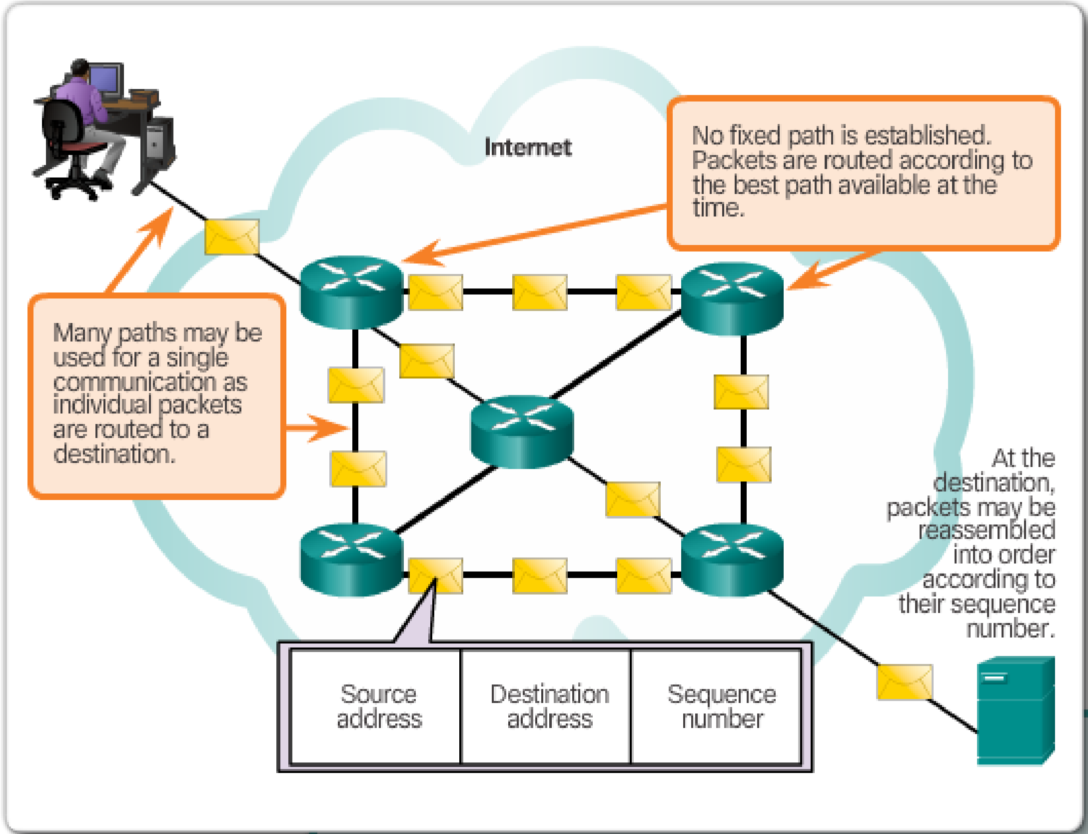
6.0.1.1 Chapter 6: Network Layer

Chapter 6: Network Layer

Network applications and services on one end device can communicate with applications and services running on another end device. How is this data communicated across the network in an efficient way?

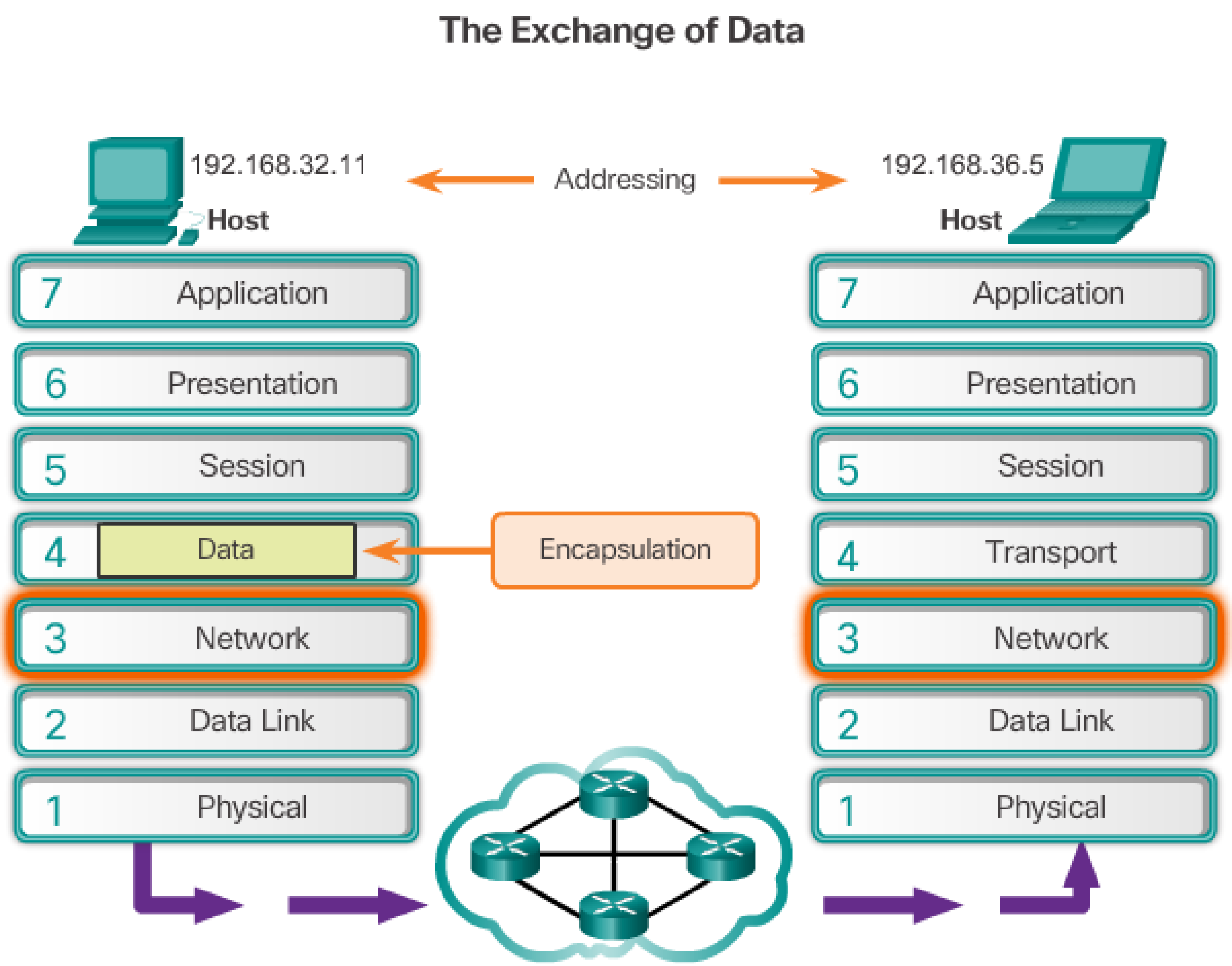
6.0.1.2 Class Activity - The Road Less Traveled...



The Network Layer uses four basic processes...

- Addressing end devices
- Encapsulation
- Routing
- De-encapsulation

6.1.1.1 The Network Layer

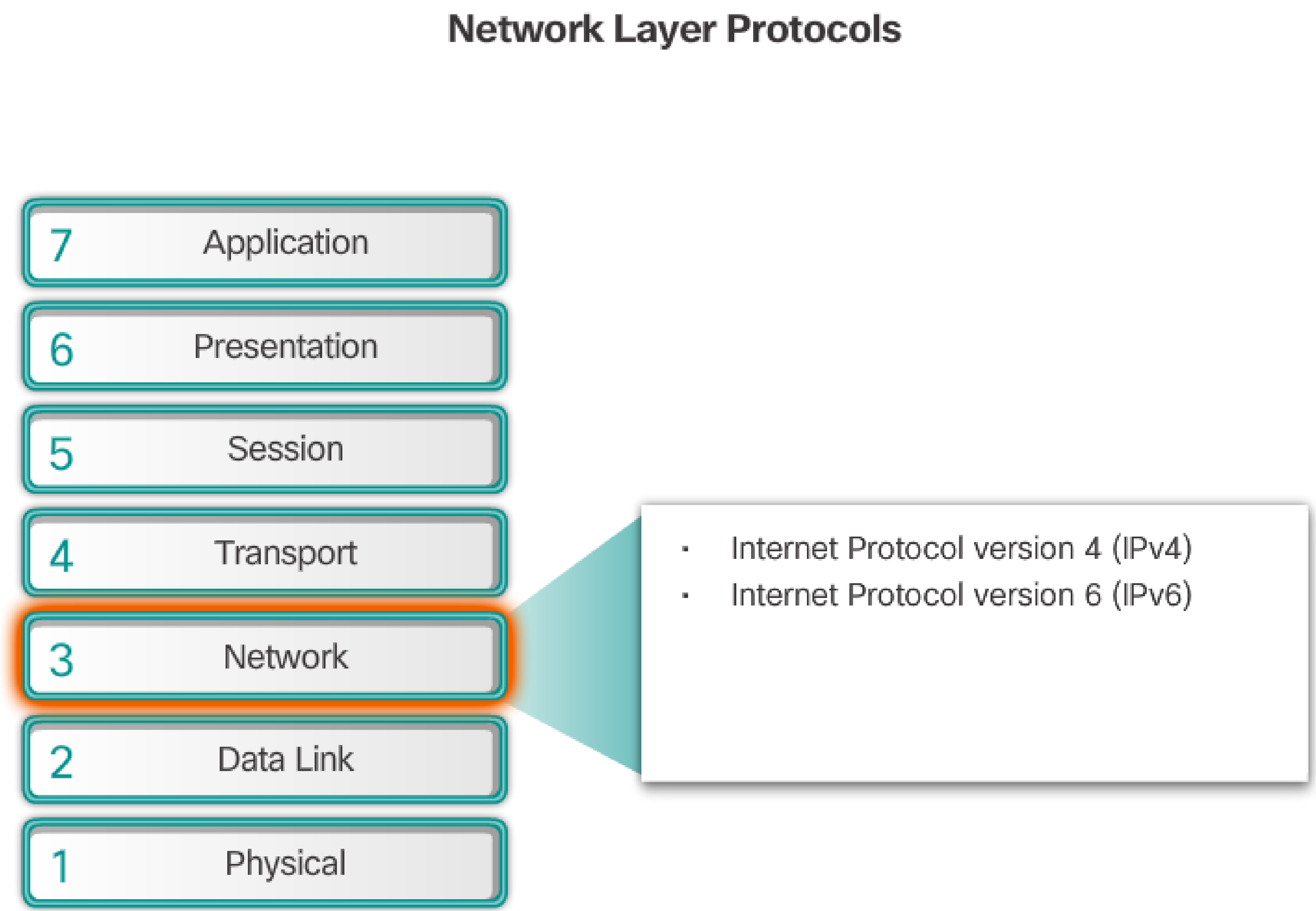


Network layer protocols forward transport layer PDUs between hosts.

The network layer, or OSI Layer 3, provides services to allow end devices to exchange data across the network. To accomplish this end-to-end transport, the network layer uses four basic processes:

1. **Addressing end devices** -
2. **Encapsulation**
3. **Routing**
4. **De-encapsulation**

6.1.1.2 Network Layer Protocols

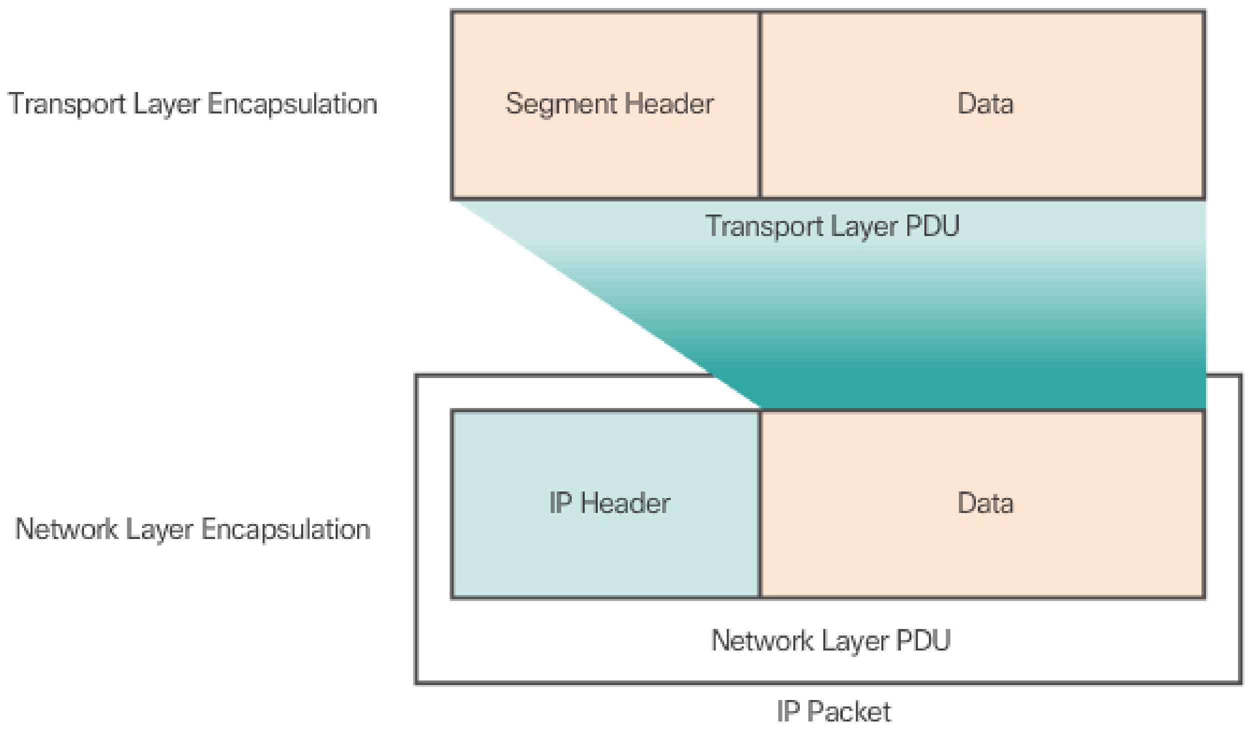


There are several network layer protocols in existence. However, only the following two are commonly implemented:

- Internet Protocol version 4 (IPv4)
- Internet Protocol version 6 (IPv6)

6.1.2.1 Encapsulating IP

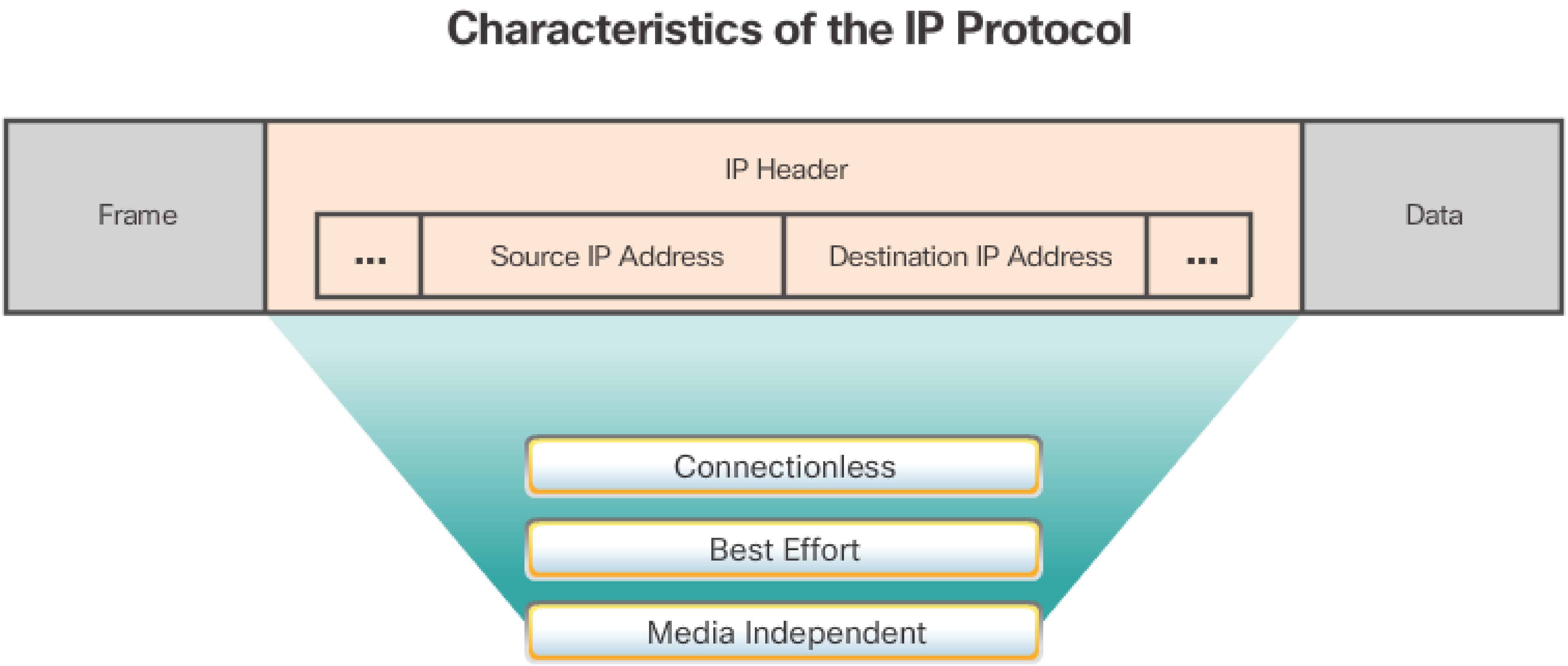
Network Layer PDU = IP Packet



The network layer adds a header so packets can be routed through complex networks and reach their destination. In TCP/IP based networks, the network layer PDU is the IP Packet.

IP encapsulates the transport layer segment by adding an IP header. This header is used to deliver the packet to the destination host. The IP header remains in place from the time the packet leaves the source host until it arrives at the destination host.

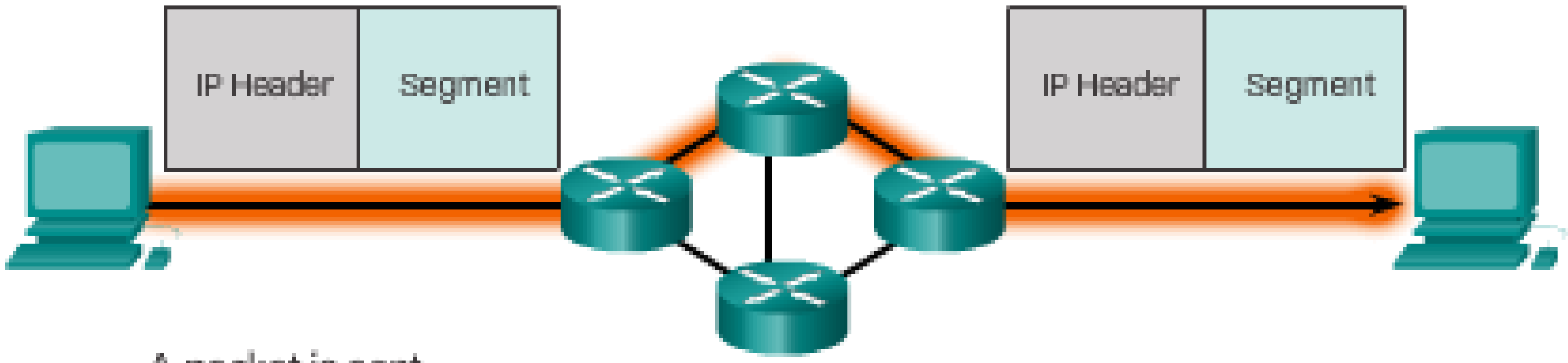
6.1.2.2 Characteristics of IP



IP was designed as a protocol with low overhead. It provides only the functions that are necessary to deliver a packet from a source to a destination over an interconnected system of networks.

6.1.2.3 IP - Connectionless

Connectionless Communication



A packet is sent.

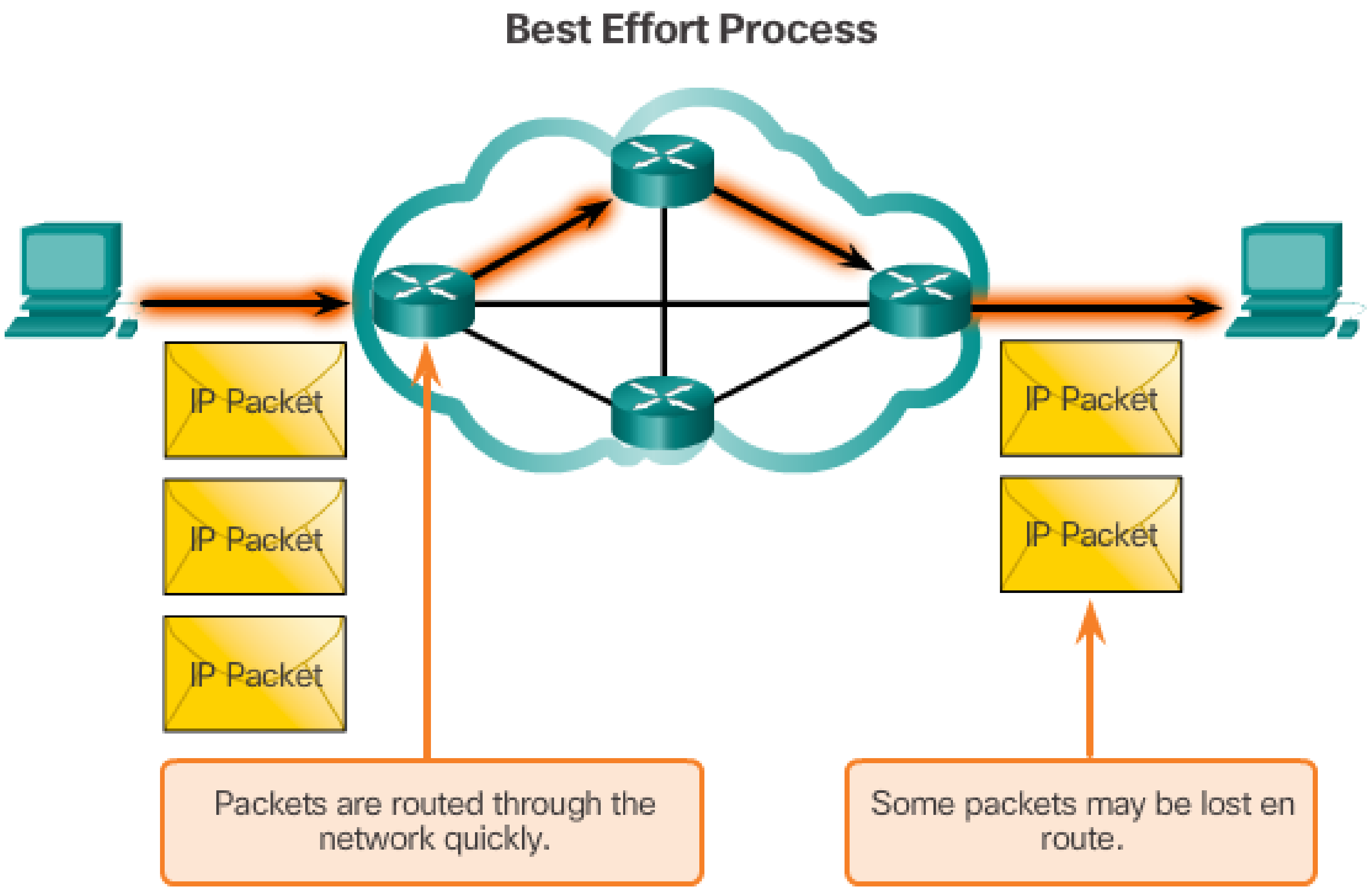
The sender doesn't know:

- If the receiver is present
- If the packet arrived
- If the receiver can read the packet

The receiver doesn't know:

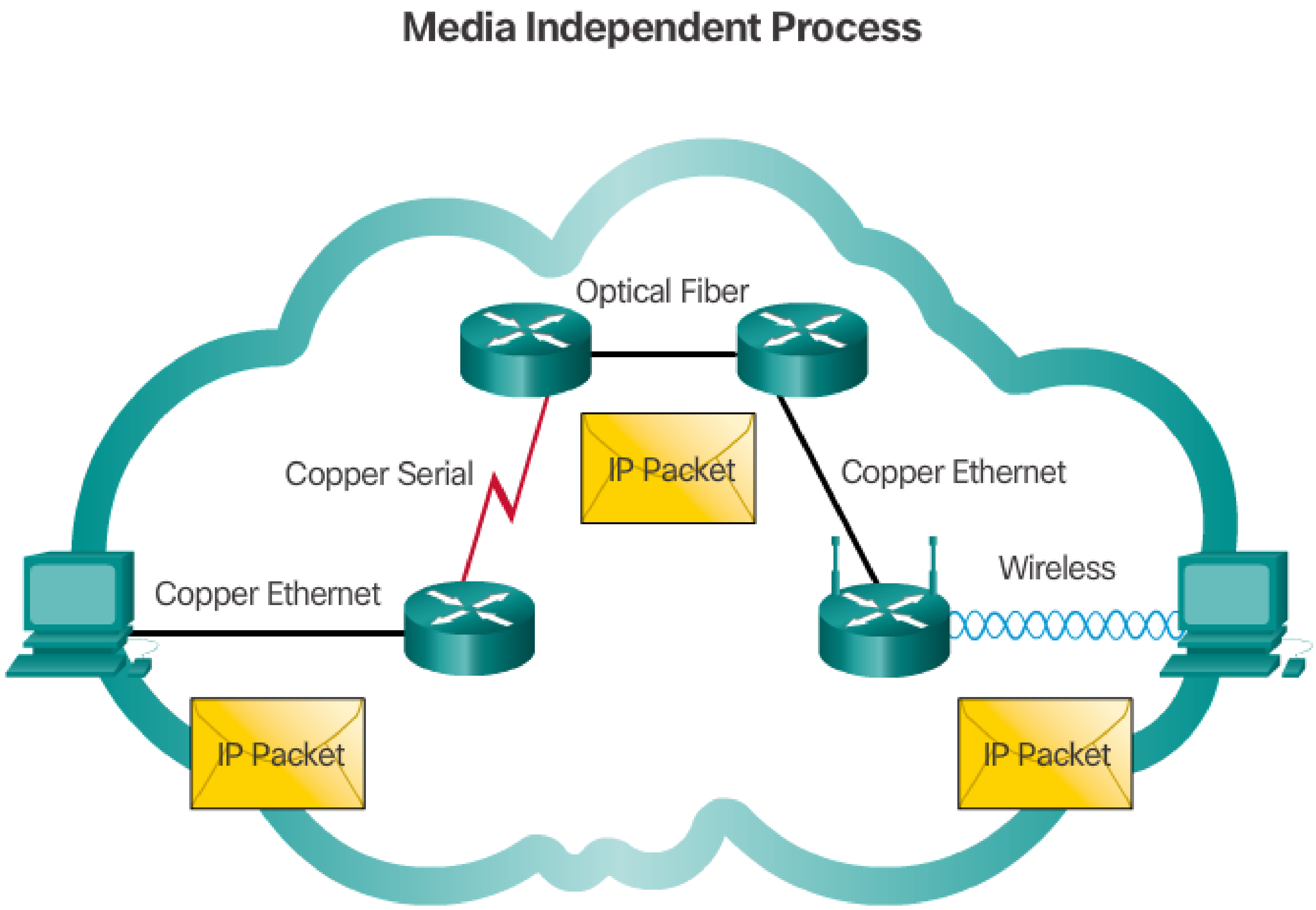
- When it is coming

6.1.2.4 IP - Best Effort Delivery



As an unreliable network layer protocol, IP does not guarantee that all sent packets will be received. Other protocols manage the process of tracking packets and ensuring their delivery.

6.1.2.5 IP - Media Independent



IP packets can travel over different media.

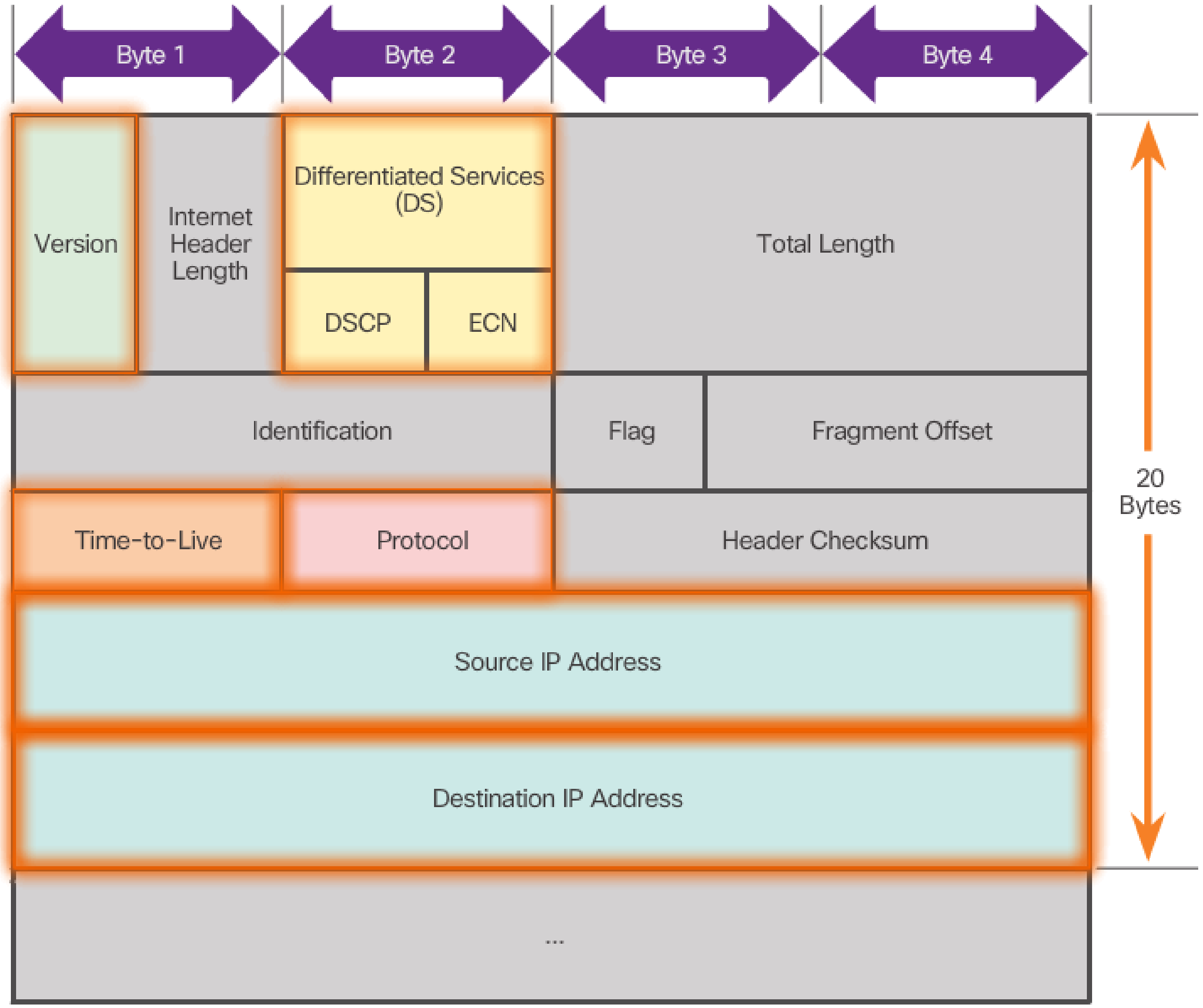
There is, however, one major characteristic of the media that the network layer considers: the maximum size of the PDU that each medium can transport. This characteristic is referred to as the maximum transmission unit (MTU). Part of the control communication between the data link layer and the network layer is the establishment of a maximum size for the packet. The data link layer passes the MTU value up to the network layer. The network layer then determines how large packets can be.

6.1.2.6 Activity - IP Characteristics

Delivery Method

Connectionless	Best Effort	Media Independent
No contact is made with the destination host before sending a packet. Will send a packet even if the destination host is not able to receive it.	Packet delivery is not guaranteed. Does not guarantee that the packet will be delivered fully without errors.	Fiber optics cabling, satellites, and wireless can all be used to route the same packet. Will adjust the size of the packet sent depending on what type of network access will be used.

6.1.3.1 IPv4 Packet Header



Version - identifies this as an IP version 4 packet.

Differentiated Services (DS) - Formerly called the Type of Service (ToS) field, the DS field is an 8-bit field used to determine the priority of each packet.

Time-to-Live (TTL) - Contains an 8-bit binary value that is used to limit the lifetime of a packet.

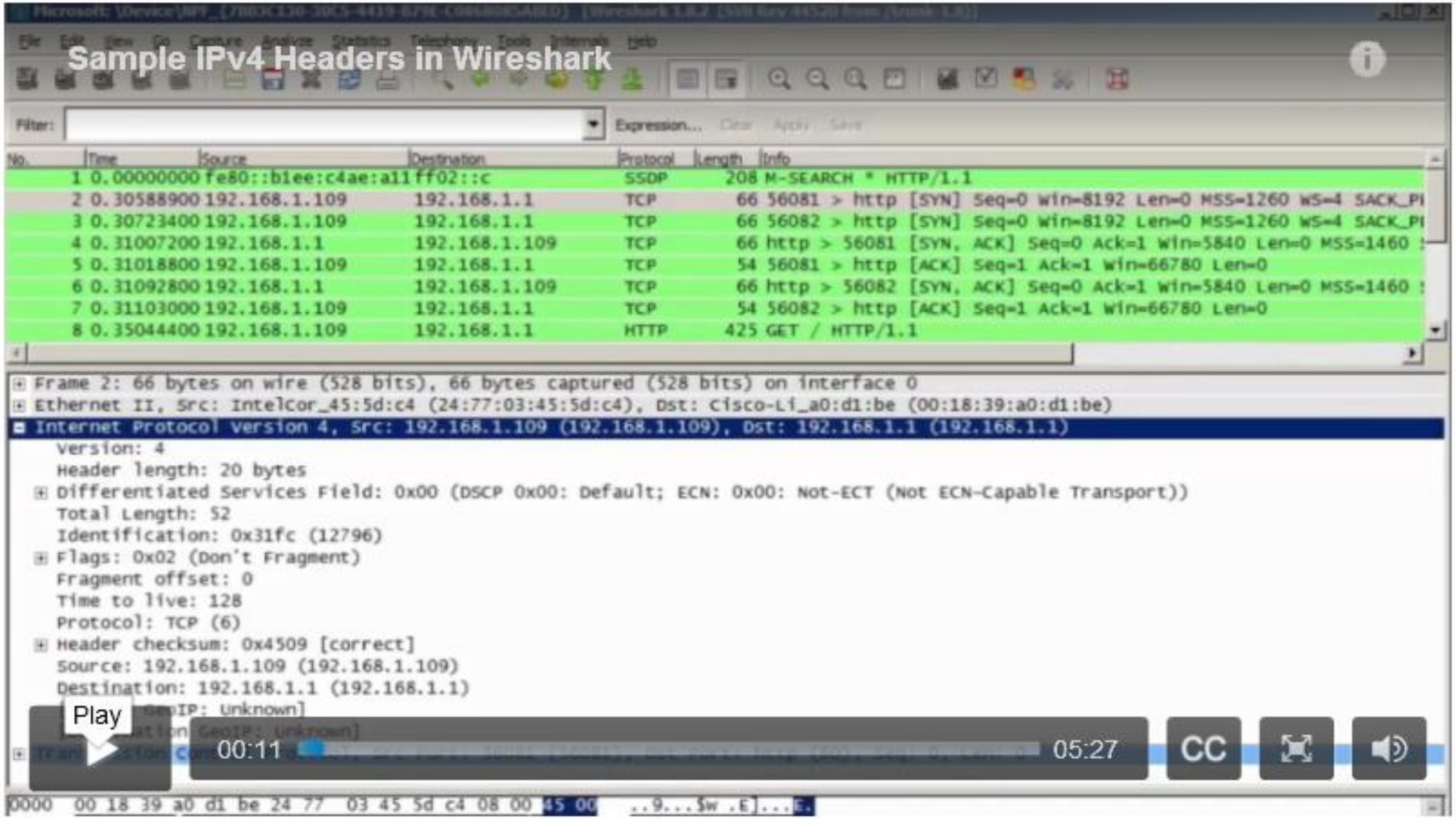
Protocol - This 8-bit binary value indicates the data payload type that the packet is carrying, which enables the network layer to pass the data to the appropriate upper-layer protocol.

Source IP Address - Contains a 32-bit binary value that represents the source IP address

Destination IP Address - Contains a 32-bit binary value that represents the destination IP address

6.1.3.2 Video Demonstration - Sample IPv4 Headers in Wireshark

Sample IPv4 Headers in Wireshark



6.1.3.3 Activity - IPv4 Header Fields

IPv4 Header Fields

Version Always set to 0100 for IPv4	**Differentiated Services** Identifies the priority of each packet
Time-to-Live Commonly referred to as hop count	**Protocol** Identifies the upper-layer protocol to be used next
Source IP Address Identifies the IP address of the sending host	**Destination IP Address** Identifies the IP address of the recipient host

6.1.4.1 Limitations of IPv4

1. **IP address depletion -**
2. **Internet routing table expansion -** A routing table is used by routers to make best path determinations. As the number of servers connected to the Internet increases, so too does the number of network routes.
3. **Lack of end-to-end connectivity -** Network Address Translation (NAT) is a technology commonly implemented within IPv4 networks. NAT provides a way for multiple devices to share a single public IPv4 address. However, because the public IPv4 address is shared, the IPv4 address of an internal network host is hidden. This can be problematic for technologies that require end-to-end connectivity.

6.1.4.2 Introducing IPv6

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

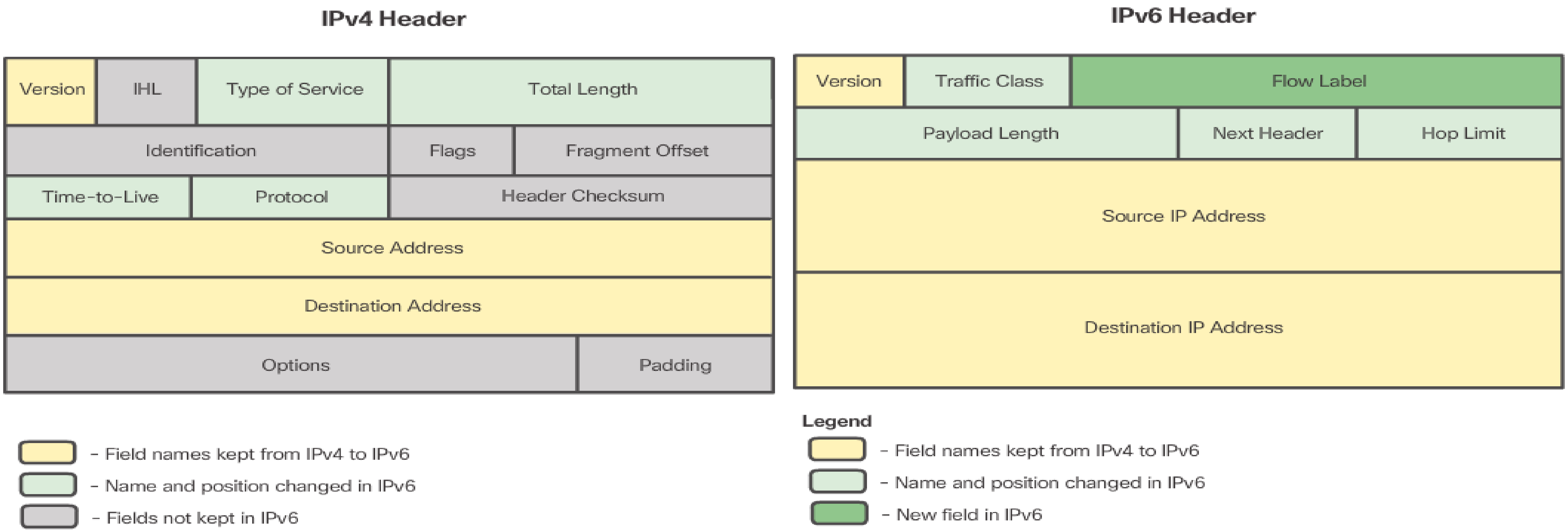
Improvements that IPv6 provides include:

Increased address space - IPv6 addresses are based on 128-bit hierarchical addressing as opposed to IPv4 with 32 bits.

Improved packet handling - The IPv6 header has been simplified with fewer fields.

Eliminates the need for NAT - With such a large number of public IPv6 addresses, NAT between a private IPv4 address and a public IPv4 is not needed

6.1.4.3 Encapsulating IPv6



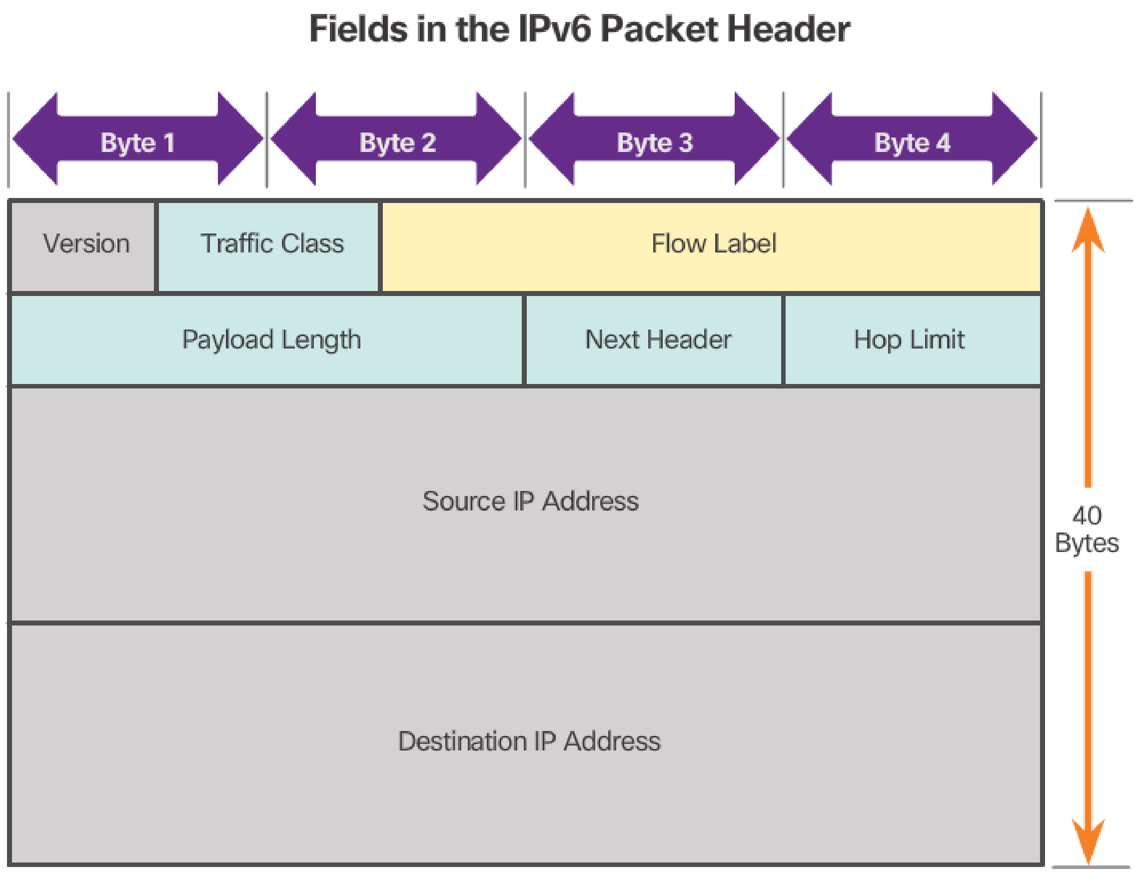
6.1.4.3 Encapsulating IPv6

IPv6 Advantages

IPv6 Advantages include:

- Simplified header format for efficient packet handling
- Larger payload for increased throughput and transport efficiency
- Hierarchical network architecture for routing efficiency
- Autoconfiguration for addresses
- Elimination of need for network address translation (NAT) between private and public addresses

6.1.4.4 IPv6 Packet Header



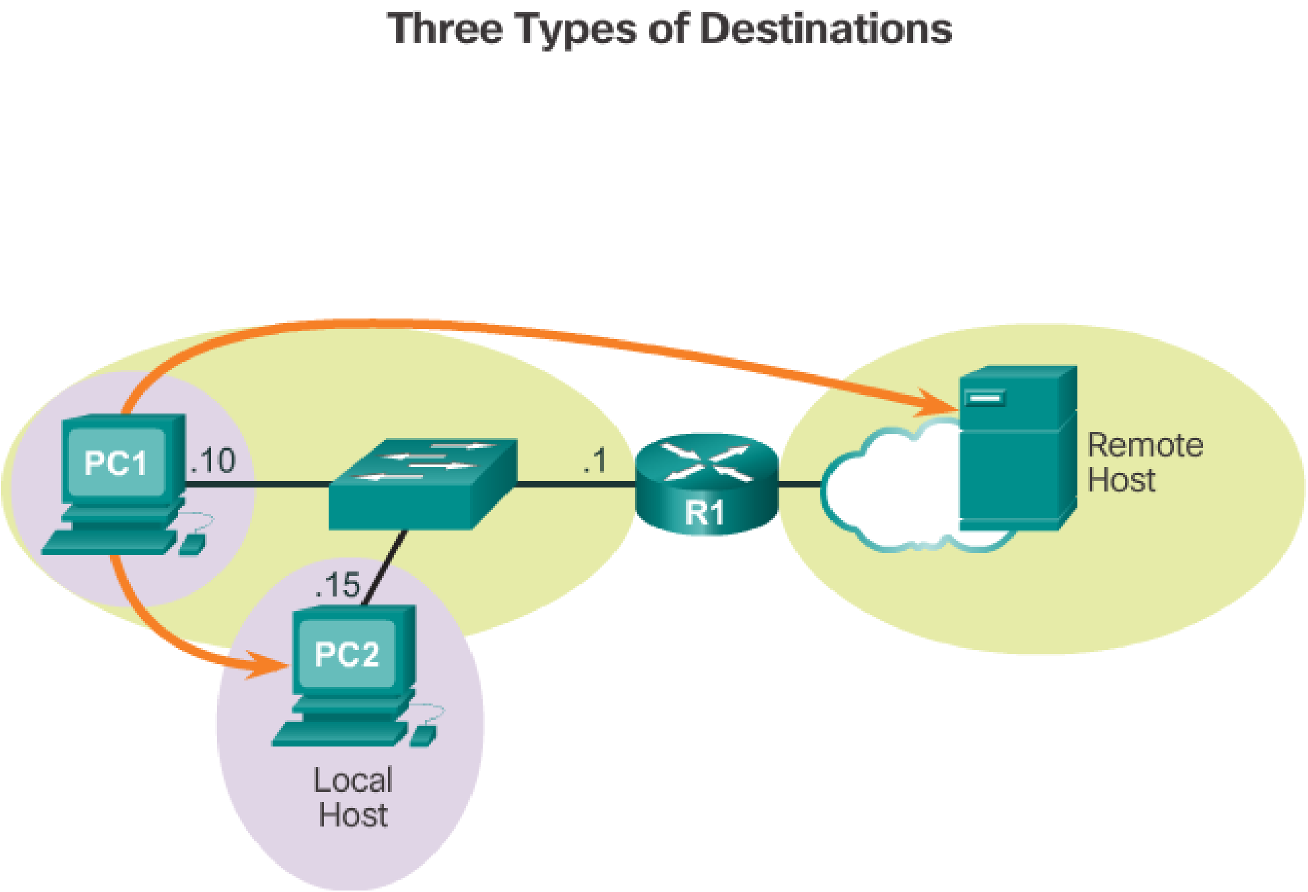
Version - identifies this as an IP version 6 packet.
Traffic Class - to the IPv4 Differentiated Services (DS) field.
Flow Label - packets with the same flow label receive the same type of handling by routers.
Payload Length - indicates the length of the data portion or payload.
Next Header - indicates the data payload type that the packet is carrying, enabling the network layer to pass the data to the appropriate upper-layer protocol.
Hop Limit - replaces the IPv4 TTL field. This value is decremented by a value of 1 by each router that forwards the packet.
Source Address - This 128-bit field identifies the IPv6 address of the sending host.
Destination Address - This 128-bit field identifies the IPv6 address of the receiving host.

6.1.4.5 Video Demonstration - Sample IPv6 Headers and Wireshark

6.1.4.6 Activity - IPv6 Header Fields

IPv6 Header Fields

Version Is always set to 0110	**Payload Length** Identifies the size of the data portion of the packet
Traffic Class Classifies packets for congestion control	**Next Header** Identifies the application type to the upper-layer protocol
Flow Label To suggest that all packets receive the same type of handling by IPv6 routers	**Hop Limit** When this value reaches 0, the sender is notified that the packet was not delivered



Itself - A host can ping itself by sending a packet to a special IPv4 address of 127.0.0.1, which is referred to as the loopback interface. Pinging the loopback interface tests the TCP/IP protocol stack on the host.

Local host - This is a host on the same local network as the sending host. The hosts share the same network address.

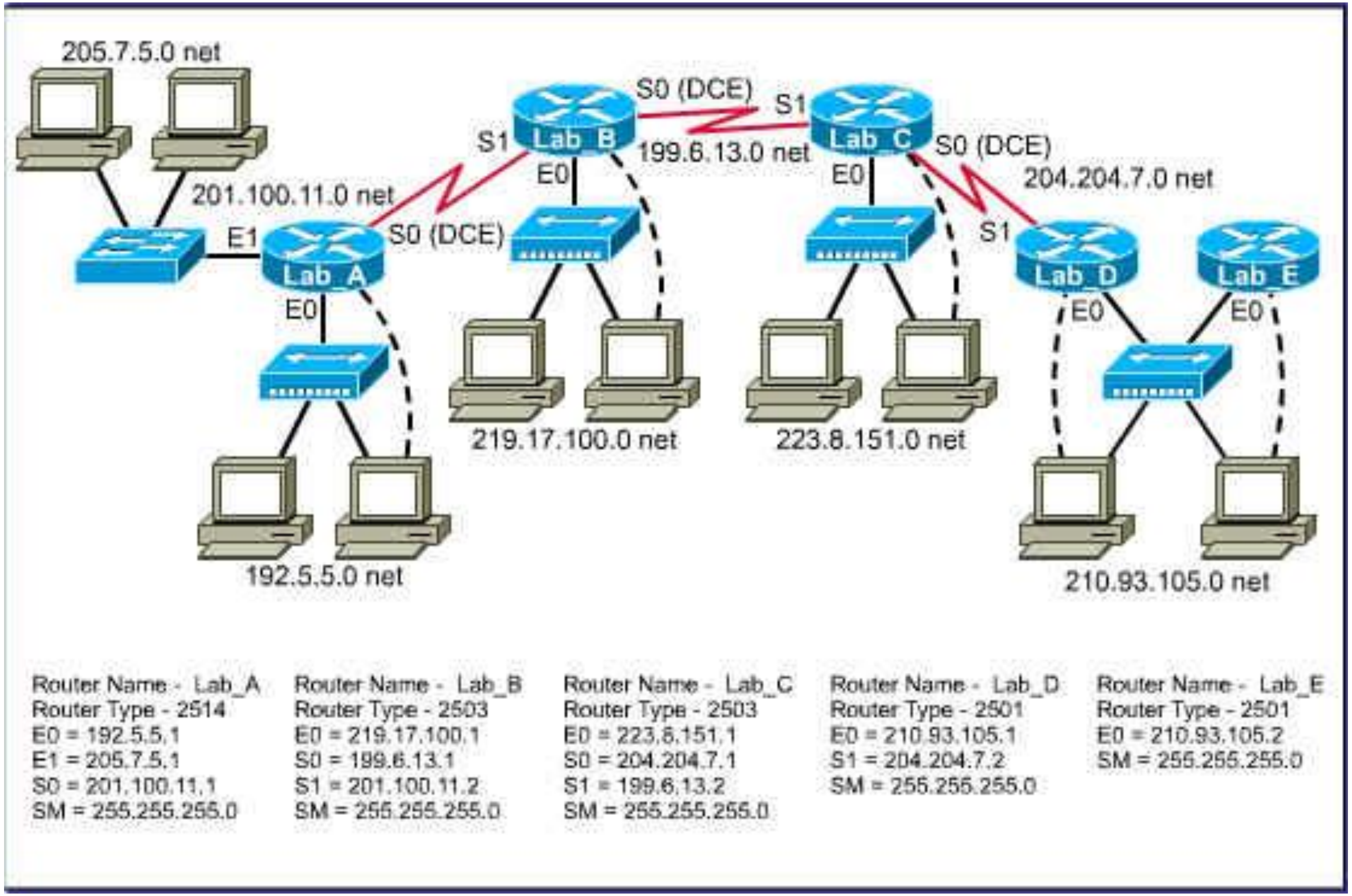
Remote host - This is a host on a remote network. The hosts do not share the same network address.

6.2.1.2 Default Gateway

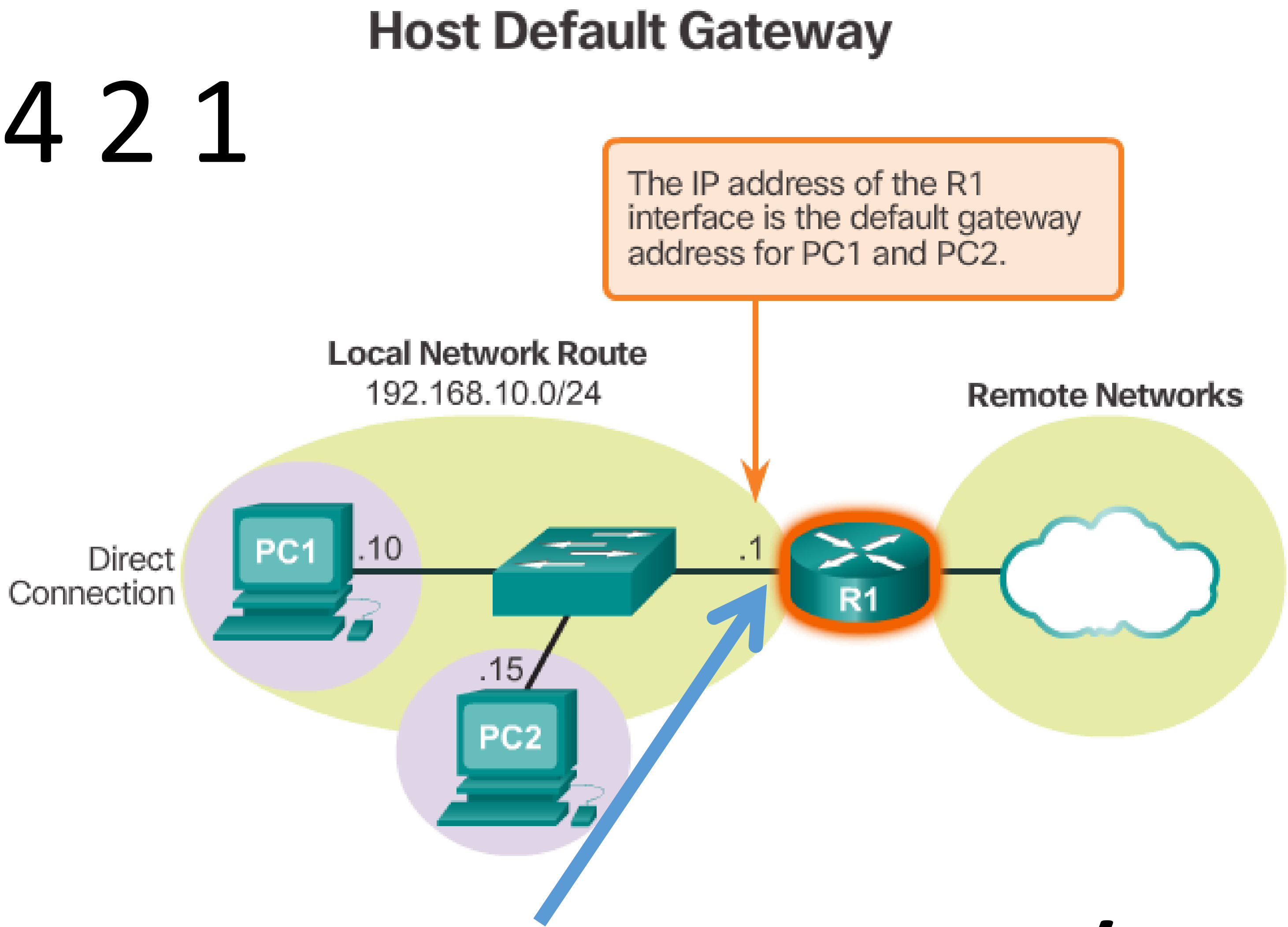
Default Gateway Functions

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



128 64 32 16 8 4 2 1



11000000.10101000.00001010.00000001/24

6.2.1.4 Host Routing Tables

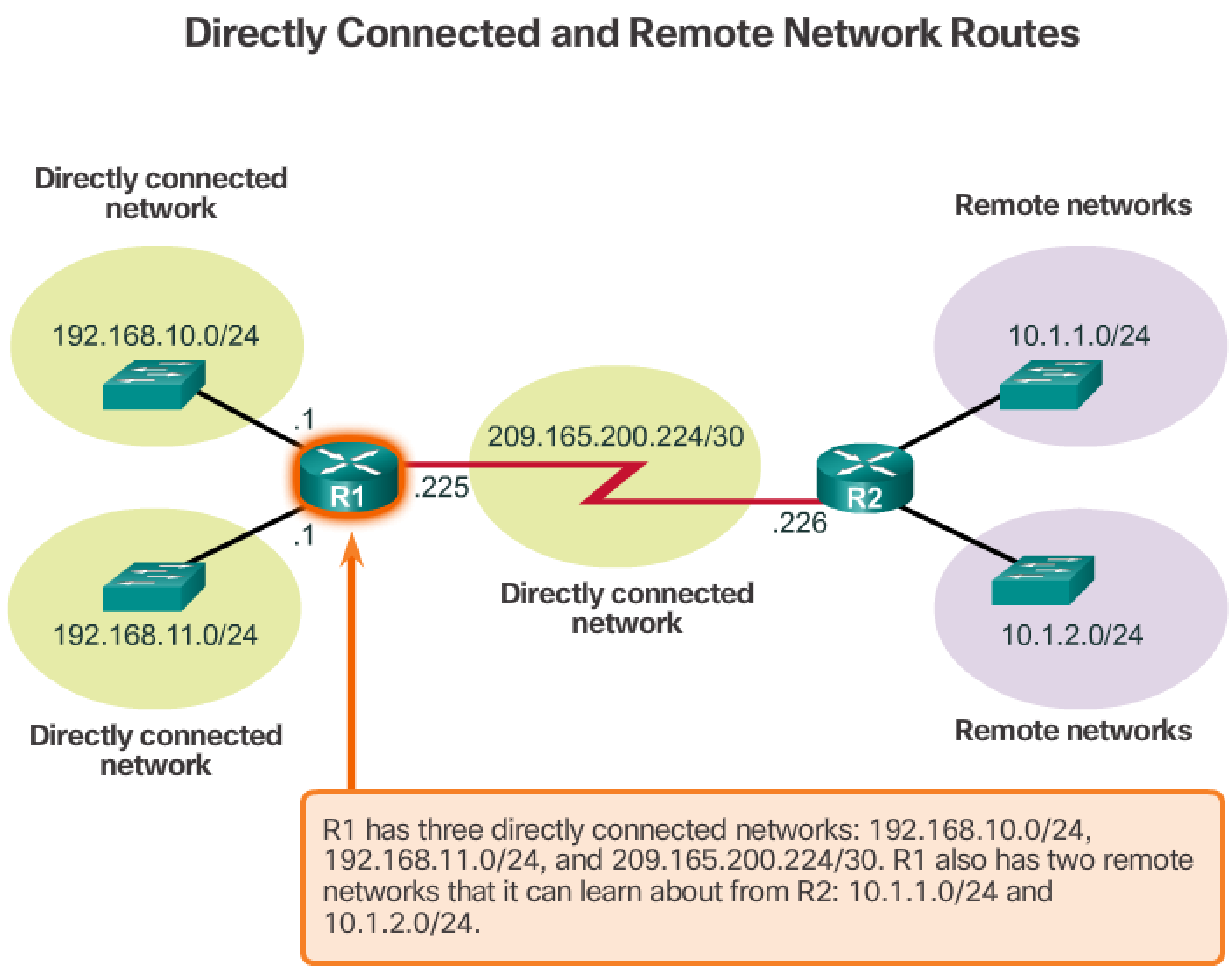
IPv4 Routing Table for PC1


```
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>
```

Entering the **netstat -r** command or the equivalent **route print** command, displays three sections related to the current TCP/IP network connections:

- **Interface List -** Lists the Media Access Control (MAC) address and assigned interface number of every network-capable interface on the host, including Ethernet, Wi-Fi, and Bluetooth adapters.
- **IPv4 Route Table -** Lists all known IPv4 routes, including direct connections, local network, and local default routes.
- **IPv6 Route Table -** Lists all known IPv6 routes, including direct connections, local network, and local default routes.

6.2.2.1 Router Packet Forwarding Decision

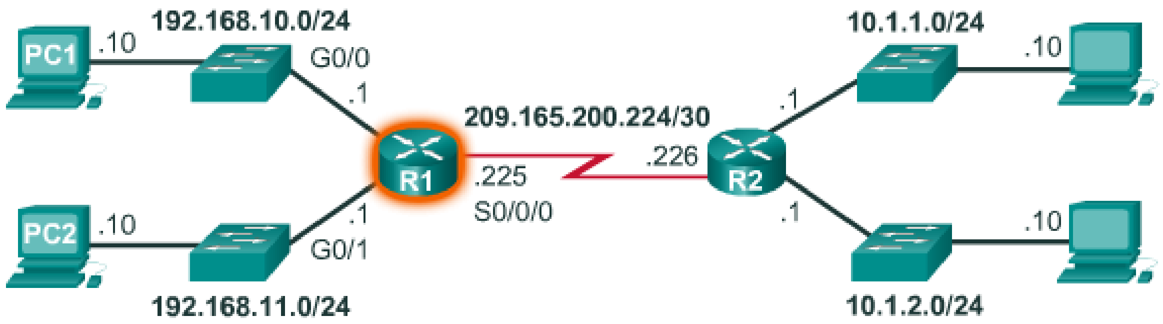


The routing table of a router

- **Directly-connected routes -** These routes come from the active router interfaces. Routers add a directly connected route when an interface is configured with an IP address and is activated. Each of the router's interfaces is connected to a different network segment.
- **Remote routes -** come from remote networks connected to other routers. Routes to these networks can be manually configured on the local router by the network administrator or dynamically configured by enabling the local router to exchange routing information with other routers using a dynamic routing protocol.
- **Default route** – Like a host, routers also use a default route as a last resort if there is no other route to the desired network in the routing table.

6.2.2.2 IPv4 Router Routing Table

R1 IPv4 Routing Table

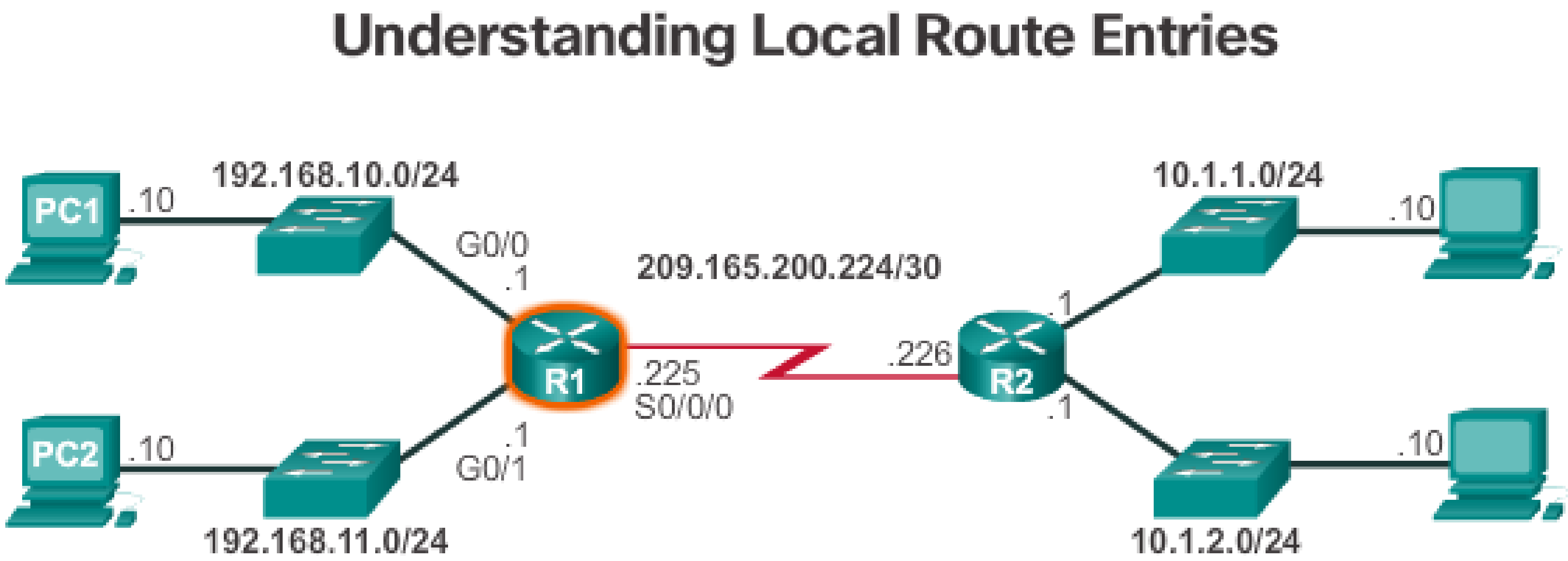



```
R1#show ip route
<output omitted>
Gateway of last resort is not set
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D       10.1.1.0/24 [90/2170112] via 209.165.200.226, 00:00:05,
        Serial0/0/0
D       10.1.2.0/24 [90/2170112] via 209.165.200.226, 00:00:05,
        Serial0/0/0
     192.168.10.0/24 is variably subnetted, 2 subnets, 3 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, 3 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, 3 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
```

6.2.2.3 Video Demonstration - Introducing the IPv4 Routing Table

IPv4 Router Routing Table

6.2.2.4 Directly Connected Routing Table Entries



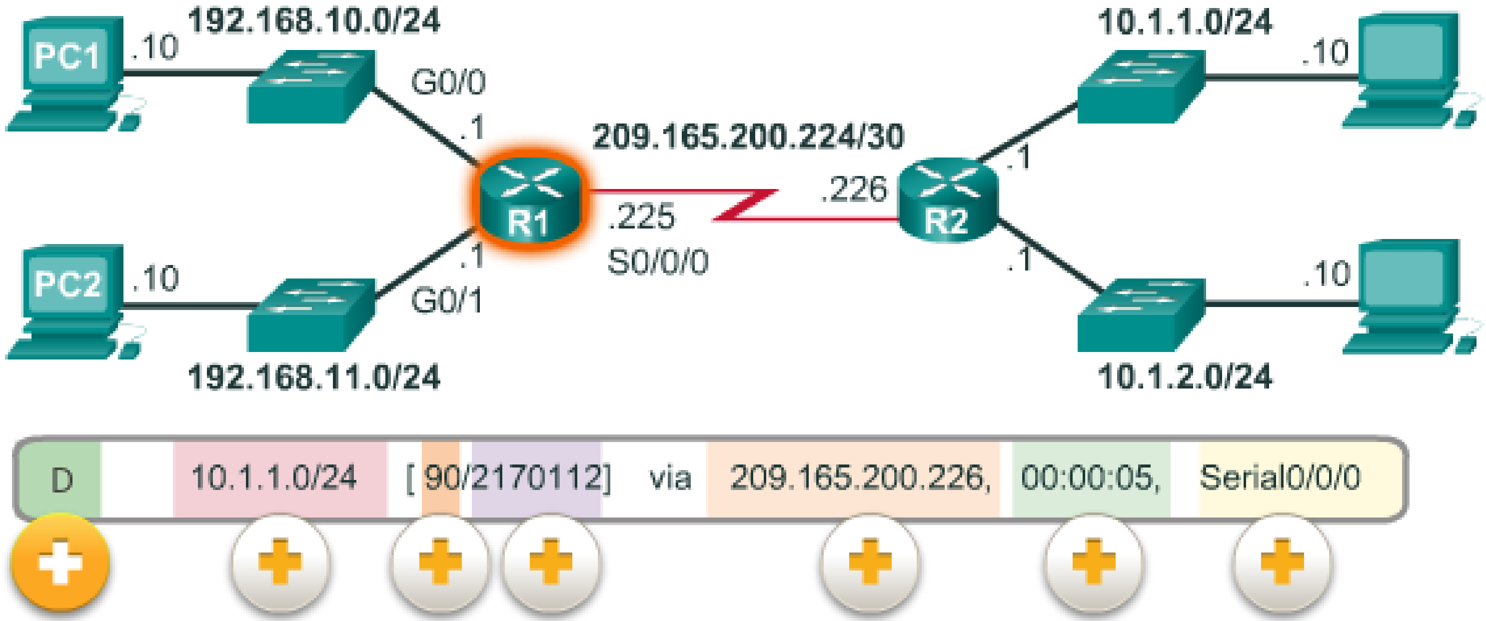

```
C    192.168.10.0/24 is directly connected, GigabitEthernet0/0
L    192.168.10.1/32 is directly connected, GigabitEthernet0/0
```

When a router interface is configured with an IPv4 address, a subnet mask, and is activated, the following two routing table entries are automatically created:

- **C** - Identifies a directly-connected network. Directly-connected networks are automatically created when an interface is configured with an IP address and activated.
- **L** - Identifies that this is a local interface. This is the IPv4 address of the interface on the router.

6.2.2.5 Remote Network Routing Table Entries

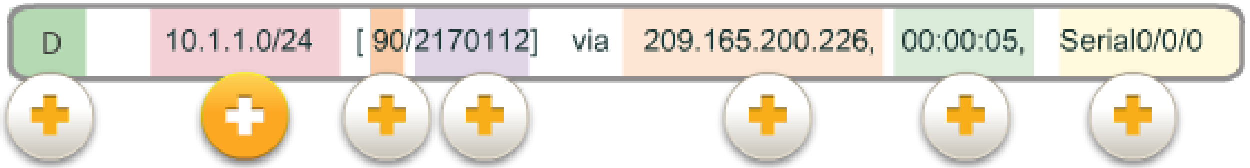
Understanding Remote Route Entries



Route Source

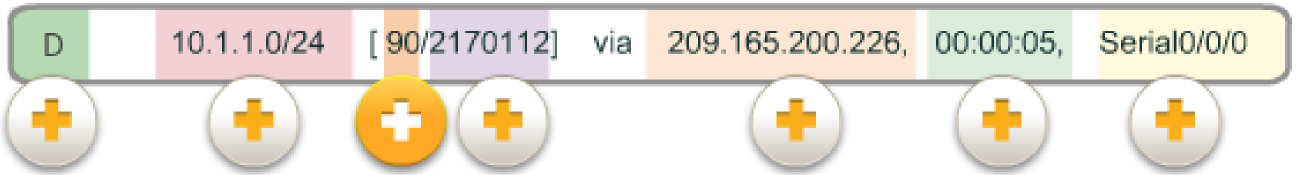
Identifies how the network was learned by the router. Common route sources include S (static route), D (Enhanced Interior Gateway Routing Protocol or EIGRP), and O (Open Shortest Path First or OSPF). Other route sources are beyond the scope of this chapter.

6.2.2.5 Remote Network Routing Table Entries



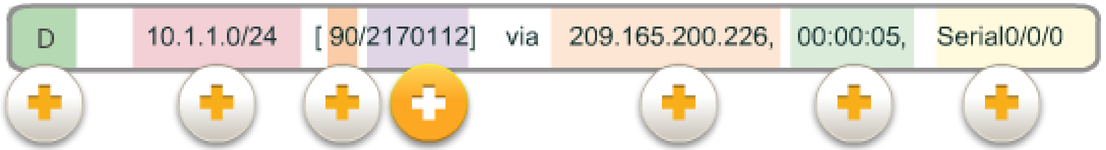
Destination Network

Identifies the destination network.



Administrative Distance

Identifies the administrative distance (i.e., trustworthiness) of the router source. Lower values indicate increased trustworthiness of the route source.



Metric

Identifies the value assigned to reach the remote network. Lower values indicate preferred routes.

Next-hop

Identifies the IP address of the next router to forward the packet.

6.2.2.5 Remote Network Routing Table Entries

D 10.1.1.0/24 [90/2170112] via 209.165.200.226, 00:00:05, Serial0/0/0

Route Timestamp

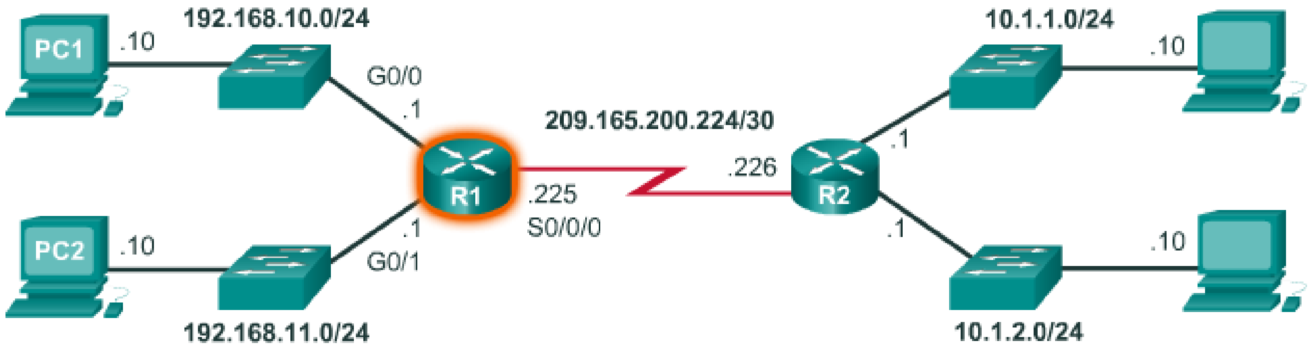
Identifies when the router was last heard from.

D 10.1.1.0/24 [90/2170112] via 209.165.200.226, 00:00:05, Serial0/0/0

Outgoing Interface

Identifies the exit interface to use to forward a packet toward the final destination.

6.2.2.6 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
     192.168.10.0/24 is variably subnetted, 2 subnets, 3 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, 3 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, 3 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
R1#
```

When a packet destined for a remote network arrives at the router, the router matches the destination network to a route in the routing table. If a match is found, the router forwards the packet to the next hop address out of the identified interface.

Refer to the sample network topology in Figure 1. Assume that either PC1 or PC2 has sent a packet destined for either the 10.1.1.0 or 10.1.2.0 network. When the packet arrives on the R1 Gigabit interface, R1 will compare the packet's destination IPv4 address to entries in its routing table. The routing table is displayed in Figure 2. Based on the content of its routing, R1 will forward the packet out of its Serial 0/0/0 interface to the next hop address 209.165.200.226.

6.2.2.7 Video Demonstration – Explaining the IPv4 Routing Table

Examine a Router IPv4 Routing Table

6.2.2.8 Activity - Identify Elements of a Router Routing Table Entry

A	B	C	D	E	F
D	192.168.1.0/24	[90/3072]	via 192.168.3.1,	00:06:03,	GigabitEthernet0/0

	A	B	C	D	E	F
1. The elapsed time since the network was discovered.					✓	
2. The administrative distance (source) and metric to reach the remote network.			✓			
3. How the network was learned by the router.	✓					
4. Shows the destination network.		✓				
5. The next hop IP address to reach the remote network.				✓		
6. The outgoing interface on the router to reach the destination network.						✓

6.3.1.1 A Router is a Computer

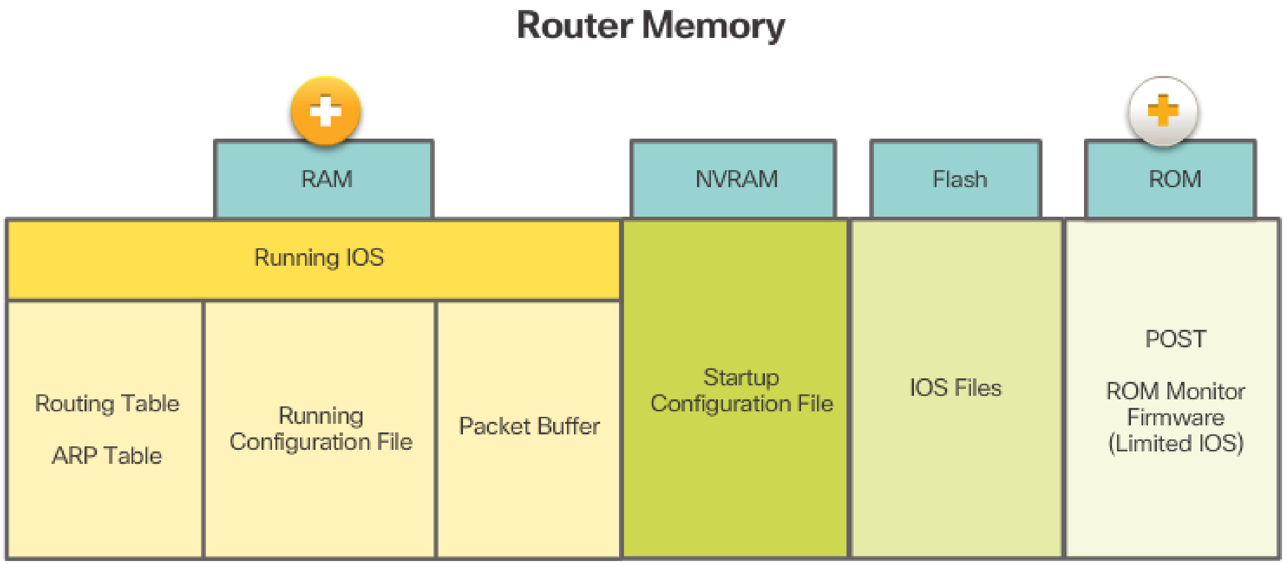
Cisco Integrated Service Routers

There are many types of infrastructure routers available. In fact, Cisco routers are designed to address the needs of many different types of businesses and networks:

- **Branch -** Teleworkers, small businesses, and medium-size branch sites. Includes Cisco Integrated Services Routers (ISR) G2 (2nd generation).
- **WAN -** Large businesses, organizations, and enterprises. Includes the Cisco Catalyst Series Switches and the Cisco Aggregation Services Routers (ASR).
- **Service Provider -** Large service providers. Includes Cisco ASR, Cisco CRS-3 Carrier Routing System, and 7600 Series routers.

6.3.1.2 Router CPU and OS

6.3.1.3 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

ROM

ROM stores the following:

- Bootup information that provides the startup instructions
- Power-on self-test (POST) that tests all the hardware components
- Limited IOS to provide a backup version of the IOS. It is used for loading a full feature IOS when it has been deleted or corrupted.

- **RAM** - This is volatile memory used in Cisco routers to store applications, processes, and data needed to be executed by the CPU.
- **ROM** - This non-volatile memory is used to store crucial operational instructions and a limited IOS. Specifically, ROM is firmware embedded on an integrated circuit inside the router which can only be altered by Cisco.
- **NVRAM** - This memory is used as the permanent storage for the startup configuration file (startup-config).
- **Flash** - Flash memory is non-volatile computer memory used as permanent storage for the IOS and other system related files such as log files, voice configuration files, HTML files, backup configurations, and more. When a router is rebooted, the IOS is copied from flash into RAM.

6.3.1.4 Inside a Router

6.3.1.5 Connect to a Router

Cisco 1941 Backplane

Auxiliary (AUX) RJ-45 port for remote management access similar to the Console port. Now considered a legacy port as it was used to provide support for dial-up modems.

Management Ports and Interfaces

In-band router interfaces are the LAN (i.e. Gigabit Ethernet) and WAN (i.e., eHWICs) interfaces configured with IP addressing to carry user traffic. Ethernet interfaces are the most common LAN connections, while common WAN connections include serial and DSL interfaces.

Management ports include the console and AUX ports which are used to configure, manage, and troubleshoot the router. Unlike LAN and WAN interfaces, management ports are not used for packet forwarding user traffic.

6.3.1.6 LAN and WAN Interfaces

Inband Router Interfaces

Serial WAN interfaces added to eHWIC0 and labeled Serial 0 (i.e., S0/0/0) and Serial 1 (i.e., S0/0/1). Serial interfaces are used for connecting routers to external WAN networks. Each serial WAN interface has its own IP address and subnet mask, which identifies it as a member of a specific network.

Ethernet LAN interfaces labeled GE 0/0 (i.e., G0/0) and GE 0/1 (i.e., G0/1). Ethernet interfaces are used for connecting to other Ethernet-enabled devices including switches, routers, firewalls, etc. Each LAN interface has its own IPv4 address and subnet mask and/or IPv6 address and prefix, which identifies it as a member of a specific network.

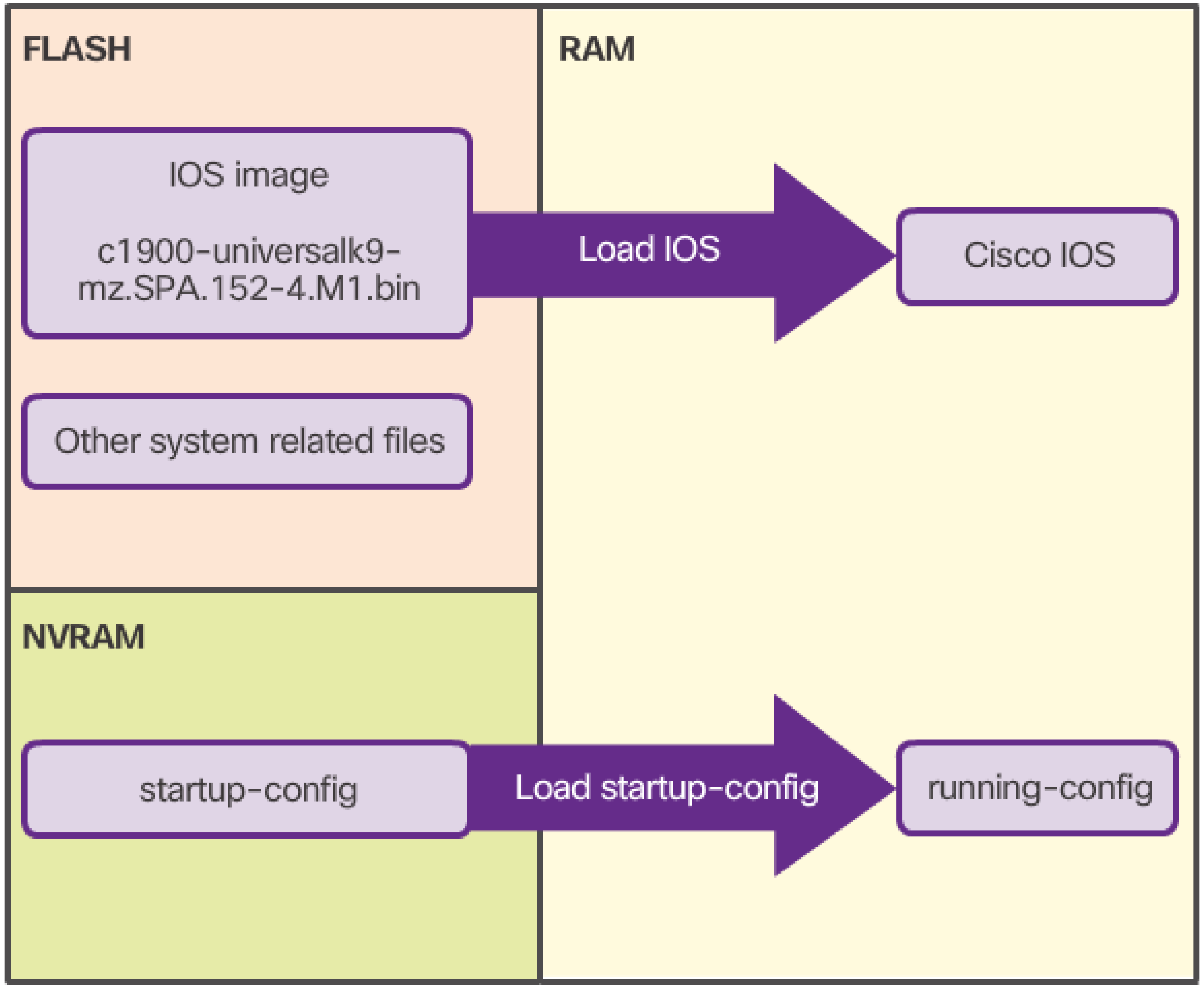
6.3.1.7 Activity - Identify Router Components

Router Component Name	Function/Description
WAN interface	Connects routers to external networks, usually over a large distance.
Telnet or SSH	A way to remotely access the CLI across a network interface.
LAN interface	Connects computers, switches, and routers for internal networking.
Console port	A local port which uses USB or low-speed, serial connections to manage network devices.
AUX port	A port to manage routers – using telephone lines and modems.

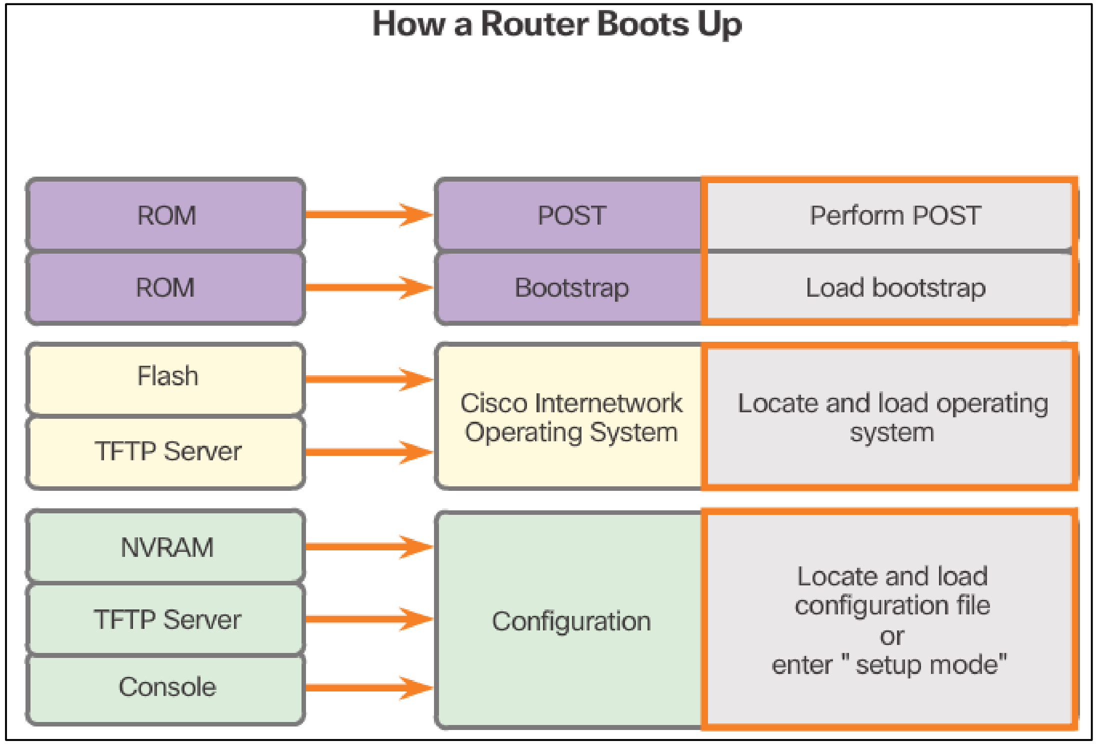
6.3.1.8 Packet Tracer - Exploring Internetworking Devices

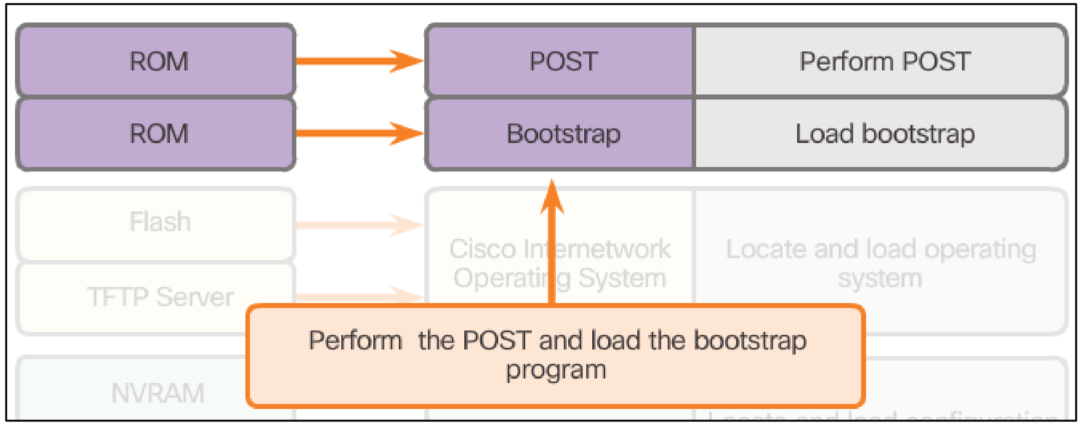
6.3.2.1 Bootset Files

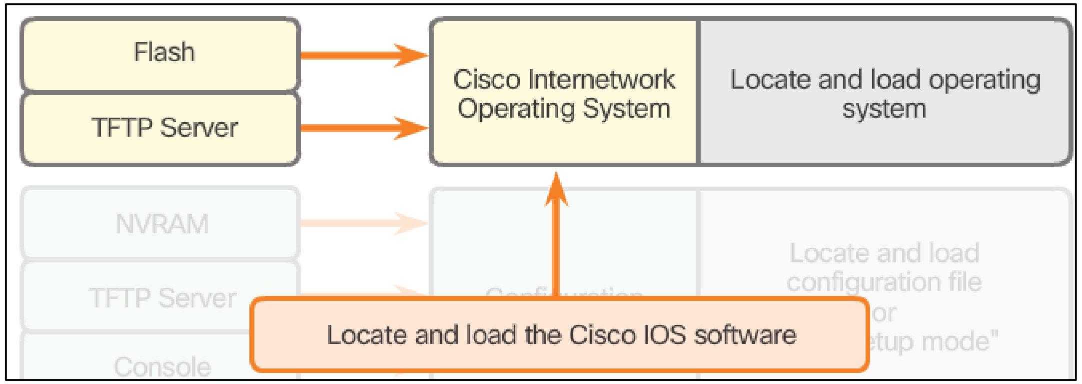
Files Copied to RAM During Bootup

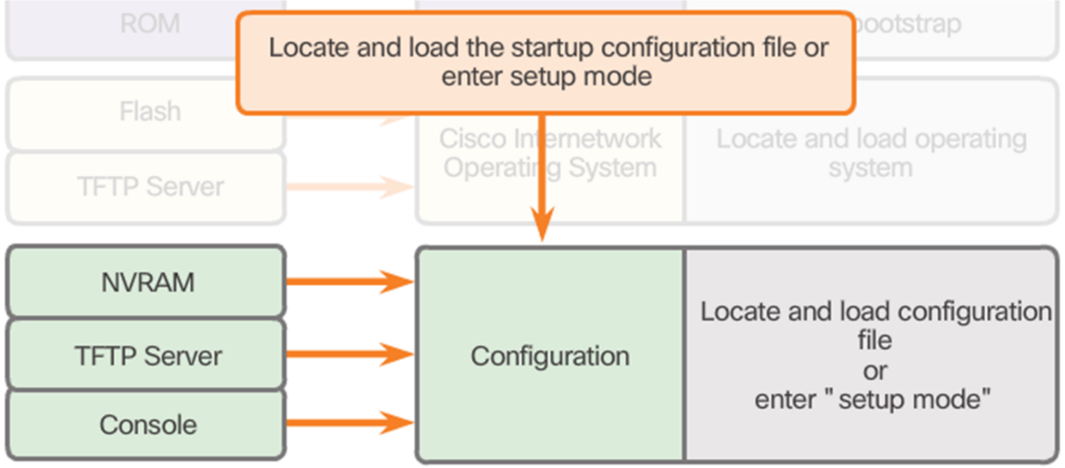


6.3.2.2 Router Bootup Process









6.3.2.3 Video Demonstration – Router Bootup Process

6.3.2.4 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 CISCO1941/K9 (revision 1.0)
with 446464K/77824K bytes of memory.
Processor board ID FTX1636848Z
```

Show Version Output

As highlighted in the figure, the **show version** command displays information about the version of the Cisco IOS software currently running on the router, the version of the bootstrap program, and information about the hardware configuration, including the amount of system memory

6.3.2.5 Video Demonstration - The show version Command

6.3.2.6 Activity - The Router Boot Process

The Router Boot Process

Perform POST (hardware check – performed by built-in ROM chip)

Load Bootstrap
(copied from ROM to RAM – locates the IOS)

Load the IOS (operating system file for the router – loaded into RAM after Bootstrap finds the IOS file to be used)

Load the Configuration File from FLASH (NVRAM), a TFTP Server OR Go into Setup Mode (to create a Configuration file)

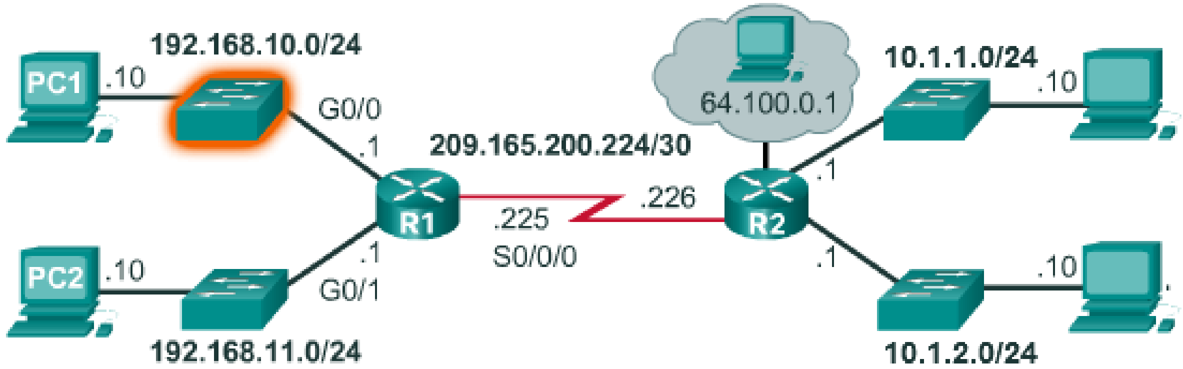
6.3.2.7 Lab - Exploring Router Physical Characteristics

6.4.1.1 Basic Switch Configuration Steps

Switch Configuration Tasks

- Configure the device name
  - hostname *name*
- Secure user EXEC mode
  - line console 0
  - password *password*
  - login
- Secure remote Telnet / SSH access
  - line vty 0 15
  - password *password*
  - login
- Secure privileged EXEC mode
  - enable secret *password*
- Secure all passwords in the config file
  - service password-encryption
- Provide legal notification
  - banner motd *delimiter message delimiter*
- Configure the management SVI
  - interface vlan 1
  - ip address *ip-address subnet-mask*
  - no shutdown
- Save the configuration
  - copy running-config startup-config

Sample Switch Configuration



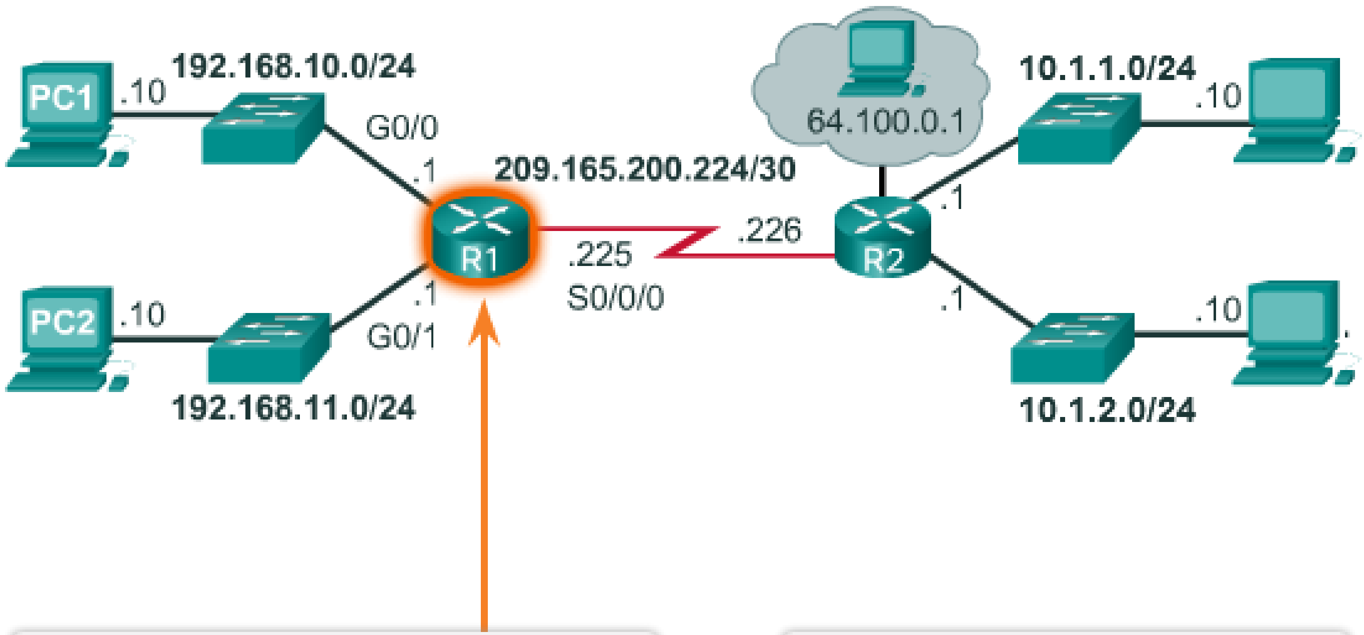

```
Switch>enable
Switch# configure terminal
Switch(config)# hostname S1
S1(config)# enable secret class
S1(config)# line console 0
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# line vty 0 15
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# exit
S1(config)# service password-encryption
```

6.4.1.2 Basic Router Configuration Steps

Limiting Device Access

- Configure the device name
  - hostname *name*
- Secure user EXEC mode
  - line console 0
  - password *password*
  - login
- Secure remote Telnet / SSH access
  - line vty 0 15
  - password *password*
  - login
- Secure privileged EXEC mode
  - enable secret *password*
- Secure all passwords in the config file
  - service password-encryption
- Provide legal notification
  - banner motd *delimiter message delimiter*
- Save the configuration
  - copy running-config startup-config

Configuring Hostname



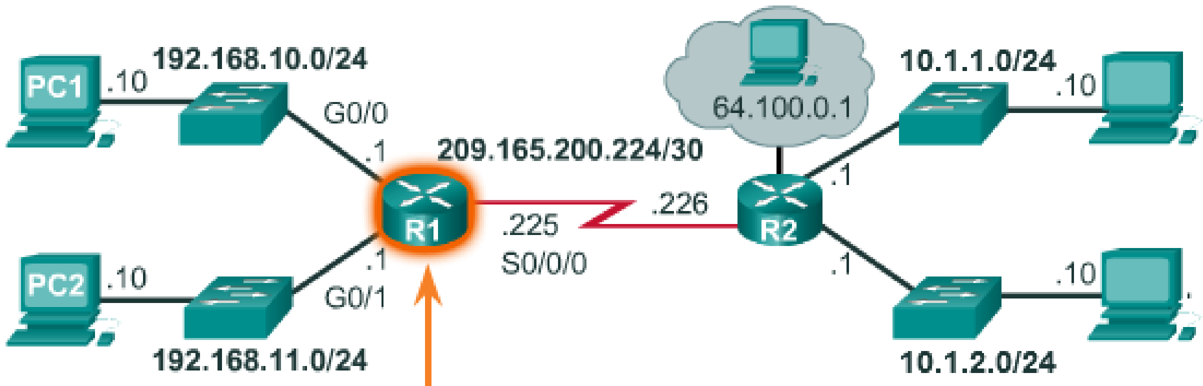

```
Router>enable
Router#configure terminal
Enter configuration
commands, one per line.
End with CNTL/Z.
Router(config)#hostname R1
R1(config)#
```

OR

```
Router>en
Router#conf t
Enter configuration
commands, one per line.
End with CNTL/Z.
Router(config)#ho R2
R2(config)#
```

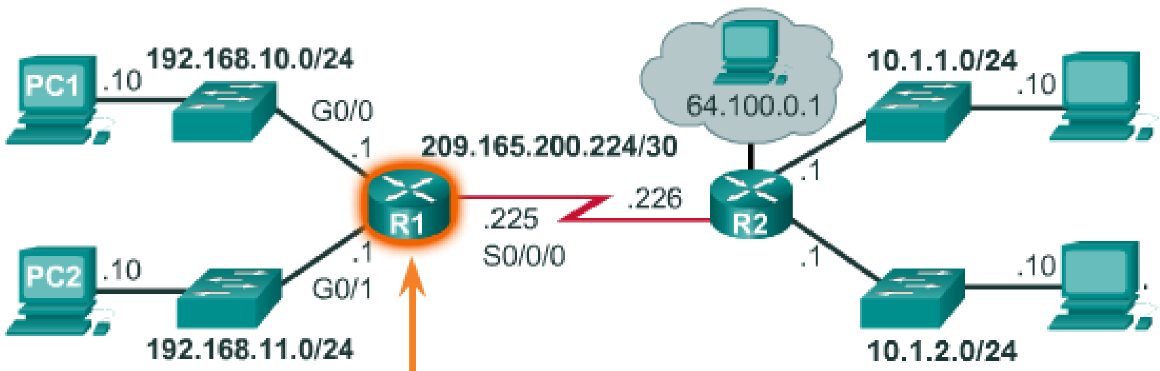
6.4.1.2 Basic Router Configuration Steps

Securing Management Access



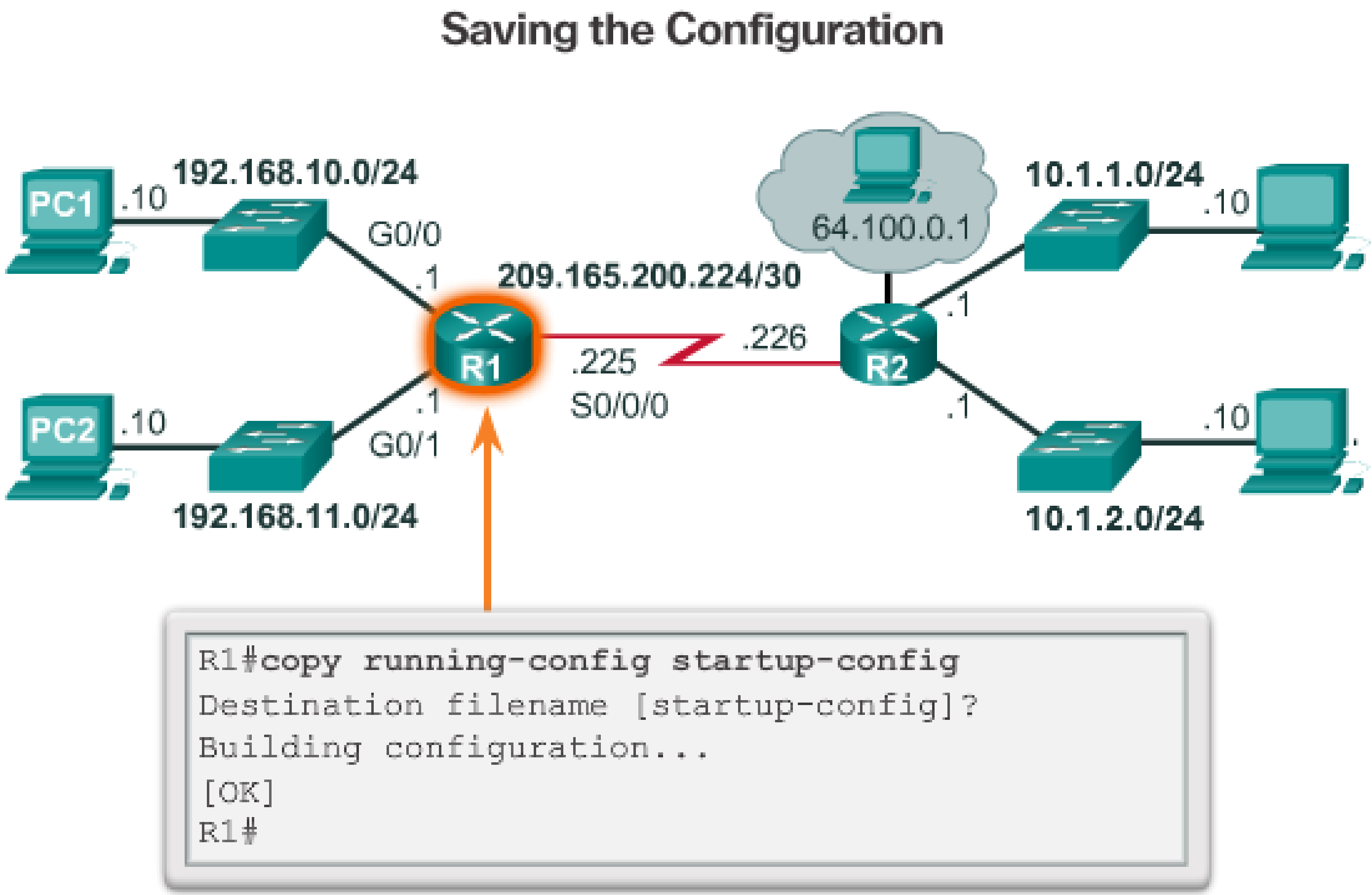

```
R1(config)#enable secret class
R1(config)#
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#
R1(config)#service password-encryption
R1(config)#
```

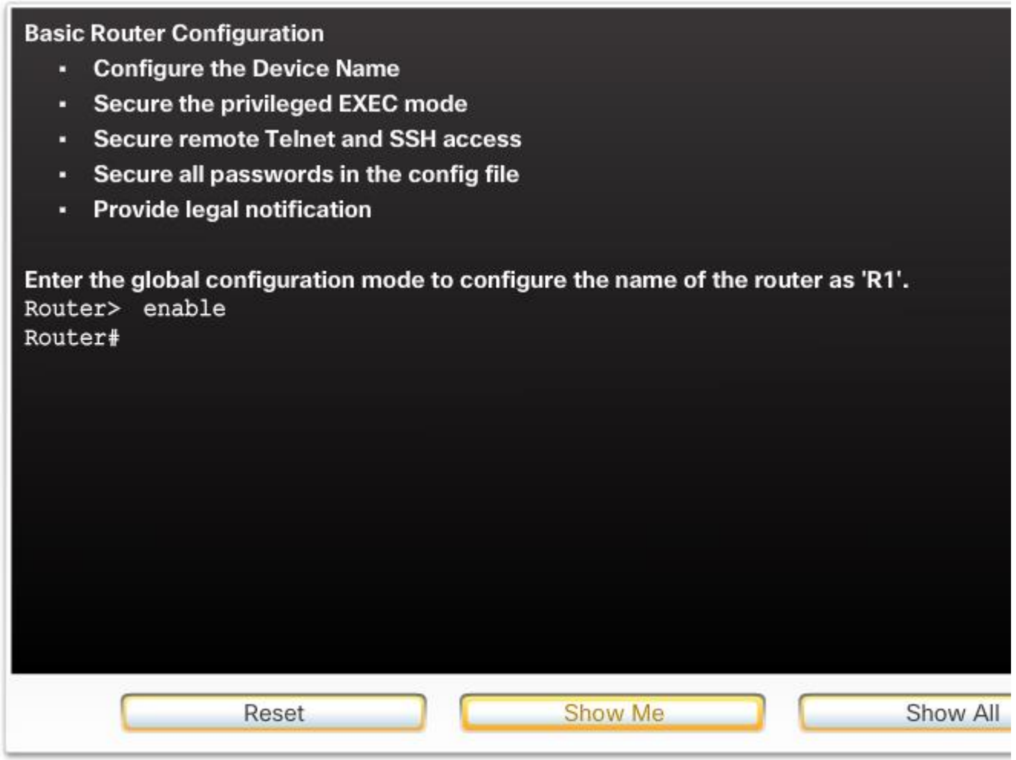
Providing Legal Notification




```
R1(config)#banner motd #
Enter TEXT message.  End with the character '#'.

*********************************************
        WARNING: Unauthorized access is
prohibited!

*********************************************
#

R1(config)#
```

6.4.1.2 Basic Router Configuration Steps



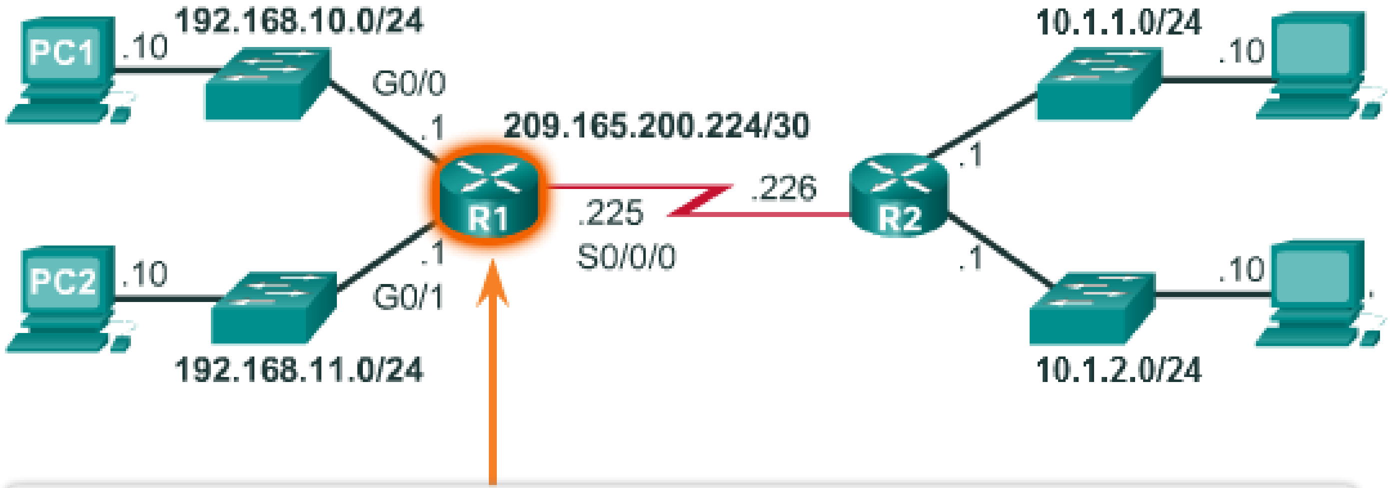


6.4.1.3 Packet Tracer - Configure Initial Router Settings

6.4.2.1 Configure Router Interfaces

Router Interface Configuration Tasks

- Configure the interface
  - **interface** *type-and-number*
  - **description** *description-text*
  - **ip address** *ipv4-address subnet-mask*
  - **no shutdown**




```
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
```

6.4.2.1 Configure Router Interfaces

Configure the GigabitEthernet 0/0 interface:

- **Configure IPv4 address as 192.168.10.1 with the subnet mask 255.255.255.0.**
- **Describe the link as 'LAN-10'.**
- **Activate the interface.**

```
R1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# interface gigabitethernet 0/0
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# description 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
```

Configure the GigabitEthernet 0/1 interface:

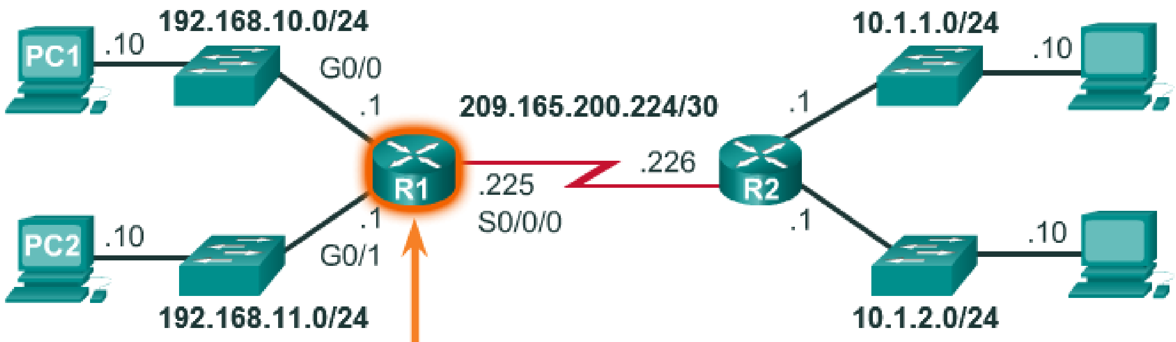
- **Configure IPv4 address as 192.168.11.1 with the subnet mask 255.255.255.0.**
- **Describe the link as 'LAN-11'**
- **Activate the interface**

```
R1(config)# interface gigabitethernet 0/1
R1(config-if)# ip address 192.168.11.1 255.255.255.0
R1(config-if)# description LAN-11
R1(config-if)# no shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
```

Reset | Show Me | Show All

6.4.2.2 Verify Interface Configuration


```
R1#show ip interface brief
Interface              IP-Address      OK?  Method Status

GigabitEthernet0/0     192.168.10.1    YES  manual up
GigabitEthernet0/1     192.168.11.1    YES  manual up
Serial0/0/0            209.165.200.225 YES  manual up
Serial0/0/1            unassigned      YES  NVRAM  administratively do
Vlan1                  unassigned      YES  NVRAM  administratively do
R1#
R1#ping 209.165.200.226

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.226
```

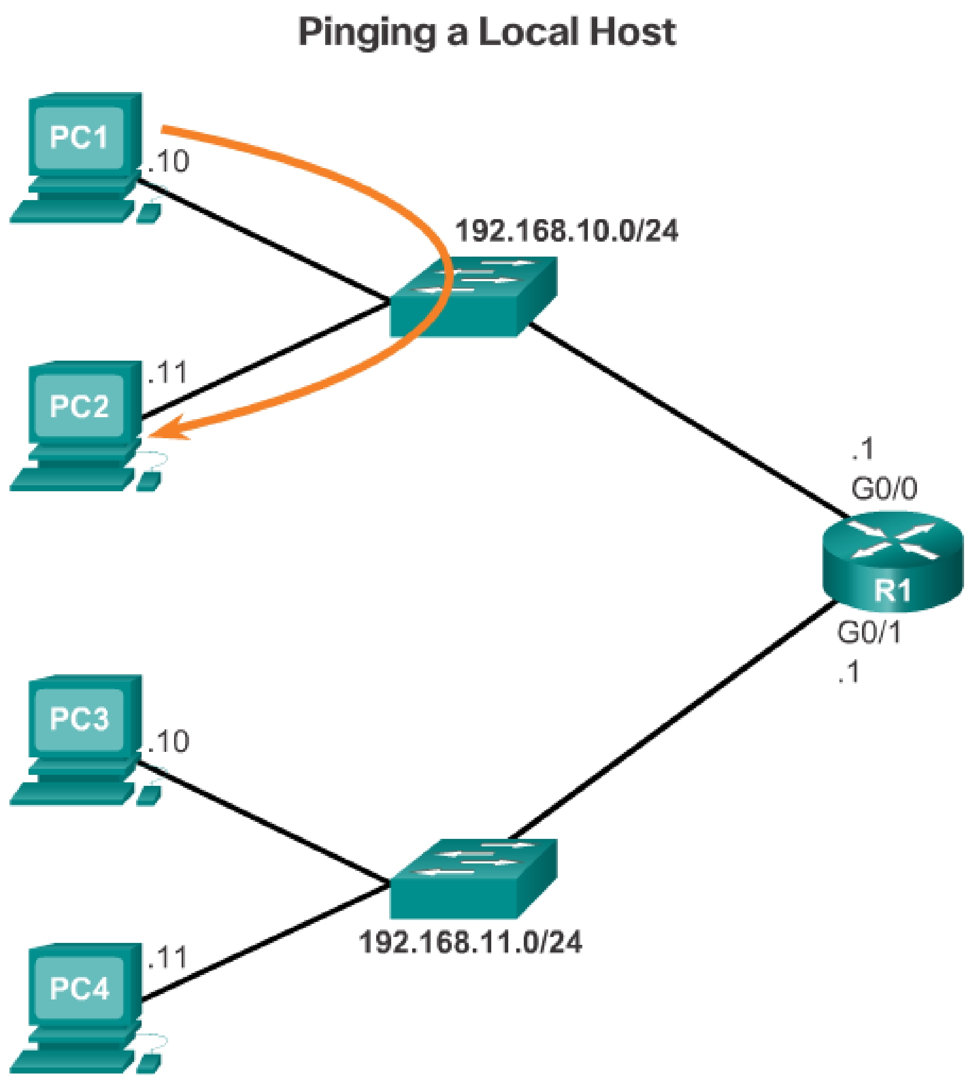


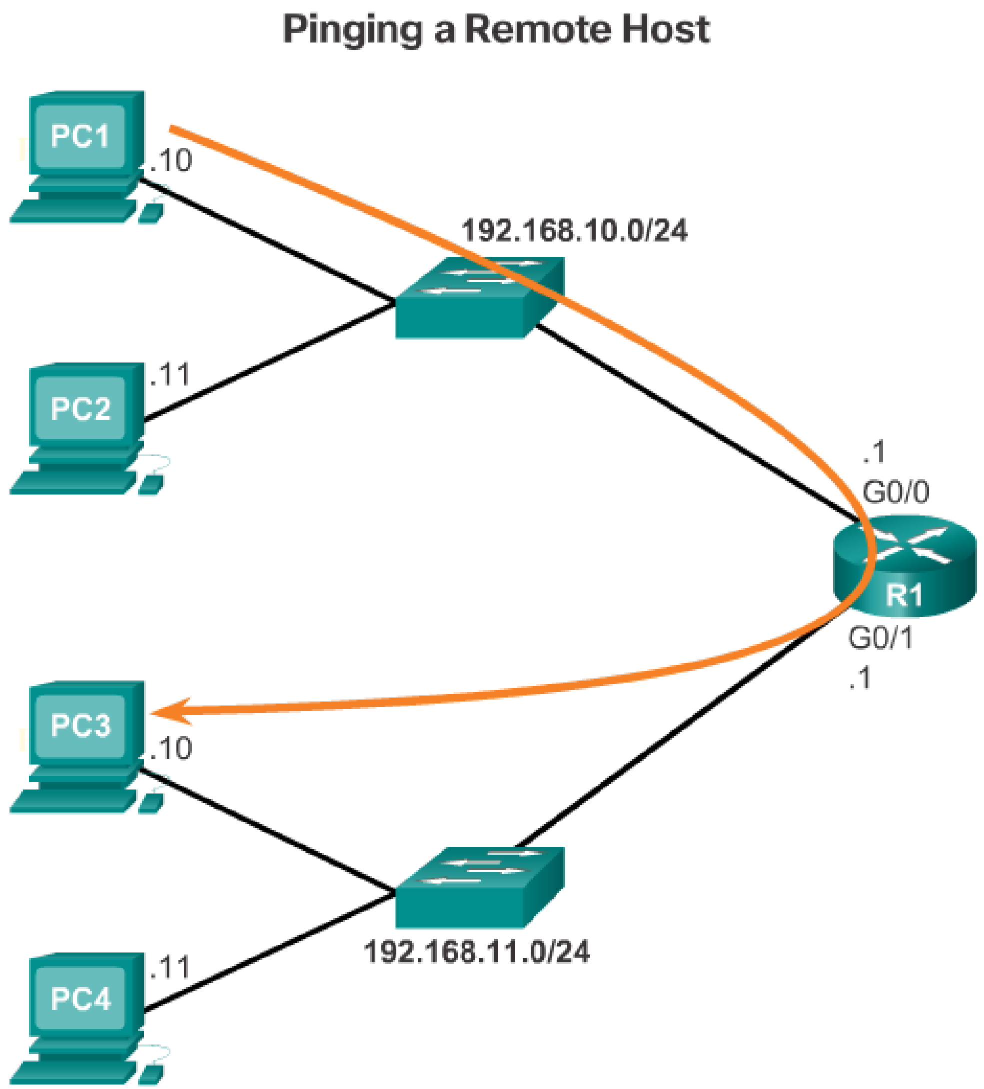

```
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP,
       M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF,
       IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1,  E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1,
       L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set
```

Other interface verification commands include:

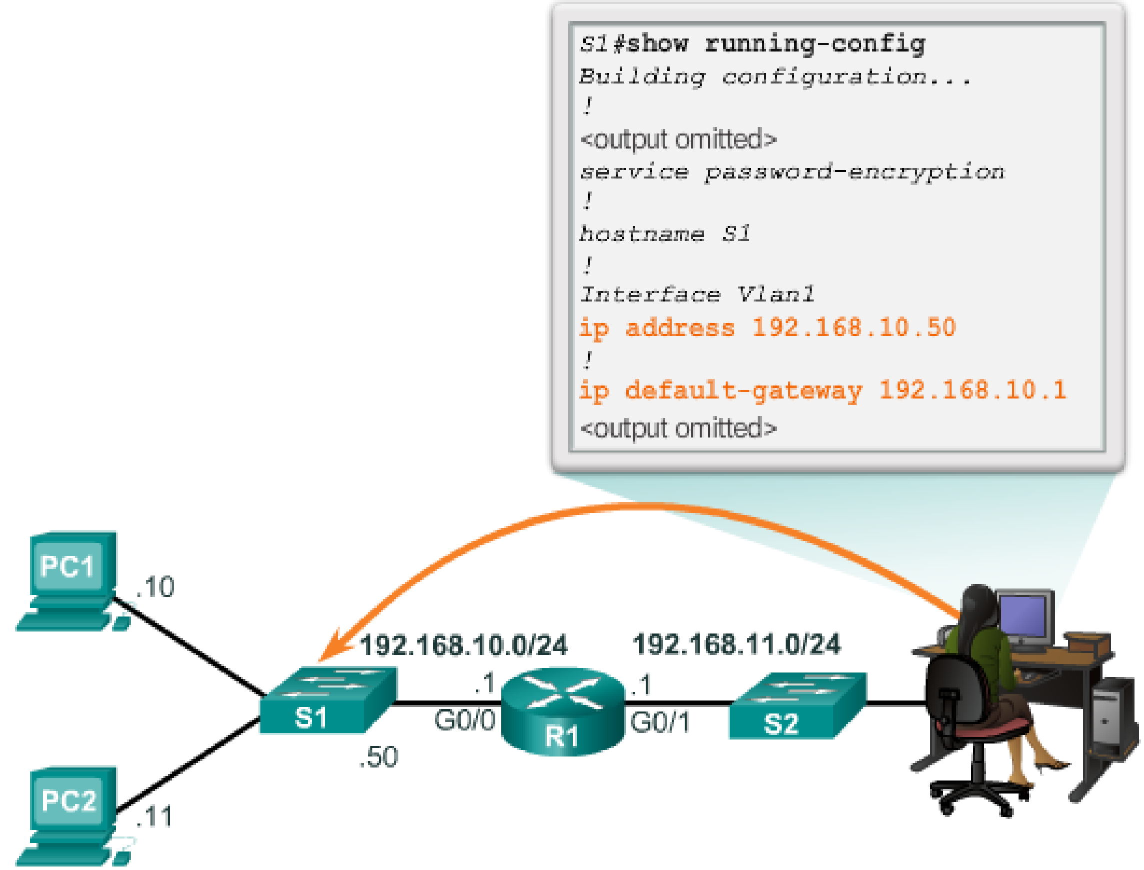
- **show ip route -** Displays the contents of the IPv4 routing table stored in RAM.
- **show interfaces -** Displays statistics for all interfaces on the device.
- **show ip interface -** Displays the IPv4 statistics for all interfaces on a router.

6.4.3.1 Default Gateway for a Host





6.4.3.2 Default Gateway for a Switch



If the default gateway was not configured on S1, response packets from S1 would not be able to reach the administrator at 192.168.11.10. The administrator would not be able to manage the device remotely.

Configuring a Switch Default Gateway

Enter global configuration and configure '192.168.10.1' as the default gateway for S1.

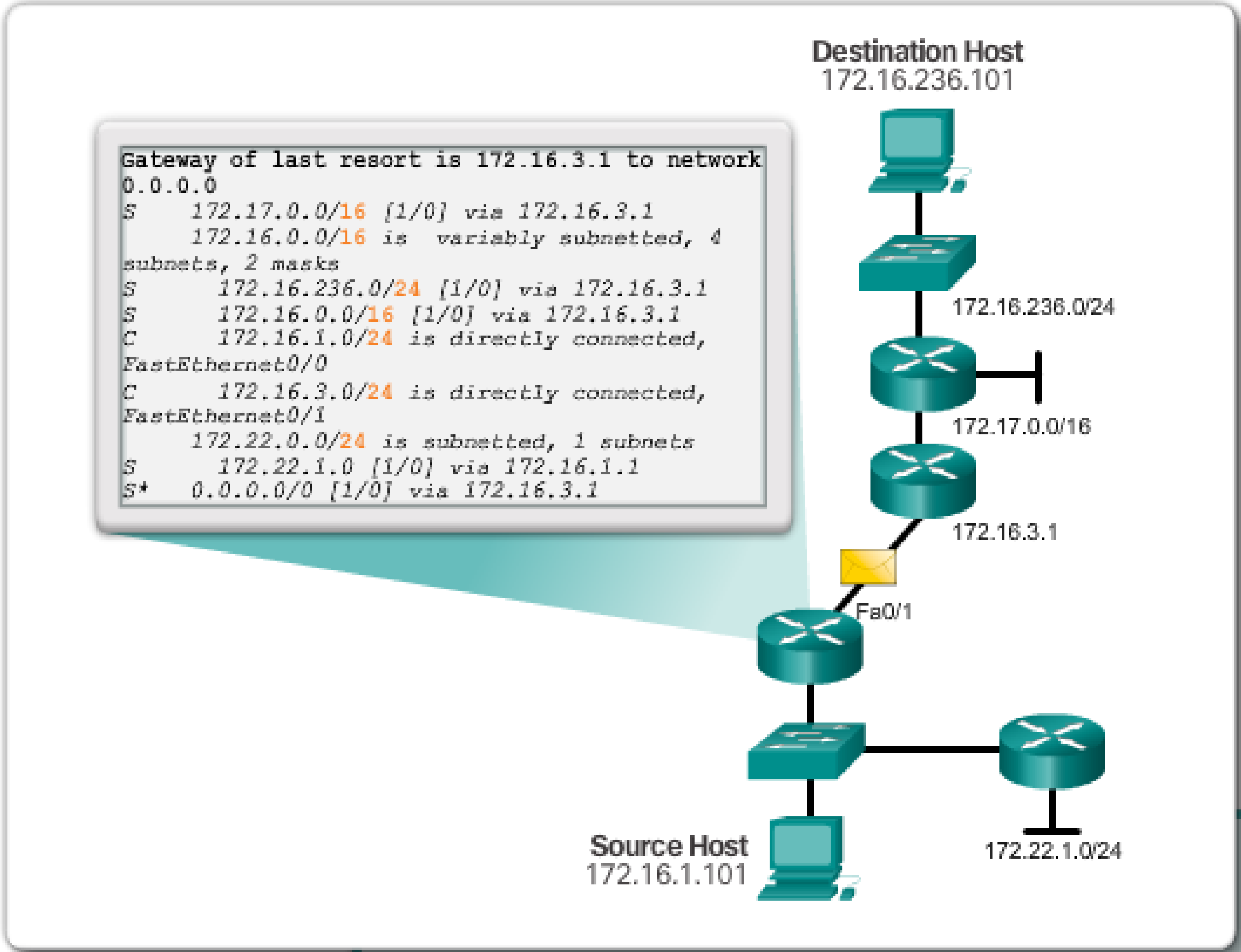
```
S1#  configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)# ip default-gateway 192.168.10.1
S1(config)#
```

You successfully configured the default gateway on a switch.

6.4.3.3 Packet Tracer - Connect a Router to a LAN

6.4.3.4 Packet Tracer - Troubleshooting Default Gateway Issues

6.5.1.1 Class Activity - Can You Read This Map?



The routing table of a router stores information about directly-connected routes and remote routes.

6.5.1.2 Lab - Building a Switch and Router Network

6.5.1.3 Packet Tracer - Skills Integration Challenge

6.5.1.4 Chapter 6: Network Layer

Thanks!!!

CISCO SYSTEMS

Thank you for your attention!