

Configuring VLAN Trunks

This chapter describes how to configure Fast Ethernet and Gigabit Ethernet VLAN trunks on a switch. For information on adding and deleting VLANs, refer to Chapter 2, “Configuring VTP and Virtual LANs.”

Switches support the following trunking methods for transmitting VLAN traffic over 100BaseT and Gigabit Ethernet ports:

- Inter-Switch Link (ISL)
- IEEE 802.1Q

In addition, you can enable ATM trunking by installing a Catalyst 2900 series XL ATM module in a Catalyst 2900 XL switch. ATM connectivity is described in the *Catalyst 2900 Series XL ATM Modules Installation and Configuration Guide*.

Note For complete syntax and usage information for the commands used in this chapter, refer to the *Cisco IOS Desktop Switching Command Reference*.

The trunking described in this chapter is not supported on all switches and modules. See the *Release Notes for Catalyst 2900 Series XL and Catalyst 3500 Series XL Cisco IOS Release 12.0(5)XP* for the list of products that support trunking.

This chapter consists of these sections:

- “How VLAN Trunks Work” section on page 3-2
- “Configuring a Trunk Port” section on page 3-4
- “Load Sharing Using STP” section on page 3-8

How VLAN Trunks Work

A trunk is a point-to-point link that transmits and receives traffic between switches or between switches and routers. Trunks carry the traffic of multiple VLANs and can extend VLANs across an entire network. 100BaseT and Gigabit Ethernet trunks use Cisco ISL (the default protocol) or industry-standard IEEE 802.1Q to carry traffic for multiple VLANs over a single link.

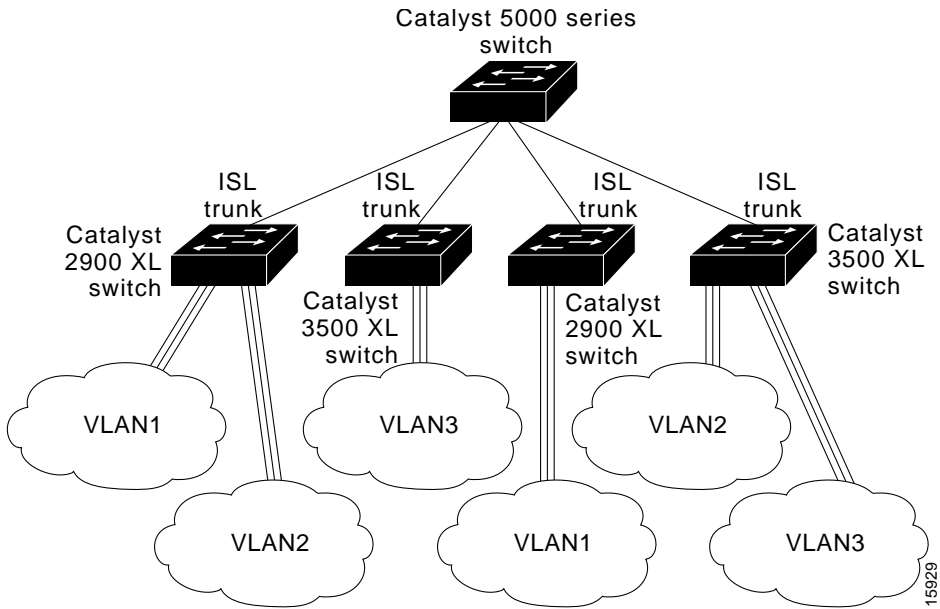
Figure 3-1 shows a network of switches that are connected by ISL trunks.

IEEE 802.1Q Configuration Considerations

IEEE 802.1Q trunks impose some limitations on the trunking strategy for a network. The following restrictions apply when using 802.1Q trunks:

- Make sure the native VLAN for an 802.1Q trunk is the same on both ends of the trunk link. If the native VLAN on one end of the trunk is different from the native VLAN on the other end, spanning-tree loops might result.
- Disabling STP on the native VLAN of an 802.1Q trunk without disabling STP on every VLAN in the network can potentially cause STP loops. We recommend that you leave STP enabled on the native VLAN of an 802.1Q trunk or disable STP on every VLAN in the network. Make sure your network is loop-free before disabling STP.

Figure 3-1 Catalyst 2900 Series XL and Catalyst 3500 Series XL Switches in an ISL Trunking Environment



Configuring a Trunk Port

This section describes how to use the CLI to configure an ISL or IEEE 802.1Q trunk port, how to define the VLANs that can use a port, and how to disable a trunk port.

If you are assigning a port on a cluster member switch to a VLAN, first log in to the member switch by using the privileged EXEC **rcommand** command. See the *Cisco IOS Desktop Switching Command Reference* for more information on how to use this command.

To define a port as an ISL trunk port, perform this task from privileged EXEC mode:

Task	Command
Step 1 Enter global configuration mode.	configure terminal
Step 2 Enter the interface configuration command mode and the port to be added to the VLAN.	interface <i>interface_id</i>
Step 3 Configure the port with a VLAN membership mode of <i>trunk</i> .	switchport mode trunk
Step 4 ¹ Configure the port to support ISL trunking.	switchport trunk encapsulation isl
Step 5 Return to privileged EXEC mode.	end
Step 6 Verify your entries.	show interface <i>interface-id</i> switchport
Step 7 Save the configuration.	copy running-config startup-config

1 To configure IEEE 802.1 Q, enter this command: **switchport trunk encapsulation dot1q**

Note The Enterprise Edition Software, Cisco IOS Release 12.0(5)XP, does not support trunk negotiation via the Dynamic Trunk Protocol (DTP), formerly known as Dynamic ISL (DISL). If you are connecting a trunk port to a Catalyst 5000 switch or other DTP device, use the non-negotiate option on the DTP-capable device to configure the switch port to not generate DTP frames.

This example shows how to configure a port as a trunk, verify the trunk configuration, and save the change to the startup configuration file:

```
Switch# configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Switch(config)# interface fa0/1  
Switch(config-if)# switchport mode trunk  
Switch(config-if)# switchport trunk encapsulation isl  
Switch(config-if)# end
```

```
Switch# show interface fa0/1 switchport  
Name: Fa0/1  
Switchport: Enabled  
Administrative mode: trunk  
→ Operational Mode: trunk  
Administrative Trunking Encapsulation: isl  
→ Operational Trunking Encapsulation: isl  
Negotiation of Trunking: Disabled  
Access Mode VLAN: 0 ((Inactive))  
Trunking Native Mode VLAN: 1 (default)  
Trunking VLANs Enabled: 1-3,1002-1005  
Trunking VLANs Active: 1-3  
Pruning VLANs Enabled: NONE
```

```
Switch# copy running-config startup-config  
Building configuration...  
[OK]  
Switch#
```

Defining the Allowed VLANs on a Trunk

A trunk port by default sends to and receives traffic from all VLANs in the VLAN database. All VLANs, 1 to 1005, are allowed on each trunk. However, you can remove VLANs from the allowed list, preventing traffic from those VLANs from passing over the trunk. To restrict the traffic a trunk carries, use the **remove** *vlan-list* parameter to remove specific VLANs from the allowed list.

Note VLANs 1 and 1002 to 1005 are reserved and cannot be removed.

To modify the allowed list of a trunk, perform this task from privileged EXEC mode:

Task	Command
Step 1 Enter global configuration mode.	configure terminal
Step 2 Enter the interface configuration command mode and the port to be added to the VLAN.	interface <i>interface_id</i>
Step 3 Configure the VLAN membership mode for trunks.	switchport mode trunk
Step 4 Define the VLANs that are <i>not</i> allowed to transmit and receive on the port. The <i>vlan-list</i> parameter is a range of VLAN IDs separated by a hyphen or specific VLAN IDs separated by commas.	switchport trunk allowed vlan remove <i>vlan-list</i>
Step 5 Return to privileged EXEC.	end
Step 6 Verify your entries.	show interface <i>interface-id</i> switchport allowed-vlan
Step 7 Save the configuration.	copy running-config startup-config

This example shows how to define the allowed VLANs list for trunk port Fa0/1 to allow VLANs 1 to 100, VLAN 250, and VLANs 500 to 1005, and how to verify the allowed VLAN list for the trunk:

```
Switch(config)# interface fa0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan remove 101-499
Switch(config-if)# switchport trunk allowed vlan add 250
Switch(config-if)# end
Switch# show interface fa0/1 switchport allowed-vlan
→ "1-100,250,500-1005"
Switch#
```

Disabling a Trunk Port

You can disable trunking on a port by returning it to its default static-access mode. To disable trunking on a port, perform the following tasks from privileged EXEC mode:

Task	Command
Step 1 Enter global configuration mode.	configure terminal
Step 2 Enter the interface configuration command mode and the port to be added to the VLAN.	interface <i>interface_id</i>
Step 3 Return the port to its default static-access mode.	no switchport mode
Step 4 Return to privileged EXEC.	end
Step 5 Verify your entries.	show interface <i>interface-id</i> switchport

This example shows how to disable trunking on a port:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface fa0/1
Switch(config-if)# no switchport mode
Switch(config-if)# end

Switch# show interface fa0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: isl
Operational Trunking Encapsulation: isl
→ Negotiation of Trunking: Disabled
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: NONE
Pruning VLANs Enabled: NONE
```

Load Sharing Using STP

Load sharing divides the bandwidth supplied by parallel trunks connecting switches. To avoid loops, Spanning-Tree Protocol (STP) normally blocks all but one parallel link between switches. With load sharing, you divide the traffic between the links according to which VLAN the traffic belongs to.

There are two ways to configure load sharing by using trunk ports: using STP port priorities or using STP path costs. If you configure load sharing using STP port priorities, both load-sharing links must be connected to the same switch. If you configure load sharing using STP path costs, each load-sharing link can be connected to the same switch or to two different switches.

Load Sharing Using STP Port Priorities

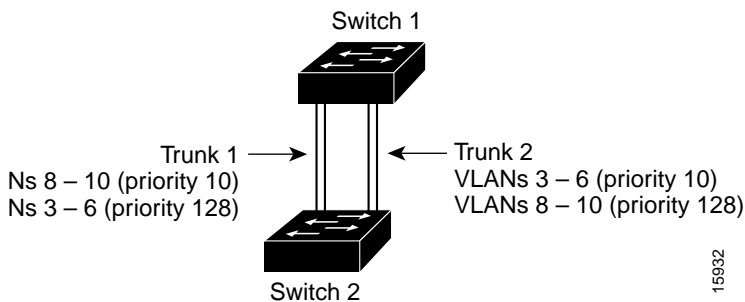
When two ports on the same switch form a loop, the port priority setting determines which port is enabled and which port is in standby mode. You can set the priorities on a parallel trunk port so that the port carries all the traffic for a given VLAN. The trunk port with the higher priority (lower values) for a VLAN is forwarding traffic for that VLAN. The trunk port with the lower priority (higher values) for the same VLAN remains in a blocking state for that VLAN. One trunk port transmits or receives all traffic for the VLAN.

Figure 3-2 shows two trunks connecting supported switches. In this example, the switches are configured as follows:

- VLANs 8 through 10 are assigned a port priority of 10 on trunk 1.
- VLANs 3 through 6 retain the default port priority of 128 on trunk 1.
- VLANs 3 through 6 are assigned a port priority of 10 on trunk 2.
- VLANs 8 through 10 retain the default port priority of 128 on trunk 2.

In this way, trunk 1 carries traffic for VLANs 8 through 10, and trunk 2 carries traffic for VLANs 3 through 6. If the active trunk fails, the trunk with the lower priority takes over and carries the traffic for all of the VLANs. There is no duplication of traffic over any trunk port.

Figure 3-2 Load Sharing by Using STP Port Priorities



Follow these steps to configure the network shown in Figure 3-2:

Step 1 Configure a VTP domain on Switch 1, and configure Switch 1 as a VTP server.

```
Switch_1# vlan database
Switch_1(vlan)# vtp domain milano
Changing VTP domain name from test to milano
Switch_1(vlan)# vtp server
Device mode already VTP SERVER.
```

Step 2 Verify the VTP information by exiting to privileged EXEC mode and displaying the VTP information for both switches.

```
Switch_1(vlan)# exit
APPLY completed.
Exiting...
Switch_1# show vtp status
VTP Version                : 2
Configuration Revision     : 0
Maximum VLANs supported locally : 68
Number of existing VLANs   : 59
VTP Operating Mode         : Server
VTP Domain Name            : milano
VTP Pruning Mode           : Disabled
VTP V2 Mode                : Disabled
VTP Traps Generation       : Disabled
MD5 digest                 : 0x53 0x97 0x06 0x02 0xF8 0x6F
0x45 0x85
Configuration last modified by 172.20.128.151 at 3-5-93 01:05:21
```



Step 3 From privileged EXEC mode, verify that the VLANs exist in the database on Switch 1.

```
Switch_1# show vlan
VLAN Name                Status    Ports
-----
1    default                 active    Fa0/2, Fa0/3, Fa0/4, Fa0/5,
                    Fa0/10, Fa0/11, Fa0/12
2    VLAN0002                active
3    VLAN0003                active
4    VLAN0004                active
5    VLAN0005                active
6    VLAN0006                active
7    VLAN0007                active
8    VLAN0008                active
9    VLAN0009                active
10   VLAN0010                active
```

Step 4 Beginning from privileged EXEC mode, configure the trunks on Switch 1 ports. The trunks default to ISL trunking.

```
Switch_1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch_1(config)# interface fa0/1
Switch_1(config-if)# switchport mode trunk
Switch_1(config-if)# end
```

```
Switch_1# show interface fa0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: isl
Operational Trunking Encapsulation: isl
Negotiation of Trunking: Disabled
Access Mode VLAN: 0 ((Inactive))
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: ALL
Trunking VLANs Active: 1-55
Pruning VLANs Enabled: NONE
```

Repeat this procedure to define the trunk ports on Switch 1 and Switch 2.

- Step 5** When the trunk links come up, VTP passes the VTP and VLAN information to Switch 2. Verify that switch 2 has learned the VLAN configuration.

```
Switch_2# show vlan
VLAN Name                Status      Ports
-----
1    default                active     Fa0/2, Fa0/3, Fa0/4, Fa0/5,
                    Fa0/10, Fa0/11, Fa0/12
2    VLAN0002              active
3    VLAN0003              active
4    VLAN0004              active
5    VLAN0005              active
6    VLAN0006              active
7    VLAN0007              active
8    VLAN0008              active
9    VLAN0009              active
10   VLAN0010              active
```

- Step 6** Use the **spanning-tree** command to assign the different port priorities on the different VLANs.

```
Switch_1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z
Switch_1(config-if)# interface fa0/1
Switch_1(config-if)# spanning-tree vlan 8 9 10 port-priority 10
Switch_1(config-if)# end
Switch_1(config)# interface fa0/2
Switch_1(config-if)# spanning-tree vlan 3 4 5 6 port-priority 10
Switch_1(config-if)# end
```

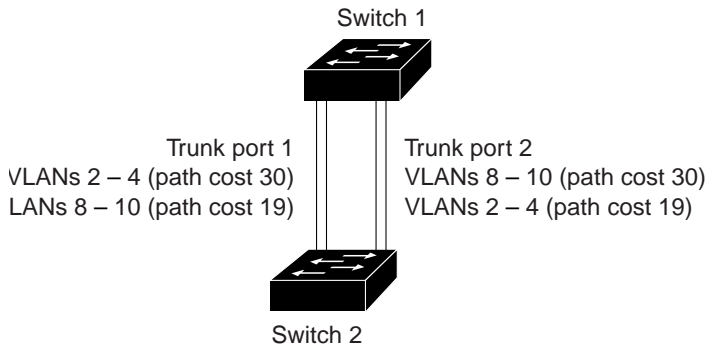
- Step 7** Verify the entries by entering the privileged EXEC **show running-config** command:

```
Switch_1# show running-config
.
→ interface FastEthernet0/1
   switchport mode trunk
   spanning-tree vlan 8 priority 10
   spanning-tree vlan 9 priority 10
   spanning-tree vlan 10 priority 10
   !
→ interface FastEthernet0/2
   switchport mode trunk
   spanning-tree vlan 3 priority 10
   spanning-tree vlan 4 priority 10
   spanning-tree vlan 5 priority 10
   spanning-tree vlan 6 priority 10
   !
   interface FastEthernet0/3
   !
   interface FastEthernet0/4
   port group 11
.
.
```

Load Sharing Using STP Path Cost

You can configure parallel trunks to share VLAN traffic by setting different path costs on a trunk and associating the path costs with different sets of VLANs. The VLANs keep the traffic separate, STP does not disable a port because there are no loops, and redundancy is maintained in the event of a lost link.

Figure 3-3 Load-Sharing Trunks with Traffic Distributed by Path Cost



16591

In this example, trunk ports 1 and 2 are 100BaseT ports. The path costs for the VLANs are assigned as follows:

- VLANs 2 through 4 are assigned a path cost of 30 on trunk port 1.
- VLANs 8 through 10 retain the default 100BaseT path cost on trunk port 1 of 19.
- VLANs 8 through 10 are assigned a path cost of 30 on trunk port 2.
- VLANs 2 through 4 retain the default 100BaseT path cost on trunk port 2 of 19.

Follow these steps to configure two parallel trunks to load share based on the STP path cost parameter:

Step 1 From privileged EXEC mode, configure the two ports as trunk ports. The trunk defaults to ISL trunking.

```
Switch_1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch_1(config)# interface fa0/1
Switch_1(config-if)# switchport mode trunk
Switch_1(config-if)# end
```

```
Switch_1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch_1(config)# interface fa0/2
Switch_1(config-if)# switchport mode trunk
Switch_1(config-if)# end
```

Step 2 Verify the entries by entering the privileged EXEC **show running-config** command:

```
Switch# show running-config
Building configuration...

Current configuration:
!
version 11.2
no service pad
no service udp-small-servers
no service tcp-small-servers
!
hostname Switch
!
enable password grandkey
!
interface VLAN1
 ip address 172.20.128.178 255.255.255.0
 no ip route-cache
!
interface FastEthernet0/1
  switchport mode trunk
  ←
!
interface FastEthernet0/2
  switchport mode trunk
  ←
```

Step 3 When the trunk links come up, Switch 1 receives the VTP information from the other switches. Verify that Switch 1 has learned the VLAN configuration.

```
Switch_1# show vlan
```

VLAN Name	Status	Ports
1 default	active	
2 VLAN0002	active	
3 VLAN0003	active	
4 VLAN0004	active	
5 VLAN0005	active	
6 VLAN0006	active	
7 VLAN0007	active	
8 VLAN0008	active	
9 VLAN0009	active	
10 VLAN0010	active	

- Step 4** Use the **spanning-tree** command to assign the cost parameter to the VLANs that use the trunk on Switch 1.

```
Switch_1# configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Switch_1(config)# interface fa0/1  
—————> Switch_1(config-if)# spanning-tree vlan 2 3 4 cost 30  
Switch_1(config-if)# end
```

```
Switch_1# configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Switch_1(config)# interface fa0/2  
—————> Switch_1(config-if)# spanning-tree vlan 8 9 10 cost 30  
Switch_1(config-if)# end
```

- Step 5** Verify the entry by entering the privileged EXEC **show running-config** command:

```
Switch# show running-config
Building configuration...

Current configuration:
!
version 11.2
no service pad
no service udp-small-servers
no service tcp-small-servers
!
hostname Switch
!
enable password grandkey
!
interface VLAN1
 ip address 172.20.128.179 255.255.255.0
 no ip route-cache
!
interface FastEthernet0/1
 switchport mode trunk
→ spanning-tree vlan 2 cost 30
 spanning-tree vlan 3 cost 30
 spanning-tree vlan 4 cost 30
!
interface FastEthernet0/2
→ spanning-tree vlan 8 cost 30
 spanning-tree vlan 9 cost 30
 spanning-tree vlan 10 cost 30
!
interface FastEthernet0/3
!
interface FastEthernet0/4
```

Redundant Links Using STP UplinkFast

Switches in hierarchical networks can be grouped into backbone switches, distribution switches, and access switches. Figure 3-4 shows a complex network where distribution switches and access switches each have at least one redundant link that is blocked by STP to prevent loops.

If a switch loses connectivity, the switch begins using the alternate paths as soon as STP selects a new root port. When STP reconfigures the new root port, other ports flood the network with multicast packets, one for each address that was learned on the port. You can limit these bursts of multicast traffic by reducing the `max-update-rate` parameter (the default for this parameter is 150 packets per second). However, if you enter zero, station-learning frames are not generated, so the STP topology converges more slowly after a loss of connectivity.

STP UplinkFast is an enhancement that accelerates the choice of a new root port when a link or switch fails or when STP reconfigures itself. The root port transitions to the forwarding state immediately without going through the listening and learning states, as it would do with normal STP procedures. UplinkFast is most useful in edge or access switches and might not be appropriate for backbone devices.

Enabling STP UplinkFast

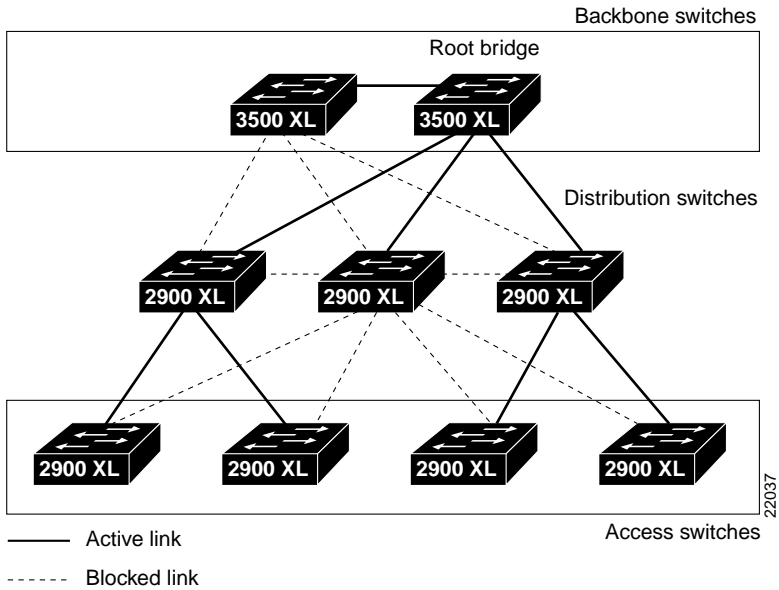
When you enable UplinkFast, it is enabled for the entire switch and cannot be enabled for individual VLANs.

Enter this command in global configuration mode to configure UplinkFast:

```
Switch(config)# spanning-tree uplinkfast [max-update-rate pkts-per-second]
```

Note When UplinkFast is enabled, the bridge priority of all VLANs is set to 49152, and the path cost of all ports and VLAN trunks is increased by 3000. This change reduces the chance that the switch will become the root port. When UplinkFast is disabled, the bridge priorities of all VLANs and path costs of all ports are set to default values.

Figure 3-4 Switches in a Hierarchical Network



Trunks Interacting with Other Features

ISL, IEEE 802.1Q, and ATM trunking interacts with other switch features in the following ways:

Port monitoring	A trunk cannot be a monitor port. A static-access port can monitor the traffic of its VLAN on a trunk port.
Port grouping	<p>ISL and 802.1Q trunks can be grouped into EtherChannel port groups, but all trunks in the group must have the same configuration. ATM ports are always trunks but cannot be part of an EtherChannel port group.</p> <p>When a group is first created, all ports follow the parameters set for the first port to be added to the group. If you change the configuration of one of the following parameters, the switch propagates the setting you entered to all ports in the group:</p> <ul style="list-style-type: none">• Allowed-VLAN list• STP path cost for each VLAN• STP port priority for each VLAN• STP Port Fast setting• Trunk status: if one port in a port group ceases to be a trunk, all port cease to be trunks.
Network port	When configured as a network port, a trunk serves as the network port for all VLANs associated with the port. A network port receives all unknown unicast traffic on a VLAN.
Secure ports	A trunk cannot be a secure port.
Blocking unicast and multicast packets on a trunk	The port block command can be used to block the forwarding of unknown unicast and multicast packets to VLANs on a trunk. However, if the trunk is acting as a network port, unknown unicast packets cannot be blocked.