Copyright Information

Disclaimer

The following publication, CCIE R&S Lab Workbook Volume I Version 5.0, is designed to assist candidates in the preparation for Cisco Systems' CCIE Routing & Switching Lab Exam. While every effort has been made to ensure that all material is as complete and accurate as possible, the enclosed material is presented on an "as is" basis. Neither the authors nor Internetwork Expert, Inc. assume any liability or responsibility to any person or entity with respect to loss or damages incurred from the information contained in this workbook.

This workbook was developed by Internetwork Expert, Inc. and is an original work of the aforementioned authors. Any similarities between material presented in this workbook and actual CCIE lab material is completely coincidental.

Table of Contents

Bridging & Switching

> **Note**
>
> Load the *Basic IP Addressing* initial configurations prior to starting.

1.1 Layer 2 Access Switchports

- Using the diagram for reference configure access VLAN assignments on SW1, SW2, SW3, and SW4 to obtain basic connectivity between the devices with Ethernet segments with the exception of R6.
- Do not use VTP to accomplish this.

1.2 Layer 2 Dynamic Switchports

- Configure all inter-switch links on SW2, SW3, and SW4 to be in dynamic auto state.
- Configure all inter-switch links on SW1 to be in dynamic desirable state.
- Using the CAM table verify that all layer 2 traffic between devices in the same VLAN, but not attached to the same switch, is transiting SW1.

1.3 ISL Trunking

- Statically set the trunking encapsulation of SW1's inter-switch links to ISL.
- Verify that SW2, SW3, & SW4 are negotiating ISL as the trunking encapsulation to SW1, and that SW1 is not negotiating ISL to SW2, SW3, and SW4.

1.4 802.1q Trunking

- Change the trunking encapsulation on SW1’s inter-switch links from static ISL to static 802.1q.
- Verify that SW2, SW3, & SW4 are negotiating 802.1q as the trunking encapsulation to SW1, and that SW1 is not negotiating 802.1q to SW2, SW3, and SW4.

1.5 802.1q Native VLAN

- Modify the native VLAN on the 802.1q trunks of SW1 so that traffic between devices in VLAN 146 is not tagged when sent over the trunk links.

1.6 Disabling DTP Negotiation

- Disable Dynamic Trunking Protocol on the trunk links of SW1.
- Verify that trunking is still occurring between SW1 & SW2, SW1 & SW3, and SW1 & SW4 without the use of DTP.

1.7 Router-On-A-Stick

- Configure the link between SW2 and R6 as an 802.1q trunk link.
- Using the subinterfaces listed in the diagram configure R6 to route traffic for both VLANs 67 and 146 on its Ethernet link.
- Verify that R6 has reachability to devices both on VLAN 67 and 146.

> **Note**
>
> Erase and reload SW1, SW2, SW3, & SW4, and load the *Basic IP Addressing* initial configurations before continuing.

1.8 VTP

- Configure all inter-switch links on SW2, SW3, and SW4 to be in dynamic auto state.
- Configure all inter-switch links on SW1 to be in dynamic desirable state.
- Configure SW2 as a VTP server in the domain CCIE.
- Configure SW1, SW3, and SW4 as VTP clients in the domain CCIE.
- Configure necessary VLAN definitions on SW2 using the diagram for reference.
- Configure access VLAN assignments on SW1, SW2, SW3, and SW4 to obtain basic connectivity between the devices with Ethernet segments.
- Configure router-on-a-stick between SW2 and R6 per the diagram so R6 has reachability to devices on VLANs 67 and 146.

1.9 VTP Transparent

- Configure SW1 in VTP transparent mode and remove all previous VLAN definitions on it.
- Configure SW1 with only the VLAN definitions necessary to obtain basic connectivity between the devices with Ethernet segments.

1.10 VTP Pruning

- Configure SW1 in VTP client mode.
- Enable VTP pruning in the layer 2 network so that inter-switch broadcast replication is minimized.
- Verify this configuration is functional through the **`show interface trunk`** output.

1.11 VTP Prune-Eligible List

- Edit the prune-eligible list to ensure that traffic for VLAN 7 is carried on all active trunk links in the layer 2 network.
- Verify this configuration is functional through the **`show interface trunk`** output.

1.12 Layer 2 EtherChannel

- Remove all previous configurations on the links connecting SW1, SW2, SW3, and SW4.
- Configure all inter-switch links on SW2, SW3, and SW4 to be in dynamic auto state.
- Configure all inter-switch links on SW1 to be in dynamic desirable state.
- Configure Layer 2 EtherChannels on all inter-switch links between SW1 & SW2, SW1 & SW3, and SW1 & SW4.
- Use Port-Channel numbers 12, 13, and 14 respectively.
- These links should not use dynamic EtherChannel negotiation.

1.13 Layer 2 EtherChannel with PAgP

- Modify the previous EtherChannel configuration to use PAgP for dynamic negotiation.
- SW1 should initiate negotiation and the other devices should respond.

1.14 Layer 2 EtherChannel with LACP

- Modify the previous EtherChannel configuration to use LACP for dynamic negotiation.
- SW1 should initiate negotiation and the other devices should respond.

1.15 Layer 3 EtherChannel

- Configure links Fa0/16 & Fa0/17 on SW4 and links Fa0/19 & Fa0/20 on SW2 to be bound together as a Layer 3 EtherChannel.
- Use Port-Channel number 24 and the subnet 155.X.108.0/24 per the diagram.
- Ensure IP reachability is obtained between these devices over the segment.

> **Note**
>
> Erase and reload SW1, SW2, SW3, & SW4 before continuing.

1.16 802.1q Tunneling

- Configure 802.1q trunk links between SW1 & SW2's interfaces Fa0/13, SW2's interface Fa0/16 & SW3's interface Fa0/16, and SW3's interface Fa0/19 & SW4's interface Fa0/19.
- Disable all other inter-switch links.
- Configure two Ethernet subinterfaces on R1 with the IP addresses 14.0.0.1/24 and 41.0.0.1/24 using VLANs 14 and 41 respectively.
- Configure two Ethernet subinterfaces on R4's second Ethernet interface1 with the IP addresses 14.0.0.4/24 and 41.0.0.4/24 using VLANs 14 and 41 respectively.
- Using VLAN 100 configure an 802.1q tunnel between SW1 and SW4 to connect R1 and R4.
- R1 and R4 should appear to be directly connected when viewing the **`show cdp neighbor`** output.

1.17 EtherChannel over 802.1q Tunneling

- Remove the previous trunking and tunneling configuration.
- Configure an 802.1q trunk link between SW2 and SW3.
- Configure interfaces Fa0/13, Fa0/14, and Fa0/15 on SW1 as a layer 2 EtherChannel using PAgP for negotiation.
- Configure interfaces Fa0/19, Fa0/20, and Fa0/21 on SW4 as a layer 2 EtherChannel using PAgP for negotiation.
- Disable all other inter-switch links on SW1 and SW4.
- Configure SW2 and SW3 to tunnel the EtherChannel link between SW1 and SW4 using VLANs 100, 200, and 300.
- Tunnel Spanning-Tree Protocol along with CDP over these links so that SW1 and SW4 appear to be directly connected when viewing the **`show cdp neighbor`** output.
- SW1 and SW4 should form an 802.1q trunk link over this EtherChannel.
- To verify this configure SW1 and SW4's links to R1 and R4 in VLAN 146 per the diagram and ensure connectivity between R1 and R4.

> **Note**
>
> Erase and reload SW1, SW2, SW3, & SW4, and load the *Basic IP Addressing* initial configurations before continuing.

1.18 STP Root Bridge Election

- Configure the inter-switch links between SW1 & SW2, SW1 & SW3, SW2 & SW4, and SW3 & SW4 as 802.1q trunk links.
- Disable all other inter-switch links.
- Configure SW4 as a VTP server using the domain name CCIE with SW1, SW2, and SW3 as its clients.
- Configure VLAN assignments per the diagram.
- Configure SW1 as the STP Root Bridge for all active VLANs.
- If SW1 goes down SW4 should take over as the STP Root Bridge for all active VLANs.

1.19 STP Load Balancing with Port Cost

- Using Spanning-Tree cost modify the layer 2 transit network so that traffic for all active VLANs from SW2 to SW1 uses the last link between SW2 and SW4.
- If this link goes down traffic should fall over to the second link between SW2 and SW4.

1.20 STP Load Balancing with Port Priority

- Using Spanning-Tree priority modify the layer 2 transit network so that traffic for all active VLANs from SW4 to SW1 uses the last link between SW3 and SW4.
- If this link goes down traffic should fall over to the second link between SW3 and SW4.

1.21 Tuning STP Convergence Timers

- Configure the switches so that they broadcast Spanning-Tree hello packets every three seconds.
- When a new port becomes active it should wait twenty seconds before transitioning to the forwarding state.
- If the switches do not hear a configuration message within ten seconds they should attempt reconfiguration.
- This configuration should impact all currently active VLANs and any additional VLANs created in the future.

1.22 STP PortFast

- Configure Spanning-Tree PortFast on the switches so that ports connected to the internal and external routers do not have to wait for the Spanning-Tree listening and learning phases to begin forwarding.
- Do not use any global Spanning-Tree commands to accomplish this.

1.23 STP PortFast Default

- Remove the previous PortFast configuration.
- Configure Spanning-Tree PortFast on the switches so that ports connected to the internal and external routers do not have to wait for the Spanning-Tree listening and learning phases to begin forwarding.
- Do not use any interface level Spanning-Tree commands to accomplish this.

1.24 STP UplinkFast

- Configure SW2, SW3, and SW4 with Spanning-Tree UplinkFast such that if their root port is lost they immediately reconverge to an alternate connection to their upstream bridge.
- Verify this by shutting down the root port of SW2.

1.25 STP BackboneFast

- Configure Spanning-Tree BackboneFast such that if the links between SW3 and SW4 go down SW2 immediately expires its maxage timer and begins Spanning-Tree reconvergence.

1.26 STP BPDU Guard

- Configure Spanning-Tree BPDU Guard on the switches so that ports connected to the internal and external routers are disabled if a Spanning-Tree BPDU is detected.
- Once disabled the switches should attempt to re-enable the ports after two minutes.
- Do not use the global **`portfast`** command to accomplish this.

1.27 STP BPDU Guard Default

- Remove the previous BPDU Guard configuration.
- Configure Spanning-Tree PortFast on the switches so that ports connected to the internal and external routers do not have to wait for the Spanning-Tree listening and learning phases to begin forwarding.
- Configure Spanning-Tree BPDU Guard so that if a Spanning-Tree BPDU is detected on any of these ports they are disabled.
- Do not use any interface level Spanning-Tree commands to accomplish this.

1.28 STP BPDU Filter

- Remove the previous BPDU Guard configuration.
- Configure the switches so that ports connected to the internal and external routers do not send Spanning-Tree packets sent out them.
- Do not use any global Spanning-Tree commands to accomplish this.

1.29 STP BPDU Filter Default

- Remove the previous BPDU Filter configuration.
- Configure Spanning-Tree PortFast on the switches so that ports connected to the internal and external routers do not have to wait for the Spanning-Tree listening and learning phases to begin forwarding.
- Configure Spanning-Tree BPDU Filter on the switches so that the PortFast enabled ports are reverted out of PortFast state if a Spanning-Tree packet is received in them.
- Do not use any interface level Spanning-Tree commands to accomplish this.

1.30 STP Root Guard

- Configure SW1 so that the links to either SW2 or SW3 are disabled if either SW2, SW3, or SW4 is elected the Spanning-Tree Root Bridge for any VLAN.

1.31 STP Loop Guard

- Configure Spanning-Tree Loop Guard to prevent unidirectional links from forming on any of the inter-switch links in the layer 2 network.

1.32 Unidirectional Link Detection

- Remove the previous Loop Guard configuration.
- Configure UDLD to prevent unidirectional links from forming on any of the inter-switch links in the layer 2 network.

Note

Erase and reload SW1, SW2, SW3, & SW4, and load the *Basic IP Addressing* initial configurations before continuing.

1.33 MST Root Bridge Election

- Configure the inter-switch links between SW1 & SW2, SW1 & SW3, SW2 & SW4, and SW3 & SW4 as 802.1q trunk links.
- Disable all other inter-switch links.
- Configure SW4 as a VTP server using the domain name CCIE with SW1, SW2, and SW3 as its clients.
- Configure VLAN assignments per the diagram.
- Configure Multiple Spanning-Tree on the switches.
- Instance 1 should service VLANs 1 - 100.
- Instance 2 should service VLANs 101 - 200.
- Instance 3 should service all other VLANs.
- Configure SW1 as the STP Root Bridge for instance 1.
- Configure SW4 as the STP Root Bridge for instance 2.
- If SW1 goes down SW2 should take over as the STP Root Bridge for instance 1.
- If SW4 goes down SW3 should take over as the STP Root Bridge for instance 2.

1.34 MST Load Balancing with Port Cost

- Using Spanning-Tree cost modify the layer 2 transit network so that traffic for MST instance 1 from SW2 to SW1 uses the last link between SW2 and SW4.
- If this link goes down traffic should fall over to the second link between SW2 and SW4.

1.35 MST Load Balancing with Port Priority

- Remove the previous STP cost modifications.
- Set the cost for MST instance 1 on SW3's links to SW1 to be 100,000.
- Using Spanning-Tree priority modify the layer 2 transit network so that traffic for MST instance 1 from SW4 to SW1 uses the last link between SW3 and SW4.
- If this link goes down traffic should fall over to the second link between SW3 and SW4.

1.36 MST and Rapid Spanning Tree

- Configure Rapid Spanning-Tree on the switches so that ports connected to the internal and external routers immediately begin forwarding when enabled.

1.37 Protected Ports

- Create a new SVI for VLAN22 on SW2 and assign it the IP address 192.10.X.8/24, where X is your rack number.
- Configure port protection on SW2 so that R2 and BB2 cannot directly communicate with each other, but can communicate with SW2's VLAN22 interface.

1.38 Storm Control

- Configure SW1 to limit unicast traffic received from R1 to 100 pps.
- Configure SW1 to limit broadcast traffic received from R6 to 10Mbps.
- Configure SW1 to limit broadcast traffic received from R4 to 1Mbps using a relative percentage of the interface bandwidth.

1.39 MAC-Address Table Static Entries & Aging

- Ensure reachability on VLAN 146 between R1, R4, and R6.
- Configure a static CAM entry on SW4 so that frames destined to the MAC address of R4's interface connected to VLAN 146 are dropped; once complete R1 and R6 should have reachability to each other, but not R4.
- Configure static CAM entry for that MAC address of R6's connection to VLAN 146 to ensure that this address is not allowed to roam.

1.40 SPAN

- Configure SW1 so that all traffic transiting VLAN 146 is redirected to a host located on port Fa0/24.
- Configure SW4 so that all traffic coming from and going to R4's connection to VLAN 146 is redirected to a host located on port Fa0/24; Inbound traffic from the Linux host should be placed into VLAN 146.

1.41 RSPAN

- Disable the trunk links between SW1 and SW2.
- Create VLAN 500 as an RSPAN VLAN on all switches in the topology.
- Configure SW2 so that traffic received from and sent to R4's connection to VLAN 43 is redirected to the RSPAN VLAN.
- Configure SW1 to receive traffic from the RSPAN VLAN and redirect it to a host connected to port Fa0/24.
- Inbound traffic on the link connected to this host should be placed in VLAN 146.

1.42 Voice VLAN

- Ports Fa0/2, Fa0/4, and Fa0/6 on SW1 will be connected to Cisco IP phones in the near future.
- Configure port Fa0/2 with an access VLAN assignment of 146 and a voice VLAN assignment of 600.
- Enable Spanning-Tree portfast on this link and ensure that CDP is enabled.
- Configure port Fa0/4 as an 802.1q trunk link.
- Configure SW1 so that only VLANs 146 and 600 are permitted on this switchport, so that STP BPDUs received on the port are filtered out, and so that the interface runs in STP portfast mode.
- Configure VLAN 146 as the native VLAN for this port and so that VLAN 600 is advertised as the voice VLAN via CDP.
- Configure port Fa0/6 with an access VLAN assignment of 146, and for voice VLAN frames to use dot1p tagging.

1.43 IP Phone Trust and CoS Extend

- Enable MLS QoS globally on SW1.
- Configure SW1 to trust the CoS of frames received on the ports connected to the IP phones.
- This trust should only occur if the Cisco IP phone is present and advertises itself via CDP.
- SW1 should enforce a CoS value of 1 to any appliance connected to the second port of the IP phone.

1.44 Smartport Macros

- Configure a macro on SW1 named VLAN_146 that when applied to an interface will set it to be an access switchport, apply VLAN 146 as the access vlan, and filter Spanning-Tree BPDUs.
- Apply this macro to ports Fa0/7 and Fa0/8 on the switch.

> **Note**
>
> Erase and reload all devices to a blank configuration before continuing.

1.45 Flex Links

- Configure links Fa0/16 between SW2 and SW3 as an 802.1q trunk.
- Configure link Fa0/16 on SW1 and Fa0/13 on SW3 as an 802.1q trunk.
- Configure links Fa0/13 & Fa0/14 between SW1 and SW2 as an 802.1q trunked EtherChannel.
- Disable all other inter-switch links.
- Configure R1's Ethernet interface with the IP address 10.0.0.1/24, R2's Ethernet interface with the IP address 10.0.0.2/24, and R3's second Ethernet interface with the IP address 10.0.0.3/24.
- Configure flex links on SW1 so that traffic from R1 to R3 uses the EtherChannel to SW2.
- If the EtherChannel goes down traffic should immediately switch over to use the link between SW1 and SW3.
- If the EtherChannel and all its members comes back up traffic should forward back over this link after 20 seconds.

1.46 Fallback Bridging

- Configure R4's second Ethernet interface with the IP address 104.0.0.4/24, and with the IPv6 address 2001::4/24.
- Configure R6's second Ethernet interface with the IP address 106.0.0.6/24, and with the IPv6 address 2001::6/24.
- Configure interface VLAN104 on SW4 with the IP address 104.0.0.10/24, and configure interface Fa0/4 in VLAN 104.
- Configure interface Fa0/6 on SW4 with the IP address 106.0.0.10/24.
- Enable RIPv2 on all of these links.
- Configure fallback bridging on SW4 to bridge the IPv6 subnet of R4 and R6 together.

Note

Erase and reload all devices to a blank configuration before continuing.

1.47 Private VLANs

- Configure the first Ethernet interfaces of R1, R2, R3, R4, R5, and R6 with IP addresses 100.0.0.Y/24, where Y is the device number.
- Configure the first inter-switch link between SW1 and SW2 as a trunk.
- Configure the primary VLAN 100 to service private VLANs 1000, 2000, and 3000.
- VLANs 1000 and 2000 should be community VLANs, while VLAN 3000 should be an isolated VLAN.
- Assign VLAN 1000 to the links connecting to R2 & R3, VLAN 2000 to the links connecting to R4 & R5, and VLAN 3000 to R6.
- The link connecting to R1 should be a promiscuous port.
- Ensure that R1 can reach all devices, R2 can reach R3, and R4 can reach R5.
- No other connectivity should be allowed within this topology.

Bridging & Switching Solutions

1.1 Layer 2 Access Switchports

- Using the diagram for reference configure access VLAN assignments on SW1, SW2, SW3, and SW4 to obtain basic connectivity between the devices with Ethernet segments with the exception of R6.
- Do not use VTP to accomplish this.

Configuration

```
SW1:
vlan 7,58,67,79,146
!
interface FastEthernet0/1
 switchport access vlan 146
!
interface FastEthernet0/5
 switchport access vlan 58

SW2:
vlan 8,22,43,58
!
interface FastEthernet0/2
 switchport access vlan 22
!
interface FastEthernet0/4
 switchport access vlan 43
!
interface FastEthernet0/24
 switchport access vlan 22

SW3:
vlan 5,9,43,79
!
interface FastEthernet0/5
 switchport access vlan 5
!
interface FastEthernet0/24
 switchport access vlan 43

SW4:
vlan 10,146
!
interface FastEthernet0/4
 switchport access vlan 146
```


Verification

Note

For hosts connected to different physical switches but in the same VLAN, such as R1 and R4, to get IP connectivity to each other Spanning-Tree Protocol must be forwarding end-to-end between the hosts. An STP instance is automatically created on the Catalyst 3550 and 3560 platforms for a VLAN when the VLAN is created, which implies that the switches in the transit path for the VLAN need to know about it in the VLAN database.

In most designs this is accomplished through VTP, but in this design it is accomplished simply by issuing the **vlan** command on all switches that need to know about it. Since trunking is preconfigured between all switches in the initial configurations, end-to-end transport is achieved.

Note that in this solution the VLANs created on the switches are not identical. Instead only the minimum number of necessary VLANs are created. The same connectivity result can be achieved by simply configuring the command **vlan 5,7,8,9,10,22,43,58,67,79,146** on all devices. The functional difference is that SW4 for example, who does not need VLAN 5, does not have an STP instance created for VLAN 5. In many production designs these considerations must be taken into account as all platforms have a maximum limitation of the amount of VLANs and STP instances they can support.

In either case for this example however, the final verification is to ensure that the VLANs are assigned correctly, per the **show interface status** or **show vlan** output, and that end-to-end connectivity exists.

```
Rack1SW1#ping 155.1.79.9

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 155.1.79.9, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/9 ms

Rack1SW1#ping 155.1.37.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 155.1.37.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/9 ms
```



```
Rack1SW2#ping 155.1.58.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 155.1.58.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/8 ms

Rack1R1#ping 155.1.146.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 155.1.146.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms

Rack1R2#ping 192.10.1.254

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.10.1.254, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/8 ms

Rack1R4#ping 204.12.1.254

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 204.12.1.254, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/8 ms

Rack1SW1#show interface status

Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/1                        connected    146        a-full  a-100 10/100BaseTX
Fa0/2                        notconnect   1            auto   auto 10/100BaseTX
Fa0/3                        connected    routed     a-half   a-10 10/100BaseTX
Fa0/4                        notconnect   1            auto   auto 10/100BaseTX
Fa0/5                        connected    58         a-half   a-10 10/100BaseTX
Fa0/6                        notconnect   1            auto   auto 10/100BaseTX
Fa0/7                        notconnect   1            auto   auto 10/100BaseTX
Fa0/8                        notconnect   1            auto   auto 10/100BaseTX
Fa0/9                        notconnect   1            auto   auto 10/100BaseTX
Fa0/10                       notconnect   1            auto   auto 10/100BaseTX
Fa0/11                       notconnect   1            auto   auto 10/100BaseTX
Fa0/12                       notconnect   1            auto   auto 10/100BaseTX
Fa0/13                       connected    trunk      a-full  a-100 10/100BaseTX
Fa0/14                       connected    trunk      a-full  a-100 10/100BaseTX
Fa0/15                       connected    trunk      a-full  a-100 10/100BaseTX
Fa0/16                       connected    trunk      a-full  a-100 10/100BaseTX
Fa0/17                       connected    trunk      a-full  a-100 10/100BaseTX
Fa0/18                       connected    trunk      a-full  a-100 10/100BaseTX
Fa0/19                       connected    trunk      a-full  a-100 10/100BaseTX
Fa0/20                       connected    trunk      a-full  a-100 10/100BaseTX
Fa0/21                       connected    trunk      a-full  a-100 10/100BaseTX
Fa0/22                       notconnect   1            auto   auto 10/100BaseTX
Fa0/23                       notconnect   1            auto   auto 10/100BaseTX
Fa0/24                       notconnect   1            auto   auto 10/100BaseTX
Gi0/1                        notconnect   1            auto   auto Not Present
Gi0/2                        notconnect   1            auto   auto Not Present
```


Rack1SW2#show interface status

```
Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/1                        notconnect   1            auto   auto 10/100BaseTX
Fa0/2                        connected    22         a-full  a-100 10/100BaseTX
Fa0/3                        notconnect   1            auto   auto 10/100BaseTX
Fa0/4                        connected    43         a-half   a-10 10/100BaseTX
Fa0/5                        notconnect   1            auto   auto 10/100BaseTX
Fa0/6                        notconnect   1            auto   auto 10/100BaseTX
Fa0/7                        notconnect   1            auto   auto 10/100BaseTX
Fa0/8                        notconnect   1            auto   auto 10/100BaseTX
Fa0/9                        notconnect   1            auto   auto 10/100BaseTX
Fa0/10                       notconnect   1            auto   auto 10/100BaseTX
Fa0/11                       notconnect   1            auto   auto 10/100BaseTX
Fa0/12                       notconnect   1            auto   auto 10/100BaseTX
Fa0/13                       connected    trunk      a-full  a-100 10/100BaseTX
Fa0/14                       connected    trunk      a-full  a-100 10/100BaseTX
Fa0/15                       connected    trunk      a-full  a-100 10/100BaseTX
Fa0/16                       connected    trunk      a-full  a-100 10/100BaseTX
Fa0/17                       connected    trunk      a-full  a-100 10/100BaseTX
Fa0/18                       connected    trunk      a-full  a-100 10/100BaseTX
Fa0/19                       connected    trunk      a-full  a-100 10/100BaseTX
Fa0/20                       connected    trunk      a-full  a-100 10/100BaseTX
Fa0/21                       connected    trunk      a-full  a-100 10/100BaseTX
Fa0/22                       notconnect   1            auto   auto 10/100BaseTX
Fa0/23                       notconnect   1            auto   auto 10/100BaseTX
Fa0/24                       connected    22         a-half   a-10 10/100BaseTX
Gi0/1                        notconnect   1            auto   auto Not Present
Gi0/2                        notconnect   1            auto   auto Not Present
```

Rack1SW3#show interface status

```
Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/1                        notconnect   1            auto   auto 10/100BaseTX
Fa0/2                        notconnect   1            auto   auto 10/100BaseTX
Fa0/3                        connected    1          a-half   a-10 10/100BaseTX
Fa0/4                        notconnect   1            auto   auto 10/100BaseTX
Fa0/5                        connected    5          a-half   a-10 10/100BaseTX
Fa0/6                        notconnect   1            auto   auto 10/100BaseTX
Fa0/7                        notconnect   1            auto   auto 10/100BaseTX
Fa0/8                        notconnect   1            auto   auto 10/100BaseTX
Fa0/9                        notconnect   1            auto   auto 10/100BaseTX
Fa0/10                       notconnect   1            auto   auto 10/100BaseTX
Fa0/11                       notconnect   1            auto   auto 10/100BaseTX
Fa0/12                       notconnect   1            auto   auto 10/100BaseTX
Fa0/13                       connected    trunk      a-full  a-100 10/100BaseTX
Fa0/14                       connected    trunk      a-full  a-100 10/100BaseTX
Fa0/15                       connected    trunk      a-full  a-100 10/100BaseTX
Fa0/16                       connected    trunk      a-full  a-100 10/100BaseTX
Fa0/17                       connected    trunk      a-full  a-100 10/100BaseTX
Fa0/18                       connected    trunk      a-full  a-100 10/100BaseTX
Fa0/19                       connected    trunk      a-full  a-100 10/100BaseTX
Fa0/20                       connected    trunk      a-full  a-100 10/100BaseTX
Fa0/21                       connected    trunk      a-full  a-100 10/100BaseTX
Fa0/22                       notconnect   1            auto   auto 10/100BaseTX
Fa0/23                       notconnect   1            auto   auto 10/100BaseTX
Fa0/24                       connected    43         a-half   a-10 10/100BaseTX
Gi0/1                        notconnect   1            auto   auto Not Present
Gi0/2                        notconnect   1            auto   auto Not Present
```


SW4#show interface status

Port	Name	Status	Vlan	Duplex	Speed	Type
Fa0/1		notconnect	1	auto	auto	10/100BaseTX
Fa0/2		notconnect	1	auto	auto	10/100BaseTX
Fa0/3		notconnect	1	auto	auto	10/100BaseTX
Fa0/4		connected	146	a-half	a-10	10/100BaseTX
Fa0/5		notconnect	1	auto	auto	10/100BaseTX
Fa0/6		notconnect	1	auto	auto	10/100BaseTX
Fa0/7		notconnect	1	auto	auto	10/100BaseTX
Fa0/8		notconnect	1	auto	auto	10/100BaseTX
Fa0/9		notconnect	1	auto	auto	10/100BaseTX
Fa0/10		notconnect	1	auto	auto	10/100BaseTX
Fa0/11		notconnect	1	auto	auto	10/100BaseTX
Fa0/12		notconnect	1	auto	auto	10/100BaseTX
Fa0/13		connected	trunk	a-full	a-100	10/100BaseTX
Fa0/14		connected	trunk	a-full	a-100	10/100BaseTX
Fa0/15		connected	trunk	a-full	a-100	10/100BaseTX
Fa0/16		connected	trunk	a-full	a-100	10/100BaseTX
Fa0/17		connected	trunk	a-full	a-100	10/100BaseTX
Fa0/18		connected	trunk	a-full	a-100	10/100BaseTX
Fa0/19		connected	trunk	a-full	a-100	10/100BaseTX
Fa0/20		connected	trunk	a-full	a-100	10/100BaseTX
Fa0/21		connected	trunk	a-full	a-100	10/100BaseTX
Fa0/22		notconnect	1	auto	auto	10/100BaseTX
Fa0/23		notconnect	1	auto	auto	10/100BaseTX
Fa0/24		notconnect	1	auto	auto	10/100BaseTX
Gi0/1		notconnect	1	auto	auto	unknown
Gi0/2		notconnect	1	auto	auto	unknown

1.2 Layer 2 Dynamic Switchports

- Configure all inter-switch links on SW2, SW3, and SW4 to be in dynamic auto state.
- Configure all inter-switch links on SW1 to be in dynamic desirable state.
- Using the CAM table verify that all layer 2 traffic between devices in the same VLAN, but not attached to the same switch, is transiting SW1.

Configuration

```
SW1:
interface range FastEthernet0/13 - 21
 switchport mode dynamic desirable

SW2:
interface range FastEthernet0/13 - 21
 switchport mode dynamic auto

SW3:
interface range FastEthernet0/13 - 21
 switchport mode dynamic auto

SW4:
interface range FastEthernet0/13 - 21
 switchport mode dynamic auto
```

Verification

> **Note**
>
> This verification is performed after R6's router-on-a-stick configuration is completed.

```
Rack1R4#ping 155.1.146.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 155.1.146.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

Rack1R4#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  155.1.146.4            -   0011.2031.4461  ARPA   FastEthernet0/1
Internet  155.1.146.6            0   000f.24da.2220  ARPA   FastEthernet0/1
```


With SW1's inter-switch links in dynamic desirable state, and all other switches inter-switch links in dynamic auto state, trunks will only be formed from SW1 to SW2, SW1 to SW3, and SW1 to SW4. This is because SW1 initiates trunking negotiation through DTP (desirable), and SW2, SW3, and SW4 only respond to DTP negotiation requests (auto). The result of this is indirectly verified by correlating the MAC addresses of R4 and R6 to the CAM table.

R4's port Fa0/1 is connected to SW4's port Fa0/4.

```
Rack1SW4#show mac-address-table dynamic address 0011.2031.4461
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 146    0011.2031.4461    DYNAMIC     Fa0/4
Total Mac Addresses for this criterion: 1
```

R6's port Fa0/0 is connected to SW2's port Fa0/6.

```
Rack1SW2#show mac-address-table dynamic address 000f.24da.2220
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    000f.24da.2220    DYNAMIC     Fa0/6
 146    000f.24da.2220    DYNAMIC     Fa0/6
Total Mac Addresses for this criterion: 2
```


If SW2 and SW4 were trunking directly, traffic would forward between their connected ports for VLAN 146. Instead SW2 sees R4's MAC address reachable via port Fa0/13 to SW1, and SW4 sees R6's MAC address reachable via port Fa0/13 to SW1. The CAM table, which is built from the result of STP forwarding and blocking, is the final layer 2 verification of how traffic is actually forwarded through the switched network.

```
Rack1SW2#show mac-address-table dynamic address 0011.2031.4461
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 146    0011.2031.4461    DYNAMIC     Fa0/13
Total Mac Addresses for this criterion: 1

Rack1SW4#show mac-address-table dynamic address 000f.24da.2220
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 146    000f.24da.2220    DYNAMIC     Fa0/13
Total Mac Addresses for this criterion: 1
```


1.3 ISL Trunking

- Statically set the trunking encapsulation of SW1's inter-switch links to ISL.
- Verify that SW2, SW3, & SW4 are negotiating ISL as the trunking encapsulation to SW1, and that SW1 is not negotiating ISL to SW2, SW3, and SW4.

Configuration

```
SW1:
interface range FastEthernet0/13 - 21
 switchport trunk encapsulation isl
```

Verification

> **Note**
>
> SW1's inter-switch links are running in DTP desirable mode (initiating trunking) with ISL encapsulation statically set. These can be seen under the *Mode* and *Encapsulation* columns from the **`show interface trunk`** output.

```
Rack1SW1#show interface trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa0/13      desirable    isl            trunking      1
Fa0/14      desirable    isl            trunking      1
Fa0/15      desirable    isl            trunking      1
Fa0/16      desirable    isl            trunking      1
Fa0/17      desirable    isl            trunking      1
Fa0/18      desirable    isl            trunking      1
Fa0/19      desirable    isl            trunking      1
Fa0/20      desirable    isl            trunking      1
Fa0/21      desirable    isl            trunking      1

<output omitted>
```


SW2, SW3, and SW4's inter-switch links are in DTP auto mode, which means they will accept negotiation in from the other side but not initiate it. Since SW1 is statically set to ISL encapsulation, SW2, SW3, and SW4 must agree to this or DTP negotiation will fail. Successful negotiation can be seen in this output since the encapsulation is *n-isl*, for *negotiated* ISL.

```
Rack1SW2#show interface trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa0/13      auto         n-isl          trunking      1
Fa0/14      auto         n-isl          trunking      1
Fa0/15      auto         n-isl          trunking      1

<output omitted>

Rack1SW3#show interface trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa0/13      auto         n-isl          trunking      1
Fa0/14      auto         n-isl          trunking      1
Fa0/15      auto         n-isl          trunking      1

<output omitted>

Rack1SW4#show interface trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa0/13      auto         n-isl          trunking      1
Fa0/14      auto         n-isl          trunking      1
Fa0/15      auto         n-isl          trunking      1

<output omitted>
```


1.4 802.1q Trunking

- Change the trunking encapsulation on SW1's inter-switch links from static ISL to static 802.1q.
- Verify that SW2, SW3, & SW4 are negotiating 802.1q as the trunking encapsulation to SW1, and that SW1 is not negotiating 802.1q to SW2, SW3, and SW4.

Configuration

```
SW1:
interface range FastEthernet0/13 - 21
 switchport trunk encapsulation dot1q
```

Verification

> **Note**
>
> Similar to the previous case, SW1 is running in DTP desirable mode, but now has its trunking encapsulation statically set to 802.1q.

```
Rack1SW1#show interface trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa0/13      desirable    802.1q         trunking      1
Fa0/14      desirable    802.1q         trunking      1
Fa0/15      desirable    802.1q         trunking      1
Fa0/16      desirable    802.1q         trunking      1
Fa0/17      desirable    802.1q         trunking      1
Fa0/18      desirable    802.1q         trunking      1
Fa0/19      desirable    802.1q         trunking      1
Fa0/20      desirable    802.1q         trunking      1
Fa0/21      desirable    802.1q         trunking      1
<output omitted>
```


SW2, SW3, and SW4 must now agree to using dot1q trunking, as seen in the *n-802.1q* output, for *negotiated* dot1q.

```
Rack1SW2#show interface trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa0/13      auto         n-802.1q       trunking      1
Fa0/14      auto         n-802.1q       trunking      1
Fa0/15      auto         n-802.1q       trunking      1
<output omitted>

Rack1SW3#show interface trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa0/13      auto         n-802.1q       trunking      1
Fa0/14      auto         n-802.1q       trunking      1
Fa0/15      auto         n-802.1q       trunking      1
<output omitted>

Rack1SW4#show interface trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa0/13      auto         n-802.1q       trunking      1
Fa0/14      auto         n-802.1q       trunking      1
Fa0/15      auto         n-802.1q       trunking      1
<output omitted>
```


1.5 802.1q Native VLAN

- Modify the native VLAN on the 802.1q trunks of SW1 so that traffic between devices in VLAN 146 is not tagged when sent over the trunk links.

Configuration

```
SW1:
interface range FastEthernet0/13 - 21
 switchport trunk native vlan 146

SW2:
interface range FastEthernet0/13 - 15
 switchport trunk native vlan 146

SW3:
interface range FastEthernet0/13 - 15
 switchport trunk native vlan 146

SW4:
interface range FastEthernet0/13 - 15
 switchport trunk native vlan 146
```

Verification

Note

The IEEE 802.1q trunking encapsulation standard defines the term *native* VLAN to describe traffic sent and received on an interface running 802.1q encapsulation that does not have an 802.1q tag actually inserted. When the switch sends a frame that belongs to the native VLAN, it is sent the same as if 802.1q was not configured. When the switch receives a frame on an interface running 802.1q that does not have a tag, it assumes it is part of the native VLAN. For this reason the switches on both ends of an 802.1q trunk link must agree on what the native VLAN is, otherwise traffic can unexpectedly leak between broadcast domain boundaries.

The native VLAN defaults to 1 unless modified. In this case the native VLAN is modified to 146 on both ends of the link.


```
Rack1SW1#show interface trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa0/13      desirable    802.1q         trunking      146
Fa0/14      desirable    802.1q         trunking      146
Fa0/15      desirable    802.1q         trunking      146
Fa0/16      desirable    802.1q         trunking      146
Fa0/17      desirable    802.1q         trunking      146
Fa0/18      desirable    802.1q         trunking      146
Fa0/19      desirable    802.1q         trunking      146
Fa0/20      desirable    802.1q         trunking      146
Fa0/21      desirable    802.1q         trunking      146

<output omitted>

Rack1SW2#show interface trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa0/13      auto         n-802.1q       trunking      146
Fa0/14      auto         n-802.1q       trunking      146
Fa0/15      auto         n-802.1q       trunking      146

<output omitted>

Rack1SW3#show interface trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa0/13      auto         n-802.1q       trunking      146
Fa0/14      auto         n-802.1q       trunking      146
Fa0/15      auto         n-802.1q       trunking      146

<output omitted>

Rack1SW4#show interface trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa0/13      auto         n-802.1q       trunking      146
Fa0/14      auto         n-802.1q       trunking      146
Fa0/15      auto         n-802.1q       trunking      146

<output omitted>
```


1.6 Disabling DTP Negotiation

- Disable Dynamic Trunking Protocol on the trunk links of SW1.
- Verify that trunking is still occurring between SW1 & SW2, SW1 & SW3, and SW1 & SW4 without the use of DTP.

Configuration

```
SW1:
interface range FastEthernet0/13 - 21
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport nonegotiate

SW2:
interface range FastEthernet0/13 - 15
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport nonegotiate

SW3:
interface range FastEthernet0/13 - 15
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport nonegotiate

SW4:
interface range FastEthernet0/13 - 15
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport nonegotiate
```


Verification

Note

DTP negotiation can be disabled two ways, with the **switchport mode access** command, or with the **switchport nonegotiate** command. If trunking is needed, but DTP is disabled, it must be statically configured with the **switchport mode trunk** command. This design is most commonly used when a switch is trunking to a device that does not support DTP, such as an IOS router's routed Ethernet interface (not an EtherSwitch interface), or a server's NIC card.

```
Rack1SW1#show interface fa0/13 switchport | include Negotiation
Negotiation of Trunking: Off

Rack1SW1#show interface trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa0/13      on           802.1q         trunking      146
Fa0/14      on           802.1q         trunking      146
Fa0/15      on           802.1q         trunking      146
Fa0/16      on           802.1q         trunking      146
Fa0/17      on           802.1q         trunking      146
Fa0/18      on           802.1q         trunking      146
Fa0/19      on           802.1q         trunking      146
Fa0/20      on           802.1q         trunking      146
Fa0/21      on           802.1q         trunking      146

<output omitted>
```



```
Rack1SW2#show interface trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa0/13      on           802.1q         trunking      146
Fa0/14      on           802.1q         trunking      146
Fa0/15      on           802.1q         trunking      146

<output omitted>

Rack1SW3#show interface trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa0/13      on           802.1q         trunking      146
Fa0/14      on           802.1q         trunking      146
Fa0/15      on           802.1q         trunking      146

<output omitted>

Rack1SW4#show interface trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa0/13      on           802.1q         trunking      146
Fa0/14      on           802.1q         trunking      146
Fa0/15      on           802.1q         trunking      146

<output omitted>
```


1.7 Router-On-A-Stick

- Configure the link between SW2 and R6 as an 802.1q trunk link.
- Using the subinterfaces listed in the diagram configure R6 to route traffic for both VLANs 67 and 146 on its Ethernet link.
- Verify that R6 has reachability to devices both on VLAN 67 and 146.

Configuration

```
SW2:
vlan 67,146
!
interface FastEthernet0/6
 switchport trunk encapsulation dot1q
 switchport mode trunk

R6:
interface FastEthernet0/0.67
 encapsulation dot1q 67
 ip address 155.1.67.6 255.255.255.0
!
interface FastEthernet0/0.146
 encapsulation dot1q 146
 ip address 155.1.146.6 255.255.255.0
```

Verification

Note

Router-on-a-stick is the legacy implementation of inter-VLAN routing, which is typically replaced in most designs now with layer 3 Switch Virtual Interfaces (SVIs) on layer 3 switches. In router-on-a-stick a layer 2 switch trunks multiple VLANs to a router, the router accepts a layer 2 packet in the physical interface, categorizes it based on the VLAN tag, rebuilds the layer 2 frame, and sends the packet back to the switch.

Note that since the router does not support DTP negotiation on its routed Ethernet interface, the attached switch must issue the **`switchport mode trunk`** command. The **`switchport nonegotiate`** command, while recommended, is not required on the switch. Also to minimize the amount of broadcast traffic that the router receives the switch should ideally edit the allowed list of the trunk going to the router to only allow the VLANs that the router is encapsulating. This is generally necessary since the router does not support VTP pruning on its routed trunk interface.


```
Rack1R6#ping 155.1.67.7

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 155.1.67.7, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/5 ms

Rack1R6#ping 155.1.146.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 155.1.146.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

Rack1SW2#show interface fa0/6 trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa0/6       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/6       1-4094

Port        Vlans allowed and active in management domain
Fa0/6       1-6,8,22,26,43,58,67,100,146

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/6       1-6,8,22,26,43,58,67,100,146
```


1.8 VTP

- Configure all inter-switch links on SW2, SW3, and SW4 to be in dynamic auto state.
- Configure all inter-switch links on SW1 to be in dynamic desirable state.
- Configure SW2 as a VTP server in the domain CCIE.
- Configure SW1, SW3, and SW4 as VTP clients in the domain CCIE.
- Configure necessary VLAN definitions on SW4 using the diagram for reference.
- Configure access VLAN assignments on SW1, SW2, SW3, and SW4 to obtain basic connectivity between the devices with Ethernet segments.
- Configure router-on-a-stick between SW2 and R6 per the diagram so R6 has reachability to devices on VLANs 67 and 146.

Configuration

```
R6:
interface FastEthernet0/0.67
 encapsulation dot1q 67
 ip address 155.1.67.6 255.255.255.0
!
interface FastEthernet0/0.146
 encapsulation dot1q 146
 ip address 155.1.146.6 255.255.255.0

SW1:
vtp domain CCIE
vtp mode client
!
interface range FastEthernet0/13 - 21
 switchport mode dynamic desirable
!
interface FastEthernet0/1
 switchport access vlan 146
!
interface FastEthernet0/5
 switchport access vlan 58

SW2:
vtp domain CCIE
vlan 5,7,8,9,10,22,43,58,67,79,146
!
interface FastEthernet0/2
 switchport access vlan 22
!
interface FastEthernet0/4
 switchport access vlan 43
!
interface FastEthernet0/6
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
```



```
interface FastEthernet0/24
 switchport access vlan 22
!
interface range FastEthernet0/13 - 21
 switchport mode dynamic auto

SW3:
vtp domain CCIE
vtp mode client
!
interface FastEthernet0/5
 switchport access vlan 5
!
interface FastEthernet0/24
 switchport access vlan 43
!
interface range FastEthernet0/13 - 21
 switchport mode dynamic auto

SW4:
vtp domain CCIE
vtp mode client
!
interface FastEthernet0/4
 switchport access vlan 146
!
interface range FastEthernet0/13 - 21
 switchport mode dynamic auto
```


Verification

Note

VLAN Trunking Protocol (VTP) can be used in the Ethernet domain to simplify the creation and management of VLANs, however it does not dictate the traffic flow of VLANs or the actual assignments. The first step in running VTP is to ensure that the switches are trunking with each other. Next, the VTP domain name is configured, and all other switches without domain names configured inherit this. Lastly on the VTP server the VLAN definitions are created.

To verify this configuration compare the output of the **`show vtp status`** command on all devices in the domain. If the domain name, the number of existing VLANs, and the Configuration Revision Number all match, the domain is converged. If authentication is configured the MD5 digest field should be compared as well.

```
Rack1SW1#show vtp status
VTP Version                     : 2
Configuration Revision          : 1
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 16
VTP Operating Mode              : Client
VTP Domain Name                 : CCIE
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x7C 0x80 0x15 0x50 0xA2 0x06 0x41
0x6A
Configuration last modified by 150.1.10.10 at 5-20-08 07:55:18

Rack1SW2#show vtp status
VTP Version                     : 2
Configuration Revision          : 1
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 16
VTP Operating Mode              : Server
VTP Domain Name                 : CCIE
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x7C 0x80 0x15 0x50 0xA2 0x06 0x41
0x6A
Configuration last modified by 150.1.10.10 at 5-20-08 07:55:18
```



```
Rack1SW3#show vtp status
VTP Version                     : 2
Configuration Revision          : 1
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 16
VTP Operating Mode              : Client
VTP Domain Name                 : CCIE
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x7C 0x80 0x15 0x50 0xA2 0x06 0x41
0x6A
Configuration last modified by 150.1.10.10 at 5-20-08 07:55:18

Rack1SW4#show vtp status
VTP Version                     : 2
Configuration Revision          : 1
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 16
VTP Operating Mode              : Client
VTP Domain Name                 : CCIE
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x7C 0x80 0x15 0x50 0xA2 0x06 0x41
0x6A
Configuration last modified by 150.1.10.10 at 5-20-08 07:55:18
Local updater ID is 155.1.10.10 on interface Vl10 (lowest numbered VLAN
interface found)
```


show vlan or **show vlan brief** can also be compared to ensure that the VLAN numbers and names properly propagated throughout the VTP domain.

```
Rack1SW1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/4, Fa0/6, Fa0/7
                                                Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                Fa0/12, Fa0/22, Fa0/23, Fa0/24
                                                Gi0/1, Gi0/2
5    VLAN0005                         active
7    VLAN0007                         active
8    VLAN0008                         active
9    VLAN0009                         active
10   VLAN0010                         active
22   VLAN0022                         active
43   VLAN0043                         active
58   VLAN0058                         active    Fa0/5
67   VLAN0067                         active
79   VLAN0079                         active
146  VLAN0146                         active    Fa0/1
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

Rack1SW2#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/3, Fa0/5, Fa0/7
                                                Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                Fa0/12, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Gi0/1, Gi0/2
5    VLAN0005                         active
7    VLAN0007                         active
8    VLAN0008                         active
9    VLAN0009                         active
10   VLAN0010                         active
22   VLAN0022                         active    Fa0/2, Fa0/24
43   VLAN0043                         active    Fa0/4
58   VLAN0058                         active
67   VLAN0067                         active
79   VLAN0079                         active
146  VLAN0146                         active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```



```
Rack1SW3#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Gi0/1
                                                Gi0/2
5    VLAN0005                         active    Fa0/5
7    VLAN0007                         active
8    VLAN0008                         active
9    VLAN0009                         active
10   VLAN0010                         active
22   VLAN0022                         active
43   VLAN0043                         active    Fa0/24
58   VLAN0058                         active
67   VLAN0067                         active
79   VLAN0079                         active
146  VLAN0146                         active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

Rack1SW4#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gi0/1, Gi0/2
5    VLAN0005                         active
7    VLAN0007                         active
8    VLAN0008                         active
9    VLAN0009                         active
10   VLAN0010                         active
22   VLAN0022                         active
43   VLAN0043                         active
58   VLAN0058                         active
67   VLAN0067                         active
79   VLAN0079                         active
146  VLAN0146                         active    Fa0/4
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```


1.9 VTP Transparent

- Configure SW1 in VTP transparent mode and remove all previous VLAN definitions on it.
- Configure SW1 with only the VLAN definitions necessary to obtain basic connectivity between the devices with Ethernet segments.

Configuration

```
SW1:
vtp mode transparent
no vlan 2-1000
vlan 7,43,58,67,79,146
```

Verification

> **Note**
>
> VTP devices running in transparent mode do not install VTP updates received, but will continue to forward them on unmodified if the domain name matches its locally configured domain. The configuration revision number of zero indicates that it is not participating in the update sequence of the rest of the domain.

```
Rack1SW1#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 11
VTP Operating Mode              : Transparent
VTP Domain Name                 : CCIE
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x4D 0xD1 0x7E 0x5F 0xE4 0x00 0xB6 0x86
Configuration last modified by 155.1.37.7 at 5-20-08 07:55:18
```


Since VTP does not directly relate to STP forwarding, traffic from the server/client or from an entirely different VTP domain can be in the same broadcast domain as the transparent switches ports as long as STP is forwarding end to end. In this particular case SW1 does not have VLANs 7, 43, 67, or 79 locally assigned, but it is in the physical layer 2 transit path for these. This implies that these VLANs must be created, otherwise traffic will be received inbound but not forwarded outbound as there will be no STP instance associated with the VLAN.

```
Rack1SW1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/4, Fa0/6, Fa0/7
                                                Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                Fa0/12, Fa0/22, Fa0/23, Fa0/24
                                                Gi0/1, Gi0/2
7    VLAN0007                         active
43   VLAN0043                         active
58   VLAN0058                         active    Fa0/5
67   VLAN0067                         active
79   VLAN0079                         active
146  VLAN0146                         active    Fa0/1
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Changes in the rest of the VTP domain, such as VLAN adds or removes, do not affect the transparent switches.

```
Rack1SW2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Rack1SW2(config)#vlan 123
Rack1SW2(config-vlan)#end
Rack1SW2#

Rack1SW2#show vlan | include ^123
123  VLAN0123                         active
123  enet  100123     1500  -      -      -        -    -        0      0

Rack1SW3#show vlan | include ^123
123  VLAN0123                         active
123  enet  100123     1500  -      -      -        -    -        0      0

Rack1SW1#show vlan | include ^123
```

1.10 VTP Pruning

- Configure SW1 in VTP client mode.
- Enable VTP pruning in the layer 2 network so that inter-switch broadcast replication is minimized.
- Verify this configuration is functional through the **`show interface trunk`** output.

Configuration

```
SW2:
vtp pruning
```

Verification

> **Note**
>
> VTP pruning eliminates the need to statically remove VLANs from the allowed trunking list of a port by having the switches automatically communicate to each other which VLANs they have locally assigned or are in the transit path for.
>
> The **`show interface pruning`** command indicates what traffic the local switch told its neighbor that it needs, via the *VLAN traffic requested of neighbor* field. These VLANs are either ones locally assigned or those that the local switch is in the layer 2 transit path for. The *Vlans pruned for lack of request by neighbor* field indicates the VLANs that the upstream neighbor did *not* request.
>
> In the below output this means that SW1 is not forwarding VLAN 7 to SW3, because SW3 did not request it. This output can be confusing because what SW1 sees as pruned for lack of request is the opposite of what SW3 sees as requested.

```
Rack1SW1#show interface fa0/16 pruning

Port        Vlans pruned for lack of request by neighbor
Fa0/16      7-8,10,22,58,67,146

Port        Vlan traffic requested of neighbor
Fa0/16      1,5,7-10,22,43,58,67,79,146

Rack1SW3#show interface fa0/13 pruning

Port        Vlans pruned for lack of request by neighbor
Fa0/13      none

Port        Vlan traffic requested of neighbor
Fa0/13      1,5,9,43,79
```


If the network is converged all devices in the VTP domain should agree that pruning is enabled, as seen in the below **show vtp status** output. Note that transparent switches cannot participate in pruning because they do not read the payload of the VTP updates they are receiving from their adjacent neighbors.

```
Rack1SW1#show vtp status
VTP Version                     : 2
Configuration Revision          : 6
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 16
VTP Operating Mode              : Client
VTP Domain Name                 : CCIE
VTP Pruning Mode                : Enabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x4F 0x03 0x83 0x1F 0x24 0xE1 0x01
0x45
Configuration last modified by 155.1.8.8 at 5-20-08 08:27:49

Rack1SW2#show vtp status
VTP Version                     : 2
Configuration Revision          : 6
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 16
VTP Operating Mode              : Server
VTP Domain Name                 : CCIE
VTP Pruning Mode                : Enabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x4F 0x03 0x83 0x1F 0x24 0xE1 0x01
0x45
Configuration last modified by 155.1.8.8 at 5-20-08 08:27:49
Local updater ID is 155.1.8.8 on interface Vl8 (lowest numbered VLAN
interface found)

Rack1SW3#show vtp status
VTP Version                     : 2
Configuration Revision          : 6
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 16
VTP Operating Mode              : Client
VTP Domain Name                 : CCIE
VTP Pruning Mode                : Enabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x4F 0x03 0x83 0x1F 0x24 0xE1 0x01
0x45
Configuration last modified by 155.1.8.8 at 5-20-08 08:27:49
```



```
Rack1SW4#show vtp status
VTP Version                     : 2
Configuration Revision          : 6
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 16
VTP Operating Mode              : Server
VTP Domain Name                 : CCIE
VTP Pruning Mode                : Enabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x4F 0x03 0x83 0x1F 0x24 0xE1 0x01
0x45
Configuration last modified by 155.1.8.8 at 5-20-08 08:27:49
Local updater ID is 155.1.10.10 on interface Vl10 (lowest numbered VLAN
interface found)
```

To quickly view what traffic is not being pruned, and hence actually forwarded, issue the show interface trunk command. The final field of Vlans in spanning tree forwarding state and not pruned means that the VLAN is created, is allowed on the link, is running STP, and is not pruned.

```
Rack1SW1#show interface trunk | begin pruned
Port        Vlans in spanning tree forwarding state and not pruned
Fa0/13      1,5,7-10,22,43,58,67,79,146
Fa0/14      1
Fa0/15      1
Fa0/16      1,5,9,43,79
Fa0/17      none
Fa0/18      none
Fa0/19      10,146
Fa0/20      none
Fa0/21      none

Rack1SW2#show interface trunk | begin pruned
Port        Vlans in spanning tree forwarding state and not pruned
Fa0/6       1,5,7-10,22,43,58,67,79,146
Fa0/13      5,7,9-10,43,58,67,79,146
Fa0/14      none
Fa0/15      none

Rack1SW3#show interface trunk | begin pruned
Port        Vlans in spanning tree forwarding state and not pruned
Fa0/13      1,5,7-10,22,43,58,67,79,146
Fa0/14      1
Fa0/15      1

Rack1SW4#show interface trunk | begin pruned
Port        Vlans in spanning tree forwarding state and not pruned
Fa0/13      1,5,7-10,22,43,58,67,79,146
Fa0/14      1
Fa0/15      1
```


1.11 VTP Prune-Eligible List

- Edit the prune-eligible list to ensure that traffic for VLAN 7 is carried on all active trunk links in the layer 2 network.
- Verify this configuration is functional through the **`show interface trunk`** output.

Configuration

```
SW1:
interface FastEthernet0/13
 switchport trunk pruning vlan 2-6,8-1001
!
interface FastEthernet0/14
 switchport trunk pruning vlan 2-6,8-1001
!
interface FastEthernet0/15
 switchport trunk pruning vlan 2-6,8-1001
!
interface FastEthernet0/16
 switchport trunk pruning vlan 2-6,8-1001
!
interface FastEthernet0/17
 switchport trunk pruning vlan 2-6,8-1001
!
interface FastEthernet0/18
 switchport trunk pruning vlan 2-6,8-1001
!
interface FastEthernet0/19
 switchport trunk pruning vlan 2-6,8-1001
!
interface FastEthernet0/20
 switchport trunk pruning vlan 2-6,8-1001
!
interface FastEthernet0/21
 switchport trunk pruning vlan 2-6,8-1001

SW2:
interface FastEthernet0/13
 switchport trunk pruning vlan 2-6,8-1001
!
interface FastEthernet0/14
 switchport trunk pruning vlan 2-6,8-1001
!
interface FastEthernet0/15
 switchport trunk pruning vlan 2-6,8-1001
```



```
SW3:
interface FastEthernet0/13
 switchport trunk pruning vlan 2-6,8-1001
!
interface FastEthernet0/14
 switchport trunk pruning vlan 2-6,8-1001
!
interface FastEthernet0/15
 switchport trunk pruning vlan 2-6,8-1001

SW4:
interface FastEthernet0/13
 switchport trunk pruning vlan 2-6,8-1001
!
interface FastEthernet0/14
 switchport trunk pruning vlan 2-6,8-1001
!
interface FastEthernet0/15
 switchport trunk pruning vlan 2-6,8-1001
```


Verification

> **Note**
>
> The implementation of the prune eligible list, which is controlled by the **`switchport trunk pruning vlan`** command, is commonly confusing because it is essentially the *opposite* of the editing the allowed list of the trunk. By default all VLANs 2-1001 (not the default or extended VLANs) can be pruned off of a trunk link.
>
> This means that if the switch does not have VLAN 7 assigned, and is not in the transit path for VLAN 7, it can tell its adjacent switches not to send it VLAN 7 traffic. However, if VLAN 7 is removed from the prune eligible list, the switch must report that it *does* need VLAN 7, and the traffic cannot be pruned.
>
> This can be seen in the change of the output below, where SW1 sends VLAN 7 traffic over all links that are forwarding for STP, even though the devices on the other end of the link don't actually need VLAN 7.

```
Rack1SW1#show interface trunk | begin pruned
Port        Vlans in spanning tree forwarding state and not pruned
Fa0/13      1,5,7-10,22,43,58,67,79,146
Fa0/14      1,7
Fa0/15      1,7
Fa0/16      1,5,7,9,43,79
Fa0/17      none
Fa0/18      none
Fa0/19      7,10,146
Fa0/20      7
Fa0/21      7

Rack1SW2#show interface trunk | begin pruned
Port        Vlans in spanning tree forwarding state and not pruned
Fa0/6       1,5,7-10,22,43,58,67,79,146
Fa0/13      5,7,9-10,43,58,67,79,146
Fa0/14      none
Fa0/15      none

Rack1SW3#show interface trunk | begin pruned
Port        Vlans in spanning tree forwarding state and not pruned
Fa0/13      1,5,7-10,22,43,58,67,79,146
Fa0/14      1,7
Fa0/15      1,7

Rack1SW4#show interface trunk | begin pruned
Port        Vlans in spanning tree forwarding state and not pruned
Fa0/13      1,5,7-10,22,43,58,67,79,146
Fa0/14      1
Fa0/15      1
```


1.12 Layer 2 EtherChannel

- Remove all previous configurations on the links connecting SW1, SW2, SW3, and SW4.
- Configure all inter-switch links on SW2, SW3, and SW4 to be in dynamic auto state.
- Configure all inter-switch links on SW1 to be in dynamic desirable state.
- Configure Layer 2 EtherChannels on all inter-switch links between SW1 & SW2, SW1 & SW3, and SW1 & SW4.
- Use Port-Channel numbers 12, 13, and 14 respectively.
- These links should not use dynamic EtherChannel negotiation.

Configuration

```
SW1:
interface FastEthernet0/13
 switchport mode dynamic desirable
 channel-group 12 mode on
!
interface FastEthernet0/14
 switchport mode dynamic desirable
 channel-group 12 mode on
!
interface FastEthernet0/15
 switchport mode dynamic desirable
 channel-group 12 mode on
!
interface FastEthernet0/16
 switchport mode dynamic desirable
 channel-group 13 mode on
!
interface FastEthernet0/17
 switchport mode dynamic desirable
 channel-group 13 mode on
!
interface FastEthernet0/18
 switchport mode dynamic desirable
 channel-group 13 mode on
!
interface FastEthernet0/19
 switchport mode dynamic desirable
 channel-group 14 mode on
!
interface FastEthernet0/20
 switchport mode dynamic desirable
 channel-group 14 mode on
!
interface FastEthernet0/21
 switchport mode dynamic desirable
 channel-group 14 mode on
```



```
SW2:
interface FastEthernet0/13
 channel-group 12 mode on
!
interface FastEthernet0/14
 channel-group 12 mode on
!
interface FastEthernet0/15
 channel-group 12 mode on

SW3:
interface FastEthernet0/13
 channel-group 13 mode on
!
interface FastEthernet0/14
 channel-group 13 mode on
!
interface FastEthernet0/15
 channel-group 13 mode on

SW4:
interface FastEthernet0/13
 channel-group 14 mode on
!
interface FastEthernet0/14
 channel-group 14 mode on
!
interface FastEthernet0/15
 channel-group 14 mode on
```


Verification

Note

For an EtherChannel to form all member interfaces must agree on the same configuration, and both ends of the channel must agree on the same negotiation protocol. In the below **show etherchannel summary** output the *Protocol* field is null, which means that no negotiation was used. This comes from the *on* mode of the **channel-group** command. This output also shows that the *Port-channel* is in the (SU) state, which means layer 2 switchport that is up, and the members *Ports* are in the (P) state, which is in the port-channel.

```
Rack1SW1#show etherchannel summary
Flags:  D - down        P - 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
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 3
Number of aggregators:           3

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------
12     Po12(SU)         -        Fa0/13(P)   Fa0/14(P)   Fa0/15(P)
13     Po13(SU)         -        Fa0/16(P)   Fa0/17(P)   Fa0/18(P)
14     Po14(SU)         -        Fa0/19(P)   Fa0/20(P)   Fa0/21(P)
```


Since SW1's member interfaces were dynamic desirable switchports, the Port-Channel interfaces that are spawned from them inherit these attributes. This means that the channel interfaces on SW1 will initiate negotiation, and the other channels on SW2, SW3, and SW4 should respond.

```
Rack1SW1#show interface trunk

Port        Mode         Encapsulation  Status        Native vlan
Po12        desirable    n-isl          trunking      1
Po13        desirable    n-isl          trunking      1
Po14        desirable    n-isl          trunking      1

Port        Vlans allowed on trunk
Po12        1-4094
Po13        1-4094
Po14        1-4094

Port        Vlans allowed and active in management domain
Po12        1,5,7-10,22,43,58,67,79,146
Po13        1,5,7-10,22,43,58,67,79,146
Po14        1,5,7-10,22,43,58,67,79,146

Port        Vlans in spanning tree forwarding state and not pruned
Po12        1,5,7-10,22,43,58,67,79,146
Po13        1,5,9,43,79
Po14        1,10,146
```


An additional way to verify that a layer 2 channel is working correctly is to view the spanning-tree topology. If STP sees the single port-channel interface running one instance of STP, channeling has occurred properly. This is due to the fact that without channeling some member interfaces would be in the STP forwarding state, and some blocking, but with channeling they are all forwarding.

```
Rack1SW1#show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    32778
             Address     000c.3045.4180
             Cost        9
             Port        168 (Port-channel13)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     001b.d490.7c00
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Po12             Desg FWD 9         128.160  P2p
Po13             Root FWD 9         128.168  P2p
Po14             Desg FWD 9         128.176  P2p

Rack1SW2#show etherchannel summary
Flags:  D - down        P - 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
        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
------+-------------+-----------+-----------------------------------
12     Po12(SU)         -        Fa0/13(P)   Fa0/14(P)   Fa0/15(P)
```



```
Rack1SW2#show interface trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa0/6       on           802.1q         trunking      1
Po12        auto         n-isl          trunking      1

Port        Vlans allowed on trunk
Fa0/6       1-4094
Po12        1-4094

Port        Vlans allowed and active in management domain
Fa0/6       1,5,7-10,22,43,58,67,79,146
Po12        1,5,7-10,22,43,58,67,79,146

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/6       1,5,7-10,22,43,58,67,79,146
Po12        1,5,7,9-10,43,58,67,79,146

Rack1SW2#show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    32778
             Address     000c.3045.4180
             Cost        18
             Port        160 (Port-channel12)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     001b.d4df.ec80
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/6            Desg FWD 19        128.8    P2p
Po12             Root FWD 9         128.160  P2p
```



```
Rack1SW3#show etherchannel summary
Flags:  D - down        P - 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
        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
------+-------------+-----------+-----------------------------------
13     Po13(SU)         -        Fa0/13(P)   Fa0/14(P)   Fa0/15(P)

Rack1SW3#show interface trunk

Port        Mode         Encapsulation  Status        Native vlan
Po13        auto         n-isl          trunking      1

Port        Vlans allowed on trunk
Po13        1-4094

Port        Vlans allowed and active in management domain
Po13        1,5,7-10,22,43,58,67,79,146

Port        Vlans in spanning tree forwarding state and not pruned
Po13        1,5,7-10,22,43,58,67,79,146

Rack1SW3#show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    32778
             Address     000c.3045.4180
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     000c.3045.4180
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Po13             Desg FWD 9         128.66   P2p
```



```
Rack1SW4#show etherchannel summary
Flags:  D - down        P - 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
        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
------+-------------+-----------+-----------------------------------
14     Po14(SU)         -        Fa0/13(P)   Fa0/14(P)   Fa0/15(P)

Rack1SW4#show interface trunk

Port        Mode         Encapsulation  Status        Native vlan
Po14        auto         n-isl          trunking      1

Port        Vlans allowed on trunk
Po14        1-4094

Port        Vlans allowed and active in management domain
Po14        1,5,7-10,22,43,58,67,79,146

Port        Vlans in spanning tree forwarding state and not pruned
Po14        1,5,7-10,22,43,58,67,79,146

Rack1SW4#show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    32778
             Address     000c.3045.4180
             Cost        18
             Port        65 (Port-channel14)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     000c.3045.d600
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Po14             Root FWD 9         128.65   P2p
```


1.13 Layer 2 EtherChannel with PAgP

- Modify the previous EtherChannel configuration to use PAgP for dynamic negotiation.
- SW1 should initiate negotiation and the other devices should respond.

Configuration

```
SW1:
interface FastEthernet0/13
 switchport mode dynamic desirable
 channel-group 12 mode desirable
!
interface FastEthernet0/14
 switchport mode dynamic desirable
 channel-group 12 mode desirable
!
interface FastEthernet0/15
 switchport mode dynamic desirable
 channel-group 12 mode desirable
!
interface FastEthernet0/16
 switchport mode dynamic desirable
 channel-group 13 mode desirable
!
interface FastEthernet0/17
 switchport mode dynamic desirable
 channel-group 13 mode desirable
!
interface FastEthernet0/18
 switchport mode dynamic desirable
 channel-group 13 mode desirable
!
interface FastEthernet0/19
 switchport mode dynamic desirable
 channel-group 14 mode desirable
!
interface FastEthernet0/20
 switchport mode dynamic desirable
 channel-group 14 mode desirable
!
interface FastEthernet0/21
 switchport mode dynamic desirable
 channel-group 14 mode desirable

SW2:
interface FastEthernet0/13
 channel-group 12 mode auto
!
interface FastEthernet0/14
 channel-group 12 mode auto
!
interface FastEthernet0/15
 channel-group 12 mode auto
```



```
SW3:
interface FastEthernet0/13
 channel-group 13 mode auto
!
interface FastEthernet0/14
 channel-group 13 mode auto
!
interface FastEthernet0/15
 channel-group 13 mode auto

SW4:
interface FastEthernet0/13
 channel-group 14 mode auto
!
interface FastEthernet0/14
 channel-group 14 mode auto
!
interface FastEthernet0/15
 channel-group 14 mode auto
```

Verification

> **Note**
>
> Port Aggregation Protocol (PAgP) is a Cisco proprietary negotiation protocol for EtherChannel links. The desirable mode of PAgP, like DTP, is used to initiate negotiation, while the auto mode is used to listen for negotiation. This implies that one side running desirable with the other side running desirable or auto will result in a channel, but both sides running auto will not.

```
Rack1SW1#show etherchannel summary
Flags:  D - down        P - 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
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 3
Number of aggregators:           3

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------
12     Po12(SU)        PAgP      Fa0/13(P)   Fa0/14(P)   Fa0/15(P)
13     Po13(SU)        PAgP      Fa0/16(P)   Fa0/17(P)   Fa0/18(P)
14     Po14(SU)        PAgP      Fa0/19(P)   Fa0/20(P)   Fa0/21(P)
```



```
Rack1SW1#show interface trunk

Port        Mode         Encapsulation  Status        Native vlan
Po12        desirable    n-isl          trunking      1
Po13        desirable    n-isl          trunking      1
Po14        desirable    n-isl          trunking      1

Port        Vlans allowed on trunk
Po12        1-4094
Po13        1-4094
Po14        1-4094

Port        Vlans allowed and active in management domain
Po12        1,5,7-10,22,43,58,67,79,146
Po13        1,5,7-10,22,43,58,67,79,146
Po14        1,5,7-10,22,43,58,67,79,146

Port        Vlans in spanning tree forwarding state and not pruned
Po12        1,5,7-10,22,43,58,67,79,146
Po13        1,5,9,43,79
Po14        1,10,146

Rack1SW1#show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    32778
             Address     000c.3045.4180
             Cost        9
             Port        168 (Port-channel13)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     001b.d490.7c00
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Po12             Desg FWD 9         128.160  P2p
Po13             Root FWD 9         128.168  P2p
Po14             Desg FWD 9         128.176  P2p
```



```
Rack1SW2#show etherchannel summary
Flags:  D - down        P - 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
        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
------+-------------+-----------+-----------------------------------
12     Po12(SU)        PAgP      Fa0/13(P)   Fa0/14(P)   Fa0/15(P)

Rack1SW2#show interface trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa0/6       on           802.1q         trunking      1
Po12        auto         n-isl          trunking      1

Port        Vlans allowed on trunk
Fa0/6       1-4094
Po12        1-4094

Port        Vlans allowed and active in management domain
Fa0/6       1,5,7-10,22,43,58,67,79,146
Po12        1,5,7-10,22,43,58,67,79,146

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/6       1,5,7-10,22,43,58,67,79,146
Po12        1,5,7,9-10,43,58,67,79,146


Rack1SW2#show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    32778
             Address     000c.3045.4180
             Cost        18
             Port        160 (Port-channel12)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     001b.d4df.ec80
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/6            Desg FWD 19        128.8    P2p
Po12             Root FWD 9         128.160  P2p
```



```
Rack1SW3#show etherchannel summary
Flags:  D - down        P - 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
        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
------+-------------+-----------+-----------------------------------
13     Po13(SU)        PAgP      Fa0/13(P)   Fa0/14(P)   Fa0/15(P)

Rack1SW3#show interface trunk

Port        Mode         Encapsulation  Status        Native vlan
Po13        desirable    n-isl          trunking      1

Port        Vlans allowed on trunk
Po13        1-4094

Port        Vlans allowed and active in management domain
Po13        1,5,7-10,22,43,58,67,79,146

Port        Vlans in spanning tree forwarding state and not pruned
Po13        1,5,7-10,22,43,58,67,79,146

Rack1SW3#show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    32778
             Address     000c.3045.4180
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     000c.3045.4180
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Po13             Desg FWD 9         128.66   P2p
```



```
Rack1SW4#show etherchannel summary
Flags:  D - down        P - 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
        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
------+-------------+-----------+-----------------------------------
14     Po14(SU)        PAgP      Fa0/13(P)   Fa0/14(P)   Fa0/15(P)

Rack1SW4#show interface trunk

Port        Mode         Encapsulation  Status        Native vlan
Po14        desirable    n-isl          trunking      1

Port        Vlans allowed on trunk
Po14        1-4094

Port        Vlans allowed and active in management domain
Po14        1,5,7-10,22,43,58,67,79,146

Port        Vlans in spanning tree forwarding state and not pruned
Po14        1,5,7-10,22,43,58,67,79,146

Rack1SW4#show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    32778
             Address     000c.3045.4180
             Cost        18
             Port        65 (Port-channel14)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     000c.3045.d600
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Po14             Root FWD 9         128.65   P2p
```


1.14 Layer 2 EtherChannel with LACP

- Modify the previous EtherChannel configuration to use LACP for dynamic negotiation.
- SW1 should initiate negotiation and the other devices should respond.

Configuration

```
SW1:
interface FastEthernet0/13
 switchport mode dynamic desirable
 channel-group 12 mode active
!
interface FastEthernet0/14
 switchport mode dynamic desirable
 channel-group 12 mode active
!
interface FastEthernet0/15
 switchport mode dynamic desirable
 channel-group 12 mode active
!
interface FastEthernet0/16
 switchport mode dynamic desirable
 channel-group 13 mode active
!
interface FastEthernet0/17
 switchport mode dynamic desirable
 channel-group 13 mode active
!
interface FastEthernet0/18
 switchport mode dynamic desirable
 channel-group 13 mode active
!
interface FastEthernet0/19
 switchport mode dynamic desirable
 channel-group 14 mode active
!
interface FastEthernet0/20
 switchport mode dynamic desirable
 channel-group 14 mode active
!
interface FastEthernet0/21
 switchport mode dynamic desirable
 channel-group 14 mode active

SW2:
interface FastEthernet0/13
 channel-group 12 mode passive
!
interface FastEthernet0/14
 channel-group 12 mode passive
!
interface FastEthernet0/15
 channel-group 12 mode passive
```



```
SW3:
interface FastEthernet0/13
 channel-group 13 mode passive
!
interface FastEthernet0/14
 channel-group 13 mode passive
!
interface FastEthernet0/15
 channel-group 13 mode passive

SW4:
interface FastEthernet0/13
 channel-group 14 mode passive
!
interface FastEthernet0/14
 channel-group 14 mode passive
!
interface FastEthernet0/15
 channel-group 14 mode passive
```

Verification

> **Note**
>
> Similar to the previous variation of EtherChannel, Link Aggregation Control Protocol (LACP) is used to negotiate the formation of the channels from SW1 to SW2, SW3, and SW4. LACP is an open standard defined in IEEE 802.3ad. The active mode of LACP, like the desirable mode of PAgP, is used to initiate LACP negotiation, while the passive most is used to only respond to negotiation. Like PAgP this implies that a channel will form via LACP if one side is active and the other side is active or passive, but a channel will not form if both sides are passive.

```
Rack1SW1#show etherchannel summary
Flags:  D - down        P - 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
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 3
Number of aggregators:           3

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------
12     Po12(SU)        LACP      Fa0/13(P)   Fa0/14(P)   Fa0/15(P)
13     Po13(SU)        LACP      Fa0/16(P)   Fa0/17(P)   Fa0/18(P)
14     Po14(SU)        LACP      Fa0/19(P)   Fa0/20(P)   Fa0/21(P)
```



```
Rack1SW1#show interface trunk

Port        Mode         Encapsulation  Status        Native vlan
Po12        desirable    n-isl          trunking      1
Po13        desirable    n-isl          trunking      1
Po14        desirable    n-isl          trunking      1

Port        Vlans allowed on trunk
Po12        1-4094
Po13        1-4094
Po14        1-4094

Port        Vlans allowed and active in management domain
Po12        1,5,7-10,22,43,58,67,79,146
Po13        1,5,7-10,22,43,58,67,79,146
Po14        1,5,7-10,22,43,58,67,79,146

Port        Vlans in spanning tree forwarding state and not pruned
Po12        1,5,7-10,22,43,58,67,79,146
Po13        1,5,9,43,79
Po14        1,10,146

Rack1SW1#show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    32778
             Address     000c.3045.4180
             Cost        9
             Port        168 (Port-channel13)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     001b.d490.7c00
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 15

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Po12             Desg FWD 9         128.160  P2p
Po13             Root FWD 9         128.168  P2p
Po14             Desg FWD 9         128.176  P2p
```



```
Rack1SW2#show etherchannel summary
Flags:  D - down        P - 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
        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
------+-------------+-----------+-----------------------------------
12     Po12(SU)        LACP      Fa0/13(P)   Fa0/14(P)   Fa0/15(P)

Rack1SW2#show interface trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa0/6       on           802.1q         trunking      1
Po12        auto         n-isl          trunking      1

Port        Vlans allowed on trunk
Fa0/6       1-4094
Po12        1-4094

Port        Vlans allowed and active in management domain
Fa0/6       1,5,7-10,22,43,58,67,79,146
Po12        1,5,7-10,22,43,58,67,79,146

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/6       1,5,7-10,22,43,58,67,79,146
Po12        1,5,7,9-10,43,58,67,79,146

Rack1SW2#show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    32778
             Address     000c.3045.4180
             Cost        18
             Port        160 (Port-channel12)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     001b.d4df.ec80
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 15

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/6            Desg FWD 19        128.8    P2p
Po12             Root FWD 9         128.160  P2p
```



```
Rack1SW3#show etherchannel summary
Flags:  D - down        P - 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
        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
------+-------------+-----------+-----------------------------------
13     Po13(SU)        LACP      Fa0/13(P)   Fa0/14(P)   Fa0/15(P)

Rack1SW3#show interface trunk

Port        Mode         Encapsulation  Status        Native vlan
Po13        desirable    n-isl          trunking      1

Port        Vlans allowed on trunk
Po13        1-4094

Port        Vlans allowed and active in management domain
Po13        1,5,7-10,22,43,58,67,79,146

Port        Vlans in spanning tree forwarding state and not pruned
Po13        1,5,7-10,22,43,58,67,79,146

Rack1SW3#show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    32778
             Address     000c.3045.4180
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     000c.3045.4180
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 15

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Po13             Desg FWD 9         128.66   P2p
```



```
Rack1SW4#show etherchannel summary
Flags:  D - down        P - 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
        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
------+-------------+-----------+-----------------------------------
14     Po14(SU)        LACP      Fa0/13(P)   Fa0/14(P)   Fa0/15(P)

Rack1SW4#show interface trunk

Port        Mode         Encapsulation  Status        Native vlan
Po14        desirable    n-isl          trunking      1

Port        Vlans allowed on trunk
Po14        1-4094

Port        Vlans allowed and active in management domain
Po14        1,5,7-10,22,43,58,67,79,146

Port        Vlans in spanning tree forwarding state and not pruned
Po14        1,5,7-10,22,43,58,67,79,146

Rack1SW4#show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    32778
             Address     000c.3045.4180
             Cost        18
             Port        65 (Port-channel14)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     000c.3045.d600
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 15

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Po14             Root FWD 9         128.65   P2p
```

1.15 Layer 3 EtherChannel

- Configure links Fa0/16 & Fa0/17 on SW4 and links Fa0/19 & Fa0/20 on SW2 to be bound together as a Layer 3 EtherChannel.
- Use Port-Channel number 24 and the subnet 155.X.108.0/24 per the diagram.
- Ensure IP reachability is obtained between these devices over the segment.

Configuration

```
SW2:
interface Port-channel24
 no switchport
 ip address 155.1.108.8 255.255.255.0
!
interface FastEthernet0/19
 no switchport
 channel-group 24 mode passive
!
interface FastEthernet0/20
 no switchport
 channel-group 24 mode passive

SW4:
interface Port-channel24
 no switchport
 ip address 155.1.108.10 255.255.255.0
!
interface FastEthernet0/16
 no switchport
 channel-group 24 mode active
!
interface FastEthernet0/17
 no switchport
 channel-group 24 mode active
```


Verification

Pitfall

One common problem with forming layer 3 EtherChannel links is the order of operations. The important point to remember is that when the **channel-group** command is issued, the attributes of the member interfaces are immediately inherited by the Port-Channel interface. This means that if the **channel-group** command is issued before the **no switchport** command, the channel interface will be layer 2 and the member interfaces will be layer 3. A subsequent attempt to issue the **channel-group** command will generate an error message saying that the channel interface and the members are not compatible. To resolve this problem simply issue the **no switchport** command before the **channel-group** command.

Note

If configured properly the state of the Port-channel from the show etherchannel summary command should show (RU) for routed and in use.

```
Rack1SW2#show etherchannel 24 summary
Flags:  D - down        P - 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
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------
24     Po24(RU)        LACP      Fa0/19(P)   Fa0/20(P)

Rack1SW2#ping 155.1.108.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 155.1.108.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```


The Port-Channel interface should show up as a normal layer 3 routed interface in the IP routing table.

```
Rack1SW2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Rack1SW2(config)#ip routing
Rack1SW2(config)#end

Rack1SW2#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     155.1.0.0/24 is subnetted, 3 subnets
C       155.1.8.0 is directly connected, Vlan8
C       155.1.58.0 is directly connected, Vlan58
C       155.1.108.0 is directly connected, Port-channel24
     150.1.0.0/24 is subnetted, 1 subnets
C       150.1.8.0 is directly connected, Loopback0

Rack1SW4#show etherchannel 24 summary
Flags:  D - down        P - 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
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------
24     Po24(RU)        LACP      Fa0/16(P)   Fa0/17(P)
```


1.16 802.1q Tunneling

- Configure 802.1q trunk links between SW1 & SW2's interfaces Fa0/13, SW2's interface Fa0/16 & SW3's interface Fa0/16, and SW3's interface Fa0/19 & SW4's interface Fa0/19.
- Disable all other inter-switch links.
- Configure two Ethernet subinterfaces on R1 with the IP addresses 14.0.0.1/24 and 41.0.0.1/24 using VLANs 14 and 41 respectively.
- Configure two Ethernet subinterfaces on R4's second Ethernet interface1 with the IP addresses 14.0.0.4/24 and 41.0.0.4/24 using VLANs 14 and 41 respectively.
- Using VLAN 100 configure an 802.1q tunnel between SW1 and SW4 to connect R1 and R4.
- R1 and R4 should appear to be directly connected when viewing the **`show cdp neighbor`** output.

Configuration

```
R1:
interface FastEthernet0/0
 no shutdown
!
interface FastEthernet0/0.14
 encapsulation dot1Q 14
 ip address 14.0.0.1 255.255.255.0
!
interface FastEthernet0/0.41
 encapsulation dot1Q 41
 ip address 41.0.0.1 255.255.255.0

R4:
interface FastEthernet0/1
 no shutdown
!
interface FastEthernet0/1.14
 encapsulation dot1Q 14
 ip address 14.0.0.4 255.255.255.0
!
interface FastEthernet0/1.41
 encapsulation dot1Q 41
 ip address 41.0.0.4 255.255.255.0
```



```
SW1:
system mtu 1504
!
interface FastEthernet0/1
 switchport access vlan 100
 switchport mode dot1q-tunnel
 l2protocol-tunnel cdp
 no cdp enable
!
interface FastEthernet0/13
 switchport trunk encapsulation dot1q
 switchport mode trunk

SW2:
system mtu 1504
!
interface FastEthernet0/13
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/16
 switchport trunk encapsulation dot1q
 switchport mode trunk

SW3:
system mtu 1504
!
interface FastEthernet0/16
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/19
 switchport trunk encapsulation dot1q
 switchport mode trunk

SW4:
system mtu 1504
!
interface FastEthernet0/4
 switchport access vlan 100
 switchport mode dot1q-tunnel
 l2protocol-tunnel cdp
 no cdp enable
!
interface FastEthernet0/19
 switchport trunk encapsulation dot1q
 switchport mode trunk
```


Verification

Note

802.1q tunneling, or QinQ tunneling, is commonly used by Metro Ethernet providers to offer a transparent layer 2 VPN to end customers. This design has the distinct advantage over layer 3 MPLS tunnels, as the customer edge device does not have to run a routing protocol with the service provider, and an advantage over layer 2 MPLS AToM or VPLS tunnels for the service provider as the equipment and platform requirements are very moderate.

Dot1q tunneling works by simply taking all traffic received by the customer, and appending a new Ethernet header with a new 802.1q tag onto it. This *metro tag* is used as a unique identifier for the particular customer. Combined with the layer 2 tunneling feature protocols such as CDP, STP, and VTP can be transparently transported between customer sites with no complex requirements in the customer network.

In this example VLAN 100 is used as the metro tag, or tunnel VLAN, for the dot1q tunnel transport between R1 and R4. When R1 and R4 send traffic that is already dot1q tagged from their subinterfaces into the switch network, the new tag of 100 is appended. This can be easily verified through the **`show cdp neighbor`** output on R1 or R4, as even though they are not connected CDP thinks that they are.

```
Rack1R4#show cdp neighbor
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
Rack1R1          Fas 0/1            125         R S I      2610XM    Fas 0/0
```


With the addition of the second 802.1q encapsulation an Ethernet frame already at the normal MTU of 1500 bytes will be using 1504 bytes in the service provider transit path. For this reason the **system mtu** command is adjusted on the layer 2 switches to allow for frames of this size. Note that a reload of the device is necessary before the MTU change actually goes into effect.

```
Rack1R4#ping 14.0.0.1 size 1500 df-bit

Type escape sequence to abort.
Sending 5, 1500-byte ICMP Echos to 14.0.0.1, timeout is 2 seconds:
Packet sent with the DF bit set
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/8 ms

Rack1R4#ping 41.0.0.1 size 1500 df-bit

Type escape sequence to abort.
Sending 5, 1500-byte ICMP Echos to 41.0.0.1, timeout is 2 seconds:
Packet sent with the DF bit set
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/8 ms
```

Although SW1, SW2, SW3, and SW4 do not know about the customer's VLANs of 14 and 41, they are still able to transport these as they are encapsulated inside VLAN 100.

```
Rack1SW1#show spanning-tree vlan 14

Spanning tree instance(s) for vlan 14 does not exist.

Rack1SW1#show spanning-tree vlan 41

Spanning tree instance(s) for vlan 41 does not exist.

Rack1SW1#show interface trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa0/13      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/13      1-4094

Port        Vlans allowed and active in management domain
Fa0/13      1,100

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/13      1,100
```



```
Rack1SW2#show spanning-tree vlan 14

Spanning tree instance(s) for vlan 14 does not exist.

Rack1SW2#show spanning-tree vlan 41

Spanning tree instance(s) for vlan 41 does not exist.

Rack1SW2#show interface trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa0/13      on           802.1q         trunking      1
Fa0/16      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/13      1-4094
Fa0/16      1-4094

Port        Vlans allowed and active in management domain
Fa0/13      1,100
Fa0/16      1,100

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/13      1,100
Fa0/16      1,100

Rack1SW3#show spanning-tree vlan 14

Spanning tree instance(s) for vlan 14 does not exist.

Rack1SW3#show spanning-tree vlan 41

Spanning tree instance(s) for vlan 41 does not exist.

Rack1SW3#show interface trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa0/16      on           802.1q         trunking      1
Fa0/19      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/16      1-4094
Fa0/19      1-4094

Port        Vlans allowed and active in management domain
Fa0/16      1,100
Fa0/19      1,100

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/16      1,100
Fa0/19      1,100
```



```
Rack1SW4#show spanning-tree vlan 14

Spanning tree instance(s) for vlan 14 does not exist.

Rack1SW4#show spanning-tree vlan 41

Spanning tree instance(s) for vlan 41 does not exist.

Rack1SW4#show interface trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa0/19      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/19      1-4094

Port        Vlans allowed and active in management domain
Fa0/19      1,100

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/19      1,100
```


1.17 EtherChannel over 802.1q Tunneling

- Remove the previous trunking and tunneling configuration.
- Configure an 802.1q trunk link between SW2 and SW3.
- Configure interfaces Fa0/13, Fa0/14, and Fa0/15 on SW1 as a layer 2 EtherChannel using PAgP for negotiation.
- Configure interfaces Fa0/19, Fa0/20, and Fa0/21 on SW4 as a layer 2 EtherChannel using PAgP for negotiation.
- Disable all other inter-switch links on SW1 and SW4.
- Configure SW2 and SW3 to tunnel the EtherChannel link between SW1 and SW4 using VLANs 100, 200, and 300.
- Tunnel Spanning-Tree Protocol along with CDP over these links so that SW1 and SW4 appear to be directly connected when viewing the **`show cdp neighbor`** output.
- SW1 and SW4 should form an 802.1q trunk link over this EtherChannel.
- To verify this configure SW1 and SW4's links to R1 and R4 in VLAN 146 per the diagram and ensure connectivity between R1 and R4.

Configuration

```
R1:
interface FastEthernet0/0
 ip address 155.1.146.1 255.255.255.0

R4:
interface FastEthernet0/1
 ip address 155.1.146.4 255.255.255.0

SW1:
vlan 146
!
interface FastEthernet0/1
 switchport access vlan 146
!
interface FastEthernet0/13
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 14 mode desirable
!
interface FastEthernet0/14
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 14 mode desirable
!
interface FastEthernet0/15
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 14 mode desirable
```



```
SW2:
vlan 100,200,300
!
interface FastEthernet0/13
 switchport access vlan 100
 switchport mode dot1q-tunnel
 l2protocol-tunnel cdp
 l2protocol-tunnel stp
 l2protocol-tunnel point-to-point pagp
!
interface FastEthernet0/14
 switchport access vlan 200
 switchport mode dot1q-tunnel
 l2protocol-tunnel cdp
 l2protocol-tunnel stp
 l2protocol-tunnel point-to-point pagp
!
interface FastEthernet0/15
 switchport access vlan 300
 switchport mode dot1q-tunnel
 l2protocol-tunnel cdp
 l2protocol-tunnel stp
 l2protocol-tunnel point-to-point pagp
!
interface FastEthernet0/16
 switchport trunk encapsulation dot1q
 switchport mode trunk

SW3:
vlan 100,200,300
!
interface FastEthernet0/16
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/19
 switchport access vlan 100
 switchport trunk encapsulation dot1q
 switchport mode dot1q-tunnel
 l2protocol-tunnel cdp
 l2protocol-tunnel stp
 l2protocol-tunnel point-to-point pagp
!
interface FastEthernet0/20
 switchport access vlan 200
 switchport mode dot1q-tunnel
 l2protocol-tunnel cdp
 l2protocol-tunnel stp
 l2protocol-tunnel point-to-point pagp
!
interface FastEthernet0/21
 switchport access vlan 300
 switchport mode dot1q-tunnel
 l2protocol-tunnel cdp
 l2protocol-tunnel stp
 l2protocol-tunnel point-to-point pagp
```



```
SW4:
vlan 146
!
interface FastEthernet0/4
 switchport access vlan 146
!
interface FastEthernet0/19
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 14 mode auto
!
interface FastEthernet0/20
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 14 mode auto
!
interface FastEthernet0/21
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 14 mode auto
```

Verification

> **Note**
>
> By creating separate point-to-point tunnels through the usage of separate metro tags an EtherChannel between two customer edge switches can be transparently tunneled over the service provider network.

```
Rack1R4#ping 155.1.146.1 size 1500 df-bit

Type escape sequence to abort.
Sending 5, 1500-byte ICMP Echos to 155.1.146.1, timeout is 2 seconds:
Packet sent with the DF bit set
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/8 ms
```


SW1, who is the customer edge device, sees the root port for VLAN 146 as the port-channel interface, and the root bridge ID of 000c.3045.d600.

```
Rack1SW1#show spanning-tree vlan 146

VLAN0146
  Spanning tree enabled protocol ieee
  Root ID     Priority    32914
              Address     000c.3045.d600
              Cost        9
              Port        176 (Port-channel14)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32914  (priority 32768 sys-id-ext 146)
              Address     001b.d490.7c00
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.3    P2p
Po14             Root FWD 9         128.176  P2p
```

SW4 agrees with this root bridge election for VLAN 146, indicating that these two devices are in the same spanning-tree domain for this VLAN.

```
Rack1SW4#show spanning-tree vlan 146

VLAN0146
  Spanning tree enabled protocol ieee
  Root ID     Priority    32914
              Address     000c.3045.d600
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32914  (priority 32768 sys-id-ext 146)
              Address     000c.3045.d600
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/4            Desg FWD 19        128.4    P2p
Po14             Desg FWD 9         128.65   P2p
```


SW2 and SW3 do not agree on the STP topology for VLAN 146 the same as SW1 and SW4, because STP BPDUs received from SW1 and SW4 are transparently tunneled inside the metro VLAN tags of 100, 200, and 300.

```
Rack1SW2#show spanning-tree vlan 146

Spanning tree instance(s) for vlan 146 does not exist.

Rack1SW3#show spanning-tree vlan 146

Spanning tree instance(s) for vlan 146 does not exist.

Rack1SW1#show etherchannel summary
Flags:  D - down        P - 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
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 3
Number of aggregators:           3

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
14     Po14(SU)        PAgP      Fa0/13(P)   Fa0/14(P)   Fa0/15(P)
```

SW1 and SW4 think that they are directly connected over these tunneled channel ports via CDP.

```
Rack1SW1#show cdp neighbor
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

Device ID      Local Intrfce         Holdtme   Capability    Platform   Port ID
Rack1SW4       Fas 0/15              153            S I      WS-C3550-2Fas 0/21
Rack1SW4       Fas 0/14              153            S I      WS-C3550-2Fas 0/20
Rack1SW4       Fas 0/13              153            S I      WS-C3550-2Fas 0/19
Rack1R1        Fas 0/1               131          R S I     2610XM    Fas 0/0
Rack1R3        Fas 0/3               128          R S I     2611XM    Fas 0/0
Rack1R5        Fas 0/5               124          R S I     2611XM    Fas 0/0
```


1.18 STP Root Bridge Election

- Configure the inter-switch links between SW1 & SW2, SW1 & SW3, SW2 & SW4, and SW3 & SW4 as 802.1q trunk links.
- Disable all other inter-switch links.
- Configure SW4 as a VTP server using the domain name CCIE with SW1, SW2, and SW3 as its clients.
- Configure VLAN assignments per the diagram.
- Configure SW1 as the STP Root Bridge for all active VLANs.
- If SW1 goes down SW4 should take over as the STP Root Bridge for all active VLANs.

Configuration

```
SW1:
vtp domain CCIE
vtp mode client
!
spanning-tree vlan 1,5,7-10,22,43,58,67,79,146 priority 0
!
interface FastEthernet0/1
 switchport access vlan 146
!
interface FastEthernet0/5
 switchport access vlan 58
!
interface FastEthernet0/13
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/14
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/15
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/16
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/17
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/18
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/19
 shutdown
!
```



```
interface FastEthernet0/20
 shutdown
!
interface FastEthernet0/21
 shutdown

SW2:
vtp domain CCIE
vtp mode client
!
interface FastEthernet0/2
 switchport access vlan 22
!
interface FastEthernet0/4
 switchport access vlan 43
!
interface FastEthernet0/6
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/13
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/14
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/15
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/16
 shutdown
!
interface FastEthernet0/17
 shutdown
!
interface FastEthernet0/18
 shutdown
!
interface FastEthernet0/19
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/20
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/21
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/24
 switchport access vlan 22
```



```
SW3:
vtp domain CCIE
vtp mode client
!
interface FastEthernet0/5
 switchport access vlan 5
!
interface FastEthernet0/13
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/14
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/15
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/16
 shutdown
!
interface FastEthernet0/17
 shutdown
!
interface FastEthernet0/18
 shutdown
!
interface FastEthernet0/19
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/20
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/21
 switchport trunk encapsulation dot1q
 switchport mode trunk

SW4:
vtp domain CCIE
vlan 5,7,8,9,10,22,43,58,67,79,146
!
spanning-tree vlan 1,5,7-10,22,43,58,67,79,146 priority 4096
!
interface FastEthernet0/4
 switchport access vlan 146
!
interface FastEthernet0/13
 shutdown
!
interface FastEthernet0/14
 shutdown
!
interface FastEthernet0/15
 shutdown
```



```
!
interface FastEthernet0/16
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/17
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/18
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/19
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/20
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/21
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

Verification

```
Rack1SW1#show spanning-tree vlan 146 | include root
              This bridge is the root
Rack1SW1#show spanning-tree vlan 1 | include root
              This bridge is the root
Rack1SW1#show spanning-tree vlan 5 | include root
              This bridge is the root
Rack1SW1#show spanning-tree vlan 7 | include root
              This bridge is the root
Rack1SW1#show spanning-tree vlan 8 | include root
              This bridge is the root
Rack1SW1#show spanning-tree vlan 9 | include root
              This bridge is the root
Rack1SW1#show spanning-tree vlan 10 | include root
              This bridge is the root
Rack1SW1#show spanning-tree vlan 22 | include root
              This bridge is the root
Rack1SW1#show spanning-tree vlan 43 | include root
              This bridge is the root
Rack1SW1#show spanning-tree vlan 58 | include root
              This bridge is the root
Rack1SW1#show spanning-tree vlan 67 | include root
              This bridge is the root
Rack1SW1#show spanning-tree vlan 79 | include root
              This bridge is the root
Rack1SW1#show spanning-tree vlan 146 | include root
              This bridge is the root
```


Note

STP root bridge election is based on the priority and MAC address fields of the Bridge ID. The device with the lowest priority value is elected the root. If there is a tie in priority the device with the lowest MAC address is elected root. SW1 with the local priority of one, the configured priority of zero plus the system id extension (VLAN number), shows that *This bridge is the root*. The root bridge should show the same priority and MAC address for both the Root ID and the Bridge ID, and list all interfaces as Designated (downstream facing). In this case SW1's BID is 1.001b.d490.7c00.

```
Rack1SW1#show spanning-tree vlan 1

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    1
              Address     001b.d490.7c00
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    1      (priority 0 sys-id-ext 1)
              Address     001b.d490.7c00
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/13           Desg FWD 19        128.15   P2p
Fa0/14           Desg FWD 19        128.16   P2p
Fa0/15           Desg FWD 19        128.17   P2p
Fa0/16           Desg FWD 19        128.18   P2p
Fa0/17           Desg FWD 19        128.19   P2p
Fa0/18           Desg FWD 19        128.20   P2p
```


SW2 agrees that the device with the BID 1.001b.d490.7c00 is the root, and uses the port Fa0/13 with a total cost of 19 to reach it. SW2's local BID is a priority of 32769, the default of 32768 plus the system id extension 1, and the MAC address 001b.d4df.ec80.

```
Rack1SW2#show spanning-tree vlan 1

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    1
              Address     001b.d490.7c00
              Cost        19
              Port        15 (FastEthernet0/13)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     001b.d4df.ec80
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/6            Desg FWD 19        128.8    P2p
Fa0/13           Root FWD 19        128.15   P2p
Fa0/14           Altn BLK 19        128.16   P2p
Fa0/15           Altn BLK 19        128.17   P2p
Fa0/19           Desg FWD 19        128.21   P2p
Fa0/20           Desg FWD 19        128.22   P2p
Fa0/21           Desg FWD 19        128.23   P2p
```


SW3 agrees that the device with the BID 1.001b.d490.7c00 is the root, and uses the port Fa0/13 with a total cost of 19 to reach it. SW3's local BID is a priority of 32769, the default of 32768 plus the system id extension 1, and the MAC address 000c.3045.4180.

```
Rack1SW3#show spanning-tree vlan 1

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    1
              Address     001b.d490.7c00
              Cost        19
              Port        13 (FastEthernet0/13)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     000c.3045.4180
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/13           Root FWD 19        128.13   P2p
Fa0/14           Altn BLK 19        128.14   P2p
Fa0/15           Altn BLK 19        128.15   P2p
Fa0/19           Desg FWD 19        128.19   P2p
Fa0/20           Desg FWD 19        128.20   P2p
Fa0/21           Desg FWD 19        128.21   P2p
```


Likewise SW4 agrees that the device with the BID 1.001b.d490.7c00 is the root, but SW4 has a lower priority than SW2 or SW3. This means that if the root bridge were to fail SW4 would be next in line to take over the root status.

```
Rack1SW4#show spanning-tree vlan 1

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    1
              Address     001b.d490.7c00
              Cost        38
              Port        19 (FastEthernet0/19)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    4097   (priority 4096 sys-id-ext 1)
              Address     000c.3045.d600
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/16           Altn BLK 19        128.16   P2p
Fa0/17           Altn BLK 19        128.17   P2p
Fa0/18           Altn BLK 19        128.18   P2p
Fa0/19           Root FWD 19        128.19   P2p
Fa0/20           Altn BLK 19        128.20   P2p
Fa0/21           Altn BLK 19        128.21   P2p
```


When SW1's trunk links are down SW4 should assume the role of the root bridge since it has the next lowest bridge priority value.

```
Rack1SW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Rack1SW1(config)#interface range fa0/13 - 18
Rack1SW1(config-if-range)#shut
Rack1SW1(config-if-range)#

Rack1SW4#show spanning-tree vlan 1

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    4097
             Address     000c.3045.d600
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    4097   (priority 4096 sys-id-ext 1)
             Address     000c.3045.d600
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 15

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/16           Desg LIS 19        128.16   P2p
Fa0/17           Desg LIS 19        128.17   P2p
Fa0/18           Desg LIS 19        128.18   P2p
Fa0/19           Desg FWD 19        128.19   P2p
Fa0/20           Desg LIS 19        128.20   P2p
Fa0/21           Desg LIS 19        128.21   P2p
```


1.19 STP Load Balancing with Port Cost

- Using Spanning-Tree cost modify the layer 2 transit network so that traffic for all active VLANs from SW2 to SW1 uses the last link between SW2 and SW4.
- If this link goes down traffic should fall over to the second link between SW2 and SW4.

Configuration

```
SW2:
interface FastEthernet0/13
 spanning-tree cost 1000
!
interface FastEthernet0/14
 spanning-tree cost 1000
!
interface FastEthernet0/15
 spanning-tree cost 1000
!
interface FastEthernet0/20
 spanning-tree cost 2
!
interface FastEthernet0/21
 spanning-tree cost 1
```

Verification

```
Rack1SW2#show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    10
             Address     001b.d490.7c00
             Cost        19
             Port        15 (FastEthernet0/13)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     001b.d4df.ec80
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/13           Root FWD 19        128.15   P2p
Fa0/14           Altn BLK 19        128.16   P2p
Fa0/15           Altn BLK 19        128.17   P2p
Fa0/19           Desg FWD 19        128.21   P2p
Fa0/20           Desg FWD 19        128.22   P2p
Fa0/21           Desg FWD 19        128.23   P2p
```


Note

The default cost to the root bridge from SW2 before configuration changes is 19. By changing the links to SW1 to a cost of 1000 they are the least preferred path. By changing the last link to SW4 to a cost of 1 the end to end path cost on that link becomes 39, which is the most preferred (1 to SW4, 19 from SW4 to SW3, 19 from SW3 to SW1). With the second to last link having a cost of 2, the end to end path cost will be 40, and will therefore be the second most preferred link.

```
Rack1SW2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Rack1SW2(config)#interface range fa0/13 - 15
Rack1SW2(config-if-range)#spanning-tree cost 1000
Rack1SW2(config-if-range)#interface fa0/21
% Command exited out of interface range and its sub-modes.
  Not executing the command for second and later interfaces
Rack1SW2(config-if)#spanning-tree cost 1
Rack1SW2(config-if-range)#interface fa0/20
Rack1SW2(config-if)#spanning-tree cost 2
Rack1SW2(config-if)#end
Rack1SW2#

Rack1SW2#show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    10
             Address     001b.d490.7c00
             Cost        39
             Port        23 (FastEthernet0/21)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     001b.d4df.ec80
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 15

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/13           Altn BLK 1000      128.15   P2p
Fa0/14           Altn BLK 1000      128.16   P2p
Fa0/15           Altn BLK 1000      128.17   P2p
Fa0/19           Altn BLK 19        128.21   P2p
Fa0/20           Altn BLK 2         128.22   P2p
Fa0/21           Root FWD 1         128.23   P2p
```


1.20 STP Load Balancing with Port Priority

- Using Spanning-Tree priority modify the layer 2 transit network so that traffic for all active VLANs from SW4 to SW1 uses the last link between SW3 and SW4.
- If this link goes down traffic should fall over to the second link between SW3 and SW4.

Configuration

```
SW3:
interface FastEthernet0/20
 spanning-tree port-priority 16
!
interface FastEthernet0/21
 spanning-tree port-priority 0
```

Verification

Note

Before configuration changes:

```
Rack1SW4#show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    10
             Address     001b.d490.7c00
             Cost        38
             Port        19 (FastEthernet0/19)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    4106   (priority 4096 sys-id-ext 10)
             Address     000c.3045.d600
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/16           Desg FWD 19        128.16   P2p
Fa0/17           Desg FWD 19        128.17   P2p
Fa0/18           Desg FWD 19        128.18   P2p
Fa0/19           Root FWD 19        128.19   P2p
Fa0/20           Altn BLK 19        128.20   P2p
Fa0/21           Altn BLK 19        128.21   P2p
```



```
Rack1SW4#show spanning-tree vlan 10 detail

 VLAN0010 is executing the ieee compatible Spanning Tree protocol
  Bridge Identifier has priority 4096, sysid 10, address 000c.3045.d600
  Configured hello time 2, max age 20, forward delay 15
  Current root has priority 10, address 001b.d490.7c00
  Root port is 19 (FastEthernet0/19), cost of root path is 38
  Topology change flag not set, detected flag not set
  Number of topology changes 5 last change occurred 00:08:08 ago
          from FastEthernet0/16
  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

 Port 16 (FastEthernet0/16) of VLAN0010 is forwarding
   Port path cost 19, Port priority 128, Port Identifier 128.16.
   Designated root has priority 10, address 001b.d490.7c00
   Designated bridge has priority 4106, address 000c.3045.d600
   Designated port id is 128.16, designated path cost 38
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   Link type is point-to-point by default
   BPDU: sent 266, received 119

 Port 17 (FastEthernet0/17) of VLAN0010 is forwarding
   Port path cost 19, Port priority 128, Port Identifier 128.17.
   Designated root has priority 10, address 001b.d490.7c00
   Designated bridge has priority 4106, address 000c.3045.d600
   Designated port id is 128.17, designated path cost 38
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   Link type is point-to-point by default
   BPDU: sent 266, received 118

 Port 18 (FastEthernet0/18) of VLAN0010 is forwarding
   Port path cost 19, Port priority 128, Port Identifier 128.18.
   Designated root has priority 10, address 001b.d490.7c00
   Designated bridge has priority 4106, address 000c.3045.d600
   Designated port id is 128.18, designated path cost 38
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   Link type is point-to-point by default
   BPDU: sent 266, received 119

 Port 19 (FastEthernet0/19) of VLAN0010 is forwarding
   Port path cost 19, Port priority 128, Port Identifier 128.19.
   Designated root has priority 10, address 001b.d490.7c00
   Designated bridge has priority 32778, address 000c.3045.4180
   Designated port id is 128.19, designated path cost 19
   Timers: message age 2, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   Link type is point-to-point by default
   BPDU: sent 71, received 1126
```



```
Port 20 (FastEthernet0/20) of VLAN0010 is blocking
  Port path cost 19, Port priority 128, Port Identifier 128.20.
  Designated root has priority 10, address 001b.d490.7c00
  Designated bridge has priority 32778, address 000c.3045.4180
  Designated port id is 128.20, designated path cost 19
  Timers: message age 3, forward delay 0, hold 0
  Number of transitions to forwarding state: 1
  Link type is point-to-point by default
  BPDU: sent 69, received 1125

Port 21 (FastEthernet0/21) of VLAN0010 is blocking
  Port path cost 19, Port priority 128, Port Identifier 128.21.
  Designated root has priority 10, address 001b.d490.7c00
  Designated bridge has priority 32778, address 000c.3045.4180
  Designated port id is 128.21, designated path cost 19
  Timers: message age 3, forward delay 0, hold 0
  Number of transitions to forwarding state: 1
  Link type is point-to-point by default
  BPDU: sent 69, received 1125
```

Since interfaces Fa0/19 – 21 on SW4 all have the same end to end path cost of 38 the designated (upstream) bridge-id is compared. Since SW4 is connected to SW3 out all three links, there is a tie in the designated bridge-id, and the designated (upstream) port id is compared. Since the upstream port number of Fa0/19 is 19, versus 20 and 21, Fa0/19 is the root port on SW4.

By changing the upstream priority on SW3 on ports Fa0/20 and Fa0/21, SW4 prefers the port with the lowest designated port priority. If interface Fa0/21 on SW4 goes down it will compare the upstream priority of Fa0/20 (16) with the upstream priority of Fa0/19 (128), and Fa0/20 will be chosen.

```
Rack1SW3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Rack1SW3(config)#interface fa0/21
Rack1SW3(config-if)#spanning-tree port-priority 0
Rack1SW3(config-if)#interface fa0/20
Rack1SW3(config-if)#spanning-tree port-priority 16
Rack1SW3(config-if)#end
Rack1SW3#
```



```
Rack1SW4#show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    10
             Address     001b.d490.7c00
             Cost        38
             Port        21 (FastEthernet0/21)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    4106   (priority 4096 sys-id-ext 10)
             Address     000c.3045.d600
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 15

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/16           Desg FWD 19        128.16   P2p
Fa0/17           Desg FWD 19        128.17   P2p
Fa0/18           Desg FWD 19        128.18   P2p
Fa0/19           Altn BLK 19        128.19   P2p
Fa0/20           Altn BLK 19        128.20   P2p
Fa0/21           Root LRN 19        128.21   P2p

Rack1SW4#show spanning-tree vlan 10 detail

 VLAN0010 is executing the ieee compatible Spanning Tree protocol
  Bridge Identifier has priority 4096, sysid 10, address 000c.3045.d600
  Configured hello time 2, max age 20, forward delay 15
  Current root has priority 10, address 001b.d490.7c00
  Root port is 21 (FastEthernet0/21), cost of root path is 38
  Topology change flag set, detected flag not set
  Number of topology changes 6 last change occurred 00:00:19 ago
          from FastEthernet0/19
  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 15

 Port 16 (FastEthernet0/16) of VLAN0010 is forwarding
   Port path cost 19, Port priority 128, Port Identifier 128.16.
   Designated root has priority 10, address 001b.d490.7c00
   Designated bridge has priority 4106, address 000c.3045.d600
   Designated port id is 128.16, designated path cost 38
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   Link type is point-to-point by default
   BPDU: sent 293, received 119

 Port 17 (FastEthernet0/17) of VLAN0010 is forwarding
   Port path cost 19, Port priority 128, Port Identifier 128.17.
   Designated root has priority 10, address 001b.d490.7c00
   Designated bridge has priority 4106, address 000c.3045.d600
   Designated port id is 128.17, designated path cost 38
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   Link type is point-to-point by default
   BPDU: sent 294, received 118
```



```
 Port 18 (FastEthernet0/18) of VLAN0010 is forwarding
   Port path cost 19, Port priority 128, Port Identifier 128.18.
   Designated root has priority 10, address 001b.d490.7c00
   Designated bridge has priority 4106, address 000c.3045.d600
   Designated port id is 128.18, designated path cost 38
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   Link type is point-to-point by default
   BPDU: sent 294, received 119

 Port 19 (FastEthernet0/19) of VLAN0010 is blocking
   Port path cost 19, Port priority 128, Port Identifier 128.19.
   Designated root has priority 10, address 001b.d490.7c00
   Designated bridge has priority 32778, address 000c.3045.4180
   Designated port id is 128.19, designated path cost 19
   Timers: message age 3, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   Link type is point-to-point by default
   BPDU: sent 71, received 1152

 Port 20 (FastEthernet0/20) of VLAN0010 is blocking
   Port path cost 19, Port priority 128, Port Identifier 128.20.
   Designated root has priority 10, address 001b.d490.7c00
   Designated bridge has priority 32778, address 000c.3045.4180
   Designated port id is 16.20, designated path cost 19
   Timers: message age 2, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   Link type is point-to-point by default
   BPDU: sent 69, received 1152

 Port 21 (FastEthernet0/21) of VLAN0010 is learning
   Port path cost 19, Port priority 128, Port Identifier 128.21.
   Designated root has priority 10, address 001b.d490.7c00
   Designated bridge has priority 32778, address 000c.3045.4180
   Designated port id is 0.21, designated path cost 19
   Timers: message age 2, forward delay 7, hold 0
   Number of transitions to forwarding state: 1
   Link type is point-to-point by default
   BPDU: sent 70, received 1153
```


1.21 Tuning STP Convergence Timers

- Configure the switches so that they broadcast Spanning-Tree hello packets every three seconds.
- When a new port becomes active it should wait twenty seconds before transitioning to the forwarding state.
- If the switches do not hear a configuration message within ten seconds they should attempt reconfiguration.
- This configuration should impact all currently active VLANs and any additional VLANs created in the future.

Configuration

```
SW1:
spanning-tree vlan 1-4094 hello-time 3
spanning-tree vlan 1-4094 forward-time 10
spanning-tree vlan 1-4094 max-age 10
```

Verification

```
Rack1SW3#show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    10
             Address     001b.d490.7c00
             Cost        19
             Port        13 (FastEthernet0/13)
             Hello Time   3 sec  Max Age 10 sec  Forward Delay 10 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     000c.3045.4180
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/13           Root FWD 19        128.13   P2p
Fa0/14           Altn BLK 19        128.14   P2p
Fa0/15           Altn BLK 19        128.15   P2p
Fa0/19           Desg FWD 19        128.19   P2p
Fa0/20           Desg FWD 19         16.20   P2p
Fa0/21           Desg FWD 19           0.21   P2p
```


Note

Downstream devices from the root bridge inherit the timers configured on the root. With a forward delay of 10 seconds configured on SW1 the downstream switches should take 10 seconds in each of the listening and learning phases during convergence. The below timestamps indicate that a new root port was elected at 04:56:40 on SW3 and transitions from blocking to listening. 10 seconds later, at 04:56:50, the port transitions from listening to learning. Finally 10 seconds after that, at 04:57:00, the port transitions into forwarding.

```
Rack1SW3#debug spanning-tree events
Spanning Tree event debugging is on
Rack1SW3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Rack1SW3(config)#service timestamps log
Rack1SW3(config)#logging console 7
Rack1SW3(config)#interface fa0/13
Rack1SW3(config-if)#shut

04:56:40: STP: VLAN0001 new root port Fa0/14, cost 19
04:56:40: STP: VLAN0001 Fa0/14 -> listening
04:56:40: STP: VLAN0005 new root port Fa0/14, cost 19
04:56:40: STP: VLAN0005 Fa0/14 -> listening
<output omitted>
04:56:43: STP: VLAN0001 sent Topology Change Notice on Fa0/14
04:56:43: STP: VLAN0005 sent Topology Change Notice on Fa0/14
<output omitted>
04:56:50: STP: VLAN0001 Fa0/14 -> learning
04:56:50: STP: VLAN0005 Fa0/14 -> learning
<output omitted>
04:57:00: STP: VLAN0001 sent Topology Change Notice on Fa0/14
04:57:00: STP: VLAN0001 Fa0/14 -> forwarding
04:57:00: STP: VLAN0005 sent Topology Change Notice on Fa0/14
04:57:00: STP: VLAN0005 Fa0/14 -> forwarding
<output omitted>
```


1.22 STP PortFast

- Configure Spanning-Tree PortFast on the switches so that ports connected to the internal and external routers do not have to wait for the Spanning-Tree listening and learning phases to begin forwarding.
- Do not use any global Spanning-Tree commands to accomplish this.

Configuration

```
SW1:
interface FastEthernet0/1
 spanning-tree portfast
!
interface FastEthernet0/5
 spanning-tree portfast

SW2:
interface FastEthernet0/2
 spanning-tree portfast
!
interface FastEthernet0/4
 spanning-tree portfast
!
interface FastEthernet0/6
 spanning-tree portfast trunk
!
interface FastEthernet0/24
 spanning-tree portfast

SW3:
interface FastEthernet0/5
 spanning-tree portfast
!
interface FastEthernet0/24
 spanning-tree portfast

SW4:
interface FastEthernet0/4
 spanning-tree portfast
```


Verification

> **Note**
>
> Portfast is used to override the listening and learning phases of spanning-tree, also called the forwarding delay, and transition immediately to forwarding.

```
Rack1SW1#show spanning-tree interface fa0/1 portfast
VLAN0146         enabled

Rack1SW1#debug spanning-tree event
Spanning Tree event debugging is on
Rack1SW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Rack1SW1(config)#service timestamp log
Rack1SW1(config)#logging console 7
Rack1SW1(config)#interface fa0/1
Rack1SW1(config-if)#shutdown
05:08:43: %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to
administratively down
05:08:44: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to down
```

When interface Fa0/1 is shutdown and subsequently brought back up it immediately transitions to the forwarding state.

```
Rack1SW1(config-if)#no shutdown
Rack1SW1(config-if)#
05:08:52: set portid: VLAN0146 Fa0/1: new port id 8003
05:08:52: STP: VLAN0146 Fa0/1 ->jump to forwarding from blocking
Rack1SW1(config-if)#
05:08:53: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to
up
05:08:54: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to up
Rack1SW1(config-if)#end
Rack1SW1#
```


1.23 STP PortFast Default

- Remove the previous PortFast configuration.
- Configure Spanning-Tree PortFast on the switches so that ports connected to the internal and external routers do not have to wait for the Spanning-Tree listening and learning phases to begin forwarding.
- Do not use any interface level Spanning-Tree commands to accomplish this.

Configuration

```
SW1:
spanning-tree portfast default

SW2:
spanning-tree portfast default

SW3:
spanning-tree portfast default

SW4:
spanning-tree portfast default
```


Verification

> **Note**
>
> Portfast default has the same affect as the interface level portfast command, however it is automatically enabled on all interfaces at the same time. This command is the equivalent of issuing the **`spanning-tree portfast`** command under an interface range that encompasses all interfaces.

```
Rack1SW1#show run interface fa0/1
Building configuration...

Current configuration : 61 bytes
!
interface FastEthernet0/1
 switchport access vlan 146
end

Rack1SW1#show spanning-tree interface fa0/1 portfast
VLAN0146         enabled

Rack1SW1#debug spanning-tree event
Spanning Tree event debugging is on
Rack1SW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Rack1SW1(config)#interface fa0/1
Rack1SW1(config-if)#shutdown
Rack1SW1(config-if)#
05:13:55: %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to
administratively down
05:13:56: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to down
Rack1SW1(config-if)#no shutdown
Rack1SW1(config-if)#
05:14:03: set portid: VLAN0146 Fa0/1: new port id 8003
05:14:03: STP: VLAN0146 Fa0/1 ->jump to forwarding from blocking
Rack1SW1(config-if)#
05:14:03: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to
up
05:14:04: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to up
Rack1SW1(config-if)#
```


1.24 STP UplinkFast

- Configure SW2, SW3, and SW4 with Spanning-Tree UplinkFast such that if their root port is lost they immediately reconverge to an alternate connection to their upstream bridge.
- Verify this by shutting down the root port of SW2.

Configuration

```
SW2:
spanning-tree uplinkfast

SW3:
spanning-tree uplinkfast

SW4:
spanning-tree uplinkfast
```

Verification

> **Note**
>
> The Cisco proprietary UplinkFast feature is used to speed up convergence time when the direct failure of the local root port occurs. In this particular design interface Fa0/13 on SW2 is the current root port.

```
Rack1SW2#show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    10
             Address     001b.d490.7c00
             Cost        4000
             Port        15 (FastEthernet0/13)
             Hello Time   3 sec  Max Age 10 sec  Forward Delay 10 sec

  Bridge ID  Priority    49162  (priority 49152 sys-id-ext 10)
             Address     001b.d4df.ec80
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300
  Uplinkfast enabled

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/6            Desg FWD 3019      128.8    P2p
Fa0/13           Root FWD 4000      128.15   P2p
Fa0/14           Altn BLK 4000      128.16   P2p
Fa0/15           Altn BLK 4000      128.17   P2p
Fa0/19           Altn BLK 3019      128.21   P2p
Fa0/20           Altn BLK 3002      128.22   P2p
Fa0/21           Altn BLK 3001      128.23   P2p
```


With the failure of the root port the next alternate port is immediately transitioned to the root port in forwarding state, and the CAM table is flooded out this new root port to expedite the learning phase of upstream neighbors.

```
Rack1SW2#debug spanning-tree event
Spanning Tree event debugging is on
Rack1SW2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Rack1SW2(config)#service timestamp log
Rack1SW2(config)#logging console 7
Rack1SW2(config)#interface fa0/13
Rack1SW2(config-if)#shut
Rack1SW2(config-if)#
05:16:42: STP: VLAN0001 new root port Fa0/14, cost 4000
05:16:42: %SPANTREE_FAST-7-PORT_FWD_UPLINK: VLAN0001 FastEthernet0/14
moved to Forwarding (UplinkFast).
05:16:42: STP: VLAN0005 new root port Fa0/14, cost 4000
05:16:42: STP: VLAN0007 new root port Fa0/14, cost 4000
05:16:42: STP: VLAN0008 new root port Fa0/14, cost 4000
05:16:42: STP: VLAN0009 new root port Fa0/14, cost 4000
05:16:42: STP: VLAN0010 new root port Fa0/14, cost 4000
05:16:42: STP: VLAN0022 new root port Fa0/14, cost 4000
05:16:42: STP: VLAN0043 new root port Fa0/14, cost 4000
05:16:42: STP: VLAN0058 new root port Fa0/14, cost 4000
05:16:42: STP: VLAN0067 new root port Fa0/14, cost 4000
05:16:42: STP: VLAN0079 new root port Fa0/14, cost 4000
05:16:42: STP: VLAN0146 new root port Fa0/14, cost 4000
05:16:44: %LINK-5-CHANGED: Interface FastEthernet0/13, changed state to
administratively down
05:16:45: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/13, changed state to down
05:16:45: STP: VLAN0001 sent Topology Change Notice on Fa0/14
05:16:45: STP: VLAN0005 sent Topology Change Notice on Fa0/14
05:16:45: STP: VLAN0007 sent Topology Change Notice on Fa0/14
05:16:45: STP: VLAN0008 sent Topology Change Notice on Fa0/14
05:16:45: STP: VLAN0009 sent Topology Change Notice on Fa0/14
05:16:45: STP: VLAN0010 sent Topology Change Notice on Fa0/14
05:16:45: STP: VLAN0022 sent Topology Change Notice on Fa0/14
05:16:45: STP: VLAN0043 sent Topology Change Notice on Fa0/14
05:16:45: STP: VLAN0058 sent Topology Change Notice on Fa0/14
05:16:45: STP: VLAN0067 sent Topology Change Notice on Fa0/14
05:16:45: STP: VLAN0079 sent Topology Change Notice on Fa0/14
05:16:45: STP: VLAN0146 sent Topology Change Notice on Fa0/14
05:16:58: %SYS-5-CONFIG_I: Configured from console by console
```


1.25 STP BackboneFast

- Configure Spanning-Tree BackboneFast such that if the links between SW3 and SW4 go down SW2 immediately expires its maxage timer and begins Spanning-Tree reconvergence.

Configuration

```
SW1:
spanning-tree backbonefast

SW2:
spanning-tree backbonefast

SW3:
spanning-tree backbonefast

SW4:
spanning-tree backbonefast
```

Verification

> **Note**
>
> The Cisco proprietary BackboneFast feature is used to speed up convergence when an indirect failure occurs upstream in the network by immediately expiring the max_age timer. In this design SW2's root port is towards SW4 on Fa0/21.

```
Rack1SW2#show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    10
             Address     001b.d490.7c00
             Cost        39
             Port        23 (FastEthernet0/21)
             Hello Time   3 sec  Max Age 10 sec  Forward Delay 10 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     001b.d4df.ec80
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 10

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/6            Desg FWD 19        128.8    P2p
Fa0/13           Altn BLK 1000      128.15   P2p
Fa0/14           Altn BLK 1000      128.16   P2p
Fa0/15           Altn BLK 1000      128.17   P2p
Fa0/19           Altn BLK 19        128.21   P2p
Fa0/20           Altn BLK 2         128.22   P2p
Fa0/21           Root FWD 1         128.23   P2p
```


SW4 loses its path to the root bridge causing it to send inferior BPDUs downstream to SW2. Since BackboneFast is enabled, SW2 generates Root Link Query (RLQ) PDUs to check if it should expire max_age for its current BPDUs and begin reconvergence.

```
Rack1SW4#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Rack1SW4(config)#interface range fa0/19 – 21
Rack1SW4(config-if)#shutdown
Rack1SW4(config-if)#

Rack1SW2#debug spanning-tree backbonefast
Spanning Tree backbonefast general debugging is on
Rack1SW2#
STP FAST: received inferior BPDU on VLAN0001 FastEthernet0/19.
STP FAST: sending RLQ request PDU on VLAN0001(1) Fa0/13 Vlan1
STP FAST: sending RLQ request PDU on VLAN0001(1) Fa0/14 Vlan1
STP FAST: sending RLQ request PDU on VLAN0001(1) Fa0/15 Vlan1
STP FAST: sending RLQ request PDU on VLAN0001(1) Fa0/20 Vlan1
STP FAST: sending RLQ request PDU on VLAN0001(1) Fa0/21 Vlan1
STP FAST: received inferior BPDU on VLAN0001 FastEthernet0/20.
STP FAST: sending RLQ request PDU on VLAN0001(1) Fa0/13 Vlan1
STP FAST: sending RLQ request PDU on VLAN0001(1) Fa0/14 Vlan1
STP FAST: sending RLQ request PDU on VLAN0001(1) Fa0/15 Vlan1
STP FAST: sending RLQ request PDU on VLAN0001(1) Fa0/21 Vlan1
STP FAST: received inferior BPDU on VLAN0001 FastEthernet0/21.
STP FAST: sending RLQ request PDU on VLAN0001(1) Fa0/13 Vlan1
STP FAST: sending RLQ request PDU on VLAN0001(1) Fa0/14 Vlan1
STP FAST: sending RLQ request PDU on VLAN0001(1) Fa0/15 Vlan1
STP FAST: received inferior BPDU on VLAN0005 FastEthernet0/19.
STP FAST: sending RLQ request PDU on VLAN0005(5) Faa0/13 Vlan5
STP FAST: sending RLQ request PDU on VLAN0005(5) Fa0/14 Vlan5
STP FAST: sending RLQ request PDU on VLAN0005(5) Fa0/15 Vlan5
STP FAST: sending RLQ request PDU on VLAN0005(5) Fa0/20 Vlan5
STP FAST: sending RLQ request PDU on VLAN0005(5) Fa0/21 Vlan5
STP FAST: received inferior BPDU on VLAN0005 FastEthernet0/20.
STP FAST: sending RLQ request PDU on VLAN0005(5) Fa0/13 Vlan5
STP FAST: sending RLQ request PDU on VLAN0005(5) Fa0/14 Vlan5
STP FAST: sending RLQ request PDU on VLAN0005(5) Fa0/15 Vlan5
STP FAST: sending RLQ request PDU on VLAN0005(5) Fa0/21 Vlan5
STP FAST: received inferior BPDU on VLAN0005 FastEthernet0/21.
STP FAST: sending RLQ request PDU on VLAN0005(5) Fa0/13 Vlan5
STP FAST: sending RLQ request PDU on VLAN0005(5) Fa0/14 Vlan5
STP FAST: sending RLQ request PDU on VLAN0005(5) Fa0/15 Vlan5
<output omitted>
```


1.26 STP BPDU Guard

- Configure Spanning-Tree BPDU Guard on the switches so that ports connected to the internal and external routers are disabled if a Spanning-Tree BPDU is detected.
- Once disabled the switches should attempt to re-enable the ports after two minutes.
- Do not use the global **`portfast`** command to accomplish this.

Configuration

```
SW1:
interface FastEthernet0/1
 spanning-tree bpduguard enable
!
interface FastEthernet0/5
 spanning-tree bpduguard enable
!
errdisable recovery cause bpduguard
errdisable recovery interval 120

SW2:
interface FastEthernet0/2
 spanning-tree bpduguard enable
!
interface FastEthernet0/4
 spanning-tree bpduguard enable
!
interface FastEthernet0/6
 spanning-tree bpduguard enable
!
interface FastEthernet0/24
 spanning-tree bpduguard enable
!
errdisable recovery cause bpduguard
errdisable recovery interval 120

SW3:
interface FastEthernet0/5
 spanning-tree bpduguard enable
!
interface FastEthernet0/24
 spanning-tree bpduguard enable
!
errdisable recovery cause bpduguard
errdisable recovery interval 120

SW4:
interface FastEthernet0/4
 spanning-tree bpduguard enable
!
errdisable recovery cause bpduguard
errdisable recovery interval 120
```


Verification

> **Note**
>
> The STP BPDU Guard feature is used to enforce access layer security on the termination of the STP domain. When an interface running BPDU Guard receives a BPDU (STP packet), the interface is transitioned into err-disable state. This ensures that unauthorized switches cannot be plugged into the network, for example, to perform a layer 2 man-in-the-middle (MiM) attack. If configured, the **`errdisable recovery`** feature can then be used to bring the interface out of err-disable state automatically after a configured interval.
>
> By configuring bridging on R1's link to SW1, STP BPDUs are generated and the link is sent to err-disable state.

```
Rack1R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Rack1R1(config)#bridge 1 protocol ieee
Rack1R1(config)#interface fa0/0
Rack1R1(config-if)#bridge-group 1

Rack1SW1#show spanning-tree interface fa0/1 detail
 Port 3 (FastEthernet0/1) of VLAN0146 is forwarding
   Port path cost 19, Port priority 128, Port Identifier 128.3.
   Designated root has priority 146, address 001b.d490.7c00
   Designated bridge has priority 146, address 001b.d490.7c00
   Designated port id is 128.3, designated path cost 0
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   Link type is point-to-point by default
   Bpdu guard is enabled
   BPDU: sent 4500, received 0

Rack1SW1#
09:00:09: %SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port FastEthernet0/1
with BPDU Guard enabled. Disabling port.
09:00:09: %PM-4-ERR_DISABLE: bpduguard error detected on Fa0/1, putting Fa0/1
in err-disable state
09:00:10: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to down
09:02:09: %PM-4-ERR_RECOVER: Attempting to recover from bpduguard err-disable
state on Fa0/1
09:02:12: %SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port FastEthernet0/1
with BPDU Guard enabled. Disabling port.
09:02:12: %PM-4-ERR_DISABLE: bpduguard error detected on Fa0/1, putting Fa0/1
in err-disable state

Rack1SW1#show interface fa0/1 status

Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/1                        err-disabled 146          auto   auto 10/100BaseTX
```

1.27 STP BPDU Guard Default

- Remove the previous BPDU Guard configuration.
- Configure Spanning-Tree PortFast on the switches so that ports connected to the internal and external routers do not have to wait for the Spanning-Tree listening and learning phases to begin forwarding.
- Configure Spanning-Tree BPDU Guard so that if a Spanning-Tree BPDU is detected on any of these ports they are disabled.
- Do not use any interface level Spanning-Tree commands to accomplish this.

Configuration

```
SW1:
spanning-tree portfast bpduguard default
spanning-tree portfast default

SW2:
spanning-tree portfast bpduguard default
spanning-tree portfast default

SW3:
spanning-tree portfast bpduguard default
spanning-tree portfast default

SW4:
spanning-tree portfast bpduguard default
spanning-tree portfast default
```

Verification

> **Note**
>
> The BPDU Guard default feature works in conjunction with Portfast default in order to automatically enable BPDU Guard on any interfaces in the Portfast state.

```
Rack1R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Rack1R1(config)#bridge 1 protocol ieee
Rack1R1(config)#interface fa0/0
Rack1R1(config-if)#bridge-group 1

Rack1SW1#
09:07:57: %SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port
FastEthernet0/1 with BPDU Guard enabled. Disabling port.
09:07:57: %PM-4-ERR_DISABLE: bpduguard error detected on Fa0/1, putting
Fa0/1 in err-disable state
09:07:57: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to
down
```


1.28 STP BPDU Filter

- Remove the previous BPDU Guard configuration.
- Configure the switches so that ports connected to the internal and external routers do not send Spanning-Tree packets sent out them.
- Do not use any global Spanning-Tree commands to accomplish this.

Configuration

```
SW1:
interface FastEthernet0/1
 spanning-tree bpdufilter enable
!
interface FastEthernet0/5
 spanning-tree bpdufilter enable

SW2:
interface FastEthernet0/2
 spanning-tree bpdufilter enable
!
interface FastEthernet0/4
 spanning-tree bpdufilter enable
!
interface FastEthernet0/6
 spanning-tree bpdufilter enable
!
interface FastEthernet0/24
 spanning-tree bpdufilter enable

SW3:
interface FastEthernet0/5
 spanning-tree bpdufilter enable
!
interface FastEthernet0/24
 spanning-tree bpdufilter enable

SW4:
interface FastEthernet0/4
 spanning-tree bpdufilter enable
```


Verification

Note

The BPDU Filter feature, like the BPDU Guard feature, is used to terminate the STP domain. The difference between them is that when configured at the interface level the BPDU Filter feature drops all inbound BPDUs and does not send BPDUs out the interface. Unlike BPDU Guard the interface does not go into err-disable when a violation occurs. Other user traffic will continued to be forwarded inbound and outbound the port.

```
Rack1R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Rack1R1(config)#bridge 1 protocol ieee
Rack1R1(config)#interface fa0/0
Rack1R1(config-if)#bridge-group 1
Rack1R1(config-if)#end
```

R1 is configured to bridge on the Fa0/0 interface and 2 BPDUs are sent.

```
Rack1R1#show spanning-tree 1

 Bridge group 1 is executing the ieee compatible Spanning Tree protocol
  Bridge Identifier has priority 1, address 0011.bbbd.3bc0
  Configured hello time 2, max age 20, forward delay 15
  We are the root of the spanning tree
  Topology change flag set, detected flag set
  Number of topology changes 3 last change occurred 00:00:23 ago
          from FastEthernet0/0
  Times:  hold 1, topology change 35, notification 2
          hello 2, max age 20, forward delay 15
  Timers: hello 0, topology change 12, notification 0, aging 15

 Port 4 (FastEthernet0/0) of Bridge group 1 is listening
   Port path cost 19, Port priority 128, Port Identifier 128.4.
   Designated root has priority 1, address 0011.bbbd.3bc0
   Designated bridge has priority 1, address 0011.bbbd.3bc0
   Designated port id is 128.4, designated path cost 0
   Timers: message age 0, forward delay 10, hold 0
   Number of transitions to forwarding state: 0
   BPDU: sent 2, received 0
```


SW1 does not acknowledge that it received these BPDUs because BPDU Filter is configured.

```
Rack1SW1#show spanning-tree interface fa0/1 detail
 Port 3 (FastEthernet0/1) of VLAN0146 is forwarding
   Port path cost 19, Port priority 128, Port Identifier 128.3.
   Designated root has priority 146, address 001b.d490.7c00
   Designated bridge has priority 146, address 001b.d490.7c00
   Designated port id is 128.3, designated path cost 0
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   Link type is point-to-point by default
   Bpdu filter is enabled
   BPDU: sent 0, received 0
```


1.29 STP BPDU Filter Default

- Remove the previous BPDU Filter configuration.
- Configure Spanning-Tree PortFast on the switches so that ports connected to the internal and external routers do not have to wait for the Spanning-Tree listening and learning phases to begin forwarding.
- Configure Spanning-Tree BPDU Filter on the switches so that the PortFast enabled ports are reverted out of PortFast state if a Spanning-Tree packet is received in them.
- Do not use any interface level Spanning-Tree commands to accomplish this.

Configuration

```
SW1:
spanning-tree portfast bpdufilter default
spanning-tree portfast default

SW2:
spanning-tree portfast bpdufilter default
spanning-tree portfast default

SW3:
spanning-tree portfast bpdufilter default
spanning-tree portfast default

SW4:
spanning-tree portfast bpdufilter default
spanning-tree portfast default
```


Verification

Note

BPDU Filter Default works with Portfast default by allowing interfaces that should not have Portfast enabled on them to be automatically detected. When both features are configured together all interfaces run in Portfast mode except those which are receiving BPDUs.

In the below output we can see that Portfast is enabled on SW1's link Fa0/1 to R1. Once bridging is enabled on R1's link to SW1, SW1 detects that R1 is sending BPDUs and reverts the interface out of Portfast state. Note that the interface can still forward traffic and is not sent into err-disable state.

```
Rack1SW1#show spanning-tree interface fa0/1 portfast
VLAN0146         enabled

Rack1R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Rack1R1(config)#bridge 1 protocol ieee
Rack1R1(config)#interface fa0/0
Rack1R1(config-if)#bridge-group 1
Rack1R1(config-if)#end
Rack1R1#

Rack1SW1#show spanning-tree interface fa0/1 portfast
VLAN0146         disabled
```

1.30 STP Root Guard

- Configure SW1 so that the links to either SW2 or SW3 are disabled if SW2, SW3, or SW4 is elected the Spanning-Tree Root Bridge for any VLAN.

Configuration

```
SW1:
interface FastEthernet0/13
 spanning-tree guard root
!
interface FastEthernet0/14
 spanning-tree guard root
!
interface FastEthernet0/15
 spanning-tree guard root
!
interface FastEthernet0/16
 spanning-tree guard root
!
interface FastEthernet0/17
 spanning-tree guard root
!
interface FastEthernet0/18
 spanning-tree guard root
```


Verification

Note

Root Guard is similar to the BPDU Guard feature in the manner that it is used to detect STP packets and disable the interface they were received on. The difference between them is that with Root Guard the interface is only disabled (via root inconsistent state) if a *superior* BPDU is received. A superior BPDU indicates a better cost to the root bridge than what is currently installed. Therefore design-wise this feature is used to prevent a rogue device from announcing itself as the new root bridge and possibly implementing a layer 2 man-in-the-middle attack.

In the below output SW4 starts announcing superior BPDUs to SW1 by lowering its bridge priority to zero. Once SW1 receives these announcements the forwarding of VLAN 1 is disabled on the links that these BPDUs were received.

```
Rack1SW4#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Rack1SW4(config)#spanning-tree vlan 1 priority 0
Rack1SW4(config)#

Rack1SW1#
09:20:23: %SPANTREE-2-ROOTGUARD_BLOCK: Root guard blocking port
FastEthernet0/13 on VLAN0001.

Rack1SW1#show spanning-tree vlan 1

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    1
             Address     001b.d490.7c00
             This bridge is the root
             Hello Time   3 sec  Max Age 10 sec  Forward Delay 10 sec

  Bridge ID  Priority    1      (priority 0 sys-id-ext 1)
             Address     001b.d490.7c00
             Hello Time   3 sec  Max Age 10 sec  Forward Delay 10 sec
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/5            Desg FWD 19        128.7    P2p
Fa0/13           Desg BKN*19        128.15   P2p *ROOT_Inc
Fa0/14           Desg BKN*19        128.16   P2p *ROOT_Inc
Fa0/15           Desg BKN*19        128.17   P2p *ROOT_Inc
Fa0/16           Desg BKN*19        128.18   P2p *ROOT_Inc
Fa0/17           Desg BKN*19        128.19   P2p *ROOT_Inc
Fa0/18           Desg BKN*19        128.20   P2p *ROOT_Inc
```


1.31 STP Loop Guard

- Configure Spanning-Tree Loop Guard to prevent unidirectional links from forming on any of the inter-switch links in the layer 2 network.

Configuration

```
SW1:
interface FastEthernet0/13
 spanning-tree guard loop
!
interface FastEthernet0/14
 spanning-tree guard loop
!
interface FastEthernet0/15
 spanning-tree guard loop
!
interface FastEthernet0/16
 spanning-tree guard loop
!
interface FastEthernet0/17
 spanning-tree guard loop
!
interface FastEthernet0/18
 spanning-tree guard loop

SW2:
interface FastEthernet0/13
 spanning-tree guard loop
!
interface FastEthernet0/14
 spanning-tree guard loop
!
interface FastEthernet0/15
 spanning-tree guard loop
!
interface FastEthernet0/19
 spanning-tree guard loop
!
interface FastEthernet0/20
 spanning-tree guard loop
!
interface FastEthernet0/21
 spanning-tree guard loop

SW3:
interface FastEthernet0/13
 spanning-tree guard loop
!
interface FastEthernet0/14
 spanning-tree guard loop
!
interface FastEthernet0/15
 spanning-tree guard loop
!
interface FastEthernet0/19
```



```
 spanning-tree guard loop
!
interface FastEthernet0/20
 spanning-tree guard loop
!
interface FastEthernet0/21
 spanning-tree guard loop

SW4:
interface FastEthernet0/16
 spanning-tree guard loop
!
interface FastEthernet0/17
 spanning-tree guard loop
!
interface FastEthernet0/18
 spanning-tree guard loop
!
interface FastEthernet0/19
 spanning-tree guard loop
!
interface FastEthernet0/20
 spanning-tree guard loop
!
interface FastEthernet0/21
 spanning-tree guard loop
```


Verification

Note

STP Loop Guard is used to prevent STP loops from occurring due to unidirectional links. This feature is similar to Unidirectional Link Detection (UDLD), but it uses STP BPDU keepalives to determine if there is a unidirectional link.

In normal STP operation in a redundant topology some links will be designated forwarding while the other end will be blocking. If one of these blocking links transitions to forwarding state erroneously, a loop can occur. Specifically this can happen if there is a unidirectional link and the blocking port stops receiving the BPDUs that the designated port it sending. Loop guard prevents this by transitioning blocking ports into loop-inconsistent state instead of forwarding if BPDUs stop being received from the designated port.

```
Rack1SW1#show spanning-tree interface fa0/13 detail
 Port 15 (FastEthernet0/13) of VLAN0001 is blocking
   Port path cost 19, Port priority 128, Port Identifier 128.15.
   Designated root has priority 1, address 001b.d490.7c00
   Designated bridge has priority 1, address 001b.d490.7c00
   Designated port id is 128.15, designated path cost 0
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   Link type is point-to-point by default
   Loop guard is enabled on the port
   BPDU: sent 193, received 109

 Port 15 (FastEthernet0/13) of VLAN0005 is forwarding
   Port path cost 19, Port priority 128, Port Identifier 128.15.
   Designated root has priority 5, address 001b.d490.7c00
   Designated bridge has priority 5, address 001b.d490.7c00
   Designated port id is 128.15, designated path cost 0
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   Link type is point-to-point by default
   Loop guard is enabled on the port
   BPDU: sent 268, received 0

<ouput omitted>
```


1.32 Unidirectional Link Detection

- Remove the previous Loop Guard configuration.
- Configure UDLD to prevent unidirectional links from forming on any of the inter-switch links in the layer 2 network.

Configuration

```
SW1:
interface FastEthernet0/13
 udld port aggressive
!
interface FastEthernet0/14
 udld port aggressive
!
interface FastEthernet0/15
 udld port aggressive
!
interface FastEthernet0/16
 udld port aggressive
!
interface FastEthernet0/17
 udld port aggressive
!
interface FastEthernet0/18
 udld port aggressive

SW2:
interface FastEthernet0/13
 udld port aggressive
!
interface FastEthernet0/14
 udld port aggressive
!
interface FastEthernet0/15
 udld port aggressive
!
interface FastEthernet0/19
 udld port aggressive
!
interface FastEthernet0/20
 udld port aggressive
!
interface FastEthernet0/21
 udld port aggressive

SW3:
interface FastEthernet0/13
 udld port aggressive
!
interface FastEthernet0/14
 udld port aggressive
!
interface FastEthernet0/15
 udld port aggressive
```



```
!
interface FastEthernet0/19
 udld port aggressive
!
interface FastEthernet0/20
 udld port aggressive
!
interface FastEthernet0/21
 udld port aggressive

SW4:
interface FastEthernet0/16
 udld port aggressive
!
interface FastEthernet0/17
 udld port aggressive
!
interface FastEthernet0/18
 udld port aggressive
!
interface FastEthernet0/19
 udld port aggressive
!
interface FastEthernet0/20
 udld port aggressive
!
interface FastEthernet0/21
 udld port aggressive
```


Verification

Note

UDLD, like Loop Guard, is used to prevent loops due to unidirectional links. The difference between the features is that Loop Guard uses STP BPDUs to detect these failures, while UDLD uses its own keepalive.

UDLD is a Cisco proprietary feature in which peers discover each other by exchanging frames sent to the well-known MAC address 01:00:0C:CC:CC:CC. Each switch sends its own device ID along with the originator port ID and timeout value to its peer. Additionally a switch echoes back the ID of its neighbor. If no echo frame with the switch's own ID has been seen from the peer for a certain amount of time, the port is suspected to be unidirectional. What happens next depends on UDLD mode of operation.

In "Normal" mode if the physical state of port (as reported by Layer 1) is still up UDLD marks this port as "Undetermined", but does NOT shut down or disable the port, and it continues to operate under its current STP status. This mode of operation is informational and potentially less disruptive (though it does not prevent STP loops).

If UDLD is set to "Aggressive" mode, once the switch loses its neighbor it actively tries to re-establish the relationship by sending a UDLD frames 8 times every 1 second. If the neighbor does not respond after that the port is considered to be unidirectional and sent to err-disable state.

In certain designs there are unidirectional links that Loop Guard can prevent, and UDLD can not, and likewise ones that UDLD can prevent, but Loop Guard cannot. For example if a loop occurs due to a physical wiring problem, i.e. someone mistakenly mixes up the send and receive pairs of a fiber link, UDLD can detect this, but Loop Guard cannot. Likewise if there is a unidirectional link due to a failure in the STP software itself, although much more rare, Loop Guard can detect this but UDLD cannot. Based on this the features can be configured at the same time to protect against all possible unidirectional link scenarios.

Although in this design UDLD is configured on copper UTP interfaces, this case is usually not needed in a real network design due to the Fast Link Pulse (FLP) signals that already track the interface status on wired interfaces. Instead UDLD is more commonly run on Fiber Optic interfaces.

```
Rack1SW1#show udld fa0/13

Interface Fa0/13
---
Port enable administrative configuration setting: Enabled / in
aggressive mode
Port enable operational state: Enabled / in aggressive mode
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single neighbor detected
Message interval: 7
Time out interval: 5

    Entry 1
    ---
    Expiration time: 45
    Device ID: 1
    Current neighbor state: Bidirectional
    Device name: FDO1118Z0P9
    Port ID: Fa0/13
    Neighbor echo 1 device: FDO1118Z0P6
    Neighbor echo 1 port: Fa0/13

    Message interval: 15
    Time out interval: 5
    CDP Device name: Rack1SW2
```


1.33 MST Root Bridge Election

- Configure the inter-switch links between SW1 & SW2, SW1 & SW3, SW2 & SW4, and SW3 & SW4 as 802.1q trunk links.
- Disable all other inter-switch links.
- Configure SW4 as a VTP server using the domain name CCIE with SW1, SW2, and SW3 as its clients.
- Configure VLAN assignments per the diagram.
- Configure Multiple Spanning-Tree on the switches.
- Instance 1 should service VLANs 1 - 100.
- Instance 2 should service VLANs 101 - 200.
- Instance 3 should service all other VLANs.
- Configure SW1 as the STP Root Bridge for instance 1.
- Configure SW4 as the STP Root Bridge for instance 2.
- If SW1 goes down SW2 should take over as the STP Root Bridge for instance 1.
- If SW4 goes down SW3 should take over as the STP Root Bridge for instance 2.

Configuration

```
R6:
interface FastEthernet0/0.67
 encapsulation dot1q 67
 ip address 155.1.67.6 255.255.255.0
!
interface FastEthernet0/0.146
 encapsulation dot1q 146
 ip address 155.1.146.6 255.255.255.0

SW1:
vtp domain CCIE
vtp mode client
!
spanning-tree mst configuration
 name MST1
 revision 1
 instance 1 vlan 1-100
 instance 2 vlan 101-200
 instance 3 vlan 201-4094
!
spanning-tree mst 1 priority 0
!
spanning-tree mode mst
!
interface FastEthernet0/1
 switchport access vlan 146
!
```



```
interface FastEthernet0/5
 switchport access vlan 58
!
interface FastEthernet0/13
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/14
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/15
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/16
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/17
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/18
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/19
 shutdown
!
interface FastEthernet0/20
 shutdown
!
interface FastEthernet0/21
 shutdown

SW2:
vtp domain CCIE
vtp mode client
!
spanning-tree mst configuration
 name MST1
 revision 1
 instance 1 vlan 1-100
 instance 2 vlan 101-200
 instance 3 vlan 201-4094
!
spanning-tree mst 1 priority 4096
!
spanning-tree mode mst
!
interface FastEthernet0/2
 switchport access vlan 22
!
interface FastEthernet0/4
 switchport access vlan 43
!
```



```
interface FastEthernet0/6
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/13
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/14
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/15
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/16
 shutdown
!
interface FastEthernet0/17
 shutdown
!
interface FastEthernet0/18
 shutdown
!
interface FastEthernet0/19
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/20
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/21
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/24
 switchport access vlan 22

SW3:
vtp domain CCIE
vtp mode client
!
spanning-tree mst configuration
 name MST1
 revision 1
 instance 1 vlan 1-100
 instance 2 vlan 101-200
 instance 3 vlan 201-4094
!
spanning-tree mst 2 priority 4096
!
spanning-tree mode mst
!
interface FastEthernet0/5
 switchport access vlan 5
```



```
!
interface FastEthernet0/13
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/14
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/15
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/16
 shutdown
!
interface FastEthernet0/17
 shutdown
!
interface FastEthernet0/18
 shutdown
!
interface FastEthernet0/19
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/20
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/21
 switchport trunk encapsulation dot1q
 switchport mode trunk

SW4:
vtp domain CCIE
vlan 5,7,8,9,10,22,43,58,67,79,146
!
spanning-tree mst configuration
 name MST1
 revision 1
 instance 1 vlan 1-100
 instance 2 vlan 101-200
 instance 3 vlan 201-4094
!
spanning-tree mst 2 priority 0
!
spanning-tree mode mst
!
interface FastEthernet0/4
 switchport access vlan 146
!
interface FastEthernet0/13
 shutdown
!
interface FastEthernet0/14
 shutdown
```



```
!
interface FastEthernet0/15
 shutdown
!
interface FastEthernet0/16
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/17
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/18
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/19
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/20
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/21
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

Verification

Note

Multiple Spanning-Tree (MST) is an IEEE standard defined in 802.1s, and allows user-defined STP instances to be mapped to multiple VLANs. Unlike the Cisco proprietary Per-VLAN Spanning-Tree (PVST), MST can be used to eliminate the overhead of redundant STP instances in topologies where multiple VLANs, but not all VLANs, follow the same layer 2 forwarding path, while at the same time allowing for flexible failure domain separation and traffic engineering. MST essentially takes the best features of IEEE 802.1D Spanning-Tree, AKA Common Spanning-Tree, and the Cisco extensions to STP, PVST, PVST+, Rapid PVST+, and combines them.

For example in this design STP instances are created for VLANs 1 – 4094. In Common Spanning-Tree all 4094 VLANs would map to one instance. This has very little overhead but does not allow for detailed traffic engineering. With PVST there would be 4094 separate instances of STP, which allows for detailed traffic engineering but creates immense overhead. With MST three user-defined instances are created that map different portions of the VLAN space into separate instances with a similar forwarding path.

Like CST and PVST, MST uses the lowest Bridge-ID (BID) in the network to elect the Root Bridge. The BID is made up of the priority value and the MAC address. The lower priority wins the election, and if there is a tie in priority the lowest MAC address is the tie breaker. In PVST there is one root bridge election per VLAN, since there is one STP instance per VLAN, but in MST there is one election per user-defined instance.

From the **`show spanning-tree mst`** output we can see which VLANs are mapped to the particular MST instance, who the root bridge is, and how the root port election has occurred. In this case SW1 is the root for instance 1, while SW4 is the root for instance 2. SW1 is the root for instance 1 because it has a priority value of 1, which is made up of the configured priority of 0 plus the sytem-id extension of 1. In MST the sysid field is the instance number, where as in PVST the sysid is the VLAN number.

```
Rack1SW1#show spanning-tree mst 1

##### MST1    vlans mapped:   1-100
Bridge        address 001b.d490.7c00  priority      1     (0 sysid 1)
Root          this switch for MST1

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/5            Desg FWD 200000    128.7    P2p
Fa0/13           Desg FWD 200000    128.15   P2p
Fa0/14           Desg FWD 200000    128.16   P2p
Fa0/15           Desg FWD 200000    128.17   P2p
Fa0/16           Desg FWD 200000    128.18   P2p
Fa0/17           Desg FWD 200000    128.19   P2p
Fa0/18           Desg FWD 200000    128.20   P2p

Rack1SW1#show spanning-tree mst 2

##### MST2    vlans mapped:   101-200
Bridge        address 001b.d490.7c00  priority      32770 (32768 sysid 2)
Root          address 000c.3045.d600  priority      2     (0 sysid 2)
              port    Fa0/16          cost          400000    rem hops 18

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 200000    128.3    P2p
Fa0/13           Altn BLK 200000    128.15   P2p
Fa0/14           Altn BLK 200000    128.16   P2p
Fa0/15           Altn BLK 200000    128.17   P2p
Fa0/16           Root FWD 200000    128.18   P2p
Fa0/17           Altn BLK 200000    128.19   P2p
Fa0/18           Altn BLK 200000    128.20   P2p
```



```
Rack1SW2#show spanning-tree mst 1

##### MST1    vlans mapped:   1-100
Bridge        address 001b.d4df.ec80  priority      4097  (4096 sysid 1)
Root          address 001b.d490.7c00  priority      1     (0 sysid 1)
              port    Fa0/13          cost          200000    rem hops 19

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Desg FWD 200000    128.4    P2p
Fa0/4            Desg FWD 200000    128.6    P2p
Fa0/6            Desg FWD 200000    128.8    P2p
Fa0/13           Root FWD 200000    128.15   P2p
Fa0/14           Altn BLK 200000    128.16   P2p
Fa0/15           Altn BLK 200000    128.17   P2p
Fa0/19           Desg FWD 200000    128.21   P2p
Fa0/20           Desg FWD 200000    128.22   P2p
Fa0/21           Desg FWD 200000    128.23   P2p
Fa0/24           Desg FWD 2000000   128.26   Shr

Rack1SW2#show spanning-tree mst 2

##### MST2    vlans mapped:   101-200
Bridge        address 001b.d4df.ec80  priority      32770 (32768 sysid 2)
Root          address 000c.3045.d600  priority      2     (0 sysid 2)
              port    Fa0/19          cost          200000    rem hops 19

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/6            Desg FWD 200000    128.8    P2p
Fa0/13           Desg FWD 200000    128.15   P2p
Fa0/14           Desg FWD 200000    128.16   P2p
Fa0/15           Desg FWD 200000    128.17   P2p
Fa0/19           Root FWD 200000    128.21   P2p
Fa0/20           Altn BLK 200000    128.22   P2p
Fa0/21           Altn BLK 200000    128.23   P2p

Rack1SW3#show spanning-tree mst 1

##### MST1    vlans mapped:   1-100
Bridge        address 000c.3045.4180  priority      32769 (32768 sysid 1)
Root          address 001b.d490.7c00  priority      1     (0 sysid 1)
              port    Fa0/13          cost          200000    rem hops 19

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/5            Desg FWD 200000    128.5    P2p
Fa0/13           Root FWD 200000    128.13   P2p
Fa0/14           Altn BLK 200000    128.14   P2p
Fa0/15           Altn BLK 200000    128.15   P2p
Fa0/19           Desg FWD 200000    128.19   P2p
Fa0/20           Desg FWD 200000    128.20   P2p
Fa0/21           Desg FWD 200000    128.21   P2p
Fa0/24           Desg FWD 2000000   128.24   Shr
```



```
Rack1SW3#show spanning-tree mst 2

##### MST2    vlans mapped:   101-200
Bridge        address 000c.3045.4180  priority      4098  (4096 sysid 2)
Root          address 000c.3045.d600  priority      2     (0 sysid 2)
              port    Fa0/19          cost          200000    rem hops 19

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/13           Desg FWD 200000    128.13   P2p
Fa0/14           Desg FWD 200000    128.14   P2p
Fa0/15           Desg FWD 200000    128.15   P2p
Fa0/19           Root FWD 200000    128.19   P2p
Fa0/20           Altn BLK 200000    128.20   P2p
Fa0/21           Altn BLK 200000    128.21   P2p

Rack1SW4#show spanning-tree mst 1

##### MST1    vlans mapped:   1-100
Bridge        address 000c.3045.d600  priority      32769 (32768 sysid 1)
Root          address 001b.d490.7c00  priority      1     (0 sysid 1)
              port    Fa0/16          cost          400000    rem hops 18

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/16           Root FWD 200000    128.16   P2p
Fa0/17           Altn BLK 200000    128.17   P2p
Fa0/18           Altn BLK 200000    128.18   P2p
Fa0/19           Altn BLK 200000    128.19   P2p
Fa0/20           Altn BLK 200000    128.20   P2p
Fa0/21           Altn BLK 200000    128.21   P2p

Rack1SW4#show spanning-tree mst 2

##### MST2    vlans mapped:   101-200
Bridge        address 000c.3045.d600  priority      2     (0 sysid 2)
Root          this switch for MST2

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/4            Desg FWD 200000    128.4    P2p
Fa0/16           Desg FWD 200000    128.16   P2p
Fa0/17           Desg FWD 200000    128.17   P2p
Fa0/18           Desg FWD 200000    128.18   P2p
Fa0/19           Desg FWD 200000    128.19   P2p
Fa0/20           Desg FWD 200000    128.20   P2p
Fa0/21           Desg FWD 200000    128.21   P2p
```


For MST instance 1 SW1 has a priority of 1, and SW2 is next in line with a priority of 4097. When connectivity to SW1 is lost SW2 is promoted to the root bridge status.

```
Rack1SW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Rack1SW1(config)#interface range fa0/13 - 18
Rack1SW1(config-if-range)#shut
Rack1SW1(config-if-range)#

Rack1SW2#show spanning-tree mst 1

##### MST1    vlans mapped:   1-100
Bridge        address 001b.d4df.ec80  priority      4097  (4096 sysid 1)
Root          this switch for MST1

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Desg BLK 200000    128.4    P2p
Fa0/4            Desg BLK 200000    128.6    P2p
Fa0/6            Desg BLK 200000    128.8    P2p
Fa0/19           Desg FWD 200000    128.21   P2p
Fa0/20           Desg FWD 200000    128.22   P2p
Fa0/21           Desg FWD 200000    128.23   P2p
Fa0/24           Desg BLK 2000000   128.26   Shr
```


1.34 MST Load Balancing with Port Cost

- Using Spanning-Tree cost modify the layer 2 transit network so that traffic for MST instance 1 from SW2 to SW1 uses the last link between SW2 and SW4.
- If this link goes down traffic should fall over to the second link between SW2 and SW4.

Configuration

```
SW2:
interface FastEthernet0/13
 spanning-tree mst 1 cost 500000
!
interface FastEthernet0/14
 spanning-tree mst 1 cost 500000
!
interface FastEthernet0/15
 spanning-tree mst 1 cost 500000
!
interface FastEthernet0/20
 spanning-tree mst 1 cost 2
!
interface FastEthernet0/21
 spanning-tree mst 1 cost 1
```


Verification

> **Note**
>
> Similar to CST and PVST, MST uses a cost value derived from the inverse bandwidth of the interface (higher bandwidth means lower cost). The root port is chosen based on the lowest end-to-end cost to the root bridge. The **show spanning-tree mst** command shows the local cost values of the outgoing ports on the local switch.

```
Rack1SW2#show spanning-tree mst 1

##### MST1    vlans mapped:   1-100
Bridge        address 001b.d4df.ec80  priority      4097  (4096 sysid 1)
Root          address 001b.d490.7c00  priority      1     (0 sysid 1)
              port    Fa0/21          cost          400001    rem hops 17

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/2            Desg FWD 200000    128.4    P2p
Fa0/4            Desg FWD 200000    128.6    P2p
Fa0/6            Desg FWD 200000    128.8    P2p
Fa0/13           Altn BLK 500000    128.15   P2p
Fa0/14           Altn BLK 500000    128.16   P2p
Fa0/15           Altn BLK 500000    128.17   P2p
Fa0/19           Altn BLK 200000    128.21   P2p
Fa0/20           Altn BLK 2         128.22   P2p
Fa0/21           Root FWD 1         128.23   P2p
Fa0/24           Desg FWD 2000000   128.26   Shr
```


To see the entire end-to-end cost of a path the **`show spanning-tree mst detail`** command should be used. The end-to-end cost is made up of the upstream (designated) cost, plus the local port cost.In this output the alternate ports Fa0/13 – Fa0/15 have a total cost of 500,000 due to the manual cost change. Fa0/20 has a total cost of 600,000, which is 200,000 to SW4, 200,000 from SW4 to SW3, and 200,000 from SW3 to SW1. Fa0/21 wins the root port election since it has a total cost of 400,001.

```
Rack1SW2#show spanning-tree mst 1 detail

##### MST1    vlans mapped:   1-100
Bridge        address 001b.d4df.ec80  priority      4097  (4096 sysid 1)
Root          address 001b.d490.7c00  priority      1     (0 sysid 1)
              port    Fa0/21          cost          400001    rem hops 17

<output omitted>

FastEthernet0/13 of MST1 is alternate blocking
Port info             port id         128.15  priority    128  cost      500000
Designated root       address 001b.d490.7c00  priority      1  cost           0
Designated bridge     address 001b.d490.7c00  priority      1  port id   128.15
Timers: message expires in 5 sec, forward delay 0, forward transitions 3
Bpdus (MRecords) sent 1385, received 844

FastEthernet0/14 of MST1 is alternate blocking
Port info             port id         128.16  priority    128  cost      500000
Designated root       address 001b.d490.7c00  priority      1  cost           0
Designated bridge     address 001b.d490.7c00  priority      1  port id   128.16
Timers: message expires in 4 sec, forward delay 0, forward transitions 0
Bpdus (MRecords) sent 3965, received 4719

FastEthernet0/15 of MST1 is alternate blocking
Port info             port id         128.17  priority    128  cost      500000
Designated root       address 001b.d490.7c00  priority      1  cost           0
Designated bridge     address 001b.d490.7c00  priority      1  port id   128.17
Timers: message expires in 5 sec, forward delay 0, forward transitions 0
Bpdus (MRecords) sent 3971, received 4725

FastEthernet0/19 of MST1 is alternate blocking
Port info             port id         128.21  priority    128  cost      200000
Designated root       address 001b.d490.7c00  priority      1  cost      400000
Designated bridge     address 000c.3045.d600  priority  32769  port id   128.16
Timers: message expires in 5 sec, forward delay 0, forward transitions 5
Bpdus (MRecords) sent 960, received 1011

FastEthernet0/20 of MST1 is alternate blocking
Port info             port id         128.22  priority    128  cost           2
Designated root       address 001b.d490.7c00  priority      1  cost      400000
Designated bridge     address 000c.3045.d600  priority  32769  port id   128.17
Timers: message expires in 4 sec, forward delay 0, forward transitions 3
Bpdus (MRecords) sent 6085, received 6086

FastEthernet0/21 of MST1 is root forwarding
Port info             port id         128.23  priority    128  cost           1
Designated root       address 001b.d490.7c00  priority      1  cost      400000
Designated bridge     address 000c.3045.d600  priority  32769  port id   128.18
<output omitted>
```


When SW2's port Fa0/21 is down the next lowest cost path is 400,002 through Fa0/20.

```
Rack1SW2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Rack1SW2(config)#interface fa0/21
Rack1SW2(config-if)#shut
Rack1SW2(config-if)#end
Rack1SW2#
07:22:04: %LINK-5-CHANGED: Interface FastEthernet0/21, changed state to
administratively down
07:22:04: %SYS-5-CONFIG_I: Configured from console by console
07:22:05: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/21, changed state to down

Rack1SW2#show spanning-tree mst 1

##### MST1    vlans mapped:   1-100
Bridge        address 001b.d4df.ec80  priority      4097  (4096 sysid 1)
Root          address 001b.d490.7c00  priority      1     (0 sysid 1)
              port    Fa0/20          cost          400002    rem hops 17

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Desg BLK 200000    128.4    P2p
Fa0/4            Desg BLK 200000    128.6    P2p
Fa0/6            Desg BLK 200000    128.8    P2p
Fa0/13           Altn BLK 500000    128.15   P2p
Fa0/14           Altn BLK 500000    128.16   P2p
Fa0/15           Altn BLK 500000    128.17   P2p
Fa0/19           Altn BLK 200000    128.21   P2p
Fa0/20           Root FWD 2         128.22   P2p
```


1.35 MST Load Balancing with Port Priority

- Remove the previous STP cost modifications.
- Set the cost for MST instance 1 on SW3's links to SW1 to be 100,000.
- Using Spanning-Tree priority modify the layer 2 transit network so that traffic for MST instance 1 from SW4 to SW1 uses the last link between SW3 and SW4.
- If this link goes down traffic should fall over to the second link between SW3 and SW4.

Configuration

```
SW3:
interface FastEthernet0/13
 spanning-tree mst 1 cost 100000
!
interface FastEthernet0/14
 spanning-tree mst 1 cost 100000
!
interface FastEthernet0/15
 spanning-tree mst 1 cost 100000
!
interface FastEthernet0/20
 spanning-tree mst 1 port-priority 16
!
interface FastEthernet0/21
 spanning-tree mst 1 port-priority 0
```

Verification

> **Note**
>
> Like CST and PVST, MST uses the designated (upstream) port-priority as a tie breaker if the end-to-end cost is the same on multiple ports to the same upstream switch. The **`show spanning-tree mst`** only shows the local port-priority, so the below output doesn't tell us why Fa0/21 is chosen as the root port.

```
Rack1SW4#show spanning-tree mst 1

##### MST1    vlans mapped:   1-100
Bridge        address 000b.46bf.fd00  priority      32769 (32768 sysid 1)
Root          address 001a.a20f.6d00  priority      1     (0 sysid 1)
              port    Fa0/21          cost          300000    rem hops 18
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/16           Altn BLK 200000    128.16   P2p
Fa0/17           Altn BLK 200000    128.17   P2p
Fa0/18           Altn BLK 200000    128.18   P2p
Fa0/19           Altn BLK 200000    128.19   P2p
Fa0/20           Altn BLK 200000    128.20   P2p
Fa0/21           Root FWD 200000    128.21   P2p
```


The show spanning-tree mst detail shows that the lowest end-to-end cost of 300,000 is equal on ports Fa0/19, Fa0/20, and Fa0/21. Since all three of these ports share the same designated bridge-id, the designated port-id is checked. The port-id is made of the port-priority and the internally assigned port number. Fa0/21 has the lowest designated port-id of 0.21, versus Fa0/20's 16.20 and Fa0/19's 128.19.

```
Rack1SW4#show spanning-tree mst 1 detail

##### MST1    vlans mapped:   1-100
Bridge        address 000b.46bf.fd00  priority      32769 (32768 sysid 1)
Root          address 001a.a20f.6d00  priority      1     (0 sysid 1)
              port    Fa0/21          cost          300000    rem hops 18

FastEthernet0/16 of MST1 is alternate blocking
Port info             port id         128.16  priority    128  cost      200000
Designated root       address 001a.a20f.6d00  priority      1  cost      200000
Designated bridge     address 001a.a256.7780  priority   4097  port id   128.21
Timers: message expires in 5 sec, forward delay 0, forward transitions 1
Bpdus (MRecords) sent 109, received 148

FastEthernet0/17 of MST1 is alternate blocking
Port info             port id         128.17  priority    128  cost      200000
Designated root       address 001a.a20f.6d00  priority      1  cost      200000
Designated bridge     address 001a.a256.7780  priority   4097  port id   128.22
Timers: message expires in 5 sec, forward delay 0, forward transitions 0
Bpdus (MRecords) sent 631, received 686

FastEthernet0/18 of MST1 is alternate blocking
Port info             port id         128.18  priority    128  cost      200000
Designated root       address 001a.a20f.6d00  priority      1  cost      200000
Designated bridge     address 001a.a256.7780  priority   4097  port id   128.23
Timers: message expires in 5 sec, forward delay 0, forward transitions 0
Bpdus (MRecords) sent 632, received 688

FastEthernet0/19 of MST1 is alternate blocking
Port info             port id         128.19  priority    128  cost      200000
Designated root       address 001a.a20f.6d00  priority      1  cost      100000
Designated bridge     address 000d.653a.2680  priority  32769  port id   128.19
Timers: message expires in 4 sec, forward delay 0, forward transitions 1
Bpdus (MRecords) sent 108, received 203

FastEthernet0/20 of MST1 is alternate blocking
Port info             port id         128.20  priority    128  cost      200000
Designated root       address 001a.a20f.6d00  priority      1  cost      100000
Designated bridge     address 000d.653a.2680  priority  32769  port id    16.20
Timers: message expires in 5 sec, forward delay 0, forward transitions 1
Bpdus (MRecords) sent 713, received 622

FastEthernet0/21 of MST1 is root forwarding
Port info             port id         128.21  priority    128  cost      200000
Designated root       address 001a.a20f.6d00  priority      1  cost      100000
Designated bridge     address 000d.653a.2680  priority  32769  port id     0.21
Timers: message expires in 5 sec, forward delay 0, forward transitions 1
Bpdus (MRecords) sent 599, received 507
```


When SW4 loses its connection to SW3 via Fa0/21 the next port in line is Fa0/20 with the designated port-id of 16.20.

```
Rack1SW4#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Rack1SW4(config)#interface fa0/21
Rack1SW4(config-if)#shut
Rack1SW4(config-if)#end
Rack1SW4#
00:20:12: %SYS-5-CONFIG_I: Configured from console by console
00:20:13: %LINK-5-CHANGED: Interface FastEthernet0/21, changed state to
administratively down
00:20:14: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/21,
changed state to down

Rack1SW4#show spanning-tree mst 1

##### MST1    vlans mapped:   1-100
Bridge        address 000b.46bf.fd00  priority      32769 (32768 sysid 1)
Root          address 001a.a20f.6d00  priority      1     (0 sysid 1)
              port    Fa0/20          cost          300000    rem hops 18

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/16           Altn BLK 200000    128.16   P2p
Fa0/17           Altn BLK 200000    128.17   P2p
Fa0/18           Altn BLK 200000    128.18   P2p
Fa0/19           Altn BLK 200000    128.19   P2p
Fa0/20           Root FWD 200000    128.20   P2p
```


1.36 MST and Rapid Spanning Tree

- Configure Rapid Spanning-Tree on the switches so that ports connected to the internal and external routers immediately begin forwarding when enabled.

Configuration

```
SW1:
interface FastEthernet0/1
 spanning-tree portfast
!
interface FastEthernet0/5
 spanning-tree portfast

SW2:
interface FastEthernet0/2
 spanning-tree portfast
!
interface FastEthernet0/4
 spanning-tree portfast
!
interface FastEthernet0/6
 spanning-tree portfast trunk
!
interface FastEthernet0/24
 spanning-tree portfast

SW3:
interface FastEthernet0/5
 spanning-tree portfast
!
interface FastEthernet0/24
 spanning-tree portfast

SW4:
interface FastEthernet0/4
 spanning-tree portfast
```


Verification

When MST is enabled, Rapid Spanning-Tree Protocol (RSTP) is automatically enabled. RSTP is an IEEE standard defined in 802.1w that speeds up convergence through a reliable handshaking process. RSTP defines new port "roles" to automatically allow for the functionality built into Cisco proprietary features such as PortFast and UplinkFast.

RSTP "edge" ports behave the same as PVST PortFast enabled ports. However, in order to maintain backwards compatible configurations Cisco's implementation of RSTP does not automatically elect edge ports as the standard suggests. Instead a port must be configured as an edge port with the **`spanning-tree portfast`** command.

```
Rack1SW1#show spanning-tree mst interface fa0/1

FastEthernet0/1 of MST0 is designated forwarding
Edge port: edge            (enable)         port guard : none        (default)
Link type: point-to-point (auto)            bpdu filter: disable     (default)
Boundary : internal                         bpdu guard : disable     (default)
Bpdus sent 260, received 0

Instance Role Sts Cost      Prio.Nbr Vlans mapped
-------- ---- --- --------- -------- --------------------------------
0        Desg FWD 200000    128.3    none
2        Desg FWD 200000    128.3    101-200

Rack1SW2#show spanning-tree mst interface fa0/6

FastEthernet0/6 of MST0 is designated forwarding
Edge port: edge            (trunk)          port guard : none        (default)
Link type: point-to-point (auto)            bpdu filter: disable     (default)
Boundary : internal                         bpdu guard : disable     (default)
Bpdus sent 30, received 0

Instance Role Sts Cost      Prio.Nbr Vlans mapped
-------- ---- --- --------- -------- --------------------------------
0        Desg FWD 200000    128.8    none
1        Desg FWD 200000    128.8    1-100
2        Desg FWD 200000    128.8    101-200
```


1.37 Protected Ports

- Create a new SVI for VLAN22 on SW2 and assign it the IP address 192.10.X.8/24, where X is your rack number.
- Configure port protection on SW2 so that R2 and BB2 cannot directly communicate with each other, but can communicate with SW2's VLAN22 interface.

Configuration

```
SW2:
interface FastEthernet0/2
 switchport protected
!
interface FastEthernet0/24
 switchport protected
```


Verification

> **Note**
>
> Protected ports are used to prevent traffic from being exchanged at layer 2 between two or more ports that are in the same VLAN. Traffic received in a protected port cannot be sent out another protected port, however traffic received in a protected port can be sent out a non-protected port. This feature is a much smaller subset of the Private VLAN feature, and cannot span between multiple physical switches.
>
> In this particular design the result of port protection is that R2 and SW2 can communicate, SW2 and BB2 can communicate, but R2 and BB2 cannot.

```
Rack1R2#ping 192.10.1.254

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.10.1.254, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

Rack1R2#ping 192.10.1.8

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.10.1.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

Rack1SW2#ping 192.10.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.10.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/8 ms

Rack1SW2#ping 192.10.1.254

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.10.1.254, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/8 ms

Rack1R2#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.10.1.254            0   Incomplete      ARPA
Internet  192.10.1.8              0   001a.a256.77c3  ARPA   FastEthernet0/0
Internet  192.10.1.2              -   000d.65c2.f1c0  ARPA   FastEthernet0/0
```


1.38 Storm Control

- Configure SW1 to limit unicast traffic received from R1 to 100 pps.
- Configure SW2 to limit broadcast traffic received from R6 to 10Mbps.
- Configure SW4 to limit broadcast traffic received from R4 to 1Mbps using a relative percentage of the interface bandwidth.

Configuration

```
SW1:
interface FastEthernet0/1
 storm-control unicast level pps 100

SW2:
interface FastEthernet0/6
 storm-control broadcast level 1.00

SW4:
interface FastEthernet0/4
 storm-control broadcast level bps 10m
```

Verification

> **Note**
>
> Storm control is used to limit the amount of unicast, multicast, or broadcast traffic received in a port. The most common application of this feature is to prevent broadcast storms, but it can also be used to police individual ports not to exceed a desired rate.
>
> Depending on the version of IOS the **`storm-control`** command may take units in percentage, packets per second, bits per second, or others. Make sure to use the question mark when implementing this command so that the units entered achieve the desired result.

```
Rack1SW2#show storm-control
Interface  Filter State   Upper         Lower         Current
---------  -------------  ------------  ------------  ----------
Fa0/6      Link Down          10m bps       10m bps         0 bps

Rack1SW4#show storm-control
Interface  Filter State   Upper         Lower         Current
---------  -------------  ------------  ------------  ----------
Fa0/4      Link Down         1.00%         1.00%         0.00%
```


1.39 MAC-Address Table Static Entries & Aging

- Ensure reachability on VLAN 146 between R1, R4, and R6.
- Configure a static CAM entry on SW4 so that frames destined to the MAC address of R4's interface connected to VLAN 146 are dropped; once complete R1 and R6 should have reachability to each other, but not R4.
- Configure static CAM entry for that MAC address of R6's connection to VLAN 146 to ensure that this address is not allowed to roam.

Configuration

```
SW2:
mac-address-table static 000f.23f4.e640 vlan 146 interface
FastEthernet0/6

SW4:
mac-address-table static 000a.f4b0.cfc2 vlan 146 drop
```

Verification

Note

Normally switches populate the CAM table, or MAC address table, by flooding unknown frames everywhere in the VLAN they were received in and by looking at the source MAC address of frames received in its ports. In certain circumstances this can be undesirable, such as when someone attempts to do a layer 2 MAC address spoofing attack. A simple way to prevent these types of attacks is to statically hard-code which MAC addresses are reachable via which ports.

Another static feature of the CAM table is the ability to Null route MAC addresses. Since static entries always override dynamically learned entries, if the drop keyword or an unused interface is used in the **`mac-address-table static`** command traffic destined to that MAC address will be dropped.

In this particular design R1, R4, and R6 exchange traffic on VLAN 146. SW4, who is connected to R4's port Fa0/1, dynamically learns R4's MAC address 000a.f4b0.cfc2 in port Fa0/4.

```
Rack1R1#ping 155.1.146.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 155.1.146.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms

Rack1R1#ping 155.1.146.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 155.1.146.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

Rack1R4#ping 155.1.146.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 155.1.146.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms
Rack1R4#

Rack1SW4#show mac-address-table dynamic interface fa0/4
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 146    000a.f4b0.cfc2    DYNAMIC     Fa0/4
Total Mac Addresses for this criterion: 1
```


When SW4 is configured with a static entry that matches this address with the keyword drop at the end, the dynamically learned entry is overridden. The result is that any traffic going to R4, such as the ICMP PING from R1, is dropped in the layer 2 transit path.

```
Rack1SW4#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Rack1SW4(config)#mac-address-table static 000a.f4b0.cfc2 vlan 146 drop
Rack1SW4(config)#

Rack1R1#ping 155.1.146.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 155.1.146.4, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Likewise traffic going to R6 uses the static entry as opposed to the dynamically learned entry.

```
Rack1R1#ping 155.1.146.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 155.1.146.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms

Rack1SW2#show mac-address-table address 000f.23f4.e640
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    000f.23f4.e640    DYNAMIC     Fa0/6
 146    000f.23f4.e640    STATIC      Fa0/6
```


1.40 SPAN

- Configure SW1 so that all traffic transiting VLAN 146 is redirected to a host located on port Fa0/24.
- Configure SW4 so that all traffic coming from and going to R4's connection to VLAN 146 is redirected to a host located on port Fa0/24; Inbound traffic from the Linux host should be placed into VLAN 146.

Configuration

```
SW1:
monitor session 1 source vlan 146
monitor session 1 destination interface Fa0/24

SW4:
monitor session 1 source interface Fa0/4
monitor session 1 destination interface Fa0/24 ingress vlan 146
```


Verification

Note

The Switchport Analyzer (SPAN) feature is used to redirect traffic from a port or VLAN onto another port for analysis by devices such as a packet sniffer or Intrusion Prevention Sensor (IPS). There are two variations of SPAN, Local SPAN, or just SPAN, and Remote SPAN, or RSPAN.

With Local SPAN, as seen in this design SW4, traffic coming from or going to a particular port is redirect to another local port. The source of traffic can also be a VLAN, as seen on SW1.Normally when the SPAN feature is configured the switch drops all traffic coming back in the destination port.

The ingress keyword tells the switch which access VLAN inbound traffic on the destination port should belong to.

```
Rack1SW1#show monitor session 1
Session 1
---------
Type              : Local Session
Source VLANs      :
    Both          : 146
Destination Ports : Fa0/24
    Encapsulation : Native
          Ingress : Disabled

Rack1SW4#show monitor session 1
Session 1
---------
Type              : Local Session
Source Ports      :
    Both          : Fa0/4
Destination Ports : Fa0/24
    Encapsulation : Native
          Ingress : Enabled, default VLAN = 146
```


1.41 RSPAN

- Disable the trunk links between SW1 and SW2.
- Create VLAN 500 as an RSPAN VLAN on all switches in the topology.
- Configure SW2 so that traffic received from and sent to R4's connection to VLAN 43 is redirected to the RSPAN VLAN.
- Configure SW1 to receive traffic from the RSPAN VLAN and redirect it to a host connected to port Fa0/24.
- Inbound traffic on the link connected to this host should be placed in VLAN 146.

Configuration

```
SW1:
interface FastEthernet0/13
 shutdown
!
interface FastEthernet0/14
 shutdown
!
interface FastEthernet0/15
 shutdown
!
monitor session 2 destination interface Fa0/24 ingress vlan 146
monitor session 2 source remote vlan 500

SW2:
monitor session 2 source interface Fa0/4
monitor session 2 destination remote vlan 500

SW4:
vlan 500
 remote-span
```


Verification

Note

The Remote SPAN, or RSPAN, feature is used when the source port or VLAN that is being monitored is on a different physical switch than the destination sniffer or sensor.

The first step in configuring RSPAN is to ensure that the switches in the layer 2 transit path from the source port/VLAN to the destination port are trunking at layer 2, and know about the RSPAN VLAN that is used to encapsulate and transport the monitored traffic. In this case VTP is used, so only the VTP server SW4 needs to create the VLAN. Note the remote-span keyword under the VLAN, as this is a special attribute that affects how traffic is processed when it is received in this VLAN.

Next the switch attached to the source port or VLAN creates a SPAN session. The source of this span session, in the case of SW2, is all traffic coming in port Fa0/4. The destination of the session is the RSPAN VLAN 500 itself. This means that all traffic that comes in port Fa0/4 will receive a new trunking header with a VLAN 500 tag and be sent out the trunk network.

Lastly the switch attached to the sniffer/sensor creates a SPAN session with the source as the RSPAN VLAN, and the destination as the local port. This means that the switch wants to listen for all traffic received in the RSPAN VLAN, and redirect it out a local port. In this case SW1 says that the source of the session is the *remote* vlan 500. On SW1 therefore all traffic coming in a trunk link with a tag of 500 will be redirected out port Fa0/24. Since the *ingress* keyword is also used, any traffic that SW1 receives in port Fa0/24 will be treated as if it belongs to VLAN 146.

```
Rack1SW1#show monitor session 2
Session 2
---------
Type              : Remote Destination Session
Source RSPAN VLAN : 500
Destination Ports : Fa0/24
    Encapsulation : Native
          Ingress : Enabled, default VLAN = 146
    Ingress encap : Untagged
```



```
Rack1SW2#show monitor session 2
Session 2
---------
Type               : Remote Source Session
Source Ports       :
    Both           : Fa0/4
Dest RSPAN VLAN    : 500


Rack1SW2#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/3, Fa0/5, Fa0/7
                                                Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/22
                                                Fa0/23, Gi0/1, Gi0/2
5    VLAN0005                         active
7    VLAN0007                         active
8    VLAN0008                         active
9    VLAN0009                         active
10   VLAN0010                         active
22   VLAN0022                         active    Fa0/2, Fa0/24
43   VLAN0043                         active    Fa0/4
58   VLAN0058                         active
67   VLAN0067                         active
79   VLAN0079                         active
146  VLAN0146                         active
500  VLAN0500                         active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
5    enet  100005     1500  -      -      -        -    -        0      0
7    enet  100007     1500  -      -      -        -    -        0      0
8    enet  100008     1500  -      -      -        -    -        0      0
9    enet  100009     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
22   enet  100022     1500  -      -      -        -    -        0      0
43   enet  100043     1500  -      -      -        -    -        0      0
58   enet  100058     1500  -      -      -        -    -        0      0
67   enet  100067     1500  -      -      -        -    -        0      0
79   enet  100079     1500  -      -      -        -    -        0      0
146  enet  100146     1500  -      -      -        -    -        0      0
500  enet  100500     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    srb      0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------
500

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

1.42 Voice VLAN

- Ports Fa0/2, Fa0/4, and Fa0/6 on SW1 will be connected to Cisco IP phones in the near future.
- Configure port Fa0/2 with an access VLAN assignment of 146 and a voice VLAN assignment of 600.
- Enable Spanning-Tree portfast on this link and ensure that CDP is enabled.
- Configure port Fa0/4 as an 802.1q trunk link.
- Configure SW1 so that only VLANs 146 and 600 are permitted on this switchport, so that STP BPDUs received on the port are filtered out, and so that the interface runs in STP portfast mode.
- Configure VLAN 146 as the native VLAN for this port and so that VLAN 600 is advertised as the voice VLAN via CDP.
- Configure port Fa0/6 with an access VLAN assignment of 146, and for voice VLAN frames to use dot1p tagging.

Configuration

```
SW1:
interface FastEthernet0/2
 switchport access vlan 146
 switchport voice vlan 600
 spanning-tree portfast
!
interface FastEthernet0/4
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 146
 switchport trunk allowed vlan 146,600
 switchport mode trunk
 switchport voice vlan 600
 spanning-tree portfast trunk
 spanning-tree bpdufilter enable
!
interface FastEthernet0/6
 switchport access vlan 146
 switchport voice vlan dot1p

SW4:
vlan 600
```


Verification

Note

Many models of Cisco IP Phones have a built-in three-port switch, one port to connect to the upstream switch, one port for the IP Phone itself, and the last port to connect to a desktop PC. The built-in switch is capable of separating the IP Phone and the desktop PC traffic using different VLANs. Additionally the internal switch can also use different 802.1p markings in the Class of Service (CoS) field to distinguish the IP Phone and the desktop PC frames. Based on this there are three different options for connecting the IP Phone and the desktop PC to the Catalyst switches.

Option 1 is to separate the Data VLAN for the PC and the Voice VLAN for the IP Phone. The internal IP Phone switch will tag VoIP traffic with the respective VLAN number and apply a CoS value of 5. The data frames are sent untagged and received by the upstream switch on the configured access VLAN. The connection between the IP Phone and the upstream switch is an 802.1q trunk with the native VLAN equal to the Data VLAN.

Option 2 is to use a single VLAN for Data and Voice. The IP Phone's internal switch does not tag the frames and acts as a simple bridge. The connection between the IP Phone and the upstream switch is an access port.

Option 3 is to use a single VLAN for Data and Voice, but to add an 802.1p CoS tag. Data frames received from the PC on the phone, along with VoIP frames sent from the phone get a special 802.1q header that carries a VLAN ID equal to zero and has the CoS field set to 5 for VoIP and the value instructed from the switch for data frames. The Catalyst switch accepts the frames with VLAN zero as if they are in the access VLAN, but also honors the CoS bits to calculate the switch's internal QoS tag.

For all three options the IP Phone's built-in switch should be instructed which mode to use. The command **`switchport voice vlan`** configured on an access port will communicate with the IP Phone via CDP and tell its internal switch which VLAN should be used for voice traffic. The IP Phone's internal switch will then apply the instructed VLAN tag to the voice traffic and will send the PC's data untagged. Note that there is no need to configure the port as an 802.1q trunk via the **`switchport mode trunk`** command. The switchport ASIC will automatically convert the port into a rudimentary trunk.

If no **`switchport voice vlan`** command is configured, then Option 2 applies automatically. Both voice and data packets are received on the same VLAN (the access VLAN).

If the command **`switchport voice vlan dot1p`** is configure on a switchport then the connected IP Phone's switch is instructed to apply VLAN 0 to voice traffic along with the corresponding CoS bits. Both voice and data frames will share the same VLAN configured on the access port.

Note that as soon as the **`switchport voice vlan`** command is applied to the port, the **`spanning-tree portfast`** feature is automatically enabled.

1.43 IP Phone Trust and CoS Extend

- Enable MLS QoS globally on SW1.
- Configure SW1 to trust the CoS of frames received on the ports connected to the IP phones.
- This trust should only occur if the Cisco IP phone is present and advertises itself via CDP.
- SW1 should enforce a CoS value of 1 to any appliance connected to the second port of the IP phone.

Configuration

```
SW1:
mls qos
!
interface FastEthernet0/2
 mls qos trust cos
 mls qos trust device cisco-phone
 switchport priority extend cos 1
!
interface FastEthernet0/4
 mls qos trust cos
 mls qos trust device cisco-phone
 switchport priority extend cos 1
!
interface FastEthernet0/6
 mls qos trust cos
 mls qos trust device cisco-phone
 switchport priority extend cos 1
```


Verification

Note

The QoS trust state of the port determines if frames with a CoS value are maintained or remarked as they are received. In this case these ports are configured to trust the QoS marking only if the presence of a Cisco IP Phone is sensed via CDP messages. This option is enabled with the command **`mls qos trust device cisco-phone`**. If no Cisco device is detected on the port then the QoS markings are not trusted, even if the port is configured for trust.

In addition to enforcing markings at the switchport boundary, the switch may also instruct the IP Phone's switch to apply specific CoS markings for frames received from the connected PC. The switch may either accept (trust) 802.1p bits received from the attached PC or enforce the instructed value. This feature particularly makes sense to be used with the dot1p Voice VLAN option.

```
Rack1SW1#show mls qos interface fa0/2
FastEthernet0/2
trust state: not trusted
trust mode: trust cos
trust enabled flag: dis
COS override: dis
default COS: 0
DSCP Mutation Map: Default DSCP Mutation Map
Trust device: cisco-phone
qos mode: port-based
```


1.44 Smartport Macros

- Configure a macro on SW1 named VLAN_146 that when applied to an interface will set it to be an access switchport, apply VLAN 146 as the access vlan, and filter Spanning-Tree BPDUs.
- Apply this macro to ports Fa0/7 and Fa0/8 on the switch.

Configuration

```
SW1:
macro name VLAN_146
switchport mode access
switchport access vlan 146
spanning-tree bpdufilter enable
@
```

Verification

> **Note**
>
> Smartport Macros are used to define a well known template of configuration to apply onto multiple interfaces. This feature is useful in large switching environments where general categories of ports can be defined, such as access, server, uplink, and have them share common configuration templates.
>
> In this particular design the macro is used to apply three attributes to the interface, the switchport mode, the access VLAN, and the BPDU Filter feature. The result seen from the show run output is identical to that which would be achieved by manually entering these commands on both interfaces, with the addition of the **`macro description`** telling us which macro was applied.

```
Rack1SW1#config t
Rack1SW1(config)#interface range fa0/7-8
Rack1SW1(config-if-range)#macro apply VLAN_146
Rack1SW1(config-if-range)#end
02:11:37: %SYS-5-CONFIG_I: Configured from console by console

Rack1SW1#show run interface fa0/7
Building configuration...

Current configuration : 146 bytes
!
interface FastEthernet0/7
 switchport access vlan 146
 switchport mode access
 macro description VLAN_146
 spanning-tree bpdufilter enable
end
```



```
Rack1SW1#show run interface fa0/8
Building configuration...

Current configuration : 146 bytes
!
interface FastEthernet0/8
 switchport access vlan 146
 switchport mode access
 macro description VLAN_146
 spanning-tree bpdufilter enable
end
```

A number of default Smartport Macros exist in the switch, and can be seen by issuing the **show parser macro** command.

```
Rack1SW1#show parser macro
Total number of macros = 6
------------------------------------------------------------
Macro name : cisco-global
Macro type : default global
# Enable dynamic port error recovery for link state failures.
errdisable recovery cause link-flap
errdisable recovery interval 60

# Config Cos to DSCP mappings
mls qos map cos-dscp 0 8 16 26 32 46 46 56

# Enable aggressive mode UDLD on all fiber uplinks
udld aggressive

# Enable Rapid PVST+ and Loopguard
spanning-tree mode rapid-pvst
spanning-tree loopguard default
spanning-tree extend system-id
------------------------------------------------------------
Macro name : cisco-desktop
Macro type : default interface
# macro keywords $access_vlan
# Basic interface - Enable data VLAN only
# Recommended value for access vlan should not be 1
switchport access vlan $access_vlan
switchport mode access

# Enable port security limiting port to a single
# MAC address -- that of desktop
switchport port-security
switchport port-security maximum 1

# Ensure port-security age is greater than one minute
# and use inactivity timer
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity

# Configure port as an edge network port
```



```
spanning-tree portfast
spanning-tree bpduguard enable
------------------------------------------------------------
<output omitted>
```

A default macro can be applied as follows.

```
Rack1SW1#show run interface fa0/10
Building configuration...

Current configuration : 34 bytes
!
interface FastEthernet0/10
end

Rack1SW1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Rack1SW1(config)#interface fa0/10
Rack1SW1(config-if)#macro apply cisco-desktop $access_vlan 10
%Warning: portfast should only be enabled on ports connected to a single
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface  when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION

%Portfast has been configured on FastEthernet0/10 but will only
 have effect when the interface is in a non-trunking mode.
Rack1SW1(config-if)#end
Rack1SW1#show run interface fa0/10
Building configuration...

Current configuration : 332 bytes
!
interface FastEthernet0/10
 switchport access vlan 10
 switchport mode access
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 macro description cisco-desktop
 spanning-tree portfast
 spanning-tree bpduguard enable
end
```


1.45 Flex Links

- Configure links Fa0/16 between SW2 and SW3 as an 802.1q trunk.
- Configure link Fa0/16 on SW1 and Fa0/13 on SW3 as an 802.1q trunk.
- Configure links Fa0/13 & Fa0/14 between SW1 and SW2 as an 802.1q trunked EtherChannel.
- Disable all other inter-switch links.
- Configure R1's Ethernet interface with the IP address 10.0.0.1/24, R2's Ethernet interface with the IP address 10.0.0.2/24, and R3's second Ethernet interface with the IP address 10.0.0.3/24.
- Configure flex links on SW1 so that traffic from R1 to R3 uses the EtherChannel to SW2.
- If the EtherChannel goes down traffic should immediately switch over to use the link between SW1 and SW3.
- If the EtherChannel and all its members comes back up traffic should forward back over this link after 20 seconds.

Configuration

```
R1:
interface FastEthernet0/0
 ip address 10.0.0.1 255.255.255.0

R2:
interface FastEthernet0/0
 ip address 10.0.0.2 255.255.255.0

R3:
interface FastEthernet0/1
 ip address 10.0.0.3 255.255.255.0

SW1:
interface Port-channel1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport backup interface Fa0/16
 switchport backup interface Fa0/16 preemption mode forced
 switchport backup interface Fa0/16 preemption delay 20
!
interface FastEthernet0/13
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 1 mode on
!
interface FastEthernet0/14
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 1 mode on
!
```



```
interface FastEthernet0/16
 switchport trunk encapsulation dot1q
 switchport mode trunk

SW2:
interface Port-channel1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/13
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 1 mode on
!
interface FastEthernet0/14
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 1 mode on
!
interface FastEthernet0/16
 switchport trunk encapsulation dot1q
 switchport mode trunk

SW3:
interface FastEthernet0/13
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/16
 switchport trunk encapsulation dot1q
 switchport mode trunk
```


Verification

Note

The Flex Links feature is used as an alternative to Spanning-Tree Protocol in environments where physical loops occur in the layer 2 network. Flex Links work like the **backup interface** feature on the routers, in which a layer 2 physical interface or Port-Channel is configured as the "active" link, and another layer 2 link is configured as the "backup". STP is automatically disabled on both links when Flex Links are enabled.

The backup link operates in standby mode, and waits for the line protocol of the active link to go down. If the line protocol of the active link is down, the backup link becomes active and immediately starts forwarding. When the active link's line protocol status comes back up, the backup link goes back into standby state and stops forwarding traffic.

In this particular design SW1 has Port-Channel1 configured as the active link and FastEthernet0/16 configured as the backup.

```
Rack1SW1#show interfaces po1 switchport backup

Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
Port-channel1           FastEthernet0/16        Active Up/Backup Standby
```

```
Rack1R1#ping 10.0.0.3 repeat 5000

Type escape sequence to abort.
Sending 5000, 100-byte ICMP Echos to 10.0.0.3, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
<output omitted>
```

SW2's Port-Channel1 interface is shutdown, causing SW1's link to go down.

```
Rack1SW2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Rack1SW2(config)#interface po1
Rack1SW2(config-if)#shut
Rack1SW2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed
state to down
%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to
administratively down
%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to
administratively down
```


SW1 detects this and immediately activates port Fa0/16.

```
Rack1SW1#debug backup all
Switch Backup Interface all debugging is on
sw_backup_int: intf Po1, state 1, transition for event 0
sw_backup_int: Po1 is now Down
BACKUP_INT: idb Po1, peer Fa0/16, state Down
sw_backup_int: intf Fa0/16, state 2, transition for event 1
sw_backup_int: Fa0/16 is now Up
BACKUP_INT: intf Po1, updating vtp pruning join bits
BACKUP_INT: intf Fa0/16, updating vtp pruning join bits
BACKUP_INT: intf Po1, state up, bandwidth 100000 Kbps
BACKUP_INT: setting WB
BACKUP_INT: clearing WB
BACKUP_INT: Pair Po1 Fa0/16 mode bandwidth, delay 20 seconds,
Unscheduled
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/13,
changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/14,
changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed
state to down
BACKUP_INT: intf Po1, state down, bandwidth 100000 Kbps
BACKUP_INT: setting WB
BACKUP_INT: clearing WB
BACKUP_INT: Pair Po1 Fa0/16 mode bandwidth, delay 20 seconds,
Unscheduled
Rack1SW1#
%LINK-3-UPDOWN: Interface FastEthernet0/13, changed state to down
%LINK-3-UPDOWN: Interface Port-channel1, changed state to down
%LINK-3-UPDOWN: Interface FastEthernet0/14, changed state to down

Rack1SW1#show interfaces po1 switchport backup

Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
Port-channel1           FastEthernet0/16        Active Down/Backup Up
```

R1, who was sending traffic to R3 while the failure occurred, dropped one packet out of 5000. This implies that the network converged in less than four seconds, as the default timeout for a ping is two seconds.

```
[Resuming connection 1 to r1 ... ]
<output omitted>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 99 percent (4999/5000), round-trip min/avg/max = 1/2/48
ms
Rack1R1#
```


When the Po1 interface of SW1 comes back up, a preemption delay counter starts, as configured with the **preemption delay 20** command. After the 20 second delay expires, the bandwidth of the Fa0/16 interface is compared with Po1 due to the **preemption mode bandwidth** command. Since Po1 has a higher bandwidth value it preempts Fa0/16, and Fa0/16 goes into the standby state.

```
Rack1SW2(config)#int po1
Rack1SW2(config-if)#no shut

Rack1SW1#
%LINK-3-UPDOWN: Interface FastEthernet0/13, changed state to up
%LINK-3-UPDOWN: Interface FastEthernet0/14, changed state to up
sw_backup_int: intf Po1, state 0, transition for event 2
sw_backup_int: Po1 is now Waiting to sync
BACKUP_INT: idb Po1, peer Fa0/16, state Waiting to sync
sw_backup_int: intf Po1, state 3, transition for event 6
sw_backup_int: Po1 is now Waiting for peer state
BACKUP_INT: idb Po1, peer Fa0/16, state Waiting for peer state
sw_backup_int: intf Fa0/16, state 1, transition for event 5
BACKUP_INT: idb Fa0/16, peer Po1, state Up
sw_backup_int: intf Po1, state 4, transition for event 3
sw_backup_int: Po1 is now Standby
BACKUP_INT: intf Po1, state up, bandwidth 200000 Kbps
BACKUP_INT: setting WB
BACKUP_INT: clearing WB
BACKUP_INT: AI Po1 ai_state 2 ai_bw 200000, BI Fa0/16 bi_state 1 bi_bw 100000
BACKUP_INT: Pair Po1 Fa0/16 mode bandwidth, delay 20 seconds, Scheduled
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/13, changed state
to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/14, changed state
to up
%LINK-3-UPDOWN: Interface Port-channel1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to
up
BACKUP_INT: intf Po1, state up, bandwidth 200000 Kbps
BACKUP_INT: setting WB
BACKUP_INT: clearing WB
BACKUP_INT: AI Po1 ai_state 2 ai_bw 200000, BI Fa0/16 bi_state 1 bi_bw 100000
BACKUP_INT: Pair Po1 Fa0/16 mode bandwidth, delay 20 seconds, Scheduled
Rack1SW1#
BACKUP_INT: AI Po1 ai_state 2 ai_bw 200000, BI Fa0/16 bi_state 1 bi_bw 100000
%BACKUP_INTERFACE-5-PREEMPT: Preempting interface Fa0/16 in backup pair (Po1,
Fa0/16), preemption mode is bandwidth
<output omitted>

Rack1SW1#show interfaces po1 switchport backup

Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
Port-channel1           FastEthernet0/16        Active Up/Backup Standby
```


1.46 Fallback Bridging

- Configure R4's second Ethernet interface with the IP address 104.0.0.4/24, and with the IPv6 address 2001::4/24.
- Configure R6's second Ethernet interface with the IP address 106.0.0.6/24, and with the IPv6 address 2001::6/24.
- Configure interface VLAN104 on SW4 with the IP address 104.0.0.10/24, and configure interface Fa0/4 in VLAN 104.
- Configure interface Fa0/6 on SW4 with the IP address 106.0.0.10/24.
- Enable RIPv2 on all of these links.
- Configure fallback bridging on SW4 to bridge the IPv6 subnet of R4 and R6 together.

Configuration

```
R4:
interface FastEthernet0/1
 ip address 104.0.0.4 255.255.255.0
 ipv6 address 2001::4/64
!
router rip
 version 2
 no auto-summary
 network 104.0.0.0

R6:
interface FastEthernet0/1
 ip address 106.0.0.6 255.255.255.0
 ipv6 address 2001::6/64
!
router rip
 version 2
 no auto-summary
 network 106.0.0.0

SW4:
vlan 104
!
bridge 1 protocol vlan-bridge
!
interface FastEthernet0/4
 switchport access vlan 104
!
interface FastEthernet0/6
 no switchport
 ip address 106.0.0.10 255.255.255.0
 bridge-group 1
!
interface Vlan104
 ip address 104.0.0.10 255.255.255.0
 bridge-group 1
!
```



```
ip routing
!
router rip
 version 2
 no auto-summary
 network 104.0.0.0
 network 106.0.0.0
```

Verification

Note

The Fallback Bridging feature is used to bridge non-routed protocols between SVIs or native layer 3 routed interfaces. This feature is similar in theory to the Concurrent Routing and Bridging (CRB) and Integrated Routing and Bridging (IRB) features on the routers, where one protocol stack is routed on an interface while another protocol stack is bridged.

For example if a Catalyst switch has two layer 3 interfaces configured, VLAN 10 with the IP subnet 10.0.0.0/8, and VLAN 20 with the IP subnet 20.0.0.0/8, traffic from host 10.0.0.1 and 20.0.0.1 is routed at layer 3. If fallback bridging is configured on the SVI interfaces of VLAN 10 and VLAN 20, 10.0.0.1 and 20.0.0.1 are in different IPv4 subnets, but can be in the same IPX network and have their IPX traffic bridged together.

There are only two steps to implement this feature, create the fallback bridge group with the **`bridge [num] protocol vlan-bridge`** command, and apply it to the layer 3 interfaces with the **`bridge-group [num]`** command.

In this design the feature is tested by bridging IPv6 traffic between R4 and R6. This is done by configuring fallback bridging on SW4's SVI interface VLAN104 connecting to R4 and the native layer 3 routed interface FastEthernet0/6 connecting to R6. In this topology SW4 is a 3550 running IOS 12.2(25), which does not support IPv6 routing. This means that IPv4 will be routed, but IPv6 can be bridged through fallback bridging.

We can see the result of this design is that when R4 does a traceroute to R6 via IPv4, the traffic is routed to SW4, and then sent to R6. However when IPv6 traceroute is done between R4 and R6 they appear to be directly connected.

```
Rack1R4#traceroute 106.0.0.6
Translating "106.0.0.6"

Type escape sequence to abort.
Tracing the route to 106.0.0.6

  1 104.0.0.10 4 msec 0 msec 4 msec
  2 106.0.0.6 0 msec *  0 msec

Rack1R4#traceroute 2001::6

Type escape sequence to abort.
Tracing the route to 2001::6

  1 2001::6 4 msec 0 msec 0 msec
```


1.47 Private VLANs

- Configure the first Ethernet interfaces of R1, R2, R3, R4, R5, and R6 with IP addresses 100.0.0.Y/24, where Y is the device number.
- Configure the first inter-switch link between SW1 and SW2 as a trunk.
- Configure the primary VLAN 100 to service private VLANs 1000, 2000, and 3000.
- VLANs 1000 and 2000 should be community VLANs, while VLAN 3000 should be an isolated VLAN.
- Assign VLAN 1000 to the links connecting to R2 & R3, VLAN 2000 to the links connecting to R4 & R5, and VLAN 3000 to R6.
- The link connecting to R1 should be a promiscuous port.
- Ensure that R1 can reach all devices, R2 can reach R3, and R4 can reach R5.
- No other connectivity should be allowed within this topology.

Configuration

```
R1:
interface FastEthernet0/0
 ip address 100.0.0.1 255.255.255.0

R2:
interface FastEthernet0/0
 ip address 100.0.0.2 255.255.255.0

R3:
interface FastEthernet0/0
 ip address 100.0.0.3 255.255.255.0

R4:
interface FastEthernet0/0
 ip address 100.0.0.4 255.255.255.0

R5:
interface FastEthernet0/0
 ip address 100.0.0.5 255.255.255.0

R6:
interface FastEthernet0/0
 ip address 100.0.0.6 255.255.255.0
```



```
SW1:
vtp domain PVLANS
vtp mode transparent
!
vlan 100
  private-vlan primary
  private-vlan association 1000,2000,3000
!
vlan 1000
  private-vlan community
!
vlan 2000
  private-vlan community
!
vlan 3000
  private-vlan isolated
!
interface FastEthernet0/1
 switchport private-vlan mapping 100 1000,2000,3000
 switchport mode private-vlan promiscuous
!
interface FastEthernet0/3
 switchport private-vlan host-association 100 1000
 switchport mode private-vlan host
!
interface FastEthernet0/5
 switchport private-vlan host-association 100 2000
 switchport mode private-vlan host
!
interface FastEthernet0/13
 switchport trunk encapsulation dot1q
 switchport mode trunk

SW2:
vtp domain PVLANS
vtp mode transparent
!
vlan 100
  private-vlan primary
  private-vlan association 1000,2000,3000
!
vlan 1000
  private-vlan community
!
vlan 2000
  private-vlan community
!
vlan 3000
  private-vlan isolated
!
interface FastEthernet0/2
 switchport private-vlan host-association 100 1000
 switchport mode private-vlan host
!
interface FastEthernet0/4
 switchport private-vlan host-association 100 2000
 switchport mode private-vlan host
```



```
!
interface FastEthernet0/6
 switchport private-vlan host-association 100 3000
 switchport mode private-vlan host
!
interface FastEthernet0/13
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

Verification

Note

The Private VLAN (PVLANs) feature is similar in theory to the Protected Ports feature, in which two or more ports can be in the same VLAN but cannot directly communicate at layer 2. Private VLANs expand this concept much further however, and allow very complex security policies that can span between multiple physical switches.

Private VLANs split a single broadcast domain, that is normally defined by a single VLAN, into multiple isolated broadcast subdomains, that are defined by primary VLAN and its secondary VLANs. In essence the feature allows us to configure VLANs inside a VLAN.

Design-wise this feature is commonly used in environments like shared ISP co-location, in which customers are on the same VLAN and same IP subnet, but should not communicate directly with each other, or in Multiple Dwelling Units (MDUs) such as hotels or office buildings, where two hotel rooms or offices may be in the same subnet and VLAN but should not communicate directly.

Pitfall

The Private VLAN feature requires VTP to run in transparent mode.

Note

While the theory of PVLANs is relatively straight forward, the implementation can be confusing due to the different terms that Cisco uses to describe VLANs and ports, and the syntax in which they are bound together.

First we must define the different port roles used in PVLANs. These are promiscuous ports, community ports, and isolated ports. Promiscuous ports are allowed to talk to all other ports within the VLAN. Isolated ports are only allowed to talk to promiscuous ports. Community ports are allowed to talk to other ports in their own community, but not ports in different communities, and can talk to any promiscuous ports.

Configuration-wise the port roles are defined by the interface's association to a primary VLAN, and one or more secondary VLANs. First the secondary VLANs are created, and defined as either community or isolated. Next the primary VLAN is defined, and the secondary VLANs are associated with the primary VLAN.

Next the command **`switchport mode private-vlan promiscuous`** or **`switchport mode private-vlan host`** is configured at the interface level. As you might guess the *promiscuous* option defines that the port role is promiscuous, while the *host* option defines that the port role is either community or isolated. Lastly the port is assigned to both the primary and secondary VLANs, which defines what other ports it can talk to.

In this case the link to R1 has the command **`switchport private-vlan mapping 100 1000,2000,3000`** configured, which means that it is a promiscuous port in the primary VLAN 100 and can talk to all ports in the secondary VLANs 1000, 2000, and 3000.

The link to R3 has the command **`switchport private-vlan host-association 100 1000`** configured, which means that is it a member of the primary VLAN 100 and the secondary VLAN 1000. Since VLAN 1000 was defined as a community VLAN, this implies that R3 can talk to all other ports in VLAN 1000 and any promiscuous ports belonging to VLAN 100.


```
Rack1SW1#show vlan private-vlan

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------
100     1000      community         Fa0/1, Fa0/3
100     2000      community         Fa0/1, Fa0/5
100     3000      isolated          Fa0/1

Rack1SW2#show vlan private-vlan

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------
100     1000      community         Fa0/2
100     2000      community         Fa0/4
100     3000      isolated          Fa0/6
```

Final verification for this configuration can be obtained by sending traffic to the broadcast address of 255.255.255.255 from all devices. As defined in the requirements R1 can talk to all routers, since it is a promiscuous port.

```
Rack1R1#ping 255.255.255.255 repeat 1

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 255.255.255.255, timeout is 2
seconds:

Reply to request 0 from 100.0.0.2, 4 ms
Reply to request 0 from 100.0.0.4, 4 ms
Reply to request 0 from 100.0.0.3, 4 ms
Reply to request 0 from 100.0.0.5, 4 ms
Reply to request 0 from 100.0.0.6, 4 ms
```

R2 can talk to R3, who is in the same community, and R1 who is a promiscuous port.

```
Rack1R2#ping 255.255.255.255 repeat 1

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 255.255.255.255, timeout is 2
seconds:

Reply to request 0 from 100.0.0.1, 4 ms
Reply to request 0 from 100.0.0.3, 4 ms
```


R3 can talk to R2, who is in the same community, and R1 who is a promiscuous port.

```
Rack1R3#ping 255.255.255.255 repeat 1

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 255.255.255.255, timeout is 2
seconds:

Reply to request 0 from 100.0.0.1, 4 ms
Reply to request 0 from 100.0.0.2, 4 ms
```

R4 can talk to R5, who is in the same community, and R1 who is a promiscuous port.

```
Rack1R4#ping 255.255.255.255 repeat 1

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 255.255.255.255, timeout is 2
seconds:

Reply to request 0 from 100.0.0.1, 4 ms
Reply to request 0 from 100.0.0.5, 4 ms
```

R5 can talk to R4, who is in the same community, and R1 who is a promiscuous port.

```
Rack1R5#ping 255.255.255.255 repeat 1

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 255.255.255.255, timeout is 2
seconds:

Reply to request 0 from 100.0.0.1, 4 ms
Reply to request 0 from 100.0.0.4, 4 ms
```

Since R6 is an isolated port it can only talk to the promiscuous port, R1.

```
Rack1R6#ping 255.255.255.255 repeat 1

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 255.255.255.255, timeout is 2
seconds:

Reply to request 0 from 100.0.0.1, 4 ms
```


