Implementing Scalable Medium-Sized Networks

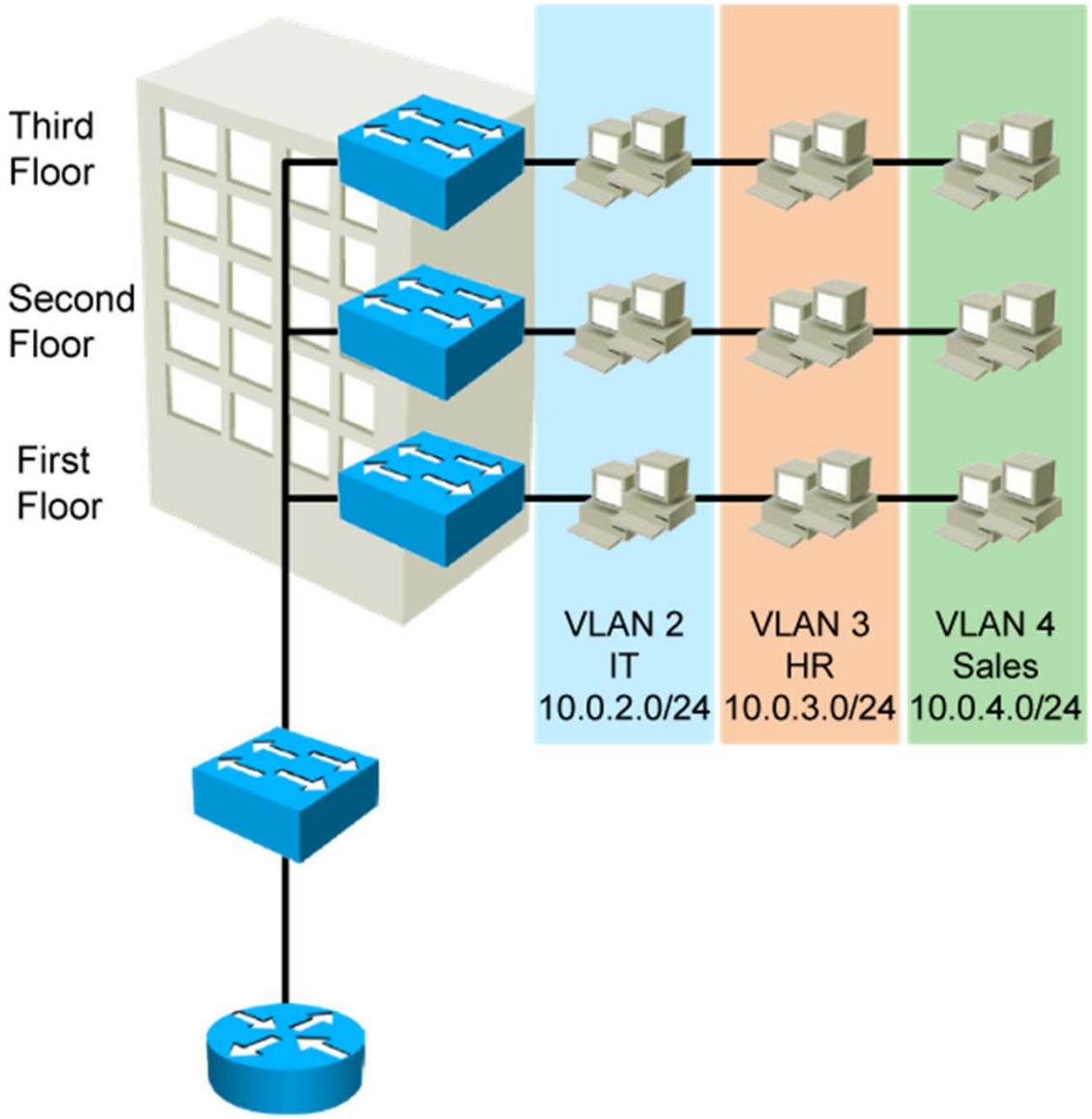
Interconnecting Cisco Networking Devices, Part 2 (ICND2) v2.0

Troubleshooting VLAN Connectivity

Implementing Scalable Medium-Sized Networks

VLAN Overview

- A VLAN has these characteristics:
  - An independent LAN network
  - A broadcast domain
  - A logical network (subnet)
- VLANs address these needs:
  - Segmentation
  - Security
  - Network flexibility



Creating VLANs

```
SwitchX#configure terminal
SwitchX(config)#vlan 2
SwitchX(config-vlan)#name switchlab99
```

- Adds VLAN 2 and names it "switchlab99"

```
SwitchX#configure terminal
SwitchX(config)#interface FastEthernet 0/2
SwitchX(config-if)#switchport access vlan 2
```

- Assigns interface FastEthernet 0/2 to VLAN 2

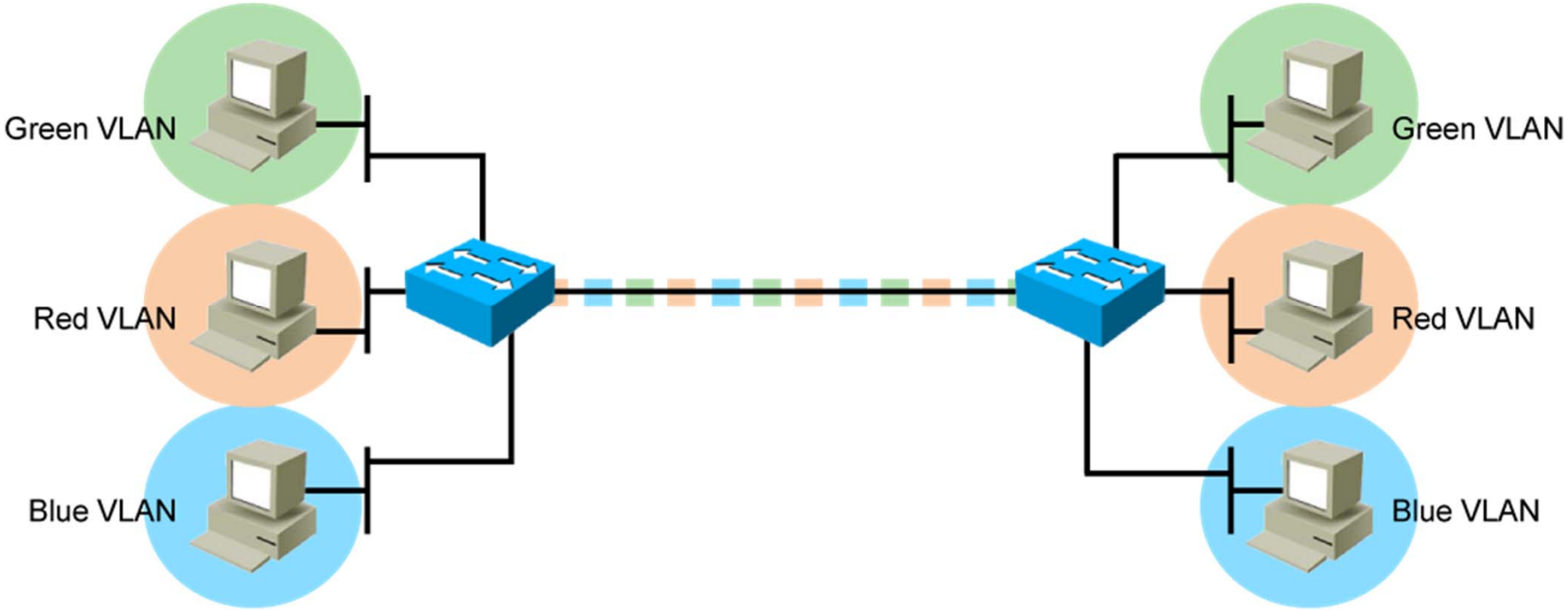
Creating VLANs (Cont.)

```
SwitchX#show vlan

VLAN Name                              Status    Ports
---- --------------------------------  -------   ---------------------
1  default                             active     Fa0/1
2  switchlab99                         active     Fa0/2
3  1002 fddi-default                   act/unsup
<output omitted>
```

- Displays information on all configured VLANs

Trunk Operation

A trunk can carry traffic for multiple VLANs.



Configuring Trunks

- Enter interface configuration mode.
- Configure the Fa0/11 interface as a VLAN trunk.
- The native VLAN is changed to VLAN 99.

```
SwitchX#configure terminal
SwitchX(config)#interface fa0/11
SwitchX(config-if)#switchport mode trunk
SwitchX(config-if)#switchport trunk native vlan 99
```

Configuring Trunks (Cont.)

```
SwitchX#show interfaces FastEthernet 0/11 switchport
Name: Fa0/11
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 99
Trunking Native Mode VLAN: 99
 <output omitted>
```

- Verifies switchport settings on FastEthernet 0/11

```
SwitchX#show interfaces FastEthernet 0/11 trunk

Port          Mode    Encapsulation      Status Native vlan
Fa0/11          on           802.1q    trunking         99

<output omitted>
```

- Verifies that FastEthernet 0/11 is trunking

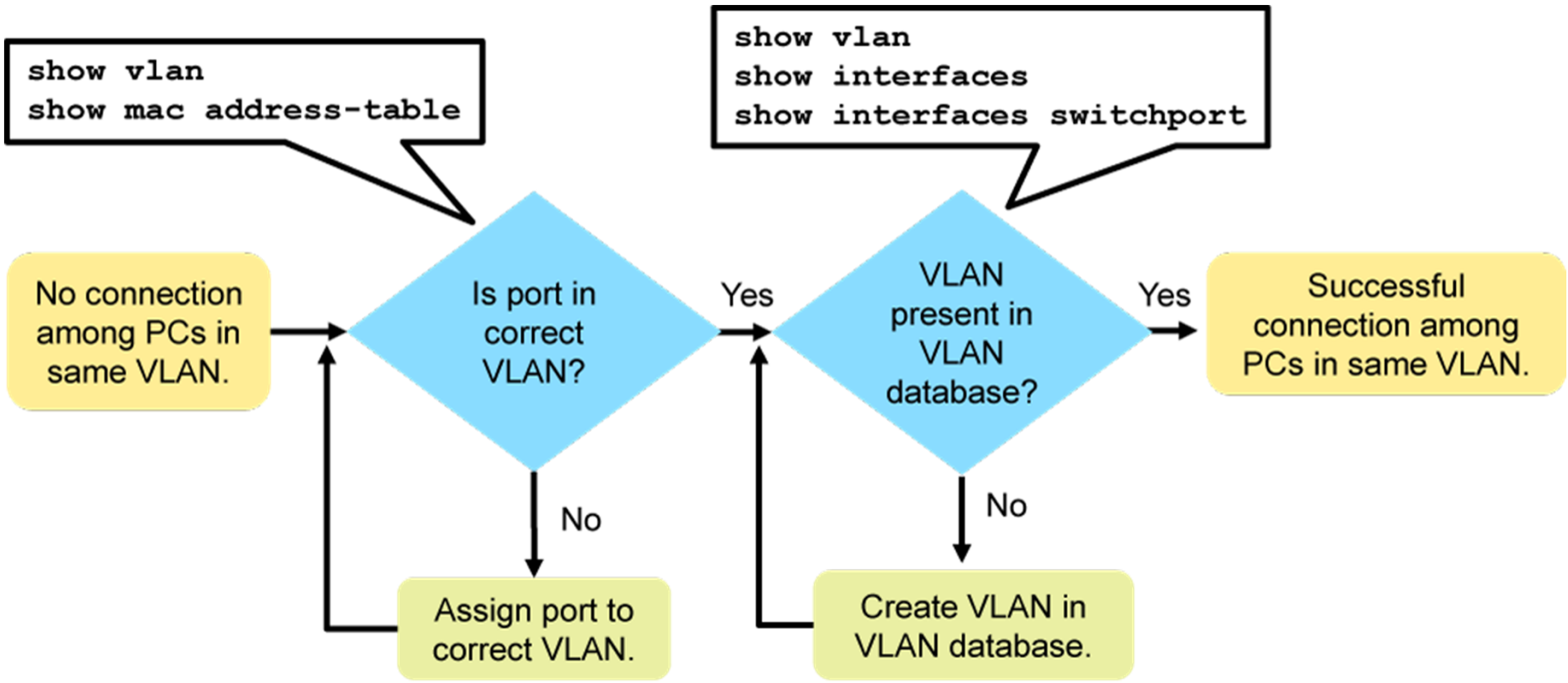
Dynamic Trunking Protocol

Switchport mode interactions:

- Manual configuration is recommended.
- Configure the port as trunk or access on both switches.
- The command **nonegotiate** disables negotiation.

	Dynamic Auto	**Dynamic Desirable**	**Trunk**	**Access**
Dynamic auto	Access	Trunk	Trunk	Access
Dynamic desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	**Trunk**	Limited connectivity
Access	Access	Access	Limited connectivity	**Access**

VLAN Troubleshooting



VLAN Troubleshooting (Cont.)

```
SW1#show mac address-table interface FastEthernet 0/1
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  10    000c.296a.a21c    DYNAMIC     Fa0/1
  10    000f.34f9.9181    DYNAMIC     Fa0/1
Total Mac Addresses for this criterion: 2
```

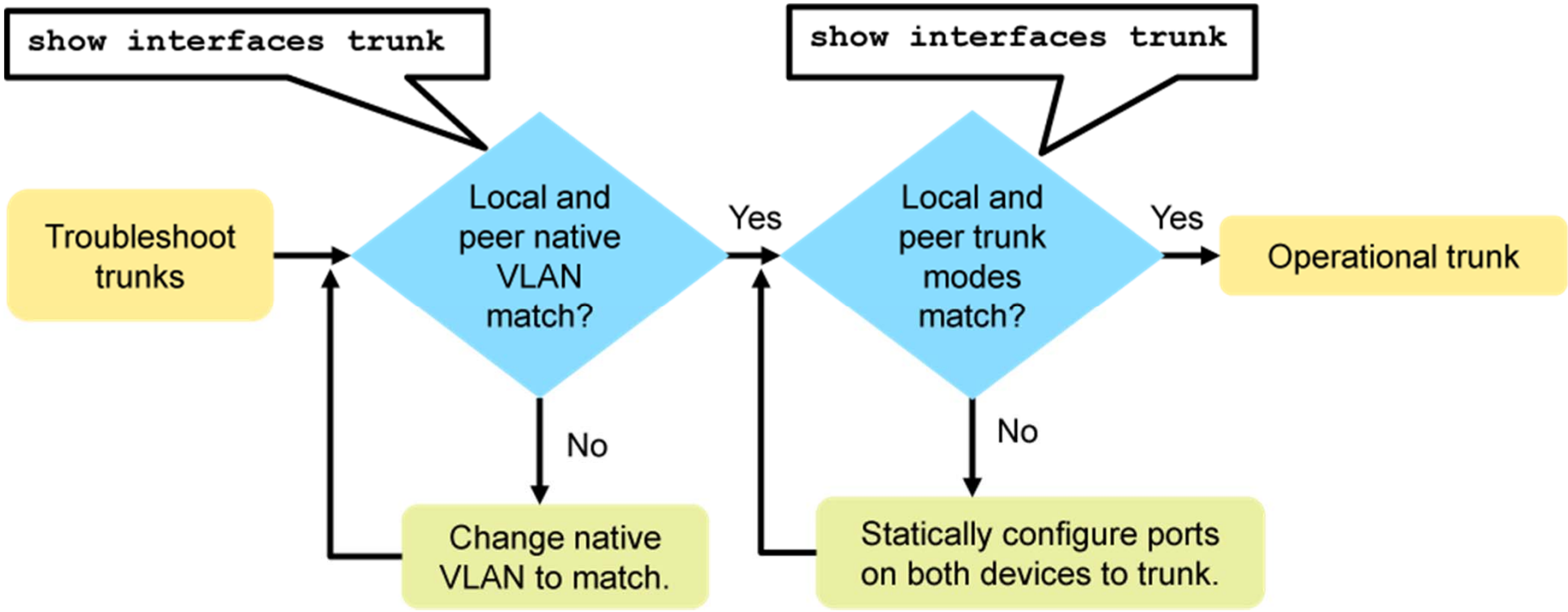
- MAC address table verification

VLAN Troubleshooting (Cont.)

```
SW1#show interfaces FastEthernet 0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 10 (Inactive)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
<output omitted>
```

- Troubleshoot missing VLANs

Trunk Troubleshooting



Trunk Troubleshooting (Cont.)

```
SW1#show interfaces FastEthernet 0/3 trunk

Port        Mode             Encapsulation  Status   Native vlan
Fa0/3       auto             802.1q         not-trunking  2

<output omitted>
```

- Verifies switchport mode, trunk establishment, and the native VLAN on SW1

```
SW2#show interfaces FastEthernet 0/3 trunk

Port        Mode             Encapsulation  Status   Native vlan
Fa0/3       auto             802.1q         not-trunking  1

<output omitted>
```

- Verifies switchport mode, trunk establishment, and the native VLAN on SW2

Summary

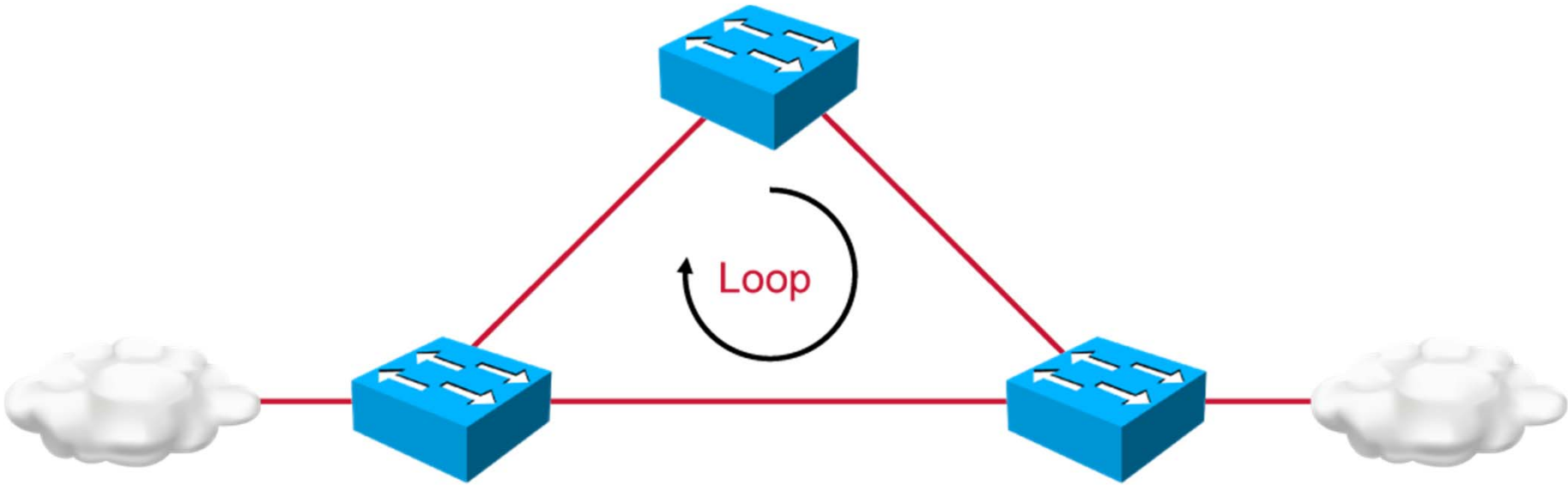
- A VLAN is a logical broadcast domain that can span multiple physical LAN segments.
- A trunk can carry traffic for multiple VLANs.
- DTP can automatically negotiate a trunk link (not recommended).
- You should verify that the port is in the correct VLAN and that the VLAN is present in the VLAN database.
- You should verify that there is no native VLAN mismatch and that a trunk is established.

Building Redundant Switched Topologies

Implementing Scalable Medium-Sized Networks

Issues in Redundant Topologies

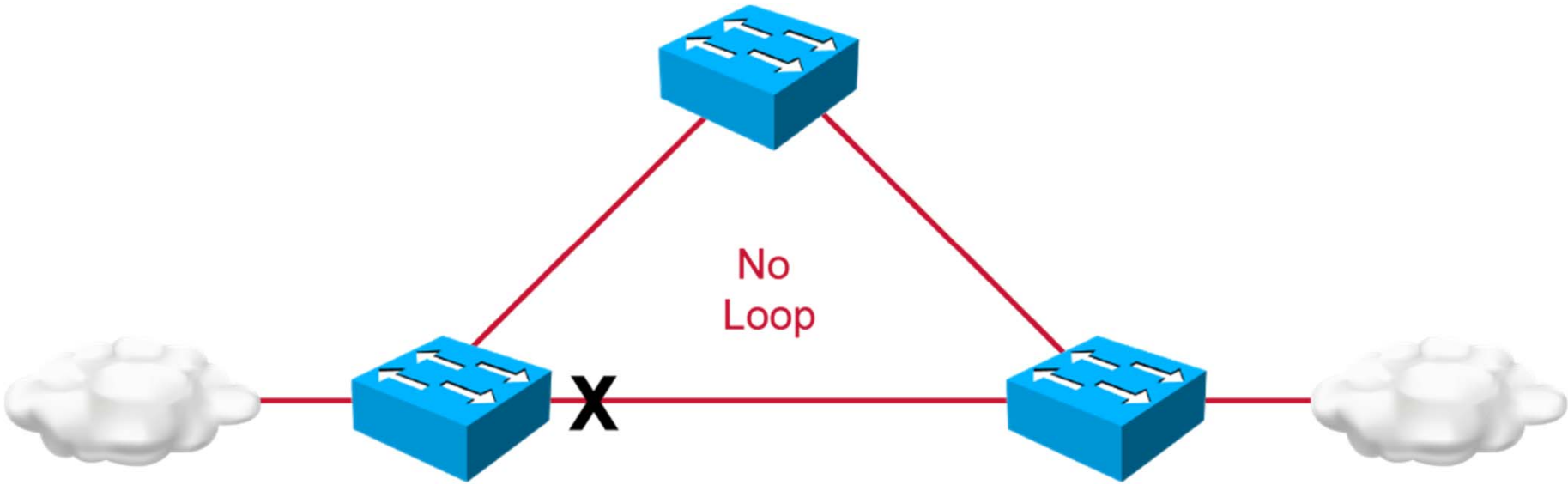
- A redundant topology eliminates single points of failure.
- A redundant switch topology causes broadcast storms, multiple frame copies, and MAC address table instability problems.
- A loop-avoidance mechanism is required.



Issues in Redundant Topologies (Cont.)

Loop resolution with Spanning Tree Protocol:

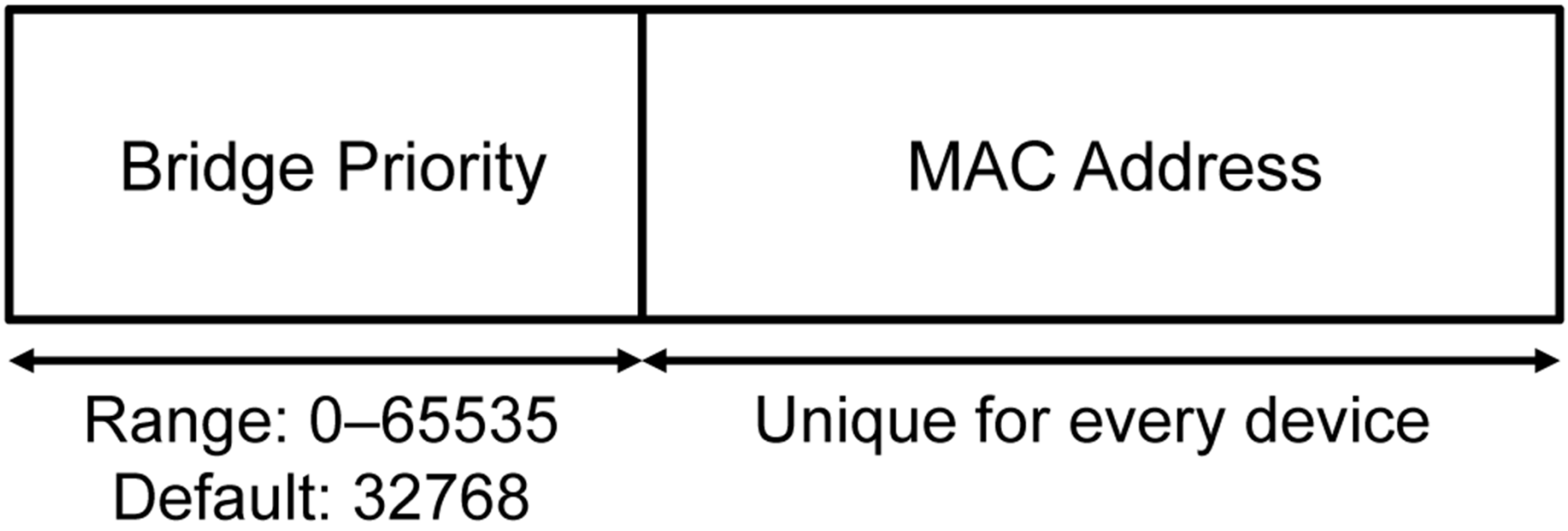
- Provides a loop-free redundant network topology by placing certain ports into a blocking state.
- Published in the IEEE 802.1D specification.



Spanning-Tree Operation

The spanning-tree algorithm follows these steps:

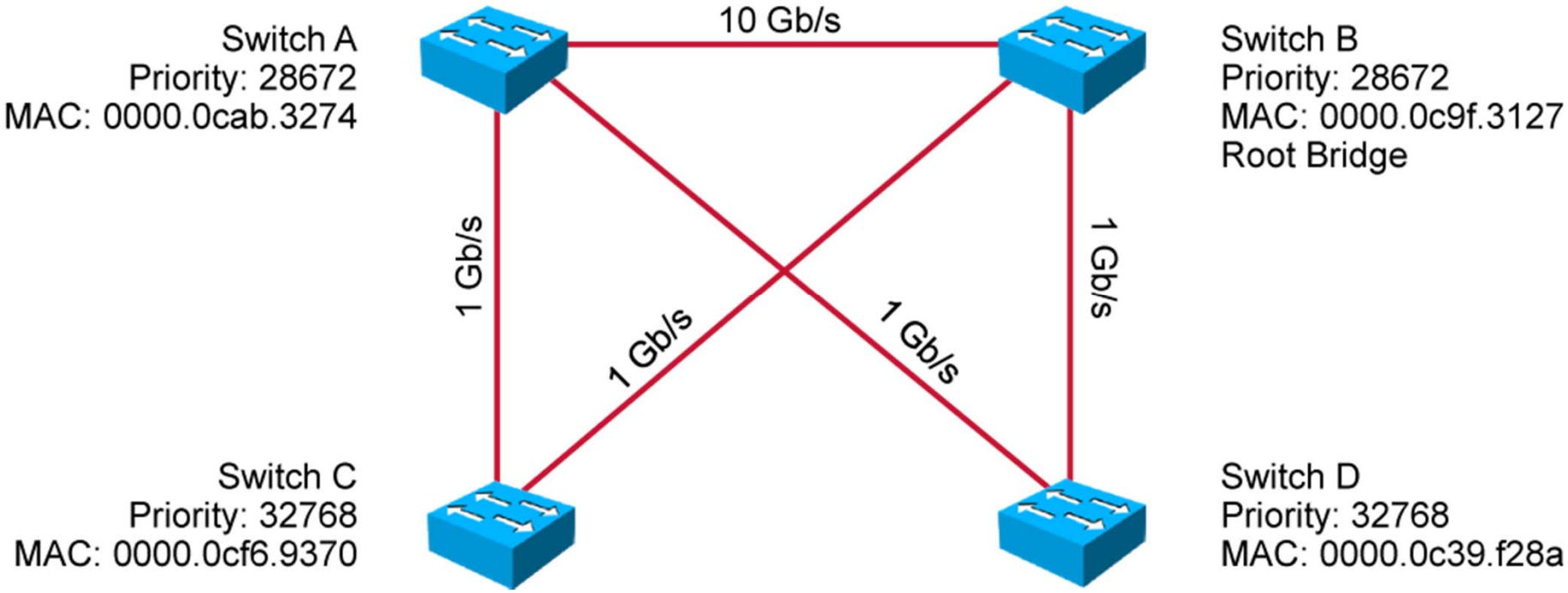
1. Elects a root bridge
2. Elects a root port for each non-root switch
3. Elects a designated port for each segment
4. Ports transition to forwarding or blocking state



Spanning-Tree Operation (Cont.)

Step 1: Elect a root bridge.

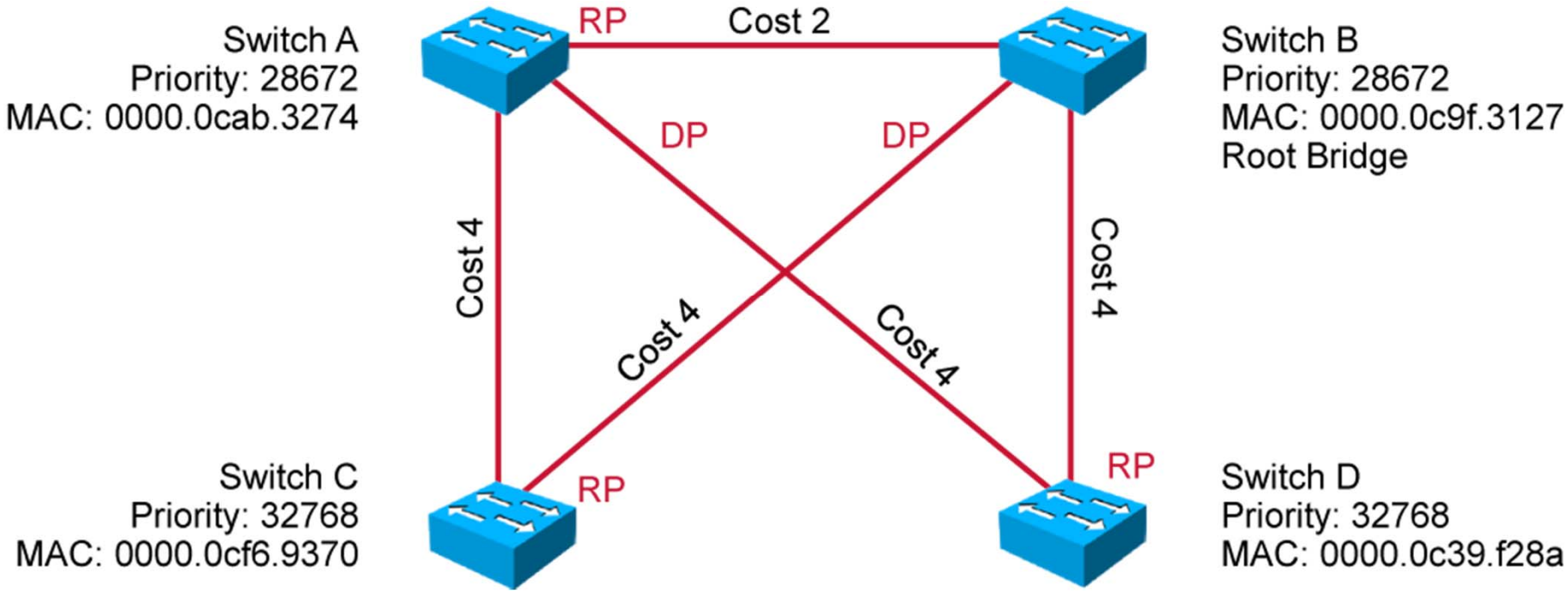
- Decision based on lowest BID.



Spanning-Tree Operation (Cont.)

Step 2: Elect a root port for each non-root switch.

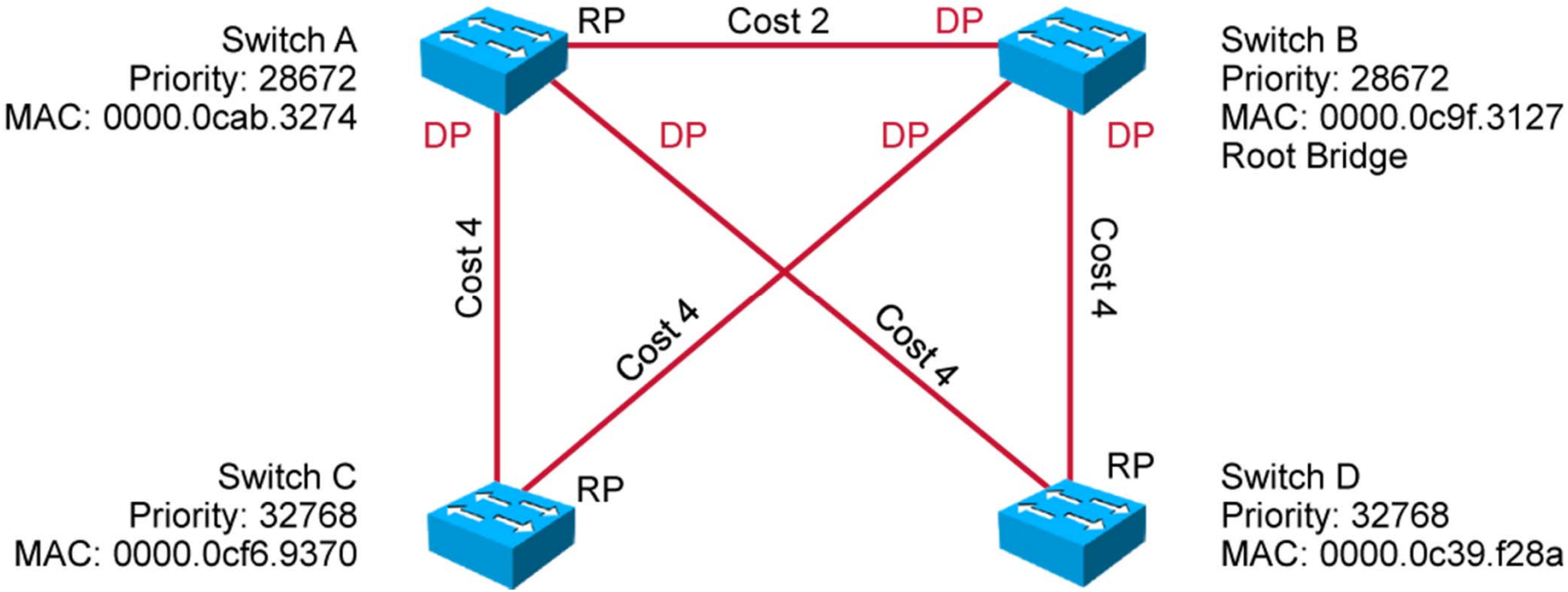
- Decision based on lowest root path cost.
- If necessary, ties are broken by upstream BID and port ID values.



Spanning-Tree Operation (Cont.)

Step 3: Elect a designated port for each segment.

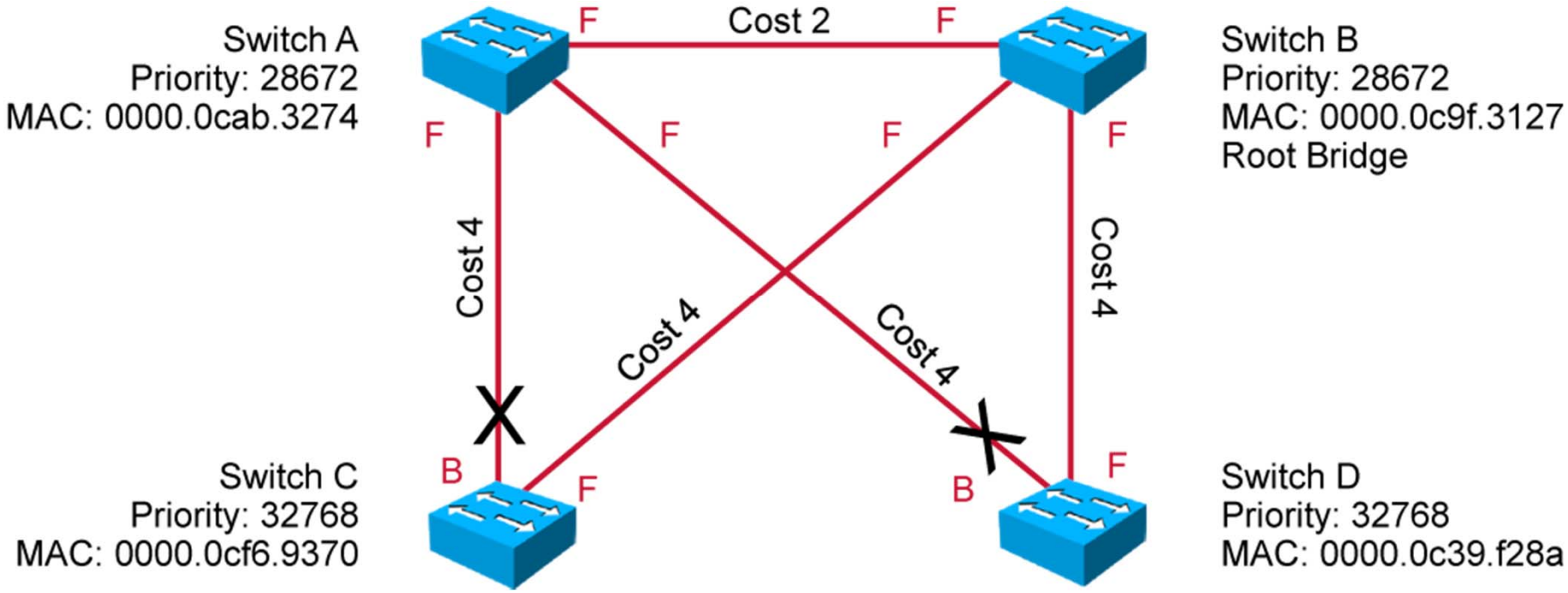
- Decision is based on the lowest root path cost.
- If necessary, ties are broken by upstream BID and port ID.



Spanning-Tree Operation (Cont.)

Step 4: The ports transition to the forwarding or blocking state.

- Root ports and designated ports transition to the forwarding state.
- Other ports stay in the blocking state.



Types of Spanning-Tree Protocols

Spanning-tree standards:

- **IEEE 802.1D:** The legacy standard for bridging and STP
  - **CST:** Assumes one spanning-tree instance for the entire bridged network, regardless of the number of VLANs
- **PVST+:** A Cisco enhancement of STP that provides a separate 802.1D spanning-tree instance for each VLAN configured in the network
- **802.1w (RSTP):** Improves convergence over 1998 STP by adding roles to ports and enhancing BPDU exchanges
- **Rapid PVST+:** A Cisco enhancement of RSTP using PVST+

Types of Spanning-Tree Protocols (Cont.)

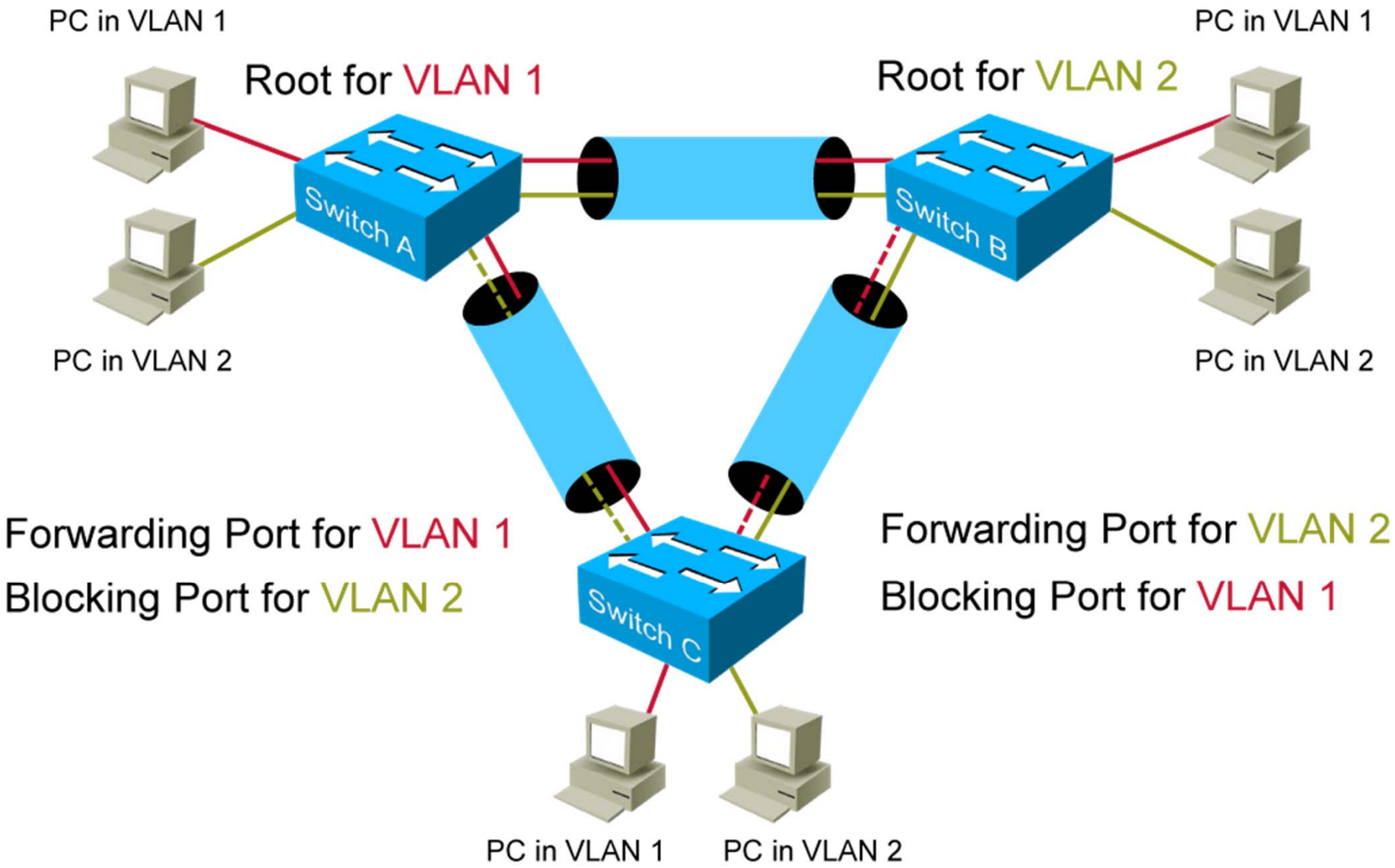
Protocol	Standard	Resources Needed	Convergence	Number of Trees
STP	802.1D	Low	Slow	One
PVST+	Cisco	High	Slow	One for every VLAN
RSTP	802.1w	Medium	Fast	One
Rapid PVST+	Cisco	Very high	Fast	One for every VLAN

Types of Spanning Tree Protocols (Cont.)

Default spanning tree configuration for Cisco Catalyst switches:

- PVST
- Enabled on all ports
- Slower convergence after topology change than with RSTP.

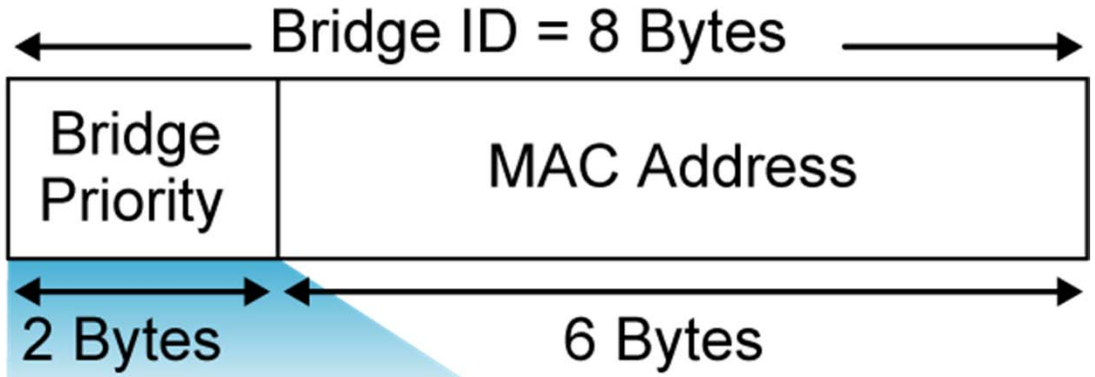
Per VLAN Spanning Tree Plus



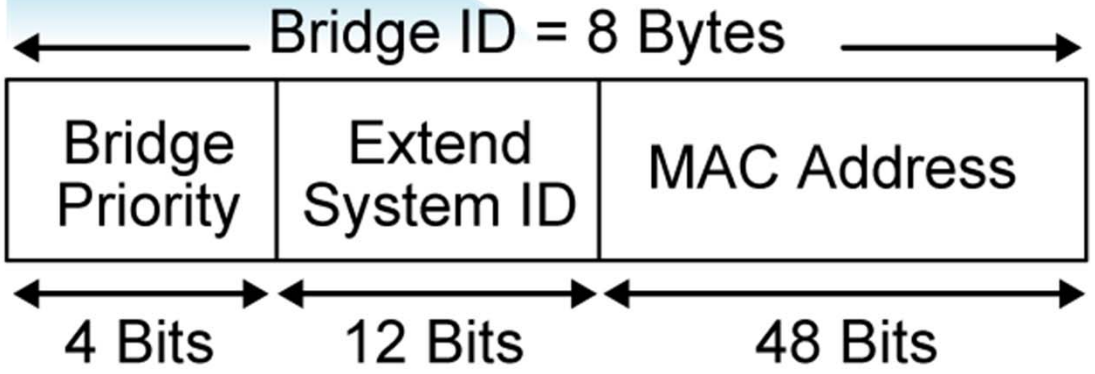
Per VLAN Spanning Tree Plus (Cont.)

System ID = VLAN

Bridge ID Without the Extended System ID



Extended Bridge ID with System ID = VLAN



Modifying the Bridge ID

```
SW1#show spanning-tree vlan 1

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    28673
              Address     001e.145e.4980
              Cost        19
              Port        3 (FastEthernet0/3)
<output omitted>
```

- SW1 is not the root bridge for VLAN1. This is the switch that is connected to FastEthernet0/3 on SW1.

Modifying the Bridge ID (Cont.)

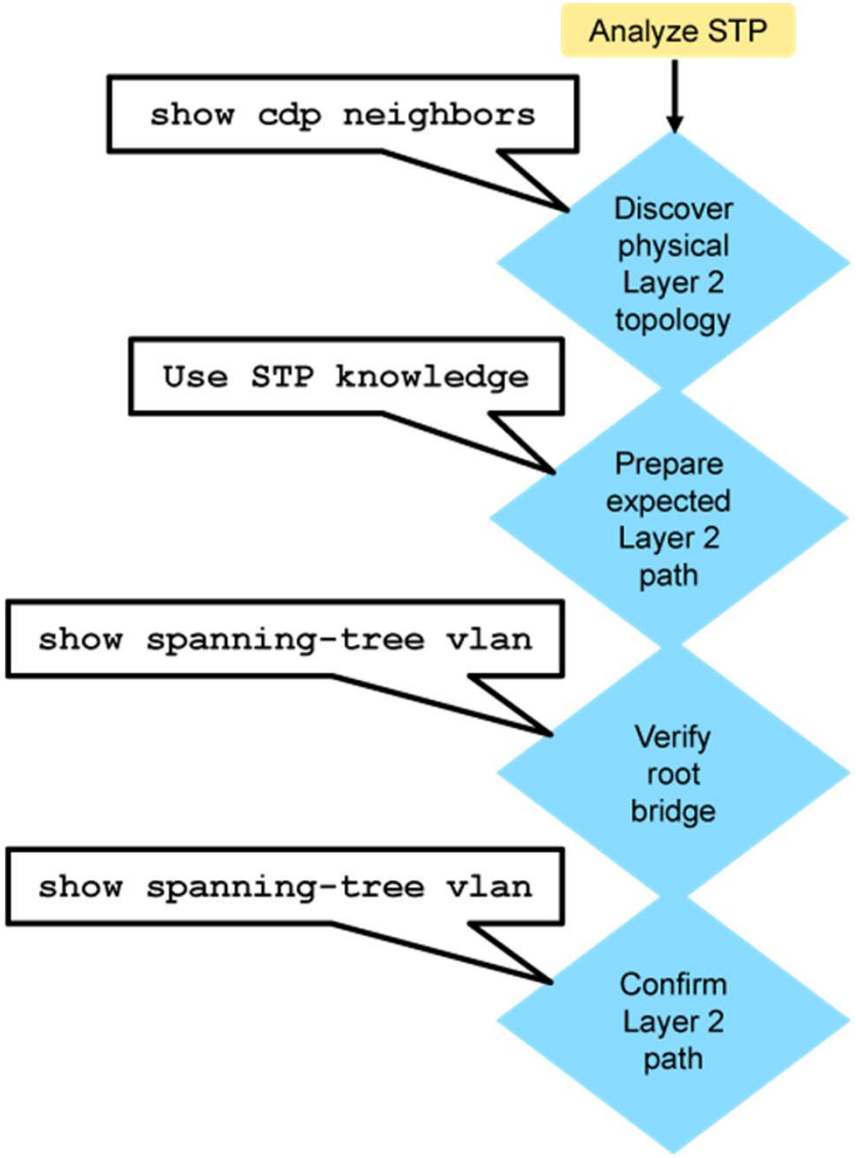
```
SW1(config)#spanning-tree vlan 1 root primary
```

- Configures SW1 as the root bridge for VLAN 1

```
SW1#show spanning-tree vlan 1

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    24577
             Address     001e.147c.6f00
             This bridge is the root
<output omitted>
```

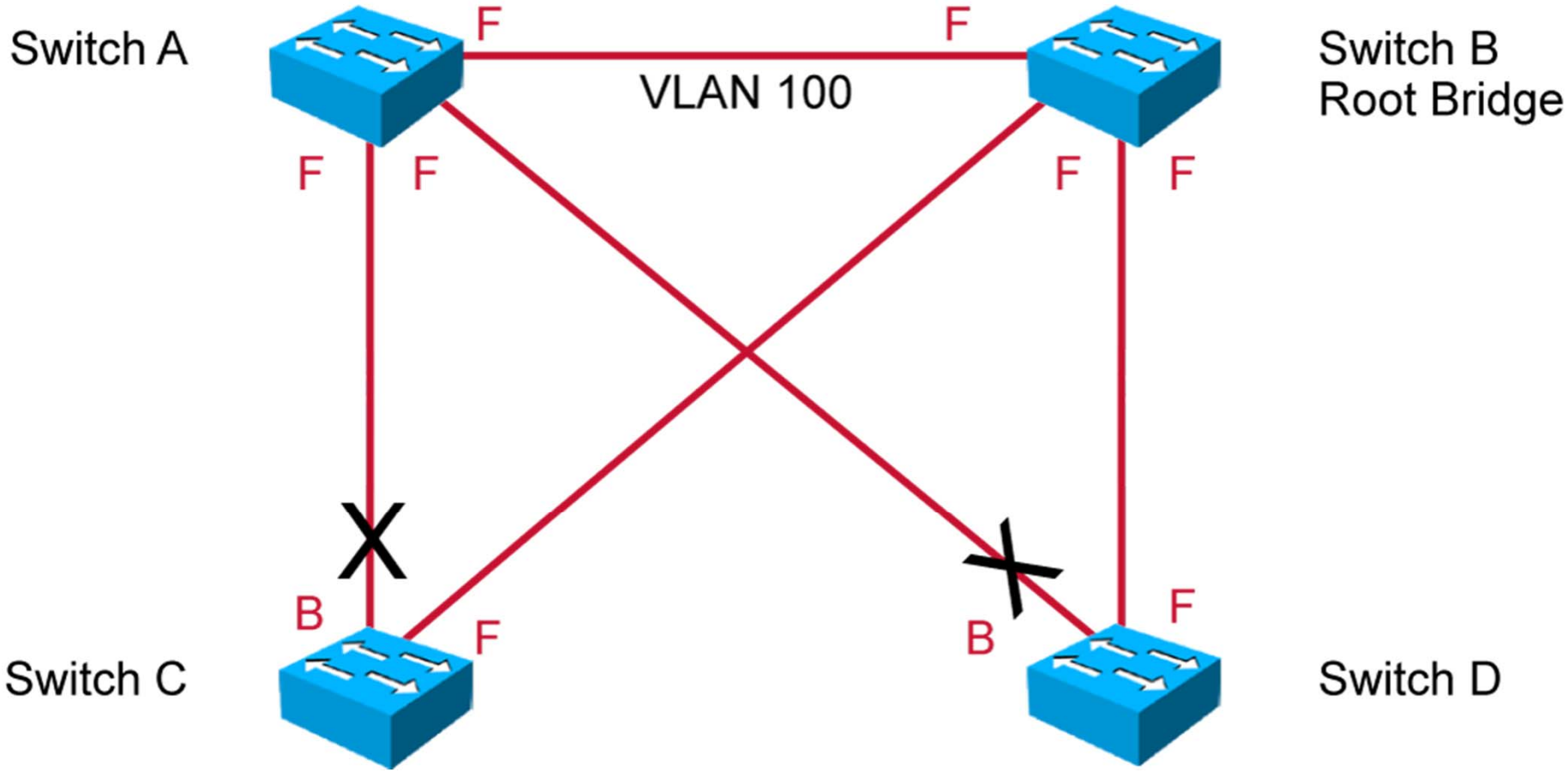
- After modification, SW1 is the root bridge for VLAN1.

Analyzing the STP Topology



Analyzing the STP Topology (Cont.)

Verify that the actual STP topology matches the expected topology.



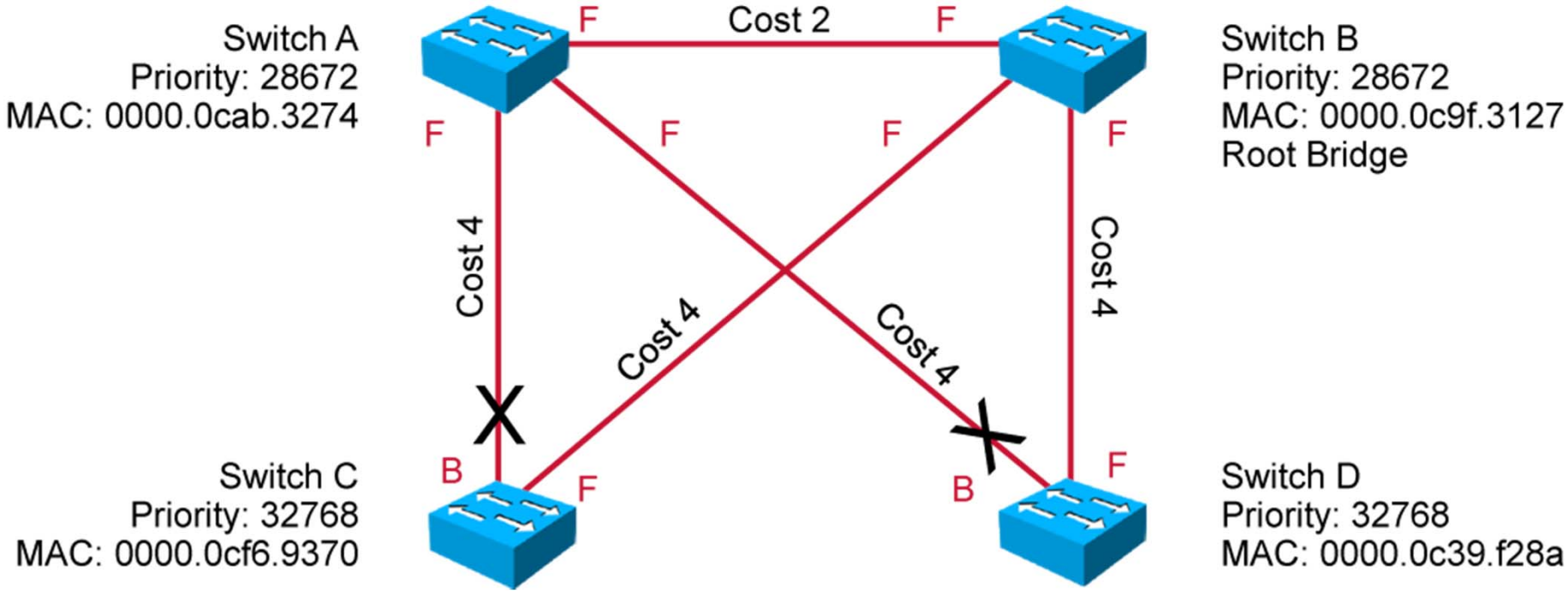
Analyzing the STP Topology (Cont.)

```
SwitchA#show spanning-tree vlan 100

VLAN0100
  Spanning tree enabled protocol ieee
  Root ID     Priority    28772
              Address     0000.0c9f.3127
              Cost        2
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    28772  (priority 28672 sys-id-ext 100)
              Address     0000.0cab.3724
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi3/1               Desg FWD 4         128.72   P2p
Gi3/2               Desg FWD 4         128.80   P2p
Te9/1               Root FWD 2         128.88   P2p
```

- Displays an overview of STP status and topology

Spanning-Tree Failure Consequences

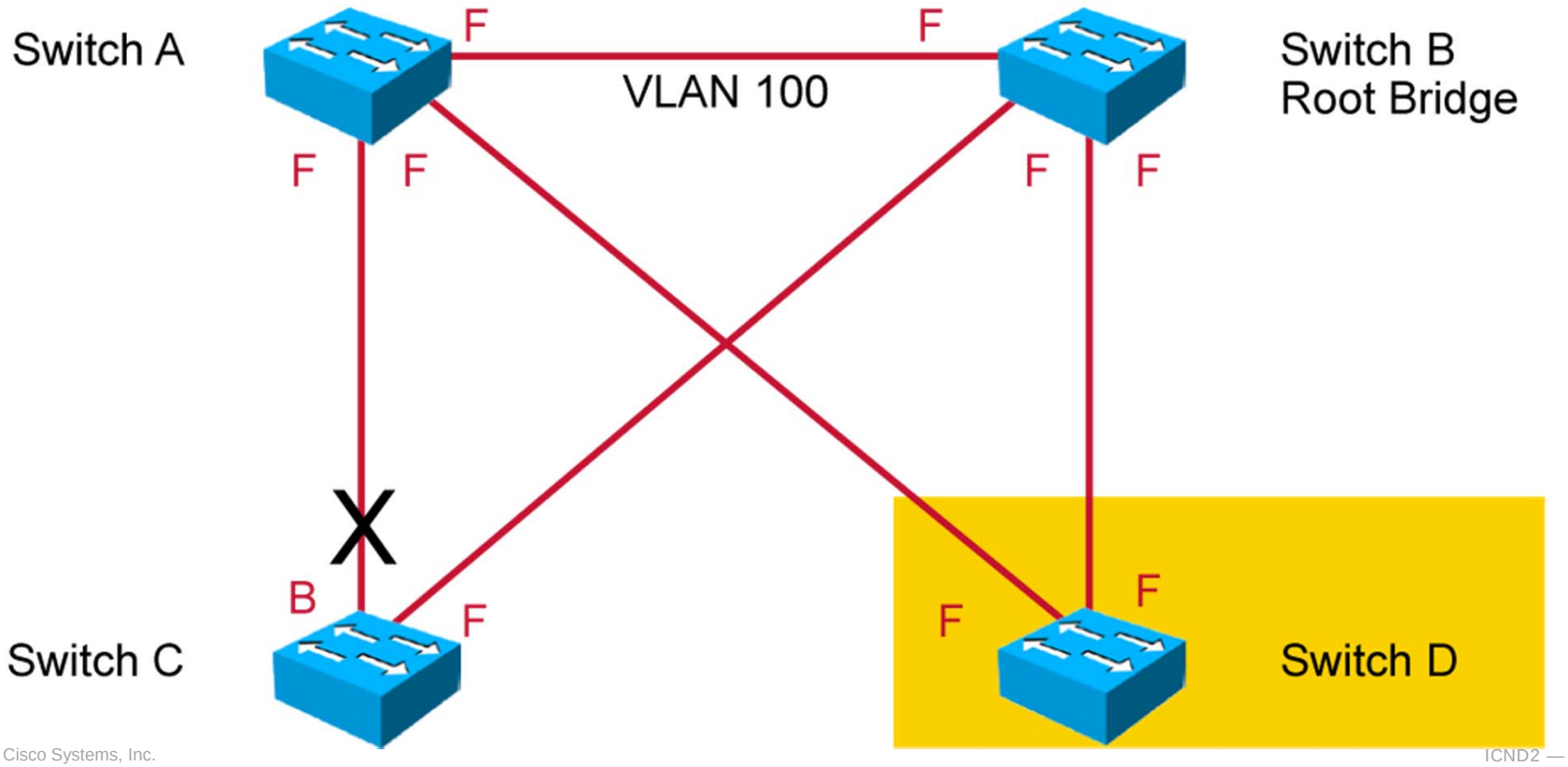
If STP fails for any reason, it fails catastrophically.



Spanning-Tree Failure Consequences (Cont.)

What will happen to this network if Switch D erroneously transitions both its ports to the forwarding state?

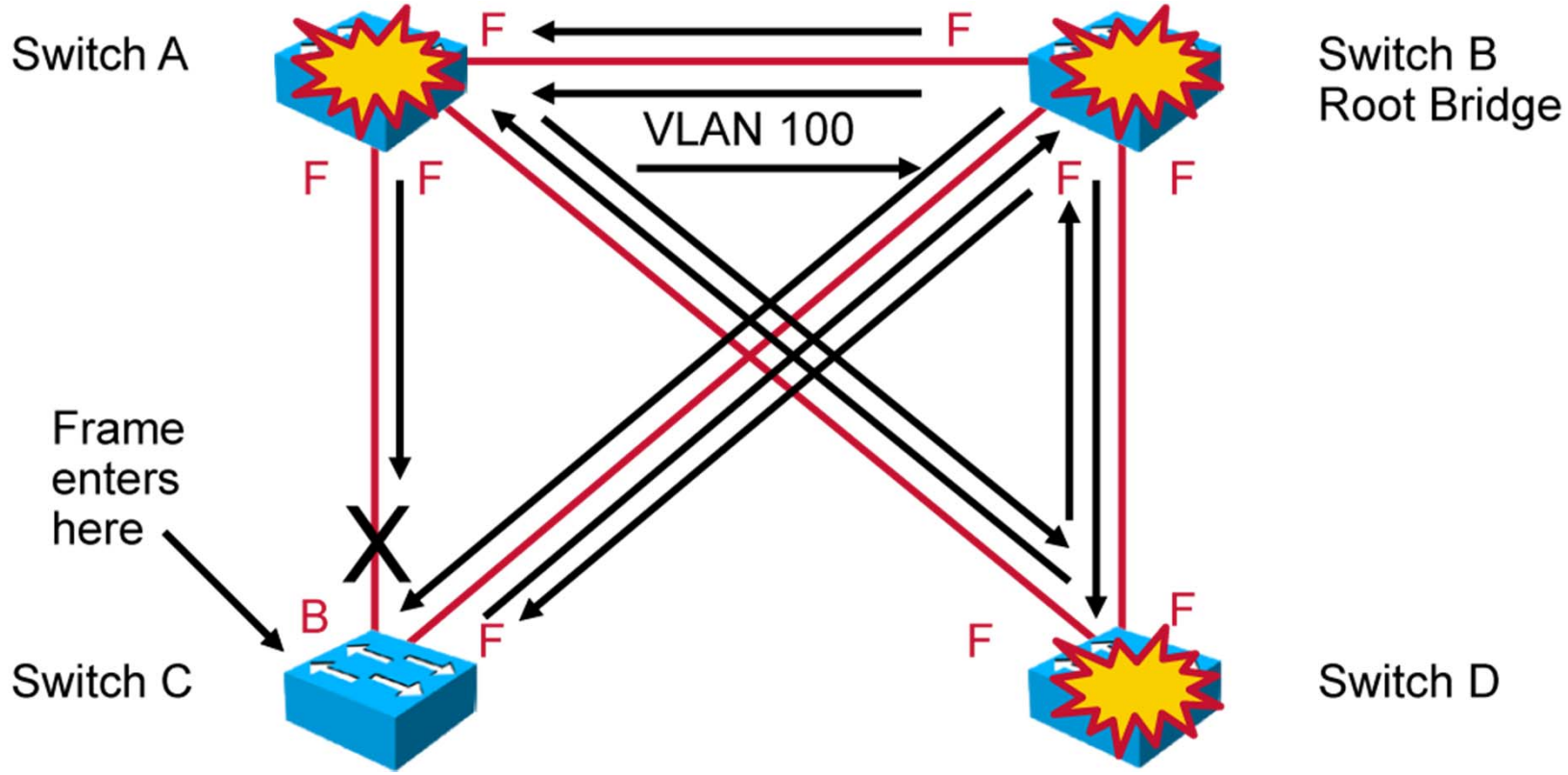
- Any frame that enters a bridging loop will continue to be forwarded by the switches indefinitely.



Spanning-Tree Failure Consequences (Cont.)

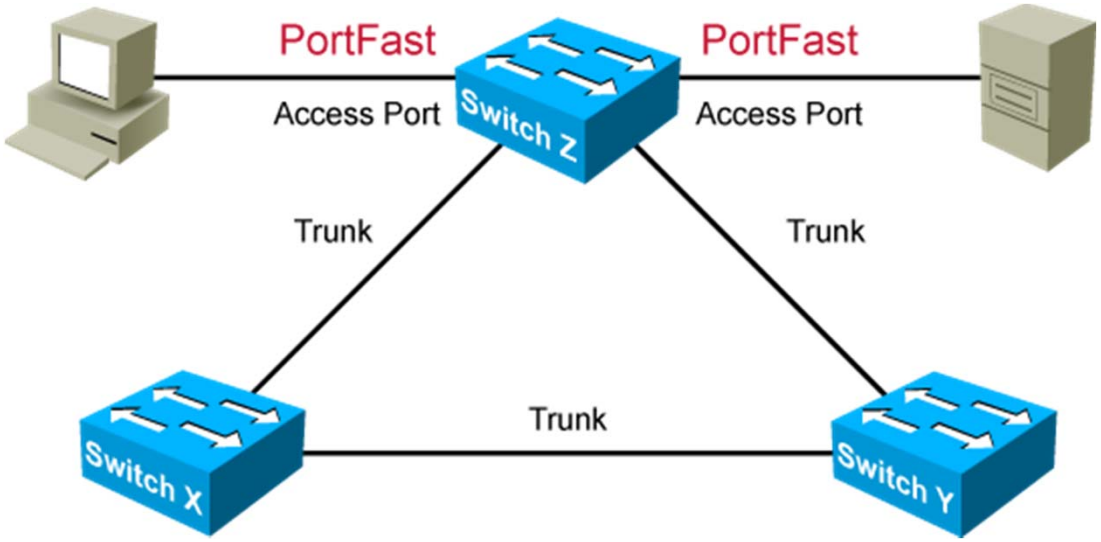
The consequences of STP failure are severe.

- The load on all links in the switched LAN quickly starts increasing.
- Due to the very high load for the CPU, the switch becomes unreachable.



PortFast and BPDU Guard

- PortFast characteristics:
  - Immediate transition to forwarding state
  - Configured only on access ports
- BPDU Guard characteristics:
  - If BPDU is received, it shuts down the port
  - Usually used in a combination with PortFast



PortFast and BPDU Guard (Cont.)

```
SwitchX(config)#interface FastEthernet0/1
SwitchX(config-if)#spanning-tree portfast
SwitchX(config-if)#spanning-tree bpduguard enable
```

- Configures BPDU guard and PortFast on interface FastEthernet0/1

```
SwitchX(config)#spanning-tree portfast bpduguard default
SwitchX(config)#spanning-tree portfast default
```

- Enables PortFast on all nontrunking interfaces and enables BPDU guard globally for all PortFast-enabled ports

PortFast and BPDU Guard (Cont.)

```
SwitchX#show running-config interface FastEternet0/1

Building configuration...

Current configuration : 57 bytes
!
interface FastEthernet0/1
  spanning-tree portfast
  spanning-tree bpduguard enable
end
```

- Verifies that PortFast and BPDU guard have been configured on interface FastEthernet0/1

```
SwitchX#show spanning-tree interface FastEthernet 0/1 portfast
VLAN0010            enabled
```

- Verifies that PortFast is enabled on FastEthernet0/1

Summary

- A redundant switch topology causes broadcast storms, multiple frame copies, and MAC address table instability problems.
- STP allows physical path redundancy while preventing the undesirable effects of active loops in the network.
- A root bridge is elected based on the lowest BID.
- There are many STP standards. PVST+ is a Cisco enhancement of STP that provides a separate 802.1D spanning-tree instance for each VLAN configured in the network.
- PVST+ requires that a separate instance of spanning tree is run for each VLAN, and the BID field must carry VID information. The BID includes the bridge priority, extended system ID, and MAC address.

Summary (Cont.)

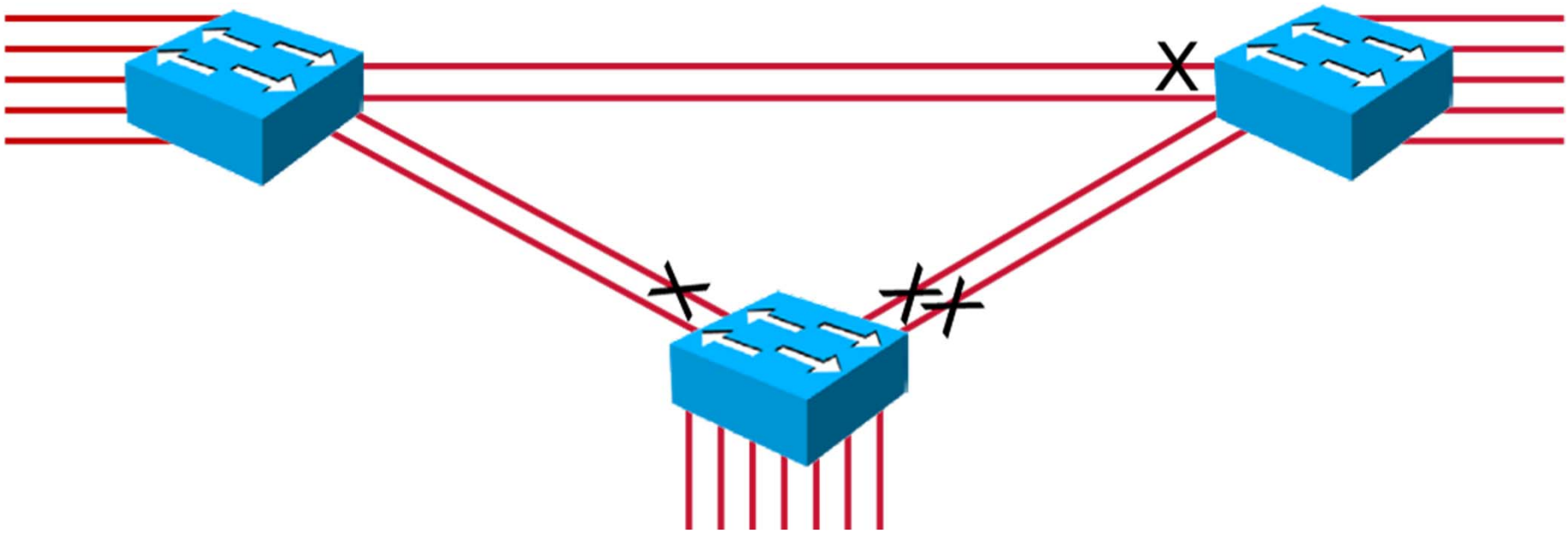
- PortFast is used on ports connected to a single workstation or server to allow those devices to connect to the network immediately.
- If you enable PortFast on a port connecting to another switch, you risk creating a spanning-tree loop. The BPDU guard feature prevents spanning-tree loops in such cases.

Improving Redundant Switched Topologies with EtherChannel

Implementing Scalable Medium-Sized Networks

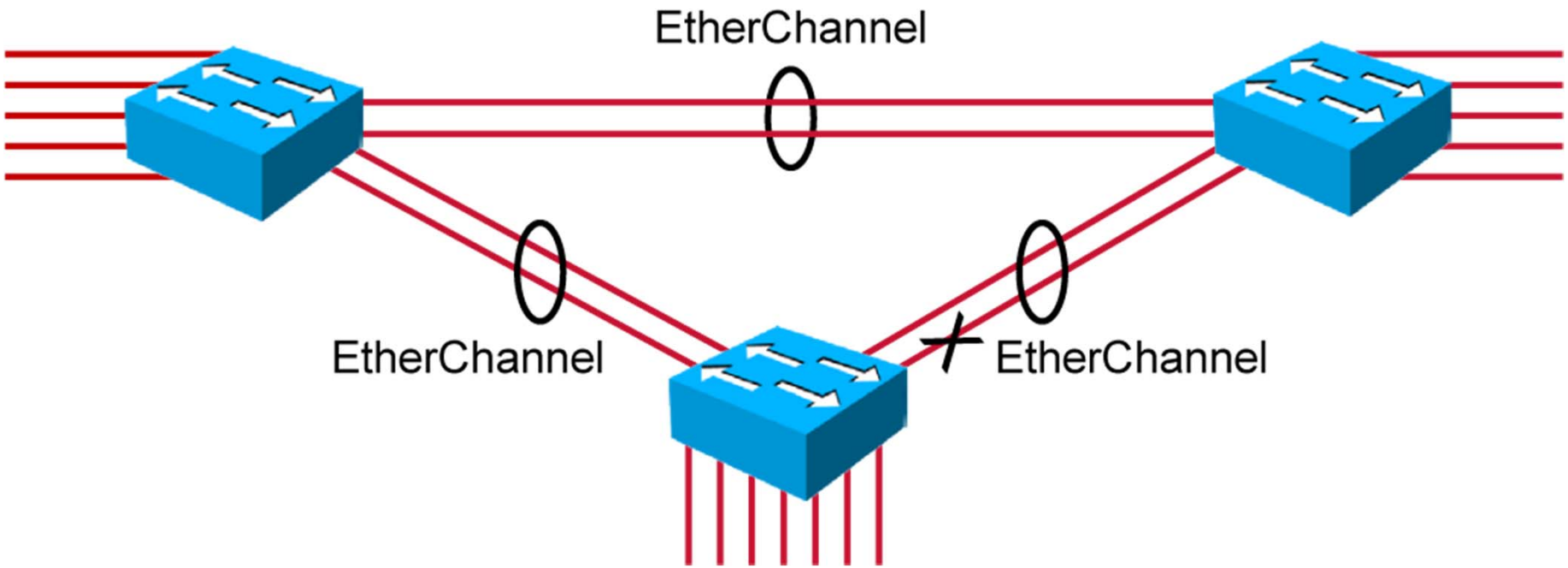
The Need for EtherChannel

- When multiple links aggregate on a switch, congestion occurs.
- One solution is to increase uplink speed, but that solution cannot scale indefinitely.
- Another solution is to multiply uplinks, but loop-prevention mechanisms disable some ports.



Advantages of EtherChannel

- Logical aggregation of links between switches
- High bandwidth
- Load sharing across links
- Viewed as one logical port to STP
- Redundancy



EtherChannel Protocols

- Two protocols exist to negotiate EtherChannel creation and maintenance:
  - PAgP is a Cisco proprietary protocol.
  - LACP is an IEEE 802.3ad standard.
- Static EtherChannel can be configured without PAgP or LACP.

EtherChannel Protocols (Cont.)

PAgP negotiates EtherChannel formation and maintenance.

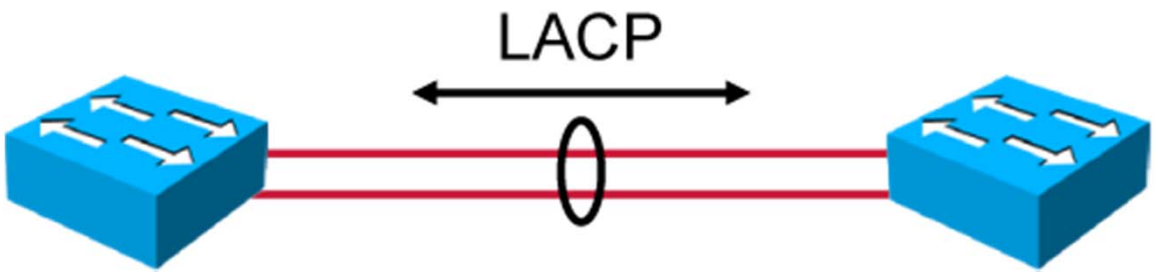
- **On:** Channel member without negotiation (no protocol).
- PAgP modes:
  - **Desirable:** Actively asking if the other side can or will participate
  - **Auto:** Passively waiting for the other side

Channel establishment	On	Desirable	Auto
On	YES	NO	NO
Desirable	NO	YES	YES
Auto	NO	YES	NO

EtherChannel Protocols (Cont.)

LACP negotiates EtherChannel formation and maintenance.

- **On:** Channel member without negotiation (no protocol).
- LACP modes:
  - **Active:** Actively asking if the other side can or will participate
  - **Passive:** Passively waiting for the other side

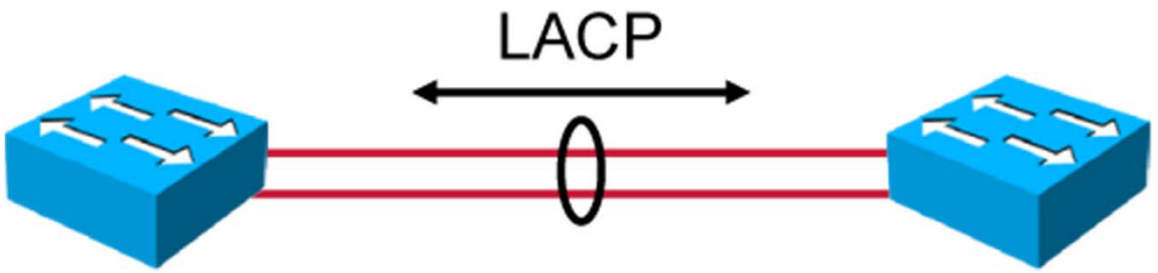


Channel Establishment	On	Active	Passive
On	YES	NO	NO
Active	NO	YES	YES
Passive	NO	YES	NO

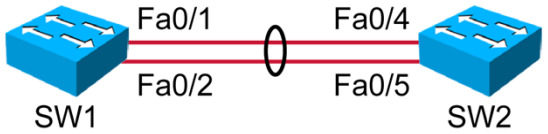
Configuring EtherChannel

All interfaces within an EtherChannel must have the same configuration:

- Speed and duplex
- Mode (access or trunk)
- Native and allowed VLANs on trunk ports
- Access VLAN on access ports



Configuring EtherChannel (Cont.)




```
SW1(config)#interface range FastEthernet0/1 - 2
SW1(config-if-range)#channel-group 1 mode active
SW1(config-if-range)#exit
SW1(config)#interface port-channel 1
SW1(config-if)#switchport mode trunk
SW1(config-if)#switchport trunk allowed vlan 1,2,20
```

- Creates EtherChannel and configures trunk on SW2

```
SW1(config)#interface range FastEthernet0/4 - 5
SW1(config-if-range)#channel-group 1 mode active
SW1(config-if-range)#exit
SW1(config)#interface port-channel 1
SW1(config-if)#switchport mode trunk
SW1(config-if)#switchport trunk allowed vlan 1,2,20
```

- Creates EtherChannel and configures trunk on SW2

Verifying EtherChannel

```
SW1#show interface Port-channel1
Port-channel1 is up, line protocol is up (connected)
  Hardware is EtherChannel, address is 000f.34f9.9182 (bia 000f.34f9.9182)
  MTU 1500 bytes, BW 200000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
<output omitted>
```

- Verifies interface status

Verifying EtherChannel (Cont.)

```
SW2#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

Number of channel-groups in use: 1
Number of aggregators:           1
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------
1      Po1(SU)         LACP      Fa0/1(P)    Fa0/2(P)
```

- Displays a one-line summary per channel group

Verifying EtherChannel (Cont.)

```
Switch#show etherchannel Port-channel
                Channel-group listing:
                ----------------------
Group: 1
----------
                Port-channels in the group:
                ---------------------------
Port-channel: Po1    (Primary Aggregator)
------------
Age of the Port-channel   = 4d:01h:29m:00s
<output omitted>
Protocol            =   LACP
<output omitted>

Ports in the Port-channel:
Index   Load   Port     EC state        No of bits
------+------+------+------------------+-----------
  0     00     Fa0/1    Active             4
  1     00     Fa0/2    Active             4
Time since last port bundled:    0d:00h:00m:18s    Fa0/2
Time since last port Un-bundled: 0d:00h:00m:32s    Fa0/2
```

- Displays port channel information

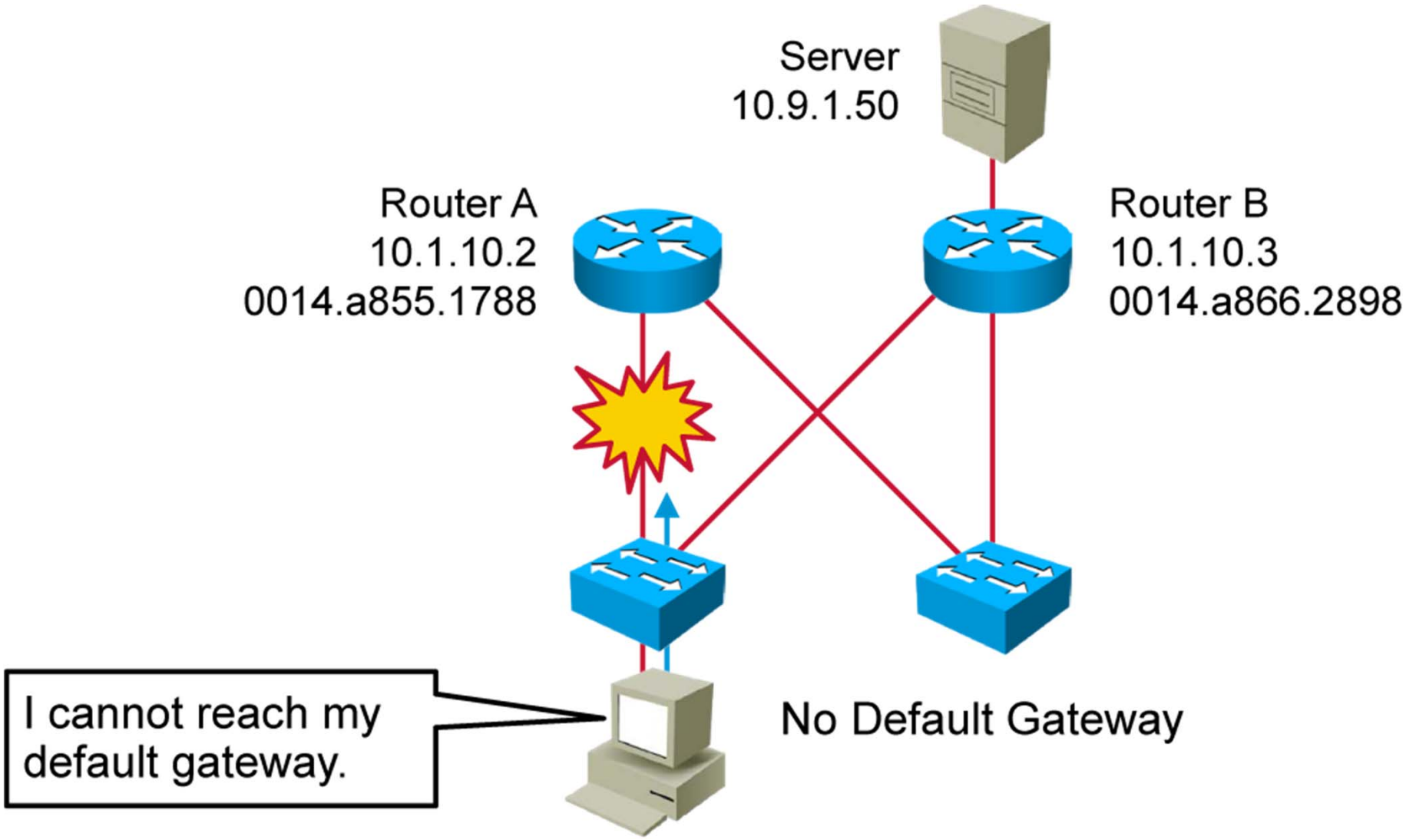
Summary

- EtherChannel is a technology that is used to group several ports into one logical channel.
- PAgP and LACP are two protocols for link aggregation. They allow ports with similar characteristics to form a channel through dynamic negotiation with adjoining switches.
- All interfaces within an EtherChannel must have the same configuration of speed and duplex mode, native and allowed VLANs on trunks, and access VLAN on access ports.
- Use the **show etherchannel summary** command to quickly identify EtherChannel groups on the switch.

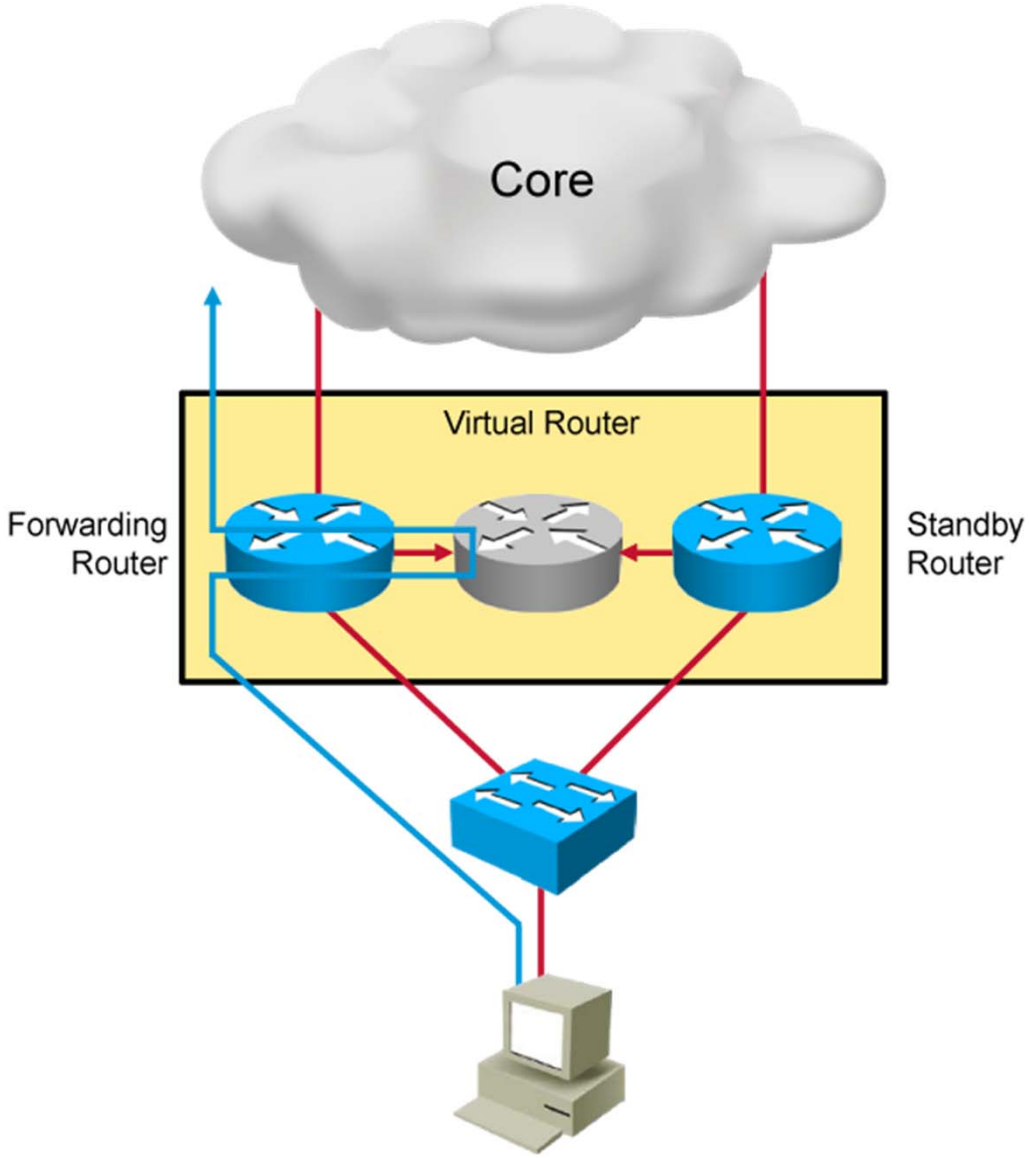
Understanding Layer 3 Redundancy

Implementing Scalable Medium-Sized Networks

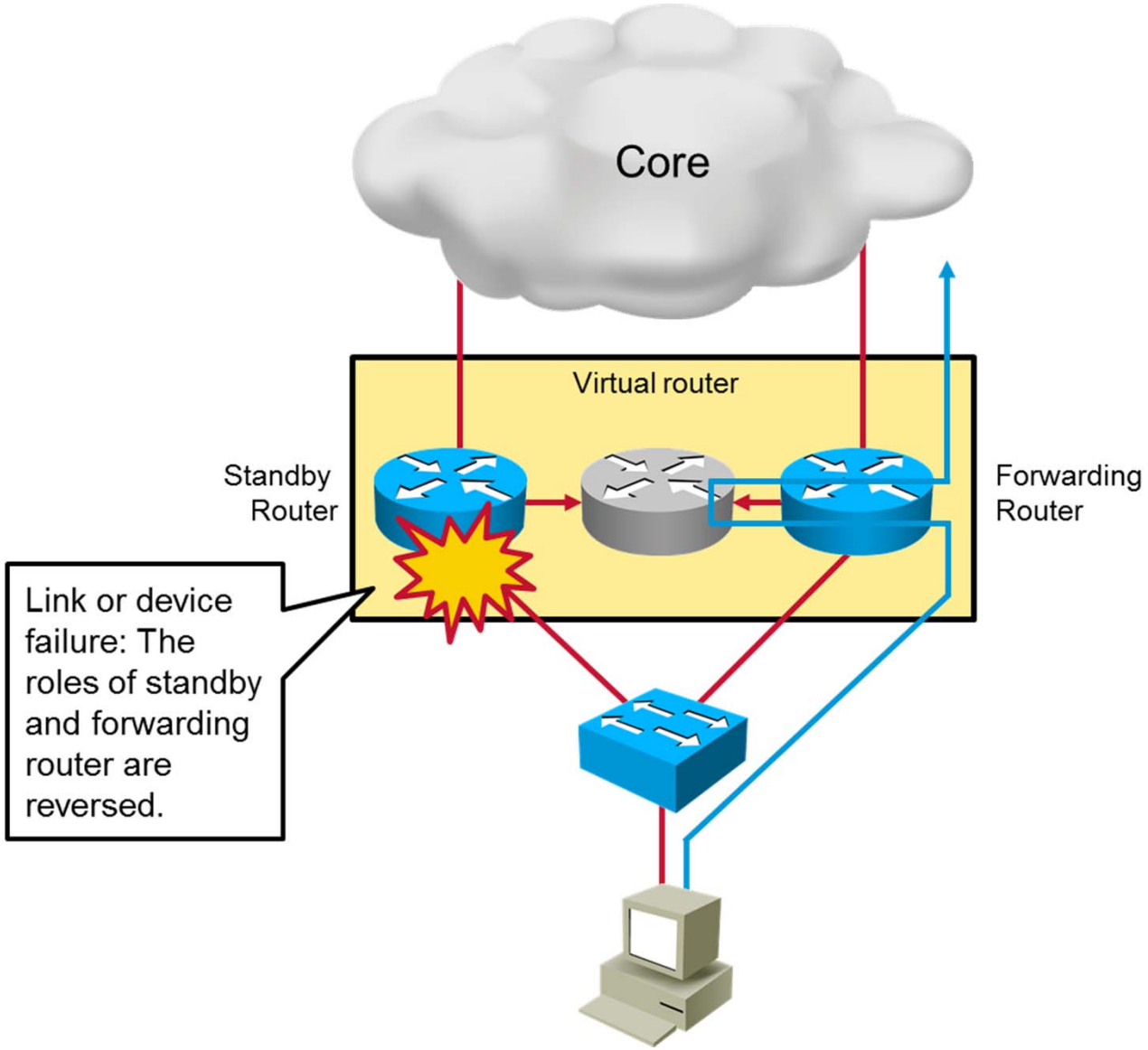
The Need for Default Gateway Redundancy



Default Gateway Redundancy



Default Gateway Redundancy (Cont.)



HSRP

- HSRP defines a group of routers—one active and one standby.
- Virtual IP and MAC addresses are shared between the two routers.
- To verify HSRP state, use the **show standby** command.
- HSRP is Cisco proprietary, and VRRP is a standard protocol.

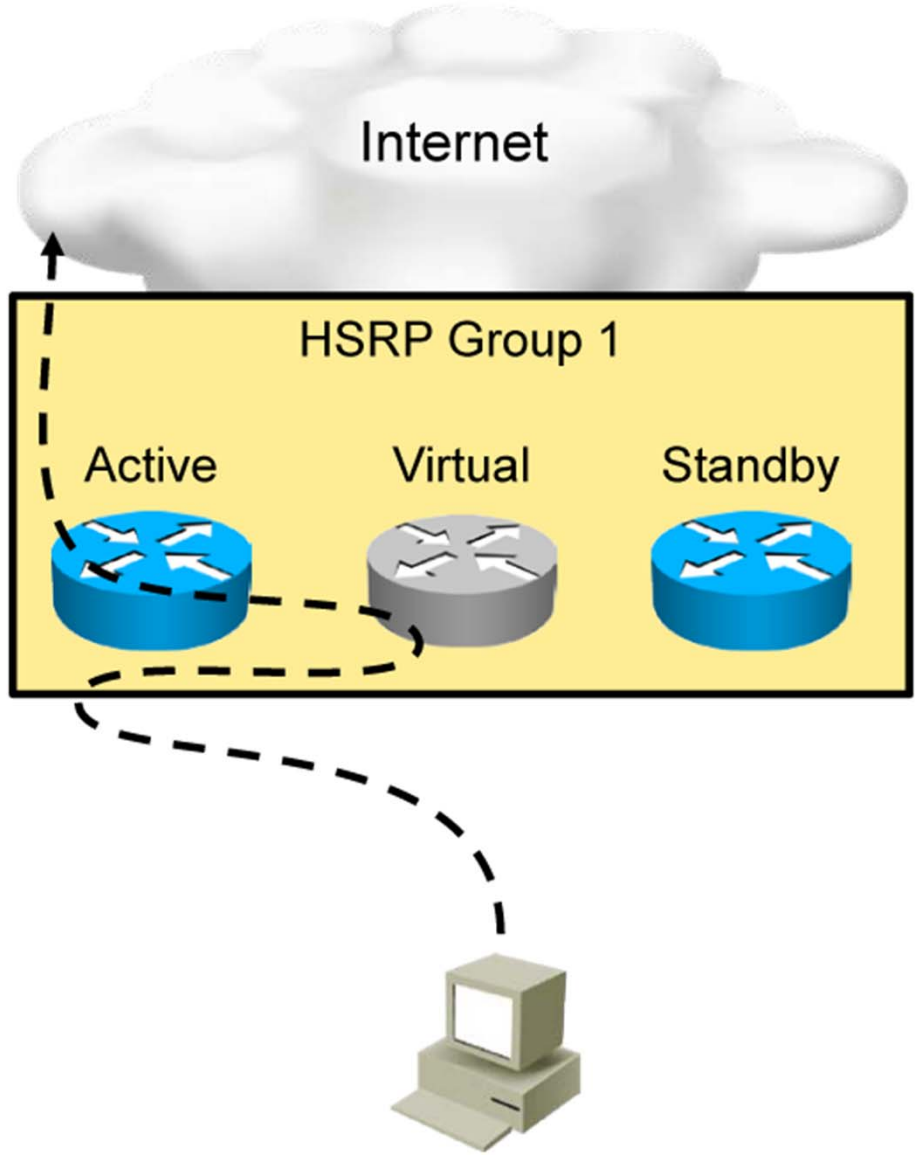
HSRP (Cont.)

```
R1#show standby
Vlan1 - Group 1
  State is Active
    2 state changes, last state change 00:00:10
  Virtual IP address is 10.1.1.100
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.800 secs
  Preemption disabled
  Active router is local
  Standby router is unknown
  Priority 100 (default 100)
  Group name is "hsrp-Vl1-1" (default)
```

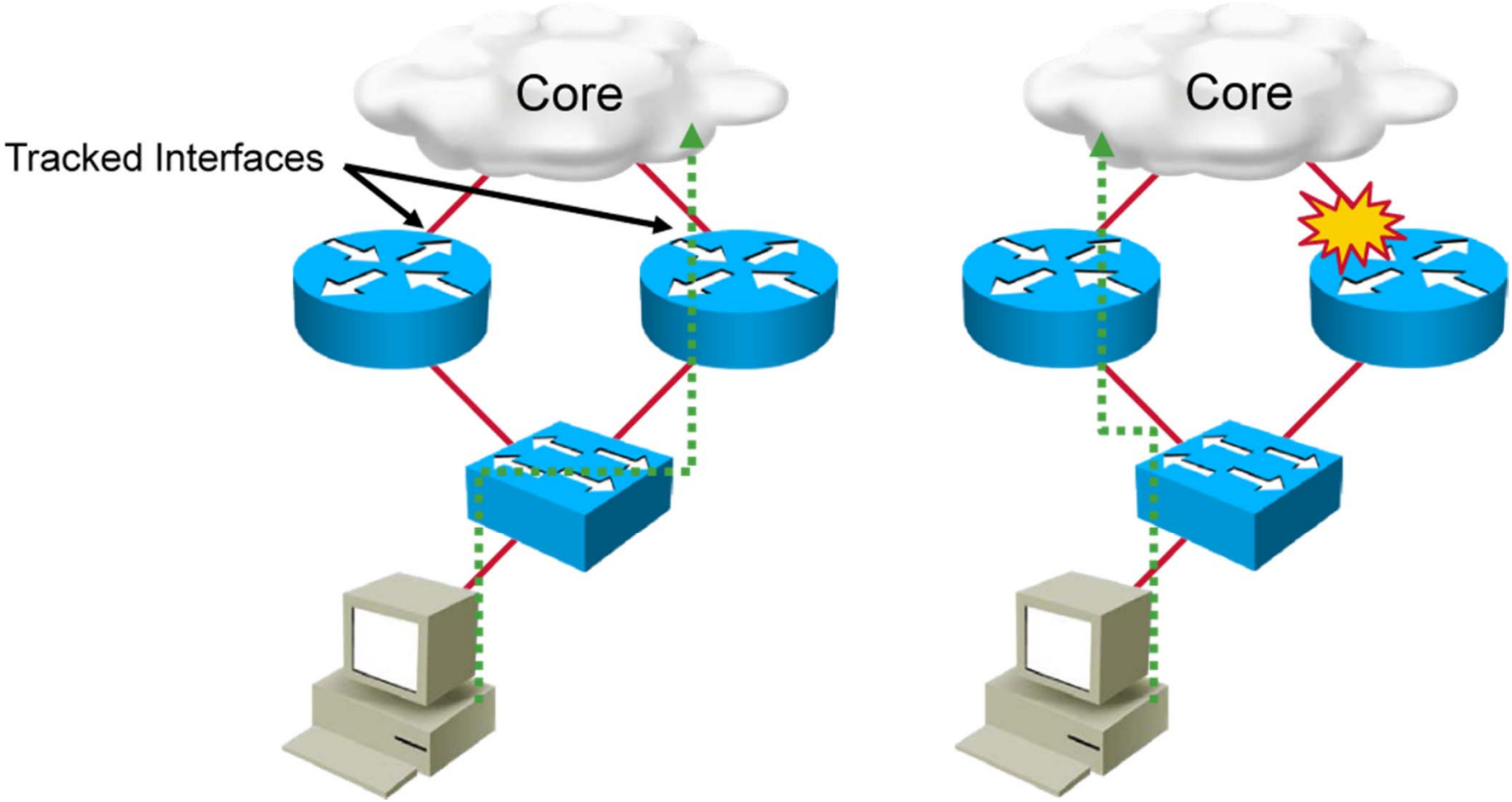
- The **show standby** command verifies the HSRP state.

HSRP (Cont.)

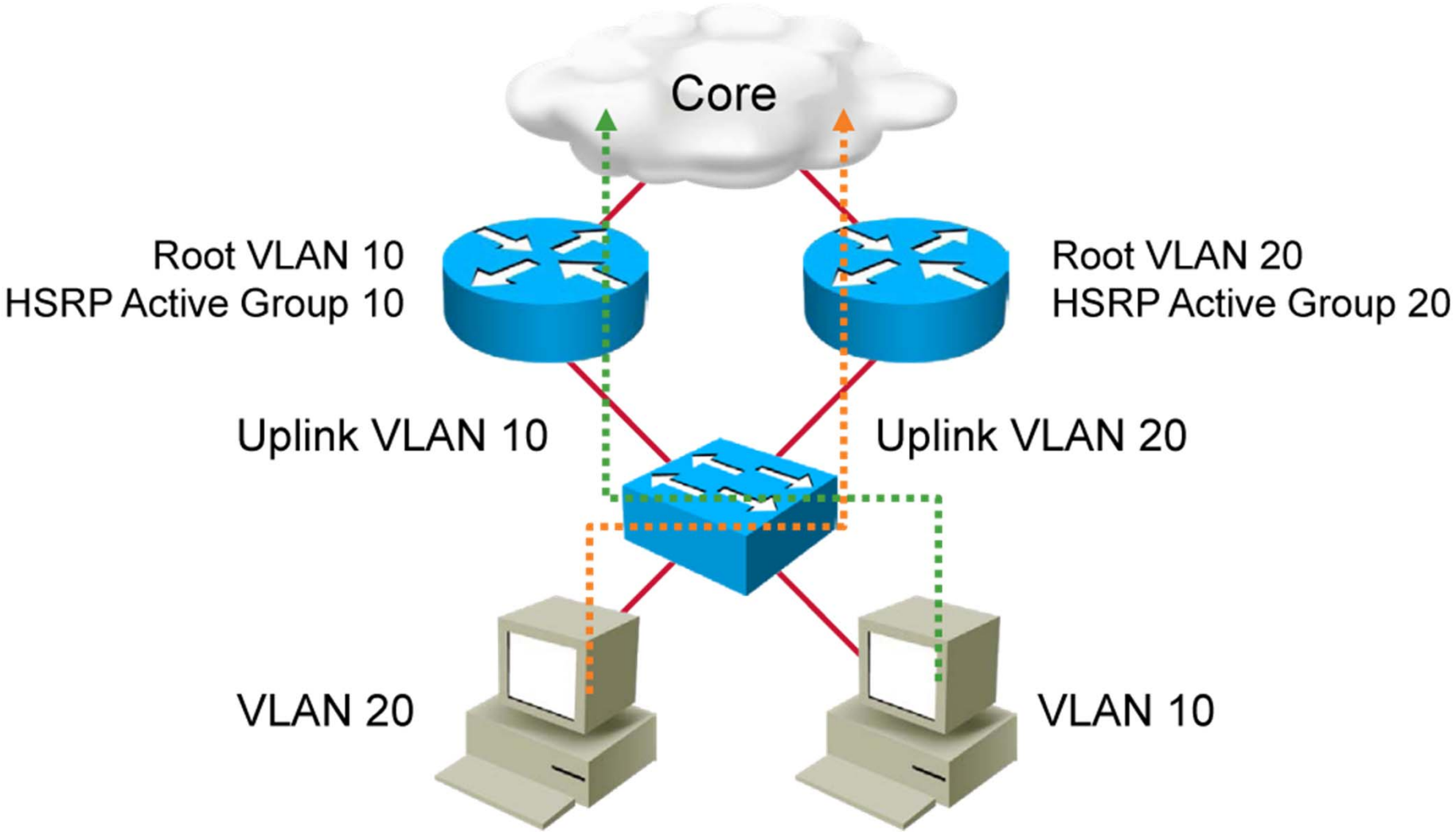
- Active router:
  - Responds to default gateway ARP requests with the virtual router MAC address
  - Assumes active forwarding of packets for the virtual router
  - Sends hello messages
  - Knows the virtual router IP address
- Standby Router:
  - Listens for periodic hello messages
  - Assumes active forwarding of packets if it does not hear from active router



HSRP Interface Tracking

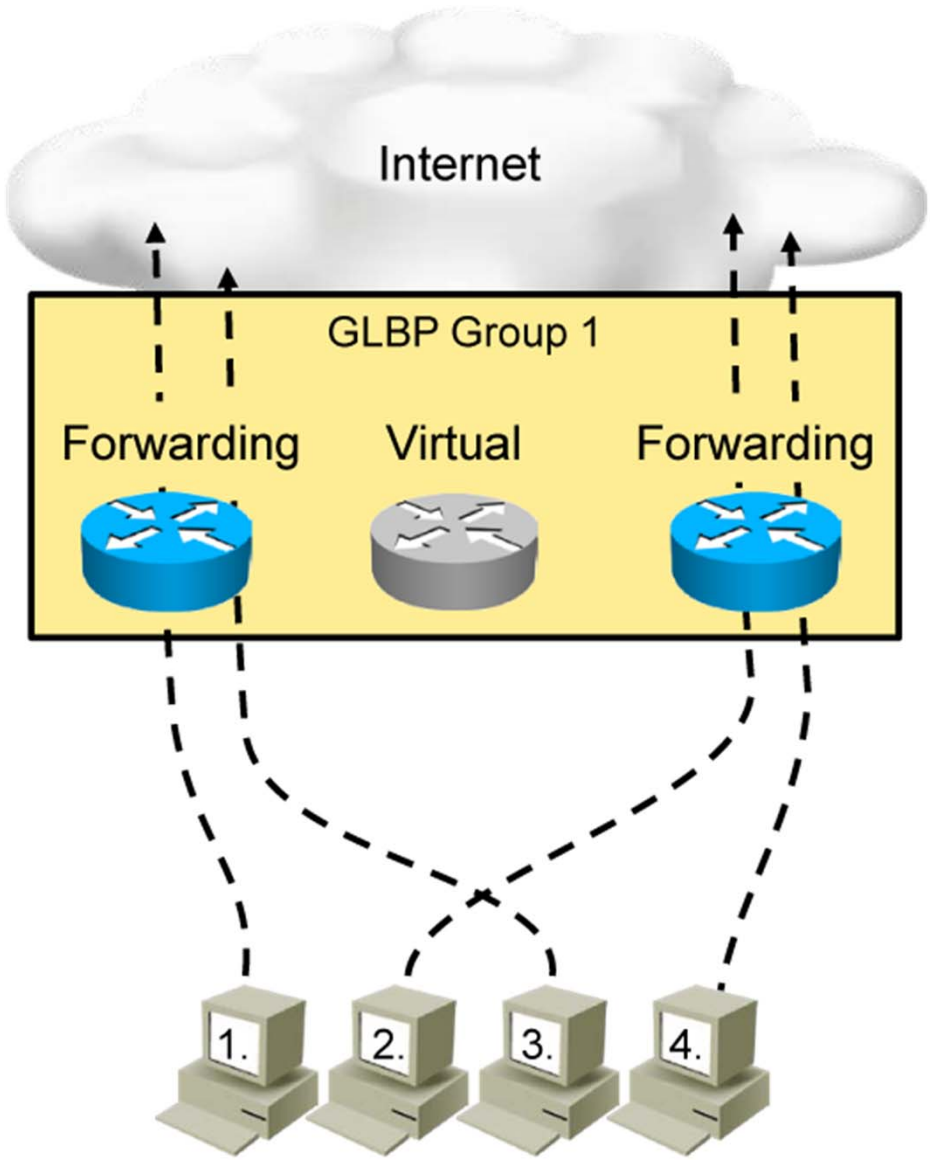


HSRP Load Balancing



Gateway Load Balancing Protocol

- Allows full use of resources on all devices without the administrative burden of creating multiple groups.
- Provides a single virtual IP address and multiple virtual MAC addresses.
- Routes traffic to single gateway distributed across routers.
- Provides automatic rerouting in the event of any failure.



Gateway Load Balancing Protocol (Cont.)

```
R1#show glbp
FastEthernet0/1 - Group 1
  State is Active
    1 state change, last state change 00:02:34
  Virtual IP address is 192.168.2.100
  <output omitted>
  Active is local
  Standby is 192.168.2.2, priority 100 (expires in 8.640 sec)
  Priority 100 (default)
  Weighting 100 (default 100), thresholds: lower 1, upper 100
  Load balancing: round-robin
  Group members:
    001e.7aa3.5e71 (192.168.2.1) local
    001e.7aa3.5f31 (192.168.2.2)
<output omitted>
```

- The **show glbp** command in this example displays information about the status of GLBP group 1.

Gateway Load Balancing Protocol (Cont.)

```
R1#show glbp
<output omitted>
There are 2 forwarders (1 active)
  Forwarder 1
    State is Active
      1 state change, last state change 00:02:23
    MAC address is 0007.b400.0101 (default)
    Owner ID is 001e.7aa3.5e71
    Redirection enabled
    Preemption enabled, min delay 30 sec
    Active is local, weighting 100
  Forwarder 2
    State is Listen
   <output omitted>
```

- The **show glbp** command in this example displays information about the status of GLBP group 1.

Summary

- End devices are typically configured with a single default gateway IP address that does not change when the network topology changes.
- Redundancy protocols provide a mechanism for determining which router should take the active role in forwarding traffic and determining when that role must be taken over by a standby router.
- HSRP defines a standby group of routers, with one router as the active router. VRRP is standard protocol that provides a similar function.
- GLBP is a Cisco proprietary solution to allow automatic selection and simultaneous use of multiple available gateways in addition to automatic failover between those gateways.

Module Summary

- A VLAN is a logical broadcast domain that can span multiple physical LAN segments.
- A loop-avoidance mechanism is required in redundant switch topologies.
- EtherChannel groups several Fast Ethernet or Gigabit Ethernet ports into one logical channel.
- With router redundancy, a set of routers works together to present the illusion of a single virtual router to the hosts on the LAN.