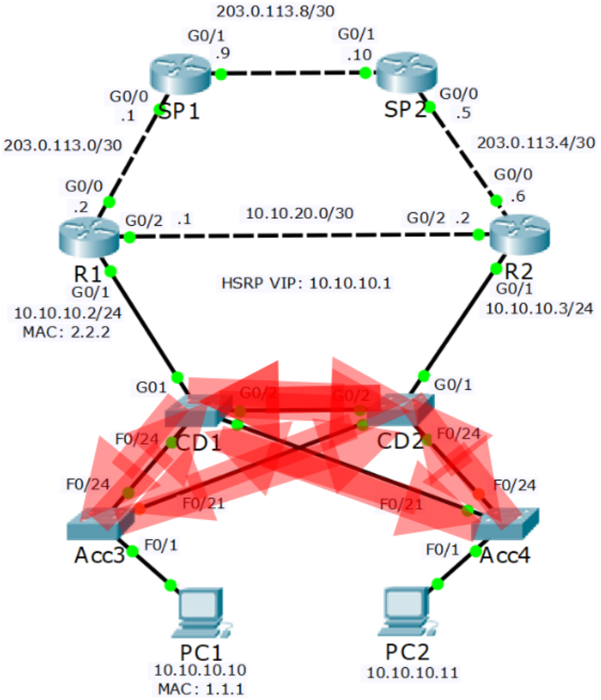
Spanning Tree Protocol

STP is used to prevent Loops in Layer 2 (Switches)
Below is the outcome of an ARP request from PC1 to R1, without STP protocol.



- There will be more broadcast traffic on a production network than a single ARP request
- We now have a broadcast storm
- The network will crash because the amount of looping broadcast traffic will quickly overwhelm the switch's CPU and bandwidth

How it works

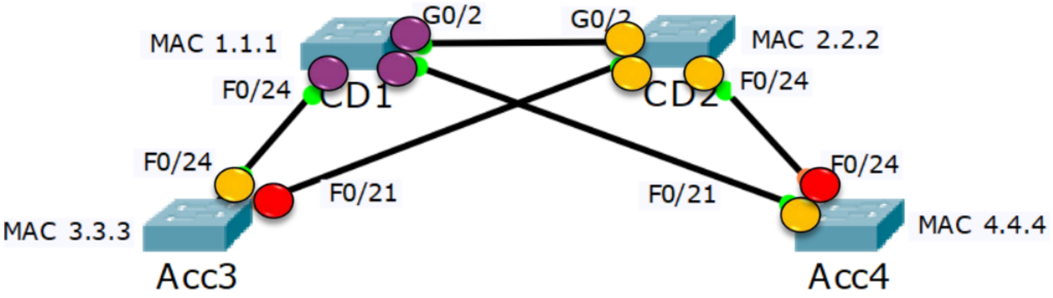
- Spanning Tree is an industry standard protocol and is enabled by default on all vendor's switches
- Switches send Bridge Protocol Data Units out all ports when they come online. These are used to detect other switches and potential loops
- The switch will not forward traffic out any port until it is certain it is loop free
- When the port first comes online it will be in a Blocking state.
- Spanning Tree will detect if the port forms a potential loop
- If there is no loop the port will transition to Forwarding
- The process can take up to 50 seconds

- The BPDU contains the switch's Bridge ID which uniquely identifies the switch on the LAN
- The Bridge ID is comprised of the switch's unique MAC address and an administrator defined Bridge Priority value
- The Bridge Priority can be from 0 – 65535, with 32768 being the default
- A Root Bridge is elected based on the switches' Bridge ID values
- The switch with the lowest Bridge Priority value is preferred (16384 is better than 49152)
- In the case of a tie the switch with the lowest MAC address will be selected
- The switches build a loop free forwarding path Tree leading back to the Root Bridge

Root, Designated and Blocking Ports

The easy way to figure out which ports are Root, Designated and Blocking:

1. Determine the Root Bridge first (best Bridge ID)
2. All ports on the Root Bridge are Designated Ports(Purple)
3. Determine the Root Ports on the other switches (lowest cost to Root Bridge)
4. The ports on the other side of those links are Designated Ports
5. On the links which are left, one port will be Blocking
6. Determine the Blocking Port (highest cost path to Root Bridge or highest Bridge ID)
7. The ports on the other side of those links are Designated Ports



Spanning Tree Versions

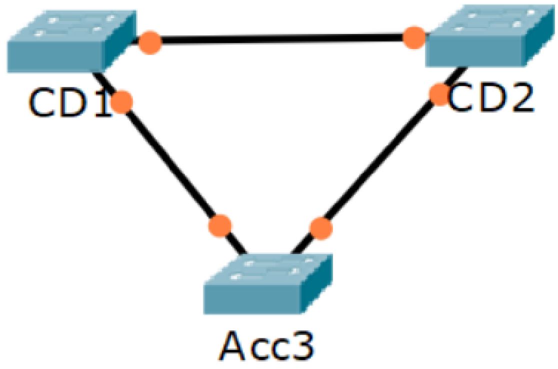
IEEE Open Standards:

- **802.1D Spanning Tree Protocol (STP)**. The original Spanning Tree implementation. Uses one Spanning Tree for all VLANs in the LAN.
- **802.1w Rapid Spanning Tree Protocol (RSTP)**. Significantly improved convergence time. Uses one Spanning Tree for all VLANs in the LAN.

- **802.1s Multiple Spanning Tree Protocol (MSTP)**. Enables grouping and mapping VLANs into different spanning tree instances for load balancing.

MSTP Load Balancing Example

- The Access Layer switches have PCs attached in multiple VLANs
- CD1 is made the Root Bridge for VLANs 10 – 19
- Traffic for these VLANs is forwarded on the link to CD1 and blocked on the link to CD2
- CD2 is made the Root Bridge for VLANs 20 – 29
- Traffic for these VLANs is forwarded on the link to CD2 and blocked on the link to CD1
- Two Spanning Tree instances run, one for each group of VLANs



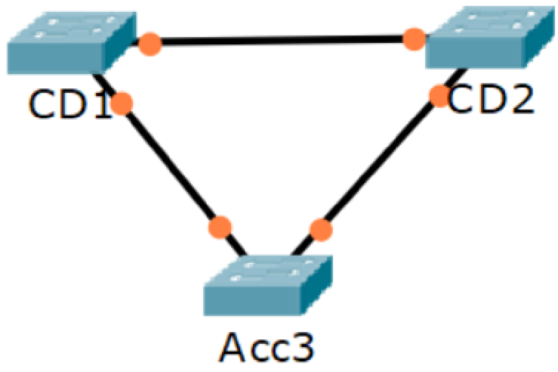
Cisco released enhancements to the open standards.

- **Per VLAN Spanning Tree Plus (PVST+)**: Cisco enhancement to 802.1D. Uses a separate Spanning Tree instance for every VLAN. This is the default on Cisco switches.
- **Rapid Per VLAN Spanning Tree Plus (RPVST+)**: Cisco enhancement to 802.1w RSTP. Significantly improved convergence time over PVST+. Uses a separate Spanning Tree instance for every VLAN.

The Cisco versions do not support grouping multiple VLANs into the same instance

PVST+ and RPVST+ Load Balancing Example

- The Access Layer switches have PCs attached in multiple VLANs
- CD1 is made the Root Bridge for VLANs 10 – 19
- Traffic for these VLANs is forwarded on the link to CD1 and blocked on the link to CD2
- CD2 is made the Root Bridge for VLANs 20 – 29
- Traffic for these VLANs is forwarded on the link to CD2 and blocked on the link to CD1
- Twenty Spanning Tree instances run, one for each VLAN



- PVST+ will assign the Root, Designated or Alternate role to ports
- Alternate Ports are Blocking Ports

STP Configuration

Acc3#show spanning-tree vlan 1

The Root Bridge Election

- Because Spanning Tree selects paths pointing towards the root bridge, it acts as a centre point of the LAN
- Best practice is to ensure a pair of high-end core switches are selected as the 1st and 2nd most preferred Root Bridge
- You can manipulate the Root Bridge election by setting Bridge priority
- The default value is 32768, with the lowest number being most preferred
- In the case of a tie the switch with the lowest MAC address will be selected
- This is liable to be the oldest switch

Core1(config)#spanning-tree vlan 1 root primary

- Configures the Core1 switch to be the Root Bridge
- This will set a Bridge Priority of 24576

Core2(config)#spanning-tree vlan 1 root secondary

- Configures the Core2 switch to be the next most preferred Root Bridge after Core1
- This will set a Bridge Priority of 28672

Spanning Tree and HSRP Relationship

- HSRP should be configured to match the Spanning Tree path
- In this example R1 should be given a higher HSRP priority than R2 so that it is selected as the HSRP active router

- This allows traffic from the PCs to take the most direct path to their default gateway
- If R2 was the HSRP active router, traffic would have to transit via an extra device over the CD1>CD2 link

Aligned ‘Active/Active’ HSRP & Spanning Tree

- **Vlan 10**

  ```
  R1(config)#interface g0/1.10
  R1(config)#encap dot1 vlan 10
  R1(config-if)#ip address 10.10.10.2 255.255.255.0
  R1(config-if)#no shutdown
  R1(config-if)#standby 1 ip 10.10.10.1
  R1(config-if)#standby 1 priority 110
  R1(config-if)#standby 1 pre-empt

  R2(config)#interface g0/1.10
  R2(config)#encap dot1 vlan 10
  R2(config-if)#ip address 10.10.10.3 255.255.255.0
  R2(config-if)#no shutdown
  R2(config-if)#standby 1 ip 10.10.10.1
  R2(config-if)#standby 1 priority 90
  ```

- **Vlan 20**

  ```
  R1(config)#interface g0/1.20
  R1(config)#encap dot1 vlan 20
  R1(config-if)#ip address 10.10.20.2 255.255.255.0
  R1(config-if)#no shutdown
  R1(config-if)#standby 1 ip 10.10.20.1
  R1(config-if)#standby 1 priority 90

  R2(config)#interface g0/1.20
  R2(config)#encap dot1 vlan 20
  R2(config-if)#ip address 10.10.20.3 255.255.255.0
  R2(config-if)#no shutdown
  R2(config-if)#standby 1 ip 10.10.20.1
  R2(config-if)#standby 1 priority 110
  R2(config-if)#standby 1 pre-empt
  ```

```
CD1(config)#spanning-tree vlan 10 root primary
CD1(config)#spanning-tree vlan 20 root secondary
```

```
    CD2(config)#spanning-tree vlan 20 root primary
    CD2(config)#spanning-tree vlan 10 root secondary
```

Spanning Tree Portfast & BPDU Guard

- It can take up to 50 seconds for Spanning Tree to transition a port to a forwarding state when it becomes active
- A loop cannot be formed on ports where a single end host is plugged in
- You can make the port transition to a forwarding state immediately when it becomes active by disabling Spanning Tree on the port

```
SW1(config)# interface f0/10
SW1(config-if)# spanning-tree portfast
SW1(config)# spanning-tree portfast default
```

- If you enable Portfast on a port and then a loop is formed through it, a broadcast storm will result
- This can be caused by users adding devices to the network or changing cabling
- You can enable BPDU Guard on Portfast ports to guard against this happening
- If a BPDU is received the port will be shut down

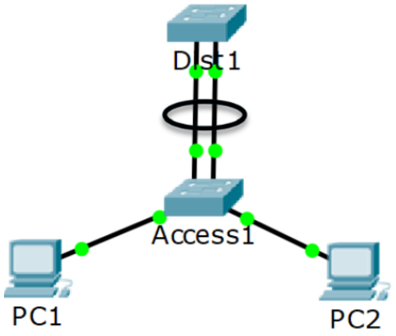
```
SW1(config)# interface f0/10
SW1(config-if)# spanning-tree portfast
SW1(config-if)# spanning-tree bpduguard enable
SW1(config)# spanning-tree portfast bpduguard default
```

- **Spanning Tree Root Guard** prevents an unintended switch from becoming the root bridge
- If a port where Root Guard is enabled receives BPDU’s that are superior than the current root bridge, it will transition the port to root- inconsistent and not forward any traffic over the port

```
SW2(config)#interface fa0/2
SW2(config-if)#spanning-tree guard root
```

EtherChannel

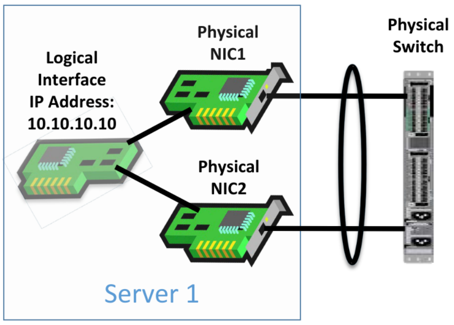
- Etherchannel groups multiple physical interfaces into a single logical interface
- Spanning Tree sees the EtherChannel as a single interface, so it does not block any ports
- We now get the full 20Gbps bandwidth



- Traffic is load balanced across all the links in the EtherChannel
- If an interface goes down its traffic will fail over to the remaining links

NIC Teaming

NIC Teaming combines multiple physical network cards into a single logical interface



1. **EtherChannel** is also known as:
    a. A Port Channel
    b. LAG Link Aggregation
    c. A link bundle
2. **NIC Teaming** is also known as:
    a. Bonding
    b. NIC balancing
    c. Link aggregation

EtherChannel - Protocols

1. **LACP Link Aggregation Control Protocol**:
    a. Open standard
    b. The switches on both sides negotiate the port channel creation and maintenance
    c. This is the preferred method
2. **PAgP Port Aggregation Protocol**:
    a. Cisco proprietary.
    b. The switches on both sides negotiate the port channel creation and maintenance.
3. **Static Etherchannel**:
    a. The switches do not negotiate creation and maintenance but the settings must still match on both sides for the port channel to come up.
    b. Use if LACP is not supported on both sides.

All protocols are configured with the *channel-group* command

- The switches on both sides must have a matching configuration
- The member interfaces must have the same settings on both sides:
- Speed and duplex
- Access or Trunk mode
- Native VLAN and allowed VLANs on trunks
- Access VLAN on access ports

LACP

- LACP interfaces can be set as either Active or Passive
- If SW1's interfaces are set as Active and SW2's as Passive, the port channel will come up
- If both sides are Passive, the port channel will not come up
- If both sides are Active, the port channel will come up
- It is recommended to configure both sides as Active so you don't have to think about which side is which

```
SW1(config)#interface range f0/23 - 24
SW1(config-if-range)#channel-group 1 mode active
```

This creates interface port-channel 1

```
SW1(config)#interface port-channel 1
```

```
SW1(config-if)#switchport mode trunk
```

Configure the interface settings on the port channel

Configure matching settings on the other switch on the other side of the links:

```
SW2(config)#interface range f0/23 - 24
SW2(config-if-range)#channel-group 1 mode active
SW2(config)#interface port-channel 1
SW2(config-if)#switchport mode trunk
```

PAgP Configuration

- PAgP interfaces can be set as either Desirable or Auto
- If one side is Desirable and the other Auto, the port channel will come up
- If both sides are Auto, the port channel will not come up
- If both sides are Desirable, the port channel will come up
- If you configure both sides as Desirable you don’t have to think about which side is which

```
SW1(config)#interface range f0/23 - 24
SW1(config-if-range)#channel-group 1 mode desirable
SW1(config)#interface port-channel 1
SW1(config-if)#switchport mode trunk
```

Configure matching settings on the switch on the other side of the links

Static Configuration

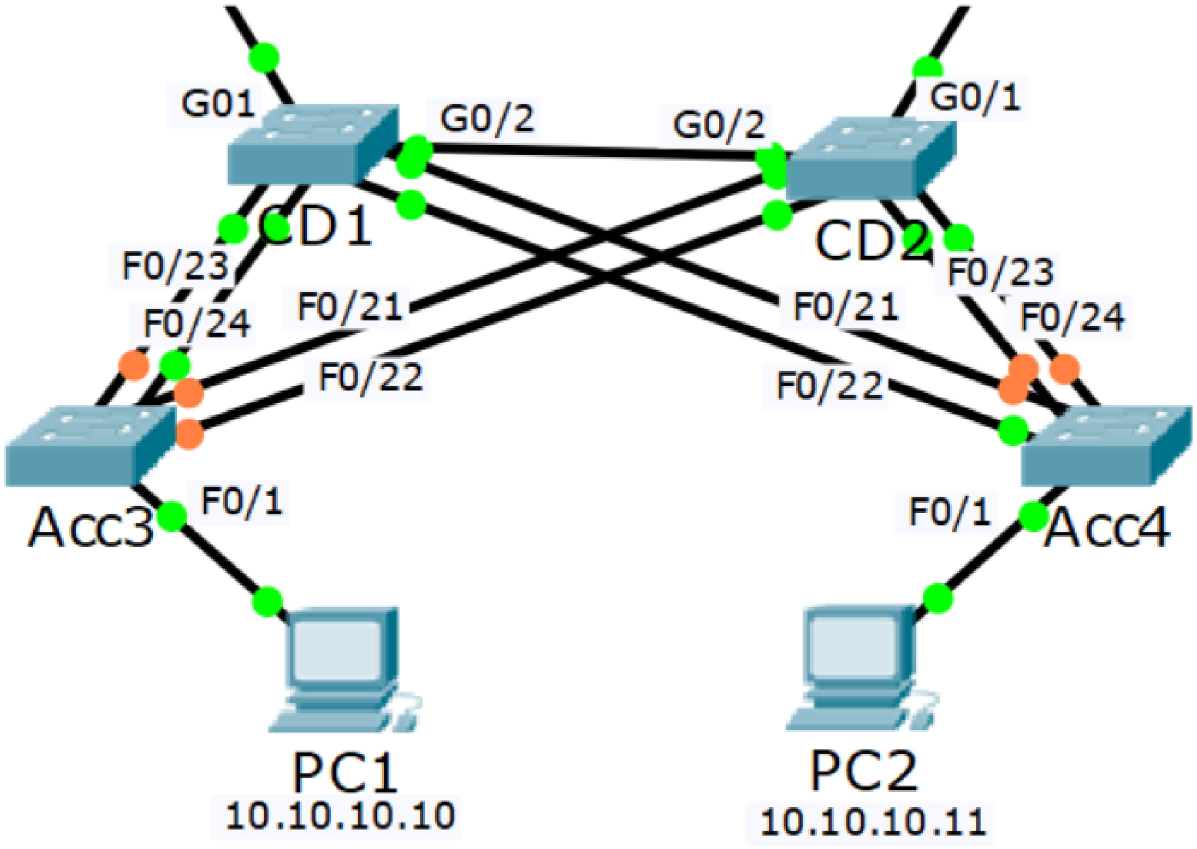
```
SW1(config)#interface range f0/23 - 24
SW1(config-if-range)#channel-group 1 mode on
SW1(config)#interface port-channel 1
SW1(config-if)#switchport mode trunk
```

Configure matching settings on the switch on the other side of the links

Show info about etherchannel

```
show etherchannel summary
```

Example



1st Port Channel – Acc3 to CD1 - LACP

Acc3 Port Channel 1:

Acc3 F0/23 – CD1 F0/23

Acc3 F0/24 – CD1 F0/24

CD1 Port Channel 1:

CD1 F0/23 - Acc3 F0/23

CD1 F0/24 - Acc3 F0/24

2nd Port Channel – Acc3 to CD2 - PAgP

Acc3 Port Channel 2:

Acc3 F0/21 – CD2 F0/21

Acc3 F0/22 – CD2 F0/22

CD2 Port Channel 2:

CD2 F0/21 - Acc3 F0/21

CD2 F0/22 - Acc3 F0/22

3rd Port Channel – Acc4 to CD2 - Static

Acc4 Port Channel 1:

Acc4 F0/23 – CD2 F0/23

Acc4 F0/24 – CD2 F0/24

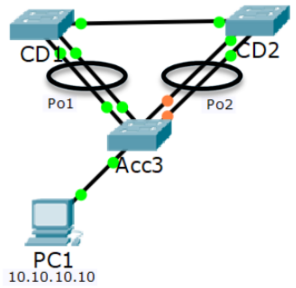
CD2 Port Channel 1:

CD2 F0/23 – Acc4 F0/23
CD2 F0/24 – Acc4 F0/24

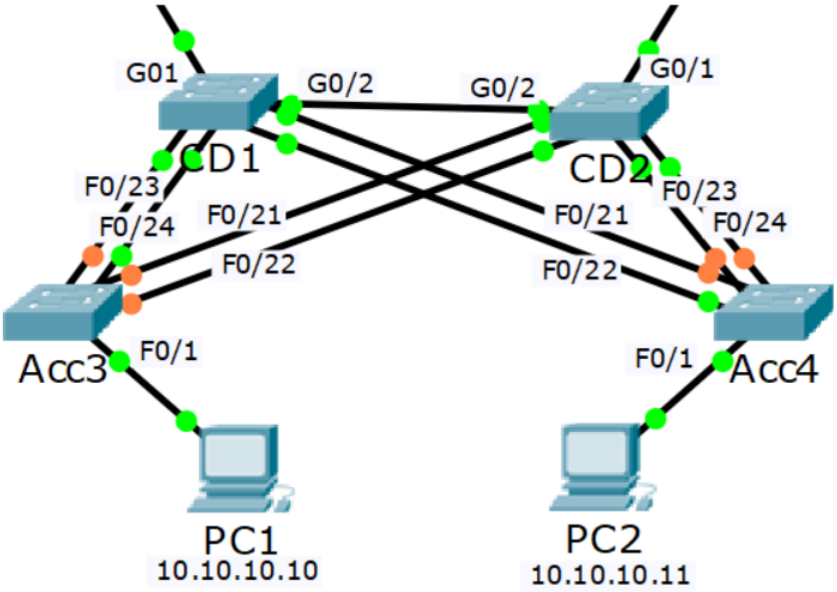
4th Port Channel – Acc4 to CD1 - LACP
Acc4 Port Channel 2:
Acc4 F0/21 – CD1 F0/21
Acc4 F0/22 – CD1 F0/22
CD1 Port Channel 2:
CD1 F0/21 – Acc4 F0/21
CD1 F0/22 – Acc4 F0/22

Multi-chassis EtherChannel

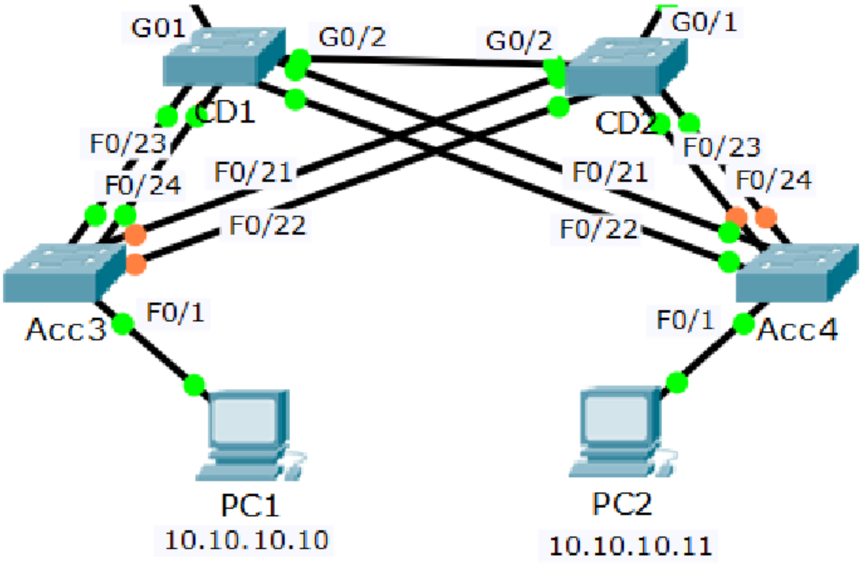
- Spanning Tree will see the port channels as two separate interfaces and block one path if a loop is formed
- This brings us back to the problem of only using half our available physical bandwidth



Before EtherChannel Configured

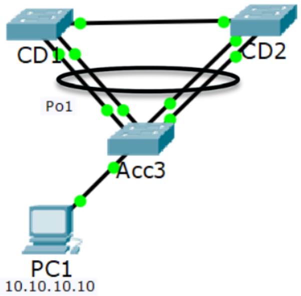


After EtherChannel Configured



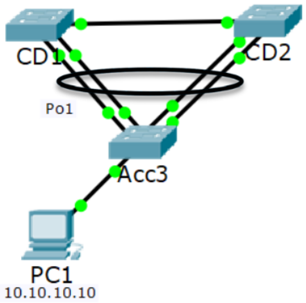
Multi-chassis EtherChannel

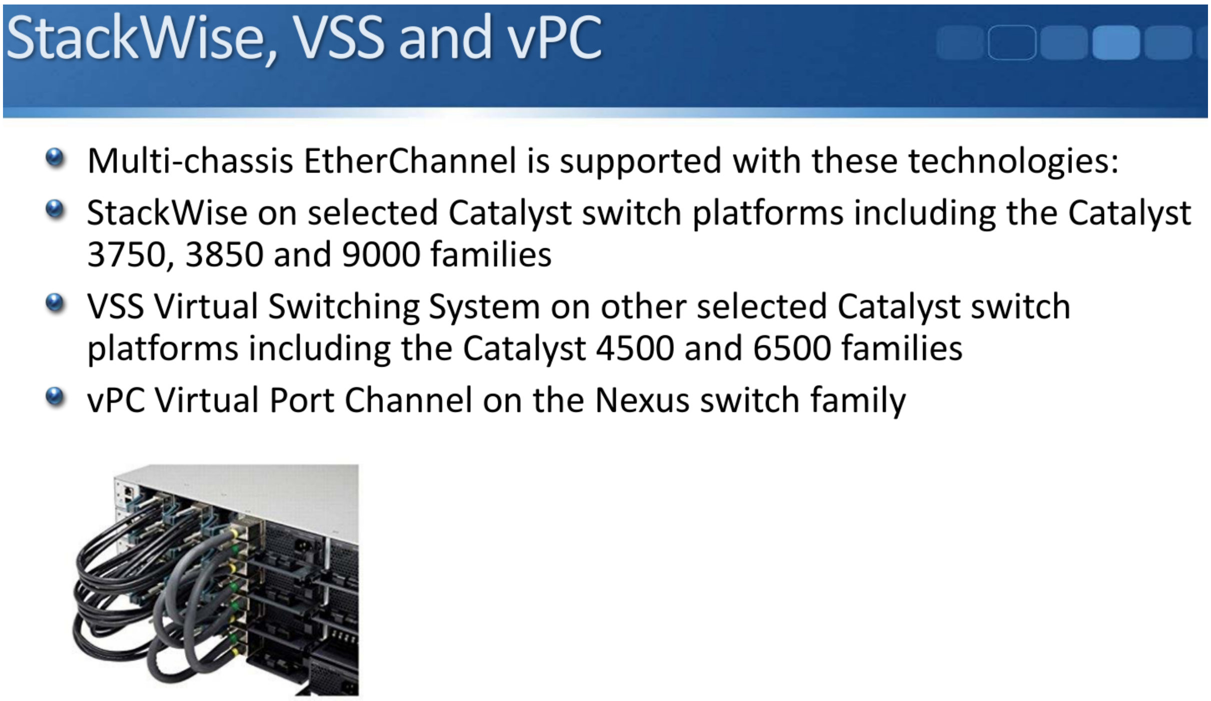
- Cisco support Multi-chassis EtherChannel technologies on some switches
- These switches support a shared EtherChannel from different switches
- The switches must be configured with matching settings



Multi-chassis EtherChannel

- Spanning Tree is still enabled but it does not detect any loops
- This supports full load balancing and redundancy across all interfaces





StackWise, VSS and vPC

- Multi-chassis EtherChannel is supported with these technologies:
- StackWise on selected Catalyst switch platforms including the Catalyst 3750, 3850 and 9000 families
- VSS Virtual Switching System on other selected Catalyst switch platforms including the Catalyst 4500 and 6500 families
- vPC Virtual Port Channel on the Nexus switch family

Layer 3 Etherchannel

```
Switch1(config)#interface range GigabitEthernet 1/0/1 - 2
Switch1(config-if-range)#no switchport
Switch1(config-if-range)#channel-group 1 mode | active | auto
| desirable | on | passive

Switch1(config)#interface port-channel 1
Switch1(config-if)#ip address 192.168.0.1 255.255.255.252
Switch1(config-if)#no shutdown
```