TOPICS COVERED:

- STP
- RAPID STP
- PORTFAST, ROOT GUARD, BPDU GUARD, BPDU FILTER
- MST
- DTP
- ETHERCHANNEL

# SPANNING TREE PROTOCOL (STP) 802.1D

- Spanning Tree Protocol (STP) enables switches to become aware of other switches through the advertisement and receipt of bridge protocol data units (BPDUs).
- STP builds a Layer 2 loop-free topology in an environment by temporarily blocking traffic on redundant ports.
- STP operates by selecting a specific switch as the master switch and running a tree-based algorithm to identify which redundant ports should not forward traffic.

STP has multiple flavours:

- 802.1D, which is the original specification
- Per-VLAN Spanning Tree (PVST) {Cisco Proprietary}
- Per-VLAN Spanning Tree Plus (PVST+) {Cisco Proprietary}
- 802.1W Rapid Spanning Tree Protocol (RSTP) {IEEE standard}
- 802.1S Multiple Spanning Tree Protocol (MST) {IEEE standard}

| |
|---|
| Catalyst switches now operate in PVST+, RSTP, and MST modes. All three of these modes are backward compatible with 802.1D. |

## IEEE 802.1D STP

The original version of STP comes from the IEEE 802.1D standards and provides support for ensuring a loop-free topology for one VLAN.

### 802.1D Port States

In the 802.1D STP protocol, every port transitions through the following states:

- Disabled: The port is in an administratively off position (that is, shut down).
- Blocking: The switch port is enabled, but the port is not forwarding any traffic to ensure that a loop is not created. The switch does not modify the MAC address table. It can only receive BPDUs from other switches. After 20 seconds, the switch port changes from the blocking state to the listening state.
- Listening: The switch port has transitioned from a blocking state and can now send or receive BPDUs. It cannot forward any other network traffic. The duration of the state correlates to the STP forwarding time. The next port state is learning. After 15 seconds, the switch port moves from the listening state to the learning state.
- Learning: The switch port can now modify the MAC address table with any network traffic that it receives. The switch still does not forward any other network traffic besides BPDUs. The duration of the state correlates to the STP forwarding time. The next port state is forwarding. After 15 seconds, the switch port moves from the learning state to the forwarding state.

- Forwarding: The switch port can forward all network traffic and can update the MAC address table as expected. This is the final state for a switch port to forward network traffic.

## STP Key Terminology

Several key terms are related to STP:

```
IOU2#sh spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     aabb.cc00.0100
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     aabb.cc00.0100
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------
Et0/0               Desg LRN 100       128.1    Shr
Et0/1               Desg LRN 100       128.2    Shr
Et0/2               Desg LRN 100       128.3    Shr
Et0/3               Desg LRN 100       128.4    Shr
Et1/0               Desg LRN 100       128.5    Shr
Et1/1               Desg LRN 100       128.6    Shr
Et1/2               Desg LRN 100       128.7    Shr
Et1/3               Desg LRN 100       128.8    Shr
Et2/0               Desg LRN 100       128.9    Shr
Et2/1               Desg LRN 100       128.10   Shr
Et2/2               Desg LRN 100       128.11   Shr
Et2/3               Desg LRN 100       128.12   Shr
Et3/0               Desg LRN 100       128.13   Shr
Et3/1               Desg LRN 100       128.14   Shr
Et3/2               Desg LRN 100       128.15   Shr
Et3/3               Desg LRN 100       128.16   Shr
```

- Root bridge: The root bridge is the most important switch in the Layer 2 topology. All ports are in a forwarding state. This switch is considered the top of the spanning tree for all path calculations by other switches. All ports on the root bridge are categorized as designated ports.

- Bridge protocol data unit (BPDU): This network packet is used for network switches to identify a hierarchy and notify of changes in the topology. A BPDU uses the destination MAC address 01:80:c2:00:00:00. There are two types of BPDUs:

- Configuration BPDU: This type of BPDU is used to identify the root bridge, root ports, designated ports, and blocking ports. The configuration BPDU consists of the following fields: STP type, root path cost, root bridge identifier, local bridge identifier, max age, hello time, and forward delay.
- Topology change notification (TCN) BPDU: This type of BPDU is used to communicate changes in the Layer 2 topology to other switches.
- Root path cost: This is the combined cost for a specific path toward the root switch.
- System priority: This 4-bit value indicates the preference for a switch to be root bridge. The default value is 32,768.
- System ID extension: This 12-bit value indicates the VLAN that the BPDU correlates to. The system priority and system ID extension are combined as part of the switch's identification of the root bridge.
- Root bridge identifier: This is a combination of the root bridge system MAC address, system ID extension, and system priority of the root bridge.
- Local bridge identifier: This is a combination of the local switch's bridge system MAC address, system ID extension, and system priority of the root bridge.
- Max age: This is the maximum length of time that passes before a bridge port saves its BPDU information. The default value is 20 seconds, but the value can be configured with the command spanning-tree vlan vlan-id max-age maxage. If a switch loses contact with the BPDU's source, it assumes that the BPDU information is still valid for the duration of the Max Age timer.
- Hello time: This is the time that a BPDU is advertised out of a port. The default value is 2 seconds, but the value can be configured to 1 to 10 seconds with the command spanning-tree vlan vlan-id hello-time hello-time.
- Forward delay: This is the amount of time that a port stays in a listening and learning state. The default value is 15 seconds, but the value can be changed to a value of 15 to 30 seconds with the command spanning-tree vlan vlan-id forward-time forward-time.

## BPDU

STP uses two types of BPDUs, configuration BPDUs and topology change notification (TCN) BPDUs.

### Configuration BPDUs:


DMA: Destination MAC address
SMA: Source MAC address
L/T: Frame length
LLC header: Logical link control header
Payload: BPDU data

| Fields | Byte |
|---|---|
| Protocol ID | 2 |
| Protocol version ID | 1 |
| BPDU type | 1 |
| Flags | 1 |
| Root ID | 8 |
| Root path cost | 4 |
| Bridge ID | 8 |
| Port ID | 2 |
| Message age | 2 |
| Max age | 2 |
| Hello time | 2 |
| Forward delay | 2 |

- Protocol ID—Fixed at 0x0000, which represents IEEE 802.1d.
- Protocol version ID—Spanning tree protocol version ID. The protocol version ID for STP is 0x00.
- BPDU type—Type of the BPDU. The value is 0x00 for a configuration BPDU.
- Flags—An 8-bit field indicates the purpose of the BPDU. The lowest bit is the Topology Change (TC) flag. The highest bit is the Topology Change Acknowledge (TCA) flag. All other bits are reserved.
- Root ID—Root bridge ID formed by the priority and MAC address of the root bridge.
- Root path cost—Cost of the path to the root bridge.
- Bridge ID—Designated bridge ID formed by the priority and MAC address of the designated bridge.
- Port ID—Designated port ID formed by the priority and global port number of the designated port.
- Message age—Age of the configuration BPDU while it propagates in the network.
- Max age—Maximum age of the configuration BPDU stored on the switch.
- Hello time—Configuration BPDU transmission interval.
- Forward delay—Delay for STP bridges to transit port state.

| BPDU Format | |
|---|---|
| **Field** | **Bits** |
| Protocol ID | 16 |
| Version | 8 |
| BPDU Type | 8 |
| Flags | 8 |
| Root ID | 64 |
| Root Path Cost | 32 |
| Bridge ID | 64 |
| Port ID | 16 |
| Message Age | 16 |
| Max Age | 16 |
| Hello Time | 16 |
| Forward Delay | 16 |
| **Default Timers** | |
| Hello | 2s |
| Forward Delay | 15s |
| Max Age | 20s |

BRIDGE ID = PRIORITY + MAC ADDRESS (Lowest Wins Always)

## 802.1D Port Types

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

1. Root port (RP): A network port that connects to the root bridge or an upstream switch in the spanning-tree topology. There should be only one root port per VLAN on a switch.

2. Designated port (DP): A network port that receives and forwards BPDU frames to other switches. Designated ports provide connectivity to downstream devices and switches. There should be only one active designated port on a link.

3. Blocking port: A network that is not forwarding traffic because of STP calculations.

# 802.1D STP Port Election

STP PORT ELECTION

1. Selecting the Root Bridge
2. Selecting the Root Port
3. Selecting Designated port & Non Designated Port

1. Selecting the Root Bridge

- The bridge with the Best (lowest) Bridge ID
- Bridge = Priority + MAC address of Switch
- Out of all Switches in Network, one is elected as a Root bridge

2. Selecting the Root Port

- Shortest part to reach to the Root bridge

3. Finding BLOCKED port!!!

- Every Non-root bridge looks the best way to go Root-bridge
    - Least Cost (Speed)
    - The Lowest forwarding Bridge ID (priority + mac addr.)
    - Lowest Forwarding Physical Port number

# Spanning Tree Path Cost

The interface STP cost is an essential component for root path calculation because the root path is found based on the cumulative interface STP cost to reach the root bridge

1. The interface STP cost was originally stored as a 16-bit value with a reference value of 20 Gbps.
2. As switches have developed with higher-speed interfaces, 20 Gbps might not be enough. Another method, called long mode, uses a 32-bit value and uses a reference speed of 20 Tbps.

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

- Devices can be configured with the long-mode interface cost with the command spanning-tree pathcost method long
- The entire Layer 2 topology should use the same setting for every device in the environment to ensure a consistent topology.

# RAPID SPANNING TREE PROTOCOL (RSTP) 802.1W

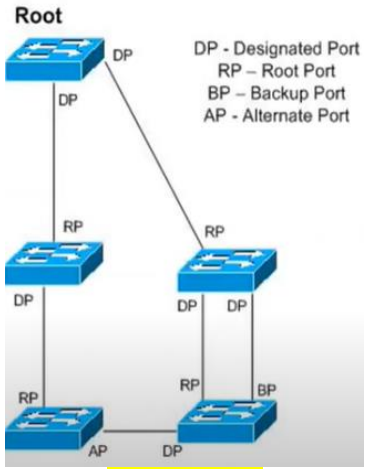
Inbuilt features of cisco proprietary like Portfast, Uplinkfast, Backbonefast

## RSTP (802.1W) Port States

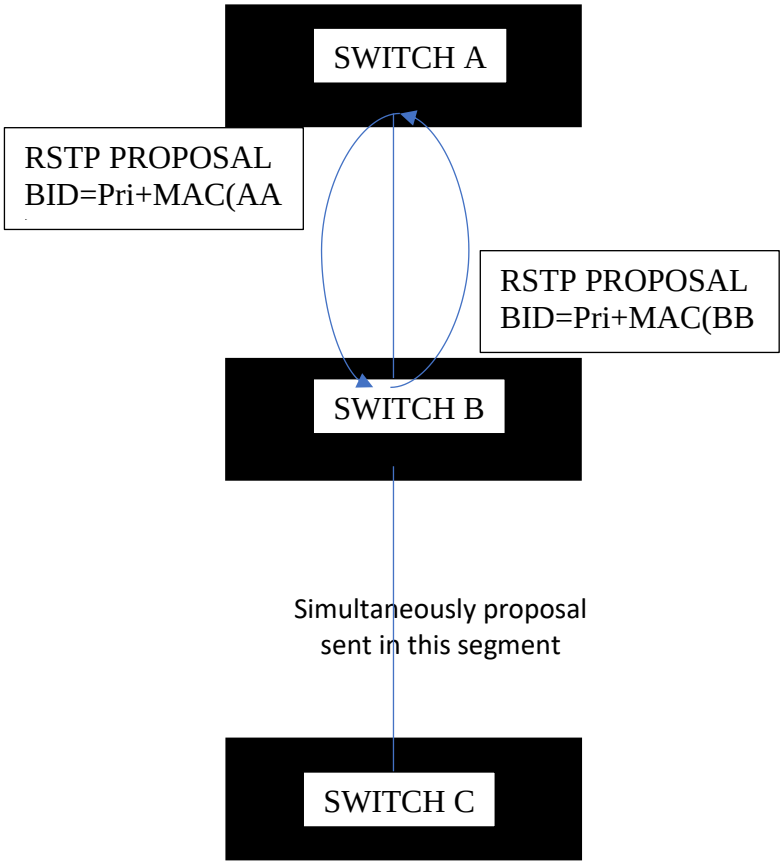
1. Discarding: The switch port is enabled, but the port is not forwarding any traffic to ensure that a loop is not created. This state combines the traditional STP states disabled, blocking, and listening.
2. Learning: The switch port modifies the MAC address table with any network traffic it receives. The switch still does not forward any other network traffic besides BPDUs. 1 second for transition.
3. Forwarding: The switch port forwards all network traffic and updates the MAC address table as expected. This is the final state for a switch port to forward network traffic.

## RSTP (802.1W) Port Roles

1. Root port (RP): A network port that connects to the root switch or an upstream switch in the spanning-tree topology. There should be only one root port per VLAN on a switch.
2. Designated port (DP): A network port that receives and forwards frames to other switches. Designated ports provide connectivity to downstream devices and switches. There should be only one active designated port on a link.
3. Alternate port: Alternate port is the port that will be promoted to root if the current root port fails. (same as Uplinkfast) when direct link to RB fails
4. Backup port: A network port that provides link redundancy toward the current root switch. backup port is a port that is connected to a LAN segment where the same switch has already a better port. A backup port exists only when multiple links connect between the same switches. (same as backbonefast)

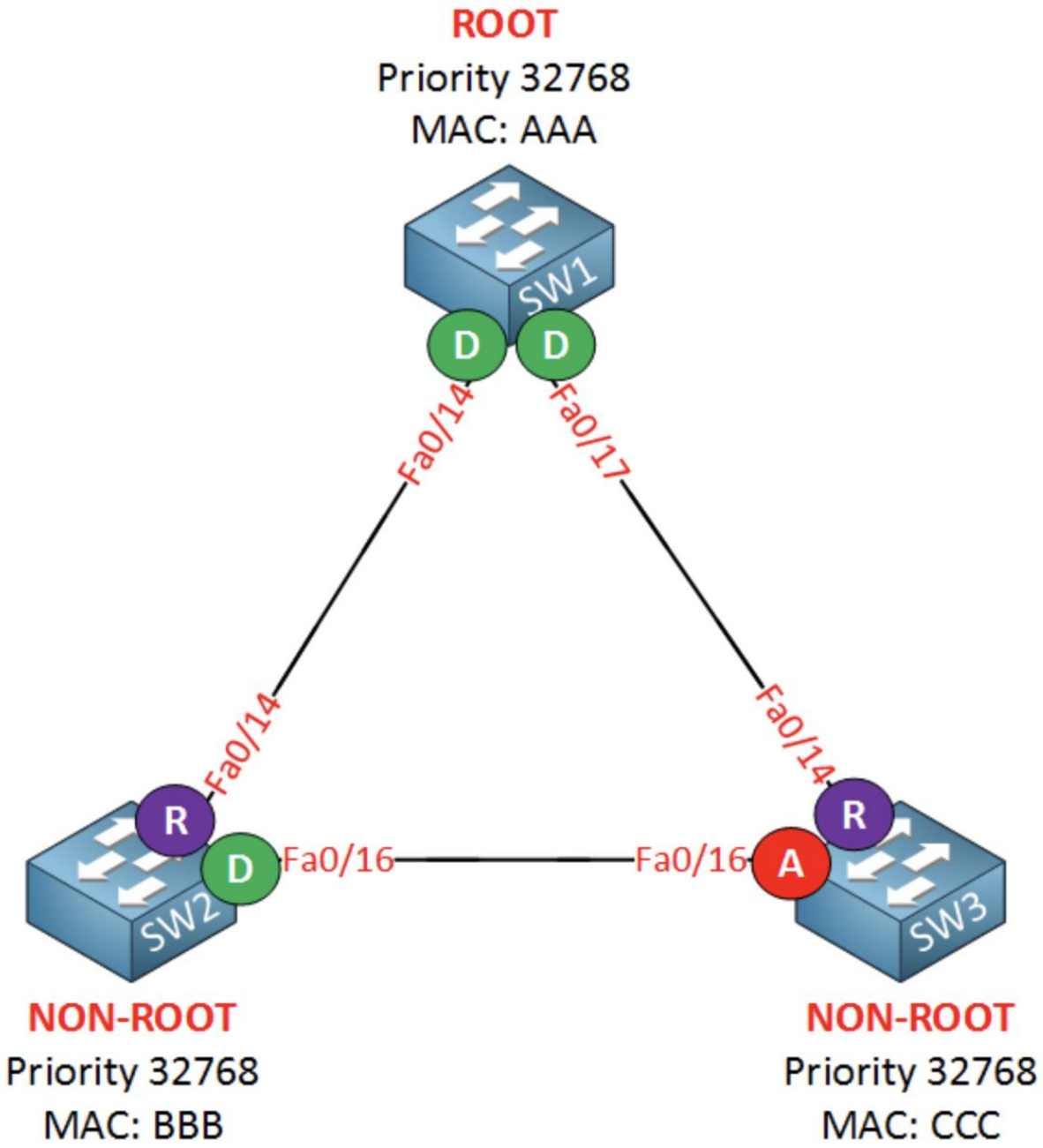



SCENERIO #1

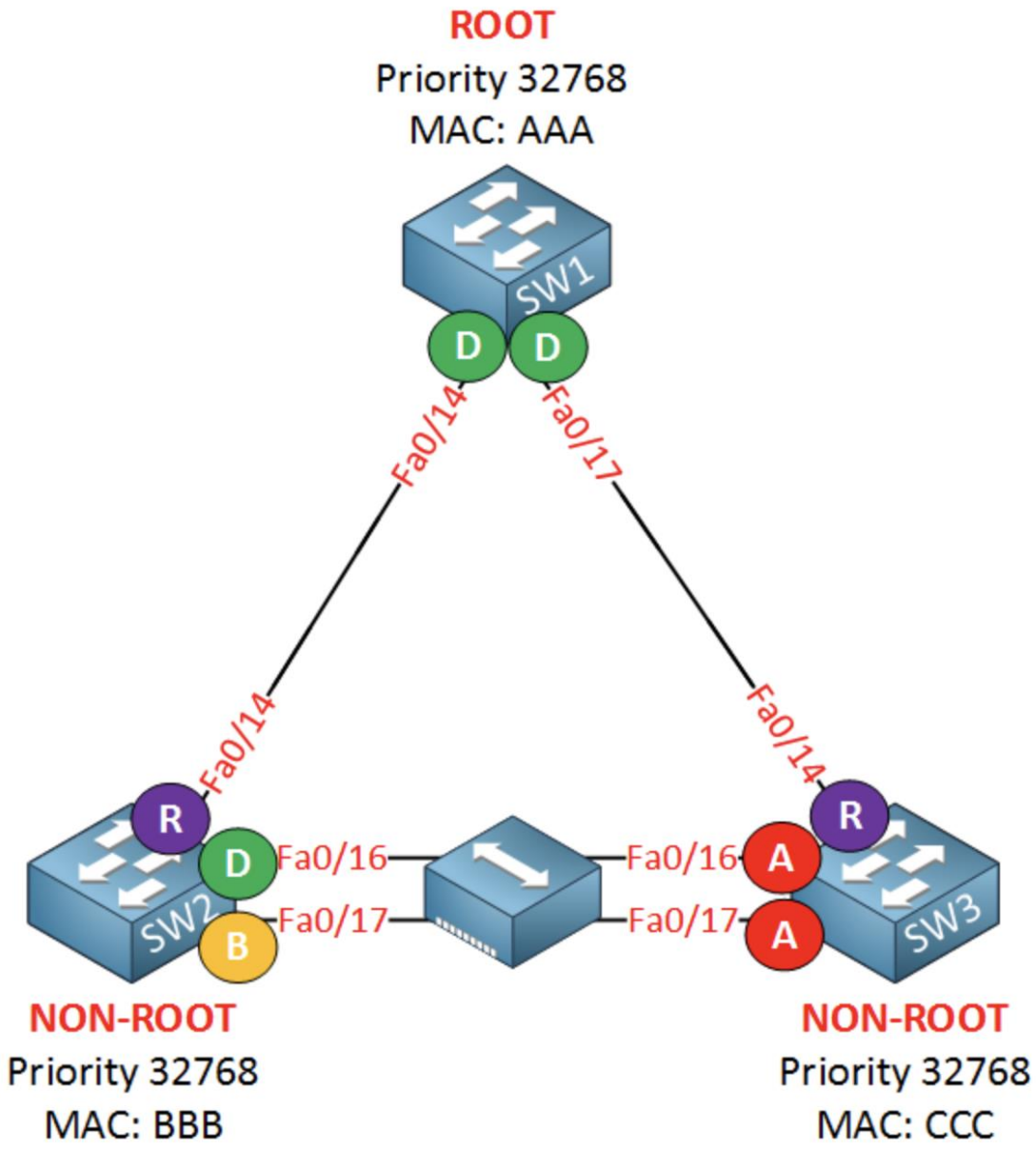

SWITCH A
RSTP PROPOSAL
BID=Pri+MAC(AA
RSTP PROPOSAL
BID=Pri+MAC(BB
SWITCH B
Simultaneously proposal
sent in this segment
SWITCH C

SCENERIO #2

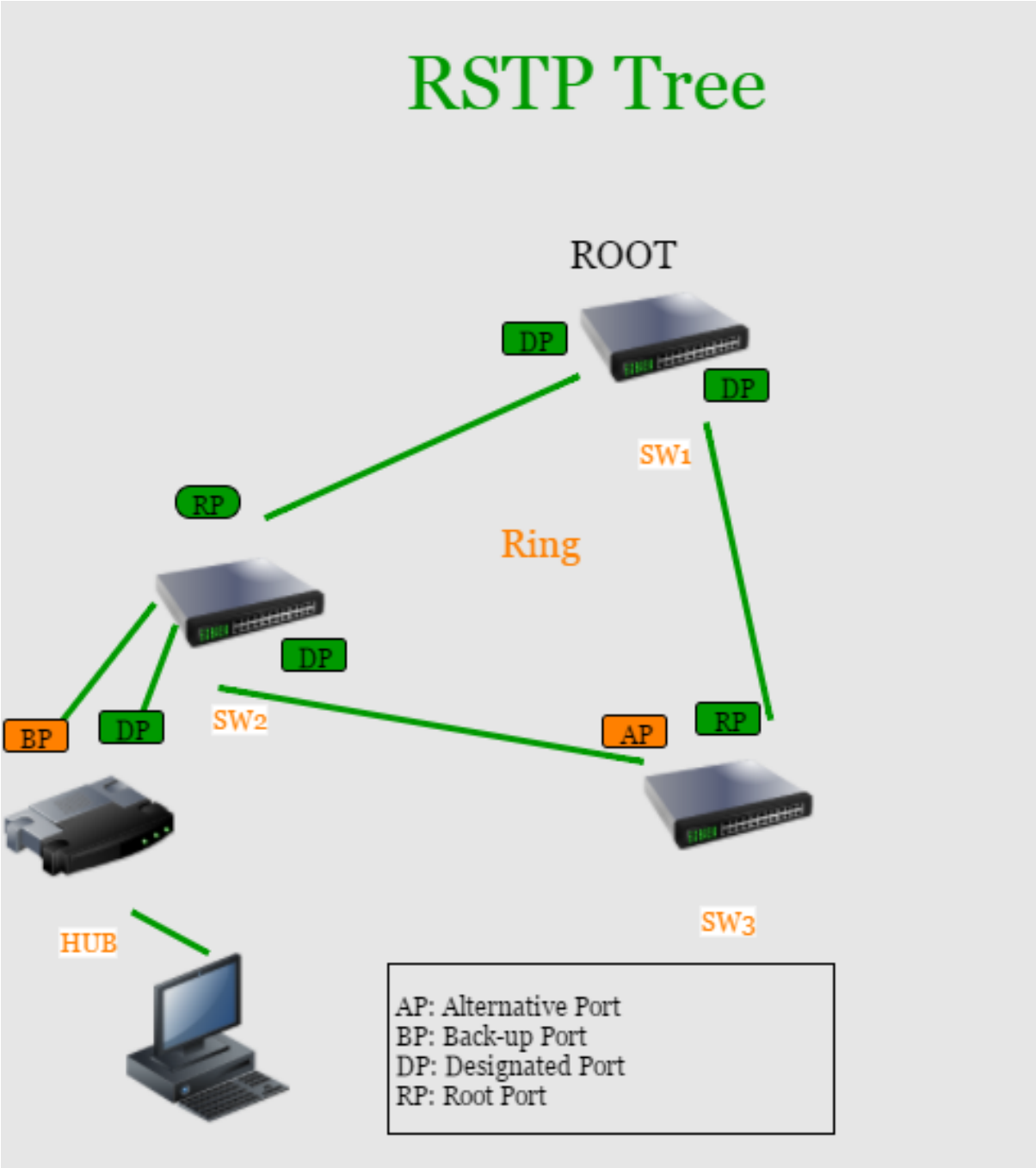
SW3_Fa0/16 = Alternate Port (equal to Blocking port)



SW3_Fa0/16 & Fa0/17 = Alternate Port (equal to Blocking port)
SW2_Fa0/16 = DP and SW2_Fa0/17 = Backup port



SCENERIO #3


RSTP Tree
ROOT
DP
DP
SW1
RP
Ring
DP
BP
DP
SW2
AP
RP
SW3
HUB
AP: Alternative Port
BP: Back-up Port
DP: Designated Port
RP: Root Port

## RSTP (802.1W) Port Types

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

## BDPU Difference in RSTP

1. In regular STP, BPDUs are originated by Root and relayed by each switch.
2. In RSTP, each switch originates BPDUs.
3. Hello = 2 sec, Dead = 6 sec in RSTP
   Whereas legacy STP has, Hello = 2sec and Dead = 20 sec

## RSTP Port Cost

| Data rate | STP cost (802.1D-1998) | RSTP cost (802.1W-2004, default value)[7]:154 |
|---|---|---|
| 4 Mbit/s | 250 | 5,000,000 |
| 10 Mbit/s | 100 | 2,000,000 |
| 16 Mbit/s | 62 | 1,250,000 |
| 100 Mbit/s | 19 | 200,000 |
| 1 Gbit/s | 4 | 20,000 |
| 2 Gbit/s | 3 | 10,000 |
| 10 Gbit/s | 2 | 2,000 |

1. Ideally the root bridge is placed on a core switch, and a secondary root bridge is designated to minimize changes to the overall spanning tree

2. Root bridge placement is accomplished by lowering the system priority on the root bridge to the lowest value possible, raising the secondary root bridge to a value slightly higher than that of the root bridge, and (ideally) increasing the system priority on all other switches.

3. This ensures consistent placement of the root bridge.

4. Modifying Priority: The priority is set with either of the following commands:

- spanning-tree vlan vlan-id priority priority: The priority is a value between 0 and 61,440, in increments of 4,096.

- spanning-tree vlan vlan-id root {primary | secondary} [diameter diameter]: This command executes a script that modifies certain values. The primary keyword sets the priority to 24,576, and the secondary keyword sets the priority to 28,672.

| |
|---|
| The optional diameter the maximum number of Layer 2 hops between a switch and the root bridge |

| |
|---|
| The best way to prevent erroneous devices from taking over the STP root role is to set the priority to 0 for the primary root switch and to 4096 for the secondary root switch. |

CLI Command to enable Rapid spanning-tree protocol

CLI COMMAND:
Switch(config)# spanning-tree mode rapid-pvst

```
IOU2#sh spanning-tree

VLAN0001
  Spanning tree enabled protocol rstp
  Root ID     Priority    32769
              Address     aabb.cc00.0100
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     aabb.cc00.0100
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------
Et0/0               Desg FWD 100       128.1    Shr
Et0/2               Desg FWD 100       128.3    Shr
Et0/3               Desg FWD 100       128.4    Shr
Et1/0               Desg FWD 100       128.5    Shr
Et1/1               Desg FWD 100       128.6    Shr
Et1/2               Desg FWD 100       128.7    Shr
Et1/3               Desg FWD 100       128.8    Shr
Et2/0               Desg FWD 100       128.9    Shr

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------

Et2/1               Desg FWD 100       128.10   Shr
Et2/2               Desg FWD 100       128.11   Shr
Et2/3               Desg FWD 100       128.12   Shr
Et3/0               Desg FWD 100       128.13   Shr
Et3/1               Desg FWD 100       128.14   Shr
Et3/2               Desg FWD 100       128.15   Shr
Et3/3               Desg FWD 100       128.16   Shr
```

Modifying STP Root Port and Blocked Switch Port Locations

spanning tree [vlan vlan-id] cost cost

Example:
IOU2(config)#int e0/2
IOU2(config-if)#spanning-tree cost 1

# STP TOPOLOGY TUNING & ENHANCEMENT

## Root Guard

Root guard is an STP feature that is enabled on a port-by-port basis; it prevents a configured port from becoming a root port.

Root guard prevents a downstream switch (often misconfigured or rogue) from becoming a root bridge in a topology.

Root guard functions by placing a port in an ErrDisabled state if a superior BPDU is received on a configured port. This prevents the configured DP with root guard from becoming an RP.

Root guard is enabled with the interface command spanning-tree guard root. Root guard is placed on designated ports toward other switches that should never become root bridges.

## STP Portfast

Interface based: spanning-tree portfast
Globally on all access ports: spanning-tree portfast default

Portfast can be enabled on trunk links with the command spanning-tree portfast trunk. However, this command should be used only with ports that are connecting to a single host (such as a server with only one NIC that is running a hypervisor with VMs on different VLANs). Running this command on interfaces connected to other switches, bridges, and so on can result in a bridging loop.

CLI Command to Enable "Portfast" on Access port:

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

## BPDU Guard

BPDU guard is a safety mechanism that shuts down ports configured with STP portfast upon receipt of a BPDU.

Assuming that all access ports have portfast enabled, this ensures that a loop cannot accidentally be created if an unauthorized switch is added to a topology.

BPDU guard is enabled globally on all STP portfast ports with the command
spanning-tree portfast bpduguard default

BPDU guard can be enabled or disabled on a specific interface with the command
spanning-tree bpduguard {enable | disable}.

```
SW1# configure terminal
SW1(config)# spanning-tree portfast bpduguard default
SW1(config)# interface gi1/0/8
SW1(config-if)# spanning-tree bpduguard disable
```

```
SW1# show interfaces status

SW1# show errdisable recovery
```

## BPDU Filter

BPDU filter simply blocks BPDUs from being transmitted out a port. BPDU filter can be enabled globally or on a specific interface

```
CLI Command:
show spanning-tree interface gi1/0/2 detail | in BPDU|Bpdu|Ethernet
```

BPDUGuard will put a switchport into err-disabled mode if any BPDU being received.

BPDU Filtering at the global level will work with Portfast interfaces, and simply kick them out of portfast if a BPDU is received.

BPDU Filtering configured on the interface level will COMPLETELY stop send/receive BPDU, and if you plug in two switches then you may have a loop because they don't 'see' each other as a problem.

## COMMAND REFERENCE

| Task | Command Syntax |
|---|---|
| Set the STP max age | spanning-tree vlan vlan-id max-age |
| Set the STP hello interval | spanning-tree vlan vlan-id hello-time hello-time |
| Set the STP forwarding delay | spanning-tree vlan vlan-id forward-time forward-time |
| Display the STP root bridge and cost | show spanning-tree root |

| | |
|---|---|
| Display the STP information (root bridge, local bridge, and interfaces) for one or more VLANs | show spanning-tree [vlan vlan-id] |
| Identify when the last TCN occurred and which port was the reason for it. | show spanning-tree [vlan vlan-id] detail |
| DEBUG Commands for STP | Debug spanning-tree events<br>Debug spanning-tree bpdu<br>Debug spanning-tree config |

QUIZ 1:

1. How many different BPDU types are there?
1. One
2. Two
3. Three
4. Four

2. What attributes are used to elect a root bridge?
1. Switch port priority
2. Bridge priority
3. Switch serial number
4. Path cost

3. The original 802.1D specification assigns what value to a 1 Gbps interface?
1. 1
2. 2
3. 4
4. 19

4. All of the ports on a root bridge are assigned what role?
1. Root port
2. Designated port
3. Superior port
4. Master port

5. Using default settings, how long does a port stay in the listening state?
1. 2 seconds
2. 5 seconds
3. 10 seconds
4. 15 seconds

6. Upon receipt of a configuration BPDU with the topology change flag set, how do the downstream switches react?
1. By moving all ports to a blocking state on all switches
2. By flushing out all MAC addresses from the MAC address table
3. By temporarily moving all non-root ports to a listening state

4. By flushing out all old MAC addresses from the MAC address table
5. By updating the Topology Change version flag on the local switch database

7. Which of the following is not an RSTP port state?
1. Blocking
2. Listening
3. Learning
4. Forwarding

8. True or false: In a large Layer 2 switch topology, the infrastructure must fully converge before any packets can be forwarded.
1. True
2. False

9. True or false: In a large Layer 2 switch topology that is running RSTP, the infrastructure must fully converge before any packets can be forwarded.
1. True
2. False

Answers to the "Do I Know This Already?" quiz:

1 B

2 B

3 C

4 B

5 D

6 D

7 A, B

8 B

9 B

QUIZ 2:

1. A switch's STP priority can be configured in increments of _____.
1. 1
2. 256
3. 2048
4. 4096

2. True or false: The advertised path cost includes the advertising link's port cost as part of the configuration BPDU advertisement.
1. True
2. False

3. True or false: The switch port with the lower STP port priority is more preferred.
1. True
2. False

4. What happens to a switch port when a BPDU is received on it when BPDU guard is enabled on that port?

1. A message syslog is generated, and the BPDU is filtered.
2. A syslog message is not generated, and the BPDU is filtered.
3. A syslog message is generated, and the port is sent back to a listening state.
4. A syslog message is generated, and the port is shut down.

5. Enabling root guard on a switch port does what?

1. Upon receipt of an inferior BPDU, the port is shut down.
2. Upon receipt of a superior BPDU, the port is shut down.
3. Upon receipt of an inferior BPDU, the BPDU is filtered.
4. When the root port is shut down, only authorized designated ports can become root ports.

6. UDLD solves the problem of _____.

1. time for Layer 2 convergence
2. a cable sending traffic in only one direction
3. corrupt BPDU packets
4. flapping network links

Answers to the “Do I Know This Already?” quiz:

1 D

2 B

3 A

4 D

5 B

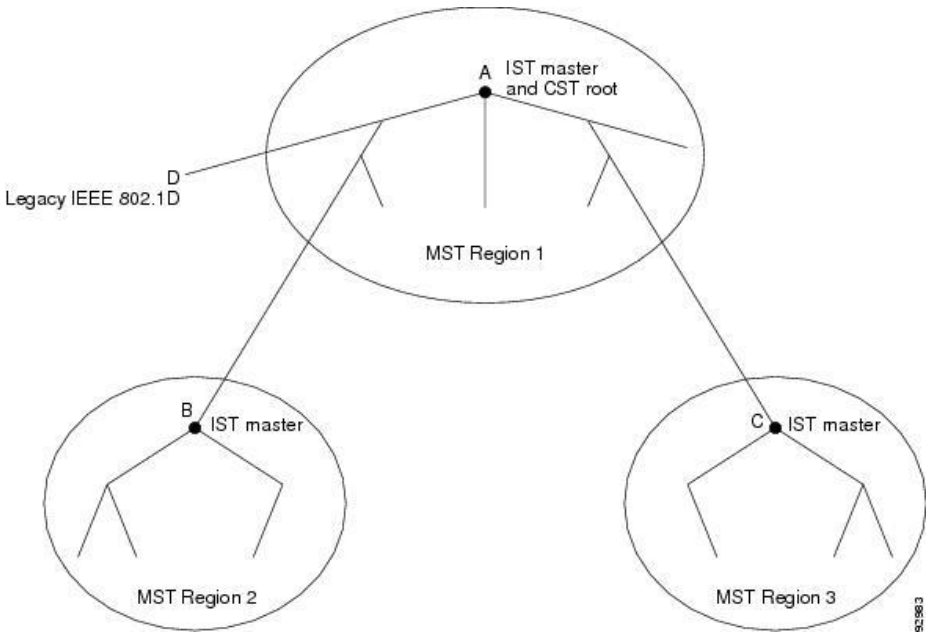
6 B

# MULTIPLE SPANNING PROTOCOL (MSTP) 802.1S

## *MSTP Features*

1. MSTP, when some ports blocked for specific VLANs the same ports may be forwarded for another VLANs.
2. **MSTP** have instances but in every instance, you can have multiple VLANs mapped in this instance so the Switch configured with **MSTP** can send one **BPDU** message contain all info about **every instance** contained in **MST Group.**
3. Standard maximum number of instances that can made by **MSTP** are **64** instances/Switch containing the default instance 0.
4. MSTP can suitable for working with all vendors.
5. For every region there is a Root Bridge called **IST Master** (Internal Spanning Tree) that elected to result loop free region; **for** every connected region there is Root Bridge called **CIST Root** (Common and Internal Spanning Tree) to result loop free between regions.
6. MST supports some of the RSTP extensions in MSTP as follows:

– UplinkFast and BackboneFast are not available in MST mode; they are part of RSTP.
– PortFast is supported
– BPDU filter and BPDU guard are supported in MST mode



## *MSTP Special Instance 0*

1. This instance called **Internal Spanning-Tree** IST.
2. This instance will be existing even if no other MST instance are created.
3. Without any additional configurations all VLANs will map to this instance.
4. This instance is the only instance that work with **STP** switches run out of **MST** region {interoperability}.

## *MSTP Port Cost*

| *Link Speed* | *Recommended Cost* |
|---|---|
| *1 Mbps* | *200 000 000* |
| *10 Mbps* | *20 000 000* |
| *100 Mbps* | *2 000 000* |
| *1 Gbps* | *20 000* |
| *10 Gbps* | *2000* |
| *100 Gbps* | *200* |
| *1 Tbps* | *20* |
| *10 Tbps* | *2* |

## *MSTP Terminology*

1. IST MASTER: Inside a region all switches elect this Switch to be the master inside this region.
2. CIST Root: Between regions the IST Master elect this Switch to be the master of entire topology.
3. New port role called **Master port**: Provides connectivity from the Region to a CIST Root that lies outside the Region
4. Alternate or Backup: Provides connectivity if other Bridges, Bridges ports or LANs fail or are erased.

```
Interface        Role Sts Cost      Prio.Nb
---------------- ---- --- --------- -------
Gi0/0            Mstr FWD 20000     128.1
```

## *MSTP Configuration*

Step #1: Define STP mode "MST"

Step #2: (Optional) Define the MST instance priority, using one of two methods:
**spanning-tree mst** instance-number **priority** priority
(The priority is a value between 0 and 61,440, in increments of 4096.)

**spanning-tree mst** instance-number **root {primary | secondary}[diameter** diameter]
(The **primary** keyword sets the priority to 24,576, and the **secondary** keyword sets the priority to 28,672.)

Step #3: Associate VLANs to an MST instance. By default, all VLANs are associated to the MST 0 instance.
The MST configuration submode must be entered with the command **spanning-tree mst configuration**.
Then the VLANs are assigned to a different MST instance with the command **instance** instance-number **vlan** vlan-id.

Step #4: Specify the mst version number. The MST version number must match for all switches in the same MST region. The MST version number is configured with the submode configuration command **revision** version.

Step #5: (Optional) Define the MST region name. MST regions are recognized by switches that share a common name. By default, a region name is an empty string. The MST region name is set with the command **name** mst-region-name.

**Example:**

```
SW1(config)# spanning-tree mode mst
SW1(config)# spanning-tree mst 0 root primary
SW1(config)# spanning-tree mst 1 root primary
SW1(config)# spanning-tree mst 2 root primary

SW1(config)# spanning-tree mst configuration
SW1(config-mst)# name ENTERPRISE_CORE
SW1(config-mst)# revision 2
SW1(config-mst)# instance 1 vlan 10,20
SW1(config-mst)# instance 2 vlan 99
```

```
SW2# show spanning-tree mst configuration
Name      [ENTERPRISE_CORE]
Revision  2     Instances configured 3

Instance  Vlans mapped
--------  ----------------------------------------------------------------
0         1-9,11-19,21-98,100-4094
1         10,20
2         9
```

## *MST Tuning*

MST supports the tuning of port cost and port priority.

**Port Cost:**

The interface configuration command **spanning-tree mst** *instance-number* **cost** *cost* sets the interface cost.

```
SW3# show spanning-tree mst 0
! Output omitted for brevity
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------
Gi1/0/1          Root FWD 20000     128.1    P2p
Gi1/0/2          Altn BLK 20000     128.2    P2p
Gi1/0/5          Desg FWD 20000     128.5    P2p
```

SW3# **configure term**
Enter configuration commands, one per line. End with CNTL/Z.
SW3(config)# **interface gi1/0/1**
SW3(config-if)# **spanning-tree mst 0 cost 1**

```
SW3# show spanning-tree mst 0
! Output omitted for brevity
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------
Gi1/0/1          Root FWD 1         128.1    P2p
Gi1/0/2          Desg FWD 20000     128.2    P2p
Gi1/0/5          Desg FWD 20000     128.5    P2p
```

**Port Priority:**

The interface configuration command **spanning-tree mst** *instance-number* **port-priority** *priority*sets the interface priority.

```
SW4# configure term
Enter configuration commands, one per line. End with CNTL/Z.
SW4(config)# interface gi1/0/5
SW4(config-if)# spanning-tree mst 0 port-priority 64
```

```
SW4# show spanning-tree mst 0
! Output omitted for brevity
##### MST0    vlans mapped:   1-9,11-19,21-98,100-4094
Interface                Role Sts Cost      Prio.Nbr Type
----------------         ---- --- --------- -------- --------------------
Gi1/0/2                  Root FWD 20000     128.2    P2p
Gi1/0/5                  Desg FWD 20000     64.5     P2p
Gi1/0/6                  Desg FWD 20000     128.6    P2p
```

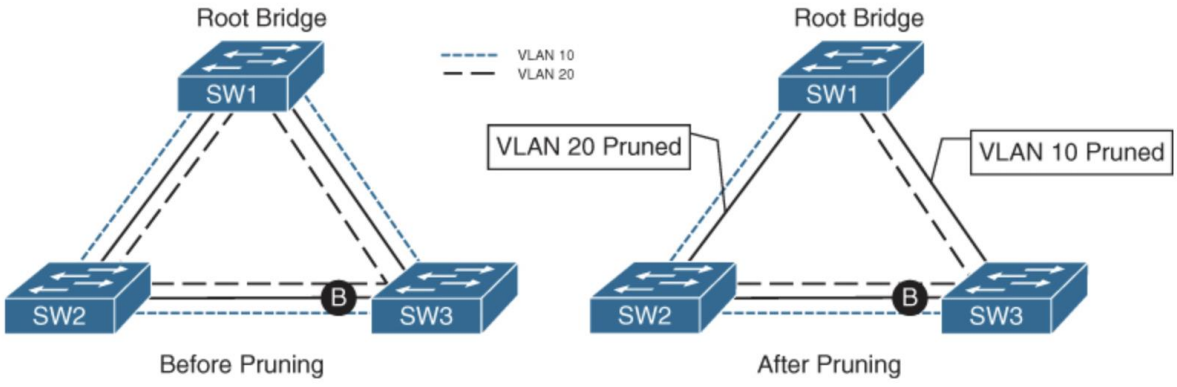
## *Common MST Misconfigurations*

There are two common misconfigurations within the MST region that network engineers should be aware of:

1. VLAN assignment to the Instances must be consistent
2. Trunk link pruning:

Pruning of VLANs on a trunk link is a common practice for load balancing. However, it is important that pruning of VLANs does not occur for VLANs in the same MST on different network links.

Sample topology (given below) in which VLAN 10 and VLAN 20 are throughout the entire topology. A junior network engineer has pruned VLANs on the trunk links between SW1 to SW2 and SW1 to SW3 to help load balance traffic. Shortly after implementing the change, users attached to SW1 and SW3 cannot talk to the servers on SW2. This is because while the VLANs on the trunk links have changed, the MSTI topology. A simple rule to follow is to only prune all the VLANs in the same MSTI for a trunk link.



## COMMAND REFERENCE

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

## Quiz

**1.** Which of the following issues does MST solve? (Choose two.)

1. Enables traffic load balancing for specific VLANs
2. Reduces the CPU and memory resources needed for environments with large numbers of VLANs
3. Overcomes MAC address table scaling limitations for environments with large numbers of devices
4. Detects issues with cabling that transmits data in one direction
5. Prevents unauthorized switches from attaching to the Layer 2 domain

**2.** With MST, VLANs are directly associated with _____.

1. areas
2. regions
3. instances
4. switches

**3.** What do CST and 802.1D have in common?

1. They support only one topology.
2. They support multiple topologies.
3. They allow for load balancing of traffic across different VLANs.
4. They provide switch authentication so that inter-switch connectivity can occur.

**4.** True or false: The MST root bridge advertises the VLAN-to-instance mappings to all other MST switches.

1. True
2. False

**5.** True or false: The MST configuration version is locally significant.

1. True
2. False

**6.** True or false: The MST topology can be tuned for root bridge placement, just like PVST+ and RSTP.

1. True
2. False

**7.** MST regions can interact with PVST+/RSTP in which of the following ways? (Choose two.)

1. The MST region is the root bridge for all VLANs.
2. The MST region is the root bridge for some VLANs.
3. The PVST+/RSTP topology is the root bridge for all VLANs.
4. The PVST+/RSTP topology is the root bridge for some VLANs.

**Answers to the "Do I Know This Already?" quiz:**

**1** A, B

**2** C

**3** A

**4** B

**5** B

**6** A

**7** A, C

# DYNAMIC TRUNKING PROTOCOL (DTP)

## *DTP FEATURES*

- DTP is cisco proprietary
- Dynamic trunk ports are established by the switch port sending Dynamic Trunking Protocol (DTP) packets to negotiate whether the other end can be a trunk port.
- If both ports can successfully negotiate an agreement, the port will become a trunk switch port.
- DTP advertises itself every 30 seconds to neighbors so that they are kept aware of its status.
- DTP requires that the VTP domain match between the two switches.
- DTP is a play and plug features for enabling "Trunking" on second side switch.

## *3 MODES OF DTP*

- **Trunk:** This mode statically places the switch port as a trunk and advertises DTP packets to the other end to establish a dynamic trunk. Place a switch port in this mode with the command **switchport mode trunk**.

- **Dynamic desirable:** In this mode, the switch port acts as an **access port**, but it listens for and advertises DTP packets to the other end to establish a dynamic trunk. If it is successful in negotiation, the port becomes a trunk port. Place a switch port in this mode with the command **switchport mode dynamic desirable**.

- **Dynamic auto:** In this mode, the switch port acts as an access port, but it only listens for DTP packets. It responds to DTP packets and, upon successful negotiation, the port becomes a trunk port. Place a switch port in this mode with the command **switchport mode dynamic auto**.

| | | Switch 2 | | |
|---|---|---|---|---|
| | | **Trunk** | **Dynamic Desirable** | **Dynamic Auto** |
| **Switch 1** | Trunk | ✓ | ✓ | ✓ |
| | Dynamic desirable | ✓ | ✓ | ✓ |
| | Dynamic auto | ✓ | ✓ | X |

A trunk link can successfully form in almost any combination of these modes unless both ends are configured as dynamic auto.

## *DTP CONFIGURATIONS*

Configure DTP AUTO on Switch Interface

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

Configure DTP Desirable on Switch Interface

```
SW2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW2(config)# interface gi1/0/1
SW2(config-if)# switchport mode dynamic desirable
```

The trunk port status is verified with the command **show interface** [*interface-id*] **trunk**

```
SW1# show interfaces trunk
! Output omitted for brevity

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

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

The mode for a statically configured trunk port is on.

## *DTP NONEGOTIATE*

A static trunk port attempts to establish and negotiate a trunk port with a neighbor by default. However, the interface configuration command **switchport nonegotiate** prevents that port from forming a trunk port with a dynamic desirable or dynamic auto switch port.

The setting is then verified by looking at the switch port status. Notice that Negotiation of Trunk now displays as Off.

```
SW1# show run interface gi1/0/2
Building configuration...
!
interface GigabitEthernet1/0/2
 switchport mode trunk
 switchport nonegotiate
end
```

```
SW1# show interfaces gi1/0/2 switchport | i Trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: ALL
```

## *DTP ATTACKS*

ATTACK#1
The DTP protocol is unauthenticated which means that a station can send false DTP packets, pretending to be a switch.

If the switchport is configured as a dynamic port, an attacker can lure the switchport to become a trunk port and he will gain access to all VLANs allowed on that trunk.

Therefore, after a network has been installed, it is the best practice to set the mode statically and deactivate the DTP protocol on a port using the command **switchport nonegotiate** (this command is necessary only for trunk ports, as the static access ports do not send DTP packets automatically).

Best Practice:
As a best practice, configure both ends of a link as a fixed port type (using **switchport mode access** or **switchport mode trunk**) to remove any uncertainty about the port's operations.

ATTACK#2
KALI LINX ATTACK DEMONSTRATION

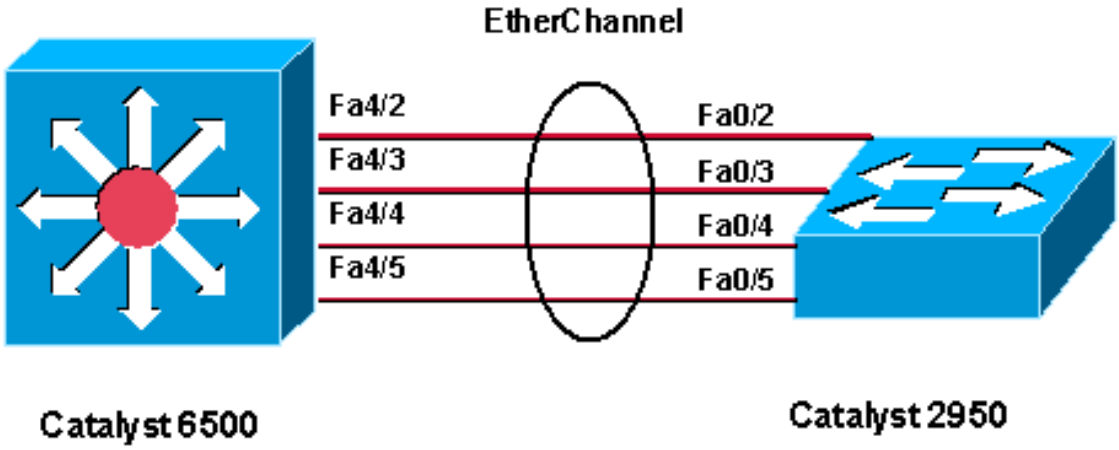
## *PREVENT DTP ATTACKS*

```
Switch1(config)# interface gigabitethernet 0/3

Switch1(config-if)# switchport mode access

Switch1(config-if)# exit
```

```
Switch1(config)# interface gigabitethernet 0/4

Switch1(config-if)# switchport trunk encapsulation dot1q

Switch1(config-if)# switchport mode trunk

Switch1(config-if)# switch port nonegotiate
```

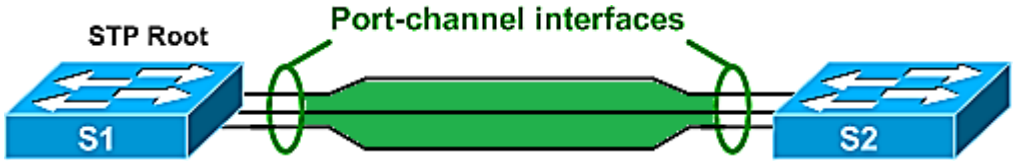
# ETHERCHANNEL BUNDLE

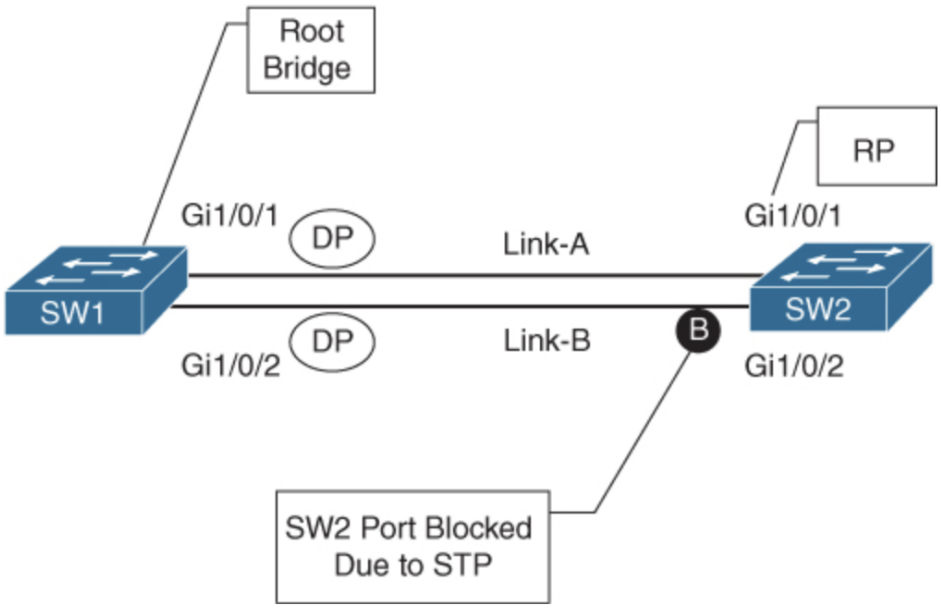
- Etherchannel, which is also, known as link aggregation or port channel.
- Etherchannel bundle multiple physical links into a single logical link or port.
- Technique to combine multiple physical link to make a single logical link.
- Etherchannel can be used for load balancing or load sharing & fault tolerance.
- Etherchannel also known as bundling, port channel or EtherChannel bundle.
- EtherChannel or port channel have three modes LACP, PAgP and ON mode.
- Etherchannel Increased bandwidth, increased availability and Load Sharing.
- Etherchannel provide Auto Configuration, Faster convergence & cheaper solution.
- Etherchannel require same duplex, speed, native, allowed VLANs & switchport mode.
- Etherchannel will load share equally distributed across all links bundled in Etherchannel.
- In EtherChannel Load balancing is done based on flows, not based on packets.
- By default, Layer 2 packets are distributed on source & destination MAC address
- By default, Layer 3 packets based on source and destination IP address.
- Maximum of eight interfaces can be aggregated to form a single logical link.
- Channel must be made up of minimum two ports and maximum 8 interfaces.
- EtherChannel or Port Channel can be configured either manually or dynamically.
- EtherChannel port groups can be run from Switch-to-Switch or Switch-to-Server.




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

Etherchannel is solution to avoid STP.



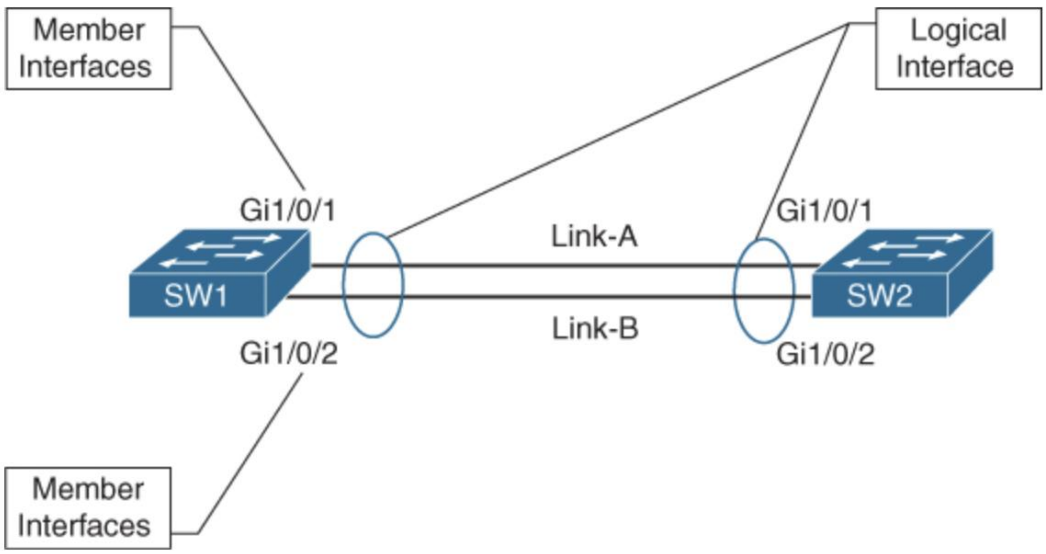



Fortunately, the physical links can be aggregated into a logical link called an EtherChannel bundle. The industry-based term for an EtherChannel bundle is *EtherChannel* (for short), or *port channel*, which is defined in the IEEE 802.3AD link aggregation specification.

The physical interfaces that are used to assemble the logical EtherChannel are called *member interfaces*.

EtherChannels can be used for either Layer 2 (access or trunk) or Layer 3 (routed) forwarding.

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



A primary advantage of using port channels is a **reduction in topology changes** when a member link line protocol goes up or down. In a traditional model, a link status change may trigger a Layer 2 STP tree calculation or a Layer 3 route calculation. A member link failure in an EtherChannel does not impact those processes, as long as one active member still remains up.

A switch can successfully form an EtherChannel by statically setting them to an **on state or by using a dynamic link aggregation protocol** to detect connectivity between devices. Most network engineers prefer to use a dynamic method as it provides a way to ensure end-to-end connectivity between devices across all network links.

## *ETHERCHANNEL MODES*

1. PAgP
2. LACP
3. On

```
Switch(config-if)#channel-group 10 mode ?
  active      Enable LACP unconditionally
  auto        Enable PAgP only if a PAgP device is detected
  desirable   Enable PAgP unconditionally
  on          Enable Etherchannel only
  passive     Enable LACP only if a LACP device is detected
```

## *PAgP (Port Aggregation Protocol):*

- PAgP stand for Port Aggregation Protocol & cisco proprietary protocol.
- PAgP automatically convert individual ports into a single logical link.
- There are two modes for the Port Aggregation Protocol (PAgP).
- **Auto**: In this PAgP mode, the interface does not initiate an EtherChannel to be established and does not transmit PAgP packets out of it. If an PAgP packet is received from the remote switch, this interface responds and then can establish a PAgP adjacency. If both devices are PAgP auto, a PAgP adjacency does not form.
- **Desirable**: In this PAgP mode, an interface tries to establish an EtherChannel and transmit PAgP packets out of it. Active PAgP interfaces can establish a PAgP adjacency only if the remote interface is configured to auto or desirable.
- Having two ends of a PAgP link in auto mode will not result in a PAgP link.
- Because neither side will negotiate to bring up the PAgP EtherChannel.
- PAgP advertises messages with the multicast MAC address 0100:0CCC:CCCC and the protocol code 0x0104
- You can have up to eight ports in a single PAgP EtherChannel or logical link.
- All ports in PAgP EtherChannel must have the same speed & duplex settings.

## *LACP (Link Aggregation Control Protocol):*

- Link Aggregation Control Protocol is the open standard 802.3ad.
- Combine multiple links into a single logical link to increase bandwidth.
- All links participating in a single logical link must have the same settings.
- All ports participating must have the same speed and duplex configuration.
- All ports participating in single logical link must be in the same VLAN.
- All ports participating in single logical link must be in same operational mode.
- No ports participating in single logical link can have SPAN configured.
- Can have up to 16 ports in LACP EtherChannel only 8 can be active at one time.
- The LACP protocol can be configured in either passive or active mode.
- **Active:** In this LACP mode, an interface tries to establish an EtherChannel and transmit LACP packets out of it. Active LACP interfaces can establish an LACP adjacency only if the remote interface is configured to active or passive.
- **Passive:** In this LACP mode, an interface does not initiate an EtherChannel to be established and does not transmit LACP packets out of it. If an LACP packet is received from the remote switch, this interface responds and then can establish an LACP adjacency. If both devices are LACP passive, an LACP adjacency does not form.
- LACP advertises messages with the multicast MAC address 0180:C200:0002.

## *EtherChannel Static (Manual):*

- Switchports can be configured to bypass LACP or PAgP protocols.
- It is simply changing the mode to ON both sides of the Switches.
- This mode is used to manually configure EtherChannel or Port Channel.
- This mode can be used if device on other end does not support PAgP or LACP.

The logical interface can be viewed with the command **show interface port-channel** *port-channel-id*.

```
SCOTSW01# show interfaces port-channel 1
Port-channel1 is up, line protocol is up (connected)
  Hardware is EtherChannel, address is 0062.ec9d.c501 (bia 0062.ec9d.c501)
  MTU 1500 bytes, BW 2000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 1000Mb/s, link type is auto, media type is
  input flow-control is off, output flow-control is unsupported
  Members in this channel: Gi1/0/1 Gi1/0/2
```

**show interface port-channel** *port-channel-id* command on SW1. Notice that the bandwidth is 2 Gbps and correlates to the two 1 Gbps interfaces in the **show etherchannel summary** command.

## *Troubleshooting EtherChannel Bundles*

It is important to remember that a port channel is a logical interface, so all the member interfaces must have the same characteristics. If they do not, problems will occur.

As a general rule, when configuring port channels on a switch, place each member interface in the appropriate switch port type (Layer 2 or Layer 3) and then associate the interfaces to a port channel. All other port-channel configuration is done via the port-channel interface.

The following configuration settings must match on the member interfaces:

- **Port type:** Every port in the interface must be consistently configured to be a Layer 2 switch port or a Layer 3 routed port.
- **Port mode:** All Layer 2 port channels must be configured as either access ports or trunk ports. They cannot be mixed.
- **Native VLAN:** The member interfaces on a Layer 2 trunk port channel must be configured with the same native VLAN, using the command **switchport trunk native vlan** *vlan-id*.
- **Allowed VLAN:** The member interfaces on a Layer 2 trunk port channel must be configured to support the same VLANs, using the command **switchport trunk allowed** *vlan-ids*.
- **Speed:** All member interfaces must be the same speed.
- **Duplex:** The duplex must be the same for all member interfaces.
- **MTU:** All Layer 3 member interfaces must have the same MTU configured. The interface cannot be added to the port channel if the MTU does not match the MTU of the other member interfaces.
- **Load interval:** The load interval must be configured the same on all member interfaces.
- **Storm control:** The member ports must be configured with the same storm control settings on all member interfaces.

Storm control compares broadcast, multicast, and unknown unicast traffic regularly with their respective traffic thresholds on an Ethernet interface. For each type of traffic, storm control provides a lower threshold and an upper threshold.

Depending on your configuration, when a particular type of traffic exceeds its upper threshold, the interface performs either of the following operations:

- **Blocks this type of traffic and forwards other types of traffic**
- **Goes down automatically**

**storm-constrain interval** *interval*

**interface** *interface-type interface-number*
**storm-constrain** { **broadcast** | **multicast** |**unicast** } { **pps** | **kbps** | **ratio** } *max-pps-values min-pps-values*
**storm-constrain control** { **block** | **shutdown** }
**storm-constrain enable log**
**storm-constrain enable trap**

In addition to paying attention to the configuration settings listed above, check the following when troubleshooting the establishment of an EtherChannel bundle:

- Ensure that a member link is between only two devices.
- Ensure that the member ports are all active.
- Ensure that both end links are statically set to *on* and that either LACP is enabled with at least one side set to *active* or PAgP is enabled with at least one side set to *desirable*.
- Ensure that all member interface ports are consistently configured (except for LACP port priority).
- Verify the LACP or PAgP packet transmission and receipt on both devices.

## *Load Balancing Traffic with EtherChannel Bundles*

- EtherChannel provides load balancing only per frame, not per bit.
- Values has calculated by hash algorithm, that particular port accepts.
- A switch decides which member link a frame will traverse frame.
- In Etherchannel flow uses of particular port cannot be controlled.
- The hash algorithm cannot be configured or changed to load balance.
- Only influence the load balance with a frame distribution method.
- Which fields are considered is dependent on switch platform & configuration.
- EtherChannel load balancing can use MAC addresses and IP addresses.
- By default, Layer 2 packets are distributed on source & destination MAC address.
- By default, Layer 3 packets are distributed based on source & destination IP address.

| Ports in EtherChannel | Distribution across the links |
|---|---|
| 2 | 50%:50% |
| 3 | 37,5%:37,5%:25% |
| 4 | 25%:25%:25%:25% |
| 5 | 25%:25%:25%:12,5%:12,5% |
| 6 | 25%:25%:12,5%:12,5%:12,5%:12,5% |
| 7 | 25%:12,5%:12,5%:12,5%:12,5%:12,5%:12,5% |
| 8 | 12,5%:12,5%:12,5%:12,5%:12,5%:12,5%:12,5%:12,5% |

Traffic that flows across a port-channel interface is not forwarded out member links on a round-robin basis per packet.

Instead, a hash is calculated, and packets are consistently forwarded across a link based on that hash, which runs on the various packet header fields.

The load-balancing hash is a systemwide configuration that uses the global command **port-channel load-balance** *hash*.

The *hash* option has the following keyword choices:

- **dst-ip:** Destination IP address
- **dst-mac:** Destination MAC address
- **dst-mixed-ip-port:** Destination IP address and destination TCP/UDP port
- **dst-port:** Destination TCP/UDP port
- **src-dst-ip:** Source and destination IP addresses
- **src-dest-ip-only:** Source and destination IP addresses only
- **src-dst-mac:** Source and destination MAC addresses
- **src-dst-mixed-ip-port:** Source and destination IP addresses and source and destination TCP/UDP ports
- **src-dst-port:** Source and destination TCP/UDP ports only
- **src-ip:** Source IP address
- **src-mac:** Source MAC address
- **src-mixed-ip-port:** Source IP address and source TCP/UDP port
- **src-port:** Source TCP/UDP port

If the links are unevenly distributed, changing the hash value may provide a different distribution ratio across member links.

Another critical point is that a hash is a binary function, so links should be in powers of two (for example, 2, 4, 8), to be consistent. A three-port EtherChannel will not load balance as effectively as a two- or four-port EtherChannel. The best was to view the load of each member link is with the command **show etherchannel port**. The link utilization is displayed in hex under Load and displays the relative link utilization to the other member links of the EtherChannel.

| Method | Operation | Hash | Switch Model |
|---|---|---|---|
| src-ip | Source IP address | bits | All Models |
| dst-ip | Destination IP address | bits | All Models |
| src-dst-ip | Source and destination IP address | XOR | All Models |
| src-mac | Source MAC address | bits | All Models |
| dst-mac | Destination MAC address | bits | All Models |
| src-dst-mac | Source and destination MAC | XOR | All Models |
| src-port | Source port number | bits | 6500/4500 |
| dst-port | Destination port number | bits | 6500/4500 |
| src-dst-port | Source and destination port | XOR | 6500/4500 |

## *EtherChannel Misconfiguration Guard:*

- EtherChannel Guard is a way of finding out error in the etherchannel port channel.
- Etherchannel guard finding if one end of the EtherChannel is not configured properly.
- This could be that there are some parameters not matching up such as duplex a speed.
- Alternatively, it could be that one side is a trunk and the other is not trunk link or port.
- After the misconfiguration found, the switch place the interfaces in error-disabled state.
- After misconfiguration found in EtherChannel configuration the switch will display error.

Commands

SCOTSW01(config)#spanning-tree etherchannel guard misconfig
SCOTSW02(config)#spanning-tree etherchannel guard misconfig
SCOTSW01#show spanning-tree summary
SCOTSW02#show spanning-tree summary
SCOTSW01# show interfaces status err-disabled
SCOTSW02# show interfaces status err-disabled

CLI REFERENCE:

| | |
|---|---|
| Configure the LACP packet rate | **lacp rate** {**fast** \| **slow**} |
| Configure the minimum number of member links for the LACP EtherChannel to become active | **port-channel min-links** *min-links* |
| Configure the maximum number of member links in an LACP EtherChannel | **lacp max-bundle** *max-links* |
| Configure a switch's LACP system priority | **lacp system-priority** *priority* |
| Configure a switch's LACP port priority | **lacp port-priority** *priority* |
| Configure the EtherChannel load-balancing hash algorithm | **port-channel load-balance** *hash* |
| Display the contents of all current access lists | **show access-list** [*access-list-number* \| *access-list-name*} |
| Display the VTP system settings | **show vtp status** |

| | |
|---|---|
| Display the switch port DTP settings, native VLANs, and allowed VLANs | **show interface** [*interface-id*] **trunk** |
| Display a brief summary update on EtherChannel interfaces | **show etherchannel summary** |
| Display detailed information for the local EtherChannel interfaces and their remote peers | **show interface port-channel** |
| Display information about LACP neighbors | **show lacp neighbor** [**detail**] |
| Display the local LACP system identifier and priority | **show lacp** *system-id* |
| Display the LACP counters for configure interfaces | **show lacp counters** |
| Display information about PAgP neighbors | **show pagp neighbor** |
| Display the PAgP counters for configured interfaces | **show pagp counters** |
| Display the algorithm for load balancing network traffic based on the traffic type | **show etherchannel load-balance** |

**QUIZ**

**1.** Which of the following is not a switch role for VTP?

1. Client
2. Server
3. Proxy
4. Transparent
5. Off

**2.** True or false: The VTP summary advertisement includes the VLANs that were recently added, deleted, or modified.

1. True
2. False

**3.** True or false: There can be only one switch in a VTP domain that has the server role.

1. True
2. False

**4.** Which of the following is a common disastrous VTP problem with moving a switch from one location to another?

1. The domain certificate must be deleted and re-installed on the VTP server.
2. The moved switch sends an update to the VTP server and deletes VLANs.
3. The moved switch interrupts the VTP.
4. The moved switch causes an STP forwarding loop.

**5.** True or false: If two switches are connected and configured with the command **switchport mode dynamic auto**, the switches will establish a trunk link.

1. True
2. False

**6.** The command _____ prevents DTP from communicating and agreeing upon a link being a trunk port.

**1.** switchport dtp disable
**2.** switchport disable dtp
**3.** switchport nonegotiate
**4.** no switchport mode trunk handshake
**5.** server

**7.** True or false: PAgP is an industry standard dynamic link aggregation protocol.

1. True
2. False

**8.** An EtherChannel bundle allows for link aggregation for which types of ports? (Choose all that apply.)

1. Access
2. Trunk
3. Routed
4. Loopback

**9.** What are the benefits of using an EtherChannel? (Choose two.)

1. Increased bandwidth between devices
2. Reduction of topology changes/convergence
3. Smaller configuration
4. Per-packet load balancing

**10.** One switch has EtherChannel configured as auto. What options on the other switch can be configured to establish an EtherChannel bundle?

1. Auto
2. Active
3. Desirable
4. Passive

**11.** True or false: LACP and PAgP allow you to set the maximum number of member links in an EtherChannel bundle.

1. True
2. False

**Answers to the "Do I Know This Already?" quiz:**

**1** C

**2** B

**3** B

**4** B

**5** B

**6** C

**7** B

**8** A, B and D

**9** A, B

**10** C

**11** B