Chapter 1: Routing Concepts
ROUTER FUNCTIONS
Router Functions

Characteristics of a Network

- **Topology**
  - Physical topology – arrangement of the cables, network devices, and end systems; it describes how the network devices are actually interconnected with wires and cables.
  - Logical topology – describes the path over which the data is transferred in a network and how the network devices appear connected to network users.

- **Speed** – measure of the data rate in bits per second (b/s) of a given link in the network.
Characteristics of a Network

- **Cost** – purchasing of network components, as well as installation and maintenance of the network
- **Security** – how well the network is protected
- **Availability** – likelihood that the network is available for use when it is required
- **Scalability** – how easily the network can accommodate more users and data transmission requirements as they increase
- **Reliability** – dependability of the components that make up the network
A Router does the following:

- Connects one network to another network
- Determines the best route to the destination before forwarding traffic to the next router along the path
- Routes traffic between network
- Uses the routing table to determine the most efficient path to reach the destination
A router is a specialized computer that requires the same components to operate as computers including:

- Central Processing Unit (CPU)
- Operating System (OS)
  - A desktop computer might use the Windows Operating System, but a Cisco Router uses the Cisco Internetwork Operating System (IOS).
- Memory and storage (RAM, ROM, NVRAM, Flash, hard drive)
  - Non-volatile vs. volatile memory
  - Which one requires constant power to retain content?

Routers have specialized ports and network interface cards to interconnect devices to other networks.
# Router Functions

<table>
<thead>
<tr>
<th>Memory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Random Access Memory (RAM)</td>
<td>Volatile memory that provides temporary storage for various applications</td>
</tr>
<tr>
<td></td>
<td>and processes including:</td>
</tr>
<tr>
<td></td>
<td>• Running IOS</td>
</tr>
<tr>
<td></td>
<td>• Running configuration file</td>
</tr>
<tr>
<td></td>
<td>• IP routing and ARP tables</td>
</tr>
<tr>
<td></td>
<td>• Packet buffer</td>
</tr>
<tr>
<td>Read-Only Memory (ROM)</td>
<td>Non-volatile memory that provides permanent storage for:</td>
</tr>
<tr>
<td></td>
<td>• Bootup instructions</td>
</tr>
<tr>
<td></td>
<td>• Basic diagnostic software</td>
</tr>
<tr>
<td></td>
<td>• Limited IOS in case the router cannot load the full featured IOS</td>
</tr>
<tr>
<td>Non-Volatile Random Access Memory (NVRAM)</td>
<td>Non-volatile memory that provides permanent storage for the:</td>
</tr>
<tr>
<td></td>
<td>• Startup configuration file</td>
</tr>
<tr>
<td>Flash</td>
<td>Non-volatile memory that provides permanent storage for:</td>
</tr>
<tr>
<td></td>
<td>• IOS</td>
</tr>
<tr>
<td></td>
<td>• Other system-related files</td>
</tr>
</tbody>
</table>
Router Functions

- A Router is responsible for forwarding packets from network to network, from the source to the destination.
- Multiple networks on a router require multiple interfaces that each belong to a different IP network.
  - These interfaces are used to connect:
    - **LANs** – Ethernet networks that contain PCs, printers, and servers.
    - **WANs** – used to connect networks over large geographical areas such as to an ISP.
- When a packet arrives on a router’s interface, the router might be the final destination, or it may have to send it to another router to reach its final destination.
The primary functions of a router are to:
- Determine the best path to send packets
- Forward packets toward their destination

When a router receives a packet, it
- examines the destination address of the packet
- and uses the routing table to look for the best path to that network.

- When a match is found, the router encapsulates the packet into the data link frame of the outgoing exit interface and then forwards the packet out that interface to its destination.

- Routers use the routing table like a map to discover the best path to a given network.
Router Functions

- A router can handle different data link layer frame encapsulations.
  - The router might receive a frame from its Ethernet interface.

  It will have to de-encapsulate the packet to search the routing table for a matching network.

  Once it finds a match, it will encapsulate it inside of the corresponding frame required for the outgoing interface, such as a PPP frame.
Router Functions

Fast Switching

Control Plane

CPU

Ingress Interface

Data Plane

Fast Forward Cache

Egress Interface

1st Packet
2nd Packet
3rd Packet
4th Packet
5th Packet
Router Functions

1. Process switching –
   - Slower and older packet forwarding mechanism
   - Packet arrives on an interface, it is forwarded to the control plane where the CPU matches the destination address with an entry in its routing table in order to determine the exit interface
   - Slow because it does this for every packet in a stream

2. Fast Switching –
   - Common packet forwarding mechanism which uses a fast-switching cache to store the next-hop information
   - Packet arrives on an interface, it is forwarded to the control plane where the CPU searches for a match in the fast-switching cache
   - If no match, it is process-switched and forwarded to the exit interface
   - Packet flow information stored in the fast-switching cache for quick lookup

3. Cisco Express Forwarding – CEF
   - Fastest, most recent, and preferred packet-forwarding mechanism
   - CEF builds a Forwarding Information Base (FIB) and an adjacency table
   - Table entries are not packet-triggered like fast switching, but change-triggered when something changes in the network topology
   - When a network has converged, the FIB and adjacency tables contain all the information a router would have to consider when forwarding a packet
   - FIB contains pre-computed reverse lookups, next hop information for routes including the interface and Layer 2 information
Router Functions
Packet Tracer – Using Traceroute to Discover the Network
Router Functions

Route tracing computer software lists the networks that data traverses from the user's originating end device to a distant destination device.

This network tool is typically executed at the command line as:

```
tracert <destination network name or end device address>
(Microsoft Windows systems)
```

or

```
traceroute <destination network name or end device address>
(UNIX, Linux systems, and Cisco devices, such as switches and routers)
```

Both `tracert` and `traceroute` determine the route taken by packets across an IP network.

The `tracert` (or `traceroute`) tool is often used for network troubleshooting. By showing a list of routers traversed, the user can identify the path taken to reach a particular destination on the network or across internetworks. Each router represents a point where one network connects to another network and through which the data packet was forwarded. The number of routers is known as the number of hops the data traveled from source to destination.

The displayed list can help identify data flow problems when trying to access a service such as a website. It can also be useful when performing tasks, such as downloading data. If there are multiple websites (mirrors) available for the same data file, one can trace each mirror to get a good idea of which mirror would be the fastest to use.
CONNECTING NETWORK DEVICES
Home Office devices might connect as follows:

- Laptops and tablets connect wirelessly to a home router.
- A network printer connects using an Ethernet cable to the switch port on the home router.
- The home router connects to the Internet service provider cable modem using an Ethernet cable.
- The cable modem connects to the ISP network.
Branch site devices might connect as follows:

- Desktop PCs, VoIP phones, and corporate resources such as file servers and printers connect to Layer 2 switches using Ethernet cables.
- Laptops and smartphones connect wirelessly to wireless access points (WAPs).
- The WAPs connect to switches using Ethernet cables.
- Layer 2 switches connect to an Ethernet interface on the edge router using Ethernet cables.
- The edge router connects to a WAN service provider.
Central site devices might connect as follows:

- Desktop PCs and VoIP phones connect to Layer 2 switches using Ethernet cables.
- Layer 2 switches connect redundantly to multilayer Layer 3 switches using Ethernet fiber-optic cables.
- Layer 3 multilayer switches connect to an Ethernet interface on the edge router using Ethernet cables.
- The corporate website server connects to the edge router interface.
- The edge router connects to a WAN SP and also to an ISP for backup purposes.
Connecting Devices - Default Gateways

- Devices need the following information for network access: IP address, subnet mask, and default gateway.
- When a host sends a packet to a device that is on the same IP network, the packet is forwarded out the host interface to the destination device. The router does not need to get involved.
- When a host sends a packet to a device on a different IP network, the packet is forwarded to the default gateway because the host device cannot communicate with devices outside of the local network.
- The default gateway is the device that routes traffic from the local network to devices on remote networks, such as devices on the Internet.

- Routers are also usually configured with their own default gateway.
When designing a new network or mapping an existing one, the documentation should identify:

- Device names
- Interfaces used in the design
- IP addresses and subnet masks
- Default gateway addresses

The figure in the left shows two useful documents:

- Topology diagram – provides a visual reference that indicates the physical and logical Layer 3 addressing.
- An addressing table – captures device names, interfaces, IPv4 addresses, subnet masks, and default gateway addresses.
Connecting Devices - Enable IP on a Host

- A host can be assigned IP address information either:
  - **Statically** –
    - Manually configure the IP address, subnet mask, default gateway and probably the DNS server IP address.
    - Servers and printers commonly use static address assignment.
  - **Dynamically** –
    - IP address information is obtained from a Dynamic Host Configuration Protocol (DHCP) server.
    - DHCP server provides an IP address, subnet mask, default gateway and probably the DNS server information.
    - Most host devices use DHCP.
Host computers connect to a wired network using a RJ-45 Ethernet cable.

Most network interface cards have one or two LED indicators next to the interface.

- Green LED indicates a good connection.
- A blinking green indicates network activity.
- No light indicates a problem with either the network cable or the network itself.

Network infrastructure devices also use LEDs to provide a quick status view. For example, a Cisco Catalyst 2960 switch:

- Green LEDs indicate a switch is functioning normally.
- Amber LEDs indicate a malfunction.

Cisco routers also use various LED indicators to provide status information.
Connecting Devices - Console Access

- Devices including routers and switches are commonly accessed using Secure Shell (SSH) or HyperText Transfer Protocol Secure (HTTPS).

- Console access is usually only required when initially configuring a device, or if remote access fails.

- Console access requires:
  - Console cable – RJ-45 to DB-9 serial cable or a USB serial cable.
  - Terminal emulation software – Tera Term, PuTTY, or HyperTerminal

- Cable is connected between the serial port of the host and the console port on the device.
  - If a host does not have a serial port, use the USB port and a USB-to-RS-232 adapter.
Network devices require IP addresses in order for the network administrator to connect to the devices using Telnet, SSH, HTTP, or HTTPS.

A switch requires an IP address to be configured on a virtual interface, called the switched virtual interface (SVI).

Commands in the figure to the left should be used to configure the IP address on vlan 1 and also the default-gateway information.
ROUTER BASIC SETTINGS
Cisco routers and switches have similar initial configuration steps:

- Name the device in order to distinguish it from other devices in the network using the `hostname` command in global config mode.

- Secure management access as shown in the figure to the left in order to secure privileged EXEC, user EXEC, and remote access.

- Configure a banner to provide legal notification of unauthorized access in global config mode: `banner motd **Authorized Access Only! **`

- Always save your configuration changes and verify your settings: `R1# copy running-config startup-config`
Layer 2 switches support LANs and have multiple FastEthernet or Gigabit Ethernet ports.

Routers support LANs and WANs and have many types of interfaces including Gigabit Ethernet and High-Speed WAN Interface Card (HWIC) slots to support WAN connections.

As shown in the figure to the left, an interface must be configured with an IP address, subnet mask, and activated with the `no shutdown` command.

Note: In a lab environment, the serial interface with the cable end labeled DCE needs to be configured with a `clock rate` command.
To configure host PC1, statically assign an IPv6 address to the host under Internet Control Protocol Version 6 (TCP/IPv6) Properties.

Configuring an IPv6 interface is very similar to configuring an IPv4 interface, use the `ipv6 address` command.

As shown in the figure, configure the interface with an IPv6 address and subnet mask prefix.

Activate the interface with the `no shutdown` command.

An interface can generate its own IPv6 link-local address without having a global unicast address by using the `ipv6 enable` interface config command.

The `clock rate 128000` command was used since this is being configured in a lab environment.
Unlike IPv4, IPv6 interfaces will typically have more than one IPv6 address.

An IPv6 device must have an IPv6 link-local address but will most likely also have an IPv6 global unicast address.

An interface can also have multiple IPv6 global unicast addresses from the same subnet.

These commands can be used to create a global unicast or link-local IPv6 address:

- `ipv6 address ipv6-address/prefix-length`
- `ipv6 address ipv6-address/prefix-length eui-64`
- `ipv6 address ipv6-address/prefix-length link-local`
An IPv4 loopback interface is typically configured on a router for testing and management purposes.

- A loopback interface is a logical interface internal to the router.
  - It is not assigned to a physical port and can not be connected to any other device.
  - It is a software interface that is automatically placed in an “up” state as long as the router is functioning.

- Some routing protocols such as OSPF require an address for identification, the loopback address can be used rather than an interface address which might go down on occasion, disrupting OSPF routing.
VERIFYING CONNECTIVITY
Verifying Connectivity of Directly Connected Networks

Verify Interface Settings

- The following commands are used to verify the operation and configuration of an interface:
  - **show ip interface brief** – Displays a summary for all interfaces including the IPv4 address of the interface as well as the current operational status.
  - **show ip route** – Displays the contents of the IPv4 routing table.
  - **show running-config interface interface-id** – Displays the commands configured on the specified interface.

- The following commands can be used to gather more detailed interface information:
  - **show interfaces** – Displays interface information and packet flow counts.
  - **show ip interface** – Displays the IPv4 related information for all interfaces on a router.
Verifying Connectivity of Directly Connected Networks

Verify IPv6 Interface Settings

- IPv6 commands used for interface configuration verification are similar to IPv4.
  - `show ipv6 interface brief` – If the output shows up/up, this shows that Layers 1 and 2 are operational
  - `show ipv6 interface interface-id` – Shows the interface status and all of the IPv6 addresses that belong to the interface.
  - `show ipv6 route` – Verifies that IPv6 networks and specific IPv6 interface addresses have been installed in the IPv6 routing table.
  - As shown in the figure to the left, a ‘C’ next to a route indicates that this is a directly connected network.
  - When the router interface is configured with a global unicast address and is in the “up/up” state, the IPv6 prefix length is added to the IPv6 routing table as a connected route.
Verifying Connectivity of Directly Connected Networks

Filter Show Command Output

- Commands that generate multiple screens of output are, by default, paused after 24 lines.
  - The spacebar allows you to see the next set of lines, while the ENTER key will display the next line.
  - Use the terminal length command to change the number of lines to be displayed.

- Another useful feature that makes it easier to view show output is by filtering the output. To enable the filtering command, use the pipe character, “|”. For example:
  - `show running-config | section line con` – shows the section that starts with “line con”
  - `show ip interface brief | include down` – includes all output that matches “down”
  - `show ip interface brief | exclude up` – “excludes all output that matches up”
  - `show running-config | begin line` – shows all the remaining output starting with “line”
The command history feature shows previously executed commands when recalled.

Press Ctrl+P or the Up Arrow key to recall commands in the history buffer.

- The most recent commands are displayed first
- Keep pressing Up Arrow to recall the commands in the history buffer.

By default, command history is enabled and the last 10 commands are stored in the history buffer.

Use the `terminal history size` user EXEC command to change this number.

Use the `show history` privileged EXEC command to display the contents of the buffer.
END OF CHAPTER 1A