

Chapter 6: Network Layer

CCNA Routing and Switching

Introduction to Networks v6.0



Chapter 6 - Sections & Objectives

▪ 6.1 Network Layer Protocols

- Explain how network layer protocols and services support communications across data networks
- Describe the purpose of the network layer in data communication.
- Explain why the IPv4 protocol requires other layers to provide reliability.
- Explain the role of the major header fields in the IPv4 packet.
- Explain the role of the major header fields in the IPv6 packet.

▪ 6.2 Routing

- Explain how routers enable end-to-end connectivity in a small to medium-sized business network.
- Explain how network devices use routing tables to direct packets to a destination network.
- Compare a host routing table to a routing table in a router.

Chapter 6 - Sections & Objectives (Cont.)

▪ 6.3 Routers

- Explain how devices route traffic in a small to medium-sized business network
 - Describe the common components and interface of a router.
 - Describe the boot-up process of a Cisco IOS router.

▪ 6.4 Configuring a Cisco Router

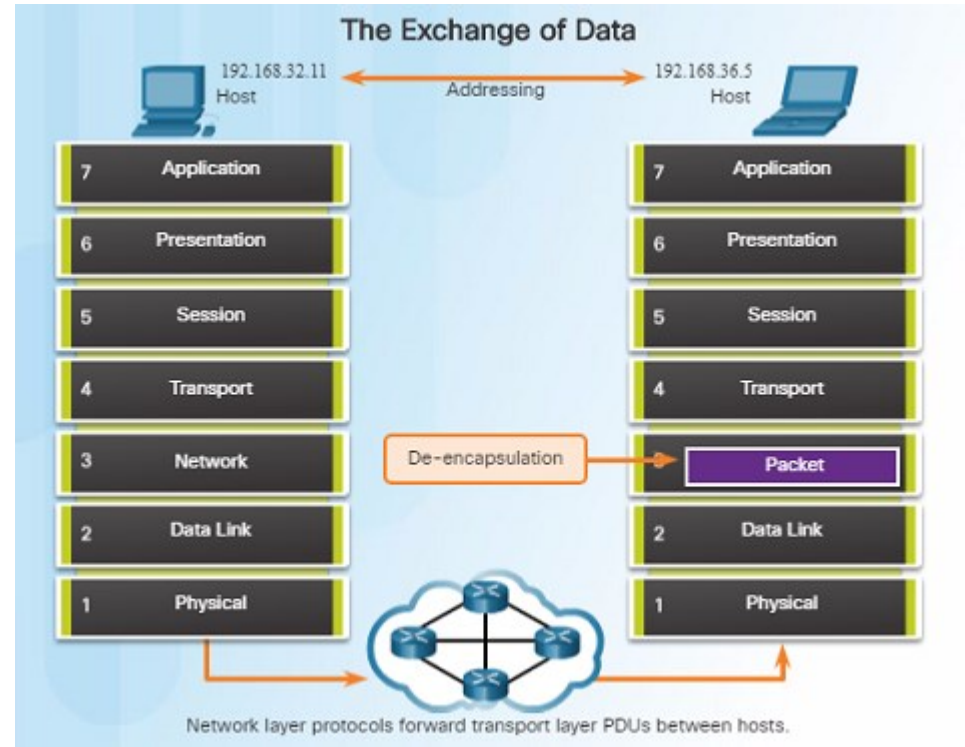
- Configure a router with basic configurations.
- Configure initial settings on a Cisco IOS router.
- Configure two active interfaces on a Cisco IOS router.
- Configure devices to use the default gateway

6.1 Network Layer Protocols

Network Layer in Communications

The Network Layer

- The network layer, which resides at OSI Layer 3, provides services that allow end devices to exchange data across a network.
- The network layer uses four processes in order to provide end-to-end transport:
 - Addressing of end devices – IP addresses must be unique for identification purposes.
 - Encapsulation – The protocol data units from the transport layer are encapsulated by adding IP header information including source and destination IP addresses.
 - Routing – The network layer provides services to direct packets to other networks. Routers select the best path for a packet to take to its destination network.
 - De-encapsulation – The destination host de-encapsulates the packet to see if it matches its own.

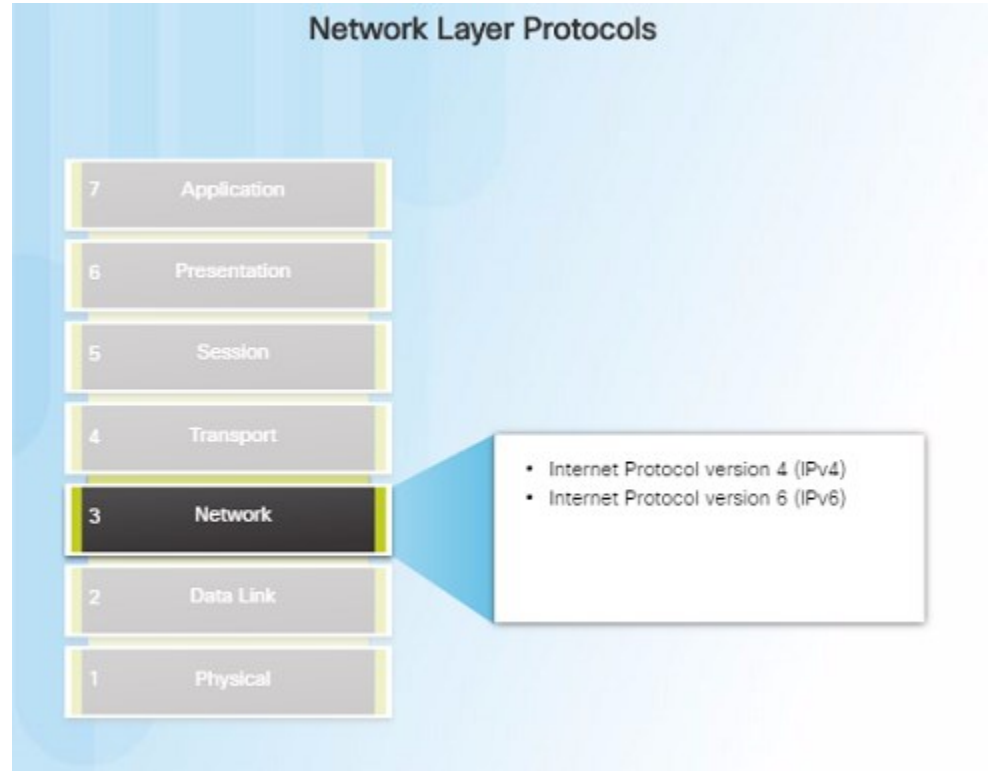


Network Layer in Communications

Network Layer Protocols

- There are several network layer protocols in existence; however, the most commonly implemented are:
 - Internet Protocol version 4 (IPv4)
 - Internet Protocol version 6 (IPv6)

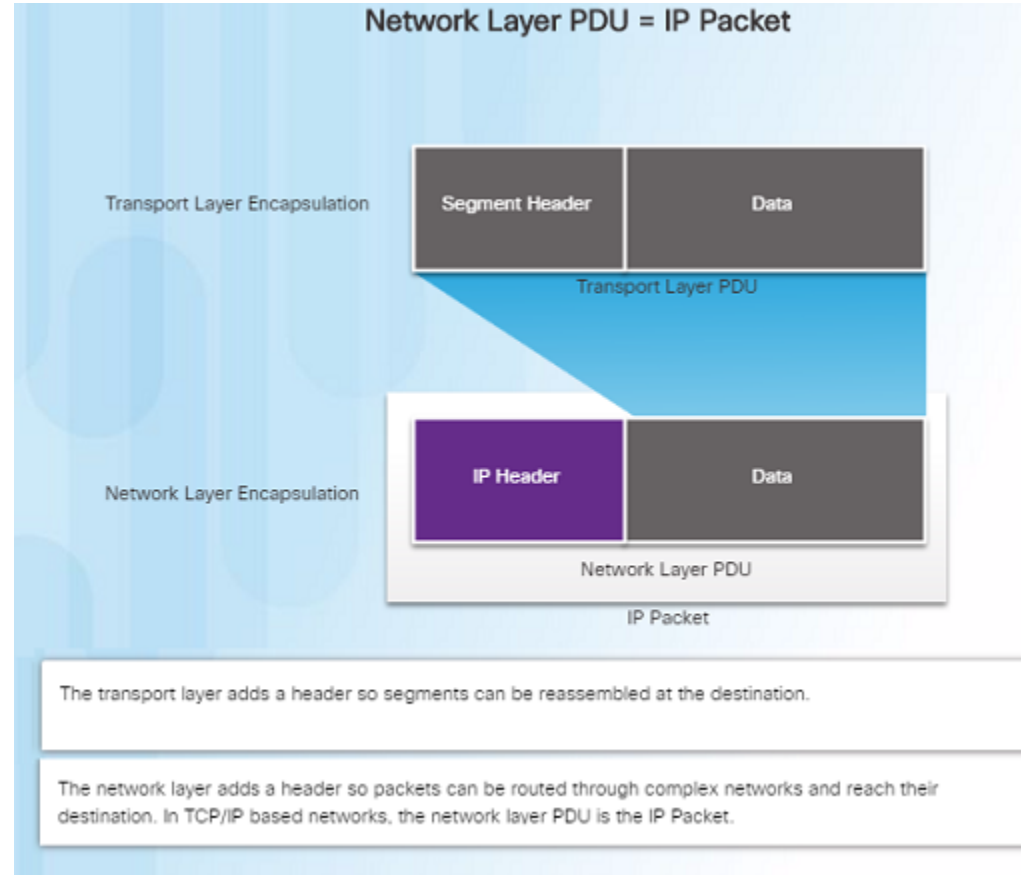
Note: Legacy network layer protocols are not discussed in this course.



Characteristics of the IP Protocol

Encapsulating IP

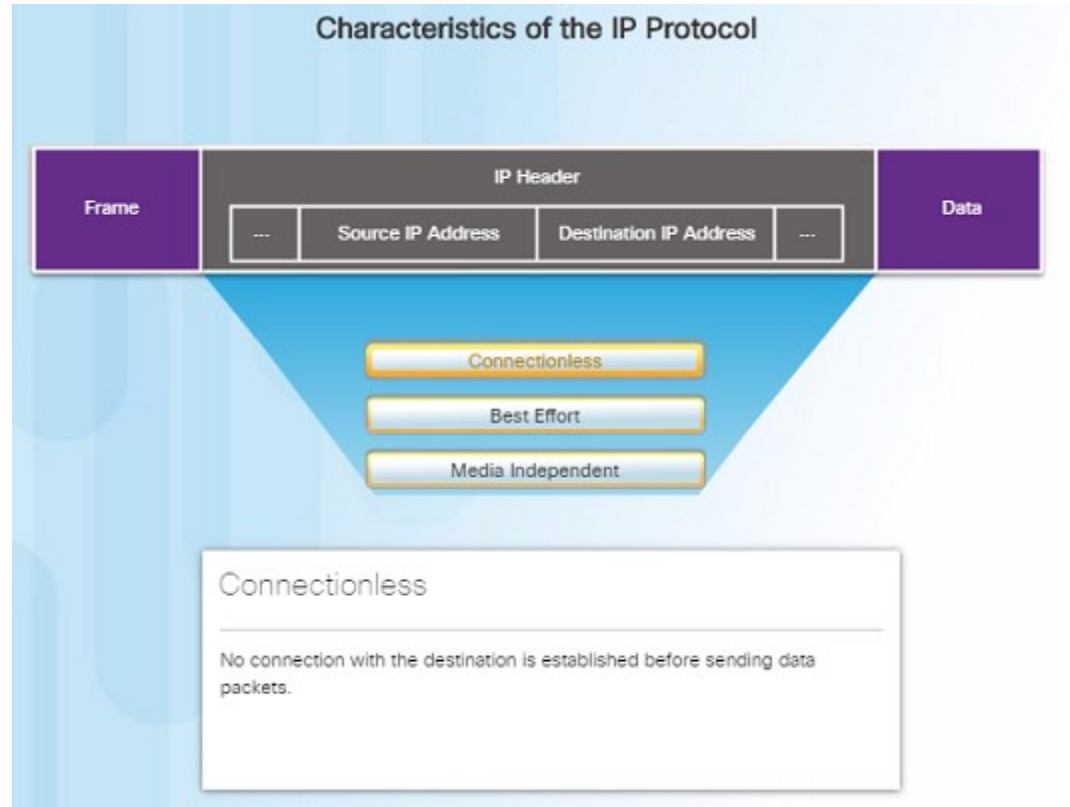
- At the network layer, IP encapsulates the transport layer segment by adding an IP header for the purpose of delivery to the destination host.
- The IP header stays the same from the source to the destination host.
- The process of encapsulating data layer by layer enables the services at different layers to scale without affecting other layers.
- Routers implement different network layer protocols concurrently over a network and use the network layer packet header for routing.



Characteristics of the IP Protocol

Characteristics of IP

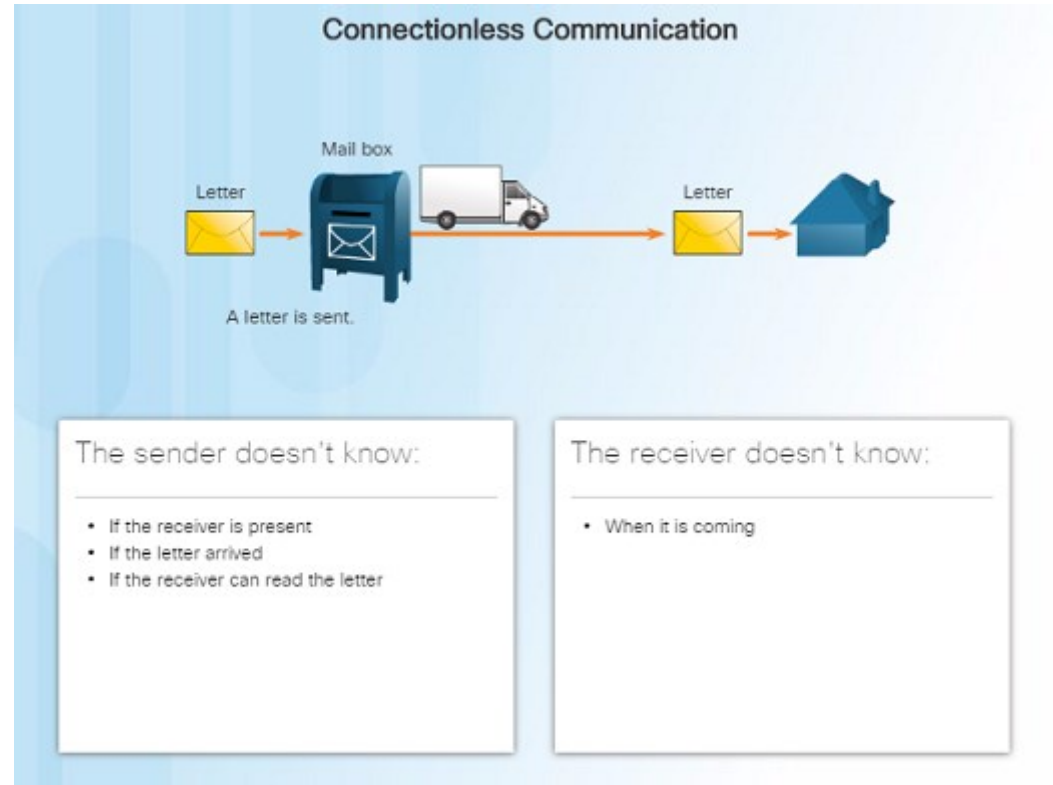
- IP was designed as a protocol with low overhead – it provides only the functions required to deliver a packet from the source to a destination.
- An IP packet is sent to the destination without prior establishment of a connection
- IP was not designed to track and manage the flow of packets.
- These functions, if required, are performed by other layers – primarily TCP



Characteristics of the IP Protocol

IP - Connectionless

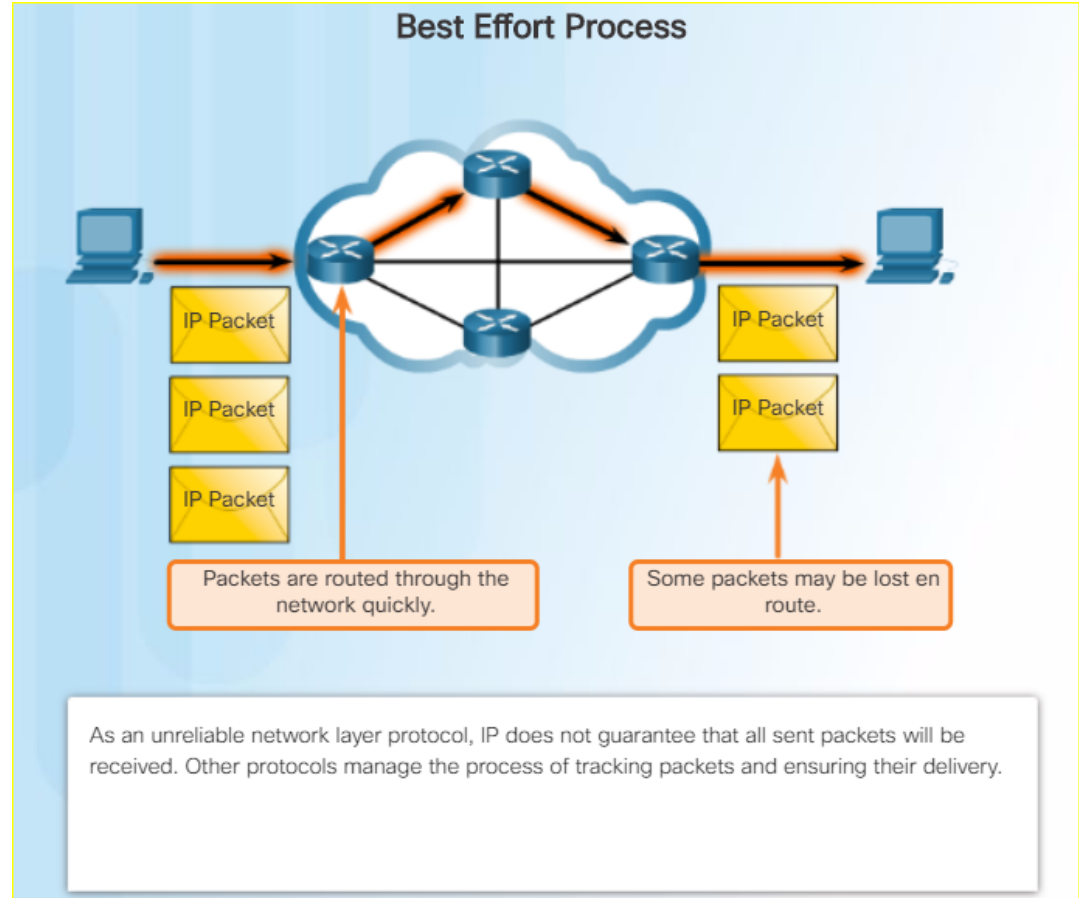
- IP is a connectionless protocol:
 - No dedicated end-to-end connection is created before data is sent.
 - Very similar process as sending someone a letter through snail mail.
 - Senders do not know whether or not the destination is present, reachable, or functional before sending packets.
 - This feature contributes to the low overhead of IP.



Characteristics of the IP Protocol

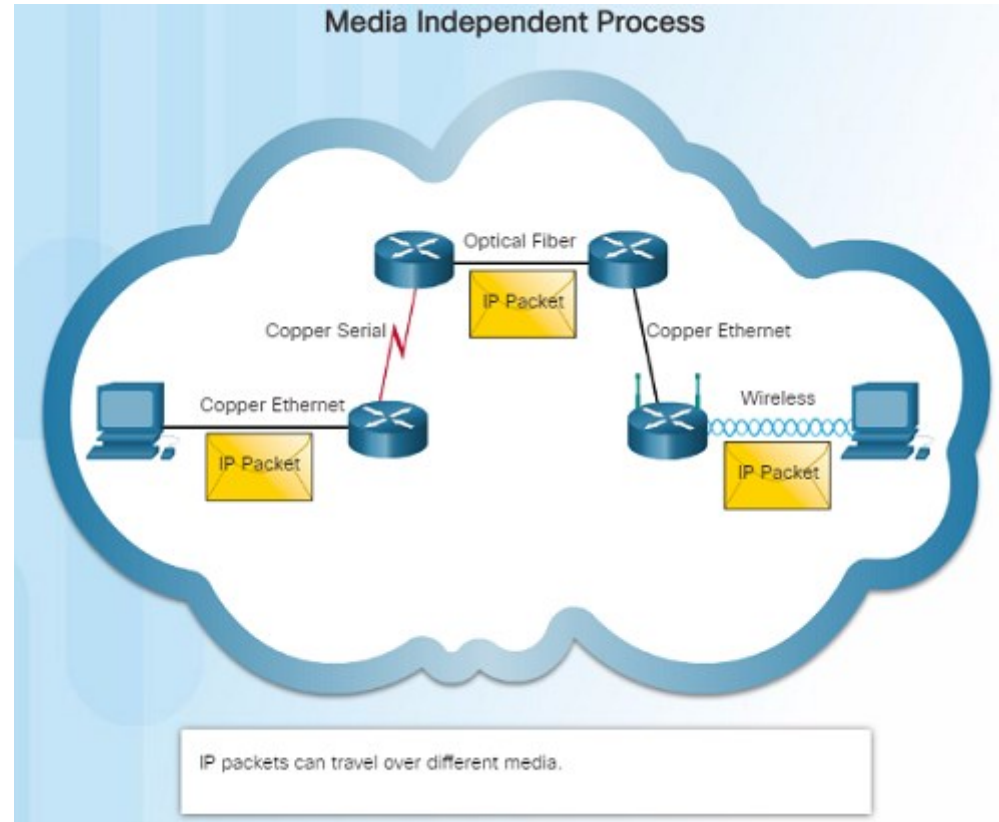
IP – Best Effort Delivery

- IP is a Best Effort Delivery protocol:
 - IP is considered “unreliable” because it does not guarantee that all packets that are sent will be received.
 - Unreliable means that IP does not have the capability to manage and recover from undelivered, corrupt, or out of sequence packets.
 - If packets are missing or not in the correct order at the destination, upper layer protocols/services must resolve these issues.



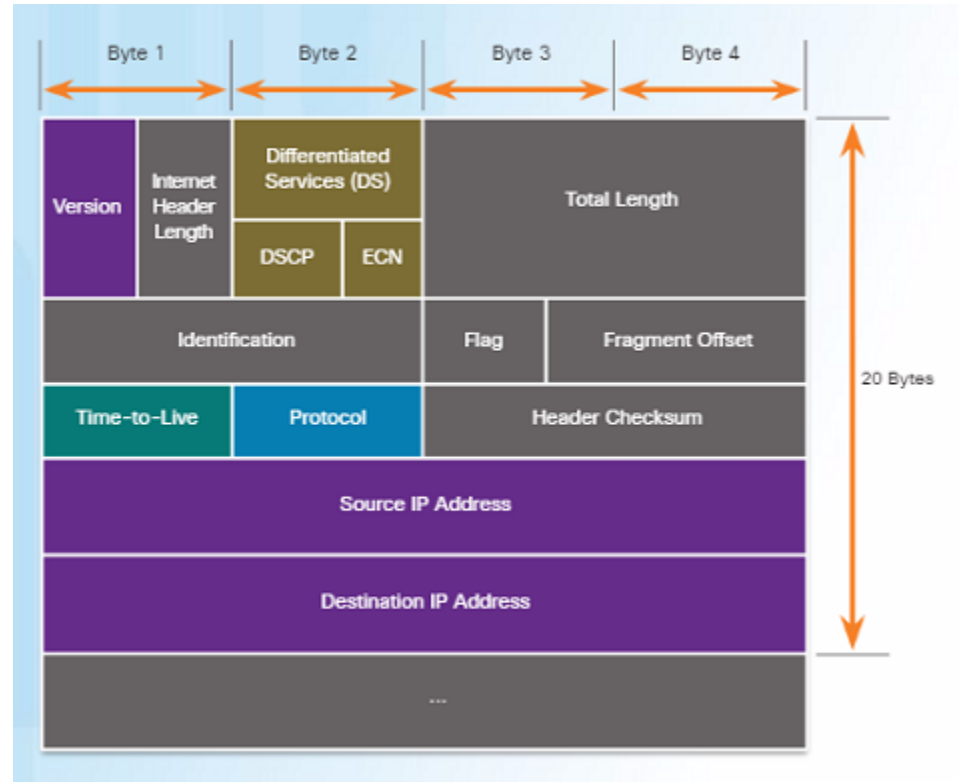
IP – Media Independent

- IP operates independently from the media that carries the data at lower layers of the protocol stack – it does not care if the media is copper cables, fiber optics or wireless.
- The OSI data link layer is responsible for taking the IP packet and preparing it for transmission over the communications medium.
- The network layer does have a maximum size of the PDU that can be transported – referred to as MTU (maximum transmission unit).
- The data link layer tells the network layer the MTU.



IPv4 Packet Header

- An IPv4 packet header consists of the fields containing binary numbers. These numbers identify various settings of the IP packet which are examined by the Layer 3 process.
- Significant fields include:
 - Version – Specifies that the packet is IP version 4
 - Differentiated Services or DiffServ (DS) – Used to determine the priority of each packet on the network.
 - Time-to-Live (TTL) – Limits the lifetime of a packet – decreased by one at each router along the way.
 - Protocol – Used to identify the next level protocol.
 - Source IPv4 Address – Source address of the packet.
 - Destination IPv4 Address – Address of destination.



Video Demonstration – Sample IPv4 Headers in Wireshark

- Wireshark is a free and open source packet and network protocol analyzer that allows you to capture and browse network traffic.



Limitations of IPv4

- IPv4 has been updated to address new challenges.
- Three major issues still exist with IPv4:
 - IP address depletion – IPv4 has a limited number of unique public IPv4 addresses available. Although there are about 4 billion IPv4 addresses, the exponential growth of new IP-enabled devices has increased the need.
 - Internet routing table expansion – A routing table contains the routes to different networks in order to make the best path determination. As more devices and servers are connected to the network, more routes are created. A large number of routes can slow down a router.
 - Lack of end-to-end connectivity – Network Address Translation (NAT) was created for devices to share a single IPv4 address. However, because they are shared, this can cause problems for technologies that require end-to-end connectivity.





Introducing IPv6

- In the early '90s, the IETF started looking at a replacement for IPv4 – which led to IPv6.
- Advantages of IPv6 over IPv4 include:
 - Increased address space – based on 128-bit addressing vs. 32-bit with IPv4
 - Improved packet handling – fewer fields with IPv6 than IPv4
 - Eliminates the need for NAT – no need to share addresses with IPv6
- There are roughly enough IPv6 addresses for every grain of sand on Earth.

How Many Addresses Are Available with IPv6?

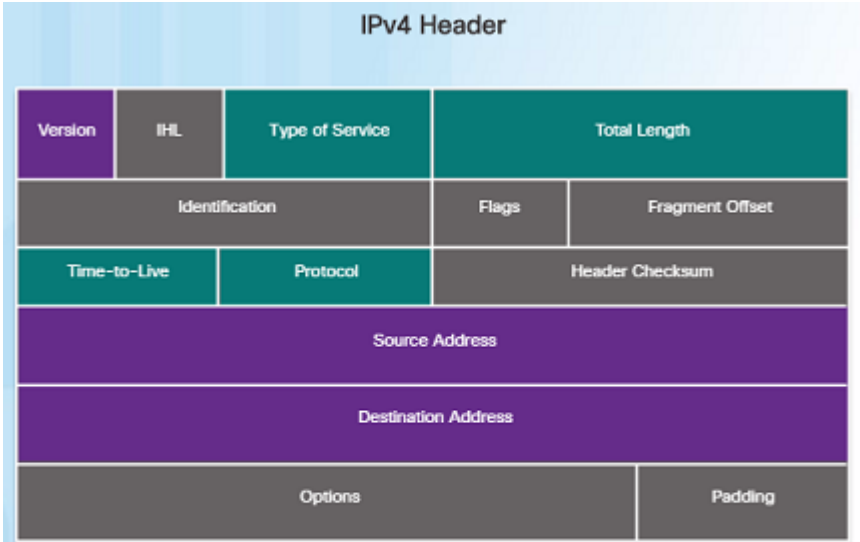
Number Name	Scientific Notation	Number of Zeros
1 Thousand	10^3	1,000
1 Million	10^6	1,000,000
1 Billion	10^9	1,000,000,000
1 Trillion	10^{12}	1,000,000,000,000
1 Quadrillion	10^{15}	1,000,000,000,000,000
1 Quintillion	10^{18}	1,000,000,000,000,000,000
1 Sextillion	10^{21}	1,000,000,000,000,000,000,000
1 Septillion	10^{24}	1,000,000,000,000,000,000,000,000
1 Octillion	10^{27}	1,000,000,000,000,000,000,000,000,000
1 Nonillion	10^{30}	1,000,000,000,000,000,000,000,000,000,000
1 Decillion	10^{33}	1,000,000,000,000,000,000,000,000,000,000,000
1 Undecillion	10^{36}	1,000,000,000,000,000,000,000,000,000,000,000,000

Legend

-  There are 4 billion IPv4 addresses
-  There are 340 undecillion IPv6 addresses

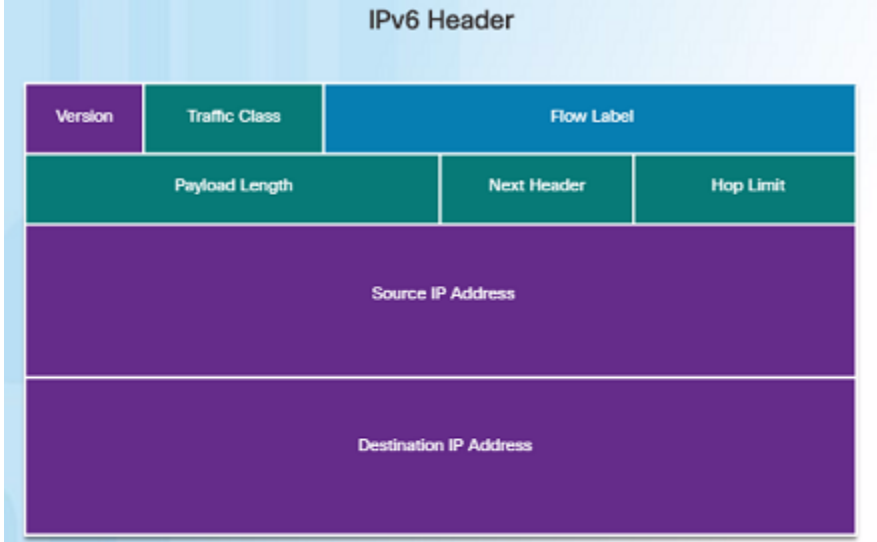
Encapsulating IPv6

- The IPv6 header is simpler than the IPv4 header.



Legend

- Field names kept from IPv4 to IPv6
- Name and position changed in IPv6
- Fields not kept in IPv6



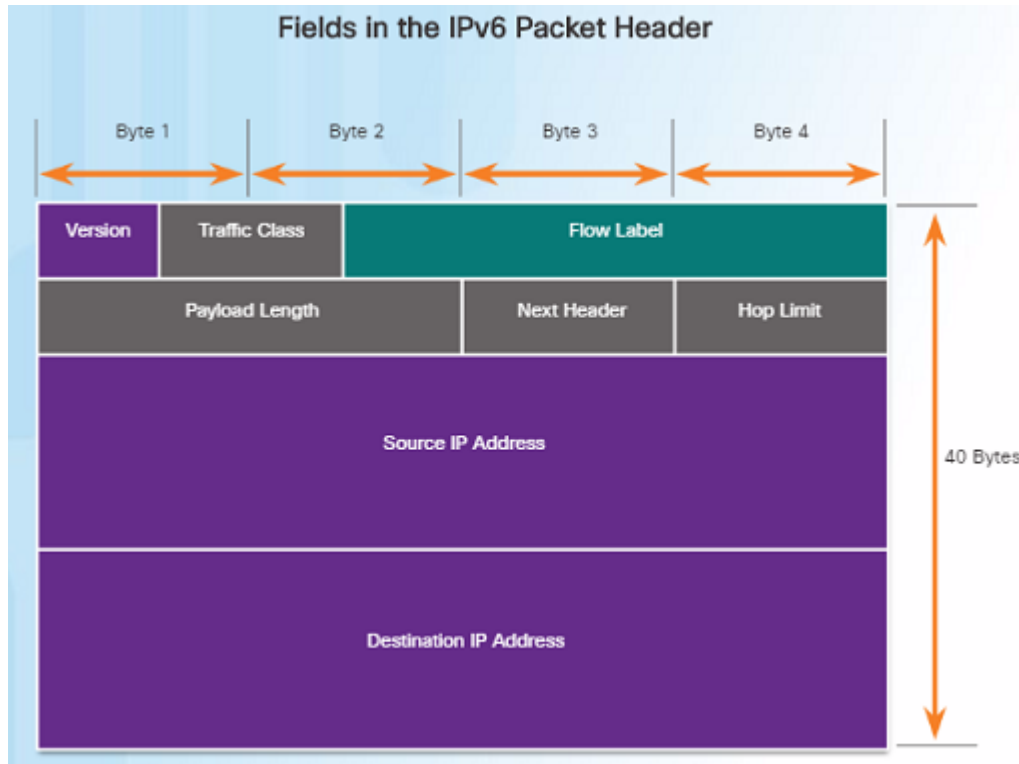
Legend

- Field names kept from IPv4 to IPv6
- Name and position changed in IPv6
- New field in IPv6

Encapsulating IPv6 (Cont.)

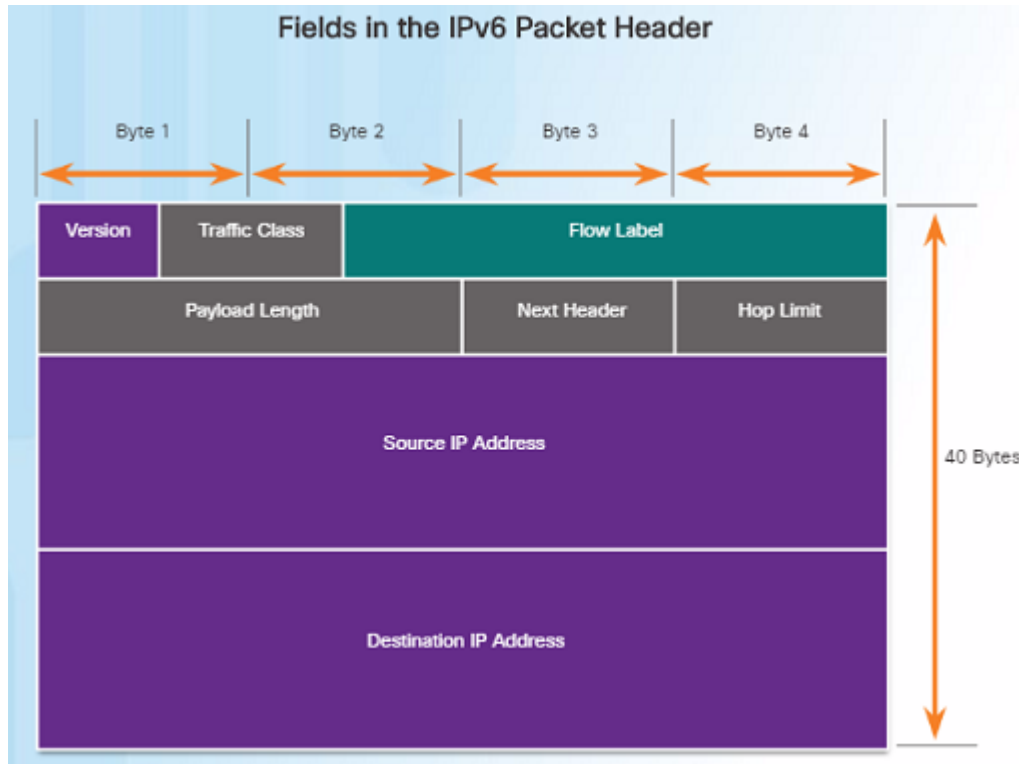
- Advantages of IPv6 over IPv4 using the simplified header:
 - Simplified header format for efficient packet handling
 - Hierarchical network architecture for routing efficiency
 - Autoconfiguration for addresses
 - Elimination of need for network address translation (NAT) between private and public addresses

IPv6 Packet Header



- IPv6 packet header fields:
 - Version – Contains a 4-bit binary value set to 0110 that identifies it as a IPv6 packet.
 - Traffic Class – 8-bit field equivalent to the IPv4 Differentiated Services (DS) field.
 - Flow Label – 20-bit field suggests that all packets with the same flow label receive the same type of handling by routers.
 - Payload Length – 16-bit field indicates the length of the data portion or payload of the packet.
 - Next Header – 8-bit field is equivalent to the IPv4 Protocol field. It indicates the data payload type that the packet is carrying.

IPv6 Packet Header (Cont.)



- IPv6 packet header fields:
 - Hop Limit – 8-bit field replaces the IPv4 TTL field. This value is decremented by 1 as it passes through each router. When it reaches zero, the packet is discarded.
 - Source IPv6 Address – 128-bit field that identifies the IPv6 address of the sending host.
 - Destination IPv6 Address – 128-bit field that identifies the IPv6 address of the receiving host.

Video Demonstration – Sample IPv6 Headers and Wireshark

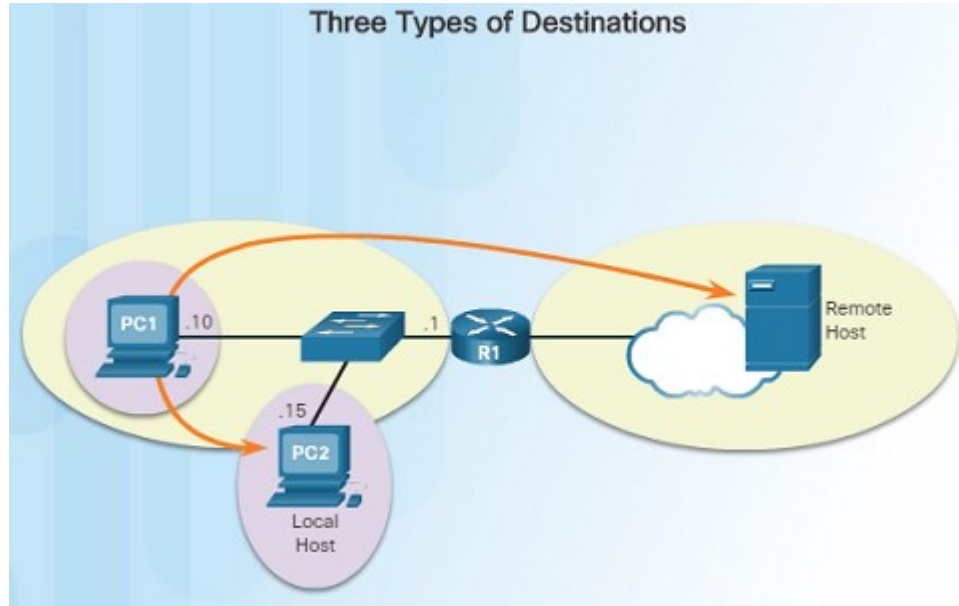
- This video demonstration walks through an IPv6 packet capture screenshot using Wireshark. The source, destination, type of packet, and purpose of the packet are discussed.
- Protocol field information for this IPv6 packet are also deciphered and discussed.



6.2 Routing

How a Host Routes

Host Forwarding Decision



- An important role of the network layer is to direct packets between hosts. A host can send a packet to:
 - Itself – A host can ping itself for testing purposes using 127.0.0.1 which is referred to as the loopback interface.
 - Local host – This is a host on the same local network as the sending host. The hosts share the same network address.
 - Remote host – This is a host on a remote network. The hosts do not share the same network address.
- The source IPv4 address and subnet mask is compared with the destination address and subnet mask in order to determine if the host is on the local network or remote network.

How a Host Routes

Default Gateway

Default Gateway Functions

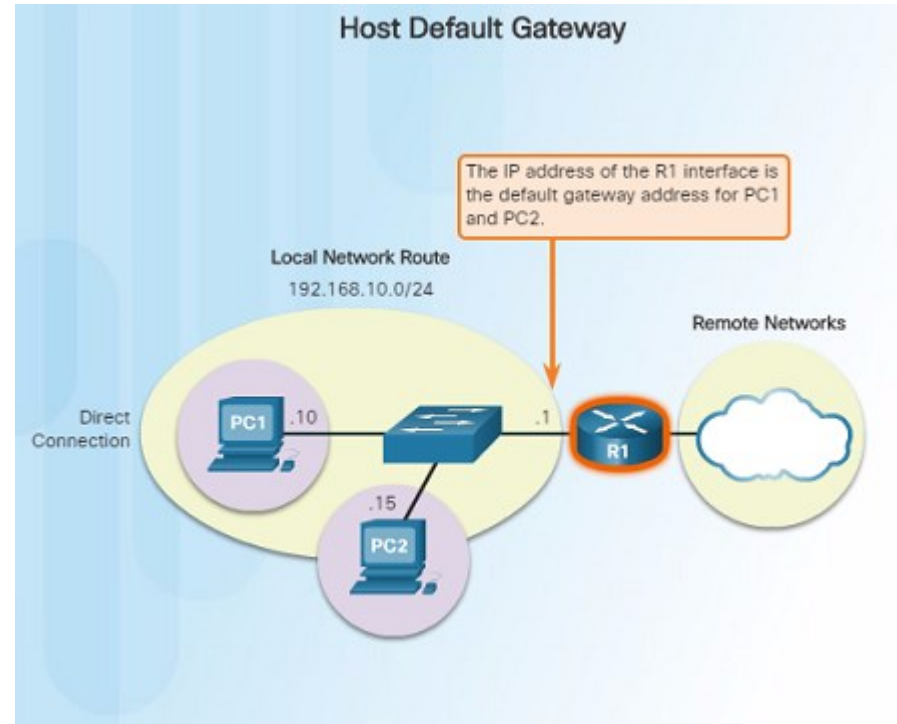
A Default Gateway ...

- Routes traffic to other networks.
- Has a local IP address in the same address range as other hosts on the network.
- Can take data in and forward data out.

- The default gateway is the network device that can route traffic out to other networks. It is the router that routes traffic out of a local network.
- This occurs when the destination host is not on the same local network as the sending host.
- The default gateway will know where to send the packet using its routing table.
- The sending host does not need to know where to send the packet other than to the default gateway – or router.

How a Host Routes Using the Default Gateway

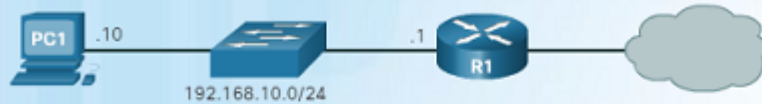
- A host's routing table usually includes a default gateway address – which is the router IP address for the network that the host is on.
- The host receives the IPv4 address for the default gateway from DHCP, or it is manually configured.
- Having a default gateway configured creates a default route in the routing table of a host - which is the route the computer will send a packet to when it needs to contact a remote network.



How a Host Routes

Host Routing Tables

IPv4 Routing Table for PC1



```
C:\Users\PC1> netstat -r
<output omitted>
IPv4 Route Table
```

=====

Active Routes:

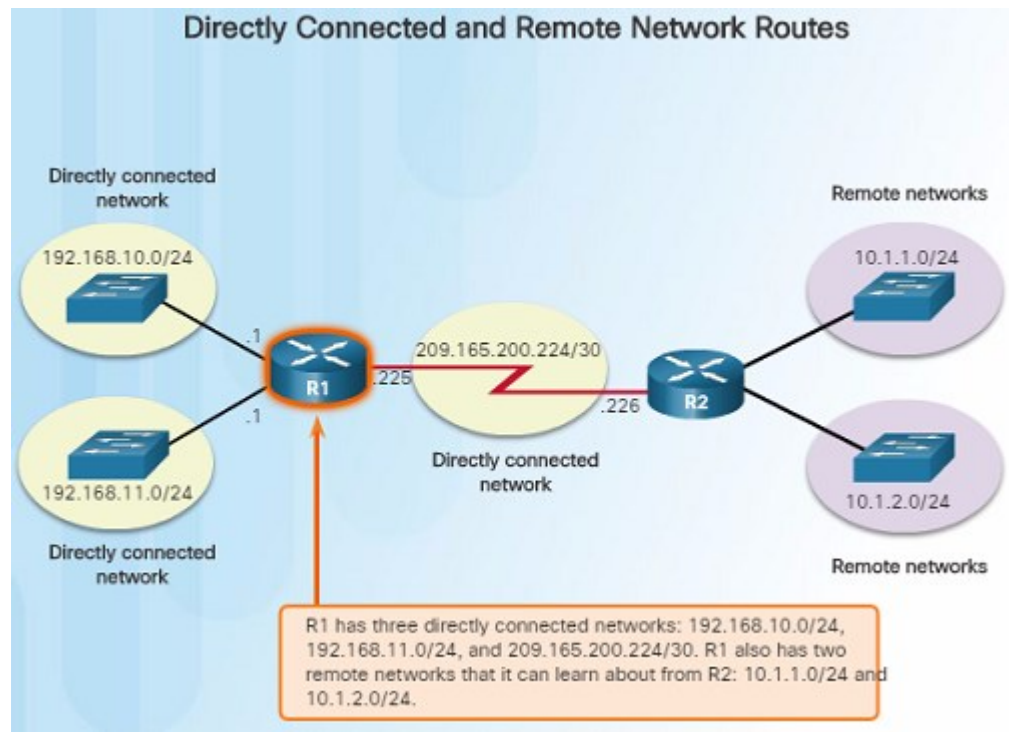
Network Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	192.168.10.1	192.168.10.10	25
127.0.0.0	255.0.0.0	On-link	127.0.0.1	306
127.0.0.1	255.255.255.255	On-link	127.0.0.1	306
127.255.255.255	255.255.255.255	On-link	127.0.0.1	306
192.168.10.0	255.255.255.0	On-link	192.168.10.10	281
192.168.10.10	255.255.255.255	On-link	192.168.10.10	281
192.168.10.255	255.255.255.255	On-link	192.168.10.10	281
224.0.0.0	240.0.0.0	On-link	127.0.0.1	306
224.0.0.0	240.0.0.0	On-link	192.168.10.10	281
255.255.255.255	255.255.255.255	On-link	127.0.0.1	306
255.255.255.255	255.255.255.255	On-link	192.168.10.10	281

=====

```
<output omitted>
```

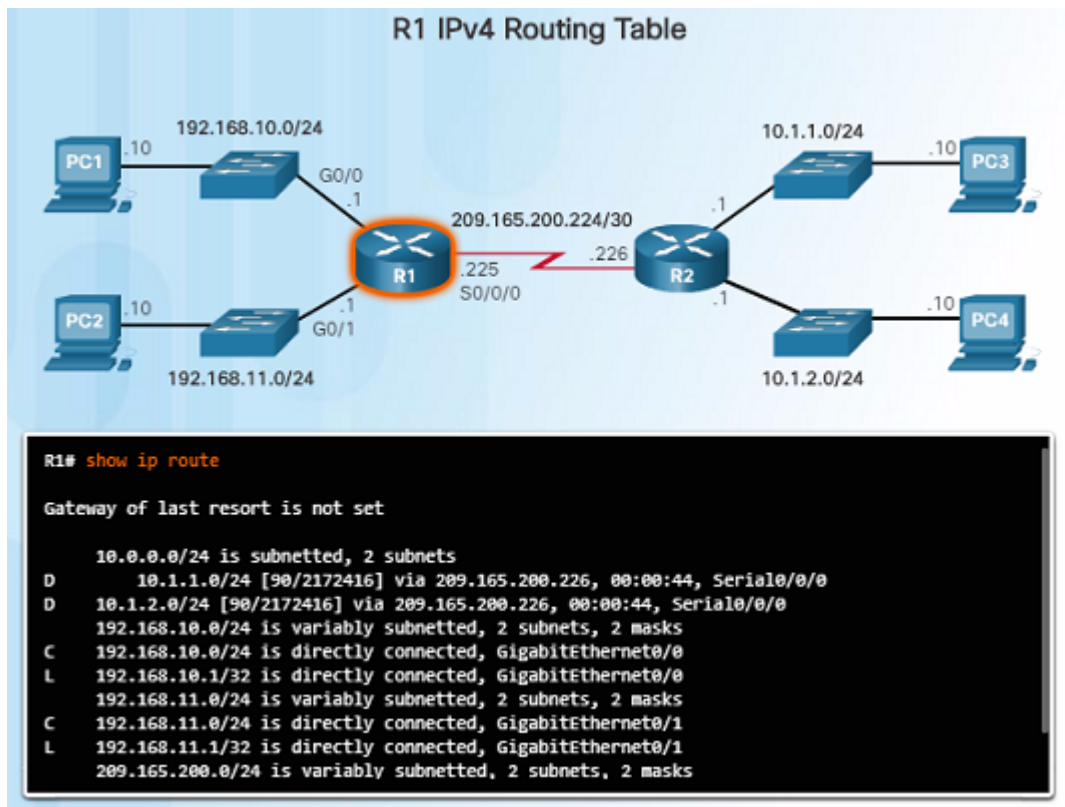
- On a Windows host, you can display the routing table using:
 - **route print**
 - **netstat -r**
- Three sections will be displayed:
 - Interface List – Lists the Media Access Control (MAC) address and assigned interface number of network interfaces on the host.
 - IPv4 Route Table – Lists all known IPv4 routes.
 - IPv6 Route Table – Lists all known IPv6 routes.

Router Packet Forwarding Decision



- When a router receives a packet destined for a remote network, the router has to look at its routing table to determine where to forward the packet. A router's routing table contains:
- Directly-connected routes – These routes come from the active router interfaces configured with IP addresses.
- Remote routes – These routes come from remote networks connected to other routers. They are either configured manually or learned through a dynamic routing protocol.
- Default route – This is where the packet is sent when a route does not exist in the routing table.

IPv4 Router Routing Table



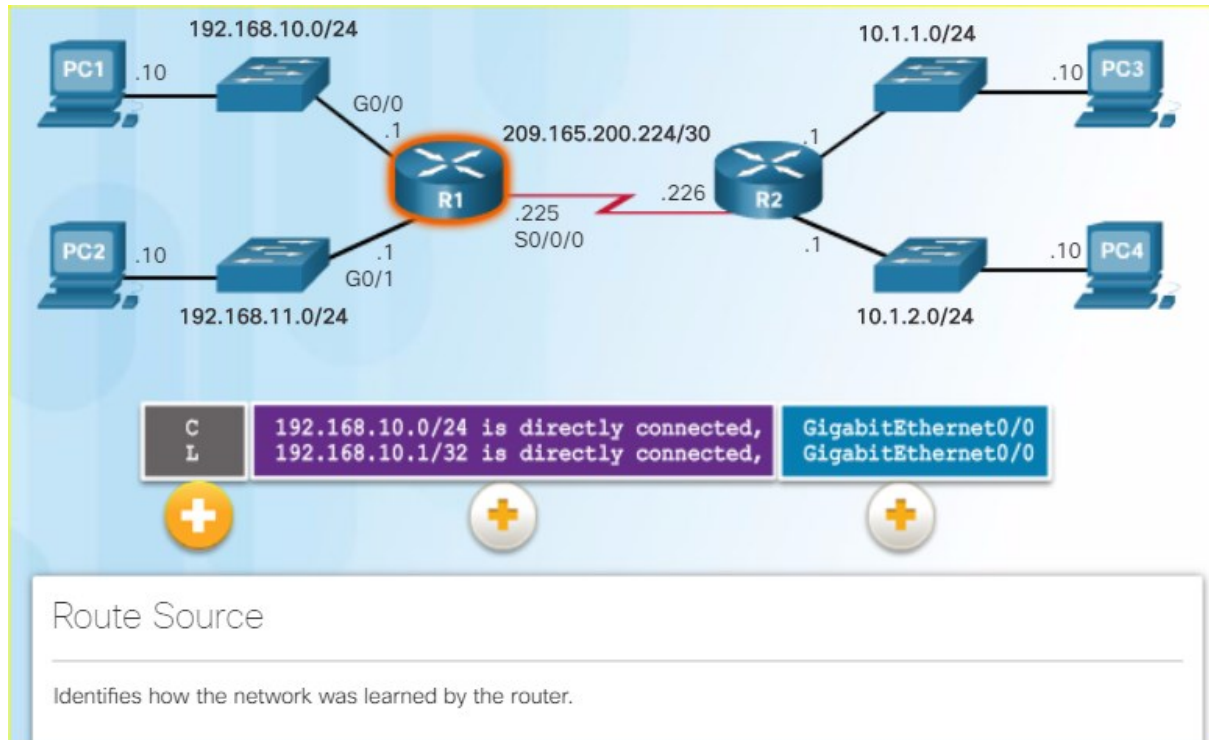
- On a Cisco IOS router, the **show ip route** command is used to display the router's IPv4 routing table. The routing table shows:
 - Directly connected and remote routes
 - How each route was learned
 - Trustworthiness and rating of the route
 - When the route was last updated
 - Which interface is used to reach the destination
- A router examines an incoming packet's header to determine the destination network. If there's a match, the packet is forwarded using the specified information in the routing table.

Video Demonstration – Introducing the IPv4 Routing Table



- A host has a routing table that can be viewed with the **netstat -r** command.
- The routing table includes routes to different networks and information about those routes. For example:
 - The **D** to the left of the 10.1.1.0/24 route indicates that it was learned via the EIGRP routing protocol.
 - The letter **C** means that the network is directly connected.
 - The default gateway of last resort is also indicated.

Directly Connected Routing Table Entries

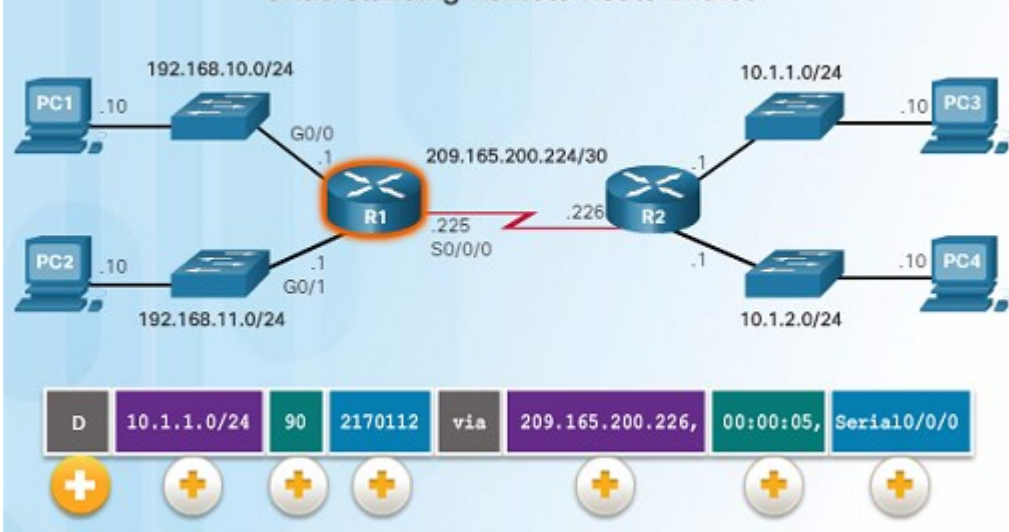


When a router interface is configured and activated, the following two routing table entries are created automatically:

- **C** – Identifies that the network is directly connected and the interface is configured with an IP address and activated.
- **L** – Identifies that it is a local interface. This is the IPv4 address of the interface on the router.

Understanding Remote Route Entries

Understanding Remote Route Entries



- The **D** represents the Route Source which is how the network was learned by the router. **D** identifies the route as an EIGRP route or (Enhanced Interior Gateway Routing Protocol)

- 10.1.1.0/24** identifies the destination network.
- 90** is the administrative distance for the corresponding network – or the trustworthiness of the route. The lower the number, the more trustworthy it is.
- 2170112** – represents the metric or value assigned to reach the remote network. Lower values indicate preferred routes.
- 209.165.200.226** – Next-hop or IP address of the next router to forward the packet.
- 00:00:05** - Route Timestamp identifies when the router was last heard from.
- Serial/0/0/0** – Outgoing Interface

Router Routing Tables

Next-Hop Address

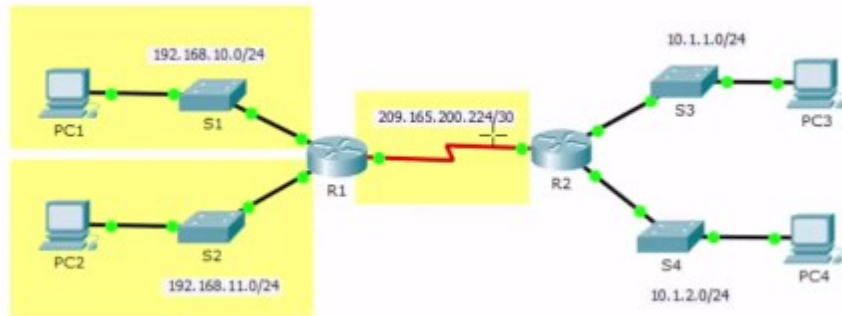


```
R1# show ip route
<output omitted>
Gateway of last resort is not set

  10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D   10.1.1.0/24 [90/2170112] via 209.165.200.226, 00:00:05,
    Serial0/0/0
D   10.1.2.0/24 [90/2170112] via 209.165.200.226, 00:00:05,
    Serial0/0/0
C   192.168.10.0/24 is variably subnetted, 2 subnets, 3 masks
L   192.168.10.0/24 is directly connected, GigabitEthernet0/0
L   192.168.10.1/32 is directly connected, GigabitEthernet0/0
C   192.168.11.0/24 is variably subnetted, 2 subnets, 3 masks
L   192.168.11.0/24 is directly connected, GigabitEthernet0/1
L   192.168.11.1/32 is directly connected, GigabitEthernet0/1
C   209.165.200.0/24 is variably subnetted, 2 subnets, 3 masks
L   209.165.200.224/30 is directly connected, Serial0/0/0
L   209.165.200.225/32 is directly connected, Serial0/0/0
R1#
```

- When a packet arrives at a router destined for a remote network, it will send the packet to the next hop address corresponding to the destination network address in its routing table.
- For example, if the R1 router in the figure to the left receives a packet destined for a device on the 10.1.1.0/24 network, it will send it to the next hop address of 209.165.200.226.
- Notice in the routing table, a default gateway address is not set – if the router receives a packet for a network that isn't in the routing table, it will be dropped.

Video Demonstration – Explaining the IPv4 Routing Table



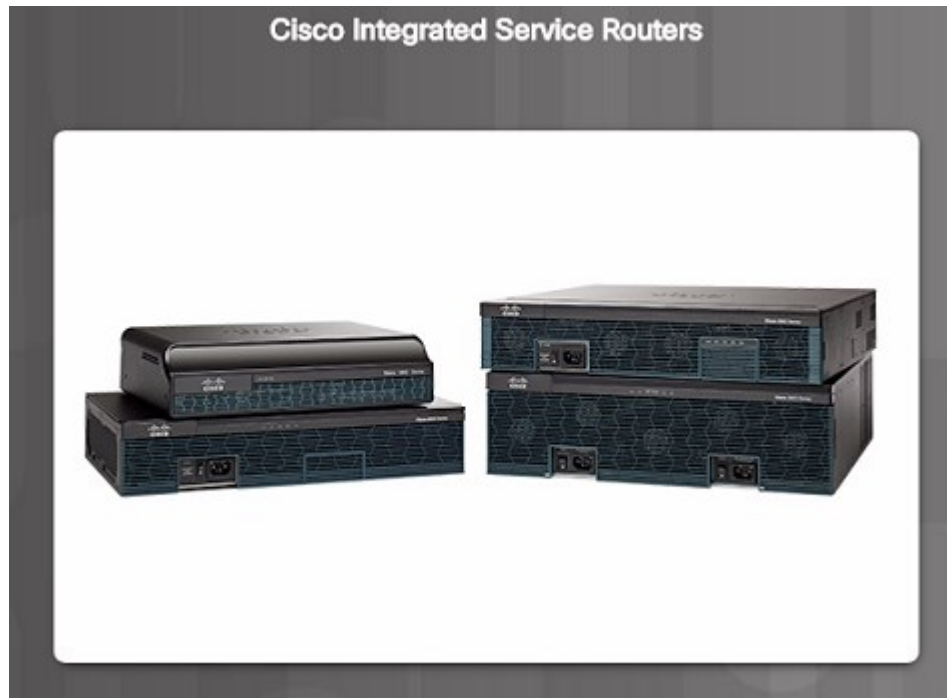
Gateway of last resort is 0.0.0.0 to network 0.0.0.0

```
10.0.0.0/24 is subnetted, 2 subnets
D    10.1.1.0/24 [90/2170112] via 209.165.200.226, 03:00:22, Serial0/0/0
D    10.1.2.0/24 [90/2170112] via 209.165.200.226, 03:00:22, Serial0/0/0
192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.10.0/24 is directly connected, GigabitEthernet0/0
L    192.168.10.1/32 is directly connected, GigabitEthernet0/0
192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.11.0/24 is directly connected, GigabitEthernet0/1
L    192.168.11.1/32 is directly connected, GigabitEthernet0/1
209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C    209.165.200.224/30 is directly connected, Serial0/0/0
L    209.165.200.225/32 is directly connected, Serial0/0/0
```

- Router R1:
 - Has three directly connected routes highlighted in yellow.
 - The first two routing entries of the routing table for networks 10.1.1.0/24 and 10.1.2.0/24 are for the remote networks connected to the R2 router.
 - R1 learned about these networks from R2 via the EIGRP dynamic routing protocol.
 - Next hop router is indicated via 209.165.200.226. This is where the router needs to forward the packet.
 - The router will send the packet to the next hop address by exiting its own Serial0/0/0 interface.
- A connected network entry does not have a next hop address. It will indicate which interface to exit out of, for example, GigabitEthernet0/0.

6.3 Routers

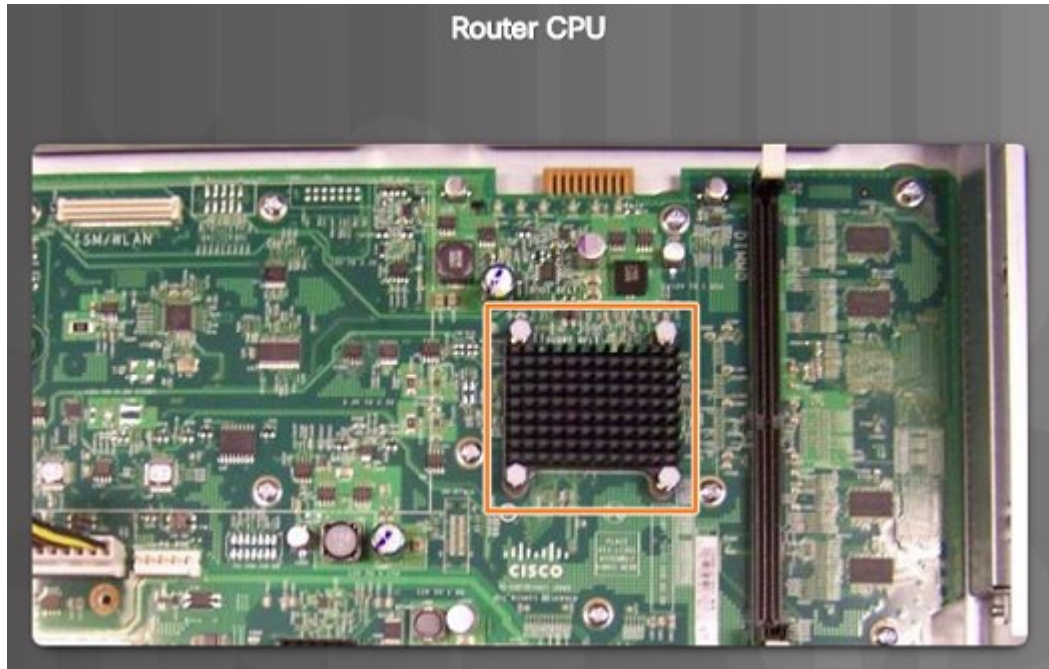
A Router is a Computer



- A router is a computer. Like computers, a router requires a CPU, an operating system, and memory.
- Cisco routers are designed to meet the needs of wide variety of businesses and networks:
 - Branch – Teleworkers, small businesses, and medium-size branch sites.
 - WAN – Large businesses, organizations and enterprises.
 - Service Provider – Large service providers.
- The focus of the CCNA certification is on the branch family of routers.

Anatomy of a Router

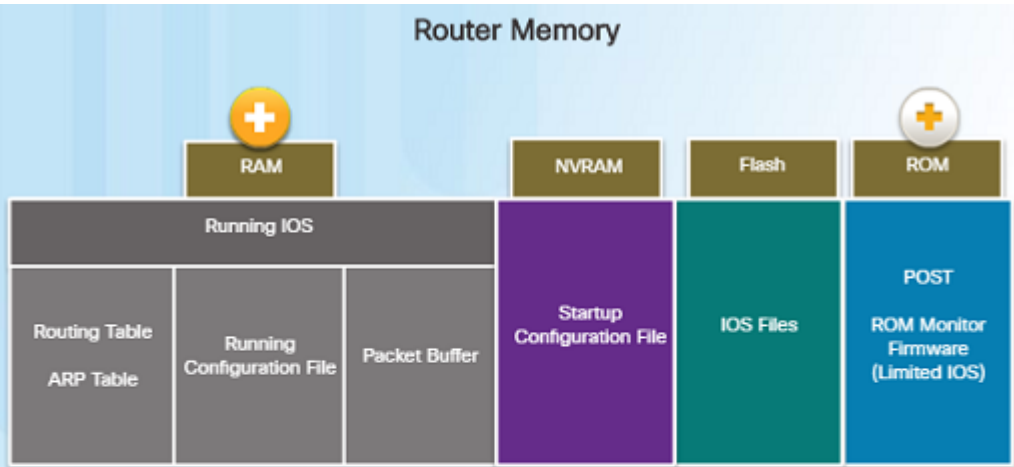
Router CPU and OS



- Like computers, Cisco routers require a CPU to execute OS instructions including system initialization, routing functions and switching functions.
- The component highlighted in the figure to the left is the CPU of a Cisco 1941 with the heatsink attached. A heatsink is used to dissipate the heat from the CPU for cooling purposes.
- The CPU requires an operating system to provide routing and switching functions. Most Cisco devices use the Cisco Internetwork Operating System (IOS).

Anatomy of a Router

Router Memory



RAM

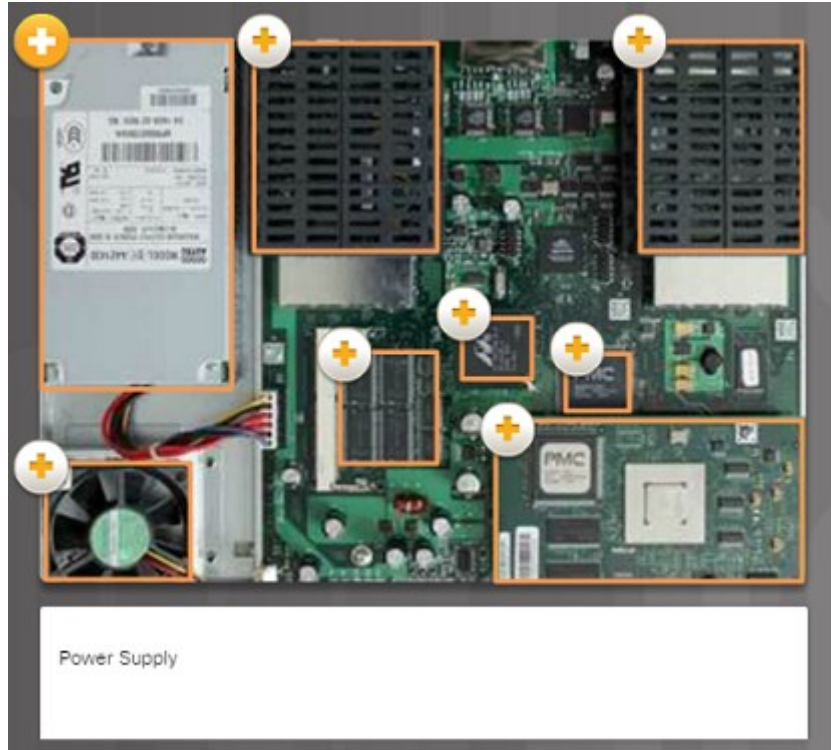
RAM uses the following applications and processes:

- The IOS image and running configuration file
- The routing table used to determine the best path to use to forward packets
- The ARP cache used to map IPv4 addresses to MAC addresses
- The Packet buffer used to temporarily store packets before forwarding to the destination

- Volatile memory – requires continual power to store information.
- Non-volatile memory – does not require continual power.
- A router uses four types of memory:
 - RAM – Volatile memory used to store applications, processes, and data needed to be executed by the CPU.
 - ROM – Non-volatile memory used to store crucial operational instructions and a limited IOS. ROM is firmware embedded on an integrated circuit inside of the router.
 - NVRAM – Non-volatile memory used as permanent storage for the startup configuration file (startup-config).
 - Flash – Non-volatile memory used as permanent storage for the IOS and other operating system files such as log or backup files.

Anatomy of a Router

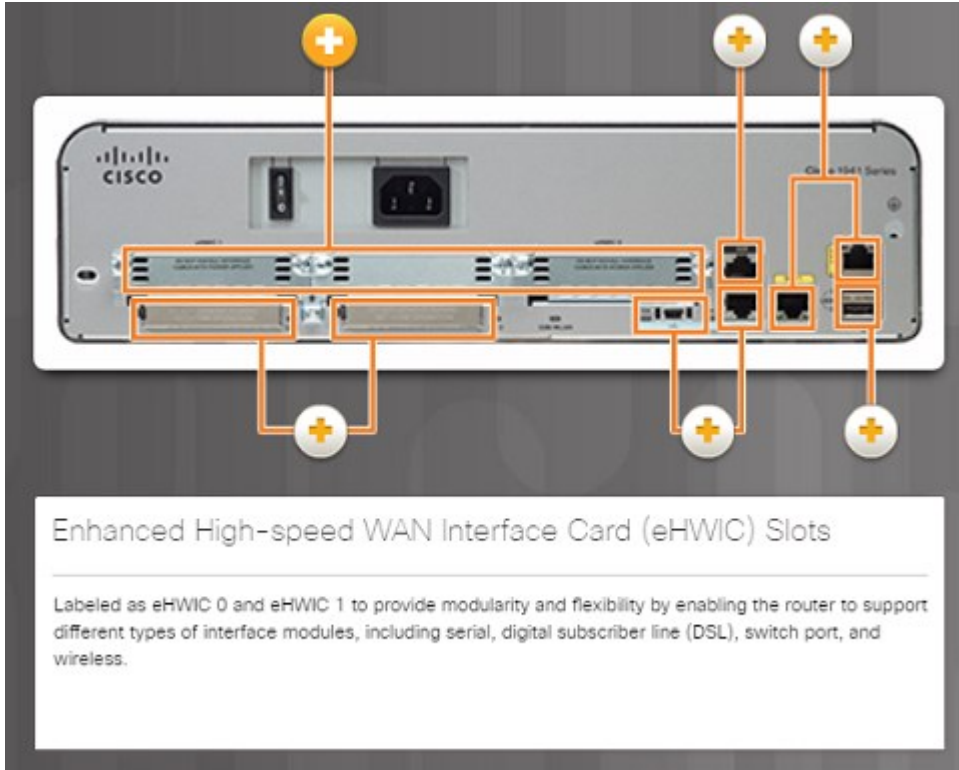
Inside a Router



- There are numerous types and models of routers, however, they all have the same general hardware components:
 - Power supply
 - Cooling fan
 - SDRAM - Synchronous Dynamic RAM
 - Non-volatile RAM (NVRAM)
 - CPU
 - Heat shields
 - Advanced Integration Module (AIM)

Anatomy of a Router

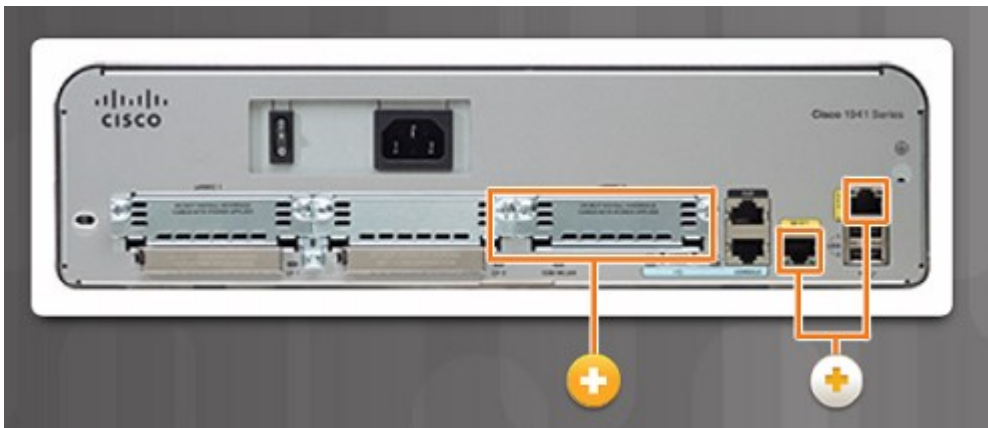
Connect to a Router



- Cisco devices, routers, and switches typically interconnect many devices. The Cisco 1941 router backplane includes the following ports and connections:
 - Enhanced High-speed WAN Interface Card (eHWIC) Slots
 - Auxiliary (AUX) – RJ-45 port for remote management.
 - Console Port – Used for initial configuration and Command Line Interface access – RJ-45 or USB Type-B (mini-B USB)
 - Gigabit Ethernet used to provide LAN access by connecting to switches, users, or to other routers.
 - Compact Flash Slots – Labeled as CF0 and CF1 and used to provide increased storage flash space upgradable to 4GB.
 - USB port – used to provide additional storage space.

LAN and WAN Interfaces

- Cisco router connections can be classified in two categories:
 - In-band router interfaces – LAN and WAN interfaces
 - Management ports – Console and AUX ports



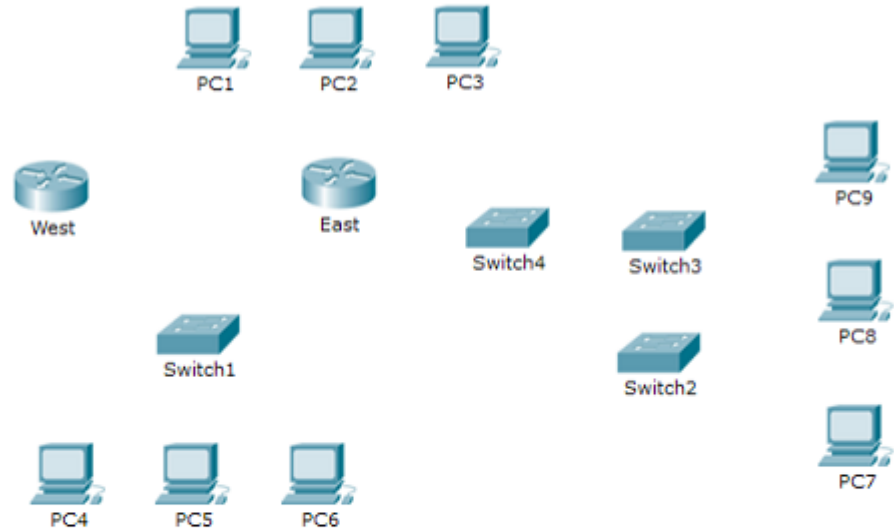
- The most common ways to access user EXEC mode in the CLI environment on a Cisco router:
 - Console – This is a physical management port that provides out-of-band access to the Cisco router. Out-of-band means that it is dedicated and does not require network services to be configured on the router.
 - Secure Shell (SSH) – This is a secure method of remotely establishing a CLI connection over a network. SSH does require active networking services configured.
 - Telnet – Telnet is an insecure method of remotely establishing a CLI session through a virtual interface over a network. The connection is not encrypted.

Anatomy of a Router

Packet Tracer – Exploring Internetworking Devices

- In this Packet Tracer activity, you will explore different options available on internetworking devices.
- You will be required to determine which options provide the necessary connectivity when connecting multiple devices.

Topology



Objectives

Part 1: Identify Physical Characteristics of Internetworking Devices

Part 2: Select Correct Modules for Connectivity

Part 3: Connect Devices

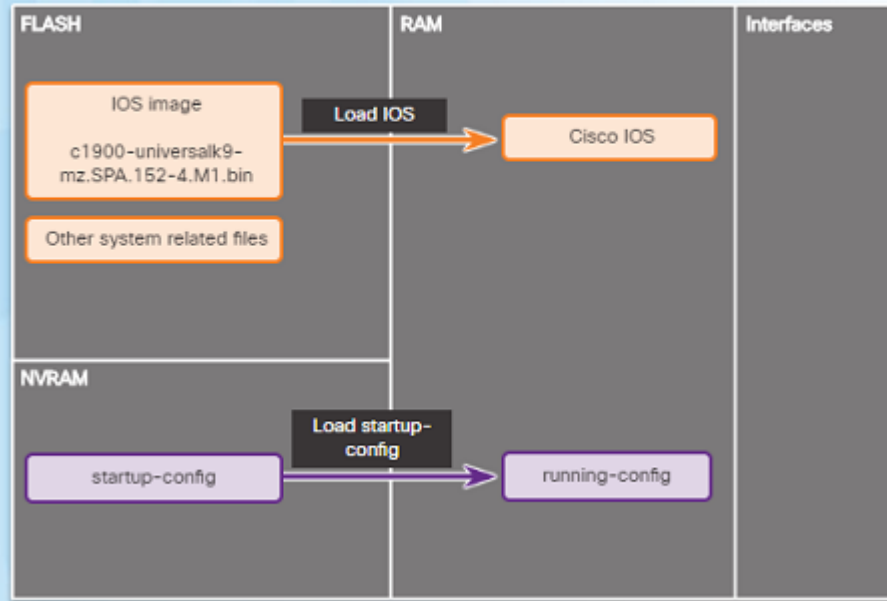
Background

In this activity, you will explore the different options available on internetworking devices. You will also be required to determine which options provide the necessary connectivity when connecting multiple devices. Finally, you will add the correct modules and connect the devices.

Router Boot-up

Bootset Files

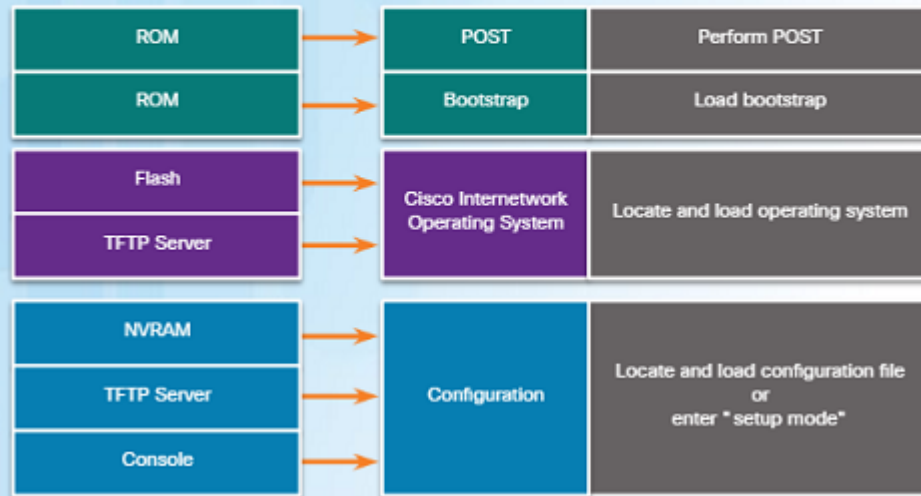
Files Copied to RAM During Bootup



- Cisco routers and switches load the IOS image and startup configuration file into RAM when they are booted.
- The running configuration is modified when the network administrator makes any changes. These changes should be saved to the startup configuration file in NVRAM in order for them to take effect on the next reboot of the router or during in the event of a power loss.

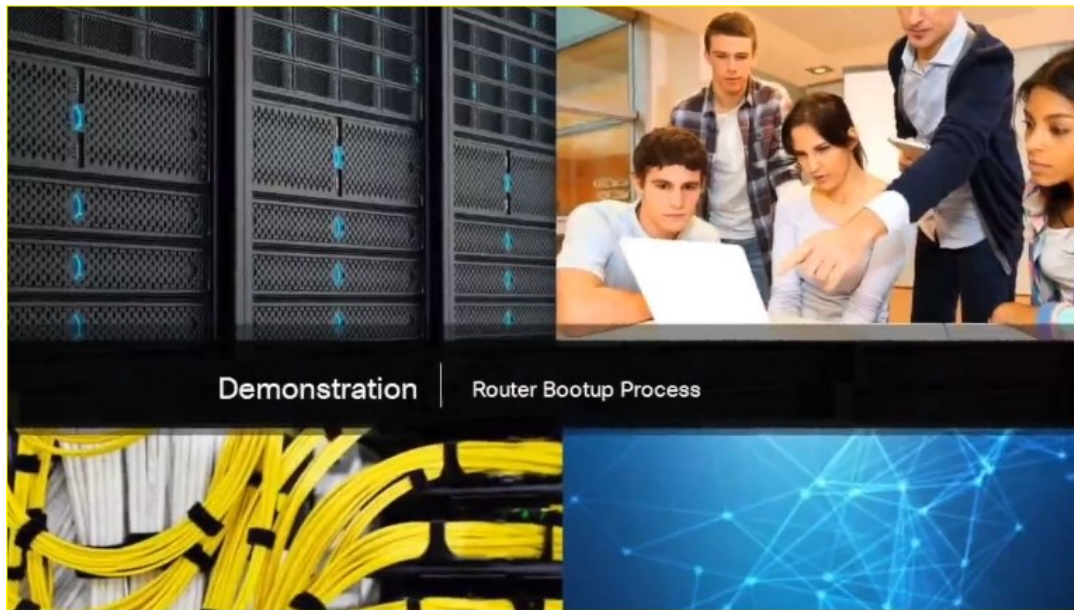
Router Bootup Process

How a Router Boots Up



- Three major phases to the bootup process of a router:
 - Perform the POST and load the bootstrap program – During the Power-on Self-Test, the router executes diagnostics from ROM on various hardware components. After the POST, the bootstrap program is copied from ROM into RAM and its job is to locate the Cisco IOS and load it into RAM.
 - Locate and load the Cisco IOS software – Typically, the IOS is stored in flash memory and is copied into RAM for execution by the CPU.
 - Locate and load the startup configuration file or enter setup mode – The bootstrap program then copies the startup config file from NVRAM into RAM and becomes the running configuration.

Video Demonstration – Router Bootup Process



- The POST checks for errors in the hardware. After the system POST, the router loads the bootstrap program from ROM.
- The purpose of the bootstrap program is to locate and load the Cisco IOS software.
- After the IOS is loaded, the router then loads the configuration file known as the startup config file which contains all of the configured settings for the router.
- If the router can't find a startup-config file, nor obtain one from a TFTP server, the router will enter initial set-up mode.

Show Version Output

```
Router# show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M),
Version 15.2(4)M1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thu 26-Jul-12 19:34 by prod_rel_team
```

```
ROM: System Bootstrap, Version 15.0(1r)M15,
RELEASE SOFTWARE (fc1)
```

```
Router uptime is 10 hours, 9 minutes
System returned to ROM by power-on
System image file is
"flash0:c1900-universalk9-mz.SPA.152-4.M1.bin"
Last reload type: Normal Reload
Last reload reason: power-on
```

```
<output omitted>
```

```
Cisco CISC01941/K9 (revision 1.0)
with 446464K/77824K bytes of memory.
Processor board ID FTX1636848Z
2 Gigabit Ethernet interfaces
2 Serial(sync/async) interfaces
1 terminal line
ROM configuration is 64 bits wide with bootfs disabled
```

- The **show version** command displays information about the version of the Cisco IOS software running on the router as well as:
- The version of the bootstrap program
- Information about the hardware configuration
- Amount of system memory

Video Demonstration – The show version Command



- This demonstration uses a Term Term terminal emulation program to connect to the console of a Cisco 1941 router for the purpose of showing the output of the **show version** command.
- What is the Cisco IOS software version that is running?
- How long has the router been up?
- What is the name of the system image file and where is it located?
 - What is the name of the distribution?
- What interfaces are on the router?

Router Boot-up

Lab – Exploring Router Physical Characteristics



Lab - Exploring Router Physical Characteristics

Topology



Objectives

Part 1: Examine Router External Characteristics

Part 2: Examine Router Internal Characteristics Using Show Commands

Background / Scenario

In this lab, you will examine the outside of the router to become familiar with its characteristics and components, such as its power switch, management ports, LAN and WAN interfaces, indicator lights, network expansion slots, memory expansion slots, and USB ports.

You will also identify the internal components and characteristics of the IOS by consoling into the router and issuing various commands, such as **show version** and **show interfaces**, from the CLI.

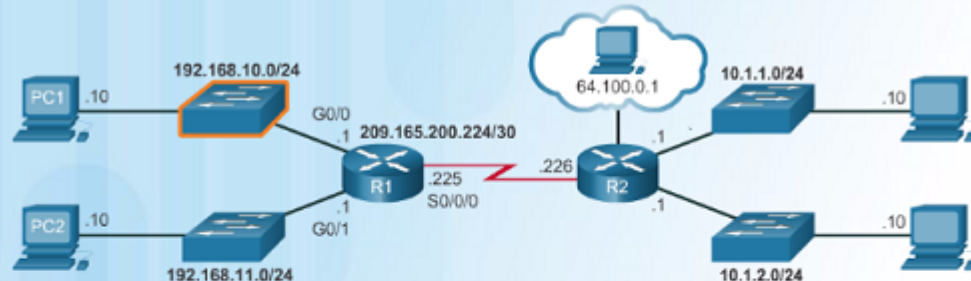
Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). Other routers and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs.

Note: Make sure that the routers have been erased and have no startup configurations. If you are unsure, contact your instructor.

6.4 Configure a Cisco Router

Basic Switch Configuration Steps

Sample Switch Configuration

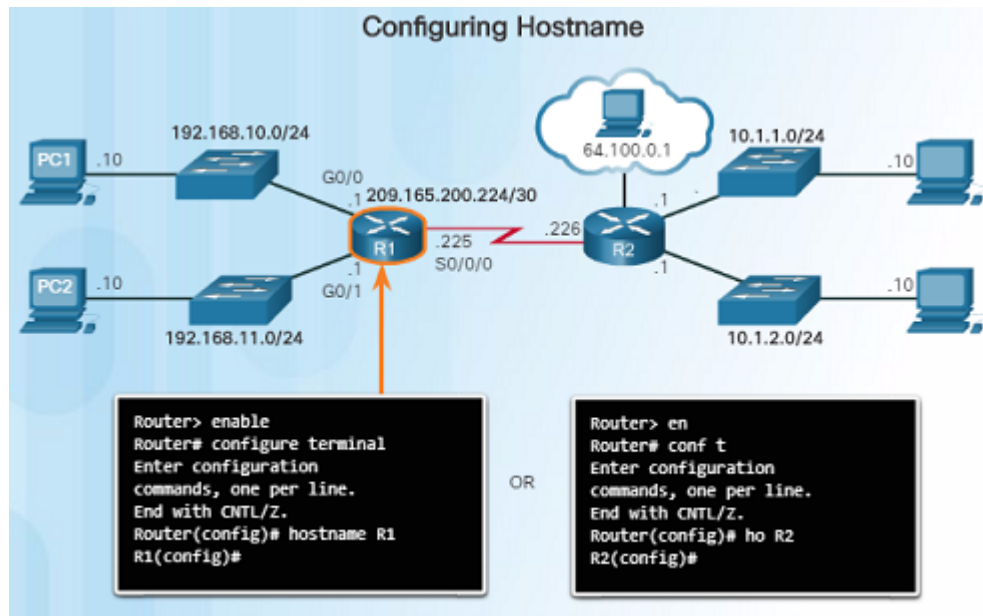


```
Switch> enable
Switch# configure terminal
Switch(config)# hostname S1
S1(config)# enable secret class
S1(config)# line console 0
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# line vty 0 15
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# exit
S1(config)# service password-encryption
S1(config)# banner motd #No unauthorized access allowed!#
S1(config)# interface vlan1
S1(config-if)# ip address 192.168.10.50 255.255.255.0
S1(config-if)# no shutdown
```

- Cisco routers and switches have many similarities in regards to their configuration:
- Support a similar operating system.
- Support similar command structure.
- Support many of the same commands.
- They also have identical initial configuration steps when implemented in a network.
- The commands on the left display a sample configuration of a switch.

Configure Initial Settings

Basic Router Configuration Steps



- Similar to the configuration of a switch on the previous slide, the initial configuration should include:
 - Configure the router's device name
 - Secure the user EXEC mode
 - Secure remote Telnet and SSH access
 - Secure privileged EXEC mode
 - Secure all passwords in the config file
 - Provide legal notification – Authorized access only
- Save the configuration

Packet Tracer – Configure Initial Router Settings



Cisco Networking Academy®

Mind Wide Open™

Packet Tracer - Configure Initial Router Settings

Topology



PCA



R1

Objectives

Part 1: Verify the Default Router Configuration

Part 2: Configure and Verify the Initial Router Configuration

Part 3: Save the Running Configuration File

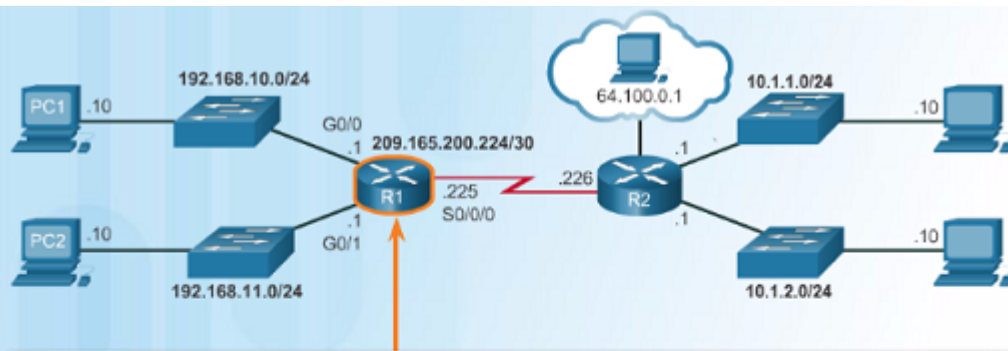
Background

In this activity, you will perform basic router configurations. You will secure access to the CLI and console port using encrypted and plain text passwords. You will also configure messages for users logging into the router. These banners also warn unauthorized users that access is prohibited. Finally, you will verify and save your

- This Packet Tracer activity will allow you to perform basic initial router configurations.

Configure Interfaces

Configure Router Interfaces

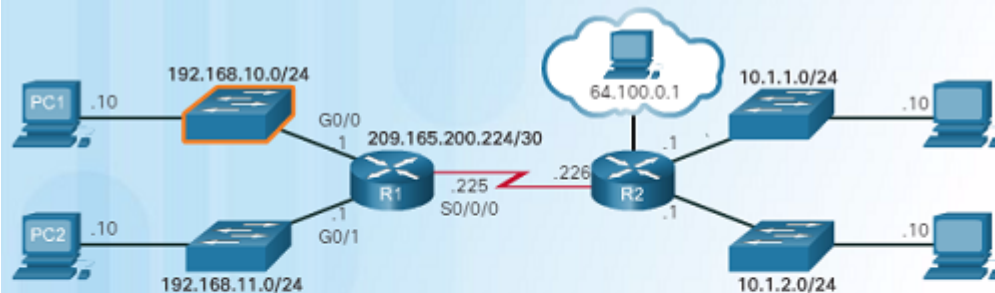


```
R1# conf t
Enter configuration commands, one per line.
End with CNTL/Z.
R1(config)#
R1(config)# interface gigabitethernet 0/0
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# description Link to LAN-10
R1(config-if)# no shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/0,
changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0,changed state to up
R1(config-if)#exit
R1(config)#
R1(config)#int g0/1
R1(config-if)#ip add 192 168 11 1 255 255 255 0
```

- For routers to be reachable by other devices in the network, the in-band interfaces must be configured. For example, a Cisco 1941 router has four in-band interfaces:
- Two Gigabit Ethernet Interfaces – G0/0 and G0/1
- One serial WAN Interface card with two interfaces – S 0/0/0 and S0/0/1
- The commands in the figure to the left provide an example of how to configure a router's interface to provide network connectivity.
- It is important that you use the command **no shutdown** when you are ready to make the interface active.

Verify Interface Configuration

The show ip interface brief Command Output



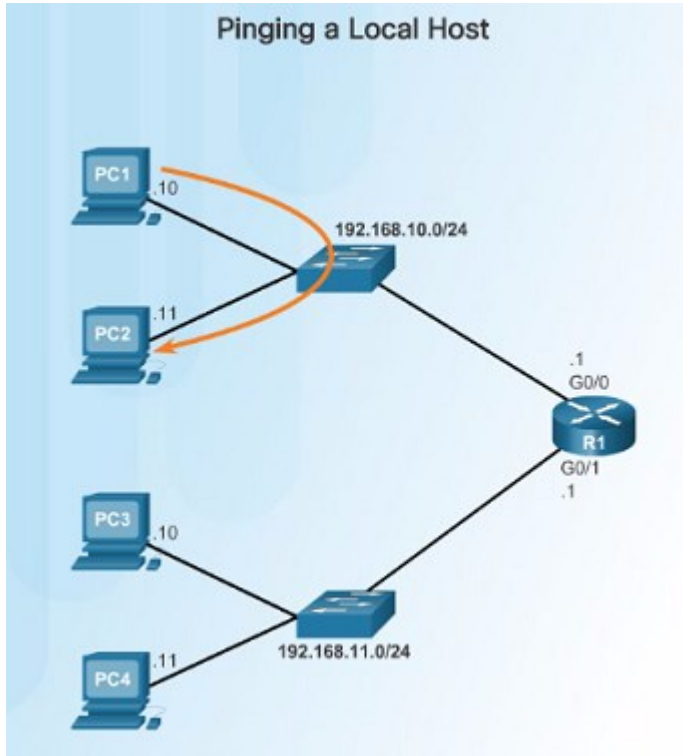
```
R1# show ip interface brief
Interface      IP-Address      OK? Method Status      Protocol
GigabitEthernet0/0 192.168.10.1    YES manual up          up
GigabitEthernet0/1 192.168.11.1    YES manual up          up
Serial0/0/0       209.165.200.225 YES manual up          up
Serial0/0/1       unassigned      YES NVRAM administratively down down
Vlan1             unassigned      YES NVRAM administratively down down
R1#
R1# ping 209.165.200.226

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.226,
timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5),
```

- After configuring an interface, or for troubleshooting purposes, there are several commands that can be used:
- **show ip interface brief** – Provides you a summarized view of all interfaces to verify if they are activated and operational. Look for Status of “up” and Protocol of “up”.
- **show ip route** – Displays the contents of the IPv4 routing table stored in RAM.
- **show interfaces** – Displays the IPv4 statistics for all interfaces on a router.
- Remember to save your configuration changes with the **copy running-config startup-config** command.

Configure the Default Gateway

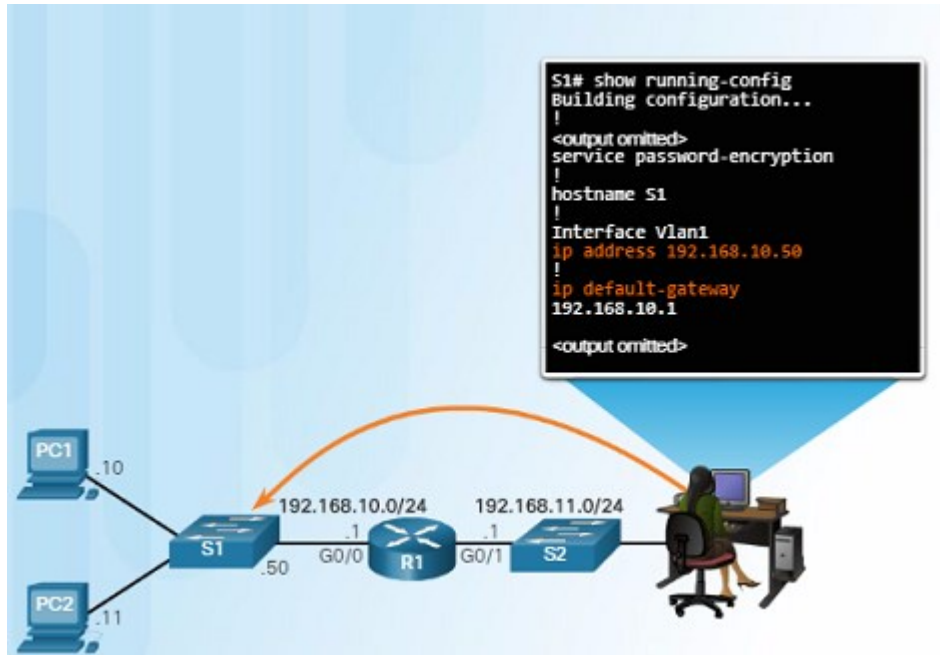
Default Gateway for a Host



- For an end device or a host to communicate over the network, it must be configured with the correct IP address information including the default gateway address.
- The default gateway is only used when the host wants to send a packet to a device on another network – if the device is on the same network, it can send it directly to that device.
- If PC1 needs to send a packet to PC3 which is on a different network, it must send it to the default gateway address of 192.168.10.1 on router R1's G0/0 interface.

Configure the Default Gateway

Default Gateway for a Switch



- Normally, a Layer 2 device, such as a switch, does not require an IP address to function.
- An IP address, subnet mask, and default gateway address are required in order to connect to it remotely (via SSH or Telnet) for configuration or administrative purposes.
- Use the command **ip default-gateway** global configuration command to configure the default gateway on a switch.
- It is important to note that a switch does not use the default gateway address to forward packets to from hosts on its local network to remote networks.

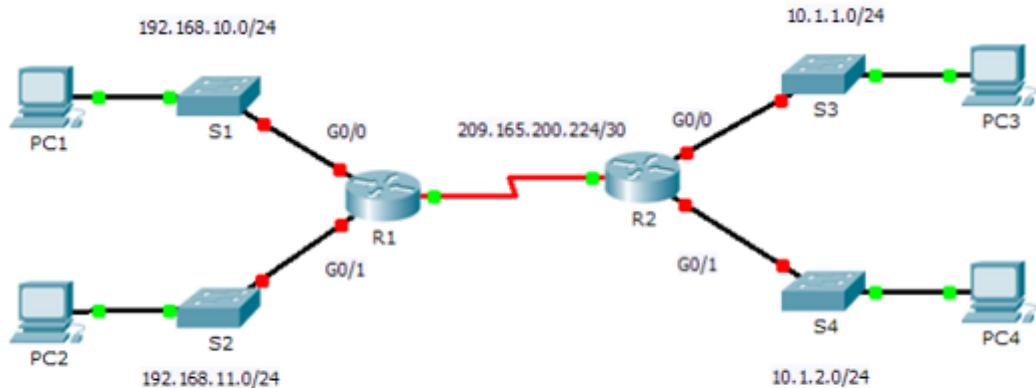
Configure the Default Gateway

Packet Tracer – Connect a Router to a LAN

- In this Packet Tracer activity, you will use various show commands to view the state of various parts of the router.
- You will also configure the router's Ethernet interfaces using IP addresses that will be provided.

Packet Tracer - Connect a Router to a LAN

Topology



Background

In this activity, you will use various **show** commands to display the current state of the router. You will then use the Addressing Table to configure router Ethernet interfaces. Finally, you will use commands to verify and test your configurations.

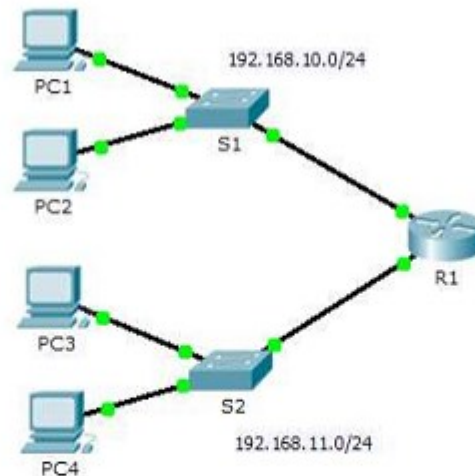
Note: The routers in this activity are partially configured. Some of the configurations are not covered in this course, but are provided to assist you in using verification commands.

Packet Tracer – Troubleshooting Default Gateway Issues

- In this Packet Tracer activity, you will continue to document the network and then verify the documentation by testing end-to-end connectivity.
- You will also have a chance to troubleshoot any connectivity issues using the following steps:
 - Verify the network documentation and use tests to isolate problems.
 - Determine an appropriate solution for a given problem.
 - Implement the solution.
 - Test to verify the problem is resolved.
 - Document the solution.

Packet Tracer - Troubleshooting Default Gateway Issues

Topology



Background

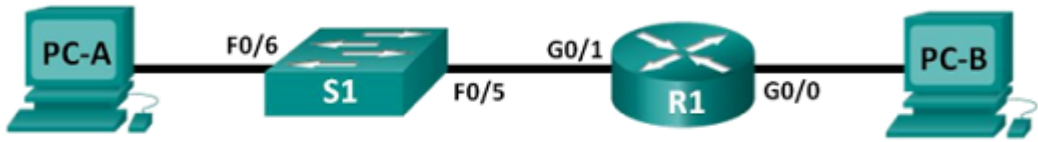
For a device to communicate across multiple networks, it must be configured with an IP address, subnet mask, and a default gateway. The default gateway is used when the host wants to send a packet to a device on another network. The default gateway address is generally the router interface address attached to the local network to which the host is connected. In this activity, you will finish documenting the network. You will then verify the network documentation by testing end-to-end connectivity and troubleshooting issues. The troubleshooting method you will use consists of the following steps:

6.5 Summary

Lab – Building a Switch and Router Network

Lab - Building a Switch and Router Network

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.0.1	255.255.255.0	N/A
	G0/1	192.168.1.1	255.255.255.0	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.0.3	255.255.255.0	192.168.0.1

Objectives

- Part 1: Set Up the Topology and Initialize Devices
- Part 2: Configure Devices and Verify Connectivity
- Part 3: Display Device Information

Packet Tracer – Skills Integration Challenge

- In this Packet Tracer activity, you will have a chance to impress your manager with your ability to configure a router and a switch connecting two LANs.
- You will verify your results by testing end-to-end connectivity and troubleshoot as necessary.

Packet Tracer - Skills Integration Challenge

Topology

You will receive one of three possible topologies.

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
	G0/0		255.255.255.0	N/A
	G0/1		255.255.255.0	N/A
	VLAN 1		255.255.255.0	
	VLAN 1		255.255.255.0	
	NIC		255.255.255.0	
	NIC		255.255.255.0	
	NIC		255.255.255.0	
	NIC		255.255.255.0	

Objectives

- Finish the network documentation.
- Perform basic device configurations on a router and a switch.
- Verify connectivity and troubleshoot any issues.

