 802.1Q tunneling, the client's VLAN tag is encapsulated in the public VLAN tag and packets with two tags will traverse on backbone network. The client's VLAN tag will be shield and only the public VLAN tag will be used to transmit. By separating data stream, the client's VLAN tag is transmitted transparently and different VLAN tags can be used repeatedly. Therefore, using 802.1Q tunneling expands the available VLAN tags.

Two types of 802.1q tunneling are supported: basic 802.1Q tunneling and selective 802.1Q tunneling. Basic 802.1Q tunneling is founded on tagging on ports and all dates will be encapsulated a common VLAN tag of the same port, so this type has great limitations in practical applications. While selective 802.1Q tunneling can separate data stream and encapsulate different VLAN tags base on different data.

8.2.2 Configuring Basic 802.1Q tunneling

Topology

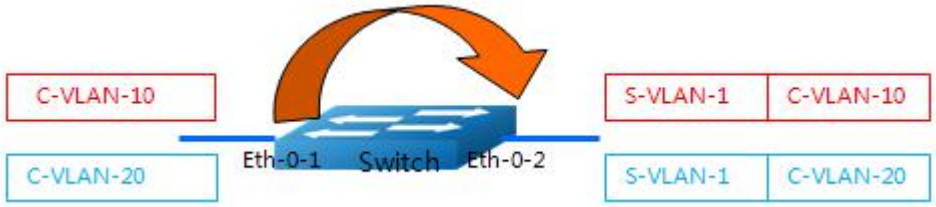

Figure 8-3 Basic 802.1Q tunneling

Configuration

Switch# configure terminal	Enter the Configure mode
Switch(config)# interface eth-0-1	Specify the interface (eth-0-1)to be configured and enter the Interface mode
Switch(config-if)# no shutdown	Enable the interface

Switch(config-if)# switchport mode dot1q-tunnel	Configure this interface to dot1q-tunnel port. By default, dot1q-tunnel port's type is basic
Switch(config-if)# end	Exit the Interface mode and enter the Exec mode
Switch# show interface switchport interface eth-0-1	Verify the configuration

Validation

This example shows how to configure a switchport to basic dot1q-tunnel port. You can use show the configuration on the switchport.

Switch# show interface switchport interface eth-0-1

```
Interface name           : eth-0-1
Switchport mode          : dot1q-tunnel(basic)
Ingress filter           : enable
Acceptable frame types   : all
Default Vlan             : 1
Configured Vlans         : 1
```

8.2.3 Configuring Selective 802.1Q tunneling

Add one tag for incoming untagged packet.

Topology

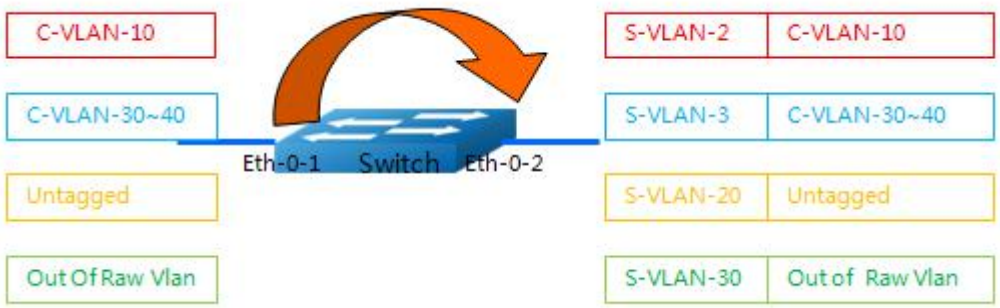

Figure 8-4 Adding one tag

Configuration

Switch# configure terminal	Enter the Configure mode
Switch(config)# vlan database	Enter the VLAN configure mode
Switch(config-vlan)# vlan 2,3,20,30	Create VLAN 2, 3,20, 30; These vlans are s-vlan
Switch(config)# ethernet evc evc_c1	Create EVC evc_c1

Switch(config-evc)# dot1q mapped-vlan 2	Set mapped-vlan id to vlan id 2
Switch(config)# ethernet evc evc_c2	Create EVC evc_c2
Switch(config-evc)# dot1q mapped-vlan 3	Set mapped-vlan id to vlan id 3
Switch(config)# ethernet evc evc_c3	Create EVC evc_c3
Switch(config-evc)# dot1q mapped-vlan 20	Set mapped-vlan id to vlan id 20
Switch(config)# ethernet evc evc_c4	Create EVC evc_c4
Switch(config-evc)# dot1q mapped-vlan 30	Set mapped-vlan id to vlan id 30
Switch(config)# vlan mapping table vm	Create vlan mapping table vm
Switch(config-vlan-mapping)# raw-vlan 10 evc evc_c1	Add vlan-mapping entry to vlan mapping table, this entry will map raw packet vlan 10 to processed vlan 2. All incoming packet with vlan id 10 will be appended with vlan 2
Switch(config-vlan-mapping)# raw-vlan 30-40 evc evc_c2	Add vlan mapping entry to vlan mapping table, these entries will map raw packet vlan 30~40 to processed vlan 3, all incoming packets with vlan-id 30~40 will be appended with vlan 3
Switch(config-vlan-mapping)# raw-vlan untagged evc evc_c3	Add vlan-mapping entry to vlan mapping table, this entry will map untagged packet to vlan 20. All incoming untagged packets will be appended with vlan 20.
Switch(config-vlan-mapping)# raw-vlan out-of-range evc evc_c4	Add vlan-mapping entry to vlan mapping table, these entries will map raw packet not in these entries above to processed vlan 30, all incoming packets not in these entries above will be appended with vlan 30
Switch(config)# interface eth-0-1	Specify the interface (eth-0-1) to be configured and enter the Interface mode
Switch(config-if)# switchport mode dot1q-tunnel	Configure interface to qinq port
Switch(config-if)# switchport dot1q-tunnel type selective	Configure dot1q-tunnel interface to selective mode
Switch(config-if)# switchport dot1q-tunnel vlan mapping table vm	Apply vlan mapping table vm on current port. The vlan mapping entry in this mapping table will be applied on this port automatically
Switch(config-if)# switchport dot1q-tunnel allowed vlan add 2,3,20,30	Add this port to vlan 2,3,20,30
Switch(config-if)# interface eth-0-2	Specify the interface (eth-0-2)to be configured and enter the Interface mode
Switch(config-if)# switchport mode trunk	Configure interface to trunk port. This port is used as uplink port

Switch(config-if)# switchport trunk allowed vlan add 2,3,20,30	Add this port to vlan 2,3,20,30
Switch(config-if)# end	Exit the Interface mode and enter the Exec mode.
Switch# show interface switchport interface eth-0-1	Verify the configuration
Switch# show vlan mapping table	Verify vlan mapping table configuration

Validation

This example shows how to configure a switchport to selective dot1q-tunnel port. You can use show the configuration on the switchport.

Switch# show interface switchport interface eth-0-1

```
Interface name           : eth-0-1
Switchport mode          : dot1q-tunnel(selective)
VLAN mapping table       : vm
Ingress filter           : enable
Acceptable frame types   : all
Default Vlan             : 1
Configured Vlans         : 1    2    3    20   30
```

Switch# show vlan mapping table

```
Table Name       EVC Name          Mapped VLAN Raw VLAN
================ ================ =========== ============================
vm               evc_c1            2           10
                 evc_c2            3           30-40
                 evc_c3            20          untagged
                 evc_c4            30          out-of-range
```

Add two tags for incoming untagged packet

Topology

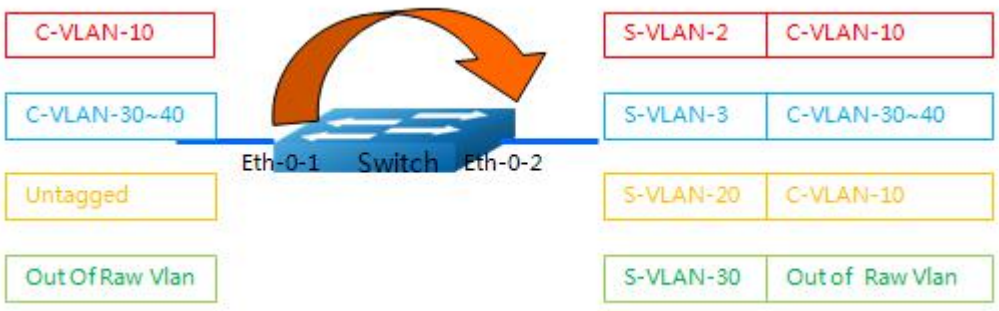

Figure 8-5 Adding two tags

Configuration

Switch# configure terminal	Enter the Configure mode
Switch(config)# vlan database	Enter the VLAN configure mode
Switch(config-vlan)# vlan 2,3,10,20,30	Create VLAN 2, 3,20, 30; These vlans are s-vlan
Switch(config)# ethernet evc evc_c1	Create EVC evc_c1
Switch(config-evc)# dot1q mapped-vlan 2	Set mapped-vlan id to vlan id 2
Switch(config-evc)# exit	Exit evc configuration mode
Switch(config)# ethernet evc evc_c2	Create EVC evc_c2
Switch(config-evc)# dot1q mapped-vlan 3	Set mapped-vlan id to vlan id 3
Switch(config-evc)# exit	Exit evc configuration mode
Switch(config)# ethernet evc evc_c3	Create EVC evc_c3
Switch(config-evc)# dot1q mapped-double-vlan 10 20	Set mapped inner vlan id to 10 and outer vlan id to 20
Switch(config-evc)# exit	Exit evc configuration mode
Switch(config)# ethernet evc evc_c4	Create EVC evc_c4
Switch(config-evc)# dot1q mapped-vlan 30	Set mapped-vlan id to vlan id 30
Switch(config-evc)# exit	Exit evc configuration mode
Switch(config)# vlan mapping table vm	Create vlan mapping table vm
Switch(config-vlan-mapping)# raw-vlan 10 evc evc_c1	Add vlan-mapping entry to vlan mapping table, this entry will map raw packet vlan 10 to processed vlan 2. All incoming packet with vlan id 10 will be appended with vlan 2
Switch(config-vlan-mapping)# raw-vlan 30-40 evc evc_c2	Add vlan mapping entry to vlan mapping table, these entries will map raw packet vlan 30~40 to processed vlan 3, all incoming packets with vlan-id 30~40 will be appended with vlan 3
Switch(config-vlan-mapping)# raw-vlan untagged evc evc_c3	Add vlan-mapping entry to vlan mapping table, this entry will map untagged packet to inner vlan 10 and outer vlan 20. All incoming untagged packets will be appended with vlan 10 and 20
Switch(config-vlan-mapping)# raw-vlan out-of-range evc evc_c4	Add vlan-mapping entry to vlan mapping table, these entries will map raw packet not in these entries above to processed vlan 30, all incoming packets not in these entries above will be appended with vlan 30
Switch(config-vlan-mapping)# exit	Exit vlan mapping configuration mode
Switch(config)# interface eth-0-1	Specify the interface (eth-0-1) to be configured and enter the Interface mode

Switch(config-if)# switchport mode dot1q-tunnel	Configure interface to qinq port
Switch(config-if)# switchport dot1q-tunnel type selective	Configure dot1q-tunnel interface to selective mode
Switch(config-if)# switchport dot1q-tunnel vlan mapping table vm	Apply vlan mapping table vm on current port. The vlan mapping entry in this mapping table will be applied on this port automatically
Switch(config-if)# switchport dot1q-tunnel native inner-vlan 10	Configure inner native vlan 10 to strip inner vlan when packet's inner vlan equals 10
Switch(config-if)# switchport dot1q-tunnel allowed vlan add 2,3,20,30	Add this port to vlan 2,3,20,30
Switch(config-if)# exit	Exit interface configuration mode
Switch(config)# interface eth-0-2	Specify the interface (eth-0-2)to be configured and enter the Interface mode
Switch(config-if)# switchport mode trunk	Configure interface to trunk port. This port is used as uplink port
Switch(config-if)# switchport trunk allowed vlan add 2,3,20,30	Add this port to vlan 2,3,20,30
Switch(config-if)# end	Exit the Interface mode and enter the Exec mode
Switch# show interface switchport interface eth-0-1	Verify the configuration
Switch# show vlan mapping table	Verify vlan mapping table configuration

Validation

This example shows how to configure a switchport to selective dot1q-tunnel port. You can use show the configuration on the switchport.

Switch# show interface switchport interface eth-0-1

```
Interface name           : eth-0-1
Switchport mode          : dot1q-tunnel(selective)
VLAN mapping table       : vm
Ingress filter           : enable
Acceptable frame types   : all
Default Vlan             : 10
Configured Vlans         : 1    2    3    20   30
```

Switch# show vlan mapping table

```
Table Name       EVC Name         Mapped VLAN Raw VLAN
================ ================ =========== ================================
vm               evc_c1           2           10
                 evc_c2           3           30-40
                 evc_c3           20(10)      untagged
                 evc_c4           30          out-of-rang
```

9 Configuring Link Aggregation

9.1 Overview

This chapter contains a sample configuration of Link Aggregation Control Protocol (LACP) . LACP is based on the 802.3ad IEEE specification. It allows bundling of several physical interfaces to form a single logical channel providing enhanced performance and redundancy. The aggregated interface is viewed as a single link to each switch. The spanning tree views it as one interface. When there is a failure in one physical interface, the other interfaces stay up and there is no disruption. This implementation supports the aggregation of maximum 16 physical Ethernet links into a single logical channel. LACP enables our device to manage link aggregation group between other devices that conform to the 802.3ad protocol. By using the LACP, the switch learns the identity of partners supporting LACP and the capabilities of each port. It then dynamically groups ports with same properties into a single logical bundle link.

9.2 References

The LACP is based on :

IEEE 802.3ad

9.3 Configure channel-group

9.3.1 Topology

In this example, 3 links are configured between the two switches S1 and S2. These three links are assigned the same administrative key (1) so that they aggregate to form a single channel 1.

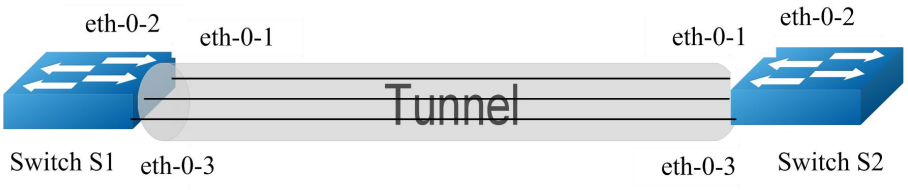

Figure 9-1 LACP

9.3.2 Configuration

Switch 1

Switch1# configure terminal	Enter the Configure mode
Switch1(config)# lacp system-priority 2000	Set the system priority of this switch. This priority is used for determining the system that is responsible for resolving conflicts in the choice of aggregation groups. A lower numerical value has a higher priority
Switch1(config)# port-channel load-balance src-mac	Set the load balance by source MAC address
Switch1(config)# interface eth-0-1	Specify the interface (eth-0-1) to be configured and enter the Interface mode
Switch1(config-if)# no shutdown	Enable the interface
Switch1(config-if)# channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system
Switch1(config-if)# exit	Exit the Interface mode and enter the Configure mode
Switch1(config)# interface eth-0-2	Specify the interface (eth-0-2) to be configured and enter the Interface mode
Switch1(config-if)# channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system
Switch1(config-if)# no shutdown	Enable the interface
Switch1(config-if)# exit	Exit the Interface mode and enter the Configure mode
Switch1(config)# interface eth-0-3	Specify the interface (eth-0-3) to be configured and enter the Interface mode
Switch1(config-if)# channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system
Switch1(config-if)# no shutdown	Enable the interface
Switch1(config-if)# end	Return to privileged EXEC mode

Switch 2

Switch2# configure terminal	Enter the Configure mode
Switch2(config)# lacp system-priority 1000	Set the system priority of this switch. This priority is used for determining the system that is responsible for resolving conflicts in the choice of aggregation groups. A lower numerical value has a higher priority
Switch2(config)# interface eth-0-1	Specify the interface (eth-0-1)to be configured and enter the Interface mode
Switch2(config-if)# no shutdown	Enable the interface
Switch2(config-if)# channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system
Switch2(config-if)# exit	Exit the Interface mode and enter the Configure mode
Switch2(config)# interface eth-0-2	Specify the interface (eth-0-2) to be configured and enter the Interface mode
Switch2(config-if)# channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system
Switch2(config-if)# no shutdown	Enable the interface
Switch2(config-if)# exit	Exit the Interface mode and enter the Configure mode
Switch2(config)# interface eth-0-3	Specify the interface (eth-0-3) to be configured and enter the Interface mode
Switch2(config-if)# channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system
Switch2(config-if)# no shutdown	Enable the interface
Switch2(config-if)# end	Return to privileged EXEC mode

9.3.3 Validation

Switch1# show channel-group summary

```
Flags:  s - suspend             H - standby
        D - down/admin down     B - in Bundle
        R - Layer3              S - Layer2
        w - wait                U - in use

Aggregator Name    Protocol       Ports
```

```
----------------+------------+----------------------------------------
agg1(SU)            LACP            eth-0-1(B) eth-0-2(B) eth-0-3(B)
```

Switch1# show interface agg1

```
Interface agg1
  Interface current state: UP
  Hardware is AGGREGATE, address is cce3.33fc.330b (bia cce3.33fc.330b)
  Bandwidth 3000000 kbits
  Index 1025 , Metric 1 , Encapsulation ARPA
  Speed - 1000Mb/s , Duplex - Full  , Media type is Aggregation
  Link speed type is autonegotiation, Link duplex type is autonegotiation
  Input flow-control is off, output flow-control is off
  The Maximum Frame Size is 1534 bytes
  VRF binding: not bound
  Label switching is disabled
  No virtual circuit configured
  ARP timeout 01:00:00,  ARP retry interval 1s
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 2 bits/sec, 0 packets/sec
    13 packets input, 1184 bytes
    Received 0 unicast, 0 broadcast, 0 multicast
    0 runts, 0 giants, 0 input errors, 0 CRC
    0 frame, 0 overrun, 0 pause input
    0 input packets with dribble condition detected
    20 packets output, 2526 bytes
    Transmitted 0 unicast, 0 broadcast, 0 multicast
    0 underruns, 0 output errors, 0 pause output
```

9.4 Configuring Static-channel-group

9.4.1 Topology

In this example, 3 links are configured between the two switches S1 and S2. These three links are assigned the same administrative key (1) so that they aggregate to form a single channel 1.

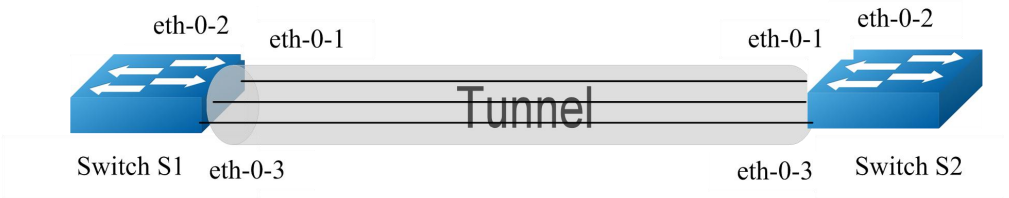

Figure 9-2 LACP

9.4.2 Configuration

Switch 1

Switch1# configure terminal	Enter the Configure mode
Switch1(config)# interface eth-0-1	Specify the interface (eth-0-1) to be configured and enter the Interface mode
Switch1(config-if)# no shutdown	Enable the interface
Switch1(config-if)# static-channel-group 1	Add this interface to channel group 1
Switch1(config-if)# exit	Exit the Interface mode and enter the Configure mode
Switch1(config)# interface eth-0-2	Specify the interface (eth-0-2) to be configured and enter the Interface mode
Switch1(config-if)# static-channel-group 1	Add this interface to channel group 1
Switch1(config-if)# no shutdown	Enable the interface
Switch1(config-if)# exit	Exit the Interface mode and enter the Configure mode
Switch1(config)# interface eth-0-3	Specify the interface (eth-0-3) to be configured and enter the Interface mode
Switch1(config-if)# static-channel-group 1	Add this interface to channel group 1
Switch1(config-if)# no shutdown	Enable the interface
Switch1(config-if)# end	Return to privileged EXEC mode

Switch 2

Switch2# configure terminal	Enter the Configure mode.
Switch2(config)# interface eth-0-1	Specify the interface (eth-0-1)to be configured and enter the Interface mode
Switch2(config-if)# no shutdown	Enable the interface
Switch2(config-if)# static-channel-group 1	Add this interface to channel group 1
Switch2(config-if)# exit	Exit the Interface mode and enter the Configure mode
Switch2(config)# interface eth-0-2	Specify the interface (eth-0-2) to be configured and enter the Interface mode
Switch2(config-if)# static-channel-group 1	Add this interface to channel group 1

Switch2(config-if)# no shutdown	Enable the interface
Switch2(config-if)# exit	Exit the Interface mode and enter the Configure mode
Switch2(config)# interface eth-0-3	Specify the interface (eth-0-3) to be configured and enter the Interface mode
Switch2(config-if)# static-channel-group 1	Add this interface to channel group 1
Switch2(config-if)# no shutdown	Enable the interface
Switch2(config-if)# end	Return to privileged EXEC mode

9.4.3 Validation

Switch1# show channel-group summary

```
Flags:  s - suspend             T - standby
        D - down/admin down     B - in Bundle
        R - Layer3              S - Layer2
        w - wait                U - in use

Aggregator Name    Protocol     Ports
----------------+------------+-------------------------------------------
agg1(SU)            Static      eth-0-1(B)   eth-0-2(B)    eth-0-3(B)
```

Switch1# show interface agg 1

```
Interface agg1
  Interface current state: UP
  Hardware is AGGREGATE, address is cce3.33fc.330b (bia a876.6b2c.9c01)
  Bandwidth 3000000 kbits
  Index 1025 , Metric 1 , Encapsulation ARPA
  Speed - 1000Mb/s , Duplex - Full  , Media type is Aggregation
  Link speed type is autonegotiation, Link duplex type is autonegotiation
  Input flow-control is off, output flow-control is off
  The Maximum Frame Size is 1534 bytes
  VRF binding: not bound
  Label switching is disabled
  No virtual circuit configured
  ARP timeout 01:00:00,  ARP retry interval 1s
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 140 bits/sec, 0 packets/sec
    0 packets input, 0 bytes
    Received 0 unicast, 0 broadcast, 0 multicast
    0 runts, 0 giants, 0 input errors, 0 CRC
    0 frame, 0 overrun, 0 pause input
    0 input packets with dribble condition detected
    1080 packets output, 60614 bytes
    Transmitted 0 unicast, 0 broadcast, 0 multicast
0 underruns, 0 output errors, 0 pause output
```

10 Configuring Flow Control

10.1 Overview

Flow control enables connected Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end. If one port experiences congestion and cannot receive any more traffic, it notifies the other port to stop sending until the condition clears. When the local device detects any congestion at its end, it can notify the link partner or the remote device of the congestion by sending a pause frame. You can use the flowcontrol interface configuration command to set the interface's ability to receive and send pause frames to on, off. The default state for ports is receive off and send off. In auto-negotiation link, local device’s flow control ability can be notified to link partner by link up/down.

10.2 Topology

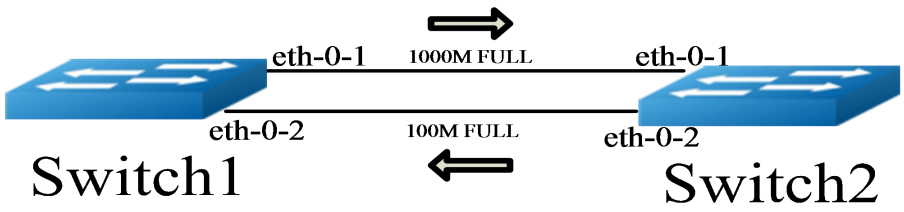

Figure 10-1 Flow Control Configuration Topology

10.3 Configuring Flow Control Send

Configure flowcontrol send

Switch# configure terminal	Enter the Configure mode
Switch1(config)# interface eth-0-1	Enter the Interface mode
Switch1(config-if)# no shutdown	Configure the port up
Switch1(config-if)# flowcontrol send on	Configure the port as flowcontrol send on
Switch1(config-if)# exit	Exit the Interface mode and enter the Configure mode

NOTE

Flow control send/receive on ability only works on full duplex link.

10.4 Configuring Flow Control Receive

Configure flow control receive

Switch# configure terminal	Enter the Configure mode
Switch(config)# interface eth-0-2	Enter the Interface mode
Switch(config-if)# no shutdown	Configure the port up
Switch(config-if)# flowcontrol receive on	Configure the port as flowcontrol receive on
Switch(config-if)# exit	Exit the Interface mode and enter the Configure mode

10.5 Validation

Switch2# show flowcontrol

```
Port       Receive FlowControl  Send FlowControl   RxPause      TxPause
           admin    oper        admin    oper
---------  -------- --------    -------- --------  -----------  -----------
eth-0-1    off      off         on       on        0            0
eth-0-2    off      off         off      off       0            0
eth-0-3    off      off         off      off       0            0
```

Switch2# show flowcontrol eth-0-1

```
Port       Receive FlowControl  Send FlowControl   RxPause      TxPause
           admin    oper        admin    oper
---------  -------- --------    -------- --------  -----------  -----------
eth-0-1    off      off         on       on        0            0
```

Switch1# show flowcontrol

```
Port       Receive FlowControl  Send FlowControl   RxPause      TxPause
           admin    oper        admin    oper
---------  -------- --------    -------- --------  -----------  -----------
eth-0-1    on       on          off      off       0            0
eth-0-2    off      off         off      off       0            0
eth-0-3    off      off         off      off       0            0
```

Switch1# show flowcontrol eth-0-1

Port	Receive FlowControl		Send FlowControl		RxPause	TxPause
	admin	oper	admin	oper		
---	---	---	---	---	---	---
eth-0-1	on	on	off	off	0	0

11 Configuring Storm Control

11.1 Overview

Storm control prevents traffic on a LAN from being disrupted by a broadcast, a multicast, or a unicast storm on one of the physical interfaces. A LAN storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance.

Storm control uses one of these methods to measure traffic activity:

- Bandwidth as a percentage of the total available bandwidth of the port (Level mode).
- Traffic rate in packets per second of the port (PPS mode).

11.2 Terminology

PPS: Packets per second

11.3 Configuring Bandwidth Percentage Storm Control

11.3.1 Topology

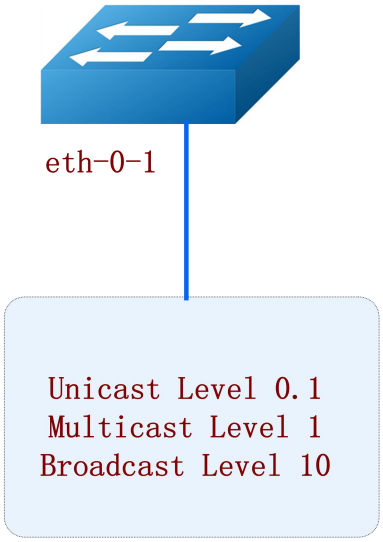

Figure 11-1 Percentage Storm Control

11.3.2 Configurations

Configuring Bandwidth Percentage Storm control:

Switch# configure terminal	Enter the Configure mode.
Switch(config)# interface eth-0-1	Enter the interface mode.
Switch(config-if)# storm-control unicast level 0.1	Set threshold to 0.1 percent of current port bandwidth.
Switch(config-if)# storm-control multicast level 1	Set threshold to 1 percent of current port bandwidth.
Switch(config-if)# storm-control broadcast level 10	Set threshold to 10 percent of current port bandwidth.
Switch(config-if)# end	Exit to exec mode.
Switch# show storm-control interface eth-0-1	Display storm control information.

11.3.3 Validation

Bridge 1

Switch# show storm-control interface eth-0-1

```
Port      ucastMode ucastLevel bcastMode bcastLevel mcastMode mcastLevel
eth-0-1 Level              0.10 Level             10.00 Level              1.00
```

11.4 Configuring Packets per-Second Storm Control

11.4.1 Topology

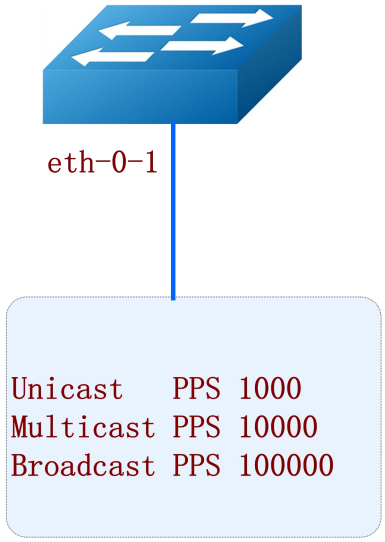

Figure 11-2 PPS Storm Control

11.4.2 Configurations

Configuring Packets per-Second Storm control:

Switch# configure terminal	Enter the Configure mode
Switch(config)# interface eth-0-1	Enter the interface mode
Switch(config-if)# storm-control unicast pps 1000	Set unicast pps to 1000 packets per seconds
Switch(config-if)# storm-control multicast pps 10000	Set multicast pps to 10000 packets per seconds
Switch(config-if)# storm-control broadcast pps 100000	Set broadcast pps to 100000 packets per seconds
Switch(config-if)# end	Exit to exec mode
Switch# show storm-control interface eth-0-1	Display storm control information

11.4.3 Validation

Bridge 1

Switch# show storm-control interface eth-0-1

```
Port     ucastMode ucastLevel bcastMode bcastLevel mcastMode mcastLevel
eth-0-1 PPS        1000         PPS        100000      PPS         10000
```

12 Configuring Layer 2 Protocols Tunneling

12.1 Overview

Customers at different sites connected across a service-provider network need to run various Layer 2 protocols to scale their topology to include all remote sites, as well as the local sites. STP must run properly, and every VLAN should build a proper spanning tree that includes the local site and all remote sites across the service-provider infrastructure.

When Layer 2 protocol tunneling is enabled, edge switches on the inbound side of the service-provider infrastructure encapsulate Layer 2 protocol packets with a new Layer 2 header and send them across the service-provider network. Core switches in the network do not process these packets but forward them as normal packets. Layer 2 protocol packets pass the service-provider infrastructure and reach customer switches on the outbound side of the service-provider network. The new Layer 2 header will be stripped when the Layer 2 protocol packets are sent to customer switches.

Layer 2 protocol tunneling can be used independently or can enhance 802.1Q tunneling.

12.2 Tunnel Designed Layer2 Protocol Packets

12.2.1 Overview

The designed Layer2 protocol packets include STP BPDU, LACP slow proto, DOT1X EAPOL.

In this example, one link is between Switch1 and Switch2. Switch1 eth-0-1 and Switch2 eth-0-1 are configured tunnel port. Switch1 eth-0-2 and Switch2 eth-0-2 are configured uplink port. If protocol packets are received on port eth-0-1 of switch1, packets should be added new Layer 2 header and sent out from uplink port. The new Layer 2 header will be as follows: MAC da should be tunnel dmac; MAC sa should be switch route-mac; VLAN ID should be tunnel vid; VLAN priority (cos) should be Layer 2 Protocol cos; Ethertype should be 0xFFEE. When the packets with new Layer 2 header are received on port eth-0-2 of switch2, new Layer 2 header will be stripped and the packets will be sent to port eth-0-1 of switch2.

12.2.2 Topology

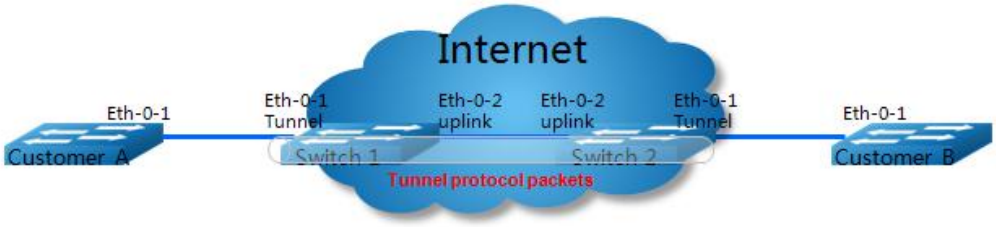

Figure 12-1 Layer 2 Tunnel Topology

12.2.3 Configurations

Switch 1 and Switch2 configurations is as follows.

Switch# configure terminal	Enter the Configure mode
Switch(config)# vlan database	Enter the VLAN configuration mode
Switch(config-vlan)# vlan 2-5	Enable vlan 2-5
Switch(config)# ethernet evc evc_c1	Create EVC evc_c1
Switch(config-evc)# dot1q mapped-vlan 2	Set mapped-vlan id to vlan id 2
Switch(config-evc)# exit	Exit to Configure mode
Switch(config)# ethernet evc evc_c2	Create EVC evc_c2
Switch(config-evc)# dot1q mapped-vlan 3	Set mapped-vlan id to vlan id 3
Switch(config-evc)# exit	Exit to Configure mode
Switch(config)# ethernet evc evc_c3	Create EVC evc_c3
Switch(config-evc)# dot1q mapped-vlan 4	Set mapped-vlan id to vlan id 4
Switch(config-evc)# exit	Exit to Configure mode
Switch(config)# ethernet evc evc_c4	Create EVC evc_c4
Switch(config-evc)# dot1q mapped-vlan 5	Set mapped-vlan id to vlan id 5
Switch(config-evc)# exit	Exit to Configure mode
Switch(config)# l2protocol enable	Enable l2protocol globally
Switch(config)# l2protocol tunnel-dmac 0100.0CCD.CDD2	Configure l2protocol tunnel dmac globally
Switch(config)# interface eth-0-1	Specify the interface (eth-0-1) to be configured and enter the Interface mode
Switch(config-if)# no shutdown	Open the interface
Switch(config-if)# switchport mode trunk	Configure interface to trunk port

Switch(config-if)# switchport trunk allowed vlan add 2-5	Allowed VLAN 2-5 to port eth-0-1
Switch(config-if)# spanning-tree port disable	Disable spanning tree for eth-0-1 before tunnel bpdu packet
Switch(config-if)# l2protocol stp tunnel evc evc_c1	Tunnel the stp bpdu packets into the SVLAN 2
Switch(config-if)# l2protocol lacp tunnel evc evc_c2	Tunnel the lacp slow protocol packets into the SVLAN 3
Switch(config-if)# l2protocol dot1x tunnel evc evc_c3	Tunnel the dot1x eapol packets into the SVLAN 4
Switch(config-evc)# exit	Exit to Configure mode
Switch(config)# interface eth-0-2	Specify the interface (eth-0-2) to be configured and enter the Interface mode
Switch(config-if)# no shutdown	Open the interface
Switch(config-if)# switchport mode trunk	Configure interface to trunk port
Switch(config-if)# switchport trunk allowed vlan add 2-5	Allowed VLAN 2-5 to port eth-0-1
Switch(config-if)# l2protocol uplink enable	Configure l2 protocol uplink port

12.2.4 Validation

You can use show command to display the configuration on the switchport.

Switch1# show l2protocol interface eth-0-1

```
Interface  PDU Address     MASK              Status     EVC
=========  ==============  ==============  ========  ================
eth-0-1    stp             FFFF.FFFF.FFFF  Tunnel     evc_c1
eth-0-1    slow-proto      FFFF.FFFF.FFFF  Tunnel     evc_c2
eth-0-1    dot1x           FFFF.FFFF.FFFF  Tunnel     evc_c3
```

Switch1# show l2protocol interface eth-0-2

```
Interface  PDU Address     MASK              Status     EVC
=========  ==============  ==============  ========  ================
eth-0-2    stp             FFFF.FFFF.FFFF  Peer       N/A
eth-0-2    slow-proto      FFFF.FFFF.FFFF  Peer       N/A
eth-0-2    dot1x           FFFF.FFFF.FFFF  Peer       N/A
eth-0-2    N/A             N/A             Uplink     N/A
```

Switch1# show l2protocol tunnel-dmac

```
Layer2 protocols tunnel destination MAC address is 0100.0ccd.cdd2
```

12.3 Tunnel Configured Layer2 Protocol Packets

12.3.1 Overview

Configured Layer2 protocol packets are the packets whose mac da is between 0180.c200.0000 and 0180.c2ff.ffff;

Configured Layer2 protocol full-mac packets are the packets whose mac da is between 0000.0000.0000 and ffff.ffff.ffff.

In this example, one link is between Switch1 and Switch2. Switch1 eth-0-1 and Switch2 eth-0-1 are configured tunnel port. Switch1 eth-0-2 and Switch2 eth-0-2 are configured uplink port. If packets with special MAC da are received on port eth-0-1 of switch1, packets should be added new Layer 2 header and sent out from uplink port. The new Layer 2 header will be as follows: MAC da should be tunnel dmac; MAC sa should be switch route-mac; VLAN ID should be tunnel vid; VLAN priority(cos) should be Layer 2 Protocol cos; Ethertype should be 0xFFEE. When the packets with new Layer 2 header are received on port eth-0-2 of switch2, new Layer 2 header will be stripped and the packets will be sent to port eth-0-1 of switch2.

12.3.2 Topology

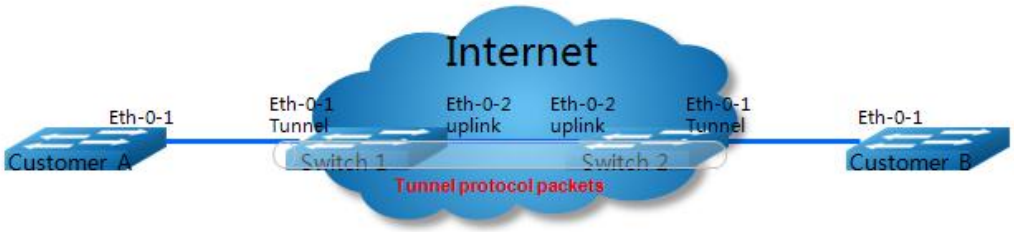

Figure 12-2 Layer 2 Tunnel Topology

12.3.3 Configurations

Switch 1 and Switch 2 configurations is as follows.

Switch# configure terminal	Enter the Configure mode
Switch(config)# vlan database	Enter the VLAN configuration mode
Switch(config-vlan)# vlan 2-4	Enable vlan 2-4
Switch(config)# ethernet evc evc_c1	Create EVC evc_c1
Switch(config-evc)# dot1q mapped-vlan 2	Set mapped-vlan id to vlan id 2
Switch(config-evc)# exit	Exit to Configure mode
Switch(config)# ethernet evc evc_c2	Create EVC evc_c2
Switch(config-evc)# dot1q mapped-vlan 3	Set mapped-vlan id to vlan id 3
Switch(config-evc)# exit	Exit to Configure mode
Switch(config)# ethernet evc evc_c3	Create EVC evc_c3

Switch(config-evc)# dot1q mapped-vlan 4	Set mapped-vlan id to vlan id 4
Switch(config-evc)# exit	Exit to Configure mode
Switch(config)# l2protocol enable	Enable l2protocol globally
Switch(config)# l2protocol tunnel-dmac 0100.0CCD.CDD2	Configure l2protocol tunnel dmac globally
Switch1(config)# l2protocol mac 1 0180.C200.0008 mask FFFF.FFFF.FFFF	Configure l2protocol mac 1 globally
Switch1(config)# l2protocol full-mac 0100.0CCC.CCCC mask FFFF.FFFF.FFFF	Configure l2protocol full-mac globally.
Switch(config)# interface eth-0-1	Specify the interface (eth-0-1) to be configured and enter the Interface mode
Switch(config-if)# no shutdown	Open the interface
Switch(config-if)# switchport mode trunk	Configure interface to trunk port.
Switch(config-if)# switchport trunk allowed vlan add 2-4	Allowed VLAN 2-4 to port eth-0-1
Switch(config-if)# spanning-tree port disable	Disable spanning tree for eth-0-1 before tunnel bpdu packet
Switch(config-if)# l2protocol mac 1 tunnel evc evc_c1	Tunnel the mac 1 into the SVLAN 2
Switch(config-if)# l2protocol full-mac tunnel evc evc_c3	Tunnel the full-mac into the SVLAN 4.
Switch(config)# interface eth-0-2	Specify the interface (eth-0-2) to be configured and enter the Interface mode
Switch(config-if)# no shutdown	Open the interface
Switch(config-if)# switchport mode trunk	Configure interface to trunk port.
Switch(config-if)# switchport trunk allowed vlan add 2-4	Allowed VLAN 2-4 to port eth-0-2
Switch(config-if)# l2protocol uplink enable	Configure l2 protocol uplink port

12.3.4 Validation

You can use show command to display the configuration on the switchport.

Switch1# show l2protocol interface eth-0-1

```
Interface   PDU Address      MASK             Status     EVC
=========   ==============   ==============   ========   ================
eth-0-1     0180.c200.0008   FFFF.FFFF.FFFF   Tunnel     evc_c1
eth-0-1     0100.0ccc.cccc   FFFF.FFFF.FFFF   Tunnel     evc_c3
eth-0-1     stp              FFFF.FFFF.FFFF   Peer       N/A
eth-0-1     slow-proto       FFFF.FFFF.FFFF   Peer       N/A
```

```
eth-0-1     dot1x             FFFF.FFFF.FFFF  Peer      N/A
eth-0-1     cfm               FFFF.FFFF.FFFF  Peer      N/A
```

Switch1# show l2protocol interface eth-0-2

```
Interface   PDU Address       MASK            Status    EVC
=========   ==============    ==============  ========  ================
eth-0-2     0180.c200.0008    FFFF.FFFF.FFFF  Peer      N/A
eth-0-2     0100.0ccc.cccc    FFFF.FFFF.FFFF  Peer      N/A
eth-0-2     stp               FFFF.FFFF.FFFF  Peer      N/A
eth-0-2     slow-proto        FFFF.FFFF.FFFF  Peer      N/A
eth-0-2     dot1x             FFFF.FFFF.FFFF  Peer      N/A
eth-0-2     cfm               FFFF.FFFF.FFFF  Peer      N/A
eth-0-2     N/A               N/A             Uplink    N/A
```

Switch1# show l2protocol tunnel-dmac

```
Layer2 protocols tunnel destination MAC address is 0100.0ccd.cdd2
```

13 Configuring MSTP

13.1 Overview

The MSTP (Multiple Spanning Tree Algorithm and Protocol (IEEE 802.1Q-2005)) enables multiple VLANs to be mapped to the same spanning-tree instance, thereby reducing the number of spanning-tree instances needed to support a large number of VLANs. The MSTP provides for multiple forwarding paths for data traffic and enables load balancing. It improves the fault tolerance of the network because a failure in one instance (forwarding path) does not affect other instances (forwarding paths). The most common initial deployment of MSTP is in the backbone and distribution layers of a Layer 2 switched network; this deployment provides the highly-available network required in a service-provider environment.

When the switch is in the multiple spanning-tree (MST) modes, the Rapid Spanning Tree Protocol (RSTP), which is based on IEEE 802.1w, is automatically enabled. The RSTP provides rapid convergence of the spanning tree through explicit handshaking that eliminates the IEEE 802.1D forwarding delay and quickly transitions root ports and designated ports to the forwarding state.

13.2 Topology

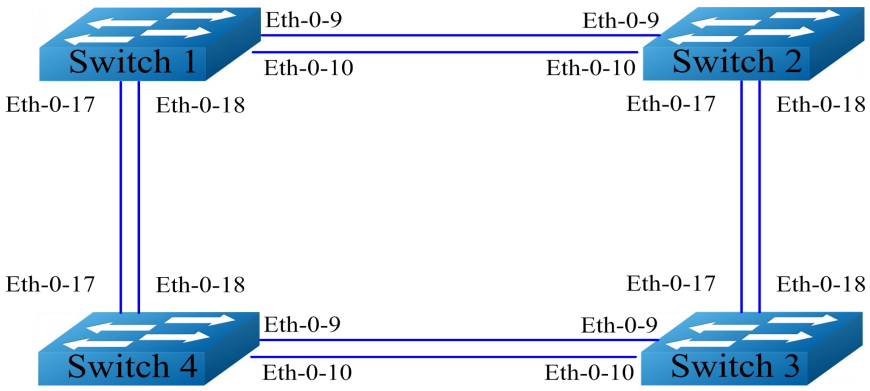

Figure 13-1 MSTP Topology

13.3 Configurations

This configuration sample assumes that you are running the Layer-2 module. If you are using the Layer-2 module, run the switchport command on each port to set the switching characteristics of Layer-2 protocols.

Configuring Switch 1 – Switch 4

Switch# configure terminal	Enter the Configure mode
Switch(config)# spanning-tree mode mstp	Configure a spanning-tree mode
Switch(config)# vlan database	Enter vlan configuration mode
Switch(config-vlan)# vlan 10	Create vlan 10 on Switch
Switch(config-vlan)# vlan 20	Create vlan 20 on Switch
Switch(config-vlan)# exit	Exit vlan configuration mode
Switch(config)# spanning-tree mst configuration	Enter the Multiple Spanning Tree configuration mode
Switch(config-mst)# region RegionName	Configure region name RegionName
Switch(config-mst)# instance 1 vlan 10	Create an instance of vlan
Switch(config-mst)# instance 2 vlan 20	Create an instance of vlan
Switch(config-mst)# exit	Exit the Multiple Spanning Tree configuration mode
Switch(config)# interface eth-0-9	Enter interface mode of interface eth-0-9
Switch(config-if)# switchport mode trunk	Configure eth-0-9 to mode trunk.
Switch(config-if)# switchport trunk allowed vlan all	Configure vlans that allowed passing the port
Switch(config-if)# no shutdown	Open the port
Switch(config-if)# exit	Exit interface mode of interface eth-0-9
Switch(config)# interface eth-0-10	Enter interface mode of interface eth-0-10
Switch(config-if)# switchport mode trunk	Configure eth-0-10 to mode trunk.
Switch(config-if)# switchport trunk allowed vlan all	Configure vlans that allowed passing the port
Switch(config-if)# no shutdown	Open the port
Switch(config-if)# exit	Exit interface mode of interface eth-0-10
Switch(config)# interface eth-0-17	Enter interface mode of interface eth-0-17

Switch(config-if)# switchport mode trunk	Configure eth-0-17 to mode trunk.
Switch(config-if)# switchport trunk allowed vlan all	Configure vlans that allowed passing the port
Switch(config-if)# no shutdown	Open the port
Switch(config-if)# exit	Exit interface mode of interface eth-0-17
Switch(config)# interface eth-0-18	Enter interface mode of interface eth-0-18
Switch(config-if)# switchport mode trunk	Configure eth-0-18 to mode trunk.
Switch(config-if)# switchport trunk allowed vlan all	Configure vlans that allowed passing the port
Switch(config-if)# no shutdown	Open the port
Switch(config-if)# exit	Exit interface mode of interface eth-0-18
Switch(config)# exit	Exit configuration mode

Configuring Switch1

Switch# configure terminal	Enter the Configure mode
Switch(config)# spanning-tree priority 0	Configure STP priority to 0
Switch(config)# spanning-tree enable	Enable spanning tree protocol The default is disable

Configuring Switch2

Switch# configure terminal	Enter the Configure mode
Switch(config)# spanning-tree instance 1 priority 0	Configure instance 1 priority to 0
Switch(config)# spanning-tree enable	Enable spanning tree protocol The default is disable

Configuring Switch3

Switch# configure terminal	Enter the Configure mode
Switch(config)# spanning-tree instance 2 priority 0	Configure instance 2 priority to 0
Switch(config)# spanning-tree enable	Enable spanning tree protocol The default is disable

Configuring Switch4

Switch# configure terminal	Enter the Configure mode
Switch(config)# spanning-tree enable	Enable spanning tree protocol The default is disable

13.4 Validation

Verify the MSTP port state on Switch 1

Switch# show spanning-tree mst brief

```
##### MST0:  Vlans: 1
Multiple spanning tree protocol Enabled
Root ID      Priority       0 (0x0000)
             Address     2225.fa28.c900
             Hello Time  2 sec  Max Age  20 sec Forward Delay 15 sec

Bridge ID    Priority       0 (0x0000)
             Address     2225.fa28.c900
             Hello Time  2 sec  Max Age  20 sec Forward Delay 15 sec
             Aging Time  300 sec

Interface     Role           State             Cost       Priority.Number      Type
--------------------------------------------------------------------------------
eth-0-9       Designated     Forwarding        20000            128.9          P2p
eth-0-10      Designated     Forwarding        20000            128.10         P2p
eth-0-17      Designated     Forwarding        20000            128.17         P2p
eth-0-18      Designated     Forwarding        20000            128.18         P2p

##### MST1:  Vlans: 10
Root ID      Priority       1 (0x0001)
             Address     9c9a.7d91.9f00
Bridge ID    Priority    32769 (0x8001)
             Address     2225.fa28.c900
Interface     Role           State             Cost       Priority.Number      Type
--------------------------------------------------------------------------------
eth-0-9       Rootport       Forwarding        20000            128.9          P2p
eth-0-10      Alternate      Discarding        20000            128.10         P2p
eth-0-17      Designated     Forwarding        20000            128.17         P2p
eth-0-18      Designated     Forwarding        20000            128.18         P2p

##### MST2:  Vlans: 20
Root ID      Priority       2 (0x0002)
             Address     304c.275b.b200
Bridge ID    Priority    32770 (0x8002)
             Address     2225.fa28.c900
Interface     Role           State             Cost       Priority.Number      Type
--------------------------------------------------------------------------------
eth-0-9       Alternate      Discarding        20000            128.9          P2p
```

```
eth-0-10    Alternate      Discarding      20000           128.10          P2p
eth-0-17    Rootport       Forwarding      20000           128.17          P2p
eth-0-18    Alternate      Discarding      20000           128.18          P2p
```

Verify the MSTP port state on Switch 2

Switch# show spanning-tree mst brief

```
##### MST0:  Vlans: 1
Multiple spanning tree protocol Enabled
Root ID     Priority       0 (0x0000)
            Address      2225.fa28.c900
            Hello Time   2 sec  Max Age  20 sec Forward Delay 15 sec

Bridge ID   Priority     32768 (0x8000)
            Address      9c9a.7d91.9f00
            Hello Time   2 sec  Max Age  20 sec Forward Delay 15 sec
            Aging Time   300 sec

Interface    Role           State             Cost       Priority.Number      Type
-------------------------------------------------------------------------------
eth-0-9     Rootport       Forwarding      20000           128.9           P2p
eth-0-10    Alternate      Discarding      20000           128.10          P2p
eth-0-17    Designated     Forwarding      20000           128.17          P2p
eth-0-18    Designated     Forwarding      20000           128.18          P2p

##### MST1:  Vlans: 10
Root ID     Priority       1 (0x0001)
            Address      9c9a.7d91.9f00
Bridge ID   Priority       1 (0x0001)
            Address      9c9a.7d91.9f00
Interface    Role           State             Cost       Priority.Number      Type
-------------------------------------------------------------------------------
eth-0-9     Designated     Forwarding      20000           128.9           P2p
eth-0-10    Designated     Forwarding      20000           128.10          P2p
eth-0-17    Designated     Forwarding      20000           128.17          P2p
eth-0-18    Designated     Forwarding      20000           128.18          P2p

##### MST2:  Vlans: 20
Root ID     Priority       2 (0x0002)
            Address      304c.275b.b200
Bridge ID   Priority     32770 (0x8002)
            Address      9c9a.7d91.9f00
Interface    Role           State             Cost       Priority.Number      Type
-------------------------------------------------------------------------------
eth-0-9     Designated     Forwarding      20000           128.9           P2p
eth-0-10    Designated     Forwarding      20000           128.10          P2p
eth-0-17    Rootport       Forwarding      20000           128.17          P2p
eth-0-18    Alternate      Discarding      20000           128.18          P2p
```

Verify the MSTP port state on Switch 3

Switch# show spanning-tree mst brief

```
##### MST0:  Vlans: 1
Multiple spanning tree protocol Enabled
```

```
Root ID     Priority       0 (0x0000)
            Address     2225.fa28.c900
            Hello Time  2 sec  Max Age  20 sec Forward Delay 15 sec

Bridge ID   Priority    32768 (0x8000)
            Address     304c.275b.b200
            Hello Time  2 sec  Max Age  20 sec Forward Delay 15 sec
            Aging Time  300 sec

Interface    Role          State             Cost      Priority.Number     Type
-------------------------------------------------------------------------------
eth-0-9      Rootport      Forwarding      20000           128.9         P2p
eth-0-10     Alternate     Discarding      20000           128.10        P2p
eth-0-17     Alternate     Discarding      20000           128.17        P2p
eth-0-18     Alternate     Discarding      20000           128.18        P2p

##### MST1:  Vlans: 10
Root ID     Priority       1 (0x0001)
            Address     9c9a.7d91.9f00
Bridge ID   Priority    32769 (0x8001)
            Address     304c.275b.b200
Interface    Role          State             Cost      Priority.Number     Type
-------------------------------------------------------------------------------
eth-0-9      Designated    Forwarding      20000           128.9         P2p
eth-0-10     Designated    Forwarding      20000           128.10        P2p
eth-0-17     Rootport      Forwarding      20000           128.17        P2p
eth-0-18     Alternate     Discarding      20000           128.18        P2p

##### MST2:  Vlans: 20
Root ID     Priority       2 (0x0002)
            Address     304c.275b.b200
Bridge ID   Priority       2 (0x0002)
            Address     304c.275b.b200
Interface    Role          State             Cost      Priority.Number     Type
-------------------------------------------------------------------------------
eth-0-9      Designated    Forwarding      20000           128.9         P2p
eth-0-10     Designated    Forwarding      20000           128.10        P2p
eth-0-17     Designated    Forwarding      20000           128.17        P2p
eth-0-18     Designated    Forwarding      20000           128.18        P2p
```

Verify the MSTP port state on Switch 4

Switch# show spanning-tree mst brief

```
##### MST0:  Vlans: 1
Multiple spanning tree protocol Enabled
Root ID     Priority       0 (0x0000)
            Address     2225.fa28.c900
            Hello Time  2 sec  Max Age  20 sec Forward Delay 15 sec

Bridge ID   Priority    32768 (0x8000)
            Address     80a4.be55.6400
            Hello Time  2 sec  Max Age  20 sec Forward Delay 15 sec
            Aging Time  300 sec

Interface    Role          State             Cost      Priority.Number     Type
```

```
--------------------------------------------------------------------------------
eth-0-9      Designated      Forwarding      20000           128.9         P2p
eth-0-10     Designated      Forwarding      20000           128.10        P2p
eth-0-17     Rootport        Forwarding      20000           128.17        P2p
eth-0-18     Alternate       Discarding      20000           128.18        P2p

##### MST1:  Vlans: 10
Root ID      Priority        1 (0x0001)
             Address         9c9a.7d91.9f00
Bridge ID    Priority        32769 (0x8001)
             Address         80a4.be55.6400
Interface    Role            State           Cost       Priority.Number     Type
--------------------------------------------------------------------------------
eth-0-9      Alternate       Discarding      20000           128.9         P2p
eth-0-10     Alternate       Discarding      20000           128.10        P2p
eth-0-17     Rootport        Forwarding      20000           128.17        P2p
eth-0-18     Alternate       Discarding      20000           128.18        P2p

##### MST2:  Vlans: 20
Root ID      Priority        2 (0x0002)
             Address         304c.275b.b200
Bridge ID    Priority        32770 (0x8002)
             Address         80a4.be55.6400
Interface    Role            State           Cost       Priority.Number     Type
--------------------------------------------------------------------------------
eth-0-9      Rootport        Forwarding      20000           128.9         P2p
eth-0-10     Alternate       Discarding      20000           128.10        P2p
eth-0-17     Designated      Forwarding      20000           128.17        P2p
eth-0-18     Designated      Forwarding      20000           128.18        P2p
```

14 Configuring MLAG

14.1 Overview

High availability data center topologies typically provide redundancy protection at the expense of oversubscription by connecting top-of-rack (TOR) switches and servers to dual aggregation switches. In these topologies, Spanning Tree Protocol prevents network loops by blocking half of the links to the aggregation switches. This reduces the available bandwidth by 50%.

Deploying MLAG removes oversubscription by configuring an MLAG link between two aggregation switches to create a single logical switching instance that utilizes all connections to the switches. Interfaces on both devices participate in a distributed port channel, enabling all active paths to carry data traffic while maintaining the integrity of the Spanning Tree topology.

MLAG provides these benefits:

- Provides higher bandwidth links as network traffic increases.
- Utilizes bandwidth more efficiently with fewer uplinks blocked by STP.
- Connects to other switches and servers by static LAG or LACP without other proprietary protocols.
- Supports normal STP operation to prevent loops.
- Supports active-active Layer-2 redundancy

14.2 Topology

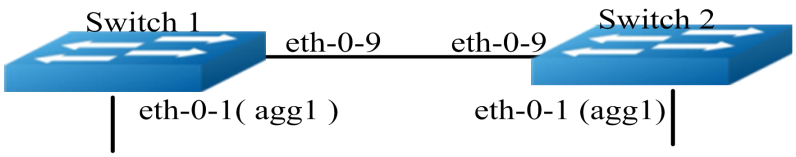

Figure 14-1 MLAG Configuration Topology

14.3 Configuration MLAG

Configuring Switch 1

Switch1 (config)# vlan database	Enter the Vlan mode
Switch1 (config-vlan)# vlan 10,4094	Create vlan 10 and vlan 4094
Switch1(config-vlan)# exit	Return to global configuration mode
Switch1 (config)# interface eth-0-1	Enter interface mode
Switch1(config-if)# static-channel-group 1	Add this interface to static agg
Switch1(config-if)# no shutdown	No shutdown the interface
Switch1(config-if)# exit	Return to global configuration mode
Switch1 (config)# interface eth-0-9	Enter interface mode
Switch1(config-if)# switchport mode trunk	Set the switchport mode to trunk
Switch1(config-if)# switchport trunk allowed vlan all	Allow all vlans on this trunk port
Switch1(config-if)# spanning-tree port disable	Disable spanning tree on peer link
Switch1(config-if)# no shutdown	No shutdown the interface
Switch1(config-if)# exit	Return to global configuration mode
Switch1 (config)# interface agg1	Enter agg interface mode
Switch1(config-if)# switchport mode trunk	Set the mode to trunk
Switch1(config-if)# switchport trunk allowed vlan add 10	Allow vlan 10 on this interface
Switch1(config-if)# mlag 1	Bind this interface to mlag id
Switch1(config-if)# exit	Return to global configuration mode
Switch1 (config)# interface vlan4094	Create interface vlan
Switch1(config-if)# ip address 12.1.1.1/24	Configure ip address on this vlan interface
Switch1(config-if)# exit	Return to global configuration mode
Switch1 (config)# mlag configuration	Enter mlag configuration mode
Switch1 (config-mlag)# peer-link eth-0-9	Configure peer link
Switch1 (config-mlag)# peer-address 12.1.1.2	Configure peer address
Switch1 (config-mlag)# exit	Return to global configuration mode

Configuring Switch2

Switch2 (config)# vlan database	Enter the Vlan mode
Switch2 (config-vlan)# vlan 10,4094	Create vlan 10 and vlan 4094
Switch2(config-vlan)# exit	Return to global configuration mode
Switch2 (config)# interface eth-0-1	Enter interface mode
Switch2(config-if)# static-channel-group 1	Add this interface to static agg
Switch2(config-if)# no shutdown	No shutdown the interface
Switch2(config-if)# exit	Return to global configuration mode
Switch2 (config)# interface eth-0-9	Enter interface mode
Switch2(config-if)# switchport mode trunk	Set the switchport mode to trunk
Switch2(config-if)# switchport trunk allowed vlan all	Allow all vlans on this trunk port
Switch2(config-if)# spanning-tree port disable	Disable spanning tree on peer link
Switch2(config-if)# no shutdown	No shutdown the interface
Switch2(config-if)# exit	Return to global configuration mode
Switch2 (config)# interface agg1	Enter agg interface mode
Switch2(config-if)# switchport mode trunk	Set the mode to trunk
Switch2(config-if)# switchport trunk allowed vlan add 10	Allow vlan 10 on this interface
Switch2(config-if)# mlag 1	Bind this interface to mlag id
Switch2(config-if)# exit	Return to global configuration mode
Switch2 (config)# interface vlan4094	Create interface vlan
Switch2(config-if)# ip address 12.1.1.2/24	Configure ip address on this vlan interface
Switch2(config-if)# exit	Return to global configuration mode
Switch2 (config)# mlag configuration	Enter mlag configuration mode
Switch2 (config-mlag)# peer-link eth-0-9	Configure peer link
Switch2 (config-mlag)# peer-address 12.1.1.1	Configure peer address
Switch2 (config-mlag)# end	Return to previlidge exec mode

14.4 Validation

Validate on Switch 1

Switch# show mlag

```
MLAG configuration:
-----------------
role         : Master
local_sysid : ea90.aecc.cc00
mlag_sysid   : ea90.aecc.cc00
peer-link    : eth-0-9
peer conf    : Yes

Switch1# show mlag interface
mlagid  local-if  local-state    remote-state
1       agg1      up             up
Switch1# show mlag peer
MLAG neighbor is 12.1.1.2, MLAG version 1
MLAG state = Established, up for 00:13:07
Last read 00:00:48, hold time is 240, keepalive interval is 60 seconds
Received 19 messages,Sent 23 messages
Open      : received 1, sent 2
KAlive    : received 15, sent 16
Fdb sync  : received 0, sent 0
Failover  : received 0, sent 0
Conf      : received 1, sent 1
STP Total: received 2, sent 4
 Global   : received 2, sent 3
 Packet   : received 0, sent 0
 Instance: received 0, sent 0
 State    : received 0, sent 1
Connections established 1; dropped 0
Local host: 12.1.1.1, Local port: 61000
Foreign host: 12.1.1.2, Foreign port: 46157
remote_sysid: baa7.8606.8b00
Switch1# show mac address-table
          Mac Address Table
------------------------------------------
(*) - Security Entry
Vlan    Mac Address        Type         Ports
----    -----------        --------     -----
10      0001.0002.0003     static       agg1(MO)
```

Validate on Switch 2

Switch# show mlag

```
MLAG configuration:
-----------------
role         : Slave
local_sysid : baa7.8606.8b00
mlag_sysid   : ea90.aecc.cc00
peer-link    : eth-0-9
peer conf    : Yes
Switch2# show mlag interface
mlagid  local-if  local-state    remote-state
1       agg1      up             up
Switch2# show mlag peer
MLAG neighbor is 12.1.1.1, MLAG version 1
MLAG state = Established, up for 00:14:29
Last read 00:00:48, hold time is 240, keepalive interval is 60 seconds
```

```
Received 23 messages,Sent 21 messages
Open      : received 1, sent 1
KAlive    : received 17, sent 17
Fdb sync  : received 0, sent 0
Failover  : received 0, sent 0
Conf      : received 1, sent 1
STP Total: received 4, sent 2
 Global   : received 3, sent 2
 Packet   : received 0, sent 0
 Instance: received 0, sent 0
 State    : received 1, sent 0
Connections established 1; dropped 0
Local host: 12.1.1.2, Local port: 46157
Foreign host: 12.1.1.1, Foreign port: 61000
remote_sysid: ea90.aecc.cc00
Switch2# show mac address-table
          Mac Address Table
------------------------------------------
(*) - Security Entry
Vlan    Mac Address        Type         Ports
----    -----------        --------     -----
10      0001.0002.0003     static       agg1(MI)
```