

Table of Contents

Table of Contents	1
C1: Switching Concepts	4
Frame Forwarding	4
2 Step Process	4
Switch Forwarding Methods	4
Switching Domains	5
Alleviated Network Congestion	6
C2: VLANs	7
Overview of VLANs	7
Benefits of VLANs	7
Types of VLANs	7
VLANs in a Multi-Switched Environment	8
VLAN Configuration	8
VLAN Ranges on Catalyst Switches	8
VLAN Creation Commands	8
VLAN Port Assignment Commands	9
Verify VLAN Information	9
Change VLAN Port Membership	9
Delete VLANs	10
VLAN Trunks	10
Trunk Configuration Commands	10
Verify Trunk Configuration	10
Reset the Trunk to the Default State	11
Dynamic Trunking Protocol	11
Negotiated Interface Modes	11
Results of a DTP Configuration	11
Verify DTP Mode	12
Troubleshooting	12
C3: Inter-VLAN Routing	14
Inter-VLAN Routing Operation	14
Inter-VLAN Routing Options	14
Configure Legacy Inter-VLAN Routing	15
Router-on-a-Stick Inter-VLAN Routing	15
Configure Router-on-a-Stick	15
Verify Subinterfaces and Routing	16
Troubleshoot Inter-VLAN Routing	16
Common Inter-VLAN Issues	16
Inter-VLAN Routing using Layer 3 Switches	17

Layer 3 Switch Configuration	17
Layer 3 Switch Inter-VLAN Routing Verification	17
Routing on Layer 3 Switch	17
Routing Configuration on Layer 3 Switch	17
C4: STP Concepts	19
Purpose of STP	19
Issues with Redundant Switch Links	19
Broadcast Storm	19
STP Operations	19
Elect a Root Port from Multiple Equal-Cost Paths	20
STP Convergence - In summary	20
STP Timers and Port States	20
Operational Details of Each Port State	21
Evolution of STP	21
RSTP Concepts	21
PortFast and BPDU Guard	22
C5: EtherChannel	23
Link Aggregation	23
EtherChannel	23
PAgP Operation	24
LACP Operation	25
Configuration Guidelines	27
Verify EtherChannel	27
C6: FHRP Concepts	28
First Hop Redundancy Protocols (FHRPs)	28
HSRP	28
C7: Routing Concepts	30
Best Path Equals Longest Match	30
*Path Determination	30
Best Path	32
Load Balancing	35
Administrative Distance	35
EIGRP	37
Implement EIGRP for IPv4	37
*C8: LAN Security Concepts	39
*AAA Components	39
Authentication	39
Authorization	39
Accounting	39
802.1X	40
Layer 2 Security Threats	40

Switch Attack Categories	40
Switch Attack Mitigation Techniques	41
MAC Address Table Flooding	41
LAN Attacks	42
VLAN Hopping Attacks	42
VLAN Double-Tagging Attacks	42
VLAN Hopping & VLAN Double-Tagging Attack Mitigation	43
DHCP Attacks	43
ARP Attacks	44
Address Spoofing Attacks	44
STP Attack	44
*C9: Switch Security Configuration	45
Mitigate MAC Address Table Attacks	45
Enable Port Security	45
Limit Maximum Number of MAC Addresses	45
Configure Way to Learn MAC Addresses	45
Port Security Aging	46
Port Security Violation Modes	46
Mitigate VLAN Attacks	47
Mitigate DHCP Attacks	48
DHCP Snooping	48
Mitigate ARP Attacks	48
Mitigate STP Attacks	49
C10: WLAN Concepts	51
* AP Categories	51
* CSMA/CA	51
WLAN Threats	51
DoS Attacks	51
* Rogue Access Points	52
Man-in-the-Middle Attack	52
Secure WLANs	52
802.11 Original Authentication Methods	52
Shared Key Authentication Methods	53
* Authenticating a Home User (WPA2 Authentication)	53
Encryption Methods	54
Authentication in the Enterprise	54
WPA 3	54

C1: Switching Concepts

Frame Forwarding

Ingress	Entering the interface
Egress	Exiting the interface

- A switch forwards based on the ingress interface and the destination MAC address.

2 Step Process

- **Step 1. Learn** - Examines **Source Address**
 - Adds the source MAC if not in switch's MAC address table / Content Addressable Memory (CAM) table
 - Resets the time out setting back to 5 minutes if the source is in the table.
- **Step 2. Forward** - Examines **Destination Address**
 - If the destination MAC is in the MAC address table, it is forwarded out the specified port
 - If a destination MAC is not in the table, it is **flooded** out all interfaces except the one it was received

Switch Forwarding Methods

Store-and-forward switching	<ul style="list-style-type: none">• Receives entire frame and ensures the frame is valid.• Cisco's preferred switching method.• 2 Primary Characteristics<ul style="list-style-type: none">○ Error Checking - The switch will check the Frame Check Sequence (FCS) for CRC errors.○ Buffering - The ingress interface will buffer the frame while it checks the FCS. It allows the switch to adjust to a potential difference in speeds between the ingress and egress ports. <p>Bytes</p> <p>Preamble 8 Destination MAC Address 6 Source MAC Address 6 Type 2 ... FCS Checksum (CRC) 4</p> <p>Store-and-forward switching entails receipt of the entire frame (up to about 9,200 bytes for jumbo frames) before a forwarding decision is made.</p>
Cut-through switching	<ul style="list-style-type: none">• Forwards the frame immediately after determining the

	<p>destination MAC address of an incoming frame and the egress port.</p> <ul style="list-style-type: none"> • Cut-through switching mode is enabled by default. • Fragment (Frag) Free method will check the destination and ensure that the frame is at least 64 bytes to eliminate runts 消除乱码. • Suitable for switches requiring latency to be under 10 microseconds. • Does not check FCS, may propagate errors. • May lead to bandwidth issues if the switch propagates too many errors. • Cannot support ports with differing speeds going from ingress to egress <p>The diagram illustrates the structure of a network frame. At the top, a horizontal bar is divided into five segments: Frame Header (purple), Network Header (grey), Transport Header (grey), Data (grey), and another small purple segment. Below this is a large blue triangle representing the frame payload. Inside the triangle, there are four fields: Preamble (8 bytes), Destination MAC Address (6 bytes), Source MAC Address (6 bytes), and Type (2 bytes). To the right of the triangle, an ellipsis indicates more fields, followed by FCS Checksum (CRC) (4 bytes). Orange arrows point from the text labels 'Bytes' to the corresponding field widths below the triangle. A callout box at the bottom states: 'Frames can begin to be forwarded as soon as the Destination MAC is received.'</p>
--	--

Switching Domains

Collision Domains	<p>When will the collision domain happen?</p> <ul style="list-style-type: none"> • One or more devices in half-duplex <p>Effect</p> <ul style="list-style-type: none"> • Lead to contention for the bandwidth 争夺宽带 <p>When will the collision domain be eliminated?</p> <ul style="list-style-type: none"> • Switches eliminate collision domains and reduce congestion • Full duplex on the link
Broadcast Domains	<ul style="list-style-type: none"> • Broadcast domain extends across all Layer 1 or 2 devices on a LAN • Only a layer 3 device (router) will break the broadcast domain (a.k.a. MAC broadcast domain)

	<ul style="list-style-type: none"> When layer 2 switch receives the broadcast, it will flood it out all interfaces except for the ingress interface Congestion and poor network performance may happen if too many broadcasts Broadcast domain will expand when the devices at Layer 1 or 2 are increasing
--	--

Alleviated Network Congestion

- Switches use **MAC address table** and **full-duplex** to **eliminate collisions** and **avoid congestion**.

Protocol	Function
Fast Port Speeds	Switches may have up to 100 Gbps port speeds
Fast Internal Switching	Uses fast internal bus or shared memory to improve performance
Large Frame Buffers	Allows for temporary storage while processing large quantities of frames
High Port Density	<ul style="list-style-type: none"> Provides many ports for devices to be connected to LAN with less cost Provides for more local traffic with less congestion

C2: VLANs

Overview of VLANs

VLAN	<ul style="list-style-type: none">• Logical connections with other similar devices• Provides segmentation of various groups of devices on the same switches• Provide organization that is more manageable<ul style="list-style-type: none">◦ Broadcasts, multicasts and unicasts are isolated in the individual VLAN◦ Each VLAN has its own unique range of IP addressing◦ Smaller broadcast domains
------	---

Benefits of VLANs

Benefits	Description
Smaller Broadcast Domains	Dividing the LAN reduces the number of broadcast domains
Improve Security	Only users in the same VLAN can communicate together
Improved IT Efficiency	VLANs can group devices with similar requirements, e.g. faculty and students
Reduced Cost	One switch can support multiple groups or VLANs
Better Performance	Small broadcast domains reduce traffic, improving bandwidth
Simpler Management	Similar groups will need similar applications and other network resources

Types of VLANs

VLAN Types	Description
Data VLAN	<ul style="list-style-type: none">• Dedicated to user-generated traffic (email and web traffic)• VLAN 1 is default data VLAN as all interfaces are assigned to this VLAN
Native VLAN	<ul style="list-style-type: none">• Used for trunk links only• All frames are tagged on an 802.1Q trunk link except for those on the native VLAN
Management VLAN	<ul style="list-style-type: none">• Used for SSH/Telnet VTY traffic and should not be carried with end user traffic

	<ul style="list-style-type: none"> The VLAN is the SVI (Switch Virtual Interface) for the Layer 2 switch
Voice VLAN	<ul style="list-style-type: none"> Voice traffic requires: <ul style="list-style-type: none"> Assured bandwidth High QoS (Quality of Service) priority Ability to avoid congestion Delay less than 150 ms from source to destination

VLANs in a Multi-Switched Environment

Trunk	<ul style="list-style-type: none"> A point-to-point link between two network devices (e.g. switches) Functions: <ul style="list-style-type: none"> Allow more than one VLAN Extend the VLAN across the entire network Supports all VLANs by default Supports 802.1Q trunking
-------	---

VLAN Configuration

VLAN Ranges on Catalyst Switches

Normal Range VLAN 1 - 1005	Extended Range VLAN 1006 - 4095
Used in Small to Medium sized businesses	Used by Service Providers
1002 - 1005 are reserved for legacy VLANs	Are in Running-Config
1, 1002 - 1005 are auto created and cannot be deleted	Supports fewer VLAN features
Stored in the vlan.dat file in flash	Requires VTP configurations
VTP can synchronize between switches	

VLAN Creation Commands

Task	IOS Command
Enter global configuration mode	configure terminal
Create a VLAN with a valid ID number	vlan <i>vlan-id</i>
Specify a unique name to identify the VLAN	name <i>vlan-name</i>

Return to the privileged EXEC mode	end
Enter global configuration mode	configure terminal

VLAN Port Assignment Commands

Task	IOS Command
Enter global configuration mode	configure terminal
Enter interface configuration mode	interface <i>interface-id</i>
Set the port to access mode	switchport mode access
Assign the port to a VLAN	switchport access vlan <i>vlan-id</i>
Return to the privileged EXEC mode	end

* For Data and Voice VLANs, an **access port** may only be assigned to **one data VLAN**.

Verify VLAN Information

Task	Command Option
Display VLAN name, status and its ports one VLAN per line	brief
Display information about the identified VLAN ID number	id <i>vlan-id</i>
Display information about the identified VLAN name. The <i>vlan-name</i> is an ASCII string from 1 to 32 characters	name <i>vlan-name</i>
Display VLAN summary information	summary

Change VLAN Port Membership

Task	Command Option
Assign another VLAN (for access mode)	switchport access vlan <i>vlan-id</i>
Unassign all VLAN to the port (for access mode)	no switchport access vlan
Show VLAN association	show vlan brief OR

	show interface fa0/18 switchport
--	----------------------------------

Delete VLANs

Task	Command
Delete VLAN	no vlan <i>vlan-id</i>
Delete all VLANs	delete flash:vlan.dat OR delete vlan.dat * Reload switch when deleting all VLANs * To restore to factory default - unplug all data cables, erase the startup-configuration and delete the vlan.dat file, then reload the device

VLAN Trunks

Trunk Configuration Commands

Task	IOS Command
Enter global configuration mode	configure terminal
Enter interface configuration mode	interface <i>interface-id</i>
Set the port to permanent trunking mode	switchport mode trunk
Sets the native VLAN to something other than VLAN 1	switchport trunk native vlan <i>vlan-id</i>
Specify the list of VLANs to be allowed on the trunk link	switchport trunk allowed vlan <i>vlan-id</i>
Return to the privileged EXEC mode	end

Verify Trunk Configuration

Task	IOS Command
Show the interface trunk configuration	show interface fa0/1 switchport

Reset the Trunk to the Default State

Task	IOS Command
Reset the default trunk settings	<pre>interface fa0/1 no switchport trunk allowed vlan no switchport trunk native vlan switchport mode access end</pre>

Dynamic Trunking Protocol

Dynamic Trunking Protocol (DTP)	<ul style="list-style-type: none"> • A proprietary Cisco protocol • On by default on Catalyst 2960 and 2950 switches • Dynamic-auto is default on the 2960 and 2950 switches • May be turned off with the nonegotiate command • May be turned back on by setting the interface to dynamic-auto • Setting a switch to a static trunk or static access will avoid negotiation issues with the switchport mode trunk or the switchport mode access commands
---------------------------------	---

Negotiated Interface Modes

Option	Description
access	Permanent access mode and negotiates to convert the neighboring link into an access link
dynamic auto	Will becomes a trunk interface if the neighboring interface is set to trunk or desirable mode
dynamic desirable	Actively seeks to become a trunk by negotiating with other auto or desirable interfaces
trunk	Permanent trunking mode and negotiates to convert the neighboring link into a trunk link

Results of a DTP Configuration

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access

Trunk	Trunk	Trunk	Trunk	Limited connectivity
Access	Access	Access	Limited connectivity	Access

Verify DTP Mode

Task	Command
Determine the current DTP mode	show dtp interface <i>interface-id</i>

Troubleshooting

Issue	Description
IP Addressing Issues with VLANs	<ul style="list-style-type: none"> Different IP networks must communicate through a router Make sure the IP address assigned to the device is correct which is within the same subnet Solution: ip address <i>ip-address subnet-mask</i>
Missing VLANs	<ul style="list-style-type: none"> If the VLAN to which the port belongs is deleted, the port becomes inactive It will unable to communicate to the rest of network It is not functional until the missing VLAN is created or the VLAN is removed from the port Solution <ul style="list-style-type: none"> vlan <i>vlan-id</i> name <i>vlan-name</i>
Native VLAN Mismatches	<ul style="list-style-type: none"> This may pose a security risk and creates unintended results E.g. one port is defined as VLAN 99 and the other port is defined as VLAN 100 Solution: switchport trunk native vlan <i>vlan-id</i>
Trunk Mode Mismatches	<ul style="list-style-type: none"> This may cause loss of network connectivity E.g. one side of the trunk is configured as an access port Solution: switchport mode trunk
Allowed VLANs on Trunks	<ul style="list-style-type: none"> It may cause unexpected traffic or no traffic to be sent over the trunk

	<ul style="list-style-type: none"> • E.g. the list of allowed VLANs does not support current VLAN trunking requirements • Solution: switchport trunk allowed vlan <i>vlan-id</i>
Incorrect Port Mode	<ul style="list-style-type: none"> • Make sure all the related switches' mode have been switched to trunk mode • Solution: switchport mode trunk
Incorrect VLAN List	<ul style="list-style-type: none"> • Make sure all the required VLAN is set as allowed vlan for the related switchport • Solution: switchport trunk allowed vlan <i>vlan-id</i>

C3: Inter-VLAN Routing

Inter-VLAN Routing Operation

Inter-VLAN Routing	A process of forwarding network traffic from one VLAN to another VLAN.
--------------------	--

Inter-VLAN Routing Options

Legacy Inter-VLAN routing	<ul style="list-style-type: none">• Legacy solution, does not scale well• Relies on using a router with multiple Ethernet interfaces• Each router interfaces connected to a switch port in different VLANs• Router interfaces served as the default gateways to the local hosts on the VLAN subnet• Not scalable and significant limitation:<ul style="list-style-type: none">◦ Relies on physical interfaces◦ Routers have limited number of physical interfaces◦ All physical interfaces of router may easily be used up if each VLAN requires one physical router interface
Router-on-a-Stick	<ul style="list-style-type: none">• Acceptable solution for small to medium-sized network• Uses only one of the router's physical interface• Physical interface is configured as 802.1Q trunk port to understand VLAN tags• Logical subinterfaces are created (1 subinterface per VLAN)• Each subinterface is configured with an IP address from the VLAN it represents• VLAN hosts are configured to use the subinterface address as a default gateway
Layer 3 switch using switched virtual interfaces (SVIs)	<ul style="list-style-type: none">• Most scalable solution for medium to large organizations• Use Layer 3 switches to provide inter-VLAN routing• Use hardware-based switching to achieve higher-packet processing rates than routers• Capabilities:<ul style="list-style-type: none">◦ Route from one VLAN to another using

	<ul style="list-style-type: none"> multiple switched virtual interfaces (SVIs) Convert a Layer 2 switchport to a Layer 3 interface (routed port) which is similar to a physical interface on Cisco IOS router Configure SVIs using the same interface vlan <i>vlan-id</i> command to create management SVI on Layer 2 switch. Layer 3 SVI must be created for each routable VLAN
--	--

Configure Legacy Inter-VLAN Routing

Switch

Task	Command
Create VLAN	vlan <i>vlan-id</i>
Assign interfaces to VLAN	interface <i>interface-id</i> switchport access vlan <i>vlan-id</i>

Router

Task	Command
Assign ip address	interface <i>interface-id</i> ip address <i>ip-address subnet-mask</i>
Turn on the interface	no shutdown

Router-on-a-Stick Inter-VLAN Routing

Configure Router-on-a-Stick

Switch

Task	Command
Enable trunking on switch port	interface <i>interface-id</i> switchport mode trunk

Router

Task	Command
Create subinterface for routable VLAN	interface <i>interface-id.vlan-id</i>
Configure encapsulation dot1Q	encapsulation dot1q <i>vlan-id</i>

Assign IP address	ip address <i>ip-address subnet-mask</i>
Turn on the interface	interface <i>interface-id</i> no shutdown * Use the interface, not the subinterface

Verify Subinterfaces and Routing

Task	Command
Show VLAN	show VLAN
Show IP route	show ip route
Test device connectivity	ping <i>ip-address</i> OR tracert <i>ip-address</i>

Troubleshoot Inter-VLAN Routing

Common Inter-VLAN Issues

Issue Type	How to Fix	How to Verify
Missing VLANs	<ul style="list-style-type: none"> Create (or re-create) the VLAN if it does not exist Ensure host port is assigned to the correct VLAN 	<ul style="list-style-type: none"> show vlan [brief] show interfaces switchport ping
Switch Trunk Port Issues	<ul style="list-style-type: none"> Ensure trunks are configured correctly Ensure port is a trunk port and enabled 	<ul style="list-style-type: none"> show interface trunk show running-conf
Switch Access Port Issues	<ul style="list-style-type: none"> Assign correct VLAN to access port Ensure port is an access port and enabled Host is incorrectly configured in the wrong subnet 	<ul style="list-style-type: none"> show interfaces switchport show running-config interface ipconfig

Router Configuration Issues	<ul style="list-style-type: none"> Router subinterface IPv4 address is incorrectly configured Router subinterface is assigned to the VLAN ID 	<ul style="list-style-type: none"> show ip interface brief show interfaces
-----------------------------	--	--

Inter-VLAN Routing using Layer 3 Switches

Layer 3 Switch Configuration

Step 1	Create VLANs.
Step 2	Create SVI VLAN interfaces. The IP address configured will serve as the default gateway for hosts in the respective VLAN.
Step 3	Configure access ports. Assign the appropriate port to the required VLAN .
Step 4	Enable IP routing. Issue the ip routing global configuration command to allow traffic to be exchanged between different VLANs. This command must be configured to enable inter-VLAN routing on a Layer 3 switch for IPv4.

Layer 3 Switch Inter-VLAN Routing Verification

Task	Command
Verify connectivity from a host to a host in another VLAN	ping <i>ip-address</i>
Verify current host IP configuration	ipconfig

Routing on Layer 3 Switch

- The VLANs have to be advertised using **static or dynamic routing** for being reached by other Layer 3 devices
- Routed port** is configured to enable routing on Layer 3 switch
 - Routed port** is created on Layer 3 switch by **disabling the switchport feature** on Layer 2 port (command: **no switchport**)
 - Configure the interface with an **IPv4 configuration** to connect to router or another Layer 3 switch (command: **ip address *ip-address subnet-mask***)

Routing Configuration on Layer 3 Switch

Step 1	Configure routed port. Use no switchport command to convert the port to a routed port, then assign an IP address and subnet mask. Enable the port.
--------	--

Step 2	Enable routing using ip routing global configuration.
Step 3	Configure routing using appropriate routing method (e.g. Single-Area OSPFv2).
Step 4	Verify routing using show ip route command.
Step 5	Verify connectivity using the ping command.

C4: STP Concepts

Purpose of STP

Spanning Tree Protocol (STP)	<ul style="list-style-type: none">• A loop-prevention network protocol that allows for redundancy while creating a loop-free Layer 2 topology• It logically blocks physical loops in a Layer 2 network, preventing frames from circling the network forever• It compensates for a failure in the network by recalculating and opening up previously blocked ports• It configures a loop-free path through the network by placing “blocking-state” ports
------------------------------	--

Issues with Redundant Switch Links

- **Path redundancy** provides multiple network services by **eliminating the possibility of a single point of failure**
- However, a **Layer 2 loop** may occur when **multiple paths exist between two devices** on an Ethernet network, and there is **no spanning tree implementation on the switches**
- Layer 2 loop may cause **MAC address table instability**, **link saturation** and **high CPU utilization on switches and end-devices** until the **switch unable to forward frames**

Broadcast Storm

- It is an **abnormally high number of broadcasts overwhelming the network** during a specific amount of time
- It can **disable network** within seconds by overwhelming switches and end devices
- It can be caused by hardware problem such as **faulty NIC** or from a **Layer 2 loop** in the network
- **Spanning tree must be enabled** on the switches to prevent these issues (**prevent Layer 2 loops from occurring**)

STP Operations

Step 1	Elect the root bridge
Step 2	Elect the root ports.
Step 3	Elect designated ports.
Step 4	Elect alternate (blocked) ports.

- **Switches use Bridge Protocol Data Units (BPDUs)** to share information about themselves and their connections
- BPDUs are used to **elect root bridge, root ports, designated ports and alternate ports**
- BPDU contains **bridge ID (BID)** that identifies which switch sent the BPDU and helps to **decide root bridge and port roles**
- BID contains **priority value, MAC address of switch and extended system ID** for **finding the lowest BID value**

Elect a Root Port from Multiple Equal-Cost Paths

- When switch has multiple equal-cost paths to the root bridge, determine port using these criteria:
 - Lowest sender BID
 - Lowest sender port priority
 - Lowest sender port ID

STP Convergence - In summary

- 3-step STP Convergence:
 1. Root Bridge Election
 2. Determine Root Port on ALL non-root bridge
 3. Determine Designated Port and Non-Designated Port per segment
- 5-step Decision Sequence:
 1. Lowest Bridge ID (For Root Bridge Election only)
 2. Lowest Root path cost
 3. Lowest SENDER BID
 4. Lowest SENDER port priority
 5. Lowest SENDER port ID

STP Timers and Port States

STP convergence requires 3 timers:

Hello Timer	<ul style="list-style-type: none"> • The hello time is the interval between BPDUs. • The default is 2 seconds but can be modified to between 1 to 10 seconds.
Forward Delay Timer	<ul style="list-style-type: none"> • The forward delay is the time that is spent in the listening and learning state. • The default is 15 seconds but can be modified to between 4 and 30 seconds.
Max Age Timer	<ul style="list-style-type: none"> • The max age is the maximum length of time that a switch waits before attempting to change the STP topology.

	<ul style="list-style-type: none"> The default is 20 seconds but can be modified to between 6 and 40 seconds.
--	--

- The **exchange of BPDU frames** between interconnected switches can help for **determining spanning tree**.
- If switch port transitions directly from blocking state to forwarding state without any information about the full topology, a temporary data loop may be created.

Operational Details of Each Port State

Port State	BDPU	MAC Address Table	Forwarding Data Frames
Blocking	Receive only	No update	No
Listening	Receive and send	No update	No
Learning	Receive and send	Updating table	No
Forwarding	Receive and send	Updating table	Yes
Disabled	None sent or received	No update	No

Evolution of STP

RSTP Concepts

Rapid Spanning Tree Protocol (RSTP) (IEEE 802.1w)	<ul style="list-style-type: none"> Increases the speed of the recalculation of spanning tree when the Layer 2 network topology changes Can achieve faster convergence in a properly configured network (e.g. few hundred milliseconds) It can immediately change alternate port to forwarding state without waiting for the network to converge 3 port states: <ul style="list-style-type: none"> Discarding Learning Forwarding 4 port roles: <ul style="list-style-type: none"> Root Port Designated Port Backup Port (backup to a shared medium like hub) Alternate Port (alternate path to root bridge)
---	---

PortFast and BPDU Guard

Before configure PortFast & BPDU Guard on switch port	<ul style="list-style-type: none">• Switch port will go through listening and learning states when a device is connected to switch port or when a switch powers up• There will be a delay of 15 seconds for each state for total 30 seconds• It may result that IPv4 client will not receive a valid IPv4 address
After configure PortFast & BPDU Guard on switch port	<ul style="list-style-type: none">• Port transitions from blocking to forwarding state immediately, avoiding 30 seconds delay• PortFast should be used on access ports only (spanning tree loop may happen if enable PortFast on a port connecting to another switch)• PortFast-enabled switch port should never receive BPDUs, else causing spanning tree loop• BPDU guard puts switch port in errdisabled (error-disabled) state upon receipt of any BPDU (prevent loops by shutting down the port, admin must manually put interface back into service)

C5: EtherChannel

Link Aggregation

- Allow redundant links between devices that will not be blocked by STP using EtherChannel.
- **Groups multiple physical Ethernet links together into one single logical link.**
- Provide **fault-tolerance, load sharing, increased bandwidth and redundancy** between switches, routers and servers.
- EtherChannel technology **combines a number of physical links between switches to increase overall speed** of switch-to-switch communication.

EtherChannel

Description	<ul style="list-style-type: none">• LAN switch-to-switch technique of grouping several Fast Ethernet or Gigabit Ethernet ports into one logical channel.• Virtual interface (a.k.a port channel) will be created after configuring EtherChannel.• Physical interfaces are bundled together into a port channel interface.
Advantages	<ul style="list-style-type: none">• Most configuration tasks can be done on the EtherChannel interface instead of on each individual port, ensuring configuration consistency throughout the links.• Relies on existing switch ports, no need to upgrade the link to a faster and more expensive connection to have more bandwidth.• Load balancing takes place between links that are part of the same EtherChannel.• Helps Spanning Tree Protocol (STP) to block a connection for preventing switching loops, it blocks the whole EtherChannel instead of individual cables. When there is only one EtherChannel link, all physical links in the EtherChannel are active because STP sees only one logical link.• When one physical cable fails, the other in the channel still carries traffic.
Code Implementation	# S1 int range f0/1-2 switchport mode trunk switchport trunk allowed vlan 10, 20 channel-group 1 mode on int port-channel 1 switchport mode trunk switchport trunk allowed vlan 10, 20

```

# S2
int range f0/1-2
switchport mode trunk
switchport trunk allowed vlan 10, 20
channel-group 1 mode on

int port-channel 1
switchport mode trunk
switchport trunk allowed vlan 10, 20

```

PAgP Operation

Description	<ul style="list-style-type: none"> Cisco-proprietary protocol that aids in automatic creation of EtherChannel links. PAgP packets are sent between EtherChannel-capable ports to negotiate the forming of a channel. When PAgP identifies matched Ethernet links, it groups the links into an EtherChannel. EtherChannel is then added to the spanning tree as a single port. PAgP checks for configuration consistency and manages link additions and failures between two switches. All ports in the same EtherChannel must have the same speed, duplex setting and VLAN information.
Modes	<ul style="list-style-type: none"> On: forces the interface to channel without PAgP. Interfaces configured in the <i>on</i> mode do not exchange PAgP packets. PAgP desirable: places an interface in an active negotiating state in which the interface initiates negotiations with other interfaces by sending PAgP packets. PAgP auto: places an interface in a passive negotiating state in which the interface responds to the PAgP packets that it receives but does not initiate PAgP negotiation.
Code	<pre> # S1 int range f0/1-2 switchport mode trunk switchport trunk allowed vlan 10, 20 channel-group 1 mode [on / desirable / auto] int port-channel 1 switchport mode trunk switchport trunk allowed vlan 10, 20 # S2 </pre>

```

int range f0/1-2
switchport mode trunk
switchport trunk allowed vlan 10, 20
channel-group 1 mode [on / desirable / auto]

int port-channel 1
switchport mode trunk
switchport trunk allowed vlan 10, 20

```

PAgP Mode Settings Example

PAgP Mode Settings Example		
S1	S2	Channel Establishment
On	On	Yes
On	Desirable / Auto	No
Desirable	Desirable	Yes
Desirable	Auto	Yes
Auto	Desirable	Yes
Auto	Auto	No

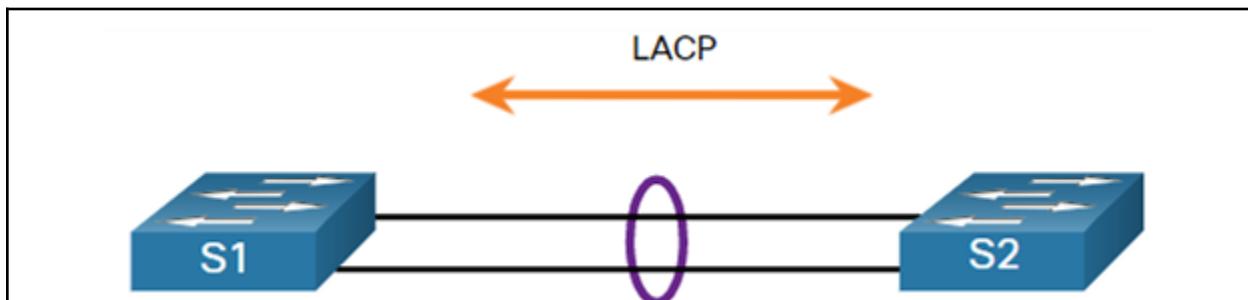
The diagram shows two blue rectangular boxes labeled 'S1' and 'S2' representing switches. They are connected by a horizontal line with a purple circle in the center. Above the line, there is a double-headed orange arrow pointing left and right, representing the PAgP protocol exchange between the two switches.

LACP Operation

Description	<ul style="list-style-type: none"> Part of IEEE specification (802.3ad) that allows several physical ports to be bundled to form a single logical channel. Can be used to facilitate EtherChannels in multivendor environments
Modes	<ul style="list-style-type: none"> On: forces the interface to channel without LACP. Interfaces configured in the on mode do not exchange LACP packets. LACP active: places a port in an active negotiating state. In this state, the port initiates negotiations with other ports by sending LACP packets. LACP passive: places a port in a passive negotiating state. In this state, the port responds to the LACP packets that it receives but does not initiate LACP packet negotiation.

Code	<pre># S1 int range f0/1-2 switchport mode trunk switchport trunk allowed vlan 10, 20 channel-group 1 mode [on / active / passive] int port-channel 1 switchport mode trunk switchport trunk allowed vlan 10, 20 # S2 int range f0/1-2 switchport mode trunk switchport trunk allowed vlan 10, 20 channel-group 1 mode [on / active / passive] int port-channel 1 switchport mode trunk switchport trunk allowed vlan 10, 20</pre>
------	---

LACP Mode Settings Example



S1	S2	Channel Establishment
On	On	Yes
On	Active / Passive	No
Active	Active	Yes
Active	Passive	Yes
Passive	Active	Yes
Passive	Passive	No

Configuration Guidelines

EtherChannel support	All Ethernet interfaces must support EtherChannel with no requirement that interfaces be physically contiguous.
Speed and duplex	Configure all interfaces in an EtherChannel to operate at the same speed and in the same duplex mode .
VLAN match	All interfaces in the EtherChannel bundle must be assigned to the same VLAN or be configured as a trunk .
Range of VLANs	An EtherChannel supports the same allowed range of VLANs on all the interfaces in a trunking EtherChannel. If the allowed range of VLANs is not the same , the interfaces do not form an EtherChannel , even when they are set to auto or desirable mode.

Verify EtherChannel

<i>show interfaces port-channel</i>	Displays the general status of the port channel interface
<i>show etherchannel summary</i>	Displays one line of information per port channel
<i>show etherchannel port-channel</i>	Displays information about a specific port channel interface
<i>show interfaces etherchannel</i>	Provide information about the role of a physical member interface of the EtherChannel

C6: FHRP Concepts

First Hop Redundancy Protocols (FHRPs)

Description	Mechanisms that provide alternate default gateways in switched networks where two or more routers are connected to the same VLANs.
Virtual router implementation	<ul style="list-style-type: none">To prevent a single point of failure at the default gatewayMultiple routers are configured to work together to present the illusion of a single router to the hosts on the LANTwo or more routers can act as a single virtual router by sharing an IP address and a MAC addressIPv4 address of the virtual router is configured as the default gateway of the workstations on a specific IPv4 segment.

Step for Router Failover

- When the **active router fails**, the redundancy protocol **transitions the standby router to the new active router role**.
- Steps take place when the active router fails:
 - The standby router stops seeing Hello messages from the forwarding router.
 - The standby router assumes the role of the forwarding router.
 - Because the **new forwarding router assumes both the IPv4 and MAC addresses of the virtual router**, the host devices see no disruption in service.

HSRP

Purpose	<ul style="list-style-type: none">Avoid losing outside network access if the default router failsHSRP is a Cisco-proprietary FHRP that is designed to allow for transparent failover of a first-hop IP device.Ensures high network availability by providing first-hop routing redundancy for IP hosts on networks configured with an IP default gateway address.
Usage	<ul style="list-style-type: none">Used in a group of routers for selecting an active device and a standby deviceActive device: used for routing packetsStandby device: takes over when the active device fails, or when pre-set conditions are met.
Priority	<ul style="list-style-type: none">By default, the router with the numerically highest IPv4 address is elected as the active router.HSRP priority can be used to determine the active router.Router with the highest HSRP priority will become an active router.By default, the HSRP priority is 100.If the priorities are equal, the router with the numerically highest IPv4 address is elected as the active router.

	<ul style="list-style-type: none"> Range of HSRP priority: 0 - 255
Preemption	<ul style="list-style-type: none"> By default, after a router becomes the active router, it will remain the active router even if another router comes online with a higher HSRP priority. Preemption must be enabled using <i>standby preempt</i> interface command to force a new HSRP election process Preemption: ability of HSRP router to trigger the re-election process to only allow router to become the active router if it has a higher priority When enabled, a router that comes online with a higher HSRP priority will assume the role of the active router.
Code	<pre>int f0/0.10 standby 1 ip 192.168.10.3 standby 1 priority 105 standby 1 preempt</pre>

HSRP States and Times

HSRP State	Description
Initial	This state is entered through a configuration change or when an interface first becomes available
Learn	The router has not determined the virtual IP address and has not yet seen a hello message from the active router. In this state, the router waits to hear from the active router.
Listen	The router knows the virtual IP address , but the router is neither the active router nor the standby router. It listens for hello messages from those routers.
Speak	The router sends periodic hello messages and actively participates in the election of the active and / or standby router.
Standby	The router is a candidate to become the next active router and sends periodic hello messages.
Active	The router won the election .

- Hello packets are sent** to the HSRP group multicast address **every 3 seconds** by default.
- Standby router** will become **active** if it **does not receive a hello message from the active router after 10 seconds**.

C7: Routing Concepts

Routing	<ul style="list-style-type: none">When a router receives an IP packet on one interface, it determines which interface to use to forward the packet to the destination.Primary functions of a router are to determine the best path to forward packets based on the information in its routing table, and to forward packets toward their destination.
---------	---

Best Path Equals Longest Match

- Best path: Longest match**
- Routing table contains route entries consisting of a **prefix (network address)** and **prefix length**.
- A minimum number of far-left bits must match between the IP address of the packet and the route in the routing table.
- The prefix length of the route in the routing table is used to determine the minimum number of far-left bits that must match.
- The **longest match** is the route in the routing table that has the **greatest number of far-left matching bits** with the **destination IP address of the packet**. The longest match is always the **preferred route**.

Path Determination

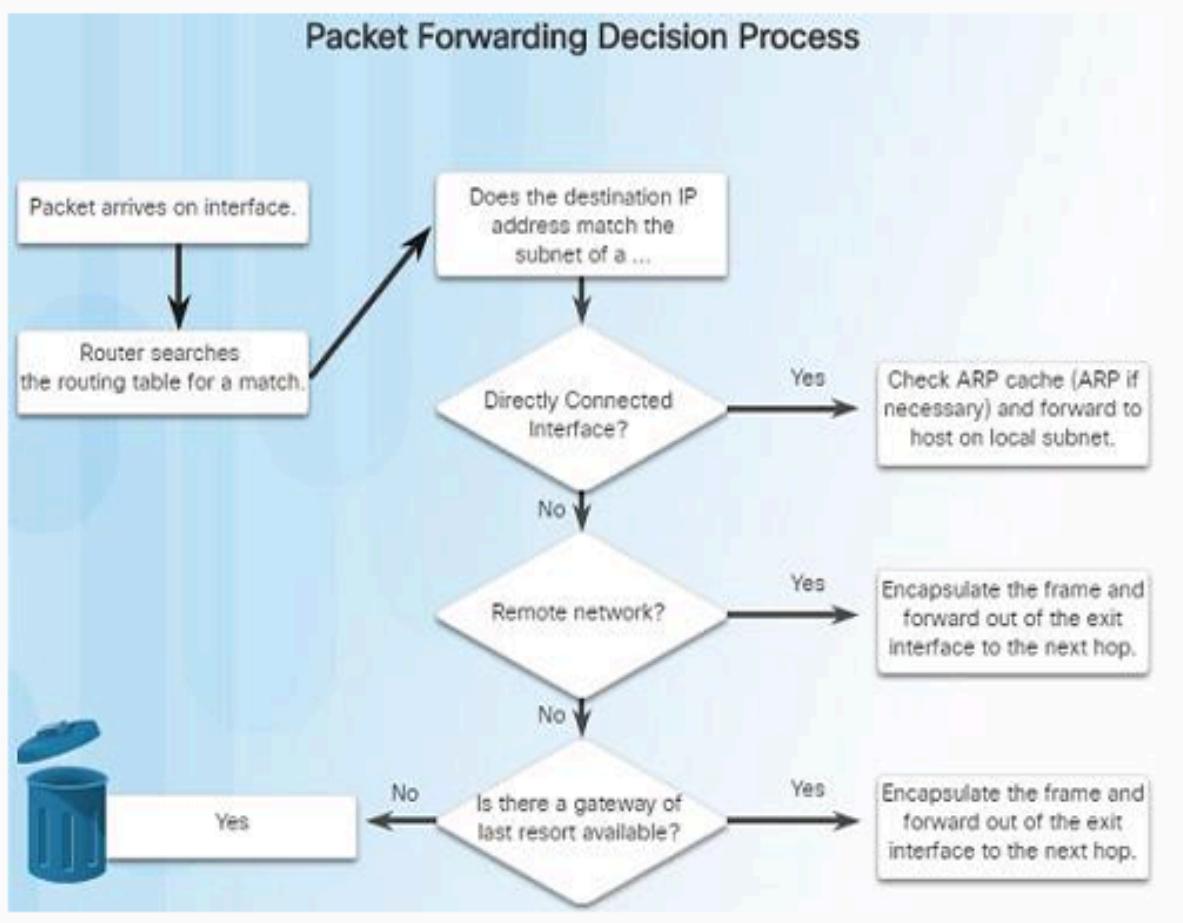
IPv4 Longest Match Example

In the table, an IPv4 packet has the **destination IPv4 address 172.16.0.10**. The router has three route entries in its IPv4 routing table that match this packet: 172.16.0.0/12, 172.16.0.0/18, and 172.16.0.0/26. Of the three routes, 172.16.0.0/26 has the **longest match** and would be **chosen to forward the packet**. For any of these routes to be considered a match there must be **at least** the number of matching bits indicated by the subnet mask of the route.

Destination IPv4 Address		Address in Binary
172.16.0.10		10101100.00010000.00000000.00001010
Route Entry	Prefix/Prefix Length	Address in Binary
1	172.16.0.0/12	10101100.00010000.00000000.00001010
2	172.16.0.0/18	10101100.00010000.00000000.00001010
3	172.16.0.10 172.16.0.0/26	10101100.00010000.00000000.00001010 10101100.00010000.00000000.00000000

*Path Determination

Routing Decisions



Directly Connected Networks	<ul style="list-style-type: none"> Added to the routing table when a local interface is configured with an IP address and subnet mask (prefix length) and is active (up and up). If the destination IP address belongs to a network that is directly connected to the router, the packet is forwarded out of that interface.
Remote Networks	<ul style="list-style-type: none"> Networks that are not directly connected to the route. Routers learn about remote networks in two ways: <ul style="list-style-type: none"> Static routes: Added to the routing table when a route is manually configured. Dynamic routing protocols: Added to the routing table when routing protocols dynamically learn about the remote network. If the destination IP address of the packet belongs to a remote network, the packet is forwarded to another router.
Default Route	Specifies a next-hop router to use when the routing table does not

	<p>contain a specific route that matches the destination IP address. The default route can be entered manually as a static route, or learned automatically from a dynamic routing protocol.</p> <ul style="list-style-type: none"> • Default route has a /0 prefix length (no bits need to match the destination IP address for route entry to be used) • It also acts as a gateway of last resort if no route is determined.
--	---

Best Path

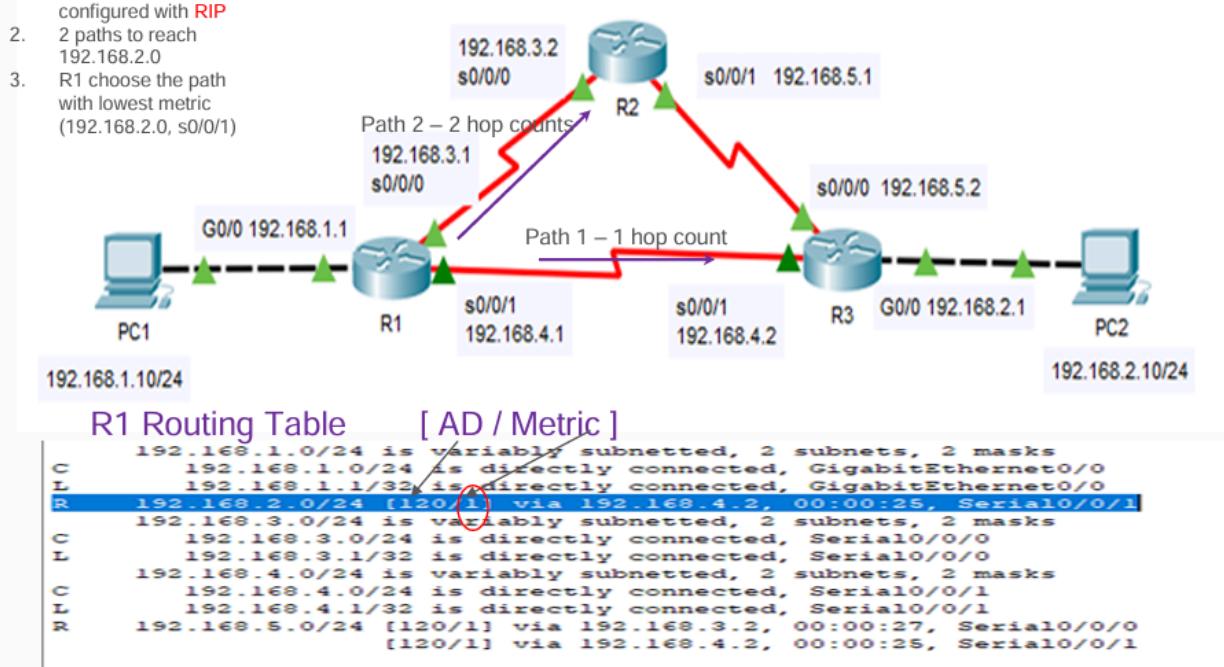
- Best path is selected based on the metric or value that is used by the routing protocol.
- The best path to a network is the path with the lowest metric. A metric is a value that is used to measure the distance to a given network.
- Dynamic routing protocols:

Routing Information Protocol (RIP)	Hop count
Open Shortest Path First (OSPF)	Cisco's cost based cumulative bandwidth from source to destination
Enhanced Interior Gateway Routing Protocol (EIGRP)	Bandwidth, delay, load, reliability

Routing Information Protocol (RIP)

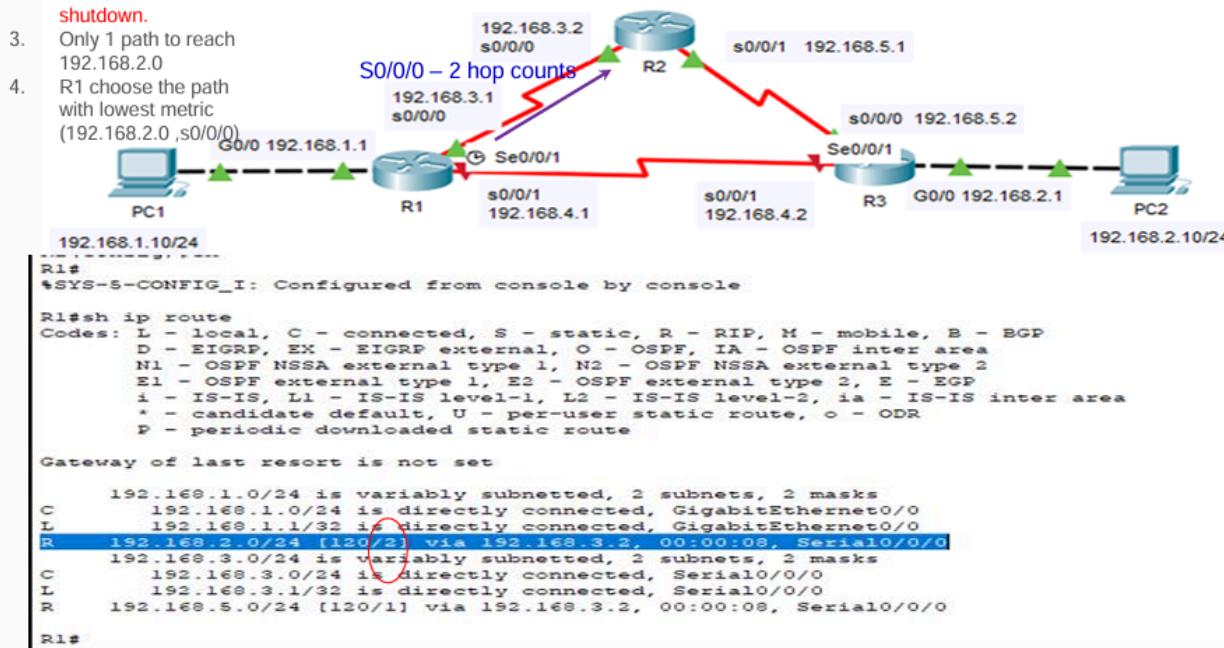
Scenario 1:

1. All routers had been configured with **RIP**
2. 2 paths to reach 192.168.2.0
3. R1 choose the path with lowest metric (192.168.2.0, s0/0/1)



Scenario 2:

1. All routers had been configured with **RIP**
2. R1 s0/0/1 is shutdown.
3. Only 1 path to reach 192.168.2.0
4. R1 choose the path with lowest metric (192.168.2.0, s0/0/0)

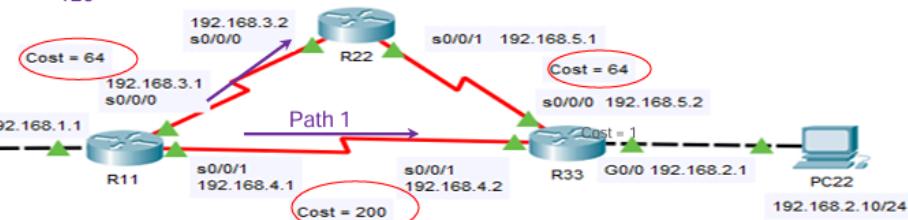


Open Shortest Path First (OSPF)

Scenario 1:

- All routers had been configured with **OSPF**
- 2 paths to reach 192.168.2.0
- R1 choose the path with lowest metric (192.168.2.0, s0/0/0)

$$\begin{aligned} \text{Path 2} \\ = 64 + 64 + 1 \\ = 129 \end{aligned}$$



```

R1#sh ip route
Codes: L - local, 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, 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

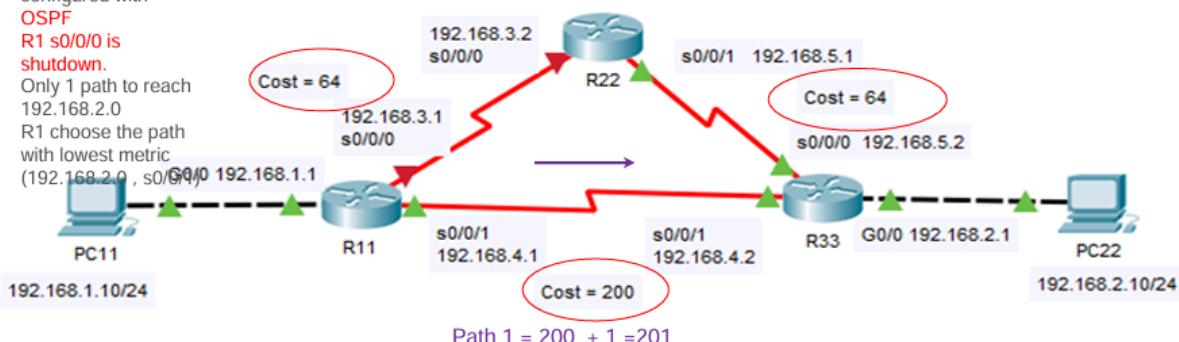
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, GigabitEthernet0/0
L        192.168.1.1/32 is directly connected, GigabitEthernet0/0
O * 192.168.2.0/24 [110/129] via 192.168.3.2, 00:05:41, Serial0/0/0
      192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.3.0/24 is directly connected, Serial0/0/0
L        192.168.3.1/32 is directly connected, Serial0/0/0
      192.168.4.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.4.0/24 is directly connected, Serial0/0/1
L        192.168.4.1/32 is directly connected, Serial0/0/1
O   192.168.5.0/24 [110/128] via 192.168.3.2, 00:05:41, Serial0/0/0

R1#
Ctrl+F6 to exit CLI focus

```

Scenario 2:

- All routers had been configured with **OSPF**
- R1 s0/0/0 is shutdown.
- Only 1 path to reach 192.168.2.0
- R1 choose the path with lowest metric (192.168.2.0, s0/0/1)



$$\text{Path 1} = 200 + 1 = 201$$

```

Gateway of last resort is not set

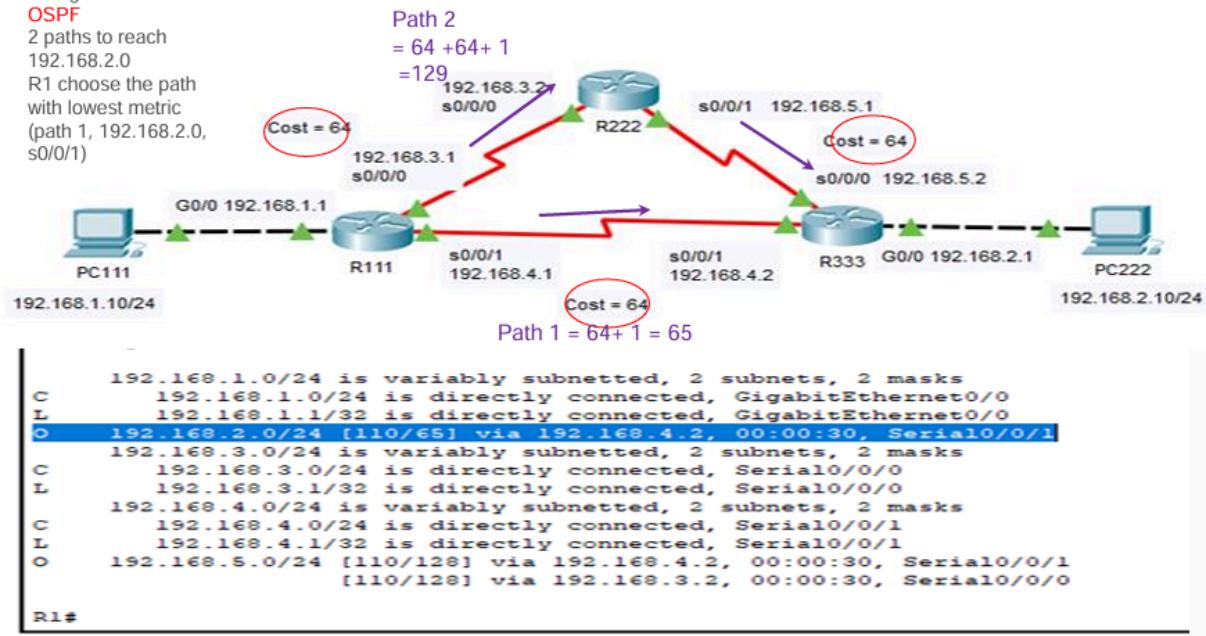
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, GigabitEthernet0/0
L        192.168.1.1/32 is directly connected, GigabitEthernet0/0
O * 192.168.2.0/24 [110/201] via 192.168.4.2, 00:00:01, Serial0/0/1
      192.168.4.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.4.0/24 is directly connected, Serial0/0/1
L        192.168.4.1/32 is directly connected, Serial0/0/1
O   192.168.5.0/24 [110/264] via 192.168.4.2, 00:00:01, Serial0/0/1

R1#

```

Scenario 3:

- All routers had been configured with **OSPF**
- 2 paths to reach 192.168.2.0
- R1 choose the path with lowest metric (path 1, 192.168.2.0, s0/0/1)



Load Balancing

- If a router has **two or more paths** with **identical metrics** to the same destination network, the router will forward the packets using **both paths equally**.
- The routing table contains a single destination network, but has multiple exit interfaces - one for each equal cost path. This is referred to as **equal cost load balancing**.
- Load balancing can increase **the effectiveness and performance** of the network.
- EIGRP** supports **unequal** cost load balancing.

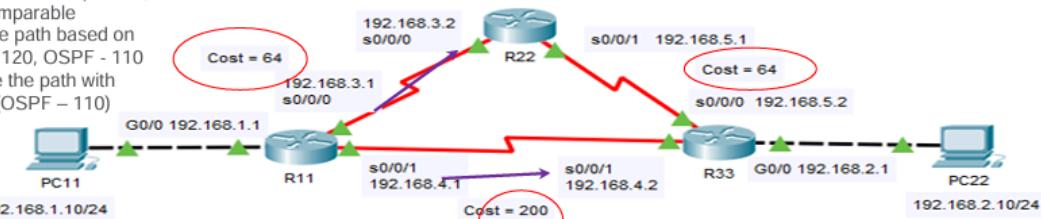
Administrative Distance

- If a router has **multiple routing protocols** configured and static routes, it is possible that the routing table might have **more than one route source for the same destination network**.
- Each routing protocol** might prefer a **different path** to reach the same destination.
- Cisco IOS uses the **administrative distance (AD)** to determine which route to install in the routing table.
- The AD represents the "**trustworthiness**" of the route. The **lower** the AD, the more **trustworthy**.

Default Administrative Distances

Route Source	Administrative Distance
Connected	0
Static	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
External EIGRP	170
Internal BGP	200

1. All routers had been configured with **OSPF** and **RIP**
2. Metrics (cost and hop count) are not comparable
3. Choose the path based on AD. RIP – 120, OSPF - 110
4. R1 choose the path with lower AD (OSPF – 110)



```

R1#sh ip route
Codes: L - local, 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, 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

      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
      C    192.168.1.0/24 is directly connected, GigabitEthernet0/0
      L    192.168.1.1/32 is directly connected, GigabitEthernet0/0
      O    192.168.2.0/24 [110/129] via 192.168.3.2, 00:05:41, Serial0/0/0
          192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
          C    192.168.3.0/24 is directly connected, Serial0/0/0
          L    192.168.3.1/32 is directly connected, Serial0/0/0
          192.168.4.0/24 is variably subnetted, 2 subnets, 2 masks
          C    192.168.4.0/24 is directly connected, Serial0/0/1
          L    192.168.4.1/32 is directly connected, Serial0/0/1
          O    192.168.5.0/24 [110/128] via 192.168.3.2, 00:05:41, Serial0/0/0

R1#

```

Ctrl+F6 to exit CLI focus

R1 Routing Table [AD / Metric]

```

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.168.1.0/24 is directly connected, GigabitEthernet0/0
L   192.168.1.1/32 is directly connected, GigabitEthernet0/0
R  192.168.2.0/24 [120/1] via 192.168.4.2, 00:00:25, Serial0/0/1
192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.168.3.0/24 is directly connected, Serial0/0/0
L   192.168.3.1/32 is directly connected, Serial0/0/0
192.168.4.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.168.4.0/24 is directly connected, Serial0/0/1
L   192.168.4.1/32 is directly connected, Serial0/0/1
R  192.168.5.0/24 [120/1] via 192.168.3.2, 00:00:27, Serial0/0/0
                                [120/1] via 192.168.4.2, 00:00:25, Serial0/0/1

```

EIGRP

- Enhanced IGRP is a Cisco-proprietary distance-vector routing protocol released in 1992.
- EIGRP was created as a classless version of IGRP.
- Ideal choice for large, multiprotocol networks built primarily on Cisco routers.

Implement EIGRP for IPv4

- Autonomous System (AS) is a collection of networks under the control of a single authority. (reference RFC 1930).
- AS numbers are needed to exchange routes between AS.
- AS numbers are usually 16-bit numbers, ranging from 0 to 65535.

Configuration Command
router eigrp [AS-group] eigrp router-id [ipv4-address] network [network-number] [wildcard-mask] passive-interface [interface] ip route 0.0.0.0 0.0.0.0 [interface] redistribute static

IP Route Common Indicators

Code	Meaning	Description
D	EIGRP	The route was learned dynamically via EIGRP (Enhanced Interior Gateway Routing Protocol).
C	Connected	The network is directly connected to one of the router's interfaces.
S	Static	The route was manually configured (a static route).
S*	Static + Default	This is a static default route , often written as S* 0.0.0.0/0 , which is used when no other specific route matches the destination IP.

EX	External learned EIGRP	It is an external EIGRP route (learned from outside the EIGRP autonomous system)
-----------	------------------------	---

*C8: LAN Security Concepts

*AAA Components

- AAA stands for Authentication, Authorization and Accounting, and provides the primary framework to set up access control on a network device.
- AAA is a way to control
 - who is permitted to access a network (authenticate)
 - what they can do while they are there (authorize)
 - audit what actions they performed while accessing the network (accounting)

Authentication

Methods of Implementing AAA Authentication

Local AAA Authentication	<ul style="list-style-type: none">• Method stores usernames and passwords locally in a network device• Users authenticate against the local database• Local AAA is ideal for small networks
Server-Based AAA Authentication	<ul style="list-style-type: none">• Router accesses a central AAA server• AAA server contains the usernames and password for all users• Router uses either the Remote Authentication Dial-In User Service (RADIUS) or Terminal Access Controller Access Control System (TACACS+) protocols to communicate with AAA server• When there are multiple routers and switches, server-based AAA is more appropriate

Authorization

- AAA authorization is **automatic** and does not require users to perform additional steps after authentication.
- Authorization **governs what users can and cannot do** on the network after they are authenticated.
- Authorization uses a set of **attributes** that describes the user's access to the network. These attributes are used by the AAA server to **determine privileges and restrictions** for that user.

Accounting

- AAA accounting **collects and reports usage data** used for **auditing or billing** purposes.
- Collected data might include the **start and stop connection times, executed commands, number of packets and number of bytes**.

- Primary use of accounting is to combine it with AAA authentication:
 - **AAA server** keeps a **detailed log** of exactly what the authenticated user does on the device. This includes all EXEC and configuration commands issued by the user.
 - The log contains numerous data fields, including the **username, the date and time, and the actual command** that was entered by the user. This information is useful when **troubleshooting devices**. It also **provides evidence for when individuals perform malicious acts**.

802.1X

- IEEE 802.1X standard is a **port-based access control and authentication protocol**.
- This protocol **restricts unauthorized workstations from connecting to a LAN through publicly accessible switch ports**.
- Authentication server **authenticates** each **workstation** that is connected to a switch port before making available any services offered by the switch or the LAN.

Client (Supplicant)	This is a device running 802.1X-compliant client software , which is available for wired or wireless devices.
Switch (Authenticator)	<ul style="list-style-type: none"> • The switch acts as an intermediary between the client and the authentication server. • It requests identifying information from the client, verifies that information with the authentication server, and relays a response to the client. • Another device that could act as an authenticator is a wireless access point.
Authentication server	The server validates the identity of the client and notifies the switch or wireless access point that the client is or is not authorized to access the LAN and switch services.

Layer 2 Security Threats

Switch Attack Categories

Category	Examples
MAC Table Attacks	Includes MAC address flooding attacks .
VLAN Attacks	Includes VLAN hopping and VLAN double-tagging attacks . It also includes attacks between devices on a common VLAN.
DHCP Attacks	Includes DHCP starvation and DHCP spoofing attacks .
ARP Attacks	Includes ARP spoofing and ARP poisoning attacks .

Address Spoofing Attacks	Includes MAC address and IP address spoofing attacks .
STP Attacks	Includes Spanning Tree Protocol manipulation attacks .

Switch Attack Mitigation Techniques

Solution	Description
Port Security	Prevents many types of attacks including MAC address flooding attacks and DHCP starvation attacks .
DHCP Snooping	Prevents DHCP starvation and DHCP spoofing attacks .
Dynamic ARP Inspection (DAI)	Prevents ARP spoofing and ARP poisoning attacks .
IP Source Guard (IPSG)	Prevents MAC and IP address spoofing attacks .

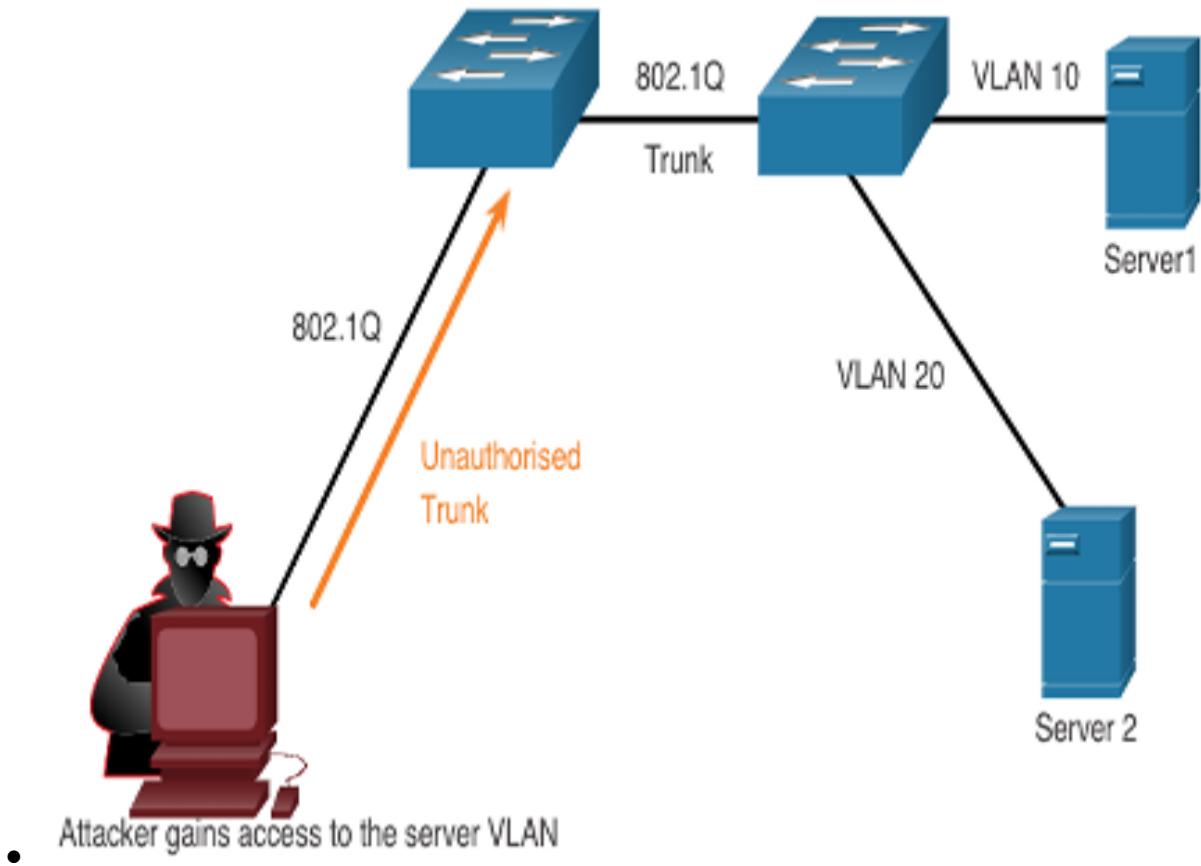
MAC Address Table Flooding

Description	<ul style="list-style-type: none"> All MAC tables have a fixed size and a switch can run out of resources when storing MAC addresses. Attackers bombard the switch with fake source MAC addresses until the switch MAC address table is full. When this occurs, the switch treats the frame as an unknown unicast and begins to flood all incoming traffic out all ports on the same VLAN without referencing the MAC table. This condition allows a threat actor to capture all of the frames sent from one host to another on the local LAN or local VLAN. This will also affect other connected Layer 2 switches. When the MAC address table of a switch is full, it starts flooding out all ports including those connected to other Layer 2 switches.
Mitigation	<ul style="list-style-type: none"> Network administrators must implement port security. It allows a specified number of source MAC addresses to be learned on the port.

LAN Attacks

VLAN Hopping Attacks

- Enables traffic from one VLAN to be seen by another VLAN without the aid of a router.
- Threat actor configures a host to act like a switch to take advantage of the automatic trunking port feature enabled by default on most switch ports.
- Configures the host to spoof 802.1Q signaling and Cisco-proprietary Dynamic Trunking Protocol (DTP) signaling to trunk with the connecting switch.
- If successful, the switch establishes a trunk link with the host and accesses all the VLANs on the switch.
- Threat actors can send and receive traffic on any VLAN, effectively hopping between VLANs.



VLAN Double-Tagging Attacks

- Threat actor sends a double-tagged 802.1Q frame to the switch. The outer header has the VLAN tag of the threat actor, which is the same as the native VLAN of the trunk port.

- The frame arrives on the first switch, which looks at the first 4-byte 802.1Q tag. The switch sees that the frame is destined for the native VLAN. The switch forwards the packet out to all native VLAN ports after stripping the VLAN tag. The frame is not retagged because it is part of the native VLAN. The inner VLAN tag is still intact and has not been inspected by the first switch.
- The frame arrives at the second switch which has no knowledge that it was supposed to be for the native VLAN. Native VLAN traffic is not tagged by the sending switch as specified in the 802.1Q specification. The second switch looks only at the inner 802.1Q tag that the threat actor inserted and sees that the frame is destined for the target VLAN. The second switch sends the frame on to the target or floods it, depending on whether there is an existing MAC address table entry for the target.

VLAN Hopping & VLAN Double-Tagging Attack Mitigation

- Disable trunking on all access ports
- Disable auto trunking on trunk links so that trunks must be manually enabled
- Be sure that the native VLAN is only used for trunk links

DHCP Attacks

- DHCP servers dynamically provide IP configuration information including:
 - IP address
 - Subnet mask
 - Default gateway
 - DNS servers
 - More to Clients
- 2 types of DHCP attacks are DHCP starvation and DHCP spoofing. Both attacks are mitigated by implementing DHCP snooping.

DHCP Starvation Attack	<ul style="list-style-type: none"> • Create a DoS for connecting clients • Require an attack tool such as Gobbler which can look at the entire scope of leasable IP addresses and tries to lease them all • It creates DHCP discovery messages with bogus MAC addresses
DHCP Spoofing Attack	<ul style="list-style-type: none"> • Occurs when a rogue DHCP server is connected to the network and provides false IP configuration parameters to legitimate clients • Wrong default gateway: provides invalid gateway or IP address of its host to create man-in-the-middle attack • Wrong DNS server: provides incorrect DNS server address pointing the user to a nefarious website • Wrong IP address: provides invalid IP address effectively creating a DoS attack on the DHCP client

ARP Attacks

- Hosts **broadcast ARP Requests** to determine the MAC address of a host with a destination IP address.
- An attacker **sends a gratuitous ARP message containing a spoofed MAC address** to a switch, and the switch would **update its MAC table accordingly**.
- Threat actor **sends unsolicited ARP Replies** to other hosts on the subnet with the MAC Address of the threat actor and the IP address of the default gateway, effectively setting up a **man-in-the-middle attack**.
- ARP spoofing and ARP poisoning are **mitigated by implementing Dynamic ARP Inspection (DAI)**.

Address Spoofing Attacks

- **IP address spoofing** is when a threat actor **hijacks a valid IP address of another device** on the subnet or uses a random IP address.
- **Difficult to mitigate**, especially when it is used inside a subnet in which the IP belongs
- **MAC address spoofing attacks** occur when the threat actors **alter the MAC address of their host** to match another known MAC address of a target host. The switch **overwrites the current MAC table entry and assigns the MAC address to the new port**. It then inadvertently **forwards frames destined for the target host to the attacking host**.
- IP and MAC address spoofing can be **mitigated by implementing IP Source Guard (IPSG)**.

STP Attack

- Network attackers manipulate the Spanning Tree Protocol (STP) to conduct an attack by **spoofing the root bridge and changing the topology of a network**.
- Attackers can then **capture all traffic for the immediate switched domain**.
- Attacking host broadcasts STP bridge protocol data units (BPDUs) containing configuration and topology changes that will force spanning-tree recalculations.
- The BPDUs sent by the attacking host announce a lower bridge priority for being elected as the root bridge.
- STP attack is **mitigated by implementing BPDU Guard on all access ports**.

*C9: Switch Security Configuration

Mitigate MAC Address Table Attacks

Mitigation	<ul style="list-style-type: none">• Enable port security with the switchport port-security interface configuration command• Limit the maximum number of MAC addresses on a port• Configure the way to learn about MAC addresses on a secure port• Set aging time for static and dynamic secure addresses on a port• Set port security violation mode <p>* Port security can only be configured on manually configured access ports or manually configured trunk ports.</p>
------------	--

Enable Port Security

```
interface f0/1  
switchport mode access  
switchport port-security  
end
```

Limit Maximum Number of MAC Addresses

```
switchport port-security maximum [value]
```

Configure Way to Learn MAC Addresses

Manually Configured

The administrator manually configures a **static MAC address(es)** by using the following command for each secure MAC address on the port

```
switchport port-security mac-address [mac-address]
```

Dynamically Learned

When the **switchport port-security** command is entered, the **current source MAC** for the device connected to the port is **automatically secured but is not added to the running configuration**. If the switch is **rebooted**, the port will have to **re-learn the device's MAC address**.

```
switchport port-security
```

Dynamically Learned - Sticky

The administrator can enable the switch to dynamically learn the MAC address and “**stick**” them to the **running configuration**

```
switchport port-security mac-address sticky
```

Port Security Aging

- Set aging time for static and dynamic secure addresses on a port

Absolute

The secure addresses on the port are deleted after the specified aging time

```
switchport port-security aging time 10  
switchport port-security aging type absolute
```

Inactivity

The secure addresses on the port are deleted if they are inactive for a specified time

```
switchport port-security aging time 10  
switchport port-security aging type inactivity
```

Port Security Violation Modes

- If the MAC address of a device attached to a port differs from the list of secure addresses, then a port violation occurs and the port enters the error-disabled state.

Mode	Description
shutdown (default)	<ul style="list-style-type: none">• The port transitions to the error-disabled state immediately• Turns off the port LED• Sends a syslog message• Increments violation counter• When a secure port is in the error-disabled state, the administrator must re-enable it by entering the shutdown and no shutdown commands.
restrict	<ul style="list-style-type: none">• The port drops packets with unknown source addresses until admin removes a sufficient number of secure MAC addresses to drop below the maximum value or increase the maximum value• Increments Security Violation counter• Generates a syslog message
protect	<ul style="list-style-type: none">• Least secure of the security violation modes• The port drops packets with unknown MAC source addresses until admin removes a sufficient number of secure MAC addresses to drop below the maximum value or increase the maximum value• No syslog message is sent

Port Security Violation Modes

Violation Mode	Discards Offending Traffic	Sends Syslog Message	Increase Violation Counter	Shuts Down Port
Protect	Yes	No	No	No
Restrict	Yes	Yes	Yes	No
Shutdown	Yes	Yes	Yes	Yes

Mitigate VLAN Attacks

- Spoofing DTP messages from the attacking host to cause the switch to enter trunking mode.
- Attacker sends traffic tagged with the target VLAN, and the switch then delivers the packets to the destination.
- Attackers can access all the VLANs on the victim switch from the rogue switch via introducing rogue switch and enabling trunking.
- Attacker uses double-tagging attack to execute VLAN hopping attack.

Steps to Mitigate VLAN Hopping Attacks:

1. Disable DTP (auto trunking) negotiations on non-trunking ports by using the switchport mode access interface configuration command.	<pre>S1(config)# interface range fa0/1 - 16 S1(config-if-range)# switchport mode access S1(config-if-range)# exit S1(config)# S1(config)# interface range fa0/17 - 20 S1(config-if-range)# switchport mode access S1(config-if-range)# switchport access vlan 1000 S1(config-if-range)# shutdown S1(config-if-range)# exit S1(config)# S1(config)# interface range fa0/21 - 24 S1(config-if-range)# switchport mode trunk S1(config-if-range)# switchport nonegotiate S1(config-if-range)# switchport trunk native vlan 999 S1(config-if-range)# end S1#</pre>
2. Disable unused ports and put them in an unused VLAN .	
3. Manually enable the trunk link on a trunking port by using the switchport mode trunk command.	
4. Disable DTP (auto trunking) negotiations on trunking ports by using the switchport nonegotiate command.	
5. Set the native VLAN to a VLAN other than VLAN 1 by using the switchport trunk native vlan <i>vlan_number</i> command.	

Mitigate DHCP Attacks

- DHCP starvation attack uses attack tools such as Gobbler to create Denial of Service (DoS) for connecting clients.
- DHCP spoofing attacks can be mitigated by using DHCP snooping on trusted ports.

DHCP Snooping

Description	<ul style="list-style-type: none">• Filters DHCP messages and rate-limits DHCP traffic on untrusted ports• Devices under administrative control (switches, routers and servers) are trusted sources• Trusted interfaces (trunk links, server ports) must be explicitly configured as trusted• Devices outside the network and all access ports are treated as untrusted sources.• DHCP snooping binding table (DHCP table) includes source MAC address of device on untrusted port and IP address assigned by the DHCP server to that device (MAC address and IP address are bound together)
Implementation	<ol style="list-style-type: none">1. Enable DHCP snooping by using the <i>ip dhcp snooping</i> global configuration command2. On trusted ports, use the <i>ip dhcp snooping trust</i> interface configuration command3. On untrusted interfaces, limit the number of DHCP discovery messages that can be received using the <i>ip dhcp snooping limit rate packets-per-second</i> interface configuration command.4. Enable DHCP snooping by VLAN, or by a range of VLANs, by using the <i>ip dhcp snooping vlan</i> global configuration command

Mitigate ARP Attacks

- Threat actor **sends unsolicited (uninvited) ARP replies** to other hosts on the subnet with the **MAC address of the threat actor and the IP address of the default gateway**.
- Switch must ensure that only **valid Requests and Replies** are relayed to prevent ARP spoofing and poisoning.
- **Dynamic ARP Inspection (DAI)** requires **DHCP snooping** and helps prevent ARP attacks by:
 - **Not relaying invalid or gratuitous ARP Replies** out to other ports in the same VLAN
 - **Intercepting** all ARP Requests and Replies on untrusted ports
 - Verifying each intercepted packet for a **valid IP-to-MAC binding**
 - **Dropping and logging** ARP Replies coming from invalid to prevent ARP poisoning
 - **Error-disabling the interface** if the configured DAI number of ARP packets is exceeded

DAI Implementation

Enable DHCP snooping globally	<i>ip dhcp snooping</i>
Enable DHCP snooping on selected VLANs	<i>ip dhcp snooping vlan [vlan]</i>
Enable DAI on selected VLANs	<i>ip arp inspection vlan [vlan]</i>
Configure trusted interfaces for DHCP snooping and ARP inspection	<i>interface [interface]</i> <i>ip dhcp snooping trust</i> <i>ip arp inspection trust</i>
Configure checking criterias • Destination MAC • Source MAC • IP address	Destination MAC <i>ip arp inspection validate dst-mac</i> Source MAC <i>ip arp inspection validate src-mac</i> IP address <i>ip arp inspection validate ip</i> All <i>ip arp inspection validate src-mac dst-mac ip</i>

Mitigate STP Attacks

- Network attackers can manipulate Spanning Tree Protocol (STP) to conduct attack by spoofing the root bridge and changing the topology of a network
- STP attacks can be mitigated by using PortFast and Bridge Protocol Data Unit (BPDU) Guard

PortFast	<ul style="list-style-type: none"> Immediately brings a port to the forwarding state from a blocking state, bypassing the listening and learning states Apply to all end-user access ports Minimize the time that access ports must wait for STP to converge <p><u>Implementation</u></p> <p>Single interface</p> <p><i>interface [interface]</i> <i>switchport mode access</i> <i>spanning-tree portfast</i></p> <p>Global</p> <p><i>spanning-tree portfast default</i></p>
BPDU Guard	<ul style="list-style-type: none"> Immediately error disables a port that receives a BPDU Like PortFast, BPDU guard should only be configured on interfaces

attached to end devices.

Implementation

Single interface

*interface [interface]
spanning-tree bpduguard enable*

Global

spanning-tree portfast bpduguard default

C10: WLAN Concepts

* AP Categories

Autonomous APs	<ul style="list-style-type: none">• Standalone device configured through a command line interface or GUI• Acts independently of others and configured or managed manually by administrator
Controller-Based APs	<ul style="list-style-type: none">• A.k.a. Lightweight APs (LAPs)• Uses Lightweight Access Point Protocol (LAPP) to communicate with WLAN controller (WLC)• Automatically configured or managed by WLC

* CSMA/CA

- WLANs are **half-duplex** and a client cannot "hear" while it is sending, making it impossible to detect a collision
- WLANs use **carrier sense multiple access with collision avoidance (CSMA/CA)** to determine how and when to send data.
- Wireless client does the following:
 1. **Listens** to the channel to see if it is **idle**, i.e. no other traffic currently on the channel.
 2. **Sends a ready to send (RTS) message** to the AP to request **dedicated access** to the network.
 3. **Receives a clear to send (CTS) message** from the AP granting access to send.
 4. **Waits a random amount of time** before restarting the process if **no CTS message** is received.
 5. **Transmit** the data.
 6. **Acknowledges** all transmissions. If a wireless client does not receive an acknowledgment, it assumes a collision occurred and restarts the process.

WLAN Threats

DoS Attacks

Causes

- Improperly configured devices
- A malicious user intentionally interfering with the wireless communication
- Accidental interference

Risk prevention

- Harden all devices

- Keep passwords secure
- Create backups
- Ensure that all configuration changes are incorporated off-hours

* Rogue Access Points

Description	<ul style="list-style-type: none"> • An AP or wireless router that has been connected to a corporate network without explicit authorization and against corporate policy. • Once connected, attacker uses it to: <ul style="list-style-type: none"> ◦ Capture MAC addresses ◦ Capture data packets ◦ Gain access to network resources ◦ Launch man-in-the-middle attack
Prevention	<ul style="list-style-type: none"> • Configure WLCs with rogue AP policies • Use monitoring software to actively monitor the radio spectrum for unauthorized APs

Man-in-the-Middle Attack

- Hacker is positioned in between two legitimate entities in order to read or modify the data passed between the two parties.
- Popular wireless MITM attack: "evil twin AP" attack (Attacker introduces a rogue AP and configures it with the same SSID as a legitimate AP).
- Solution:
 - Identifying legitimate devices on the WLAN
 - Authenticate users
 - Monitor network for abnormal devices or traffic

Secure WLANs

SSID Cloaking	<ul style="list-style-type: none"> • APs and some wireless routers allow the SSID beacon frame to be disabled. • Wireless clients must be manually configured with the SSID to connect to the network.
MAC Address Filtering	<ul style="list-style-type: none"> • Administrators manually permit or deny client wireless access based on their physical MAC hardware address.

802.11 Original Authentication Methods

Open System Authentication	<ul style="list-style-type: none"> • No password required • Used to provide free internet access in public areas like cafes, airports and hotels • Client is responsible for providing security such as through a VPN
----------------------------	---

Shared key authentication	<ul style="list-style-type: none"> provides mechanisms such as WEP, WPA, WPA2 and WPA3 to authenticate and encrypt data between a wireless client and AP Password must be pre-shared between both parties to connect
---------------------------	--

Shared Key Authentication Methods

Authentication Method	Description
Wires Equivalent Privacy	<ul style="list-style-type: none"> Original 802.11 specification designed to secure data using Rivest Cipher 4 (RC4) encryption method with a static key WEP is no longer recommended and should never be used
Wi-Fi Protected Access	<ul style="list-style-type: none"> A Wi-Fi Alliance standard that uses WEP but secures the data with much stronger Temporal Key Integrity Protocol (TKIP) encryption algorithm TKIP changes the key for each packet, making it much more difficult to hack
WPA2	<ul style="list-style-type: none"> Uses Advanced Encryption Standard (AES) for encryption AES is currently the strongest encryption protocol
WPA3	<ul style="list-style-type: none"> Next generation of Wi-Fi security All WPA3-enabled devices use the latest security methods Disallow outdated legacy protocols, and require the use of Protected Management Frames (PMF)

* Authenticating a Home User (WPA2 Authentication)

Personal	<ul style="list-style-type: none"> Intended for home or small office networks, users authenticate using a pre-shared key (PSK) Wireless clients authenticate with wireless router using pre-shared password No special authentication server is required
Enterprise	<ul style="list-style-type: none"> Intended for enterprise networks Requires a Remote Authentication Dial-In User Service (RADIUS) authentication server Devices must be authenticated by the RADIUS server and then users must authenticate using 802.1X standard, which uses the Extensible Authentication Protocol (EAP) for authentication.

Encryption Methods

Temporal Key Integrity Protocol (TKIP)	<ul style="list-style-type: none">Used by WPA and provides support for legacy WLAN equipmentMake use of WEP but encrypts the Layer 2 payload using TKIP
Advanced Encryption Standard (AES)	<ul style="list-style-type: none">Used by WPA2 and uses the Counter Cipher Mode with Block Chaining Message Authentication Code Protocol (CCMP)Allows destination hosts to recognize if the encrypted and non-encrypted bits have been altered.

Authentication in the Enterprise

RADIUS server IP address	IP address of the server
UDP port numbers	UDP ports 1812 for RADIUS Authentication, and 1813 for RADIUS Accounting, but can also operate using UDP ports 1645 and 1646
Shared key	Used to authenticate the AP with the RADIUS server

WPA 3

WPA3 - Personal	Thwarts brute force attacks by using Simultaneous Authentication of Equals (SAE)
WPA3 - Enterprise	Uses 802.1X/EAP authentication but it requires the use of 192-bit cryptographic suite and eliminates the mixing of security protocols for previous 802.11 standards
Open Network	Does not use any authentication but uses Opportunistic Wireless Encryption (OWE) to encrypt all wireless traffic
IoT Onboarding	Uses Device Provisioning Protocol (DPP) to quickly onboard IoT devices