Advanced Networking

Faculty of Technology
University of Sri Jayewardenepura
2019

Course Contents

- Based on CCNA Routing & Switching Essentials
  - 1 Routing Concepts
  - 2 Static Routing
  - 3 Dynamic Routing
  - 4 Switched Networks
  - 5 Switch Configuration
  - 6 VLANs
  - 7 Access Control Lists
  - 8 DHCP
  - 9 NAT for IPv4
  - 10 Device Discovery, Management, and Maintenance
- Not1-to-1 mapped to CCNA content, but covering key aspects

Staff

- Lecturer
  - Dr. Nimal Skandhakumar
- Instructors
  - TBC

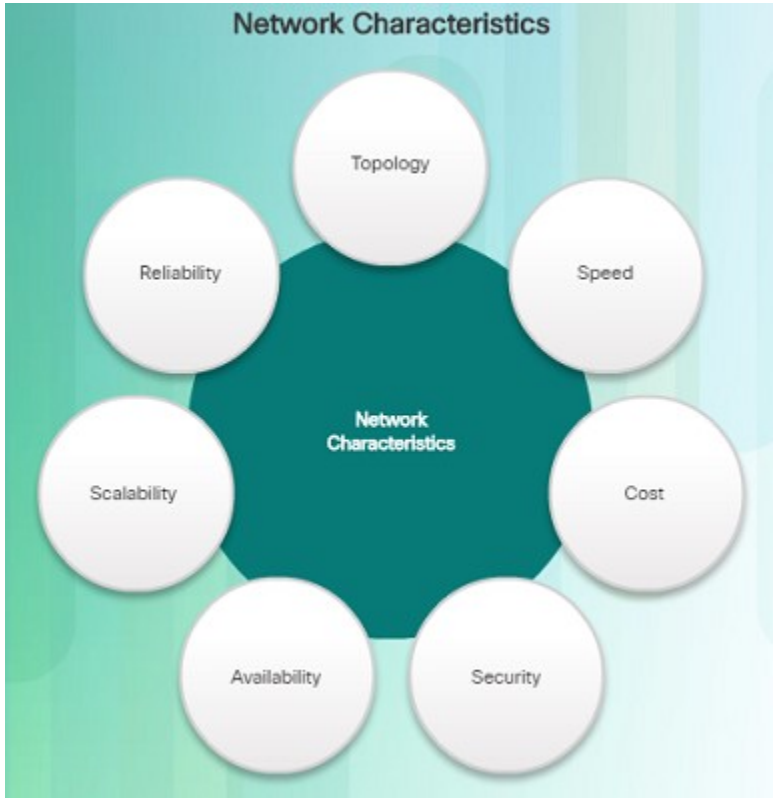
Resources

- Office Hours
  - Tuesday 1:00 PM - 2:00 PM
    - If alternative times are preferred, let me know.
- Lecture slides, etc.:
  - http://lms.tech.sjp.ac.lk/course/view.php?id=11
  - https://academic.nimal.info/

Routing Concepts

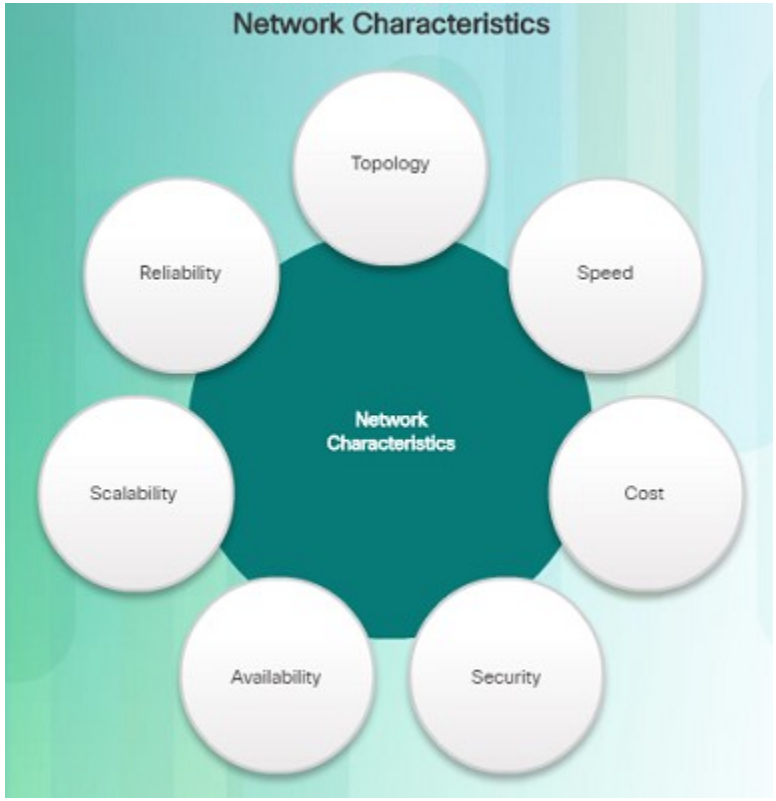
Characteristics of a Network

- Networks are relied on for web applications, IP telephony, video conferencing, interactive gaming, e-commerce, and much more.
- Characteristics referred to when discussing networks:
  - 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



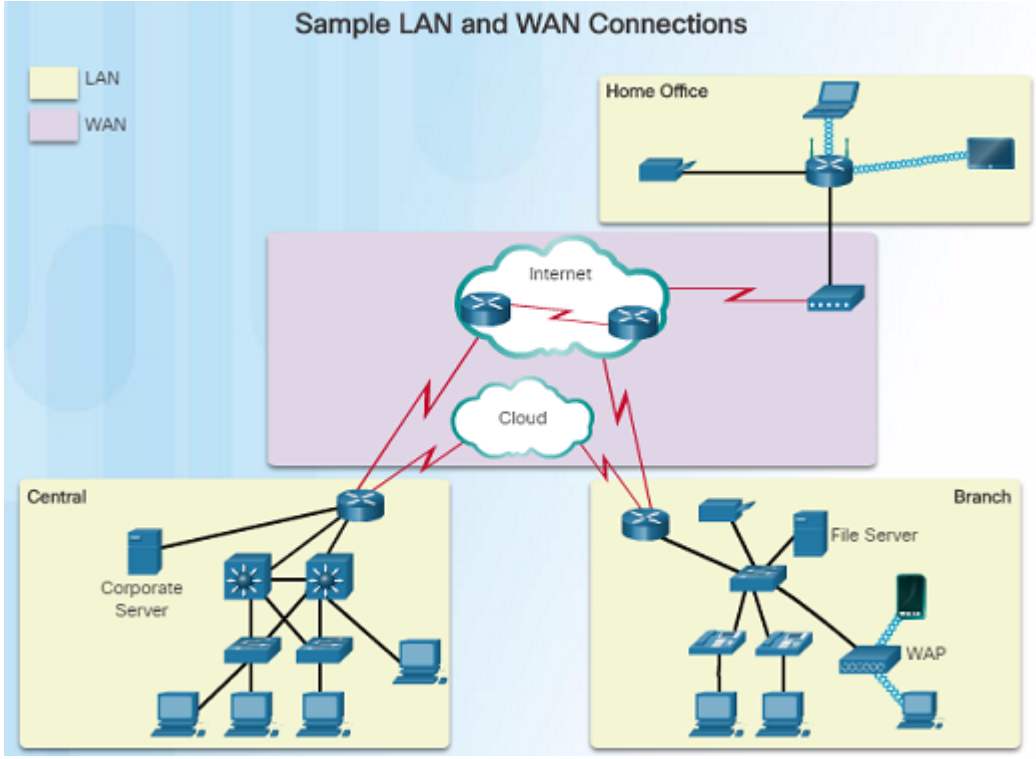
Characteristics of a Network (Cont.)

- Cost – general expense for purchasing of network components as well as installation and maintenance of the network
- Security – indicates how protected the network is, including the information that is transmitted over the network
- Availability – refers to the likelihood that the network is available for use when it is required
- Scalability – indicates how easily the network can accommodate more users and data transmission requirements as they increase
- Reliability – indicates the dependability of the components that make up the network including the routers, switches, PCs, and servers; often measured as MTBF (mean time between failures)



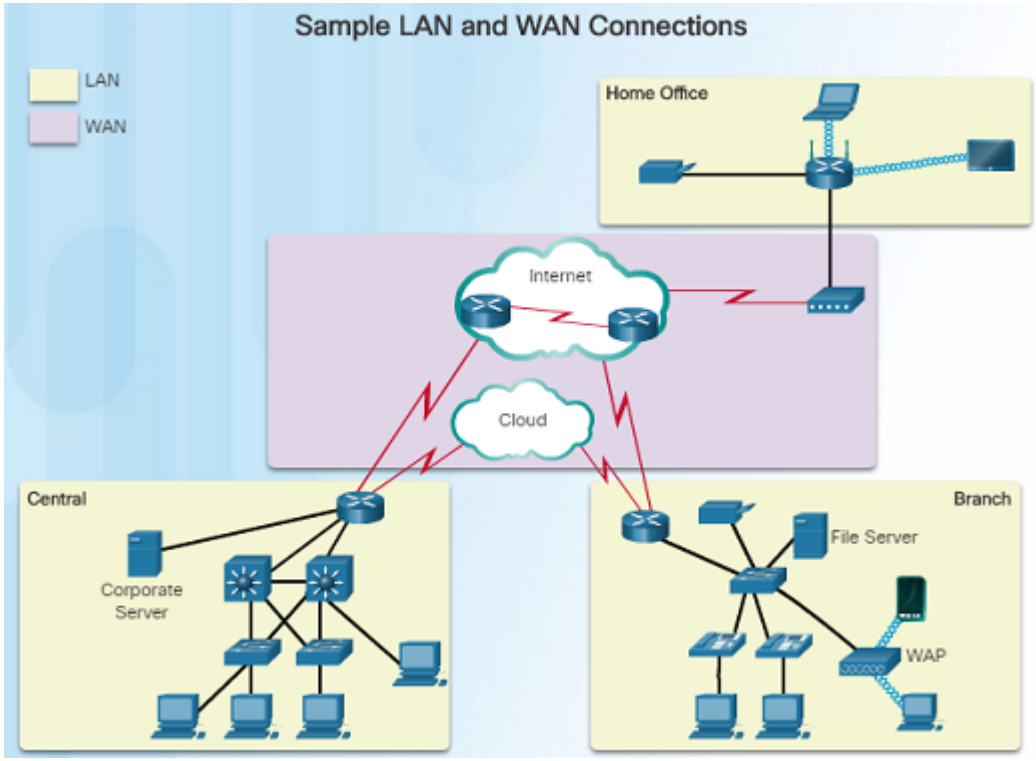
Connect to a Network

- 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.



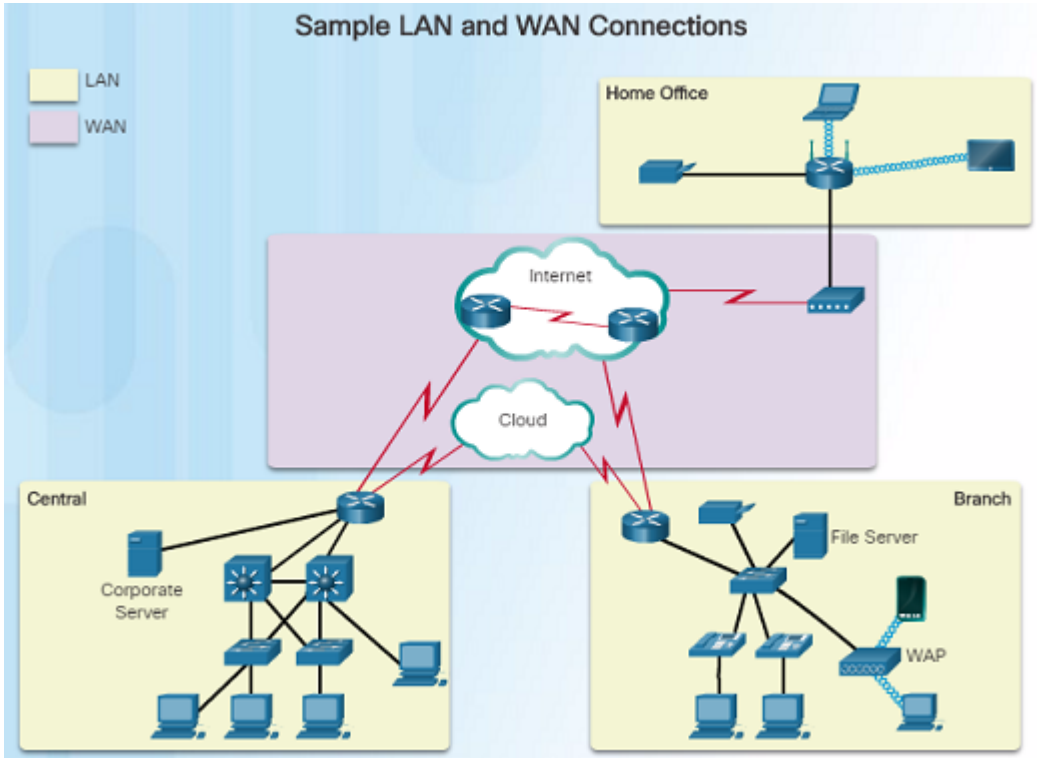
Connect to a Network (Cont.)

- 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.



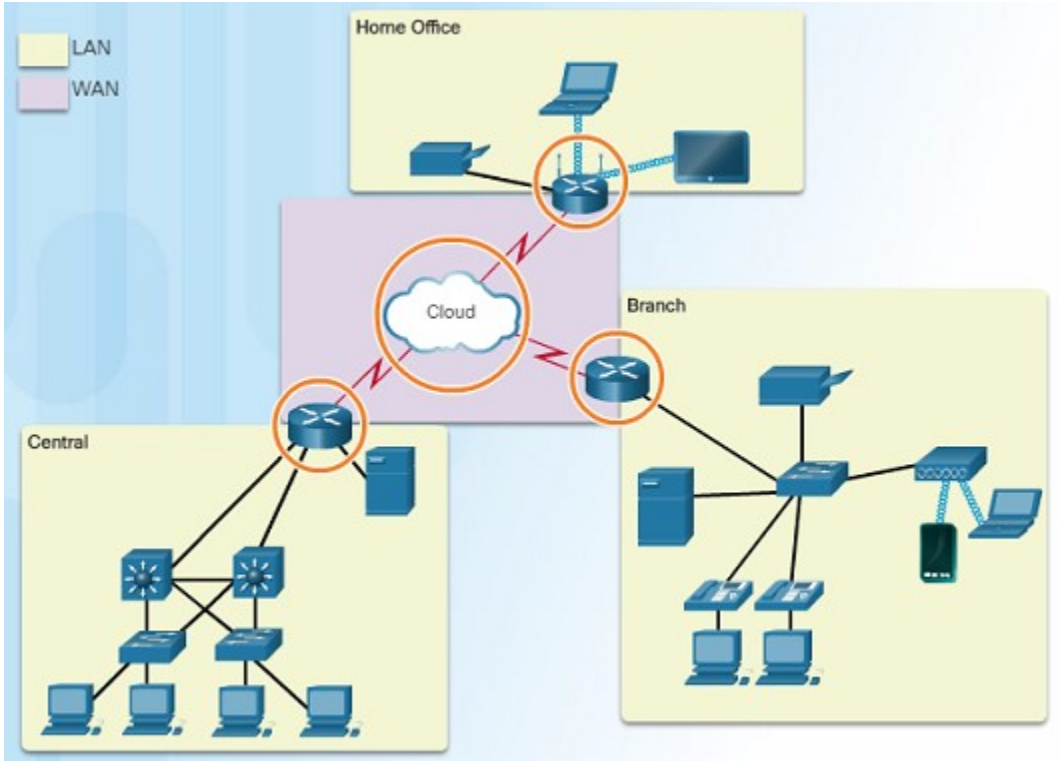
Connect to a Network (Cont.)

- 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.



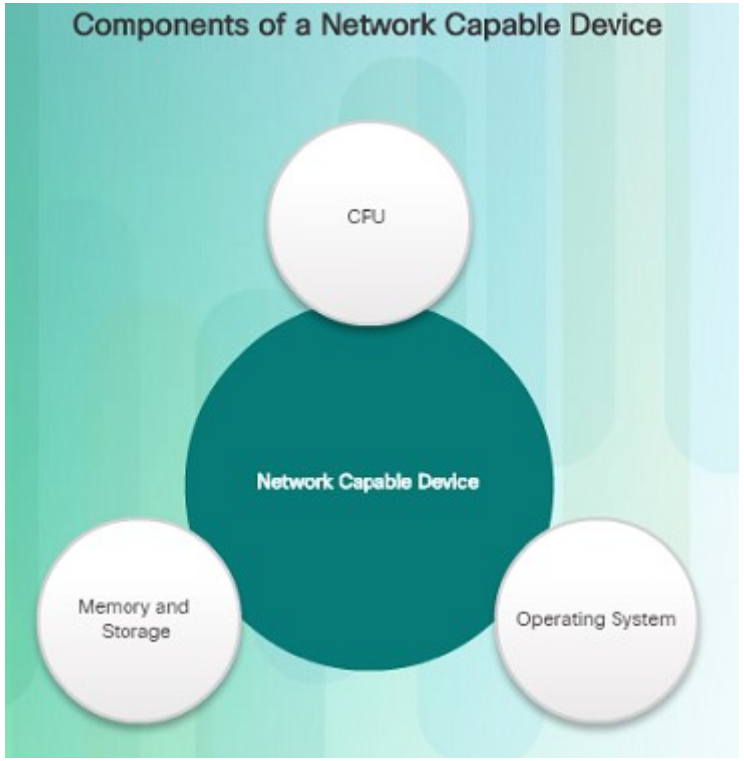
Why Routing?

- Router:
  - Connects one network to another network
  - Determines the best route to the destination before forwarding traffic to the next router along the path
  - Responsible for routing traffic between network
- Routing table used to determine the most efficient path to reach the destination



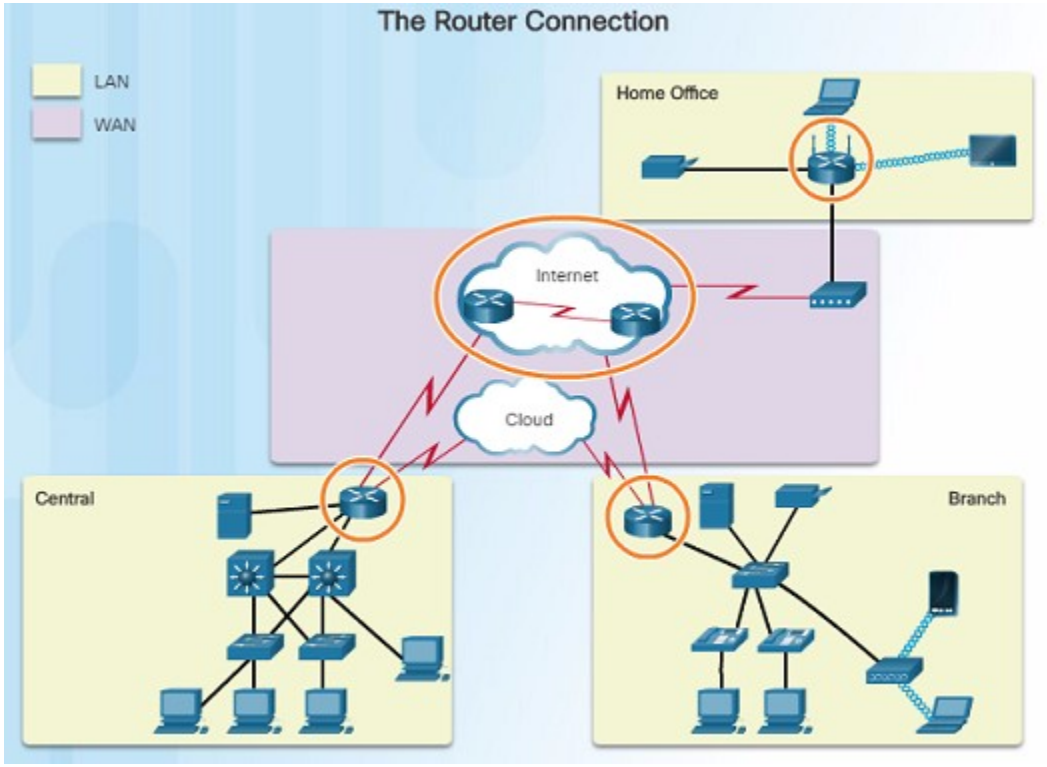
Routers are Computers

- A router is a specialized computer and 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



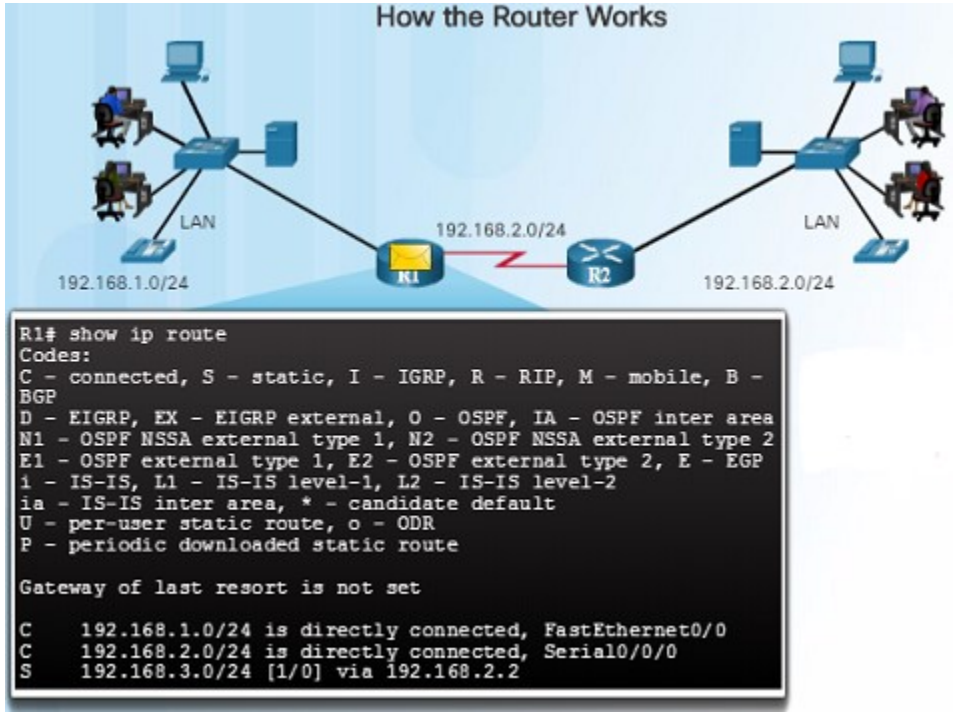
Routers Interconnect Networks

- 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.



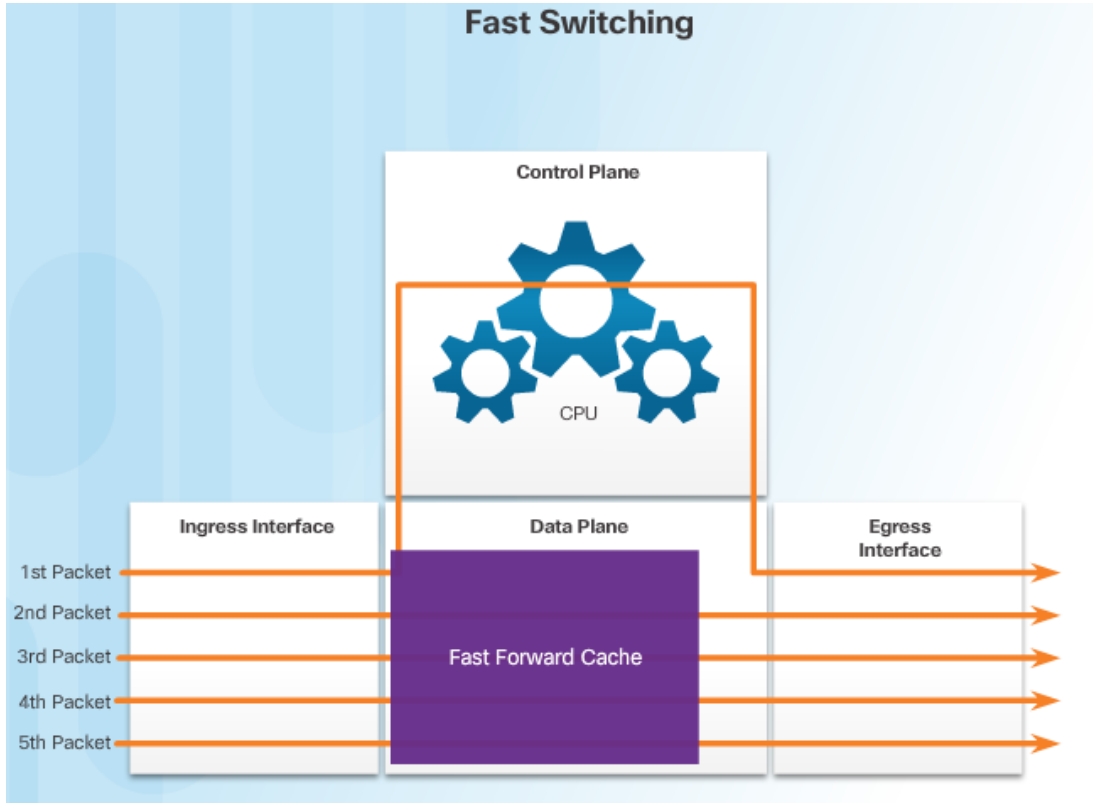
Routers Choose Best Paths

- 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.
- A router can handle different data link layer frame encapsulations.
- Routers use the routing table like a map to discover the best path to a given network.



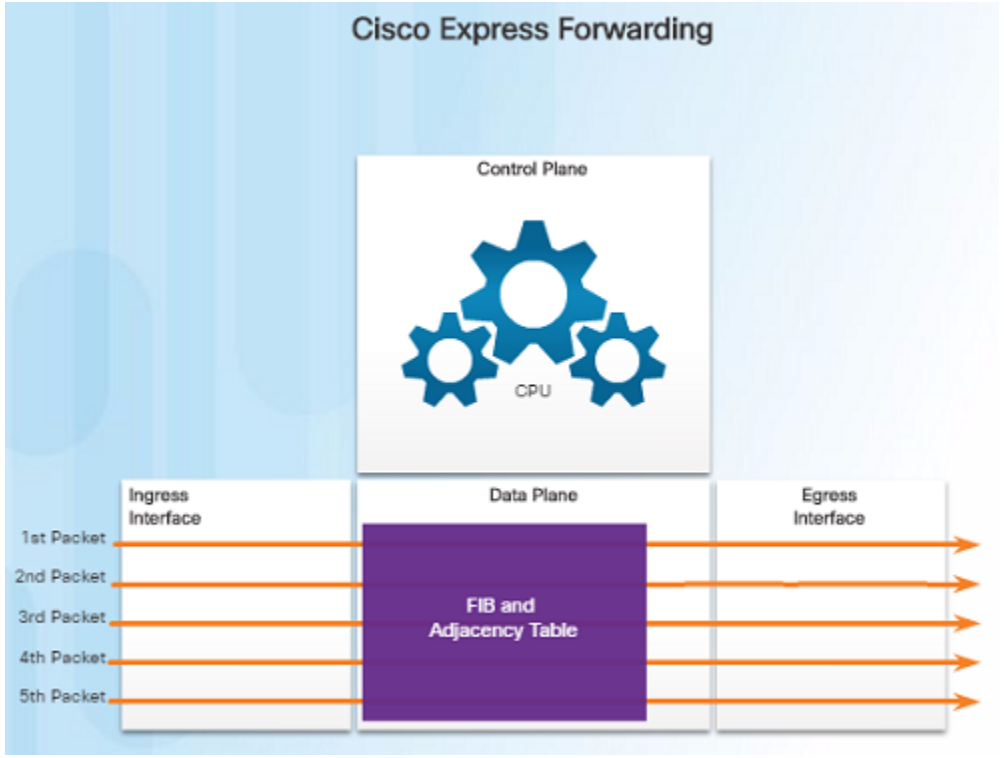
Packet Forwarding Mechanisms

- Routers support three packet-forwarding mechanisms:
  - 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
  - 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



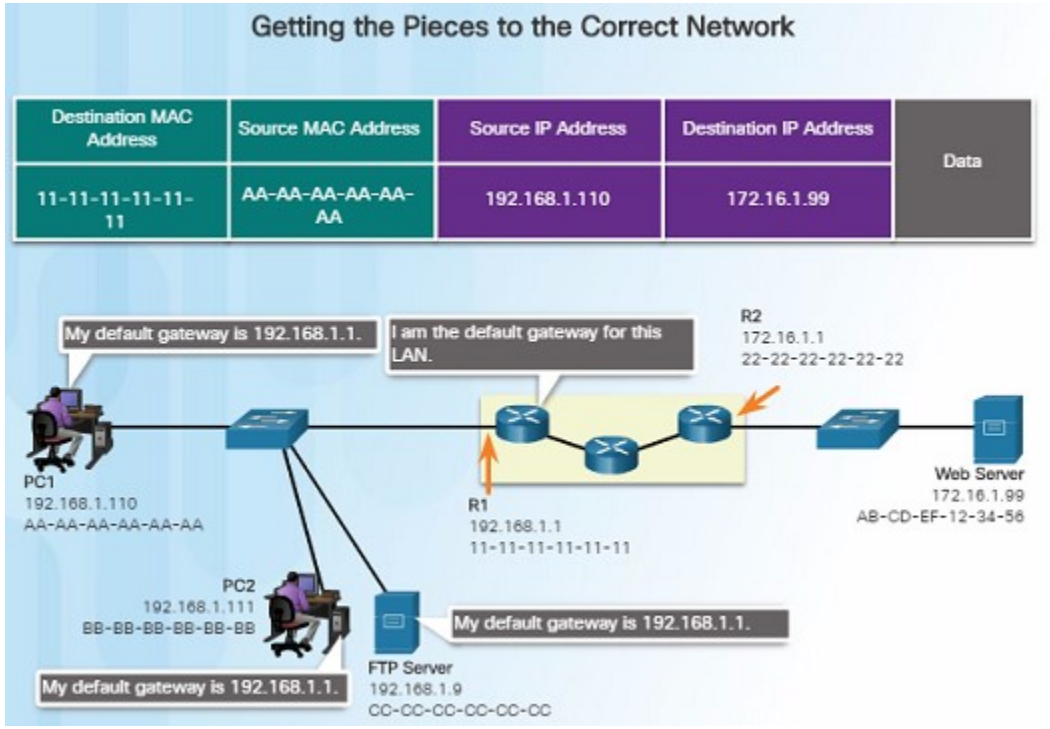
Packet Forwarding Mechanisms (Cont.)

- 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



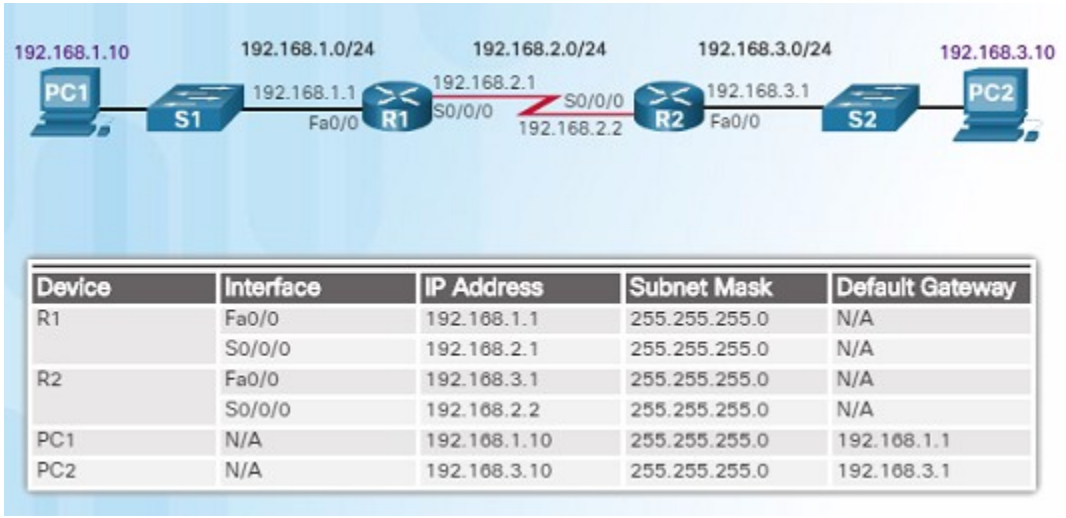
Default Gateways

- 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.



Document Network Addressing

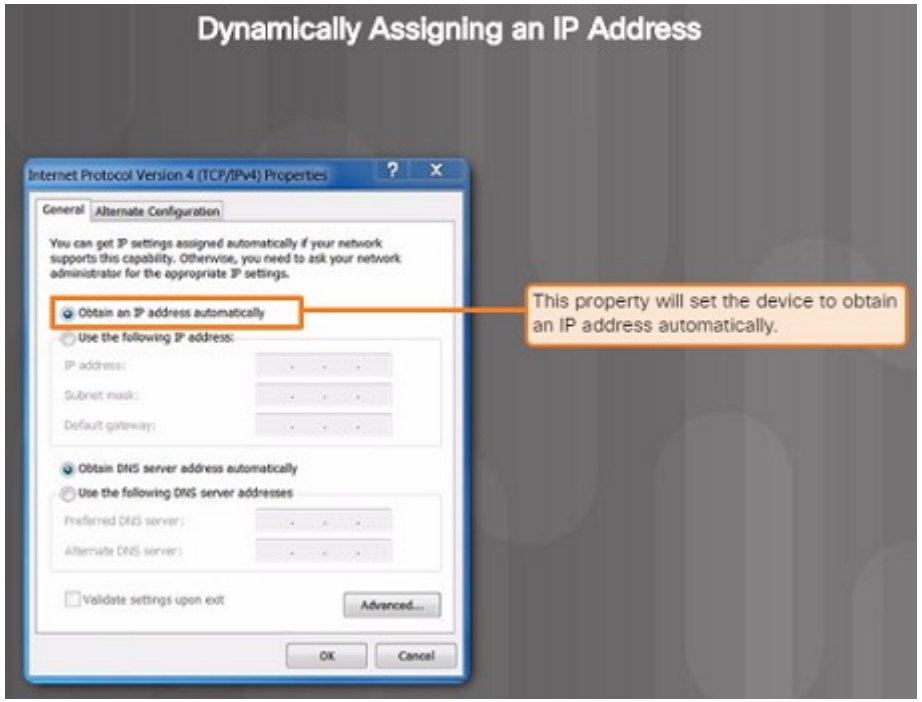
- When designing a new network or mapping an existing one, the documentation should identify:
  - Device names
  - Interfaces used in the design
  - IP addresses and subnet masks
  - Default gateway addresses
- The figure in the left shows two useful documents:
  - Topology diagram – provides a visual 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.



Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	192.168.1.1	255.255.255.0	N/A
	S0/0/0	192.168.2.1	255.255.255.0	N/A
R2	Fa0/0	192.168.3.1	255.255.255.0	N/A
	S0/0/0	192.168.2.2	255.255.255.0	N/A
PC1	N/A	192.168.1.10	255.255.255.0	192.168.1.1
PC2	N/A	192.168.3.10	255.255.255.0	192.168.3.1

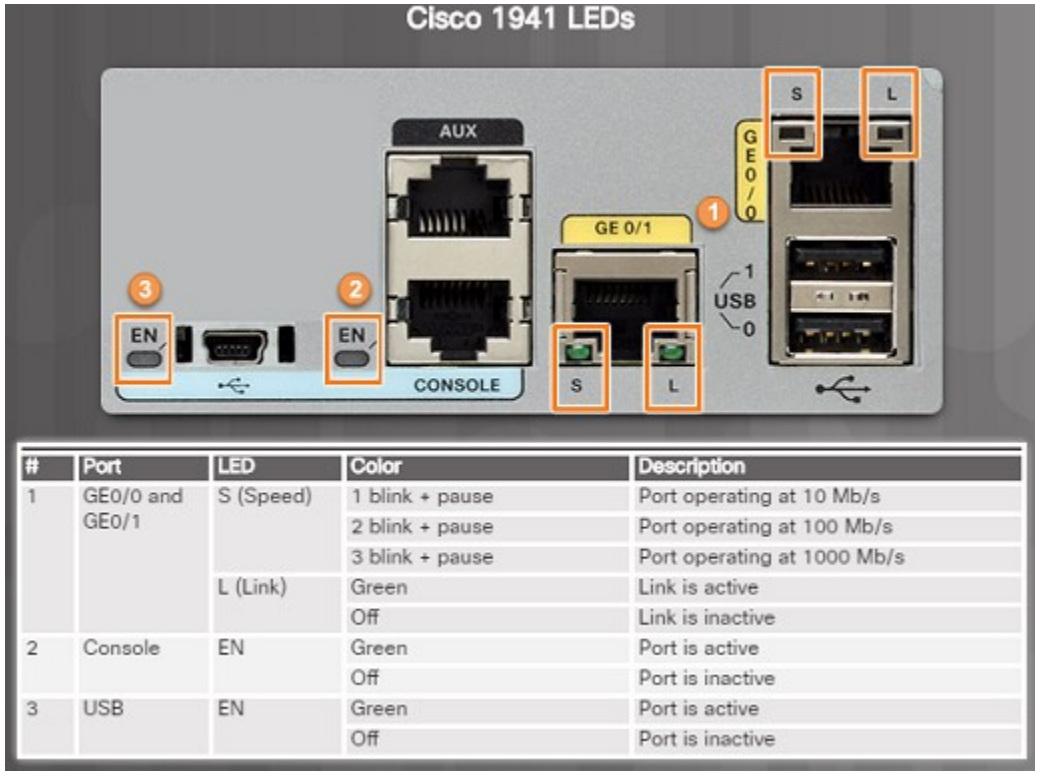
Enable IP on a Host

- 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 uses DHCP.



Device LEDs

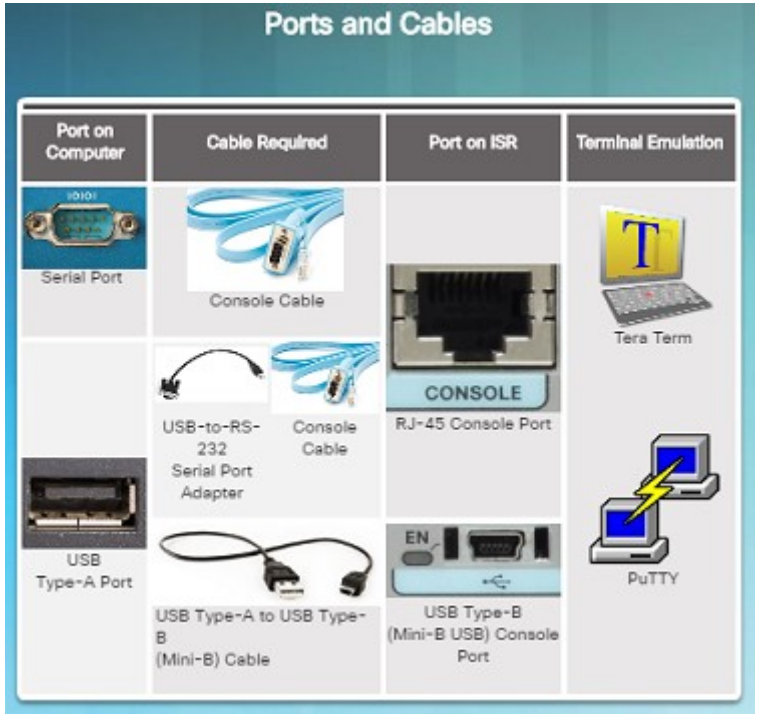
- Host computers connect to a wired network using a RJ-45 Ethernet cable.
- Most network interface cards have one or two LED indicators next to the interface.
  - Green LED indicates a good connection.
  - A blinking green indicates network activity.
  - No light indicates a problem with either the network 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.



#	Port	LED	Color	Description
1	GE0/0 and GE0/1	S (Speed)	1 blink + pause	Port operating at 10 Mb/s
			2 blink + pause	Port operating at 100 Mb/s
			3 blink + pause	Port operating at 1000 Mb/s
		L (Link)	Green	Link is active
			Off	Link is inactive
2	Console	EN	Green	Port is active
			Off	Port is inactive
3	USB	EN	Green	Port is active
			Off	Port is inactive

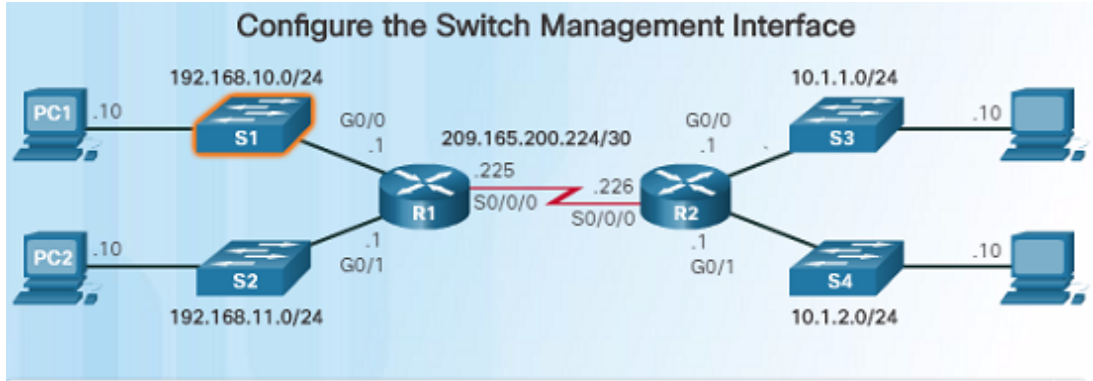
Console Access

- 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.



Enable IP on a Switch

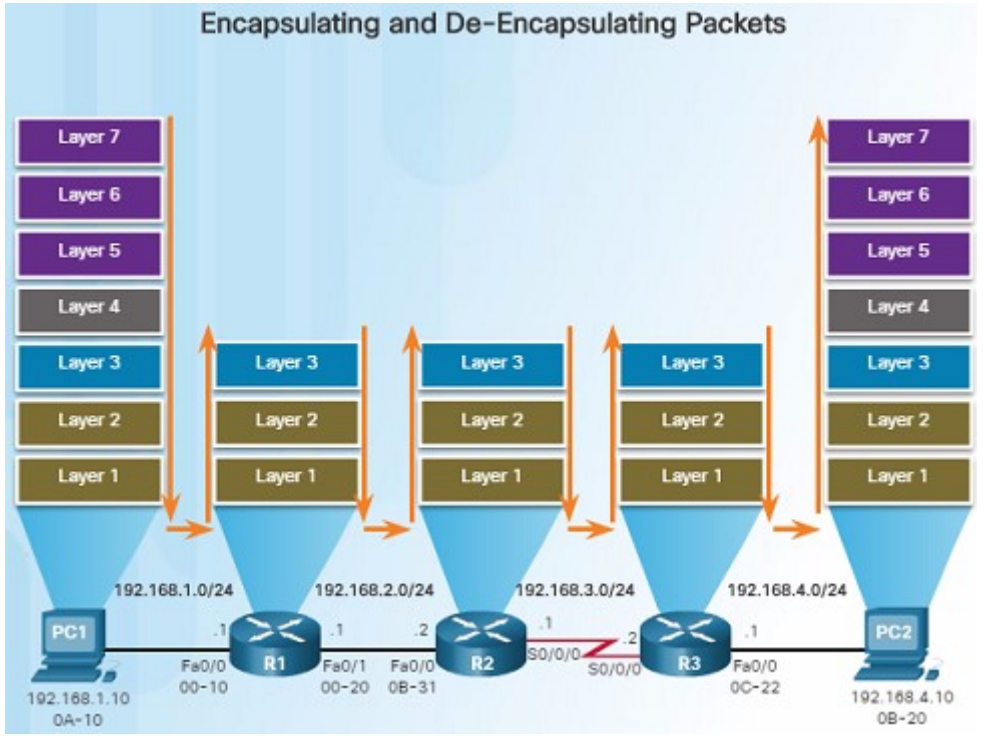
- Network devices require IP addresses in order for the network administrator to connect to the devices using Telnet, SSH, HTTP, or HTTPS.
- A switch requires an IP address to be configured on a virtual interface, called the switched virtual interface (SVI).
- Commands in the figure to the left should be used to configure the IP address on vlan 1 and also the default-gateway information.




```
S1(config)# interface vlan 1
S1(config-if)# ip address 192.168.10.2 255.255.255.0
S1(config-if)# no shutdown
%LINK-5-CHANGED: Interface Vlan1, changed state to up
S1(config-if)# exit
S1(config)#
S1(config)# ip default-gateway 192.168.10.1
S1(config)#
```

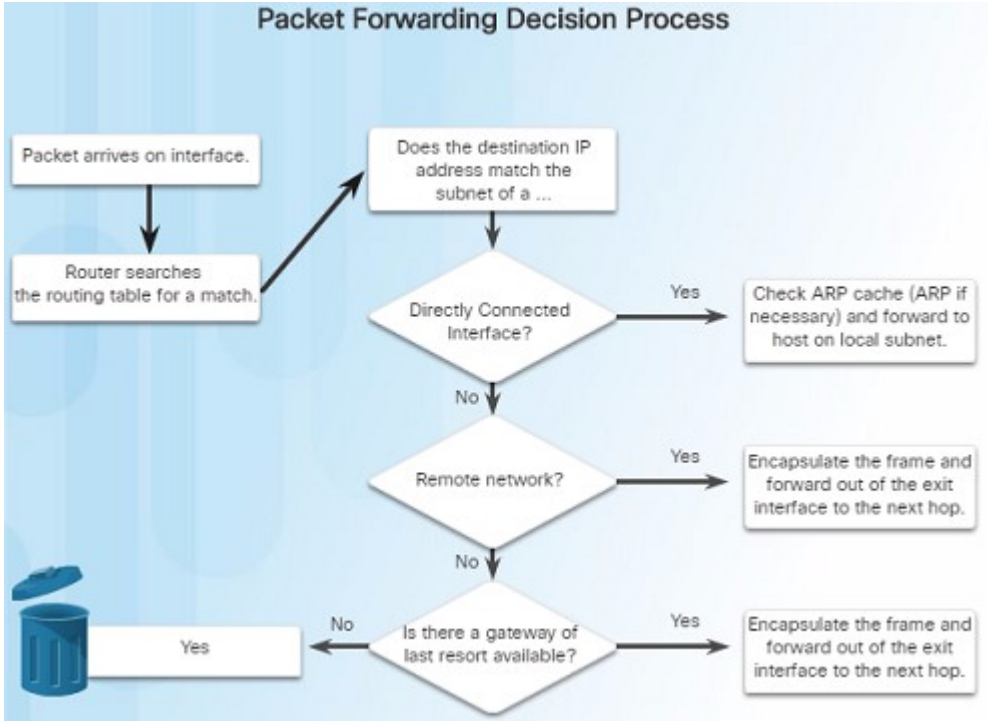
Router Switching Function

- The primary function of a router is to forward packets toward their destination.
  - Uses a switching function which is a process that accepts a packet on one interface and forwards it out of another interface. This is not to be confused with the function of a Layer 2 switch.
  - The switching function also encapsulates the packets in the appropriate data link frame type for the outgoing interface.



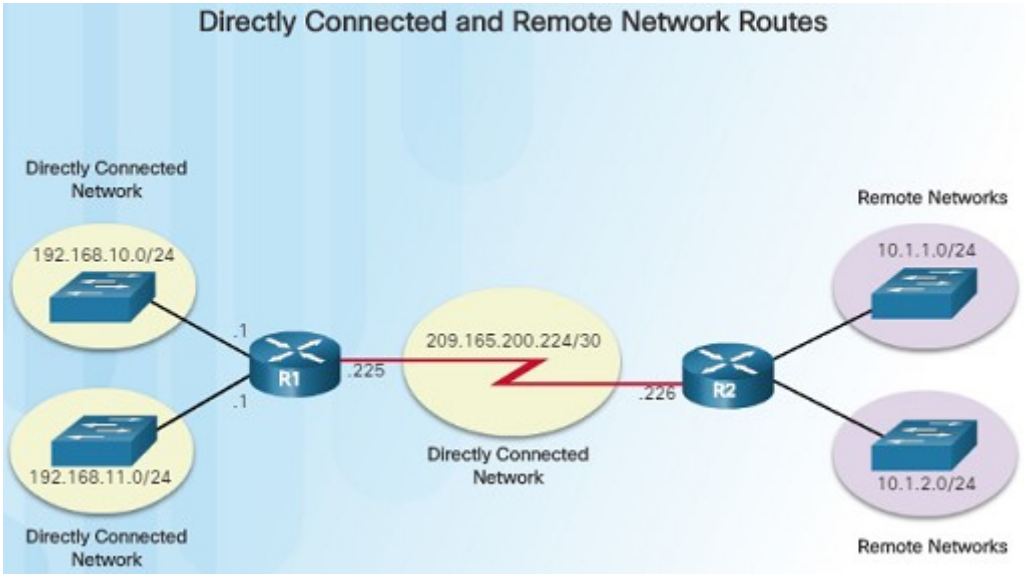
Routing Decisions

- The primary function of a router is to determine the best path to send packets.
- A routing table search results in one of three path determinations:
  - Directly connected network – 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 network – If the destination IP address of the packet belongs to a remote network, the packet is forwarded to another router.
  - No route determined – If the destination IP address does not belong to a connected network or is in the routing table, the packet is sent to Gateway of Last Resort.



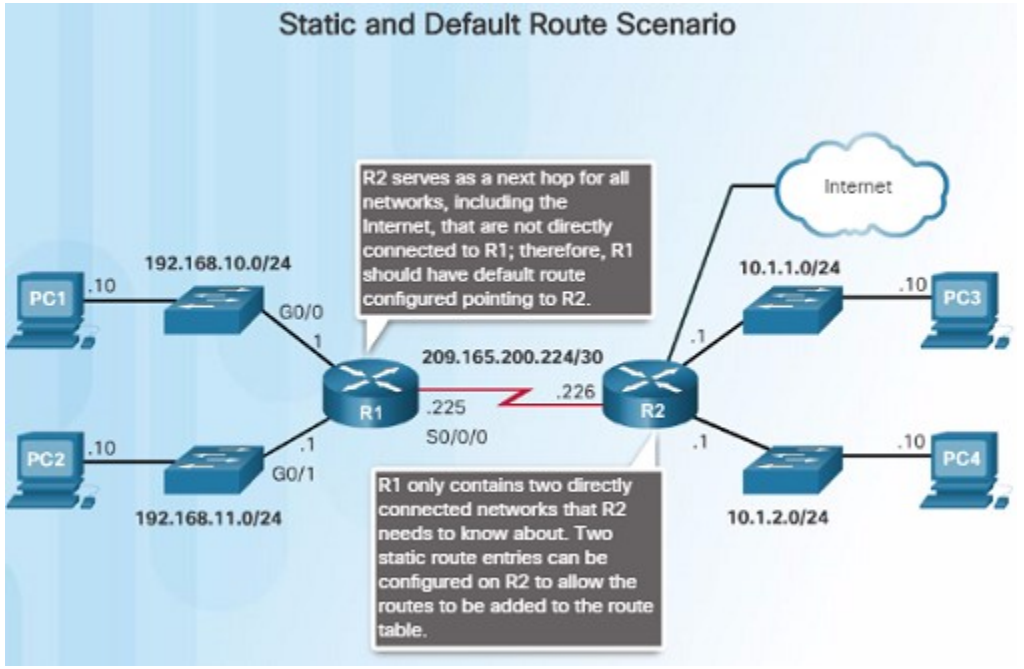
The Routing Table

- The routing table of a router stores information about:
  - Directly connected routes – Obtained from the active router interfaces.
  - Remote routes – These are remote networks connected to other routers that are learned from dynamic routing protocols or are statically configured.
- A routing table is a data file in RAM that is used to store information about directly connected and remote networks.
- The routing table contains next hop associations for remote networks. The association tells the router what the next hop is for a destination network.



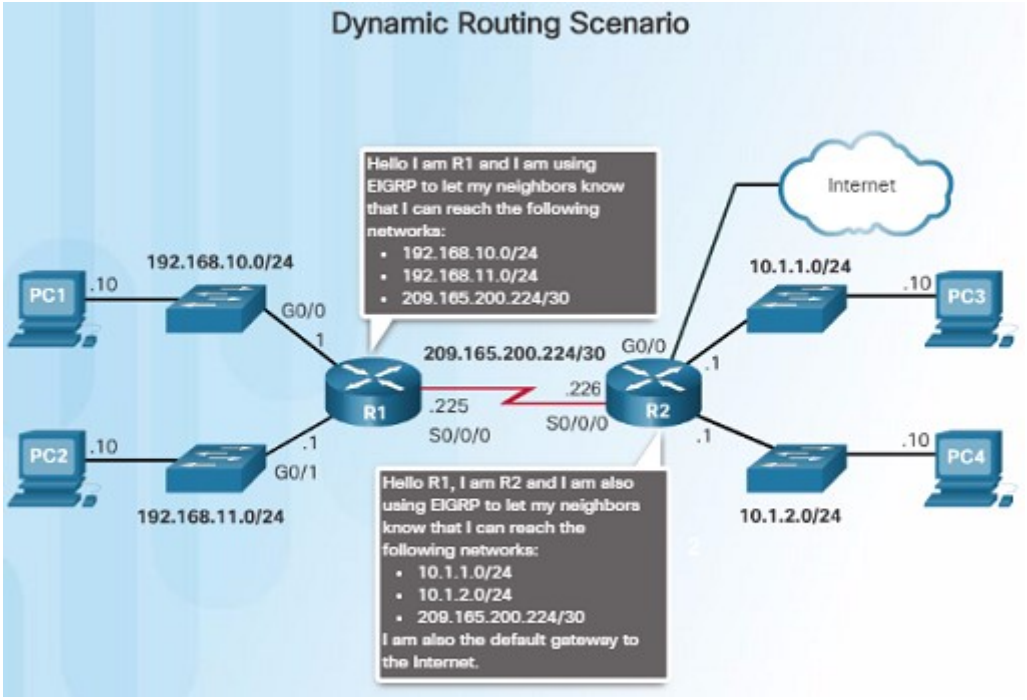
Static Routes

- After directly connected interfaces are configured and added to the routing table, then static or dynamic routing can be configured.
- Static routes are manually configured and define an explicit path between two networking devices.
- If the network topology changes, static routes must manually be reconfigured.
- Benefits of static routes include:
  - Improved security
  - Resource efficiency – less bandwidth usage and no CPU cycles are used to calculate and communicate route



Dynamic Routing

- Dynamic routing protocols are used by routers to share information about the reachability and status of remote networks.
- Rather than manually configuring static routes, dynamic routing protocols use network discovery to share information about the networks that it knows about with other routers that are using the same routing protocol.
- Routers have converged after they have finished exchanging and updating their routing tables. Routers then maintain the networks in their routing tables.



Practical Classes

- In class lab sessions will start from next week
- Lab activities will count towards continuous assessment marks
- Download and try out Packet Tracer software:
  - https://www.netacad.com/courses/packet-tracer

LMS

- LMS
  - Self Enrolment key: **2019S1AN**
  - http://lms.tech.sjp.ac.lk/course/view.php?id=11
- Contact & Feedback:
  - https://academic.nimal.info/

Ask Early, Ask Often.