

Switch Operations

Layer 2 and Layer 3 Forwarding Principles

Hubs - A basic networking device that connects multiple devices in a network segment, broadcasting incoming packets to all ports.

- Hubs flood packets out all ports, except the port it came in on.
- Works at Layer 1
- **Half Duplex Operation** - Data transmission can only occur in one direction at a time.
 - **Collision Domain** - A network segment where only one device can successfully send data at a time; collisions may occur if multiple devices transmit simultaneously.
 - **CSMA/CD (Carrier Sense Multiple Access with Collision Detection)** - Protocol used to detect collisions on a half-duplex network and retransmit data after a random backoff period.

Switches - L2/L3

- Can work bidirectionally
- Both ends must be full-duplex
- Collisions will not occur
- No CSMA/CD required

Switching Forwarding Behavior

- **Forward** - Sends the frame out the specific port where the destination MAC address resides.
- **Flood** - Sends the frame out all ports except the incoming port when the destination MAC address is unknown.

- **Filter** - Does not forward the frame because the destination MAC address is on the same port as the source.
 - How does a switch determine which action to perform:
 - Type of Destination MAC (Unicast, Broadcast, Multicast)
 - If it knows where the MAC address lives:
 - Present in the MAC address table → Forward/Filter
 - Not in the MAC address table → Flood

Populating the MAC Address Table

- If the switch doesn't have the Source MAC address in its MAC Address Table, it will learn it.
 - Addresses remain in the table by default for 5 minutes (300 seconds).
 - Timer resets to 5 minutes every time the switch hears the device speak.
 - MAC addresses can be lost if the interface status is not UP/UP.
 - You can clear the MAC address table using the command:
 - `clear mac address-table dynamic`

Frame Forwarding

- **Known Unicast Frame** (meaning the MAC address table already knows the destination MAC) = **FORWARD**
- **Broadcast Frame** (DST MAC = FF:FF:FF:FF:FF:FF) = **FLOOD**
 - Switch floods the frame out all ports except the incoming port.
 - Flooding occurs when:
 - DST MAC is unknown to the switch.
 - The switch receives a broadcast packet from a node.
- Switches do **not** share MAC addresses with each other, unlike routers that share routing information.
- When the same MAC address appears on two different ports within the same broadcast domain, subnet, or VLAN, the most recent port wins.

Router Operations

Routers route between subnets, VLANs, and broadcast domains.

- Routers prefer the **longest subnet mask** when choosing routes.
 - Codes for route sources:
 - **C (Connected)** - Directly connected interface. Interface must be UP/UP with an IP address set.
 - **L (Local)** - Always /32, representing the IP of the interface itself.
 - **S (Static)** - Manually configured route. Typically a 0.0.0.0 route to a gateway for outbound internet traffic.
 - **Dynamic Routing Protocols** - Automatically share routes between routers (details discussed later in the course).

Determining What to Put in Routing Tables

Routers install the best route from the best source:

1. Identify the best source

- a. **Administrative Distance (AD)** - A value that rates the trustworthiness of a route source; lower AD is more preferred. Remember these below.

Source	Administrative Distance
Connected	0
Static	1
eBGP	20
EIGRP	90
OSPF	110
IS-IS	115
RIP	120
External EIGRP	170
iBGP	200

2. Identify the best route from the best source

- a. **Metric** - A value used by the routing protocol to determine the best path; lower metrics are preferred. Metric is only used when there is a tie.

Source	Metric
Connected	0 because it is directly connected
Static	0 because the metric is not known
RIP	Hop Count – Max 15 hops (16 unreachable)
EIGRP	Lowest Bandwidth + Cumulative Delay of path
OSPF	Cost = sum of all the costs along the path
BGP	Attributes used to influence routing policy

3. Install the resulting route in the routing table.

- a. If two paths have the same AD and Metric. A router will load balance traffic across both paths, placing all eligible routes into the routing table for equal utilization.

Exam Note: Administrative Distance

- You can manually set the Administrative Distance (AD), but it is not required for this exam.
- Once the routing table is created, AD and metrics are automatically considered; you do not need to manually use them to determine which route to use.

Determining Routing Table Entries

- Routers use the **longest prefix match** rule to select the appropriate route:
 - Find all network entries that include the destination IP address.
 - Choose the entry with the most specific subnet mask (closest to /32) if multiple matches exist.

Frame and Packet Forwarding

- When receiving a DNS response and the destination IP is outside your subnet/broadcast domain, you must ARP for your **Default Gateway** to obtain its MAC address.
 - The '1' bits in the subnet mask identify the Network ID.
 - If the network addresses do not match:
 - ARP for the default gateway.
 - Set the destination MAC address to the default gateway (Layer 2).
 - The default gateway routes the packet based on the destination IP address (Layer 3).
- For routing inside your network, routers must rebuild the source and destination MAC addresses for router-to-router delivery.
 - /30 is a valid subnet.
 - ARP is used to obtain the MAC address unless it is already in the ARP cache.
- If a router does not have a directly connected interface for the longest prefix match, examine other routes to determine the correct exit interface.
- The **edge router** is responsible for NAT/PAT:
 - Keeps track of the local IP address.
 - Changes the source IP address to the public-facing IP through NAT or PAT.
 - PAT uses port numbers to allow multiple local hosts to share a single public IP.
- Routing rules:
 - If the route is **directly connected**, ARP for the IP address of the packet.
 - If the route is **not directly connected**, ARP for the MAC address of the next-hop IP address.

Introducing the Cisco IOS

Cisco IOS Software (IOS-XE/IOS)

- Many Cisco products use Cisco IOS Software:
 - **IOS** - Internetwork Operating System
 - **CLI** - Command Line Interface using word commands that vary based on mode.
 - Runs on Cisco Catalyst Switches and Cisco Routers.
- Cisco products that **do not** use Cisco IOS Software:
 - Cisco ASA
 - Cisco Nexus product family

How to Connect to a Cisco Device

- CLI access using a terminal emulator such as **PuTTY**
- Console Cable:
 - Serial line to connect to: COM1
 - Speed (baud): 9600
 - Data bits: 8
 - Stop bits: 1
 - Parity: None
 - Flow Control: XON/XOFF
 - Uses a **rollover cable**

CLI Mode Introduction

Prompt / Command	Mode	Description
Router>	User EXEC Mode	Guest access
Router#	Privileged EXEC Mode	Privileged access
Router(config)#	Global Configuration Mode	Configure platform-wide parameters
Router(config-if)#	Interface Configuration Mode	Configure interface-specific parameters

Cisco CLI Help

```
Router(config-if)#ip?  
(find all commands in this mode beginning with "ip")
```

```
Router(config-if)#ip ?  
(find the parameters that follow of the ip command)
```

```
Router(config-if)#ip add?  
(find all parameters of the ip command with "add" as  
the first three letters)
```

```
Router(config-if)#ip address ?  
(find the parameter that follows address)
```

```
Router(config-if)#ip address 10.1.1.1 ?  
(find the parameter that follows the IP address)
```

```
Router(config-if)#ip address 10.1.1.1 255.255.255.0 ?  
(find the options following the subnet mask)
```

Cisco CLI Error Messages

```
Router#cl <press enter>  
% Ambiguous command: 'cl'
```

```
Router#clock set <press enter>  
% Incomplete command
```

```
Router#clock seg 15:01:00 13 Jan 2021 <press enter>  
^  
% Invalid input detected at '^' marker.
```

```
Router#clock set 15:01:00 13 Month 2021 <press enter>  
^  
% Invalid input detected at '^' marker.
```

Cisco CLI Shortcuts

CLI Shortcut	Description
Tab	Completes the rest of the command
Ctrl-A	Moved cursor to the beginning of the line
Ctrl-E	Moves cursor to the end of the line
Ctrl-Z	Returns to the user EXEC prompt
Ctrl-Shift-6	Allows admin to abort a IOS process – ex: ping
Ctrl-C	Abort current command and exits configuration mode

Router and Switch History

This command will modify the history size from 10 to 50 lines.

```
Switch#terminal history size 50
```

This command will display the contents of the command buffer.

```
Switch#show history
enable
terminal history size 50
show history
```

Use the terminal length command to set the number of lines presented in the terminal.

```
Switch#terminal length 100
```

IOS Configuration Management

Inside the Switch

- **CPU** - Executes commands
- **Boot ROM** - Boot scripts (e.g., POST)
 - **ROMMON** - Used for password recovery or when the OS is corrupted
- **SDRAM** - Loads the configuration file and IOS
- **NVRAM** - Stores the startup configuration file
- **Flash** - Stores IOS image(s) and system files

Displaying IOS Configuration

- To verify the current running configuration (RAM):

```
R1# show running-config
```

- Note 1: R1# is just a sample prompt; it is not needed in the actual command.
- Note 2: Commands only need enough characters to be considered unique. For example:

```
sh ru
```

- Equivalent to:

```
show running-config
```

- To verify the contents of the startup configuration (NVRAM):

```
R1# show startup-config
```

Saving Configuration Changes

```
R1# copy running-config startup-config
```

Backup and Restore

- **Copy Commands:**

```
copy startup-config tftp    # Backup startup to TFTP
copy tftp startup-config   # Restore from TFTP to startup
```

- TFTP uses UDP port 69 and is **unencrypted**
- FTP uses TCP ports 20/21 and can use authentication

Interface States

Interface Status	Line Protocol Status	Description
Up	Up	Operational
Up	Down	L2 problem such as an encapsulation mismatch
Down	Down	L1 problem such as cable unplugged; other end of the link disconnected or admin down; speed mismatch; port is err-disabled.
Administratively down	Down	Shutdown command issued on interface

- **Duplex and Speed** are common port issues.
- **Speed-related issues** occur when there are mismatched speed settings.
 - **Result:** No connectivity (e.g., 100 Mbps and 1000 Mbps mismatch)
- **Duplex-related issues** occur when there are mismatched duplex settings.
 - **Result:** Very slow connectivity (e.g., full duplex vs half duplex)
 - Auto ↔ Auto → Works
 - Auto ↔ Half → Works
 - Auto ↔ Full → Does **not** work