Chapter 1: Packet Forwarding

Instructor Materials

CCNP Enterprise: Core Networking

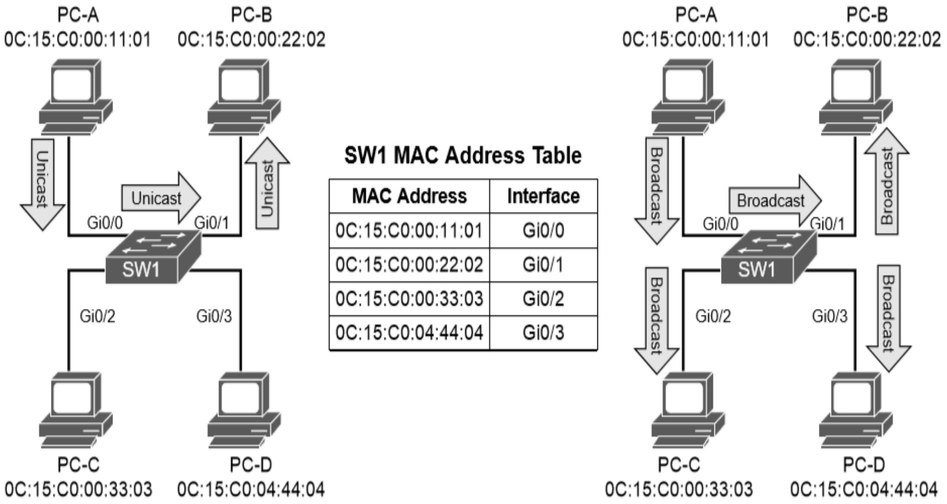
Network Device Communication

- The primary function of a network is to provide connectivity between devices.
- Today most everything is based on Transmission Control Protocol/Internet Protocol (TCP/IP).

Network Device Communication

Collision Domains on a Hub Versus a Switch

- Unknown unicast flooding occurs when a packet contains a destination MAC address that is not in the switch’s MAC address table. The switch forwards the packet out of every switch port.
- Broadcast traffic is network traffic intended for every host on the LAN and is forwarded out of every switch port interface.
- Network broadcasts do not cross Layer 3 boundaries (from one subnet to another).



SW1 MAC Address Table

MAC Address	Interface
0C:15:C0:00:11:01	Gi0/0
0C:15:C0:00:22:02	Gi0/1
0C:15:C0:00:33:03	Gi0/2
0C:15:C0:04:44:04	Gi0/3

Figure 1-3 *Unicast and Broadcast Traffic Patterns*

Network Device Communication

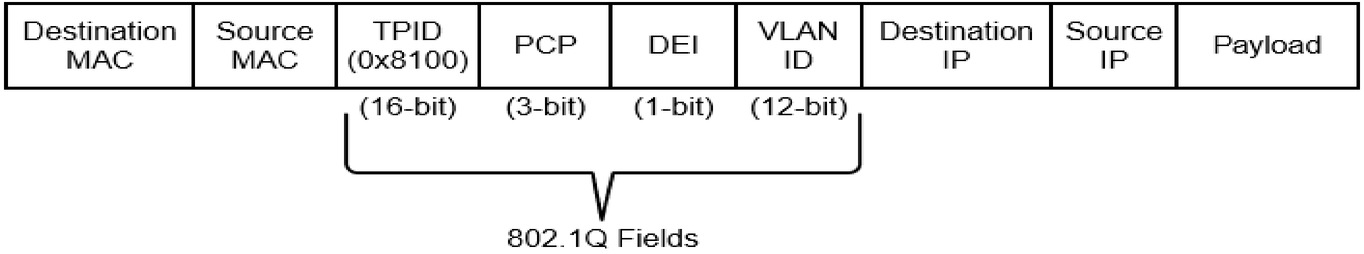
Virtual LANs

- Adding a router between LAN segments helps shrink broadcast domains.

- Virtual LANs (VLANS) provide logical segmentation by creating multiple broadcast domains on the same network switch. VLANs provide higher utilization of switch ports because a port can be associated to the necessary broadcast domain, and multiple broadcast domains can reside on the same switch.

- VLANS are defined in the IEEE 802.1Q standard, which sates that the 32 bits are added to the packet header with the following fields: tag Protocol identifier (TPID), priority code point (PCP), drop eligible indicator (DEI), and VLAN identifier (VLAN ID).

Figure 1-4 displays the VLAN packet structure.



Destination MAC	Source MAC	TPID (0x8100)	PCP	DEI	VLAN ID	Destination IP	Source IP	Payload
		(16-bit)	(3-bit)	(1-bit)	(12-bit)			

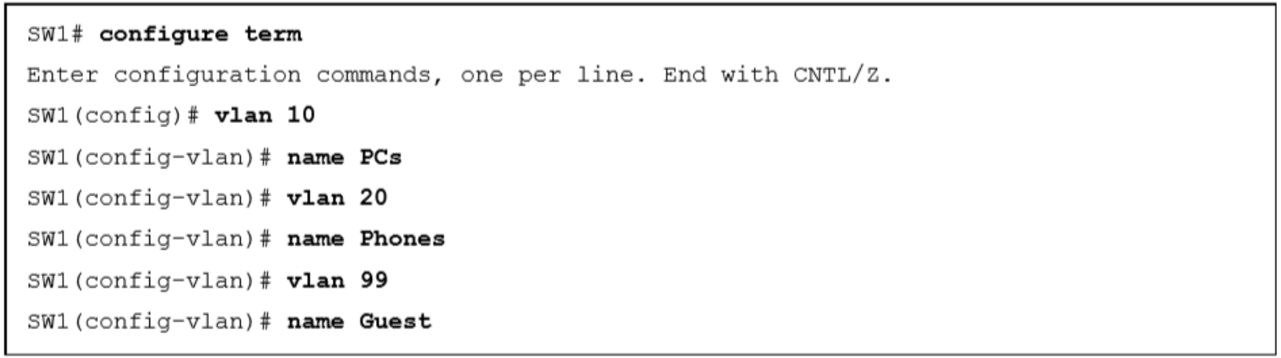
802.1Q Fields

Network Device Communication

Creating a VLAN

- VLANs are created in the global configuration.
- VLANs are named in the VLAN sub-global mode.

Example 1-1 *Creating a VLAN*



```
SW1# configure term
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)# vlan 10
SW1(config-vlan)# name PCs
SW1(config-vlan)# vlan 20
SW1(config-vlan)# name Phones
SW1(config-vlan)# vlan 99
SW1(config-vlan)# name Guest
```

VLANs and their port assignment are verified with the **show vlan [{brief | id** *vlan-id* | name *vlanname* | **summary**}] command.
The output is split into four main sections: VLAN-to-port assignments, system MTU, SPAN sessions, and private VLANs.

Optional show vlan keywords

- Optional **show vlan** keywords provide the following benefits:

- **Brief -** Displays only the relevant port-to-VLAN mappings.
- **Summary -** Displays a count of VLANs, VLANs participating in VTP, and VLANs that in the extended VLAN range.
- **id** *vlan-id* - Displays all the output from the original command but filtered to only the VLAN number that is specified.
- **name** *vlanname* - Displays all the output from the original command but filtered to only the VLAN name that is specified.

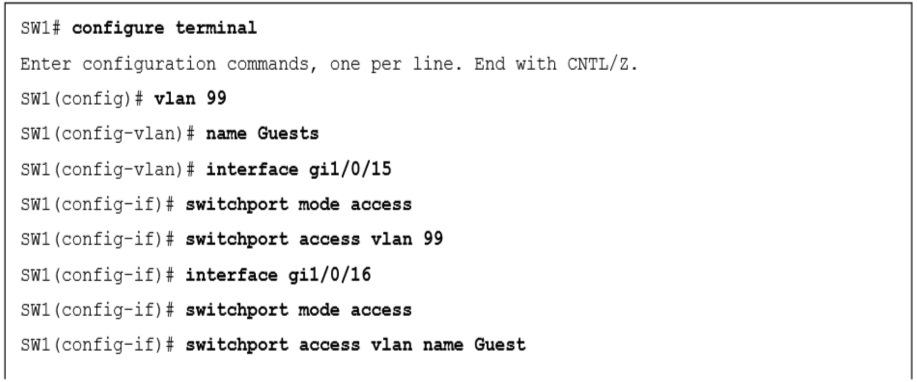
Network Device Communication

Access Ports

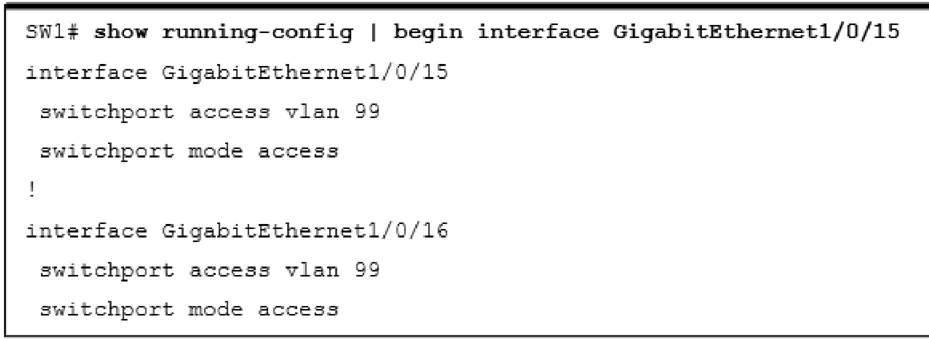
- Access ports are the fundamental building blocks of a managed switch.

- An access port is assigned to only one VLAN.
- It carries traffic from the specified VLAN to the device connected to it or from the device to other devices on the same VLAN.
- Catalyst switch ports are Layer 2 by default.
- Use the command **switchport mode access** to manually configure a port as an access port.
- A specific VLAN is associated to the port with the command **switchport access {vlan** *vlan-id* **| name** *vlanname*}.

Example 1-4 *Configuring an Access Port*



```
SW1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)# vlan 99
SW1(config-vlan)# name Guests
SW1(config-vlan)# interface gi1/0/15
SW1(config-if)# switchport mode access
SW1(config-if)# switchport access vlan 99
SW1(config-if)# interface gi1/0/16
SW1(config-if)# switchport mode access
SW1(config-if)# switchport access vlan name Guest
```



```
SW1# show running-config | begin interface GigabitEthernet1/0/15
interface GigabitEthernet1/0/15
 switchport access vlan 99
 switchport mode access
!
interface GigabitEthernet1/0/16
 switchport access vlan 99
 switchport mode access
```

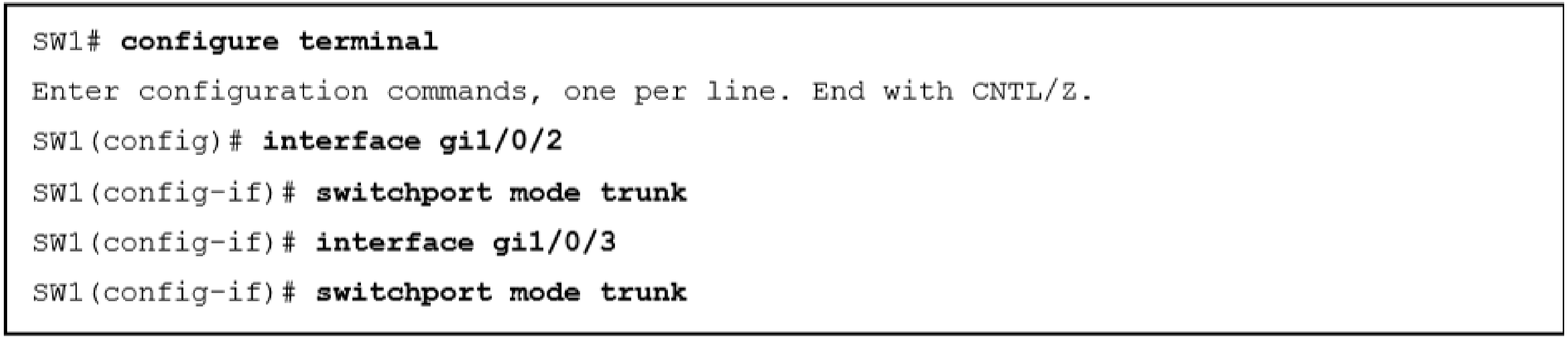
Network Device Communication

Trunk Ports

- Trunk ports can carry multiple VLANs. They are typically used when multiple VLANs need connectivity between a switch and another switch, router, or firewall and use only one port. Trunk ports are statically defined on Catalyst switches with the interface command **switch-port mode trunk**.

- Here is an example of configuring a trunk port:

Example 1-5 *Configuring a Trunk Port*



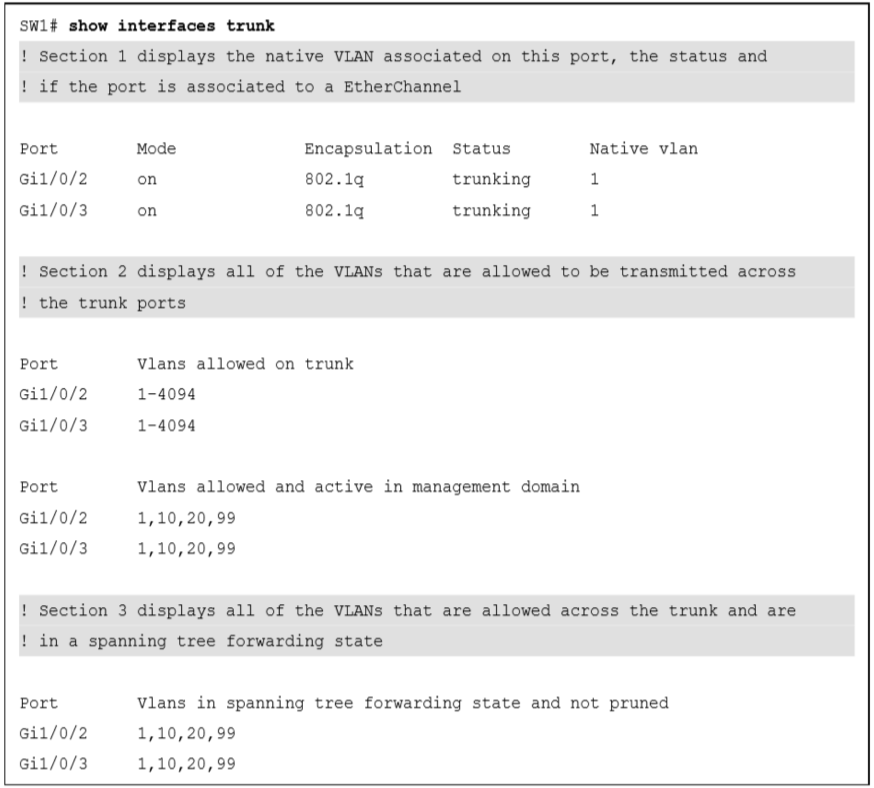
```
SW1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)# interface gi1/0/2
SW1(config-if)# switchport mode trunk
SW1(config-if)# interface gi1/0/3
SW1(config-if)# switchport mode trunk
```

Network Device Communication

Trunk Ports (Cont.)

- The command **show interfaces trunk** provides a lot of valuable information:
  - The first section lists all the interfaces that are trunk ports, the status, the association to an EtherChannel, and whether a VLAN is a native VLAN.
  - The second section of the output displays the list of VLANs that are allowed on the trunk port. Traffic can be minimized on trunk ports to restrict VLANs to specific switches, thereby restricting broadcast traffic, too.
  - The third section displays the VLANs that are in a forwarding state on the switch. Ports that are in blocking state are not listed in this section.

Example 1-6 *Verifying Trunk Port Status*



```
SW1# show interfaces trunk
! Section 1 displays the native VLAN associated on this port, the status and
! if the port is associated to a EtherChannel

Port        Mode             Encapsulation  Status        Native vlan
Gi1/0/2     on               802.1q         trunking      1
Gi1/0/3     on               802.1q         trunking      1

! Section 2 displays all of the VLANs that are allowed to be transmitted across
! the trunk ports

Port        Vlans allowed on trunk
Gi1/0/2     1-4094
Gi1/0/3     1-4094

Port        Vlans allowed and active in management domain
Gi1/0/2     1,10,20,99
Gi1/0/3     1,10,20,99

! Section 3 displays all of the VLANs that are allowed across the trunk and are
! in a spanning tree forwarding state

Port        Vlans in spanning tree forwarding state and not pruned
Gi1/0/2     1,10,20,99
Gi1/0/3     1,10,20,99
```

Native VLANs

▪In the 802.1Q standard, any traffic that is advertised or received on a trunk port without the 802.1Q VLAN tag is associated to the native VLAN.

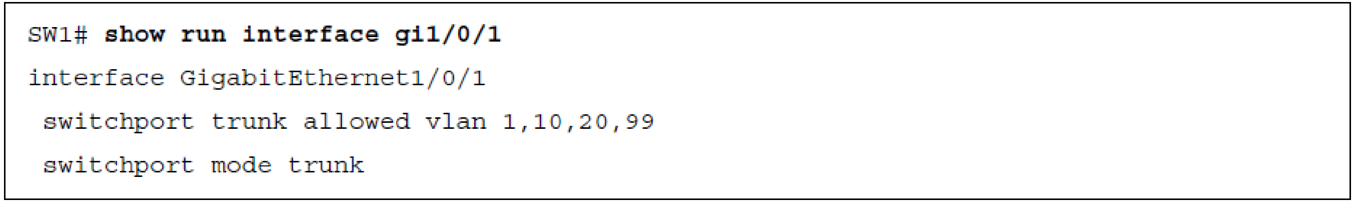
- The default native VLAN is VLAN 1.
- When a switch has two access ports configured as access ports and associated to VLAN 10—that is, a host attached to a trunk port with a native VLAN set to 10—the host could talk to the devices connected to the access ports.
- The native VLAN should match on both trunk ports, or traffic can change VLANs unintentionally. While connectivity between hosts is feasible (assuming that they are on the different VLAN numbers), this causes confusion for most network engineers and is not a best practice.
- A native VLAN is a port-specific configuration and is changed with the interface command **switchport trunk native vlan** *vlan-id*.

Network Device Communication

Allowed VLANs

- The interface command **switchport trunk allowed vlan** *vlan-ids* specifies the VLANs that are allowed to traverse the link. Example 1-7 displays sample a configuration for limiting the VLANs that can cross the Gi1/0/2 trunk port for VLANs 1, 10, 20, and 99.

Example 1-7 *Viewing the VLANs That Are Allowed on a Trunk Link*



```
SW1# show run interface gi1/0/1
interface GigabitEthernet1/0/1
 switchport trunk allowed vlan 1,10,20,99
 switchport mode trunk
```

- The full command syntax **switchport trunk allowed** {*vlan-ids* | **all | none | add** vlan-ids | **remove** *vlan-ids* | **except** *vlan-ids*} provides a lot of power in a single command.

- The optional keyword **all** allows for all VLANs, while **none** removes all VLANs from the trunk link.

- The **add** keyword adds additional VLANs to those already listed, and the **remove** keyword removes the specified VLAN from the VLANs already identified for that trunk link.

Network Device Communication

MAC Address Table

- The MAC address table is responsible for identifying the switch ports and VLANs with which a device is associated. A switch builds the MAC address table by examining the source MAC address for the traffic that it receives. This information is then maintained to shrink the collision domain (point-to-point communication between devices and switches) by reducing the amount of unknown unicast flooding.

- The MAC address table is displayed with the command **show mac address-table** [address mac-address | dynamic | vlan vlan-id]. The optional keywords with this command provide the following benefits:

  - **address** *mac-address* - Displays entries that match the explicit MAC address. This command could be beneficial on switches with hundreds of ports.

  - **dynamic** - Displays entries that are dynamically learned and are not statically set or burned in on the switch.

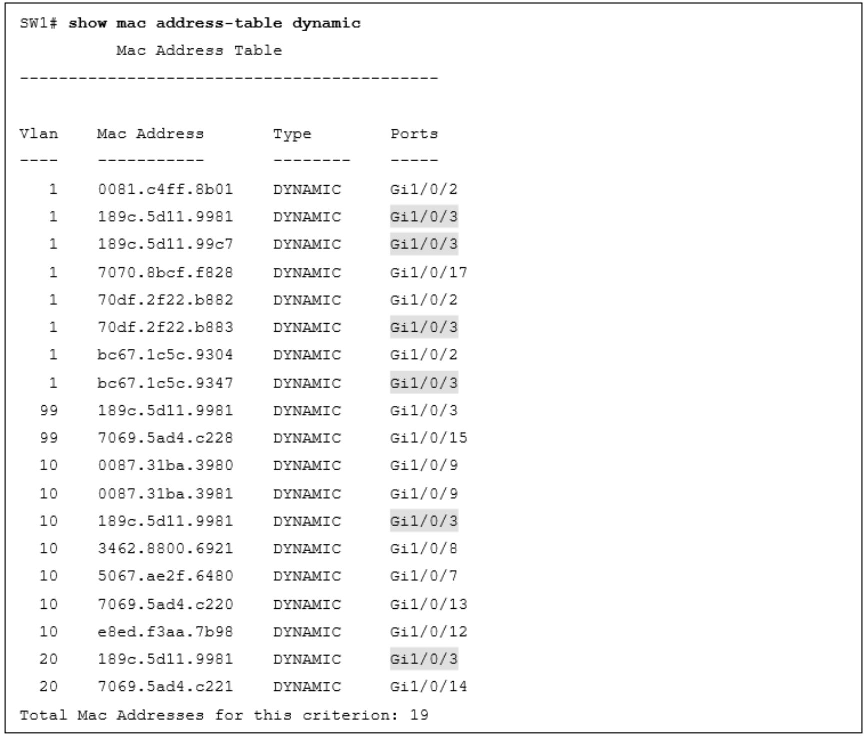
  - **vlan** *vlan-id* - Displays entries that matches the specified VLAN.

Network Device Communication

MAC Address Table (Cont.)

- The command **mac address-table static mac-address vlan** *vlan-id* {**drop | interface** *interface-id*} adds a manual entry with the ability to associate it to a specific switch port or to drop traffic upon receipt.
- The command **clear mac address-table dynamic [{address** *mac-address* | **interface** *interface-id* | **vlan** *vlan-id*}] flushes the MAC address table for the entire switch.
- The MAC address table resides in content addressable memory (CAM). The CAM uses high-speed memory that is faster than typical computer RAM due to its search techniques. The CAM table provides a binary result for any query of 0 for true or 1 for false.

Example 1-8 *Viewing the MAC Address Table*



```
SW1# show mac address-table dynamic
          Mac Address Table
-------------------------------------------


Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0081.c4ff.8b01    DYNAMIC     Gi1/0/2
   1    189c.5d11.9981    DYNAMIC     Gi1/0/3
   1    189c.5d11.99c7    DYNAMIC     Gi1/0/3
   1    7070.8bcf.f828    DYNAMIC     Gi1/0/17
   1    70df.2f22.b882    DYNAMIC     Gi1/0/2
   1    70df.2f22.b883    DYNAMIC     Gi1/0/3
   1    bc67.1c5c.9304    DYNAMIC     Gi1/0/2
   1    bc67.1c5c.9347    DYNAMIC     Gi1/0/3
  99    189c.5d11.9981    DYNAMIC     Gi1/0/3
  99    7069.5ad4.c228    DYNAMIC     Gi1/0/15
  10    0087.31ba.3980    DYNAMIC     Gi1/0/9
  10    0087.31ba.3981    DYNAMIC     Gi1/0/9
  10    189c.5d11.9981    DYNAMIC     Gi1/0/3
  10    3462.8800.6921    DYNAMIC     Gi1/0/8
  10    5067.ae2f.6480    DYNAMIC     Gi1/0/7
  10    7069.5ad4.c220    DYNAMIC     Gi1/0/13
  10    e8ed.f3aa.7b98    DYNAMIC     Gi1/0/12
  20    189c.5d11.9981    DYNAMIC     Gi1/0/3
  20    7069.5ad4.c221    DYNAMIC     Gi1/0/14
Total Mac Addresses for this criterion: 19
```

Network Device Communication

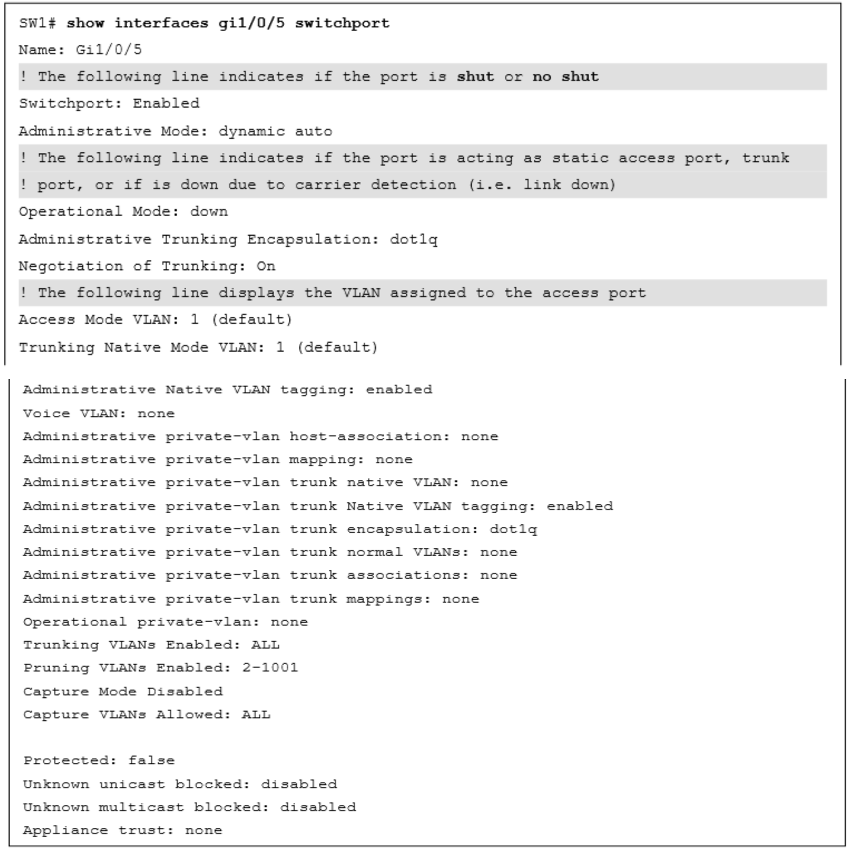
Switch Port Status

- Examining the configuration for a switch port can be useful; however, some commands stored elsewhere in the configuration preempt the configuration set on the interface.

- The command **show interfaces** *interface-id* **switchport** provides all the relevant information for a switch port’s status.

- The command **show interfaces switchport** displays the same information for all ports on the switch.

Example 1-9 *Viewing the Switch Port Status*



```
SW1# show interfaces gi1/0/5 switchport
Name: Gi1/0/5
! The following line indicates if the port is shut or no shut
Switchport: Enabled
Administrative Mode: dynamic auto
! The following line indicates if the port is acting as static access port, trunk
! port, or if is down due to carrier detection (i.e. link down)
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
! The following line displays the VLAN assigned to the access port
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

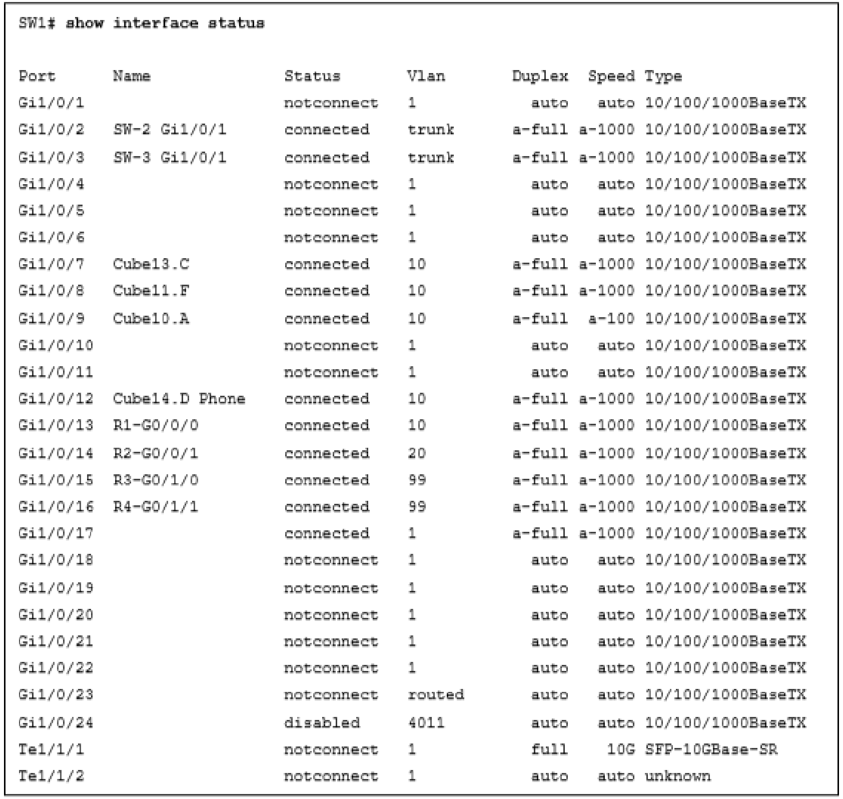
Network Device Communication

Interface Status

- The command **show interface status** is another useful command for viewing the status of switch ports in a very condensed and simplified manner.

- **Port -** Displays the interface ID or port channel.
- **Name -** Displays the configured interface description.
- **Status -** Displays connected for links where a connection was detected and established to bring up the link. Displays not connect for when a link is not detected and err-disabled when an error has been detected and the switch has disabled the ability to forward traffic out of that port.

Example 1-10 *Viewing Overall Interface Status*



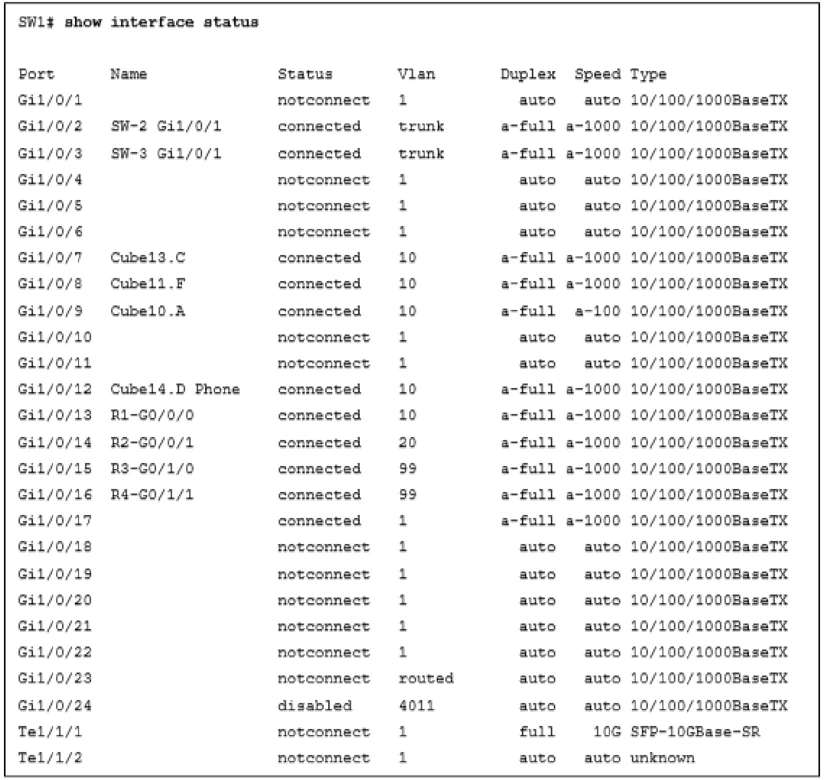
```
SW1# show interface status

Port      Name               Status       Vlan       Duplex  Speed Type
Gi1/0/1                      notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/2   SW-2 Gi1/0/1       connected    trunk      a-full a-1000 10/100/1000BaseTX
Gi1/0/3   SW-3 Gi1/0/1       connected    trunk      a-full a-1000 10/100/1000BaseTX
Gi1/0/4                      notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/5                      notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/6                      notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/7   Cube13.C           connected    10         a-full a-1000 10/100/1000BaseTX
Gi1/0/8   Cube11.F           connected    10         a-full a-1000 10/100/1000BaseTX
Gi1/0/9   Cube10.A           connected    10         a-full  a-100 10/100/1000BaseTX
Gi1/0/10                     notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/11                     notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/12  Cube14.D Phone     connected    10         a-full a-1000 10/100/1000BaseTX
Gi1/0/13  R1-G0/0/0          connected    10         a-full a-1000 10/100/1000BaseTX
Gi1/0/14  R2-G0/0/1          connected    20         a-full a-1000 10/100/1000BaseTX
Gi1/0/15  R3-G0/1/0          connected    99         a-full a-1000 10/100/1000BaseTX
Gi1/0/16  R4-G0/1/1          connected    99         a-full a-1000 10/100/1000BaseTX
Gi1/0/17                     connected    1          a-full a-1000 10/100/1000BaseTX
Gi1/0/18                     notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/19                     notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/20                     notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/21                     notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/22                     notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/23                     notconnect   routed       auto   auto 10/100/1000BaseTX
Gi1/0/24                     disabled     4011         auto   auto 10/100/1000BaseTX
Te1/1/1                      notconnect   1            full    10G SFP-10GBase-SR
Te1/1/2                      notconnect   1            auto   auto unknown
```

Network Device Communication

Interface Status (Cont.)

- **VLAN -** Displays the VLAN number assigned for access ports. Trunk links appear as trunk, and ports configured as Layer 3 interfaces display routed.
- **Duplex -** Displays the duplex of the port. If the duplex auto-negotiated, it is prefixed by a-.
- **Speed -** Displays the speed of the port. If the port speed was auto-negotiated, it is prefixed by a-.
- **Type -** Displays the type of interface for the switch port. If it is a fixed RJ-45 copper port, it includes TX in the description (for example, 10/100/1000BASE-TX). Small form-factor pluggable (SFP)–based ports are listed with the SFP model if there is a driver for it in the software; otherwise, it says unknown.

Example 1-10 *Viewing Overall Interface Status*



```
SW1# show interface status

Port      Name               Status       Vlan       Duplex  Speed Type
Gi1/0/1                      notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/2   SW-2 Gi1/0/1       connected    trunk      a-full a-1000 10/100/1000BaseTX
Gi1/0/3   SW-3 Gi1/0/1       connected    trunk      a-full a-1000 10/100/1000BaseTX
Gi1/0/4                      notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/5                      notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/6                      notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/7   Cube13.C           connected    10         a-full a-1000 10/100/1000BaseTX
Gi1/0/8   Cube11.F           connected    10         a-full a-1000 10/100/1000BaseTX
Gi1/0/9   Cube10.A           connected    10         a-full  a-100 10/100/1000BaseTX
Gi1/0/10                     notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/11                     notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/12  Cube14.D Phone     connected    10         a-full a-1000 10/100/1000BaseTX
Gi1/0/13  R1-G0/0/0          connected    10         a-full a-1000 10/100/1000BaseTX
Gi1/0/14  R2-G0/0/1          connected    20         a-full a-1000 10/100/1000BaseTX
Gi1/0/15  R3-G0/1/0          connected    99         a-full a-1000 10/100/1000BaseTX
Gi1/0/16  R4-G0/1/1          connected    99         a-full a-1000 10/100/1000BaseTX
Gi1/0/17                     connected    1          a-full a-1000 10/100/1000BaseTX
Gi1/0/18                     notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/19                     notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/20                     notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/21                     notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/22                     notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/23                     notconnect   routed       auto   auto 10/100/1000BaseTX
Gi1/0/24                     disabled     4011         auto   auto 10/100/1000BaseTX
Te1/1/1                      notconnect   1            full    10G SFP-10GBase-SR
Te1/1/2                      notconnect   1            auto   auto unknown
```

Network Device Communication

Layer 3 Forwarding and Local Network Forwarding

- Some of the Layer 3 forwarding logic occurs before Layer 2 forwarding. There are two main methodologies for Layer 3 forwarding:
  - Forwarding traffic to devices on the same subnet
  - Forwarding traffic to devices on a different subnet
- **Local Network forwarding**
  - Two devices that reside on the same subnet communicate locally. As the data is encapsulated with its IP address, the device detects that the destination is on the same network. However, the device still needs to encapsulate the Layer 2 information to the packet. It knows its own MAC address but does not initially know the destination's MAC address.
  - The Address Resolution Protocol (ARP) table provides a method of mapping Layer 3 IP addresses to Layer 2 MAC addresses by storing the IP address of a host and its corresponding MAC address.
  - The ARP table can be viewed with the command **show ip arp** [*mac-address* | *ip-address* | **vlan** *vlan-id* | *interface-id*]. The optional keywords make it possible to filter the information.

Network Device Communication

Packet Routing

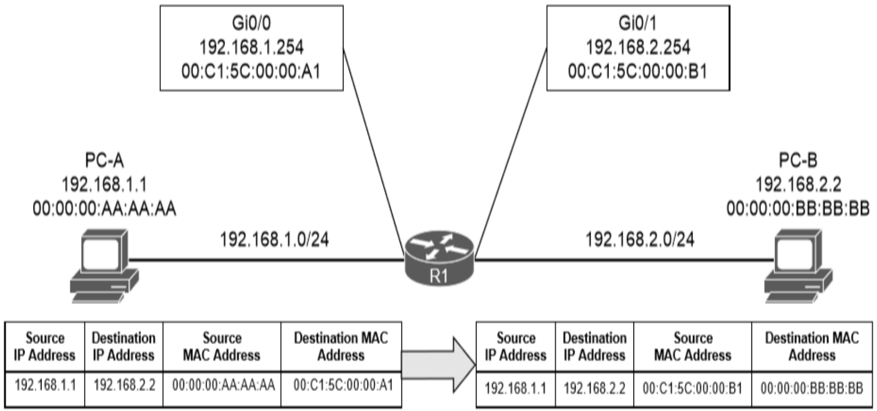
- Packets must be routed when two devices are on different networks. As the data is encapsulated with its IP address, a device detects that its destination is on a different network and must be routed. The device checks its local routing table to identify its next-hop IP address, which may be learned in one of several ways:

- From a static route entry, it can get the destination network, subnet mask, and next-hop IP address.
- A default-gateway is a simplified static default route that just asks for the local next-hop IP address for all network traffic.
- Routes can be learned from routing protocols.

Network Device Communication

Packet Routing (Cont.)

- The source device must add the appropriate Layer 2 headers (source and destination MAC addresses), but the destination MAC address is needed for the next-hop IP address.
  - The device looks for the next-hop IP addresses entry in the ARP table and uses the MAC address from the next-hop IP address's entry as the destination MAC address.
  - The next step is to send the data packet forwarding.
- The next router receives the packet based on the destination MAC address
  - It analyzes the destination IP address
  - Locates the appropriate network entry in its routing table
  - Identifies the outbound interface
  - Then finds the MAC address for the destination device (or the MAC address for the next-hop address if it needs to be routed further)



Source IP Address	Destination IP Address	Source MAC Address	Destination MAC Address
192.168.1.1	192.168.2.2	00:00:00:AA:AA:AA	00:C1:5C:00:00:A1

Source IP Address	Destination IP Address	Source MAC Address	Destination MAC Address
192.168.1.1	192.168.2.2	00:C1:5C:00:00:B1	00:00:00:BB:BB:BB

Figure 1-5 *Layer 2 Addressing Rewrite*

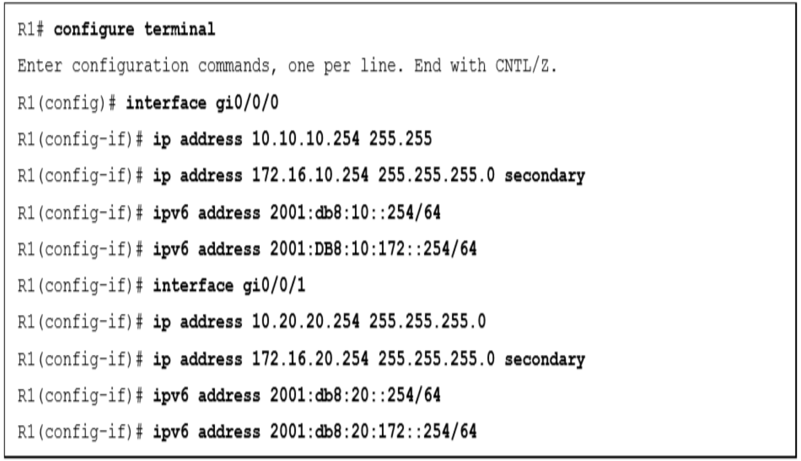
Network Device Communication

IP Address Assignment

▪Technologies and mechanisms have been created to allow IPv4 and IPv6 networks to communicate with each other. With either version, an IP address must be assigned to an interface for a router or multilayer switch to route packets.

- An interface with a configured IP address and that is in an up state injects the associated network into the router’s routing table (Routing Information Base [RIB]).
- Connected networks or routes have an administrative distance (AD) of zero.
- It is possible to attach multiple IPv4 networks to the same interface by attaching a secondary IPv4 address to the same interface with the command **ip address** *ip-address subnet-mask* **secondary**.
- IPv6 addresses are assigned with the interface configuration command **ipv6 address** *ipv6-address/prefix-length.*

Example 1-11 *Assigning IP Addresses to Routed Interfaces*



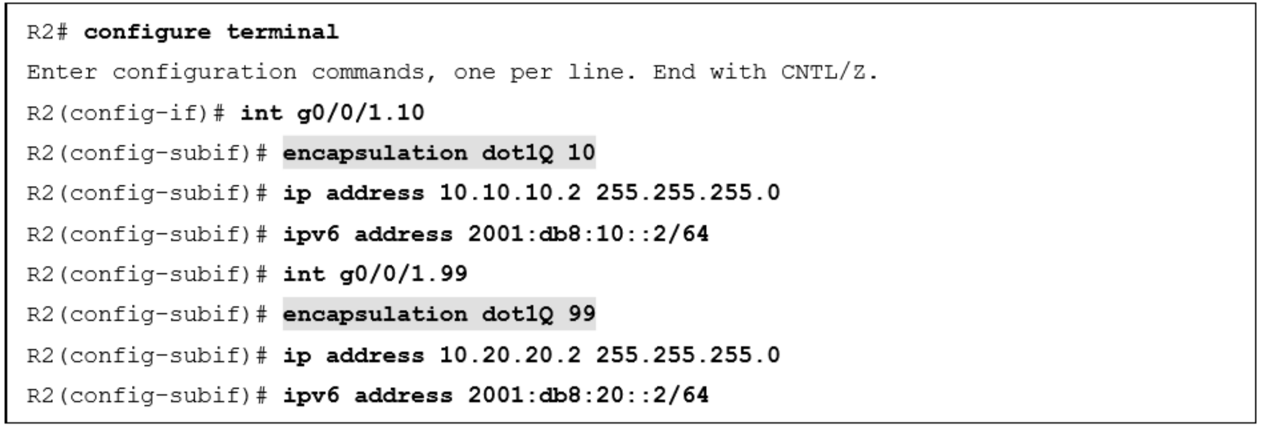
```
R1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# interface gi0/0/0
R1(config-if)# ip address 10.10.10.254 255.255
R1(config-if)# ip address 172.16.10.254 255.255.255.0 secondary
R1(config-if)# ipv6 address 2001:db8:10::254/64
R1(config-if)# ipv6 address 2001:DB8:10:172::254/64
R1(config-if)# interface gi0/0/1
R1(config-if)# ip address 10.20.20.254 255.255.255.0
R1(config-if)# ip address 172.16.20.254 255.255.255.0 secondary
R1(config-if)# ipv6 address 2001:db8:20::254/64
R1(config-if)# ipv6 address 2001:db8:20:172::254/64
```

Network Device Communication

Routed Subinterfaces

- It is possible to configuring the switch’s interface as a trunk port and creating logical subinterfaces on a router. A subinterface is created by appending a period and a numeric value after the period. Then the VLAN needs to be associated with the subinterface with the command **encapsulation dot1q** *vlan-id*.

Example 1-12 *Configuring Routed Subinterfaces*



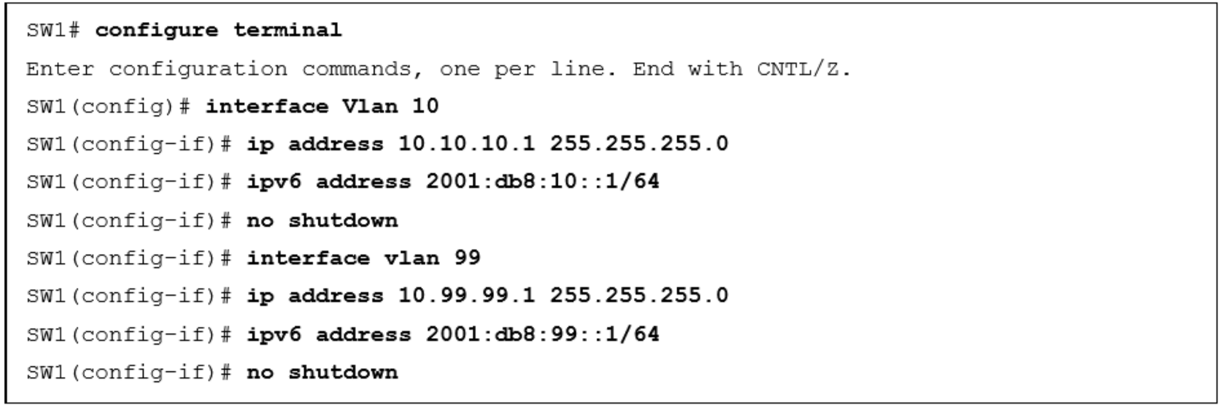
```
R2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config-if)# int g0/0/1.10
R2(config-subif)# encapsulation dot1Q 10
R2(config-subif)# ip address 10.10.10.2 255.255.255.0
R2(config-subif)# ipv6 address 2001:db8:10::2/64
R2(config-subif)# int g0/0/1.99
R2(config-subif)# encapsulation dot1Q 99
R2(config-subif)# ip address 10.20.20.2 255.255.255.0
R2(config-subif)# ipv6 address 2001:db8:20::2/64
```

Network Device Communication

Switched Virtual Interfaces

- With Catalyst switches it is possible to assign an IP address to a switched virtual interface (SVI), also known as a VLAN interface.
- An SVI is configured by defining the VLAN on the switch and then defining the VLAN interface with the command **interface vlan** *vlan-id*.
- The switch must have an interface associated to that VLAN in an up state for the SVI to be in an up state. If the switch is a multilayer switch, the SVIs can be used for routing packets between VLANs without the need of an external router.

Example 1-13 *Creating a Switched Virtual Interface (SVI)*



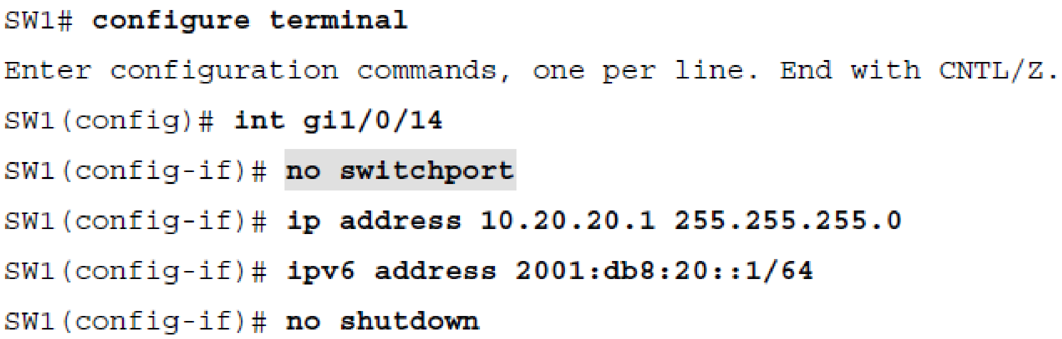
```
SW1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)# interface Vlan 10
SW1(config-if)# ip address 10.10.10.1 255.255.255.0
SW1(config-if)# ipv6 address 2001:db8:10::1/64
SW1(config-if)# no shutdown
SW1(config-if)# interface vlan 99
SW1(config-if)# ip address 10.99.99.1 255.255.255.0
SW1(config-if)# ipv6 address 2001:db8:99::1/64
SW1(config-if)# no shutdown
```

Network Device Communication

Routed Switchports

- Some network designs include a point-to-point link between switches for routing. For example, when a switch needs to connect to a router, some would build a transit VLAN (for example, VLAN 2001), associate the port connecting to the router to VLAN 2001, and then build an SVI for VLAN 2001. There is always the potential that VLAN 2001 could exist elsewhere in the Layer 2 realm or that spanning tree could impact the topology.

- Instead, the multilayer switch port can be converted from a Layer 2 switch port to a routed switch port with the interface configuration command **no switchport**. Then the IP address can be assigned to it.



```
SW1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)# int gi1/0/14
SW1(config-if)# no switchport
SW1(config-if)# ip address 10.20.20.1 255.255.255.0
SW1(config-if)# ipv6 address 2001:db8:20::1/64
SW1(config-if)# no shutdown
```

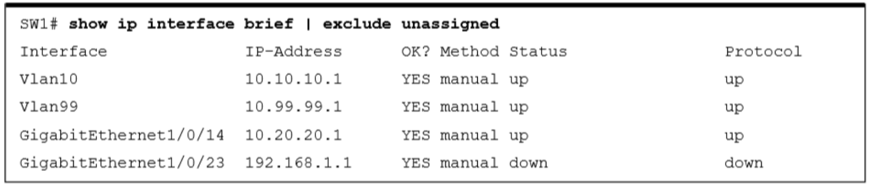
Network Device Communication

Verification of IP Addresses

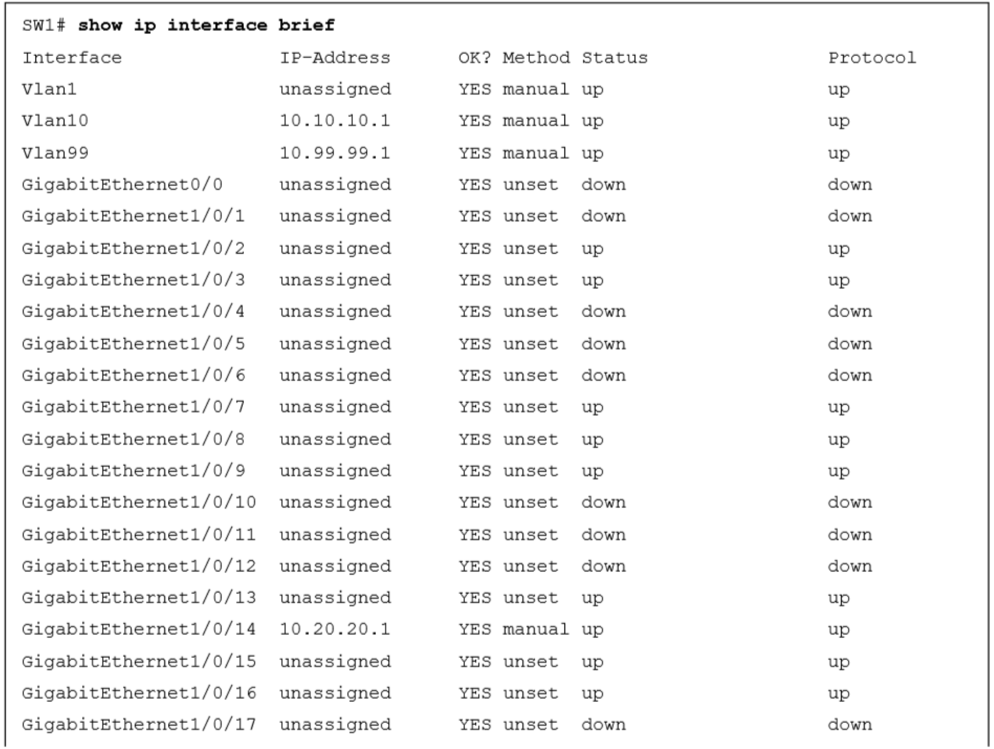
- IPv4 addresses can be viewed with the command **show ip interface [brief |** *interface-id* **| vlan** *vlan-id***].**

- This command’s output contains:

- MTU, DHCP relay, ACLs, and the primary IP address.



```
SW1# show ip interface brief | exclude unassigned
Interface              IP-Address      OK? Method Status                Protocol
Vlan10                 10.10.10.1      YES manual up                    up
Vlan99                 10.99.99.1      YES manual up                    up
GigabitEthernet1/0/14  10.20.20.1      YES manual up                    up
GigabitEthernet1/0/23  192.168.1.1     YES manual down                  down
```



```
SW1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  unassigned      YES manual up                    up
Vlan10                 10.10.10.1      YES manual up                    up
Vlan99                 10.99.99.1      YES manual up                    up
GigabitEthernet0/0     unassigned      YES unset  down                  down
GigabitEthernet1/0/1   unassigned      YES unset  down                  down
GigabitEthernet1/0/2   unassigned      YES unset  up                    up
GigabitEthernet1/0/3   unassigned      YES unset  up                    up
GigabitEthernet1/0/4   unassigned      YES unset  down                  down
GigabitEthernet1/0/5   unassigned      YES unset  down                  down
GigabitEthernet1/0/6   unassigned      YES unset  down                  down
GigabitEthernet1/0/7   unassigned      YES unset  up                    up
GigabitEthernet1/0/8   unassigned      YES unset  up                    up
GigabitEthernet1/0/9   unassigned      YES unset  up                    up
GigabitEthernet1/0/10  unassigned      YES unset  down                  down
GigabitEthernet1/0/11  unassigned      YES unset  down                  down
GigabitEthernet1/0/12  unassigned      YES unset  down                  down
GigabitEthernet1/0/13  unassigned      YES unset  up                    up
GigabitEthernet1/0/14  10.20.20.1      YES manual up                    up
GigabitEthernet1/0/15  unassigned      YES unset  up                    up
GigabitEthernet1/0/16  unassigned      YES unset  up                    up
GigabitEthernet1/0/17  unassigned      YES unset  down                  down
```

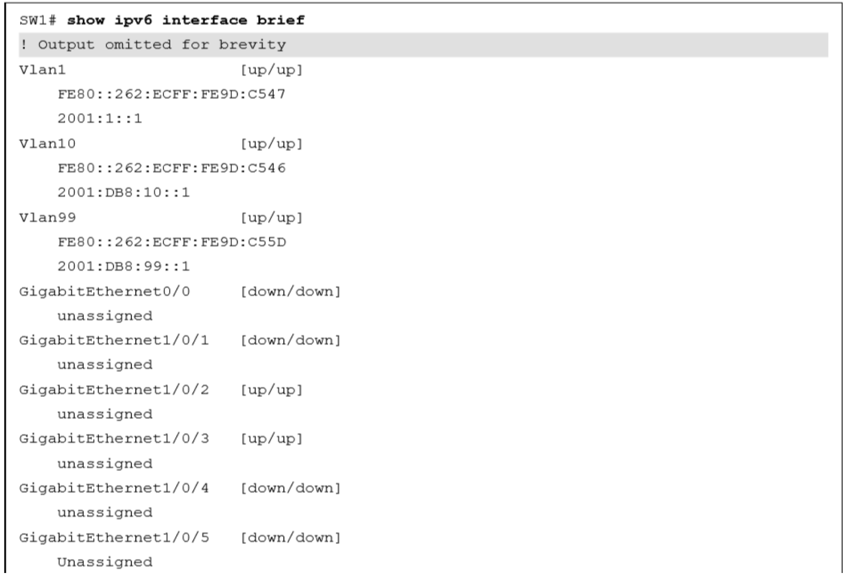
Network Device Communication

Verification of IP Addresses (Contd.)

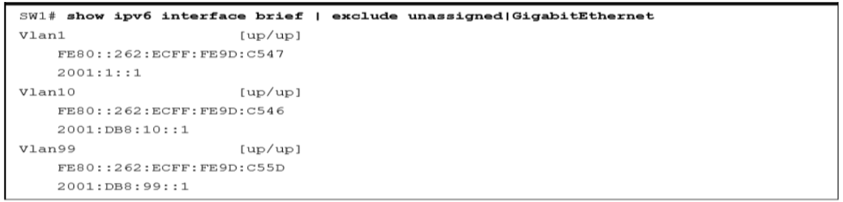
- The same information can be viewed for IPv6 addresses with the command **show ipv6 interface [brief** | *interface-id* **| vlan** *vlan-id*].

- Just as with IPv4 addresses, a CLI parser can be used to reduce the information to what is relevant, as demonstrated in Example 1-16.

Example 1-16 *Viewing Device IPv6 Addresses*



```
SW1# show ipv6 interface brief
! Output omitted for brevity
Vlan1                      [up/up]
    FE80::262:ECFF:FE9D:C547
    2001:1::1
Vlan10                     [up/up]
    FE80::262:ECFF:FE9D:C546
    2001:DB8:10::1
Vlan99                     [up/up]
    FE80::262:ECFF:FE9D:C55D
    2001:DB8:99::1
GigabitEthernet0/0         [down/down]
    unassigned
GigabitEthernet1/0/1       [down/down]
    unassigned
GigabitEthernet1/0/2       [up/up]
    unassigned
GigabitEthernet1/0/3       [up/up]
    unassigned
GigabitEthernet1/0/4       [down/down]
    unassigned
GigabitEthernet1/0/5       [down/down]
    Unassigned
```



```
SW1# show ipv6 interface brief | exclude unassigned|GigabitEthernet
Vlan1                      [up/up]
    FE80::262:ECFF:FE9D:C547
    2001:1::1
Vlan10                     [up/up]
    FE80::262:ECFF:FE9D:C546
    2001:DB8:10::1
Vlan99                     [up/up]
    FE80::262:ECFF:FE9D:C55D
    2001:DB8:99::1
```

Prepare for the Exam

Prepare for the Exam

Key Topics for Chapter 1

Description
Collision Domain
Virtual LANs (VLANs)
Access Ports
Trunk Ports
Content Addressable Memory
Address Resolution Protocol (ARP)
Packet Routing

Prepare for the Exam

Key Topics for Chapter 1 (Cont.)

Description
IP Address Assignment
Process Switching
Cisco Express Forwarding (CEF)
Ternary Content Addressable Memory
Software CEF
SDM Template

Prepare for the Exam

Key Terms for Chapter 1

Key Terms	
Access port	Forwarding Information Base (FIB)
Address Resolution Protocol (ARP)	MAC address table
Broadcast Domain	native VLAN
Cisco Express Forwarding (CEF)	process switching
collision domain	Routing Information Base (RIB)
content addressable memory (CAM)	trunk port
Layer 2 forwarding	ternary content addressable memory (TCAM)
Layer 3 forwarding	virtual LAN (VLAN)

Prepare for the Exam

Command Reference for Chapter 1

Task	Command Syntax
Define a VLAN	**vlan** *vlan-id* **name** *vlanname*
Configure and interface as a trunk port	**switchport mode trunk**
Configure an interface as an access port assigned to a specific VLAN	**switchport mode access** **switchport access** {**vlan** *vlan-id* | **name** *name*}
Configure a static MAC address entry	**mac address-table static mac-address vlan** *vlan-id* **interface** *interface-id*
Clear MAC addresses from the MAC address table	**clear mac address-table dynamic** **[{address** *mac-address* | **interface** *interface-id* | **vlan** *vlan-id*}]

Prepare for the Exam

Command Reference for Chapter 1 (Cont.)

Task	Command Syntax
Assign an IPv4 address to an interface	**ip address** *ip-address subnet-mask*
Assign a secondary IPv4 address to an interface	**ip address** *ip-address subnet-mask* **secondary**
Assign an IPv6 address to an interface	**ipv6 address** *ipv6-address/prefix-length*
Modify the SDM database	**sdm prefer {vlan | advanced**}
Display the interfaces that are configured as a trunk port and all the VLANs that they permit	**show interfaces trunk**

Prepare for the Exam

Command Reference for Chapter 1 (Cont.)

Task	Command Syntax
Display the list of VLANs and their associated ports	**show vlan [{brief | id** *vlan-id* | name *vlanname* | **summary}]**
Display the MAC address table for a switch	**show mac address-table [address** *mac-address* | **dynamic | vlan** *vlan-id*]
Display the current interface state, including duplex, speed, and link state	**show interfaces**
Display the Layer 2 configuration information for a specific switchport	**show interfaces** *interface-id* **switchport**
Display the ARP table	**show ip arp** [*mac-address* | *ip-address* **| vlan** *vlan-id* | *interface-id*].
Displays the IP interface table	**show ip interface [brief** | *interface-id* | **vlan** *vlan-id*]
Display the IPv6 interface table	**show ipv6 interface [brief** | *interface-id* | **vlan** *vlan-id]*

Thank you! Questions?

Vladimír Veselý

updated: 2023-09-20

https://www.fit.vutbr.cz/research/groups/nes@fit

Chapter 2: Spanning Tree

Instructor Materials

CCNP Enterprise: Core Networking

Spanning Tree Protocol Fundamentals

- Spanning Tree Protocol (STP) enables switches to become aware of other switches through the advertisement and receipt of bridge protocol data units (BPDUs).
- STP operates by selecting a master switch and running a tree-based algorithm to identify which redundant ports should not forward traffic.

Spanning Tree Protocol Fundamentals

Spanning Tree Versions

- STP has multiple iterations:
- 802.1D, which is the original specification
- Per-VLAN Spanning Tree (PVST)
- Per-VLAN Spanning Tree Plus (PVST+)
- 802.1W Rapid Spanning Tree Protocol (RSTP)
- 802.1S Multiple Spanning Tree Protocol (MST)
- **Note**: Catalyst switches now operate in PVST+, RSTP, and MST modes. All three of these modes are backward compatible with 802.1D.

IEEE 802.1D STP Port States

Every port transitions through the following states:

Port States	**Description**
Disabled	The port is in an administratively off position (that is, shut down).
Blocking	The switch port is enabled, but the port is not forwarding any traffic.
Listening	The switch port has transitioned from a blocking state and can now send or receive only BPDUs.
Learning	The switch port can modify the MAC address table. The switch still does not forward any other network traffic besides BPDUs.
Forwarding	The switch port can forward all network traffic and can update the MAC address table as expected.
Broken	The switch has detected a problem on a port that can have major effects. The port discards packets as long as the problem continues to exist.

802.1D STP Port Types

The 802.1D STP standard defines the following three port types:

Port Types	**Description**
Root port (RP)	A network port that connects to the root bridge or an upstream switch in the spanning-tree topology. There should be only one root port per VLAN on a switch.
Designated port (DP)	A network port that receives and forwards BPDU frames to other switches. Designated ports provide connectivity to downstream devices and switches. There should be only one active designated port on a link.
Blocking port	A network that is not forwarding traffic because of STP calculations.

Spanning Tree Protocol Fundamentals

STP Key Terminology

Terms	Description
Root Bridge	The most important switch. All ports are in a forwarding state and are categorized as designated ports.
Bridge protocol data unit (BPDU)	Used to identify a hierarchy and notify of changes in the topology There are two types of BPDUs: configuration BPDU and topology change notification BPDU.
Configuration BPDU	Used to identify the root bridge, root, designated, and blocking ports.
Topology change notification (TCN) BPDU	Used to communicate changes in the Layer 2 topology to other switches.
Root path cost	The combined cost for a specific path toward the root switch.

STP Key Terminology (Cont.)

Terms	Description
System priority	This 4-bit value indicates the preference for a switch to be root bridge. The default value is 32,768.
System ID extension	This 12-bit value indicates the VLAN that the BPDU correlates.
Root bridge identifier	This is a combination of the root bridge system MAC address, system ID extension, and system priority of the root bridge.
Local bridge identifier	This is a combination of the local switch’s bridge system MAC address, system ID extension, and system priority of the root bridge.
Max age	Maximum length of time that passes before a bridge port saves its BPDU information. The default value is 20 seconds.
Hello time	The time that a BPDU is advertised out of a port. The default value is 2 seconds, but the value can be configured to 1 to 10 seconds.
Forward delay	The amount of time that a port stays in a listening and learning state. The default value is 15 seconds.

STP Path Cost

- The root path is found based on the cumulative interface STP cost to reach the root bridge.
- The interface STP cost was originally stored as a 16-bit value with a reference value of 20 Gbps.
- Another method, called *long mode*, uses a 32-bit value and uses a reference speed of 20 Tbps.
- The original method, known as *short mode*, is the default mode.

Link Speed	Short-Mode STP Cost	Long-Mode STP Cost
10 Mbps	100	2,000,000
100 Mbps	19	200,000
1 Gbps	4	20,000
10 Gbps	2	2,000
20 Gbps	1	1,000
100 Gbps	1	200
1 Tbps	1	20
10 Tbps	1	2

Spanning Tree Protocol Fundamentals

Building the STP Topology

- This section focuses on the logic switches use to build an STP topology.
- The focus is on VLAN 1, but VLANs 10, 20, and 99 also exist.
- SW1 has been identified as the root bridge, and the RP, DP, and blocking ports have been identified.

.

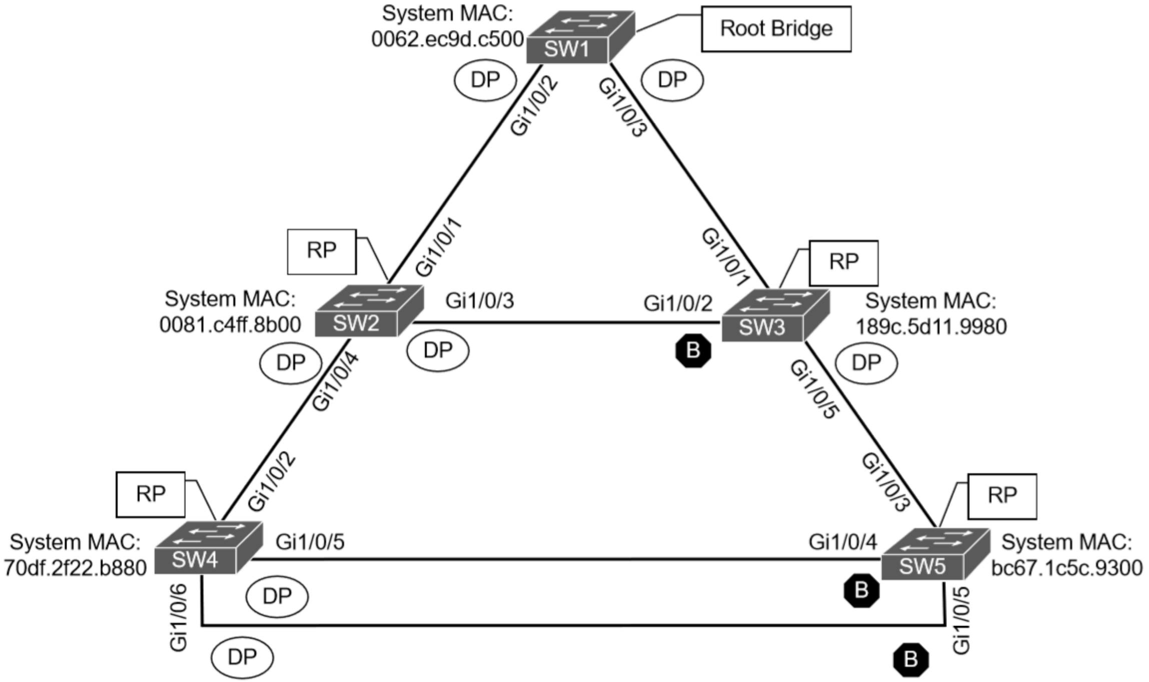


Figure 2-1 *Basic STP Topology*

Spanning Tree Protocol Fundamentals

Root Bridge Election

The first step with STP is to identify the root bridge.

As a switch initializes, it assumes that it is the root bridge and uses the local bridge identifier as the root bridge identifier.

It then listens to its neighbor’s configuration BPDU and does the following:

- If the neighbor’s configuration BPDU is inferior to its own BPDU, the switch ignores that BPDU.
- If the neighbor’s configuration BPDU is preferred to its own BPDU, the switch updates its BPDUs to include the new root bridge identifier along with a new root path cost that correlates to the total path cost to reach the new root bridge.
- This process continues until all switches in a topology have identified the root bridge switch.
- STP prefers lower priority number then goes to lower MAC address.

.

STP Root Path Costs

- The advertised root path cost is always the value calculated on the local switch.
- The local root path cost is the advertised root path cost plus the local interface port cost.
- The root path cost is always zero on the root bridge.
- Figure 2-2 illustrates the root path cost as SW1 advertises the configuration BPDUs toward SW3 and then SW3's configuration BPDUs toward SW5.

.

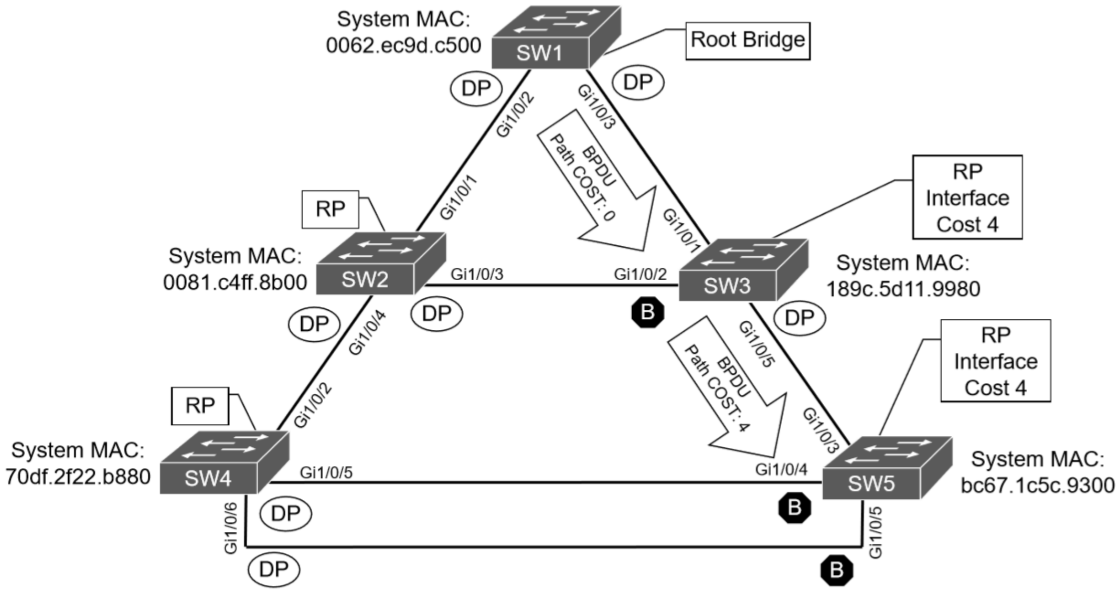


Figure 2-2 *STP Path Cost Advertisements*

Locating Root Ports

Once the Root Bridge is found, the switch must determine its Root Port.

The RP is selected using the following logic:

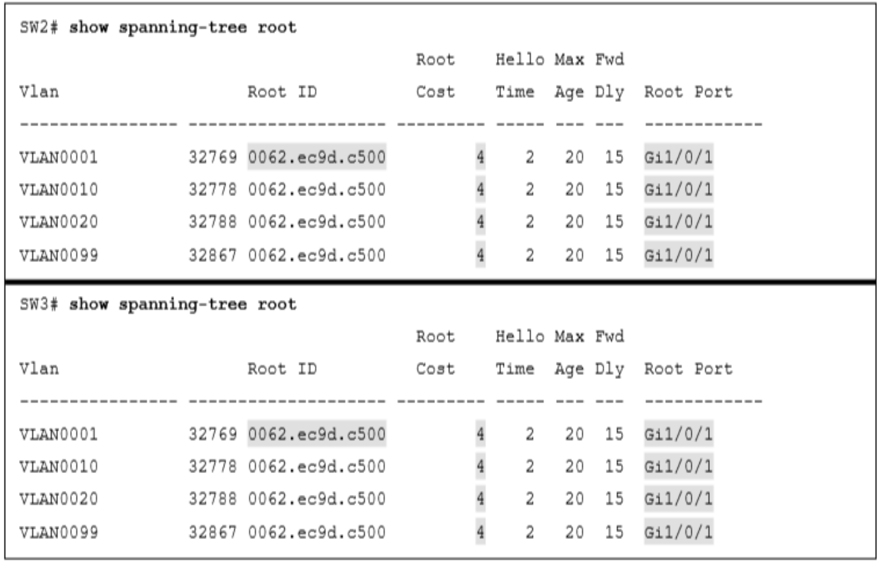
1. The interface associated to lowest path cost is more preferred.
2. The interface associated to the lowest system priority of the advertising switch is preferred next.
3. The interface associated to the lowest system MAC address of the advertising switch is preferred next.
4. When multiple links are associated to the same switch, the lowest port priority from the advertising switch is preferred.
5. When multiple links are associated to the same switch, the lower port number from the advertising switch is preferred.

Spanning Tree Protocol Fundamentals

Locating Root Ports Verified

Use the **show spanning-tree root** command to verify the Root ID and the Root Port.

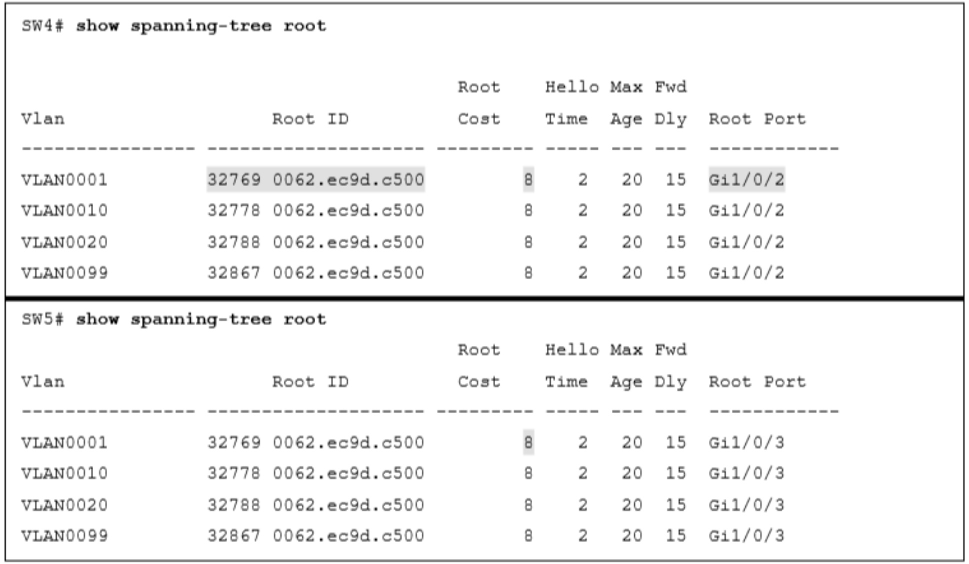
Example 2-2 *Identifying the Root Ports*



```
SW2# show spanning-tree root
                                         Root    Hello Max Fwd
Vlan                     Root ID         Cost    Time  Age Dly  Root Port
---------------- -------------------- --------- ----- --- ---  ------------
VLAN0001         32769 0062.ec9d.c500         4    2   20  15  Gi1/0/1
VLAN0010         32778 0062.ec9d.c500         4    2   20  15  Gi1/0/1
VLAN0020         32788 0062.ec9d.c500         4    2   20  15  Gi1/0/1
VLAN0099         32867 0062.ec9d.c500         4    2   20  15  Gi1/0/1
```

```
SW3# show spanning-tree root
                                         Root    Hello Max Fwd
Vlan                     Root ID         Cost    Time  Age Dly  Root Port
---------------- -------------------- --------- ----- --- ---  ------------
VLAN0001         32769 0062.ec9d.c500         4    2   20  15  Gi1/0/1
VLAN0010         32778 0062.ec9d.c500         4    2   20  15  Gi1/0/1
VLAN0020         32788 0062.ec9d.c500         4    2   20  15  Gi1/0/1
VLAN0099         32867 0062.ec9d.c500         4    2   20  15  Gi1/0/1
```

Example 2-3 *Identifying the Root Ports on SW4 and SW5*



```
SW4# show spanning-tree root

                                         Root    Hello Max Fwd
Vlan                     Root ID         Cost    Time  Age Dly  Root Port
---------------- -------------------- --------- ----- --- ---  ------------
VLAN0001         32769 0062.ec9d.c500         8    2   20  15  Gi1/0/2
VLAN0010         32778 0062.ec9d.c500         8    2   20  15  Gi1/0/2
VLAN0020         32788 0062.ec9d.c500         8    2   20  15  Gi1/0/2
VLAN0099         32867 0062.ec9d.c500         8    2   20  15  Gi1/0/2
```

```
SW5# show spanning-tree root
                                         Root    Hello Max Fwd
Vlan                     Root ID         Cost    Time  Age Dly  Root Port
---------------- -------------------- --------- ----- --- ---  ------------
VLAN0001         32769 0062.ec9d.c500         8    2   20  15  Gi1/0/3
VLAN0010         32778 0062.ec9d.c500         8    2   20  15  Gi1/0/3
VLAN0020         32788 0062.ec9d.c500         8    2   20  15  Gi1/0/3
VLAN0099         32867 0062.ec9d.c500         8    2   20  15  Gi1/0/3
```

Locating Blocked Designated Switch Ports

The RPs have been identified and all other ports are considered designated ports. If two non-root switches are connected to each other on their designated ports, one port must be set to a blocking state to prevent a forwarding loop. Calculate which ports should be blocked between two non-root switches:

1. The interface is a designated port and must not be considered an RP.
2. The switch with the lower path cost to the root bridge forwards, and the one with the higher path cost blocks. If they tie, they move on to the next step.
3. The system priority of the local switch is compared to the system priority of the remote switch. The local port is moved to a blocking state if the remote system priority is lower than that of the local switch. If they tie, they move on to the next step.
4. The system MAC address of the local switch is compared to the system priority of the remote switch. The local designated port is moved to a blocking state if the remote system MAC address is lower than that of the local switch. If the links are connected to the same switch, they move on to the next step.

Spanning Tree Protocol Fundamentals

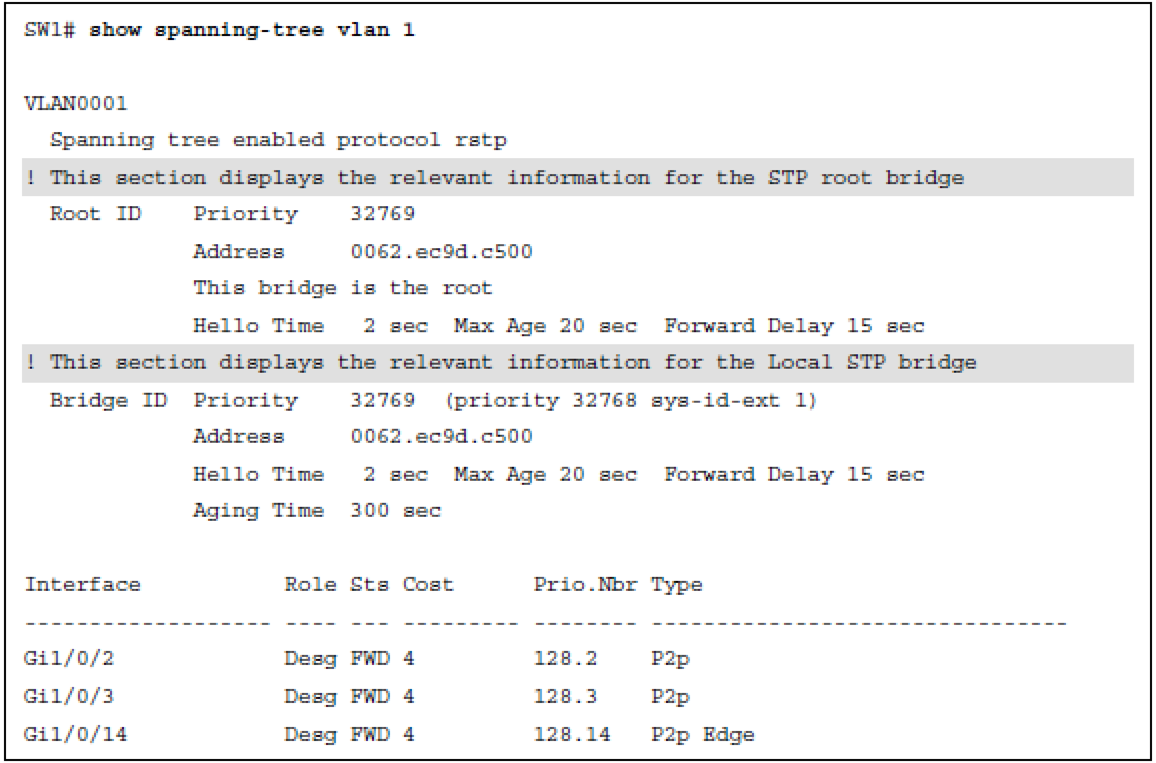
Viewing STP Information

These port types are expected on Catalyst switches:

Point-to-point (P2P) - This port type connects with another network device (PC or RSTP switch).

P2P edge -This port type specifies that portfast is enabled on this port.

Example 2-4 *Viewing SW1's STP Information*



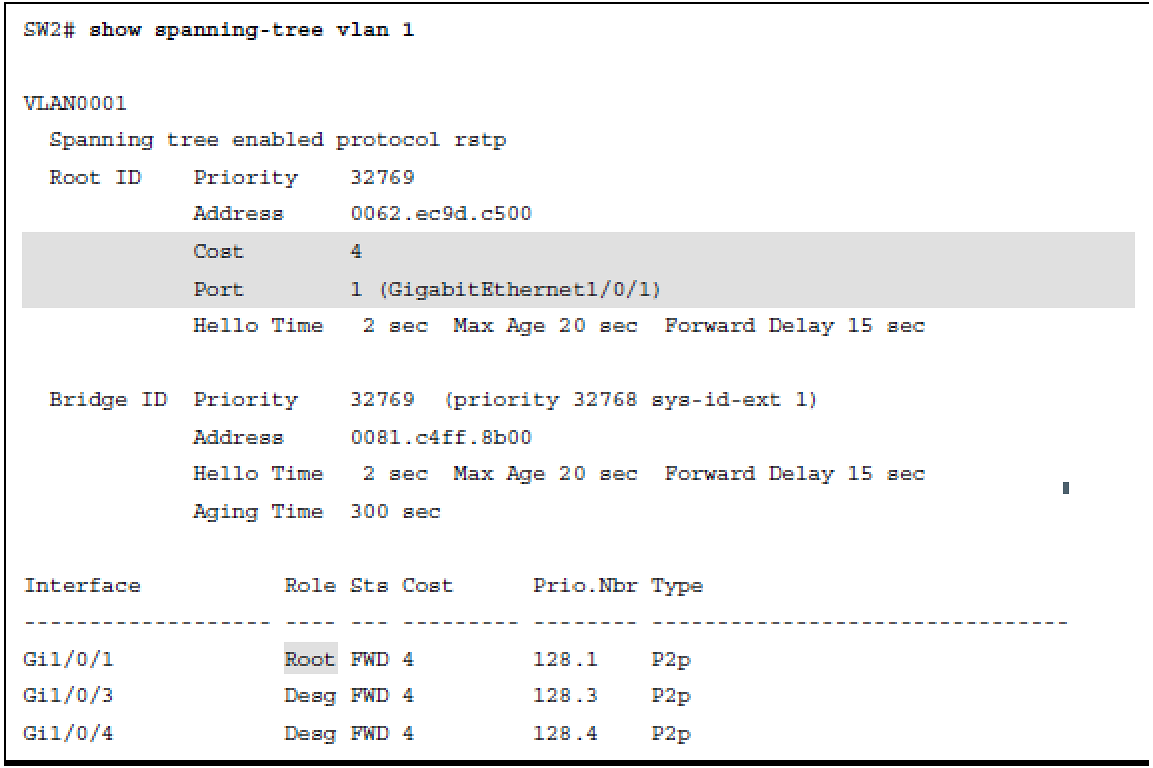
```
SW1# show spanning-tree vlan 1

VLAN0001
  Spanning tree enabled protocol rstp
! This section displays the relevant information for the STP root bridge
  Root ID    Priority    32769
             Address     0062.ec9d.c500
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
! This section displays the relevant information for the Local STP bridge
  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0062.ec9d.c500
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi1/0/2             Desg FWD 4         128.2    P2p
Gi1/0/3             Desg FWD 4         128.3    P2p
Gi1/0/14            Desg FWD 4         128.14   P2p Edge
```

Spanning Tree Protocol Fundamentals

Viewing STP Information

Verify Cost and Root Ports with the **show spanning-tree vlan 1** command.

Example 2-5 *Verifying the Root and Blocking Ports for a VLAN*

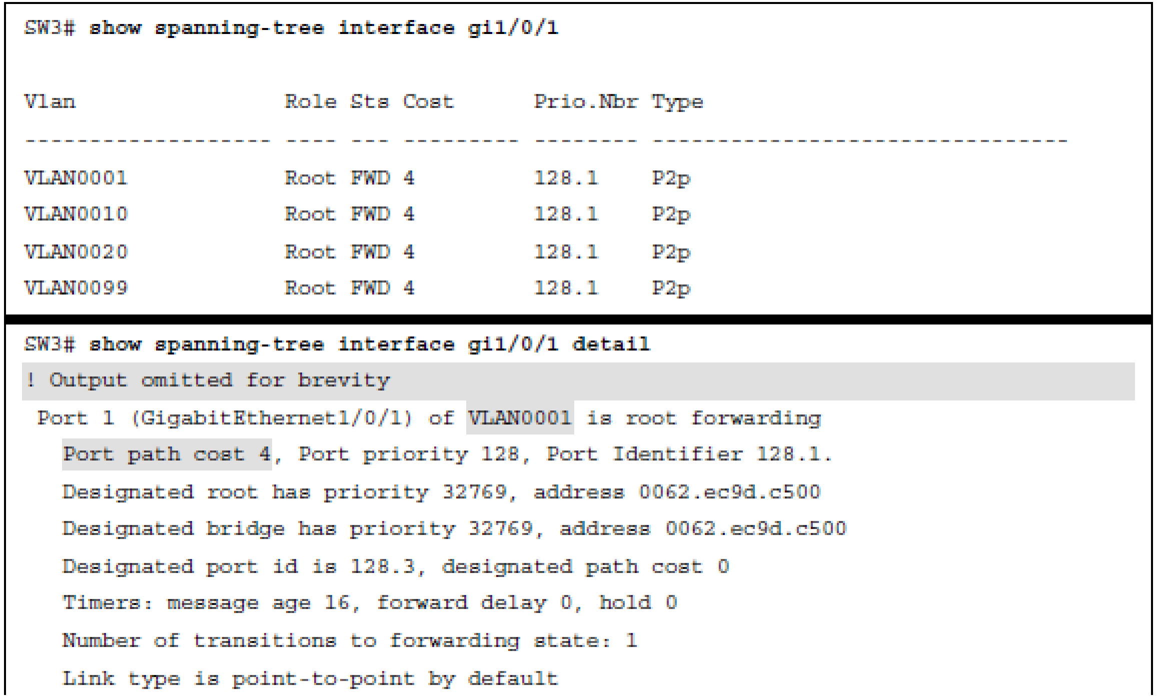


```
SW2# show spanning-tree vlan 1

VLAN0001
  Spanning tree enabled protocol rstp
  Root ID     Priority     32769
              Address      0062.ec9d.c500
              Cost         4
              Port         1 (GigabitEthernet1/0/1)
              Hello Time    2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority     32769  (priority 32768 sys-id-ext 1)
              Address      0081.c4ff.8b00
              Hello Time    2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time   300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi1/0/1             Root FWD 4         128.1    P2p
Gi1/0/3             Desg FWD 4         128.3    P2p
Gi1/0/4             Desg FWD 4         128.4    P2p
```

Spanning Tree Protocol Fundamentals

Verify VLAN Information on a Trunk

If a VLAN is missing on a trunk port, check the trunk port configuration for accuracy.



```
SW3# show spanning-tree interface gi1/0/1


Vlan                Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
VLAN0001            Root FWD 4         128.1    P2p
VLAN0010            Root FWD 4         128.1    P2p
VLAN0020            Root FWD 4         128.1    P2p
VLAN0099            Root FWD 4         128.1    P2p
```

```
SW3# show spanning-tree interface gi1/0/1 detail
! Output omitted for brevity
 Port 1 (GigabitEthernet1/0/1) of VLAN0001 is root forwarding
   Port path cost 4, Port priority 128, Port Identifier 128.1.
   Designated root has priority 32769, address 0062.ec9d.c500
   Designated bridge has priority 32769, address 0062.ec9d.c500
   Designated port id is 128.3, designated path cost 0
   Timers: message age 16, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   Link type is point-to-point by default
```

STP Topology Changes

BPDUs always flow from the root bridge toward the edge switches, unless there are changes in the topology.

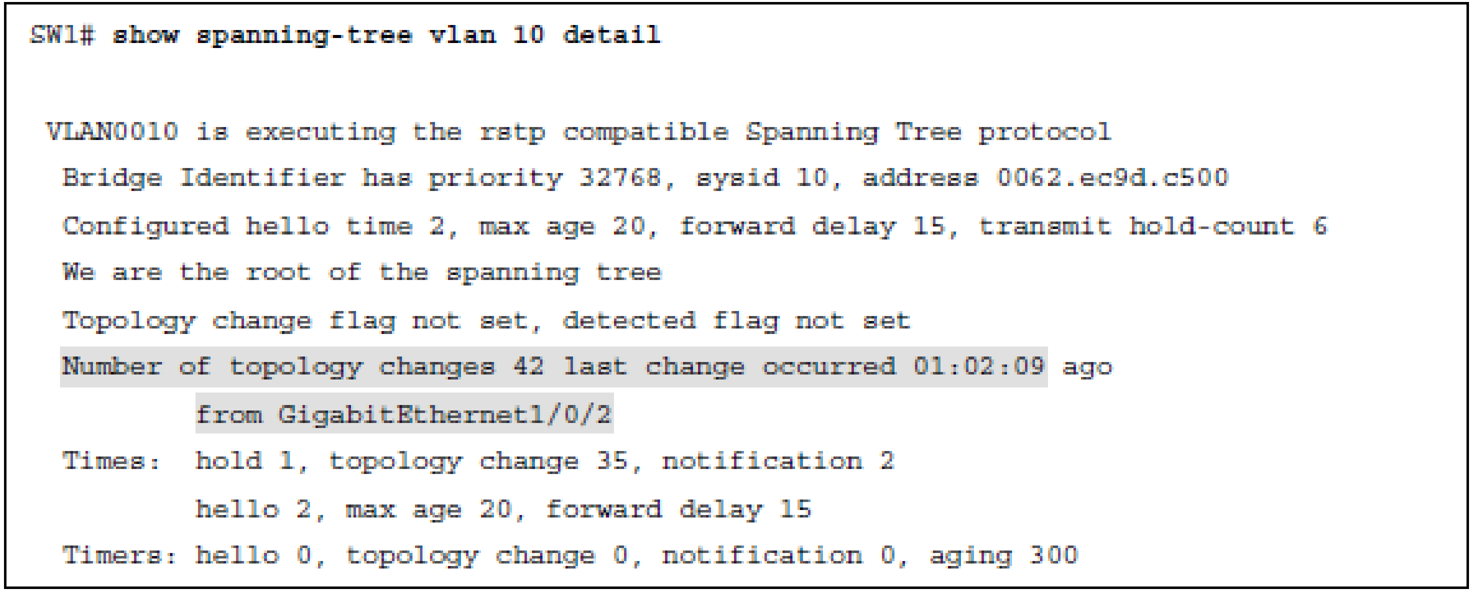
- The switch that detects a link status change sends a topology change notification (TCN) BPDU toward the root bridge out of its RP.
- If an upstream switch receives the TCN, it sends out an acknowledgment and forwards the TCN out its RP to the root bridge.
- Upon receipt of the TCN, the root bridge creates a new configuration BPDU with the Topology Change flag set, and it is then flooded to all the switches.
- When switches receive this, they set their MAC address timer to a default 15 seconds. Then the device flushes its MAC table if has not heard from a device in that last 15 seconds.
- TCNs are generated on a VLAN basis, so the impact of TCNs directly correlates to the number of hosts in a VLAN.

Spanning Tree Protocol Fundamentals

Verify STP Topology Changes

Use the **show spanning-tree vlan # detail** command to see topology changes.

Example 2-7 *Viewing a Detailed Version of Spanning Tree State*



```
SW1# show spanning-tree vlan 10 detail


 VLAN0010 is executing the rstp compatible Spanning Tree protocol
  Bridge Identifier has priority 32768, sysid 10, address 0062.ec9d.c500
  Configured hello time 2, max age 20, forward delay 15, transmit hold-count 6
  We are the root of the spanning tree
  Topology change flag not set, detected flag not set
  Number of topology changes 42 last change occurred 01:02:09 ago
          from GigabitEthernet1/0/2
  Times:  hold 1, topology change 35, notification 2
          hello 2, max age 20, forward delay 15
  Timers: hello 0, topology change 0, notification 0, aging 300
```

Rapid Spanning Tree Protocol

- IEEE 802.1D has only one topology tree and a slower convergence which can be problematic.
- Rapid Spanning Tree Protocol (RSTP) IEEE 802.1W reduces the number of port states to be faster and more efficient.

Rapid Spanning Tree Port States

IEEE 802.1D has only one topology tree which can be problematic. Larger environments with multiple VLANs need different STP topologies for traffic engineering purposes.

- Cisco created the proprietary Per-VLAN Spanning Tree (PVST) and Per-VLAN Spanning Tree Plus (PVST+)
- Rapid Spanning Tree Protocol (RSTP) IEEE 802.1W reduces the number of port states to three:

Port States	**Description**
Discarding	The switch port is enabled, but the port is not forwarding any traffic to ensure that a loop is not created.
Learning	The switch port modifies the MAC address table. The switch still does not forward any other network traffic besides BPDUs.
Forwarding	The switch port forwards all network traffic and updates the MAC address table as expected.

Rapid Spanning Tree Port Roles

RSTP defines the following port roles:

Port Roles	**Description**
Root port (RP):	A network port that connects to the root bridge or an upstream switch in the spanning-tree topology. There should be only one root port per VLAN.
Designated port (DP):	A network port that receives and forwards BPDU frames to other switches. Designated ports provide connectivity to downstream devices and switches. There should be only one active designated port on a link.
Alternate port:	A network port that provides alternate connectivity toward the root switch through a different switch.
Backup port:	A network port that provides link redundancy toward the current root switch. A backup port exists only when multiple links connect between the same switches.

Rapid Spanning Tree Port Types

RSTP defines three types of ports that are used for building the STP topology:

Port Roles	**Description**
Edge Port	A port at the edge of the network where hosts connect to the Layer 2 topology with one interface and cannot form a loop. These ports directly correlate to ports that have the STP portfast feature enabled.
Root port	A port that has the best path cost toward the root bridge. There can be only one root port on a switch.
Point-to-Point port	Any port that connects to another RSTP switch with full duplex. Full-duplex links do not permit more than two devices on a network segment, so determining whether a link is full duplex is the fastest way to check the feasibility of being connected to a switch.

Multi-access connections (Hubs) must use 802.1D.

Prepare for the Exam

Prepare for the Exam

Key Topics for Chapter 2

Description
802.1D port types
STP key terminology
Root bridge election
Locating root ports
STP topology changes
RSTP
RSTP (802.1W) port states
Building the RSTP topology

Prepare for the Exam

Key Terms for Chapter 2

Term	
bridge protocol data unit (BPDU)	root bridge
configuration BPDU	root bridge identifier
hello time	root path
designated port (DP)	cost
forward delay	root port
local bridge identifier	system priority
Max Age	system ID extension
topology change notification (TCN)	

Prepare for the Exam

Command Reference for Chapter 2

Task	Command Syntax
Set the STP max age	**spanning-tree vlan** *vlan-id* **max-age**
Set the STP hello interval	**spanning-tree vlan** *vlan-id* **hello-time** *hello-time*
Set the STP forwarding delay	**spanning-tree vlan** *vlan-id* **forward-time** *forward-time*
Display the STP root bridge and cost	**show spanning-tree root**
Display the STP information (root bridge, local bridge, and interfaces) for one or more VLANs	**show spanning-tree** [**vlan** *vlan-id*]
Identify when the last TCN occurred and which port was the reason for it.	**show spanning-tree** [**vlan** *vlan-id*] **detail**

Thank you! Questions?

Vladimír Veselý

updated: 2023-09-20

https://www.fit.vutbr.cz/research/groups/nes@fit

Chapter 3: Advanced STP Tuning

Instructor Materials

CCNP Enterprise: Core Networking

STP Topology Tuning

- In a properly designed network a switch is deliberately selected to become the root bridge and the designated and alternate ports are modified.
- Network design considerations factor in hardware platform, resiliency, and network topology.

STP Topology Tuning

Root Bridge Placement

- To ensure root bridge placement set the system priority on:
- The root bridge to the lowest value
- The secondary root bridge to a value slightly higher than that of the root bridge
- All other switches to a value higher than the secondary root bridge

Command	Description
spanning-tree vlan *vlan-id* **priority** *priority*	The priority is a value between 0 and 61,440, in increments of 4,096.
spanning-tree vlan *vlan-id* **root {primary | secondary} [diameter** *diameter***]**	The **primary** keyword sets the priority to 24,576, and the **secondary** keyword sets the priority to 28,672. The optional **diameter** command makes it possible to tune the Spanning Tree Protocol (STP) convergence and modifies the timers.

STP Topology Tuning

Configuring the Root Bridge

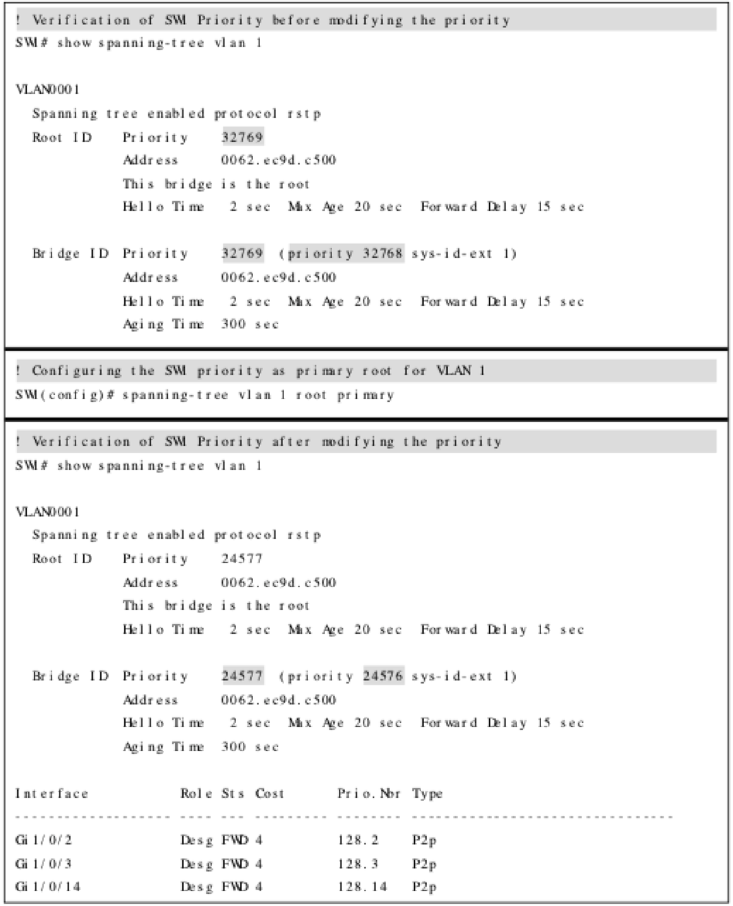
- In the example:

- The initial priority for VLAN 1 on SW1 is verified, 32,769.

- SW1 is configured to be the primary root for VLAN 1

- The priority is verified again to ensure the change took place.

Example 3-1 *Changing the STP System Priority on SW1*



```
! Verification of SW1 Priority before modifying the priority
SW1# show spanning-tree vlan 1

VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    32769
             Address     0062.ec9d.c500
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0062.ec9d.c500
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec
```

```
! Configuring the SW1 priority as primary root for VLAN 1
SW1(config)# spanning-tree vlan 1 root primary
```

```
! Verification of SW1 Priority after modifying the priority
SW1# show spanning-tree vlan 1

VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    24577
             Address     0062.ec9d.c500
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    24577  (priority 24576 sys-id-ext 1)
             Address     0062.ec9d.c500
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi1/0/2             Desg FWD 4         128.2    P2p
Gi1/0/3             Desg FWD 4         128.3    P2p
Gi1/0/14            Desg FWD 4         128.14   P2p
```

STP Topology Tuning

Configuring the Backup Root Bridge

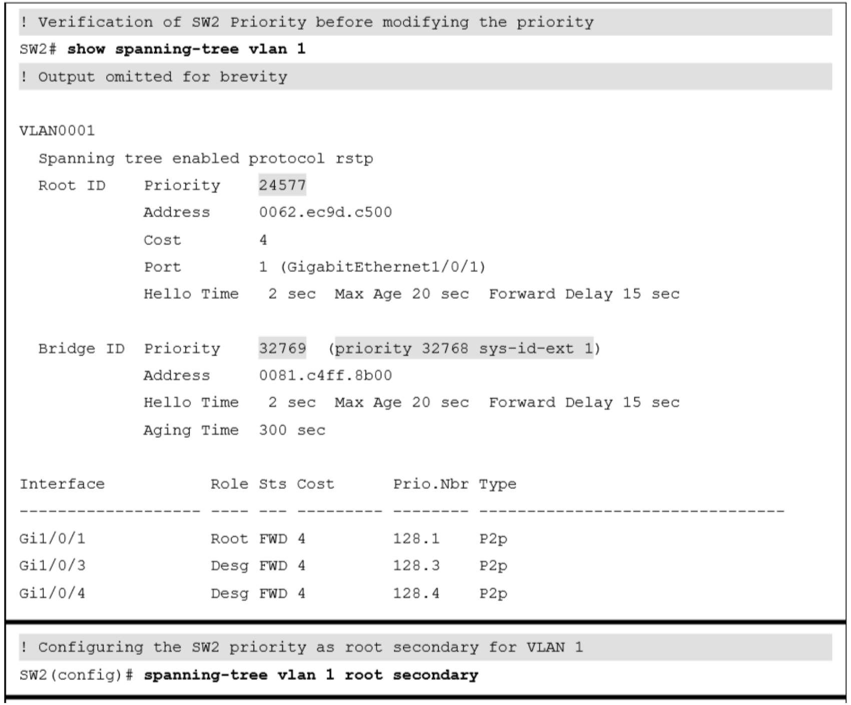
- In the example:

- The initial priority for VLAN 1 on SW2 is verified, 32,769.

- SW2 is configured to be the secondary root for VLAN 1

- The priority is verified again to ensure the change took place.

Example 3-2 *Changing the STP System Priority on SW2*



```
! Verification of SW2 Priority before modifying the priority
SW2# show spanning-tree vlan 1
! Output omitted for brevity

VLAN0001
  Spanning tree enabled protocol rstp
  Root ID     Priority     24577
              Address      0062.ec9d.c500
              Cost         4
              Port         1 (GigabitEthernet1/0/1)
              Hello Time    2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority     32769   (priority 32768 sys-id-ext 1)
              Address      0081.c4ff.8b00
              Hello Time    2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time   300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi1/0/1             Root FWD 4         128.1    P2p
Gi1/0/3             Desg FWD 4         128.3    P2p
Gi1/0/4             Desg FWD 4         128.4    P2p

! Configuring the SW2 priority as root secondary for VLAN 1
SW2(config)# spanning-tree vlan 1 root secondary
```

STP Topology Tuning

Modifying STP Root Port & Blocked Switch Port Locations

- Calculating total path cost to the root bridge:

- SW1 sends a BPDU to SW3 with the path cost of 0.
- SW3 receives the BPDU and adds its root port cost (4) to cost from the BPDU (0), resulting in the cost of 4.
- SW3 sends a BPDU to SW5 with the path cost of 4.
- SW5 receives the BPDU and adds its root port cost (4) to the cost from the BPDU (4), resulting in the cost of 8 for SW5 to reach the root bridge.

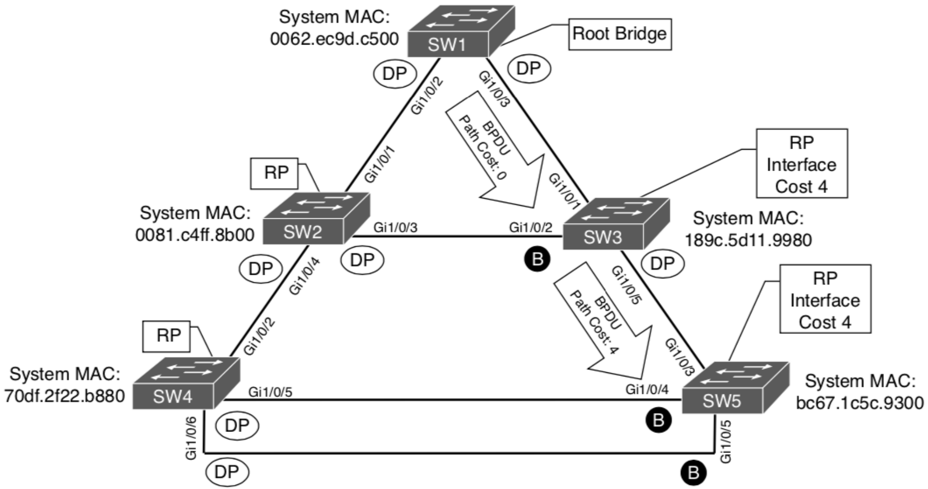


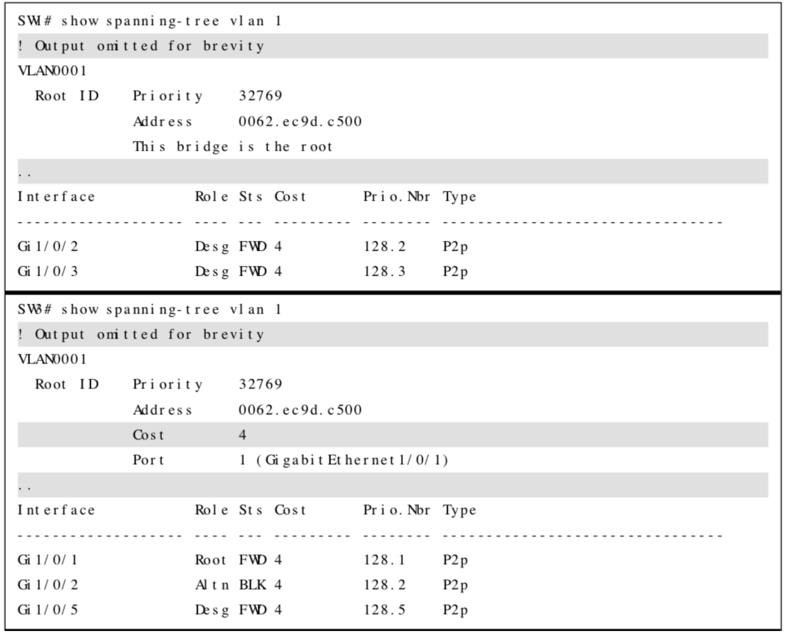
Figure 3-2 *STP Path Cost Calculation*

STP Topology Tuning

Verifying the Total Path Cost

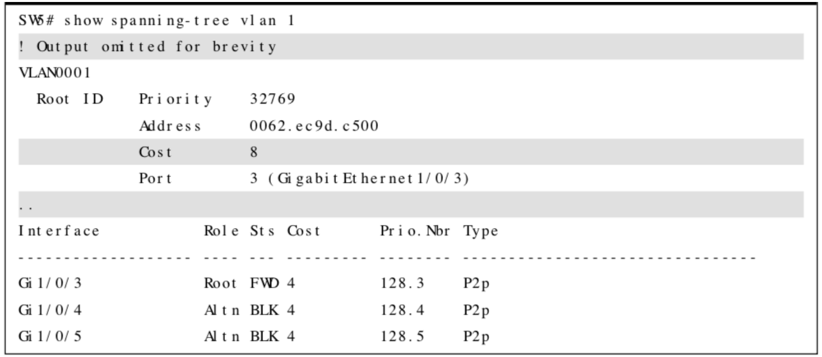
The example highlights the total path cost to the root bridge from SW3 and SW5.

Example 3-3 *Verifying the Total Path Cost*



```
SW1# show spanning-tree vlan 1
! Output omitted for brevity
VLAN0001
  Root ID    Priority    32769
             Address     0062.ec9d.c500
             This bridge is the root
..
Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi1/0/2             Desg FWD 4         128.2    P2p
Gi1/0/3             Desg FWD 4         128.3    P2p
```

```
SW3# show spanning-tree vlan 1
! Output omitted for brevity
VLAN0001
  Root ID    Priority    32769
             Address     0062.ec9d.c500
             Cost        4
             Port        1 (GigabitEthernet1/0/1)
..
Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi1/0/1             Root FWD 4         128.1    P2p
Gi1/0/2             Altn BLK 4         128.2    P2p
Gi1/0/5             Desg FWD 4         128.5    P2p
```



```
SW5# show spanning-tree vlan 1
! Output omitted for brevity
VLAN0001
  Root ID    Priority    32769
             Address     0062.ec9d.c500
             Cost        8
             Port        3 (GigabitEthernet1/0/3)
..
Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi1/0/3             Root FWD 4         128.3    P2p
Gi1/0/4             Altn BLK 4         128.4    P2p
Gi1/0/5             Altn BLK 4         128.5    P2p
```

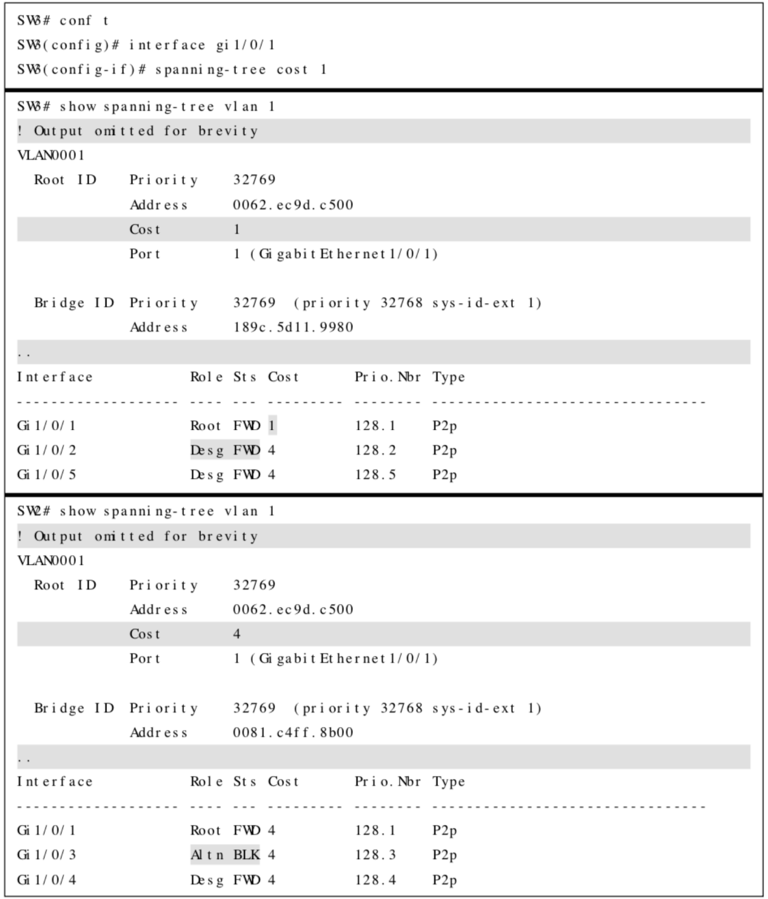
Note: There is not a total path cost in SW1’s output

STP Topology Tuning

Modifying STP Port Cost

- The **spanning tree [vlan** *vlan-id]* **cost** *cost* command can be used to modify the STP forwarding path.
- Using the spanning tree command will modify the cost for all VLANs unless the optional **vlan** keyword is used.

Example 3-4 *Modifying STP Port Cost*



```
SW3# conf t
SW3(config)# interface gi1/0/1
SW3(config-if)# spanning-tree cost 1
```

```
SW3# show spanning-tree vlan 1
! Output omitted for brevity
VLAN0001
  Root ID    Priority    32769
             Address     0062.ec9d.c500
             Cost        1
             Port        1 (GigabitEthernet1/0/1)

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     189c.5d11.9980
..
Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi1/0/1             Root FWD 1         128.1    P2p
Gi1/0/2             Desg FWD 4         128.2    P2p
Gi1/0/5             Desg FWD 4         128.5    P2p
```

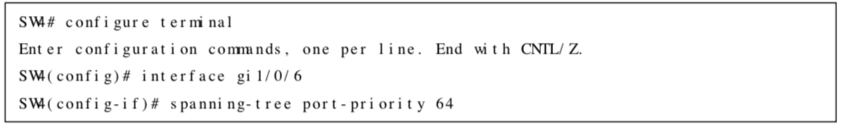
```
SW2# show spanning-tree vlan 1
! Output omitted for brevity
VLAN0001
  Root ID    Priority    32769
             Address     0062.ec9d.c500
             Cost        4
             Port        1 (GigabitEthernet1/0/1)

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0081.c4ff.8b00
..
Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi1/0/1             Root FWD 4         128.1    P2p
Gi1/0/3             Altn BLK 4         128.3    P2p
Gi1/0/4             Desg FWD 4         128.4    P2p
```

STP Topology Tuning

Modifying STP Port Priority

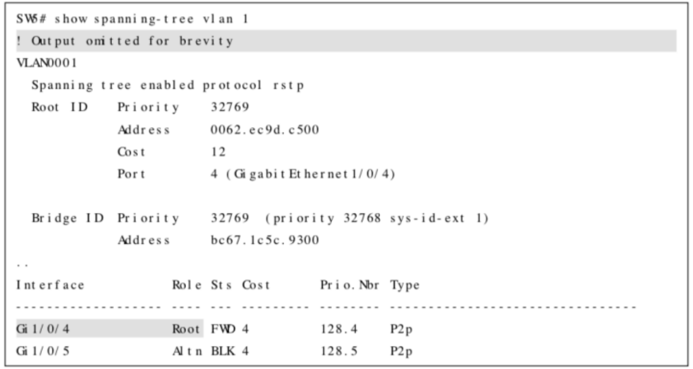
- STP port priority influences which port becomes the alternate port when multiple links are used between switches. Use the command **spanning-tree** [**vlan** *vlan-id*] **port-priority** *priority* to change the STP port priority on a switch’s interface.

Example 3-6 *Verifying Port Priority Impact on an STP Topology*



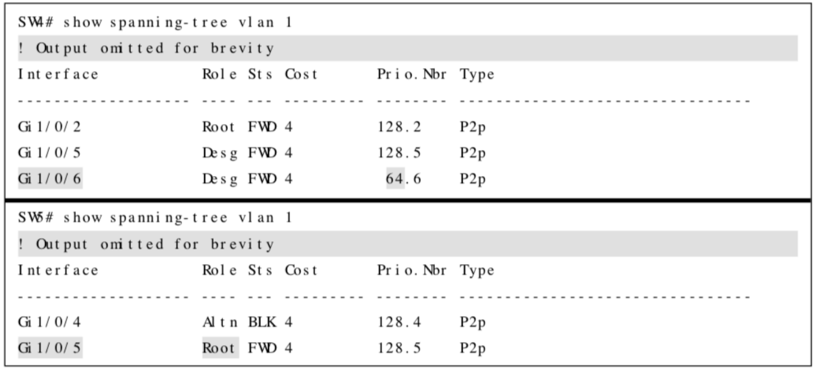
```
SW4# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW4(config)# interface gi1/0/6
SW4(config-if)# spanning-tree port-priority 64
```

Example 3-5 *Viewing STP Port Priority*



```
SW6# show spanning-tree vlan 1
! Output omitted for brevity
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    32769
             Address     0062.ec9d.c500
             Cost        12
             Port        4 (GigabitEthernet1/0/4)

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     bc67.1c5c.9300
..
Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi1/0/4             Root FWD 4         128.4    P2p
Gi1/0/5             Altn BLK 4         128.5    P2p
```

Example 3-7 *Determining the Impact of Port Priority on a Topology*



```
SW4# show spanning-tree vlan 1
! Output omitted for brevity
Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi1/0/2             Root FWD 4         128.2    P2p
Gi1/0/5             Desg FWD 4         128.5    P2p
Gi1/0/6             Desg FWD 4          64.6    P2p
```

```
SW5# show spanning-tree vlan 1
! Output omitted for brevity
Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi1/0/4             Altn BLK 4         128.4    P2p
Gi1/0/5             Root FWD 4         128.5    P2p
```

Additional STP Protection Mechanisms

- A network forwarding loop occurs when there are multiple active paths between two devices. Broadcast and multicast traffic are forwarded out every switch port continuing the forwarding loop.
- The network’s throughput is drastically effected as the switches are processing numerous frames. The switches CPU utilization will be high and memory space will be consumed. The switches might crash and users will likely notice the impact on the network.

Additional STP Protection Mechanisms

Common issues for Layer 2 forwarding loops:

- STP is disabled on a switch.
- A load balancer is misconfigured and sends traffic out multiple ports with the same MAC address.
- A virtual switch that bridges two physical ports.
- End users using an unmanaged switch or hub.

Additional STP Protection Mechanisms

Root Guard

- Root guard is an STP feature that prevents a configured port from becoming a root port.
  - It does this by placing the port in an ErrDisabled state if a superior BDPU is received on that port.
  - Root guard is placed on designated ports towards other switches that should never become root bridges.
  - Root guard is enabled on a port-by-port basis.
- Use the interface command **spanning-tree guard root** to enable root guard.

Additional STP Protection Mechanisms

STP Portfast

- STP portfast disables the topology notification notification (TCN) generation and causes access ports that come up to bypass the learning and listening states and enter the forwarding state immediately. If a BPDU is received on a portfast-enabled port, the portfast functionality is removed from that port.

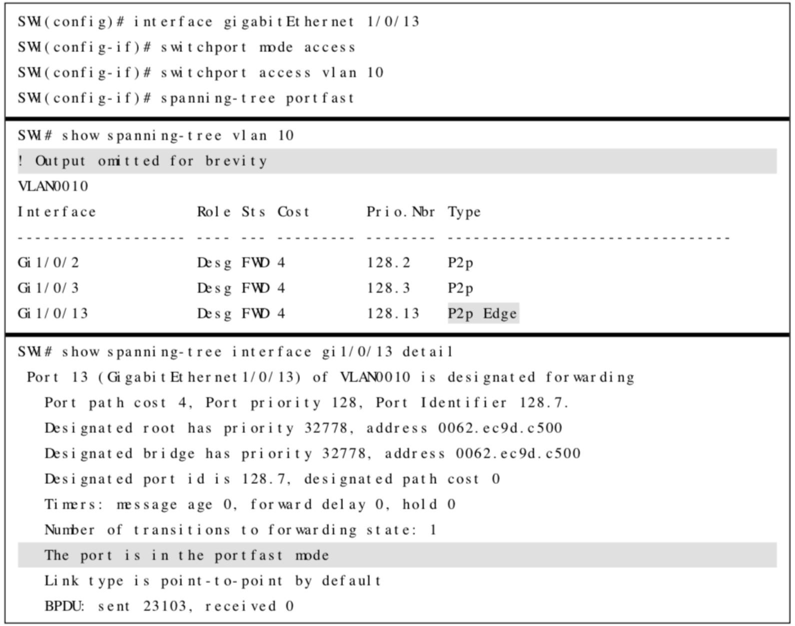
Command	Description
spanning-tree portfast	Interface command to enable portfast on a specific access port
spanning-tree portfast default	Global command to enable portfast on all access ports
spanning-tree portfast disable	Disable portfast on a port
spanning-tree portfast trunk	Command used on trunk links to enable portfast *This command should only be used with ports connected to a single host.

Additional STP Protection Mechanisms

STP Portfast Examples

- The following shows how to enable STP portfast globally and on a specific interface.

Example 3-9 *Enabling STP Portfast on Specific Interfaces*

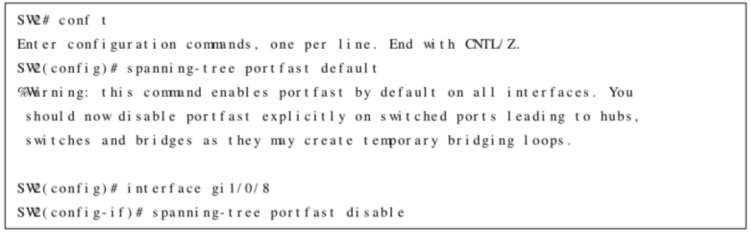


```
SW1(config)# interface gigabitEthernet 1/0/13
SW1(config-if)# switchport mode access
SW1(config-if)# switchport access vlan 10
SW1(config-if)# spanning-tree portfast
```

```
SW1# show spanning-tree vlan 10
! Output omitted for brevity
VLAN0010
Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi1/0/2             Desg FWD 4         128.2    P2p
Gi1/0/3             Desg FWD 4         128.3    P2p
Gi1/0/13            Desg FWD 4         128.13   P2p Edge
```

```
SW1# show spanning-tree interface gi1/0/13 detail
 Port 13 (GigabitEthernet1/0/13) of VLAN0010 is designated forwarding
   Port path cost 4, Port priority 128, Port Identifier 128.7.
   Designated root has priority 32778, address 0062.ec9d.c500
   Designated bridge has priority 32778, address 0062.ec9d.c500
   Designated port id is 128.7, designated path cost 0
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   The port is in the portfast mode
   Link type is point-to-point by default
   BPDU: sent 23103, received 0
```

Example 3-10 *Enabling STP Portfast Globally*



```
SW2# conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW2(config)# spanning-tree portfast default
%Warning: this command enables portfast by default on all interfaces. You
 should now disable portfast explicitly on switched ports leading to hubs,
 switches and bridges as they may create temporary bridging loops.

SW2(config)# interface gi1/0/8
SW2(config-if)# spanning-tree portfast disable
```

Prepare for the Exam

Prepare for the Exam

Key Topics for Chapter 3

Description
Root bridge placement
Root bridge values
Spanning tree port cost
Root guard
STP portfast
BPDU guard
BPDU filter

Prepare for the Exam

Key Terms for Chapter 3

Terms
BPDU filter
Root guard
STP loop guard
BPDU guard
STP portfast
Unidirectional Link Detection (UDLD)

Prepare for the Exam

Command Reference for Chapter 3

Task	Command Syntax
Configure the STP priority for a switch so that it is a root bridge or a backup root bridge	**spanning-tree vlan** vlan-id **root** {**primary** | **secondary**} [**diameter** diameter] OR **spanning-tree vlan** vlan-id **priority** priority
Configure the STP port cost	**spanning tree** [**vlan** vlan-id] **cost** cost
Configure the STP port priority on the downstream port	**spanning-tree** [**vlan** vlan-id] **port-priority** priority
Enable root guard on an interface	**spanning-tree guard root**
Enable STP portfast globally, for a specific port, or for a trunk port	**spanning-tree portfast default** OR **spanning-tree portfast** OR **spanning-tree portfast trunk**
Enable BPDU guard globally or for a specific switch port	**spanning-tree portfast bpduguard default** OR **spanning-tree bpduguard** {**enable** | **disable**}

Prepare for the Exam

Command Reference for Chapter 3 (Cont.)

Task	Command Syntax
Enable BPDU guard globally or for a specific interface	**spanning-tree portfast bpdufilter default** OR **spanning-tree bpdufilter enable**
Enable STP loop guard globally or for a specific interface	**spanning-tree loopguard default** OR **spanning-tree guard loop**
Enable automatic error recovery for BPDU guard.	**errdisable recovery cause bpduguard**
Enable BPDU guard globally or for a specific interface	**spanning-tree portfast bpdufilter default** OR **spanning-tree bpdufilter enable**
Enable STP loop guard globally or for a specific interface	**spanning-tree loopguard default** OR **spanning-tree guard loop**
Enable automatic error recovery for BPDU guard.	**errdisable recovery cause bpduguard**

Prepare for the Exam

Command Reference for Chapter 3 (Cont.)

Task	Command Syntax
Change the automatic error recovery time	**errdisable recovery interval** time-seconds
Enable UDLD globally or for a specific port	**udld enable** [**aggressive**] OR **udld port** [**aggressive**]
Display the list of STP ports in an inconsistent state	**show spanning-tree inconsistentports**
Display the list of neighbor devices running UDLD	**show udld neighbors**

Thank you! Questions?

Vladimír Veselý

updated: 2023-09-20

https://www.fit.vutbr.cz/research/groups/nes@fit

Chapter 4: Multiple Spanning Tree Protocol

Instructor Materials

CCNP Enterprise: Core Networking

Prepare for the Exam

Prepare for the Exam

Key Topics for Chapter 4

Description
Multiple Spanning Tree Protocol
MST instance
MST region
Internal Spanning Tree (IST)
MST region boundary

Prepare for the Exam

Key Terms for Chapter 4

Terms
Common Spanning Tree (CST)
Internal spanning tree (IST)
MST instance (MSTI)
MST region
MST region boundary
PVST simulation check

Prepare for the Exam

Command Reference for Chapter 4

Task	Command Syntax
Configure the switch for a basic MST region that includes all VLANS and the version number 1	**spanning-tree mode mst** **spanning-tree mst configuration** **instance** 0 **vlan** *1-4094* **revision 1**
Modify a switch’s MSTI priority or make it the root bridge for the MSTI	**spanning-tree mst** *instance-number* **priority** *priority* OR **spanning-tree mst** *instance-number* **root** {**primary |** **secondary**}[**diameter** *diameter*]
Specify additional VLANs to an MSTI	**spanning-tree mst configuration instance** *instance-number* **vlan** *vlan-id*
Change the MST version number	**spanning-tree mst configuration revision** *version*
Change the port cost for a specific MSTI	**spanning-tree mst** *instance-number* **cost** *cost*
Change the port priority for a specific MSTI	**spanning-tree mst** *instance-number* **port- priority** *priority*
Display the MST configuration	**show spanning-tree mst configuration**
Verify the MST switch status	**show spanning-tree mst** [*instance-number*]
View the STP topology for the MST	**show spanning-tree mst interface** *interface-id*

Thank you! Questions?

Vladimír Veselý

updated: 2023-09-20

https://www.fit.vutbr.cz/research/groups/nes@fit

Chapter 5: VLAN Trunks and EtherChannel Bundles

Instructor Materials

CCNP Enterprise: Core Networking

VLAN Trunking Protocol

- Cisco created the proprietary protocol, VLAN Trunking Protocol (VTP), to reduce the burden of provisioning VLANs on switches.
- Switches that participate in the same VTP domain can have a VLAN created once on a VTP server and propagated to other VTP client switches in the same VTP domain.

VLAN Trunking Protocol

The Roles of VTP

There are four roles in the VTP architecture:

VTP Roll	**Description**
Server	The server switch is responsible for the creation, modification, and deletion of VLANs within the VTP domain.
Client	The client switch receives VTP advertisements and modifies the VLANs on that switch. VLANs cannot be configured locally on a VTP client.
Transparent	VTP transparent switches receive and forward VTP advertisements but do not modify the local VLAN database. VLANs are configured only locally.
Off	A switch does not participate in VTP advertisements and does not forward them out of any ports either. VLANs are configured only locally.

VLAN Trunking Protocol

The Versions of VTP

- There are three versions of VTP:
  - Version 1 is default.
  - Versions 1 and 2 have limited propagation to VLANs numbered 1 to 1005.
  - VTP Version 3 allows for the full range of VLANs 1 to 4094.

- VTP supports having multiple VTP servers in a domain. These servers process updates from other VTP servers just as a client does.

- If a VTP domain is Version 3, the primary VTP server must be set with the executive command **vtp primary.**

VLAN Trunking Protocol

VTP Communication

VTP advertises updates by using a multicast address across the trunk links for advertising updates to all the switches in the VTP domain. The three main types of VTP advertisements:

Communication Types	Description
Summary	This advertisement occurs every 300 seconds or when a VLAN is added, removed, or changed. It includes the VTP version, domain, configuration revision number, and time stamp.
Subset	This advertisement occurs after a VLAN configuration change occurs. It contains all the relevant information for the switches to make changes to the VLANs on them.
Client Requests	This advertisement is a request by a client to receive the more detailed subset advertisement. This occurs when a switch with a lower revision number joins the VTP domain and observes a summary advertisement with a higher revision than it has stored locally.

VLAN Trunking Protocol

VTP Configuration

- The following are the steps for configuring VTP:

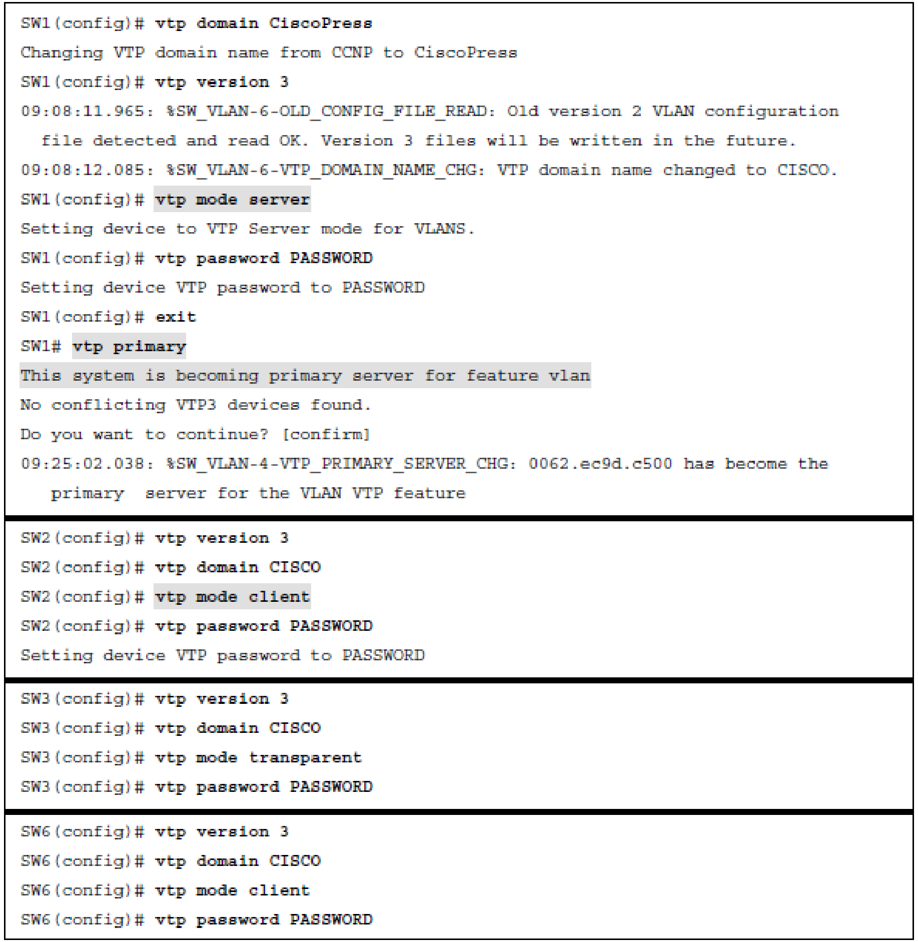
Terms	Description
Step 1	Define the VTP version with the command **vtp version** {**1** | **2** | **3**}.
Step 2	Define the VTP domain with the command **vtp domain** *domain-name*. Changing the VTP domain resets the local switch's version to 0.
Step 3	Define the VTP switch role with the command **vtp mode** { **server** | **client** | **transparent** | **none** }
Step 4	(Optional) Secure the VTP domain with the command **vtp password** *password* (This step is optional but recommended because it helps prevent unauthorized switches from joining the VTP domain.)

VLAN Trunking Protocol

VTP Configuration Example

- Example 5-1 demonstrates the VTP configuration on SW1, SW2, SW3, and SW6.
- The figure shows sample configurations for three of the VTP roles: SW1 as a client, SW3 as transparent, and the other switches as VTP clients.

Example 5-1 *Configuring the VTP Domain*



```
SW1(config)# vtp domain CiscoPress
Changing VTP domain name from CCNP to CiscoPress
SW1(config)# vtp version 3
09:08:11.965: %SW_VLAN-6-OLD_CONFIG_FILE_READ: Old version 2 VLAN configuration
  file detected and read OK. Version 3 files will be written in the future.
09:08:12.085: %SW_VLAN-6-VTP_DOMAIN_NAME_CHG: VTP domain name changed to CISCO.
SW1(config)# vtp mode server
Setting device to VTP Server mode for VLANS.
SW1(config)# vtp password PASSWORD
Setting device VTP password to PASSWORD
SW1(config)# exit
SW1# vtp primary
This system is becoming primary server for feature vlan
No conflicting VTP3 devices found.
Do you want to continue? [confirm]
09:25:02.038: %SW_VLAN-4-VTP_PRIMARY_SERVER_CHG: 0062.ec9d.c500 has become the
   primary  server for the VLAN VTP feature
```

```
SW2(config)# vtp version 3
SW2(config)# vtp domain CISCO
SW2(config)# vtp mode client
SW2(config)# vtp password PASSWORD
Setting device VTP password to PASSWORD
```

```
SW3(config)# vtp version 3
SW3(config)# vtp domain CISCO
SW3(config)# vtp mode transparent
SW3(config)# vtp password PASSWORD
```

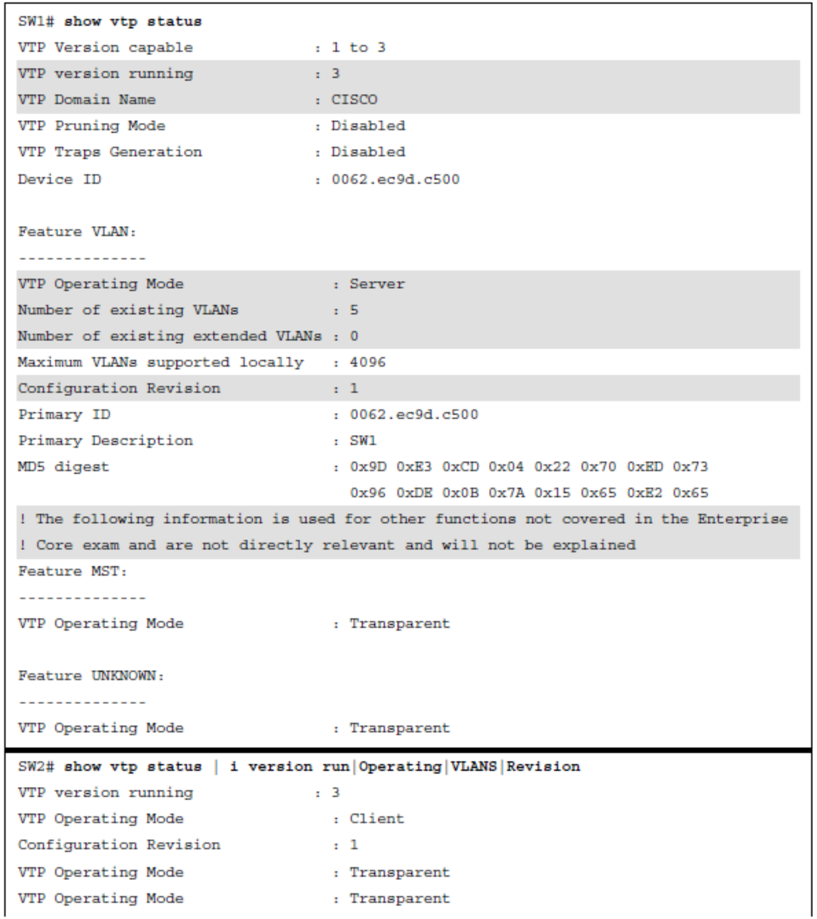
```
SW6(config)# vtp version 3
SW6(config)# vtp domain CISCO
SW6(config)# vtp mode client
SW6(config)# vtp password PASSWORD
```

VLAN Trunking Protocol

VTP Verification

- The VTP status is verified with the command **show vtp status** as shown in the example.
- The most important information displayed is the VTP version, VTP domain name, VTP mode, the number of VLANs (standard and extended), and the configuration version.

Example 5-2 *Verifying VTP*



```
SW1# show vtp status
VTP Version capable              : 1 to 3
VTP version running              : 3
VTP Domain Name                  : CISCO
VTP Pruning Mode                 : Disabled
VTP Traps Generation             : Disabled
Device ID                        : 0062.ec9d.c500

Feature VLAN:
--------------
VTP Operating Mode                 : Server
Number of existing VLANs           : 5
Number of existing extended VLANs  : 0
Maximum VLANs supported locally    : 4096
Configuration Revision             : 1
Primary ID                         : 0062.ec9d.c500
Primary Description                : SW1
MD5 digest                         : 0x9D 0xE3 0xCD 0x04 0x22 0x70 0xED 0x73
                                     0x96 0xDE 0x0B 0x7A 0x15 0x65 0xE2 0x65
! The following information is used for other functions not covered in the Enterprise
! Core exam and are not directly relevant and will not be explained
Feature MST:
--------------
VTP Operating Mode                 : Transparent

Feature UNKNOWN:
--------------
VTP Operating Mode                 : Transparent
```

```
SW2# show vtp status | i version run|Operating|VLANS|Revision
VTP version running              : 3
VTP Operating Mode                 : Client
Configuration Revision             : 1
VTP Operating Mode                 : Transparent
VTP Operating Mode                 : Transparent
```

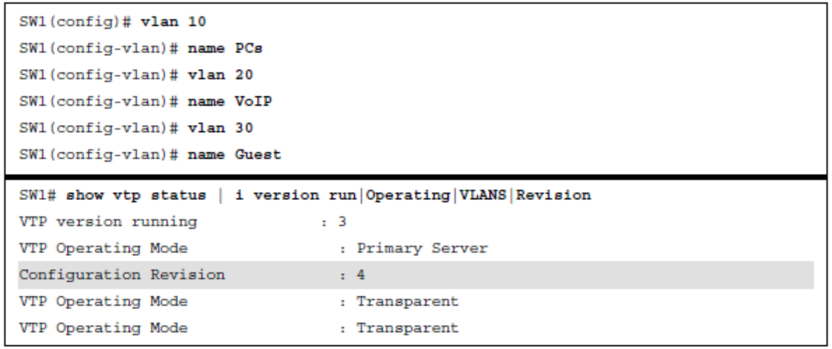
VLAN Trunking Protocol

VTP Verification (Cont.)

- It is very important that every switch that connects to a VTP domain has the VTP revision number reset to 0. Failing to reset the revision number on a switch could result in the switch providing an update to the VTP server.

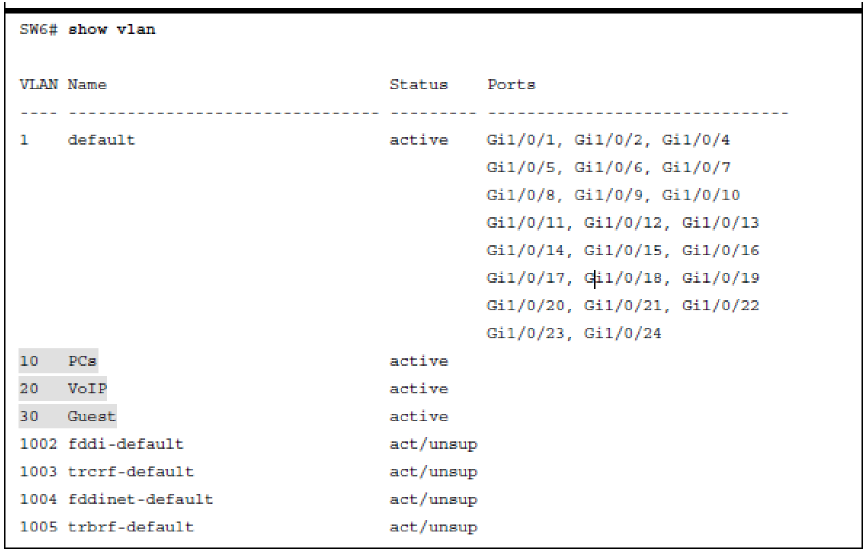
- This is not an issue if VLANs are added but is catastrophic if VLANs are removed because those VLANs will be removed throughout the domain.

Example 5-3 *Creating VLANs on the VTP Domain Server*



```
SW1(config)# vlan 10
SW1(config-vlan)# name PCs
SW1(config-vlan)# vlan 20
SW1(config-vlan)# name VoIP
SW1(config-vlan)# vlan 30
SW1(config-vlan)# name Guest
```

```
SW1# show vtp status | i version run|Operating|VLANS|Revision
VTP version running            : 3
VTP Operating Mode              : Primary Server
Configuration Revision          : 4
VTP Operating Mode              : Transparent
VTP Operating Mode              : Transparent
```



```
SW6# show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi1/0/1, Gi1/0/2, Gi1/0/4
                                                Gi1/0/5, Gi1/0/6, Gi1/0/7
                                                Gi1/0/8, Gi1/0/9, Gi1/0/10
                                                Gi1/0/11, Gi1/0/12, Gi1/0/13
                                                Gi1/0/14, Gi1/0/15, Gi1/0/16
                                                Gi1/0/17, Gi1/0/18, Gi1/0/19
                                                Gi1/0/20, Gi1/0/21, Gi1/0/22
                                                Gi1/0/23, Gi1/0/24
10   PCs                              active
20   VoIP                             active
30   Guest                            active
1002 fddi-default                     act/unsup
1003 trcrf-default                    act/unsup
1004 fddinet-default                  act/unsup
1005 trbrf-default                    act/unsup
```

EtherChannel Bundle

- Ethernet network speeds are based on powers of 10 (10 Mbps, 100 Mbps, 1 Gbps, 10 Gbps,100 Gbps).
- When a link between switches becomes saturated, how can more bandwidth be added to that link to prevent packet loss?

EtherChannel Bundle

Multiple Links

Ideally, it would be nice to plug in a second cable and double the bandwidth between the switches. However, Spanning Tree Protocol (STP) will place one of the ports into a blocking state to prevent forwarding loops, as shown in Figure 5-2.

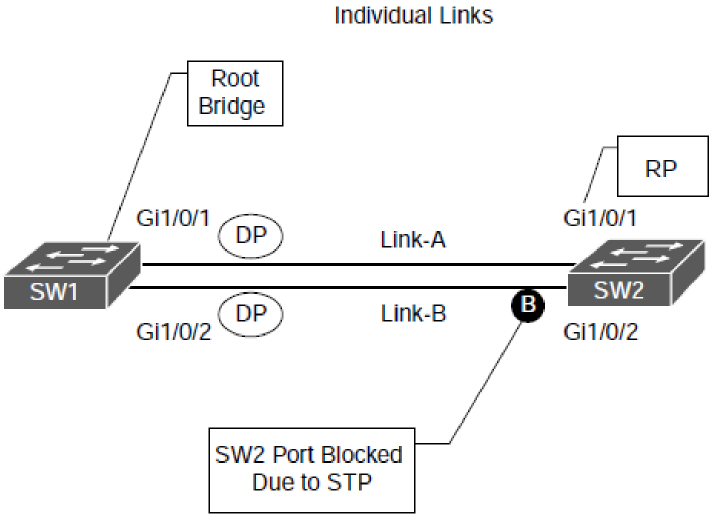


Figure 5-2 *Multiple Links with STP*

EtherChannel Components

Figure 5-3 shows some of the key components of an EtherChannel bundle between SW1 and SW2, with their Gi1/0/1 and Gi1/0/2 interfaces.

The physical links can be aggregated into a logical link called an EtherChannel bundle.

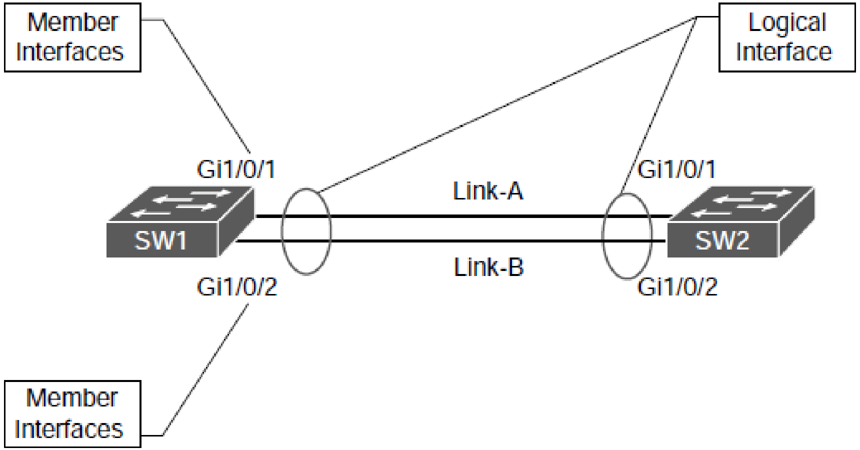


Figure 5-3 *EtherChannel Components*

EtherChannel Components (Cont.)

Aspects of EtherChannel:

- Etherchannel is defined in the IEEE 802.3AD link aggregation specification.
- STP operates on a logical link and not on a physical link.
- The logical link will have the bandwidth of any active member interfaces.
- It will load balanced across all the links.
- EtherChannels can be used for either Layer 2 (access or trunk) or Layer 3 links.

The terms EtherChannel, EtherChannel bundle, and port channel are interchanged frequently on the Catalyst platform, but other Cisco platforms only use the term port channel exclusively.

EtherChannel Link-State

- EtherChannel may be created statically or dynamically.
- Static EtherChannel does not have a health integrity check. If the physical medium degrades and keeps the line protocol in an up state, the port channel will reflect that link as viable for transferring data.
- A common scenario involves the use of intermediary devices and technologies (for example, powered network taps, IPSs, Layer 2 firewalls, DWDM) between devices. It is critical for the link state to be propagated to the other side.

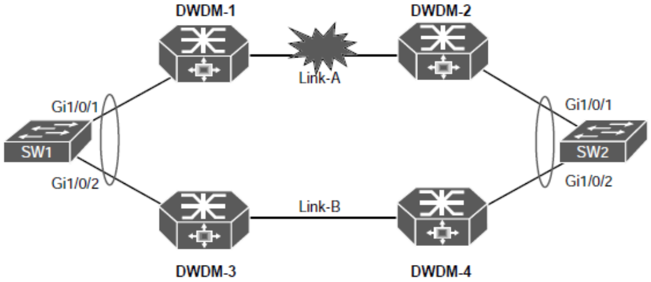


Figure 5-4 *Port-Channel Link-State Propagation and Detection*

EtherChannel Bundle

Dynamic Link Aggregation Protocols

Two common link aggregation protocols are Link Aggregation Control Protocol (LACP) and Port Aggregation Protocol (PAgP).

- PAgP is Cisco proprietary and was developed first.
- LACP was created as an open industry standard.
- All the member links must participate in the same protocol on the local and remote switches.

EtherChannel Bundle

PAgP Port Modes

PAgP advertises messages with the multicast MAC address 0100:0CCC:CCCC and the protocol code 0x0104. PAgP can operate in two modes:

PAgP Port Modes	Description
Auto	• The interface does not initiate an EtherChannel to be established and does not transmit PAgP packets out of it. • If an PAgP packet is received from the remote switch, this interface responds and then can establish a PAgP adjacency. • If both devices are PAgP auto, a PAgP adjacency does not form.
Desirable	• An interface tries to establish an EtherChannel and transmit PAgP packets out of it. • Active PAgP interfaces can establish a PAgP adjacency only if the remote interface is configured to auto or desirable.

LACP Port Modes

LACP advertises messages with the multicast MAC address 0180:C200:0002. LACP can operate in two modes:

LACP Port Modes	Description
Passive	• An interface does not initiate an EtherChannel to be established and does not transmit LACP packets out of it. • If an LACP packet is received from the remote switch, this interface responds and then can establish an LACP adjacency. • If both devices are LACP passive, an LACP adjacency does not form.
Active	• An interface tries to establish an EtherChannel and transmit LACP packets out of it. • Active LACP interfaces can establish an LACP adjacency only if the remote interface is configured to active or passive.

EtherChannel Configurations

It is possible to configure EtherChannels by going into the interface configuration mode for the member interfaces and assigning them to an EtherChannel ID and configuring the appropriate mode:

- **Static EtherChannel:** A static EtherChannel is configured with the interface parameter command **channel-group** *etherchannel-id* **mode on**.
- **LACP EtherChannel:** An LACP EtherChannel is configured with the interface parameter command **channel-group** *etherchannel-id* **mode** {**active** | **passive**}.
- **PAgP EtherChannel:** A PAgP EtherChannel is configured with the interface parameter command **channel-group** *etherchannel-id* **mode** {**auto** | **desirable**} [**non-silent**].
  - By default, PAgP ports operate in silent mode, which allows a port to establish an EtherChannel with a device that is not PAgP capable and rarely sends packets.
  - Using the optional **non-silent** keyword requires a port to receive PAgP packets before adding it to the EtherChannel, which is recommended.

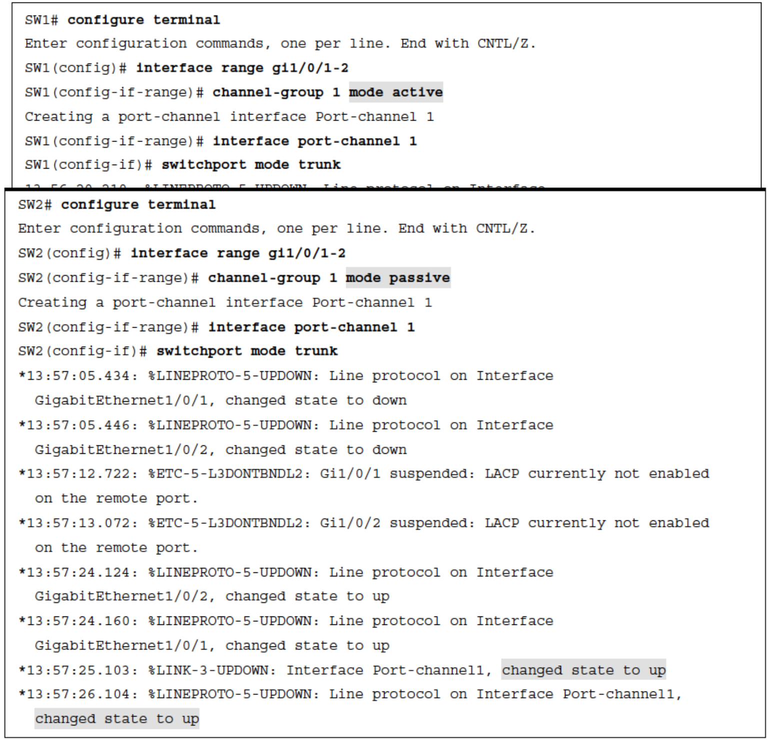
EtherChannel Bundle

EtherChannel Configurations (Cont.)

The following needs to be considered with EtherChannel configuration:

- Configuration settings for the EtherChannel are placed in the port-channel interface.
- Member interfaces need to be in the appropriate Layer 2 or Layer 3 (that is, no switch port) before being associated with the port channel.

Example 5-8 *Sample Port-Channel Configuration*



```
SW1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)# interface range gi1/0/1-2
SW1(config-if-range)# channel-group 1 mode active
Creating a port-channel interface Port-channel 1
SW1(config-if-range)# interface port-channel 1
SW1(config-if)# switchport mode trunk
13:56:20.210: %LINEPROTO-5-UPDOWN: Line protocol on Interface
```

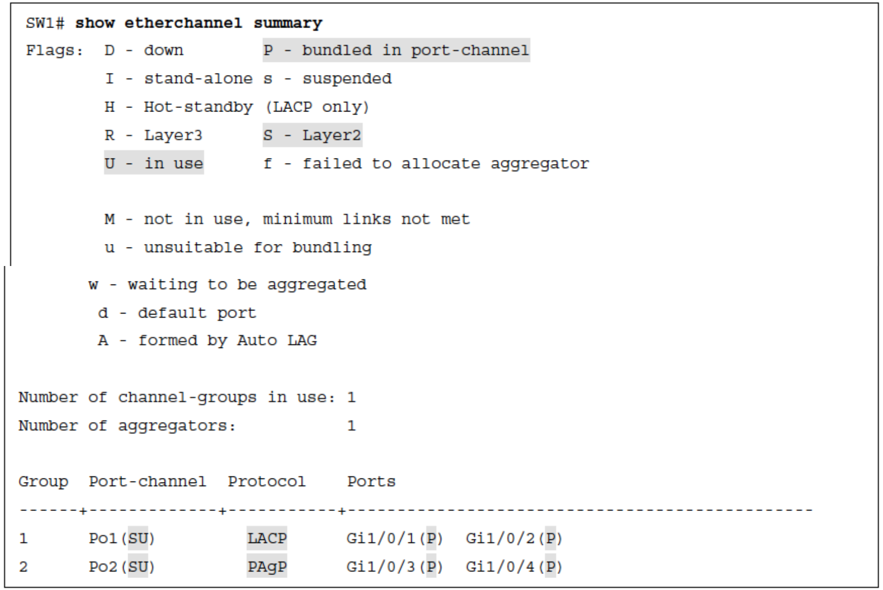
```
SW2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW2(config)# interface range gi1/0/1-2
SW2(config-if-range)# channel-group 1 mode passive
Creating a port-channel interface Port-channel 1
SW2(config-if-range)# interface port-channel 1
SW2(config-if)# switchport mode trunk
*13:57:05.434: %LINEPROTO-5-UPDOWN: Line protocol on Interface
  GigabitEthernet1/0/1, changed state to down
*13:57:05.446: %LINEPROTO-5-UPDOWN: Line protocol on Interface
  GigabitEthernet1/0/2, changed state to down
*13:57:12.722: %ETC-5-L3DONTBNDL2: Gi1/0/1 suspended: LACP currently not enabled
  on the remote port.
*13:57:13.072: %ETC-5-L3DONTBNDL2: Gi1/0/2 suspended: LACP currently not enabled
  on the remote port.
*13:57:24.124: %LINEPROTO-5-UPDOWN: Line protocol on Interface
  GigabitEthernet1/0/2, changed state to up
*13:57:24.160: %LINEPROTO-5-UPDOWN: Line protocol on Interface
  GigabitEthernet1/0/1, changed state to up
*13:57:25.103: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
*13:57:26.104: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1,
  changed state to up
```

EtherChannel Bundle

Verify Port-Channel Status

- As shown in Example 5-9, the command **show etherchannel summary** provides an overview of all the configured EtherChannels, along with the status and dynamic aggregation protocol for each one.
- When viewing the output of the **show etherchannel summary** command, the first thing that should be checked is the EtherChannel status, which is listed in the Port-channel column.
- The status should be SU, as highlighted in Example 5-9.

Example 5-9 *Viewing EtherChannel Summary Status*



```
SW1# show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
        A - formed by Auto LAG

Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------
1      Po1(SU)         LACP      Gi1/0/1(P)  Gi1/0/2(P)
2      Po2(SU)         PAgP      Gi1/0/3(P)  Gi1/0/4(P)
```

Note: The status codes are case sensitive, so please pay attention to the case of the field.

EtherChannel Logical Interface Status Fields

Logical EtherChannel Interface Status Fields are as follows:

- U - The EtherChannel interface is working properly.
- D - The EtherChannel interface is down.
- M - The EtherChannel interface has successfully established at least one LACP adjacency; however, the EtherChannel is configured with a minimum number of active interfaces that exceeds the number of active participating member interfaces. Traffic will not be forwarded across this port channel. The command **port-channel min-links** *min-member-interfaces* is configured on the port-channel interface.
- S - The port-channel interface is configured for Layer 2 switching.
- R - The port-channel interface is configured for Layer 3 routing.

EtherChannel Member Interface Status Fields

EtherChannel Member Interface Status Fields are as follows:

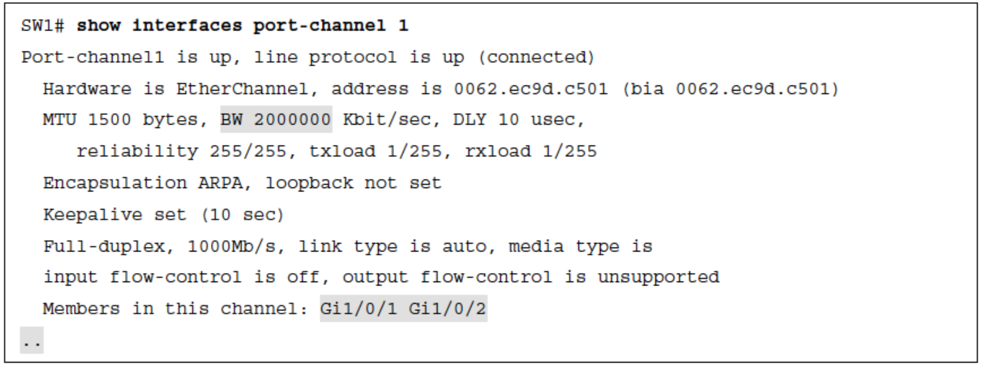
- P - The interface is actively participating and forwarding traffic for this port channel.
- H - The port-channel is configured with the maximum number of active interfaces. This interface is participating in LACP with the remote peer, but the interface is acting as a hot standby and does not forward traffic. The command **lacp max-bundle** *number-member-interfaces* is configured on the port-channel interface.
- I - The member interface has not detected any LACP activity on this interface and is treated as an individual.
- w - There is time left to receive a packet from this neighbor to ensure that it is still alive.
- s - The member interface is in a suspended state.
- r - The switch module associated with this interface has been removed from the chassis.

EtherChannel Bundle

Port-Channel Interface Status

- The logical interface can be viewed with the command **show interface port-channel** *port-channel-id*.
- The output includes traditional interface statistics and lists the member interfaces and indicates that the bandwidth reflects the combined throughput of all active member interfaces.

Example 5-10 *Viewing Port-Channel Interface Status*

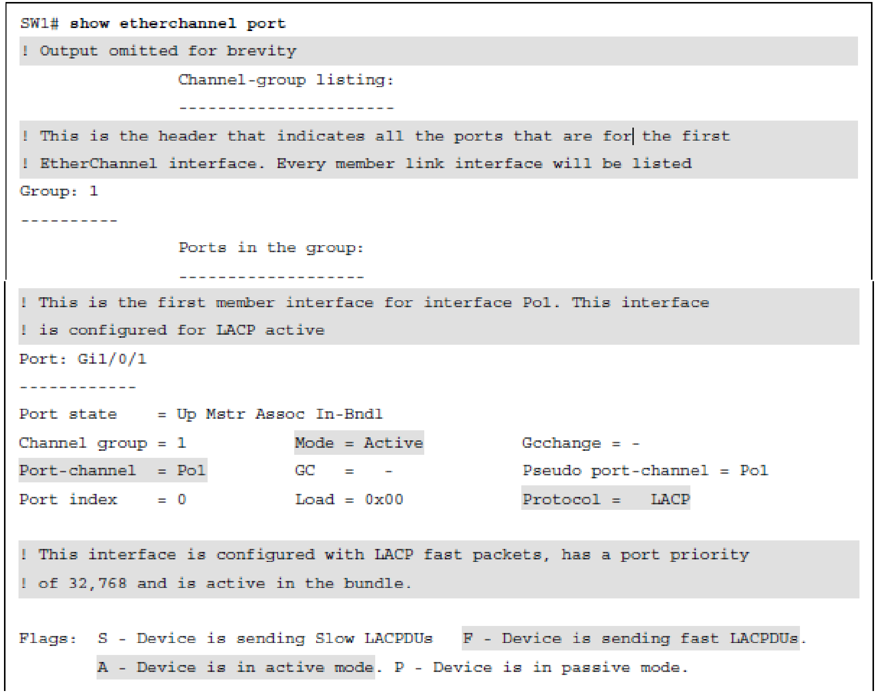


```
SW1# show interfaces port-channel 1
Port-channel1 is up, line protocol is up (connected)
  Hardware is EtherChannel, address is 0062.ec9d.c501 (bia 0062.ec9d.c501)
  MTU 1500 bytes, BW 2000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 1000Mb/s, link type is auto, media type is
  input flow-control is off, output flow-control is unsupported
  Members in this channel: Gi1/0/1 Gi1/0/2
..
```

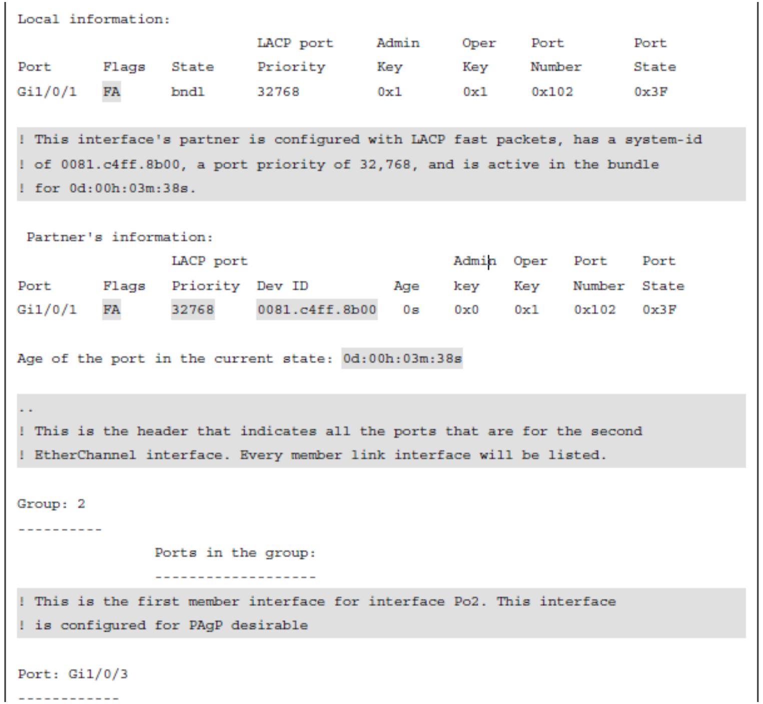
EtherChannel Bundle

EtherChannel Neighbors

Example 5-11 *Viewing show etherchannel port Output*

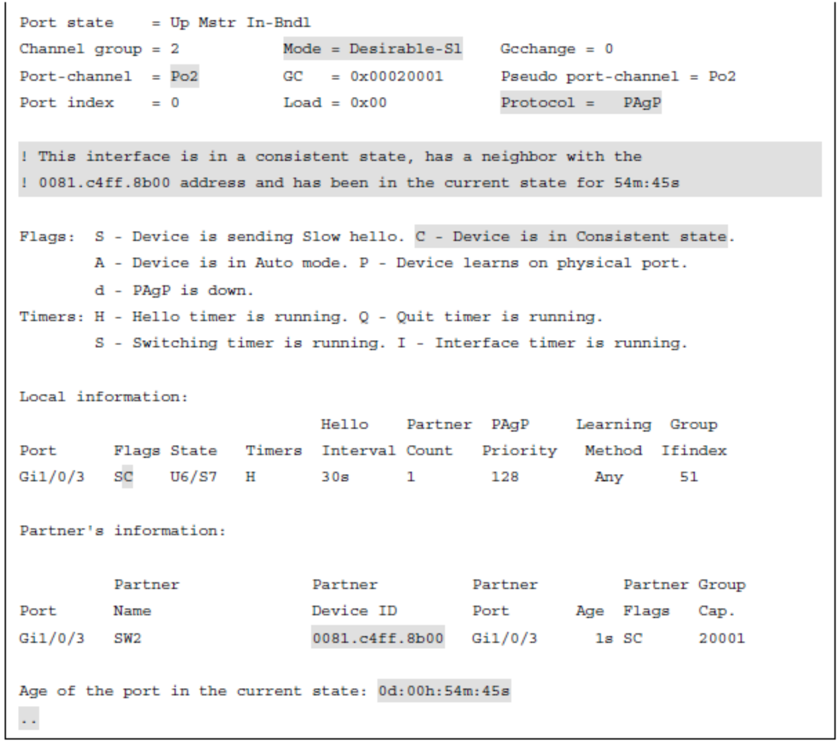


```
SW1# show etherchannel port
! Output omitted for brevity
                Channel-group listing:
                ----------------------
! This is the header that indicates all the ports that are for the first
! EtherChannel interface. Every member link interface will be listed
Group: 1
----------
                Ports in the group:
                -------------------
! This is the first member interface for interface Po1. This interface
! is configured for LACP active
Port: Gi1/0/1
------------
Port state    = Up Mstr Assoc In-Bndl
Channel group = 1           Mode = Active          Gcchange = -
Port-channel  = Po1         GC   =   -             Pseudo port-channel = Po1
Port index    = 0           Load = 0x00            Protocol =   LACP

! This interface is configured with LACP fast packets, has a port priority
! of 32,768 and is active in the bundle.

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.  P - Device is in passive mode.
```



```
Local information:
                             LACP port     Admin    Oper    Port       Port
Port      Flags   State     Priority      Key      Key     Number     State
Gi1/0/1   FA      bndl      32768         0x1      0x1     0x102      0x3F

! This interface's partner is configured with LACP fast packets, has a system-id
! of 0081.c4ff.8b00, a port priority of 32,768, and is active in the bundle
! for 0d:00h:03m:38s.

 Partner's information:
                   LACP port                        Admin  Oper   Port    Port
Port      Flags   Priority   Dev ID          Age    key    Key    Number  State
Gi1/0/1   FA      32768      0081.c4ff.8b00   0s    0x0    0x1    0x102   0x3F

Age of the port in the current state: 0d:00h:03m:38s

..
! This is the header that indicates all the ports that are for the second
! EtherChannel interface. Every member link interface will be listed.

Group: 2
----------
                Ports in the group:
                -------------------
! This is the first member interface for interface Po2. This interface
! is configured for PAgP desirable

Port: Gi1/0/3
------------
```

EtherChannel Neighbors (Cont.)



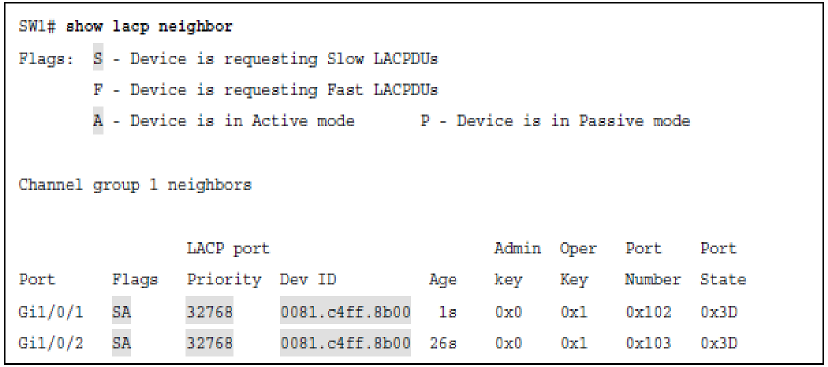
```
Port state     = Up Mstr In-Bndl
Channel group = 2             Mode = Desirable-Sl      Gcchange = 0
Port-channel  = Po2           GC   = 0x00020001        Pseudo port-channel = Po2
Port index    = 0             Load = 0x00              Protocol =   PAgP

! This interface is in a consistent state, has a neighbor with the
! 0081.c4ff.8b00 address and has been in the current state for 54m:45s

Flags:  S - Device is sending Slow hello. C - Device is in Consistent state.
        A - Device is in Auto mode. P - Device learns on physical port.
        d - PAgP is down.
Timers: H - Hello timer is running. Q - Quit timer is running.
        S - Switching timer is running. I - Interface timer is running.

Local information:
                                Hello    Partner  PAgP     Learning  Group
Port      Flags State   Timers  Interval Count   Priority   Method  Ifindex
Gi1/0/3   SC    U6/S7   H       30s      1        128        Any      51

Partner's information:

          Partner               Partner          Partner         Partner Group
Port      Name                  Device ID        Port       Age  Flags   Cap.
Gi1/0/3   SW2                   0081.c4ff.8b00   Gi1/0/3     1s  SC      20001

Age of the port in the current state: 0d:00h:54m:45s
..
```

The output from the **show etherchannel port** command can provide too much information and slow down troubleshooting when a smaller amount of information is needed.

EtherChannel Neighbors LACP and PAgP

The command **show lacp neighbor** [**detail**] displays additional information about the LACP neighbor and includes the neighbor’s system ID, system priority, and whether it is using fast or slow LACP packet intervals as part of the output.

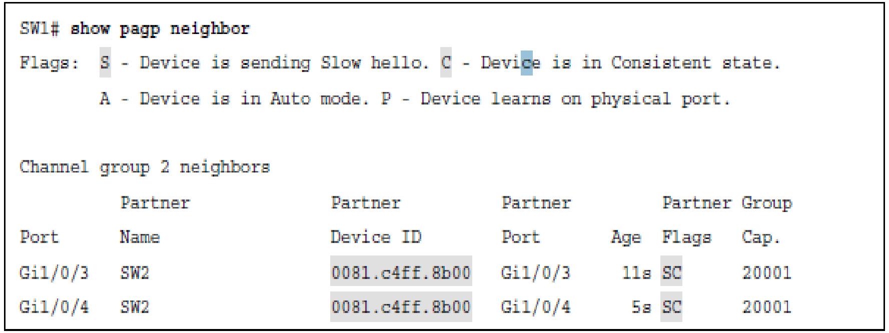
Example 5-12 *Viewing LACP Neighbor Information*



```
SW1# show lacp neighbor
Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode       P - Device is in Passive mode

Channel group 1 neighbors

                  LACP port                         Admin  Oper   Port    Port
Port      Flags   Priority  Dev ID          Age     key    Key    Number  State
Gi1/0/1   SA      32768     0081.c4ff.8b00   1s     0x0    0x1    0x102   0x3D
Gi1/0/2   SA      32768     0081.c4ff.8b00  26s     0x0    0x1    0x103   0x3D
```

The command **show pagp neighbor** displays additional information about the PAgP neighbor and includes the neighbor’s system ID, remote port number, and whether it is using fast or slow PAgP packet intervals as part of the output.

Example 5-13 *Viewing PAgP Neighbor Information*

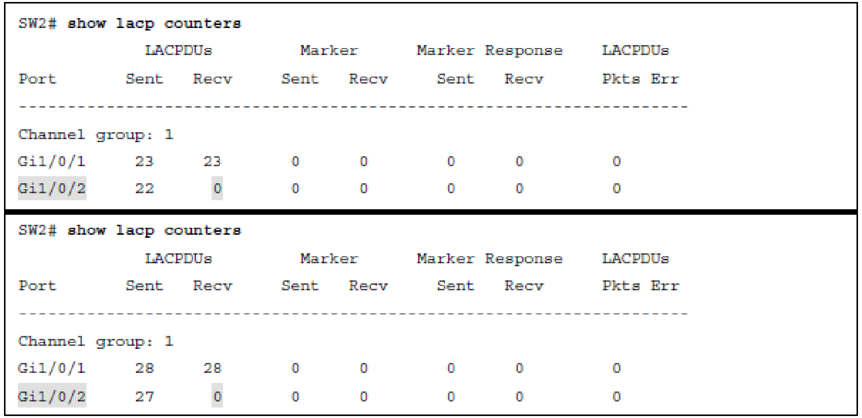


```
SW1# show pagp neighbor
Flags:  S - Device is sending Slow hello.  C - Device is in Consistent state.
        A - Device is in Auto mode.  P - Device learns on physical port.

Channel group 2 neighbors
          Partner              Partner          Partner         Partner Group
Port      Name                 Device ID        Port       Age  Flags   Cap.
Gi1/0/3   SW2                  0081.c4ff.8b00   Gi1/0/3    11s  SC      20001
Gi1/0/4   SW2                  0081.c4ff.8b00   Gi1/0/4     5s  SC      20001
```

Verifying EtherChannel Packets LACP and PAgP

- A vital step in troubleshooting the establishment of port channels is to verify that LACP or PAgP packets are being transmitted between devices.
- The first troubleshooting step that can be taken is to verify the EtherChannel counters for the appropriate protocol.
- The LACP counters can be cleared with the command **clear lacp counters**. The PAgP counters can be cleared with the command **clear pagp counters**.

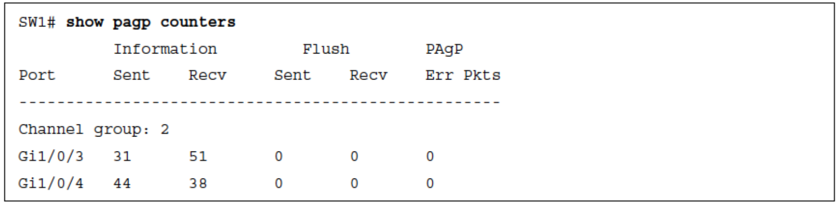
Example 5-14 *Viewing LACP Packet Counters*



```
SW2# show lacp counters
             LACPDUs         Marker      Marker Response    LACPDUs
Port       Sent   Recv     Sent   Recv     Sent   Recv      Pkts Err
---------------------------------------------------------------------
Channel group: 1
Gi1/0/1     23     23       0      0        0      0         0
Gi1/0/2     22      0       0      0        0      0         0
```

```
SW2# show lacp counters
             LACPDUs         Marker      Marker Response    LACPDUs
Port       Sent   Recv     Sent   Recv     Sent   Recv      Pkts Err
---------------------------------------------------------------------
Channel group: 1
Gi1/0/1     28     28       0      0        0      0         0
Gi1/0/2     27      0       0      0        0      0         0
```

Example 5-15 *Viewing PAgP Packet Counters*



```
SW1# show pagp counters
          Information         Flush        PAgP
Port      Sent     Recv     Sent     Recv     Err Pkts
---------------------------------------------------
Channel group: 2
Gi1/0/3   31       51       0        0        0
Gi1/0/4   44       38       0        0        0
```

Prepare for the Exam

Prepare for the Exam

Key Topics for Chapter 5

Description
VLAN Trunking Protocol (VTP)
VTP revision reset
Dynamic Trunking Protocol (DTP)
Disabling DTP
PAgP port modes
LACP port modes
EtherChannel configuration
Minimum number of port-channel member interfaces
Maximum number of port-channel member interfaces
LACP system priority
LACP interface priority
Troubleshooting EtherChannel Bundles
Load balancing traffic with EtherChannel bundles

Prepare for the Exam

Key Terms for Chapter 5

Terms
Dynamic Trunking Protocol (DTP)
EtherChannel bundle
member links
LACP interface priority
LACP system priority
load-balancing hash
VLAN Trunking Protocol (VTP)

Prepare for the Exam

Command Reference for Chapter 5

Task	Command Syntax
Configure the VTP version	**vtp version** {**1** | **2** | **3**}
Configure the VTP domain name	**vtp domain** *domain-name*
Configure the VTP mode for a switch	**vtp mode** { **server** | **client** | **transparent** | **none**} (required for the first VTP v3 server) **vtp primary**
Display the STP root bridge and cost	**switchport mode dynamic desirable**
Configure a switch port to actively attempt to establish a trunk link	**switchport mode dynamic auto**
Configure the member ports for a static EtherChannel	**channel-group** *etherchannel-id* **mode on**

Prepare for the Exam

Command Reference for Chapter 5 (Cont.)

Task	Command Syntax
Configure the member ports for a LACP EtherChannel	**channel-group** *etherchannel-id* **mode** {**active** | **passive**}
Configure the member ports for a PAgP EtherChannel	**channel-group** *etherchannel-id* **mode** {**auto** | **desirable**} [**non-silent**]
Configure the LACP packet rate	**lacp rate** {**fast** | **slow**}
Configure the minimum number of member links for the LACP EtherChannel to become active	**port-channel min-links** *min-links*
Configure the maximum number of member links in an LACP EtherChannel	**lacp max-bundle** *max-links*

Prepare for the Exam

Command Reference for Chapter 5 (Cont.)

Task	Command Syntax
Configure a switch’s LACP system priority	**lacp system-priority** *priority*
Configure a switch’s LACP port priority	**lacp port-priority** *priority*
Configure the EtherChannel load-balancing hash algorithm	**port-channel load-balance** *hash*
Display the contents of all current access lists	**show access-list** [*access-list-number* | *access-list-name*}
Display the VTP system settings	**show vtp status**
Display the switch port DTP settings, native VLANs, and allowed VLANs	**show interface** [*interface-id*] **trunk**
Display a brief summary update on EtherChannel interfaces	**show etherchannel summary**

Thank you! Questions?

Vladimír Veselý

updated: 2023-09-20

https://www.fit.vutbr.cz/research/groups/nes@fit