CCNA 200-301

CISCO ™

Lesson 13

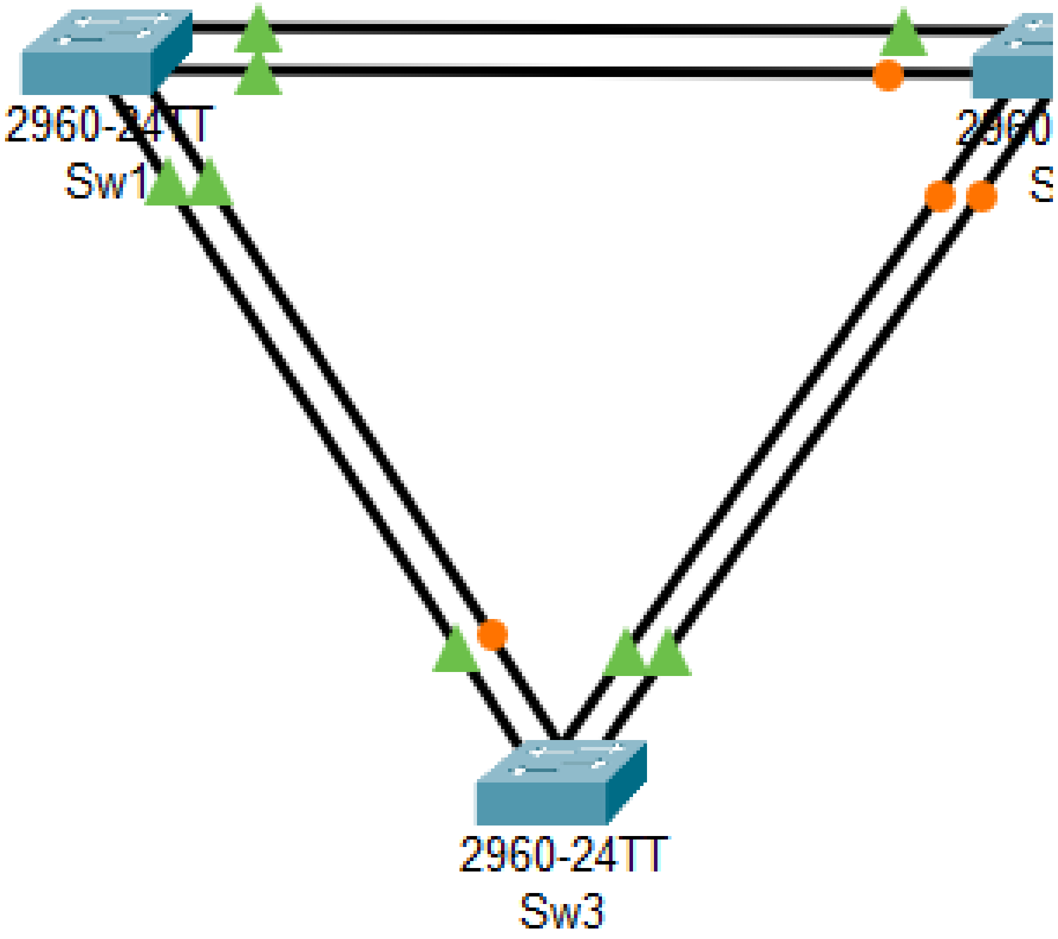
Optional STP Features

- ➢EtherChannel
- ➢PortFast
- ➢BPDUGuard

EtherChannel

Let’s suppose that we have topology with three Catalyst switches and 6 communication links. According to the topology and STP working rules STP will block alternative ports in order to prevent loops in LAN.

In convergence, it will take addinitional time to converge. Because each blocking port needs time to go from blocking to forwarding state.



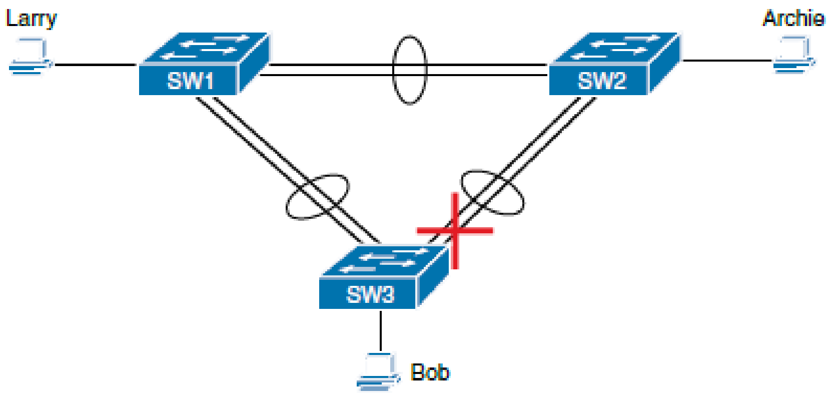
EtherChannel cont.

One of the best ways to lower STP's convergence time is to avoid convergence altogether. EtherChannel provides a way to prevent STP convergence from being needed when only a single port or cable failure occurs.

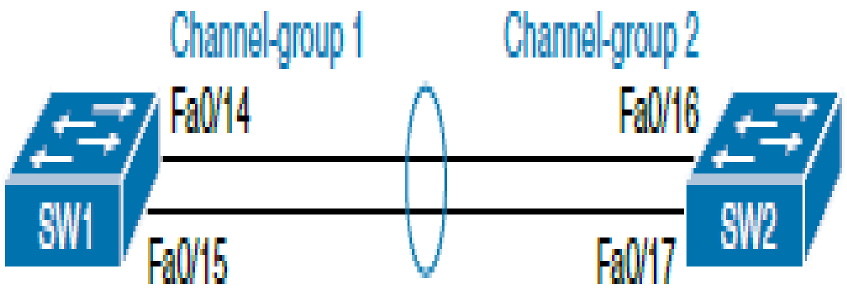
EtherChannel combines multiple parallel segments of equal speed (up to eight) between the same pair of switches, bundled into an EtherChannel. The switches treat the EtherChannel as a single interface with regard to STP. As a result, if one of the links fails, but at least one of the links is up, STP convergence does not have to occur.

Let's look at the next topology:

With EtherChannel, all the parallel links can be up and working at the same time, while reducing the number of times STP must converge, which in turn makes the network more available.



Configuring Layer 2 EtherChannel



EtherChannel Synonyms – PortChannel, Channel Group.

Manual Configuration:

Oddly, IOS uses the **channel-group** configuration command, but then to display its status, IOS uses the **show etherchannel** command. Then the output of this **show** command refers to neither an “EtherChannel” nor a “Channel-group,” instead using the term “PortChannel.”

- To configure an EtherChannel manually, follow these steps:
- **Step 1.** Add the **channel-group** *number* **mode on** command in interface configuration mode under each physical interface that should be in the channel to add it to the channel.
- **Step 2.** Use the same number for all commands on the same switch, but the channelgroup number on the neighboring switch can differ.

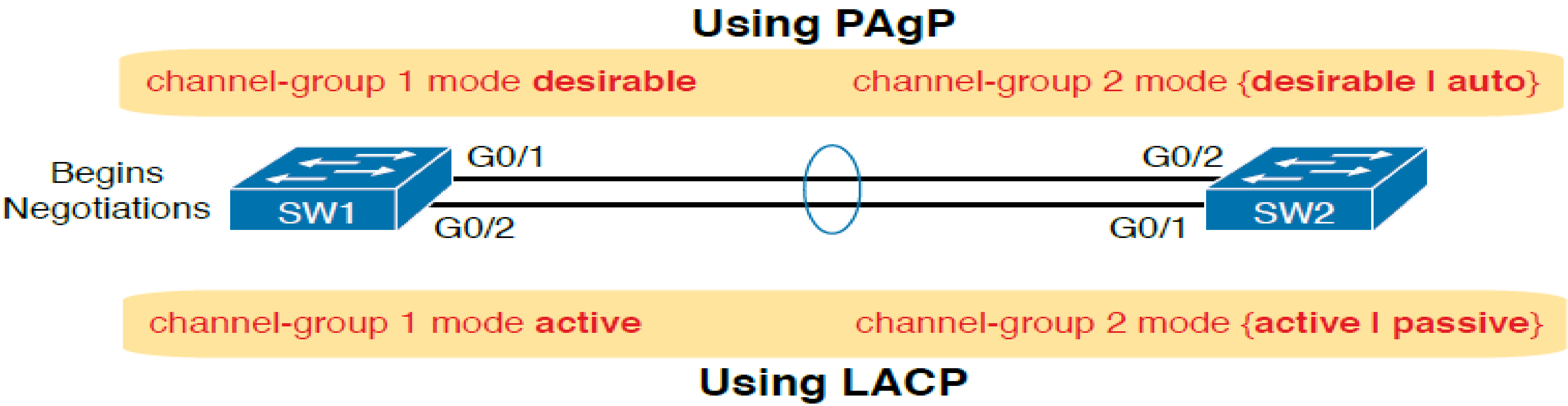
Packet Tracer Practice…

Configuring Dynamic EtherChannels

In addition to manual configuration, Cisco switches also support two different configuration options that then use a dynamic protocol to negotiate whether a particular link becomes part of an EtherChannel or not. Most Cisco Catalyst switches support the **Cisco-proprietary Port Aggregation Protocol (PAgP)** and the IEEE standard **Link Aggregation Control Protocol (LACP)**, based on IEEE standard 802.3ad.

Differences between PAgP and LACP.

- PAgP is Cisco-proprietary, LACP is Open-standard.
- PAgP supports 8 links in channel, LACP supports 16 links in channel.
- Each has fifferent modes.



```
channel-group 1 mode desirable
channel-group 2 mode {desirable I auto}
channel-group 1 mode active
channel-group 2 mode {active I passive}
```

Physical port requirements for being part of channel-group

First, before using a physical port in an EtherChannel, the switch compares the new physical port’s configuration to the existing ports in the channel. That new physical interface’s settings must be the same as the existing ports’ settings; otherwise, the switch does not add the new link to the list of approved and working interfaces in the channel.

- The list of items the switch checks includes the following:

■ Speed

■ Duplex

■ Operational access or trunking state (all must be access, or all must be trunks)

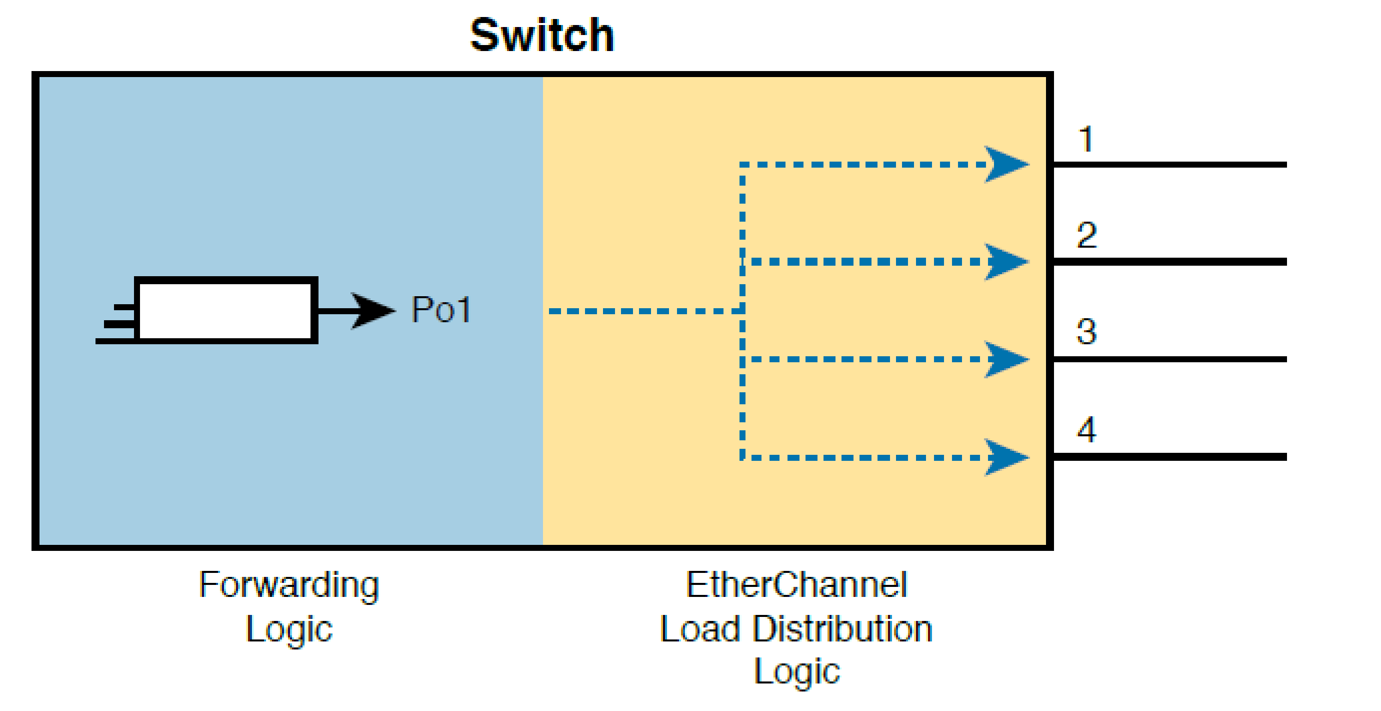
■ If an access port, the access VLAN

■ If a trunk port, the allowed VLAN list (per the **switchport trunk allowed** command)

■ If a trunk port, the native VLAN

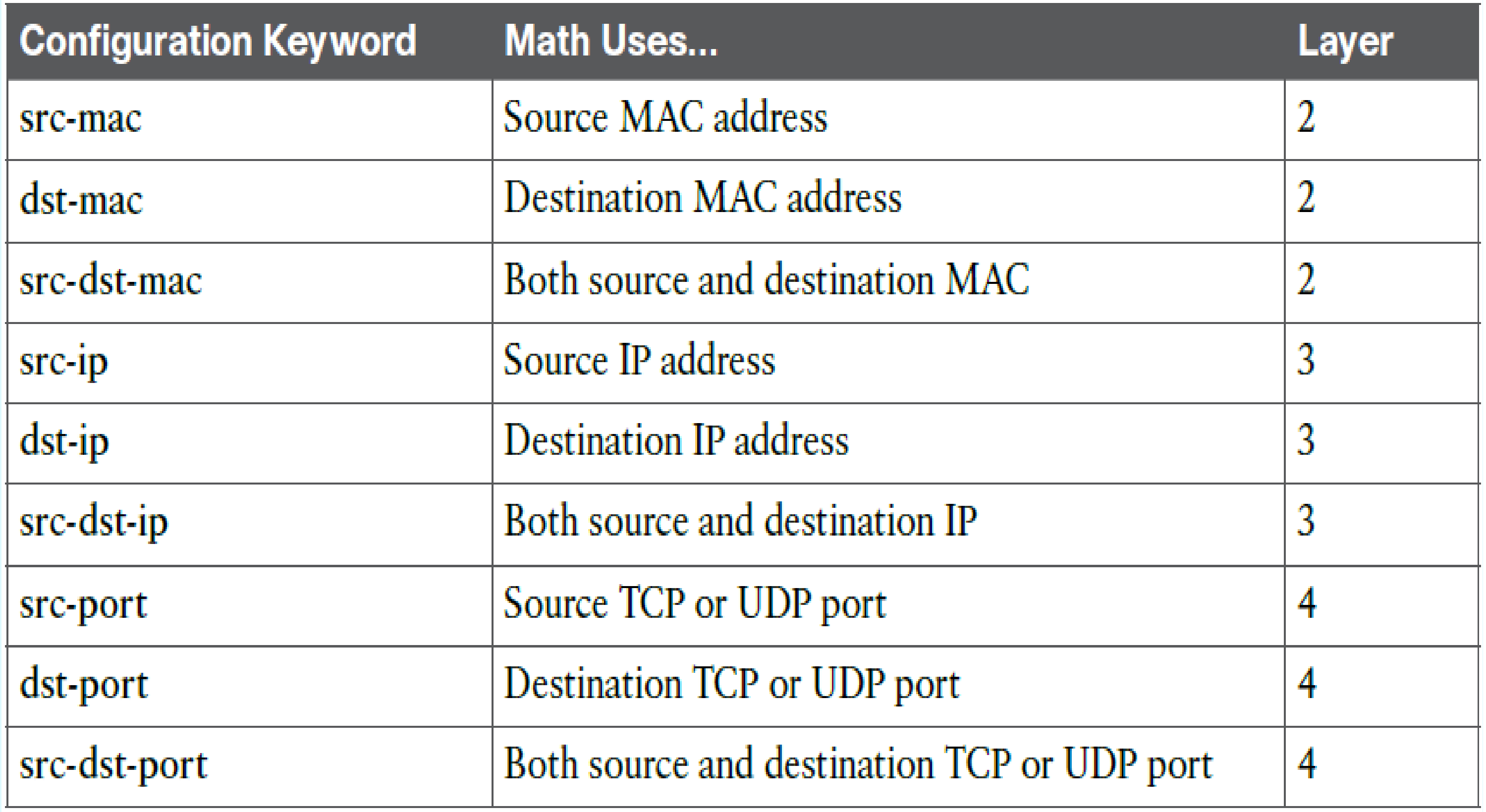
■ STP interface settings

Etherchannel Load Distribution



When using Layer 2 EtherChannels, a switch’s MAC learning process associates MAC addresses with the PortChannel interfaces and not the underlying physical ports. Later, when a switch makes a forwarding decision to send a frame out a PortChannel interface, the switch must do more work: to decide out which specific physical port to use to forward the frame. IOS documentation refers to those rules as *EtherChannel load distribution* or *load balancing*.

Etherchannel Load Distribution cont.



Configuration Keyword	Math Uses...	Layer
src-mac	Source MAC address	2
dst-mac	Destination MAC address	2
src-dst-mac	Both source and destination MAC	2
src-ip	Source IP address	3
dst-ip	Destination IP address	3
src-dst-ip	Both source and destination IP	3
src-port	Source TCP or UDP port	4
dst-port	Destination TCP or UDP port	4
src-dst-port	Both source and destination TCP or UDP port	4

Etherchannel Load Distribution (Balancing) methods

Verification command:

```
#show etherchannel load-balance
```

Changing load-balancing methods:

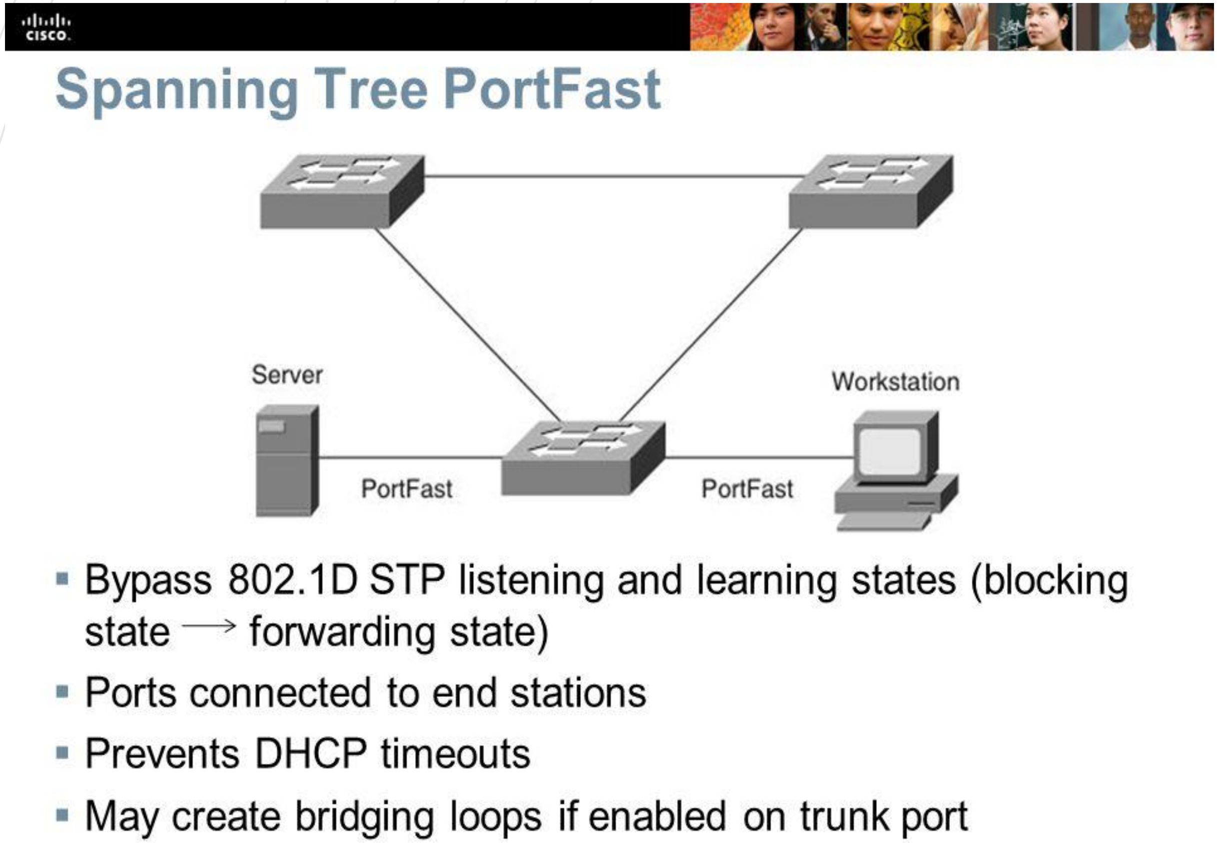
```
Switch(config)#port-channel load-balance ?
 dst-ip Dst IP Addr
 dst-mac Dst Mac Addr
 src-dst-ip Src XOR Dst IP Addr
 src-dst-mac Src XOR Dst Mac Addr
 src-ip Src IP Addr
 src-mac Src Mac Addr
```

STP PortFast feature

PortFast allows a switch to immediately transition from blocking to forwarding, bypassing listening and learning states. However, the only ports on which you can safely enable PortFast are ports on which you know that no bridges, switches, or other STP-speaking devices are connected.

PortFast is most appropriate for connections to end-user devices. If you turn on PortFast on ports connected to end-user devices, when an end-user PC boots, the switch port can move to an STP forwarding state and forward traffic as soon as the PC NIC is active. Without PortFast, each port must wait while the switch confirms that the port is a DP. With STP in particular (and not RSTP), the switch waits in the temporary listening and learning states before settling into the forwarding state.

STP PortFast Configuration



Spanning Tree PortFast

- Bypass 802.1D STP listening and learning states (blocking state → forwarding state)
- Ports connected to end stations
- Prevents DHCP timeouts
- May create bridging loops if enabled on trunk port

```
Sw(conf-if)#spanning-tree portfast
```

STP BPDUGuard feature

STP and RSTP open up the LAN to several different types of possible security exposures.

For example:

■ An attacker could connect a switch to one of these ports, one with a low STP/RSTP priority value, and become the root switch. The new STP/RSTP topology could have worse performance than the desired topology.

■ The attacker could plug into multiple ports, into multiple switches, become root, and actually forward much of the traffic in the LAN. Without the networking staff realizing it, the attacker could use a LAN analyzer to copy large numbers of data frames sent through the LAN.

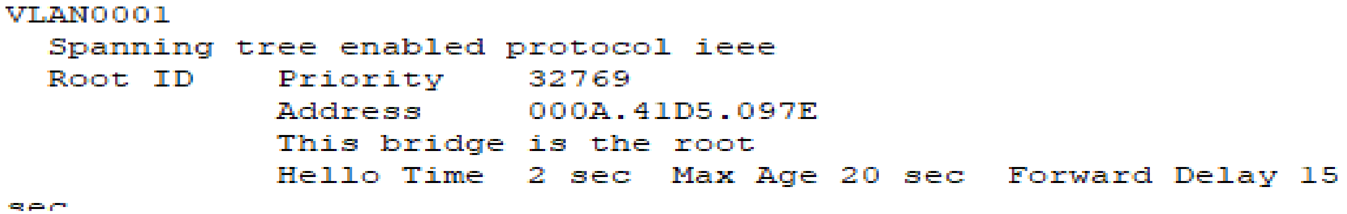
■ Users could innocently harm the LAN when they buy and connect an inexpensive consumer LAN switch (one that does not use STP/RSTP). Such a switch, without any STP/RSTP function, would not choose to block any ports and could cause a loop.

- The *Cisco BPDU Guard* feature helps defeat these kinds of problems by disabling a port if any BPDUs are received on the port. So, this feature is particularly useful on ports that should be used only as an access port and never connected to another switch.
- In addition, the BPDU Guard feature helps prevent problems with PortFast. PortFast should be enabled only on access ports that connect to user devices, not to other LAN switches. Using BPDU Guard on these same ports makes sense because if another switch connects to such a port, the local switch can disable the port before a loop is created.

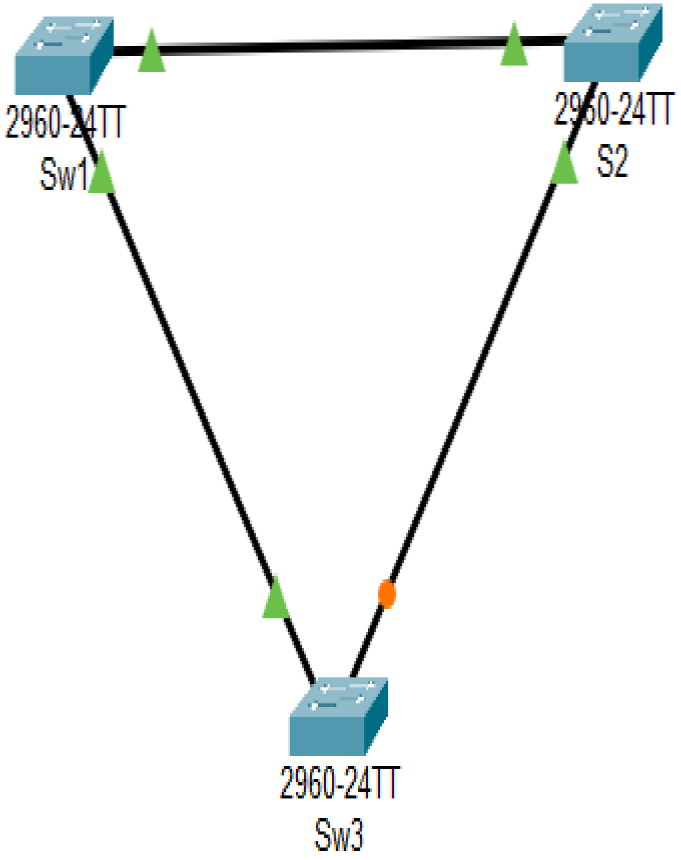
STP BPDUGuard feature cont.

Let’s suppose that we have topology with three switches:

Sw1 is the root switch and priority is 32768 + 1 (VLAN)



```
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     000A.41D5.097E
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15
sec
```

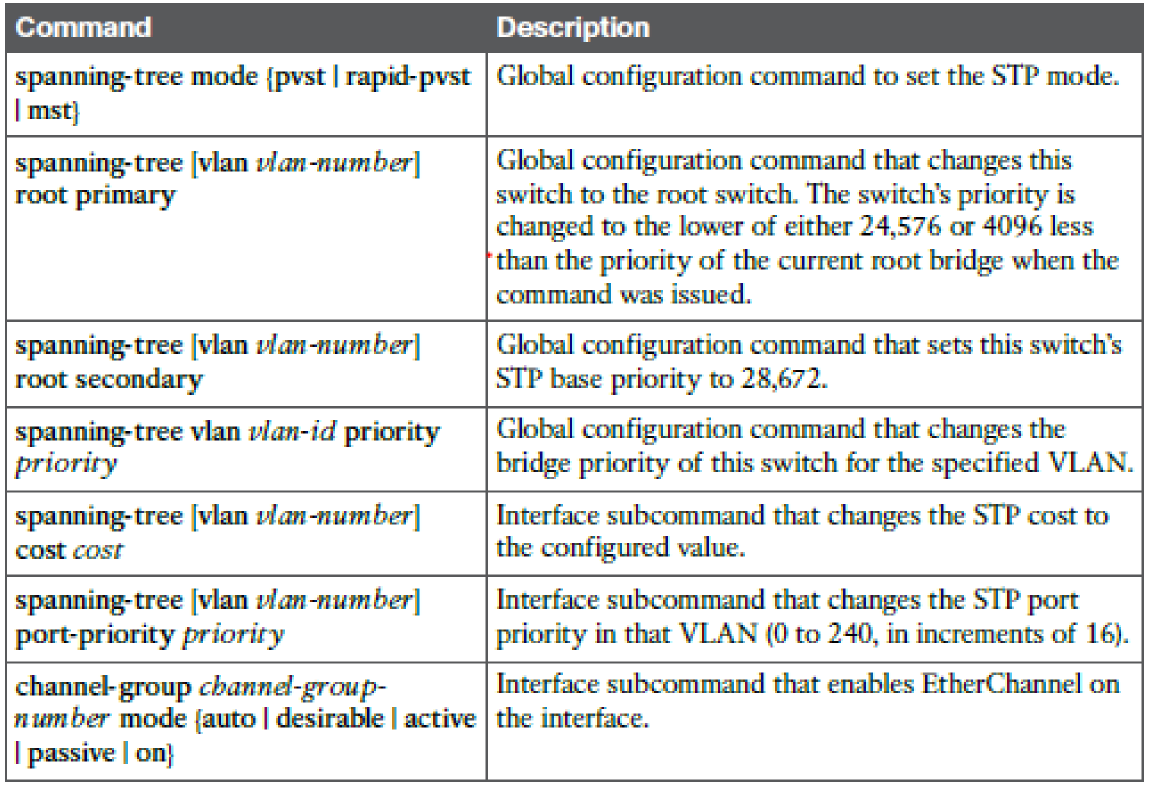


If we have new switch with the lower priority it will take root-bridge actions and change our tree without BPDUGuard.

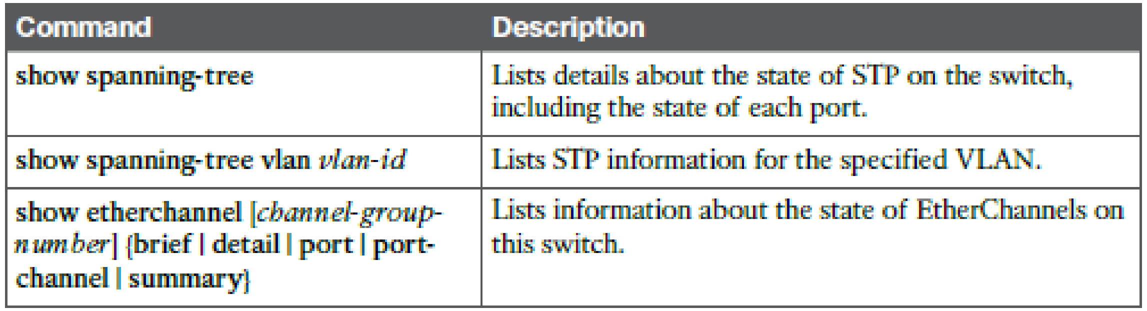
With BPDUGuard STP will make port error-disable states.

Packet-tracer example…

Essenstial commands



Command	Description
spanning-tree mode {**pvst** | **rapid-pvst** | **mst**}	Global configuration command to set the STP mode.
spanning-tree [**vlan** *vlan-number*] **root primary**	Global configuration command that changes this switch to the root switch. The switch's priority is changed to the lower of either 24,576 or 4096 less than the priority of the current root bridge when the command was issued.
spanning-tree [**vlan** *vlan-number*] **root secondary**	Global configuration command that sets this switch's STP base priority to 28,672.
spanning-tree vlan *vlan-id* **priority** *priority*	Global configuration command that changes the bridge priority of this switch for the specified VLAN.
spanning-tree [**vlan** *vlan-number*] **cost** *cost*	Interface subcommand that changes the STP cost to the configured value.
spanning-tree [**vlan** *vlan-number*] **port-priority** *priority*	Interface subcommand that changes the STP port priority in that VLAN (0 to 240, in increments of 16).
channel-group *channel-group-number* **mode** {**auto** | **desirable** | **active** | **passive** | **on**}	Interface subcommand that enables EtherChannel on the interface.



Command	Description
show spanning-tree	Lists details about the state of STP on the switch, including the state of each port.
show spanning-tree vlan *vlan-id*	Lists STP information for the specified VLAN.
show etherchannel [*channel-group-number*] {**brief** | **detail** | **port** | **port-channel** | **summary**}	Lists information about the state of EtherChannels on this switch.

That is all for Lesson 13

The key is :

Learn

Repeat

Practice

You will be able to reach your goals.

GOOD LUCK !!!!!...