Cisco Networking Academy

CCNA R&S: Introduction to Networks

Chapter 6:

The Network Layer

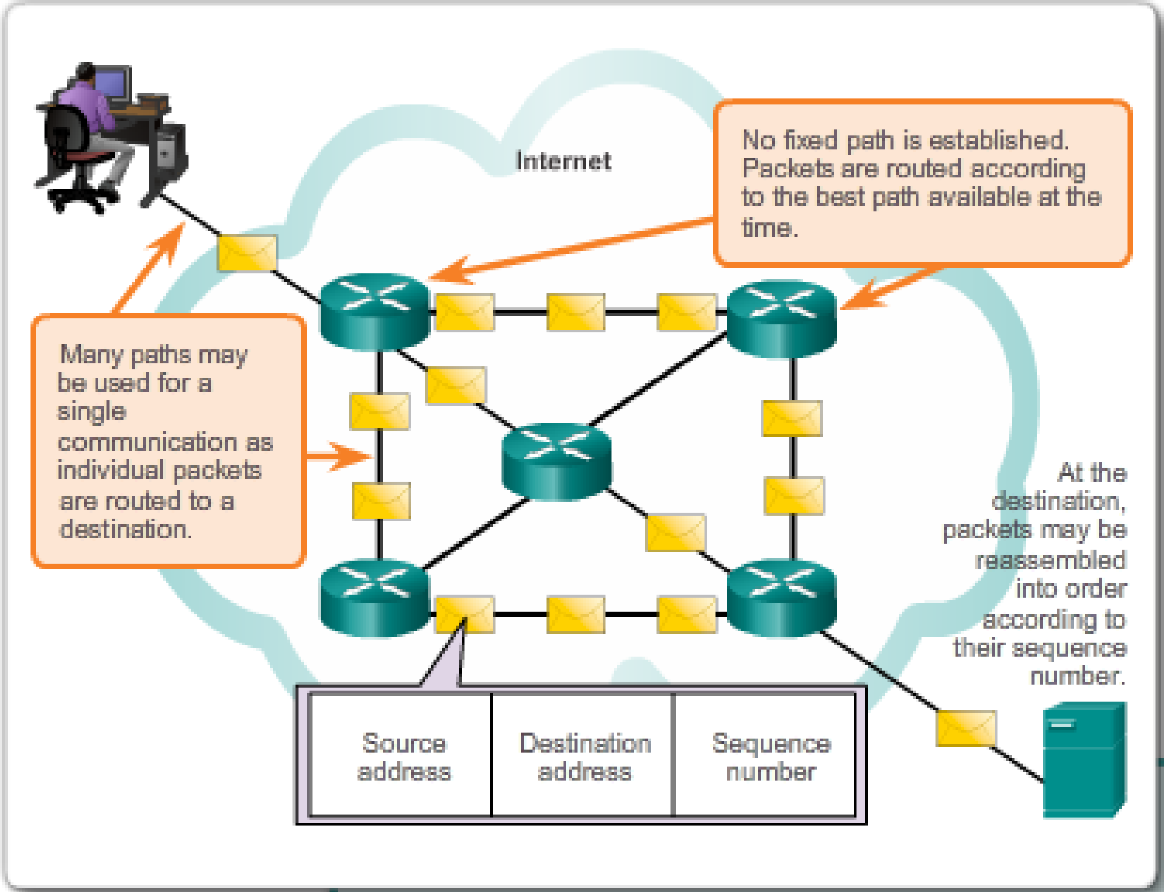
Frank Schneemann

6.0.1.1 Introduction

Upon completion of this chapter you will be able to:

- 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 and IPv6 packets.
- Explain how host devices use routing tables to direct packets to itself, a local destination, or a default gateway.
- Compare a host routing table to a routing table in a router.
- Describe the common components and interfaces of a router.
- Describe the boot-up process of a Cisco IOS router.
- Configure initial settings on a Cisco IOS router.
- Configure two active interfaces on a Cisco IOS router.
- Configure the default gateway on network devices.

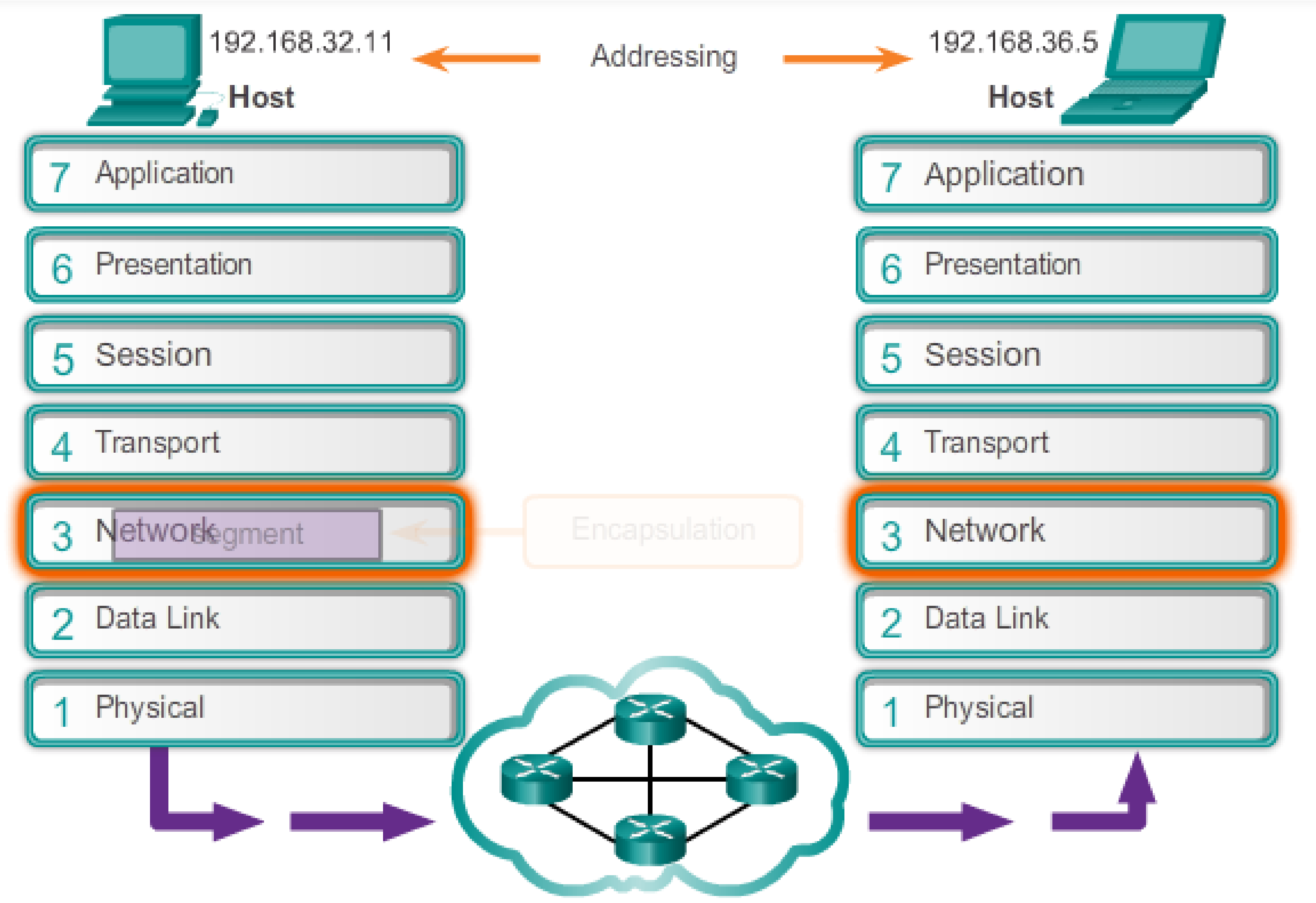
6.0.1.2 Activity – The Road Less Traveled…



The Network Layer uses four basic processes…

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

6.1.1.1 The Network Layer

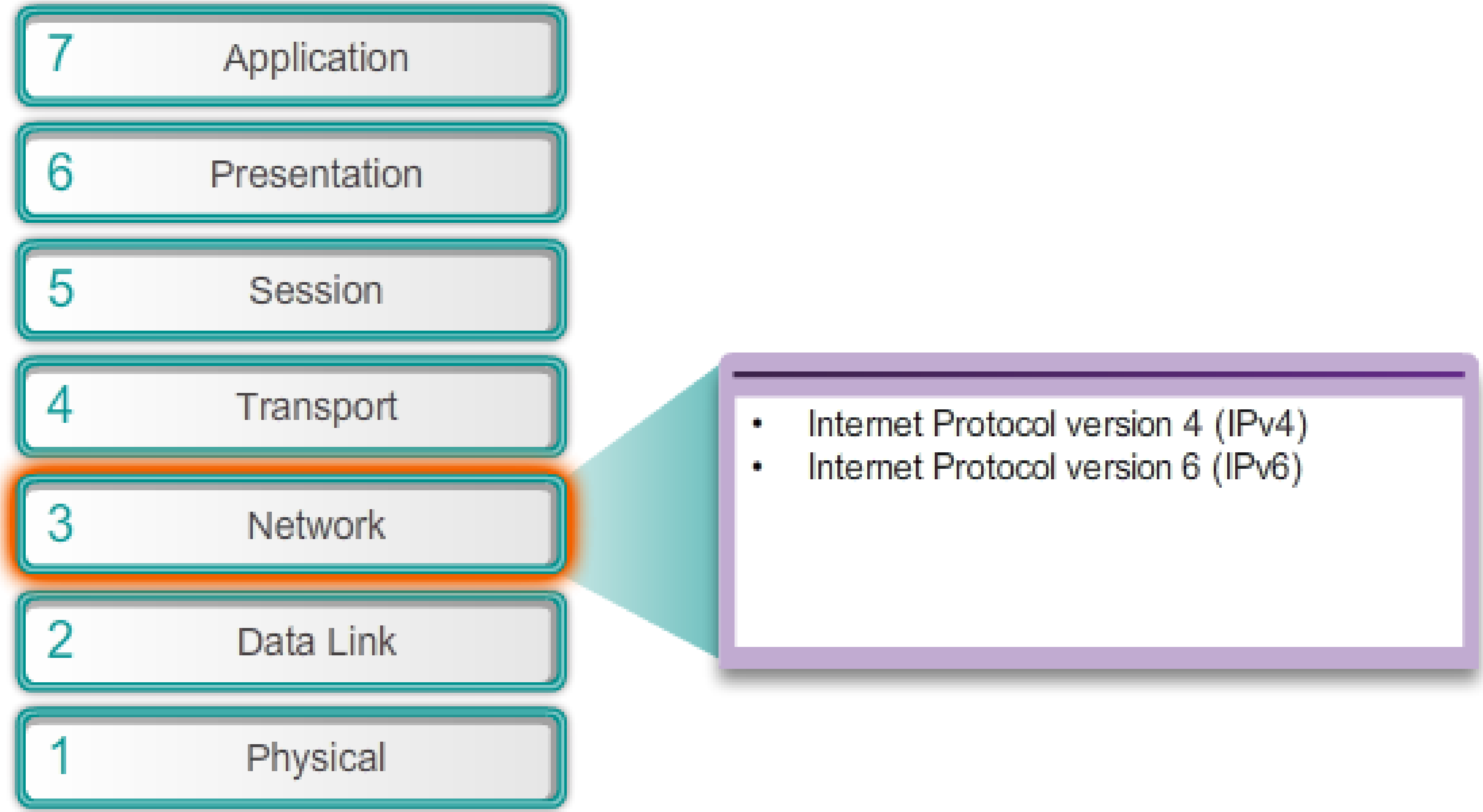


Network layer protocols forward transport layer PDUs between hosts.

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:

- **Addressing**
- **Encapsulation**
- **Routing**
- **De-encapsulation**

6.1.1.2 Network Layer Protocols

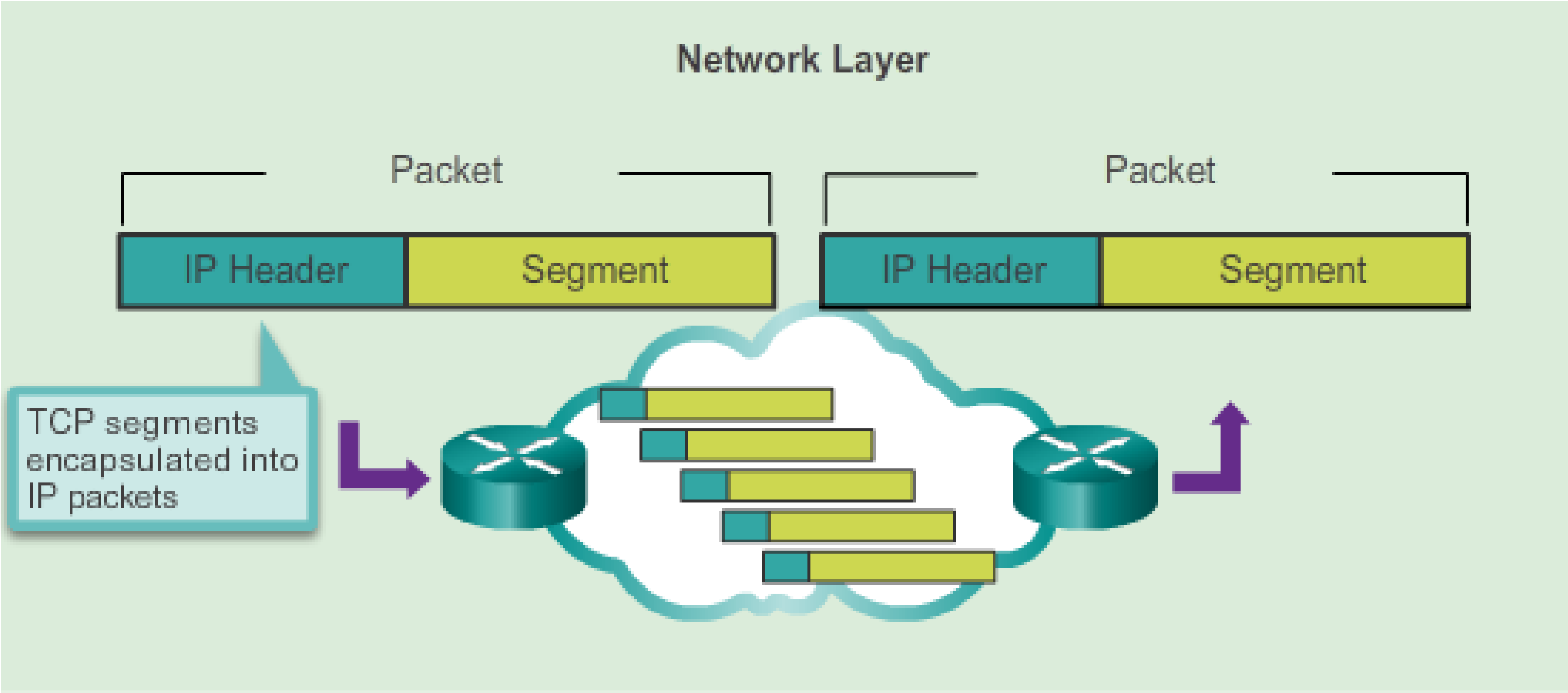


Other legacy network layer protocols that are not widely used include:

- Novell Internetwork Packet Exchange (IPX)
- AppleTalk
- Connectionless Network Service (CLNS/DECNet)

6.1.2.1 Characteristics of IP

TCP/IP

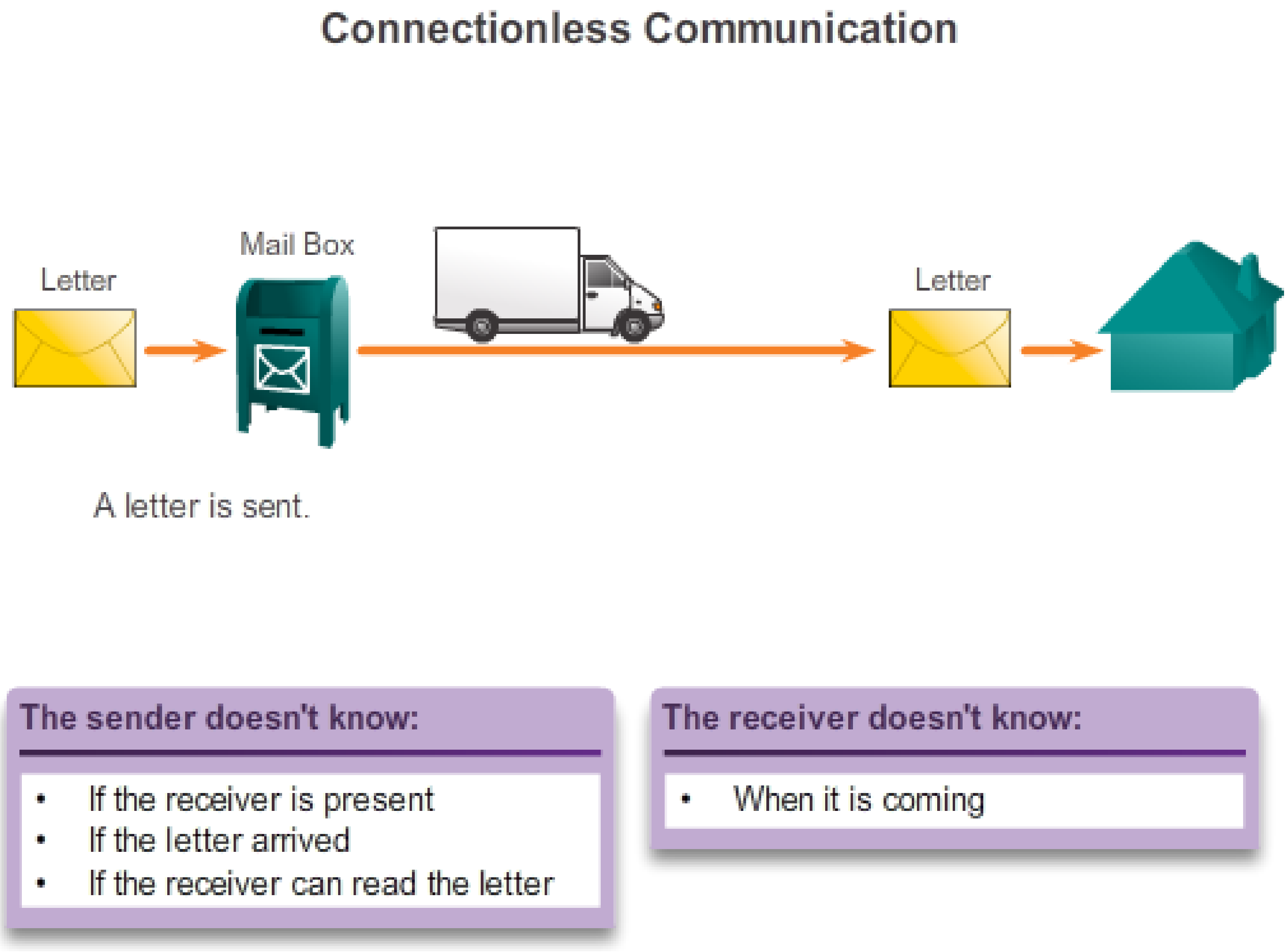


IP Packets flow through the internetwork.

The basic characteristics of IP are:

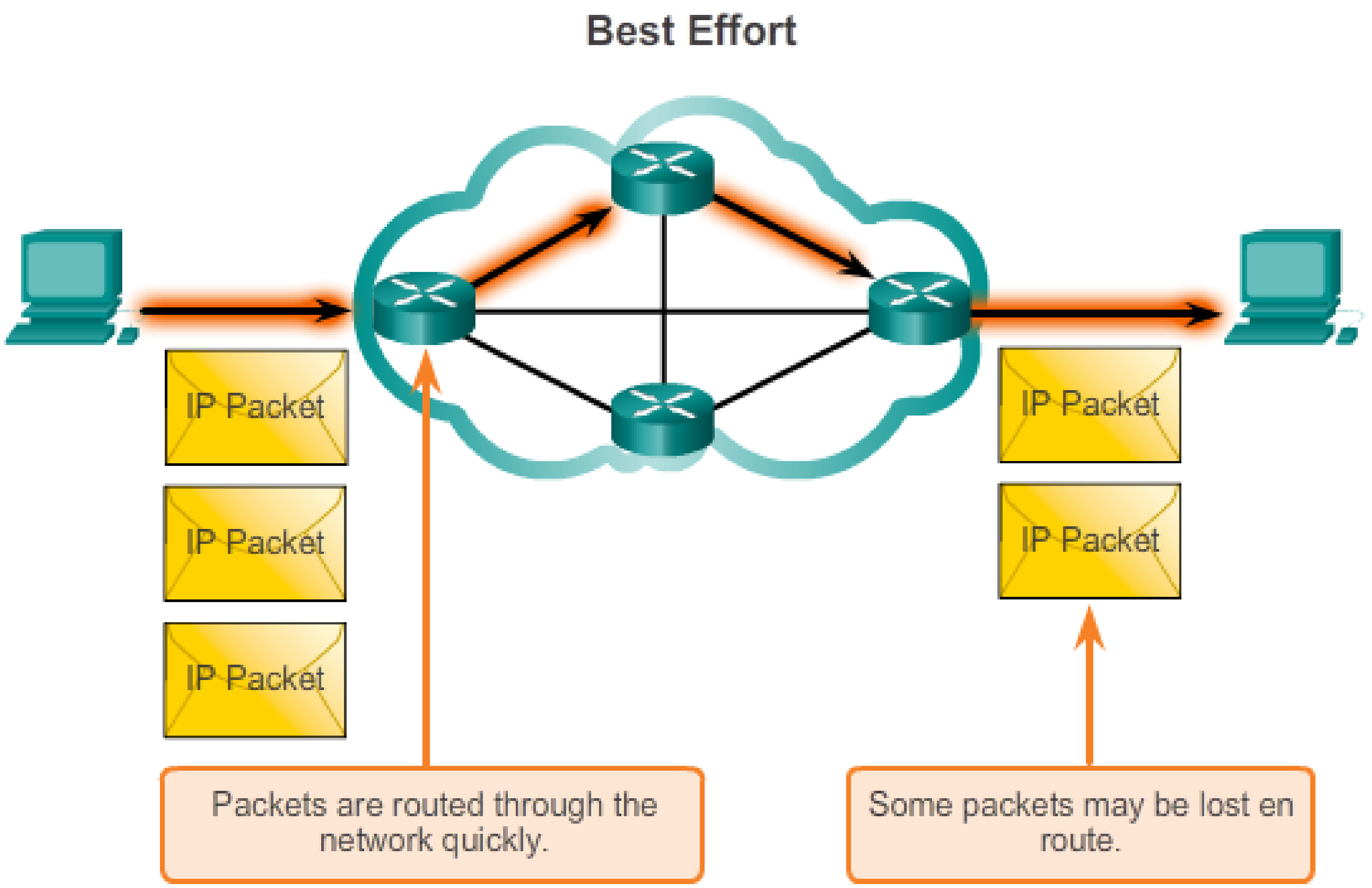
- **Connectionless** - No connection with the destination is established before sending data packets.
- **Best Effort** (unreliable) - Packet delivery is not guaranteed.
- **Media Independent** - Operation is independent of the medium carrying the data.

6.1.2.2 IP – Connectionless



IP is connectionless and, therefore, requires no initial exchange of control information to establish an end-to-end connection before packets are forwarded. IP also does not require additional fields in the protocol data unit (PDU) header to maintain an established connection.

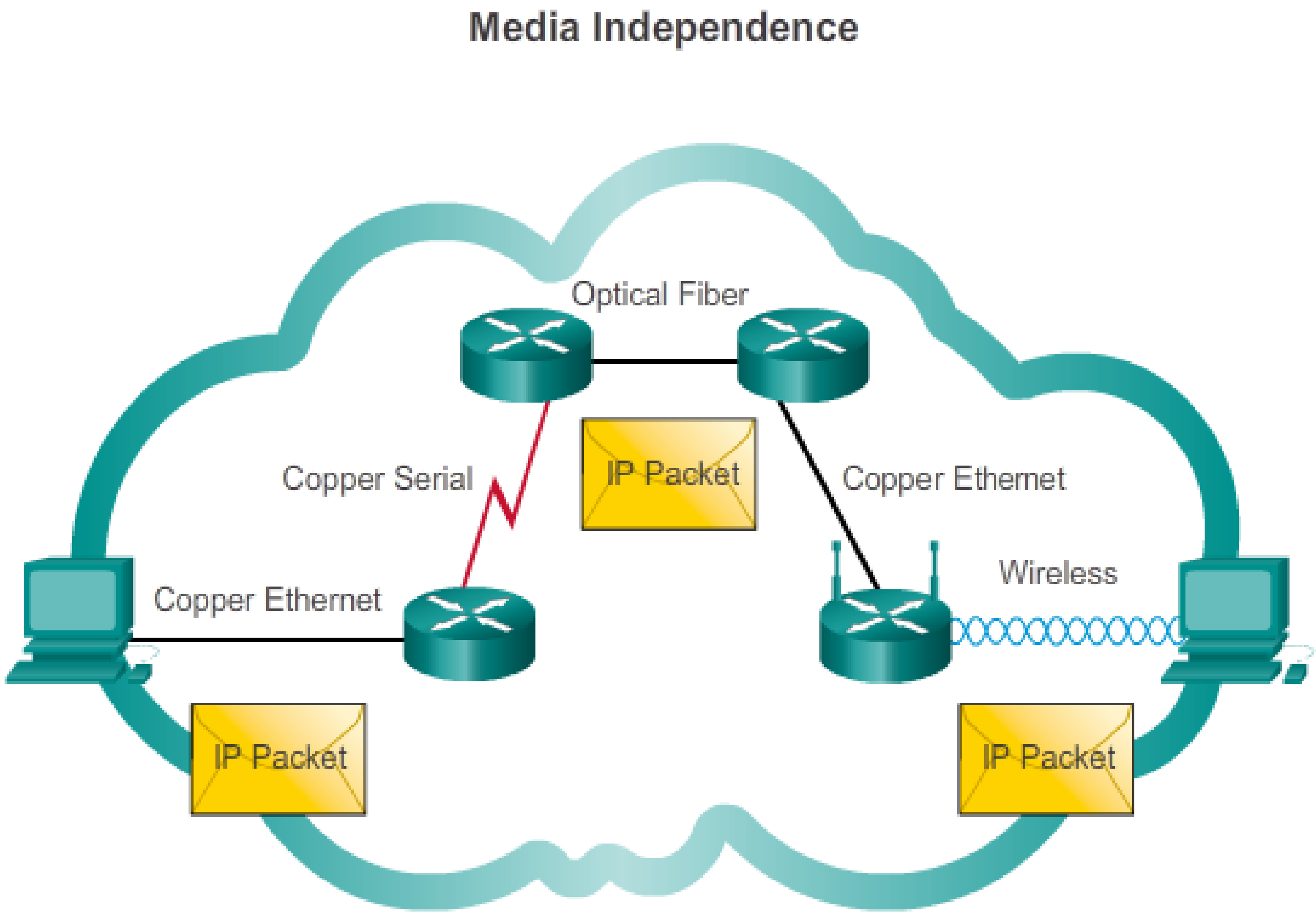
6.1.2.3 IP – Best Effort Delivery



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.

Unreliable simply means that IP does not have the capability to manage and recover from undelivered or corrupt packets. This is because while IP packets are sent with information about the location of delivery, it contains no information that can be processed to inform the sender whether delivery was successful. There is no synchronization data included in the packet header

6.1.2.4 IP – Media Independent



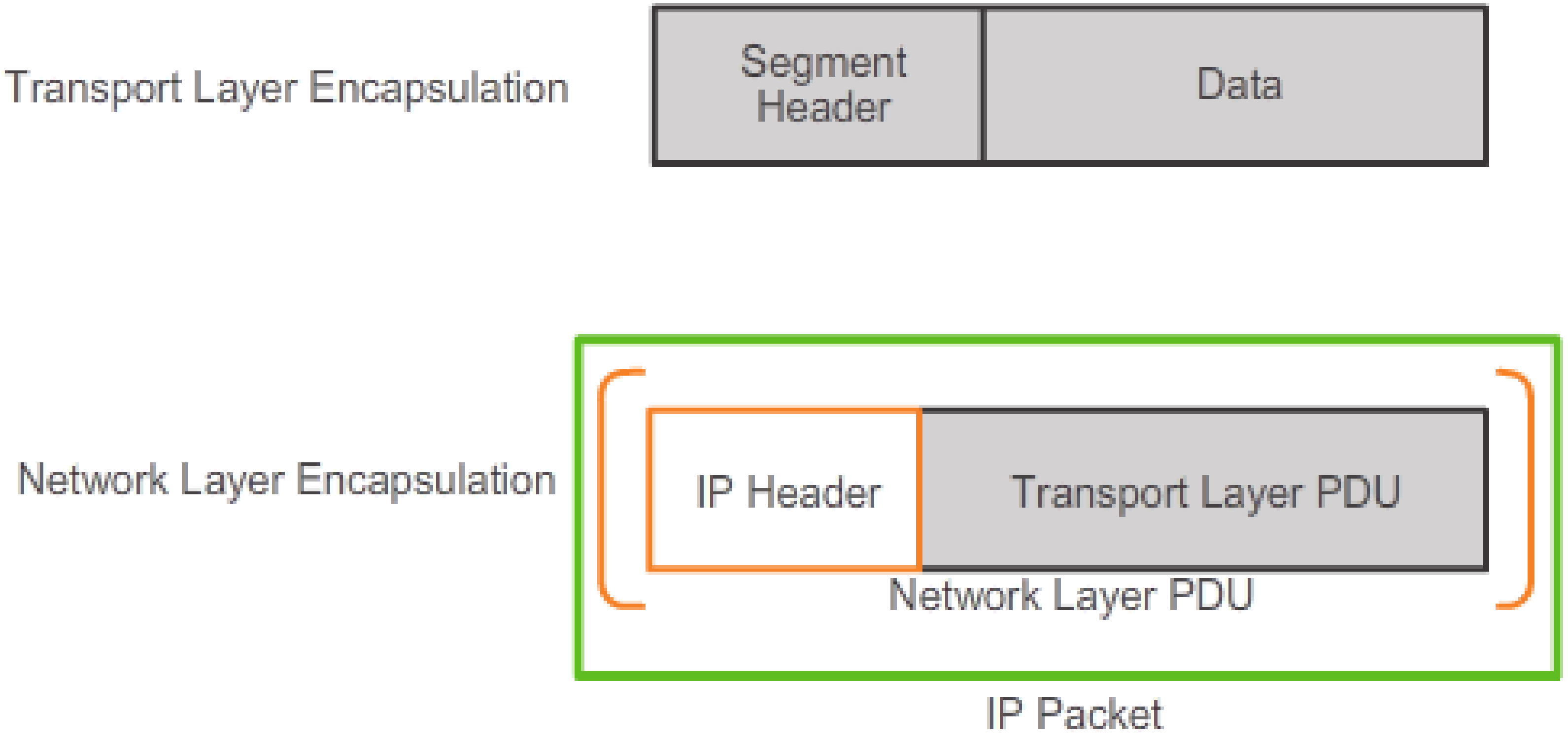
IP packets can travel over different media.

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 should be

6.1.2.5 Encapsulating IP

Generating IP Packets

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.



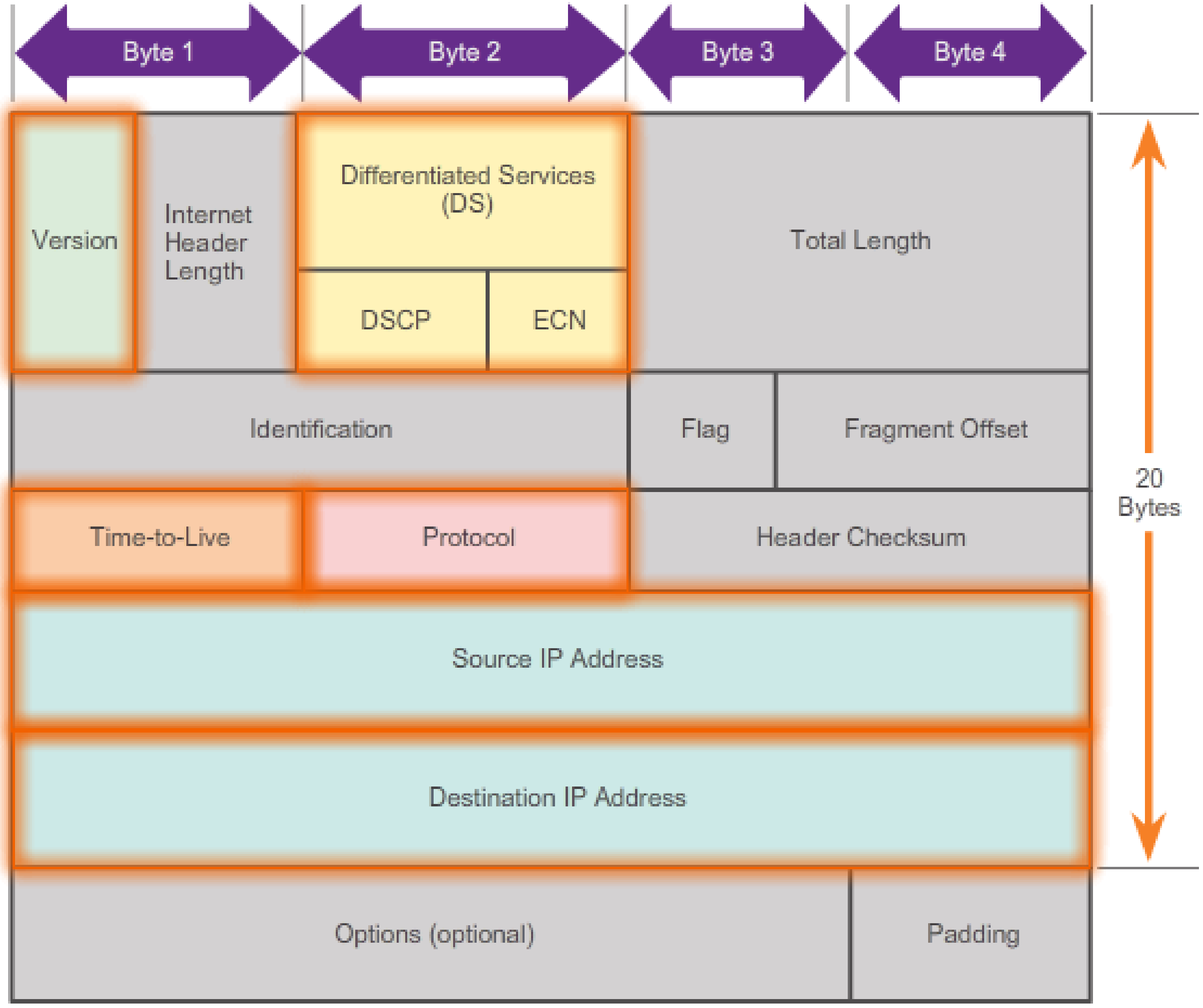
- Data
- Segments
- **Packets**
- Frames
- Bits

6.1.2.6 Activity - IP Characteristics

Delivery Method

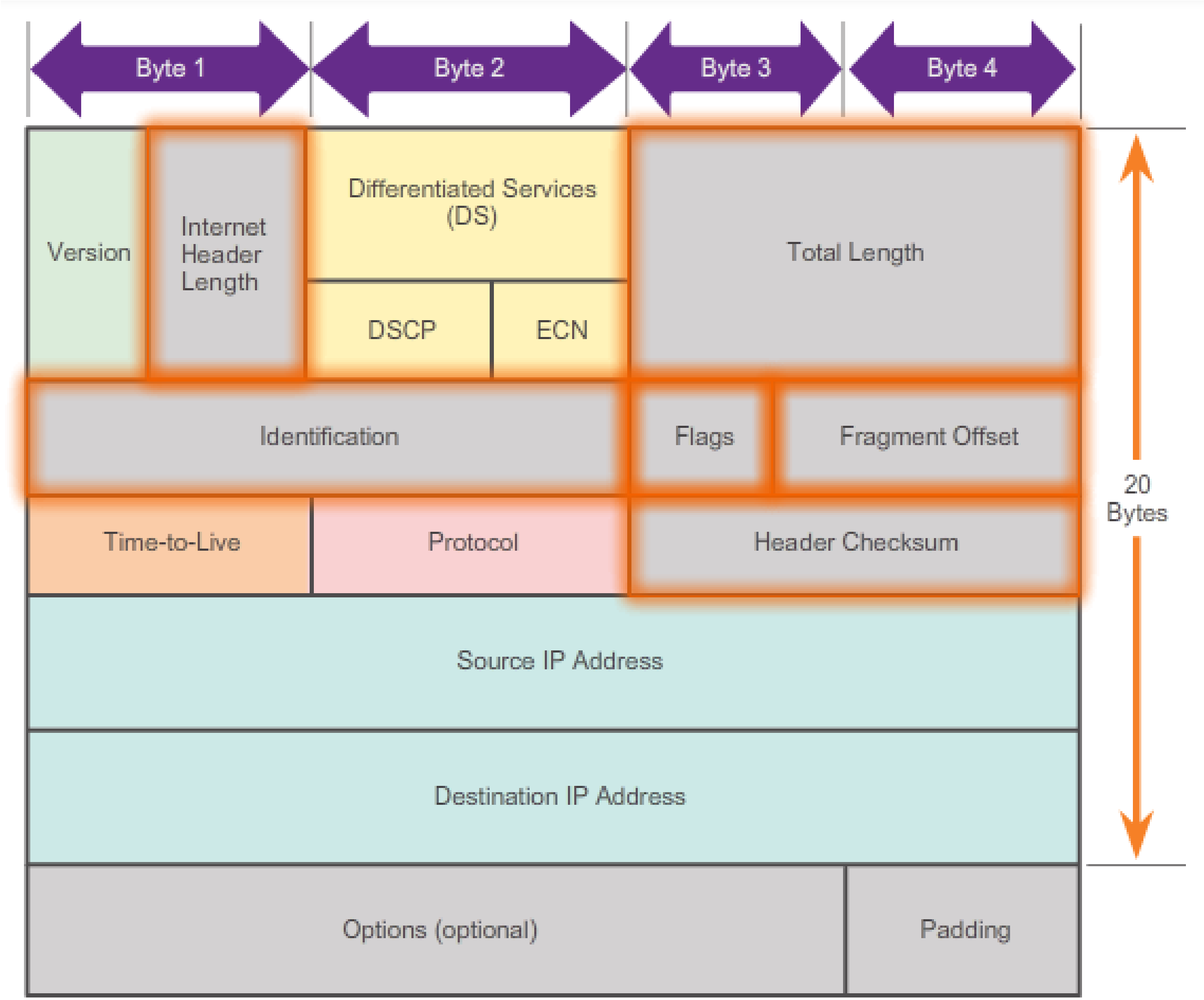
Connectionless	Best Effort	Media Independent
Will send a packet even if the destination host is not able to receive it. No contact is made with the destination host before sending a packet.	Does not guarantee that the packet will be delivered fully without errors. Packet delivery is not guaranteed.	Will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

6.1.3.1 IPv4 Packet Header



- **Version** - Contains a 4-bit binary value identifying the IP packet version. For IPv4 packets, this field is always set to 0100.
- **Differentiated Services 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
- **Source IP Address** - Contains a 32-bit binary value that represents the source IP address of the packet.
- **Destination IP Address** - Contains a 32-bit binary value that represents the destination IP address of the packet.

6.1.3.2 IPv4 Header Fields

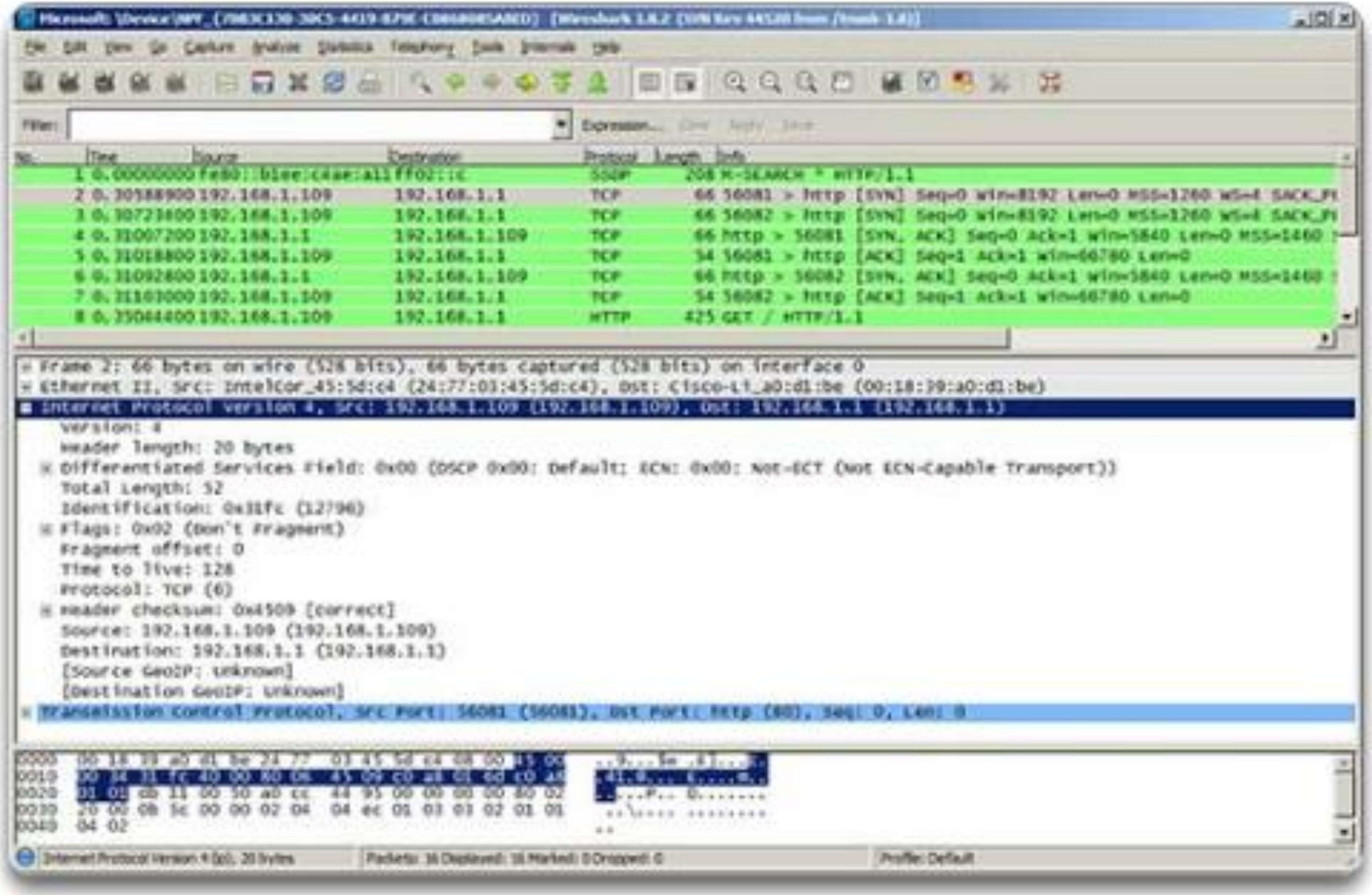


- Internet Header Length (IHL) - Contains a 4-bit binary value identifying the number of 32-bit words in the header.
- Total Length - Sometimes referred to as the Packet Length, this 16-bit field defines the entire packet (fragment) size
- Header Checksum - The 16-bit field is used for error checking of the IP header

A router may have to fragment a packet when forwarding it from one medium to another medium that has a smaller MTU.

- Identification - This 16-bit field uniquely identifies the fragment of an original IP packet.
- Flags - This 3-bit field identifies how the packet is fragmented.
- Fragment Offset - This 13-bit field identifies the order in which to place the packet fragment in the reconstruction of the original unfragmented packet.

6.1.3.3 Sample IPv4 Headers



Wireshark is a useful network monitoring tool for anyone working with networks and can be used with most labs in the Cisco Certified Network Associate (CCNA) courses for data analysis and troubleshooting. It can be used to view sample values contained in IP header fields.

6.1.3.4 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

- IP address depletion - IPv4 has a limited number of unique public IP addresses available. Although there are approximately 4 billion IPv4 addresses, the increasing number of new IP-enabled devices, always-on connections, and the potential growth of less-developed regions have increased the need for more addresses.

- Internet routing table expansion - A routing table is used by routers to make best path determinations. As the number of servers (nodes) connected to the Internet increases, so too does the number of network routes. These IPv4 routes consume a great deal of memory and processor resources on Internet routers.

- 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 IP address. However, because the public IP address is shared, the IP 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

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	1,000,000,000,000,000,000,000,000,000,000,000,000,00 0

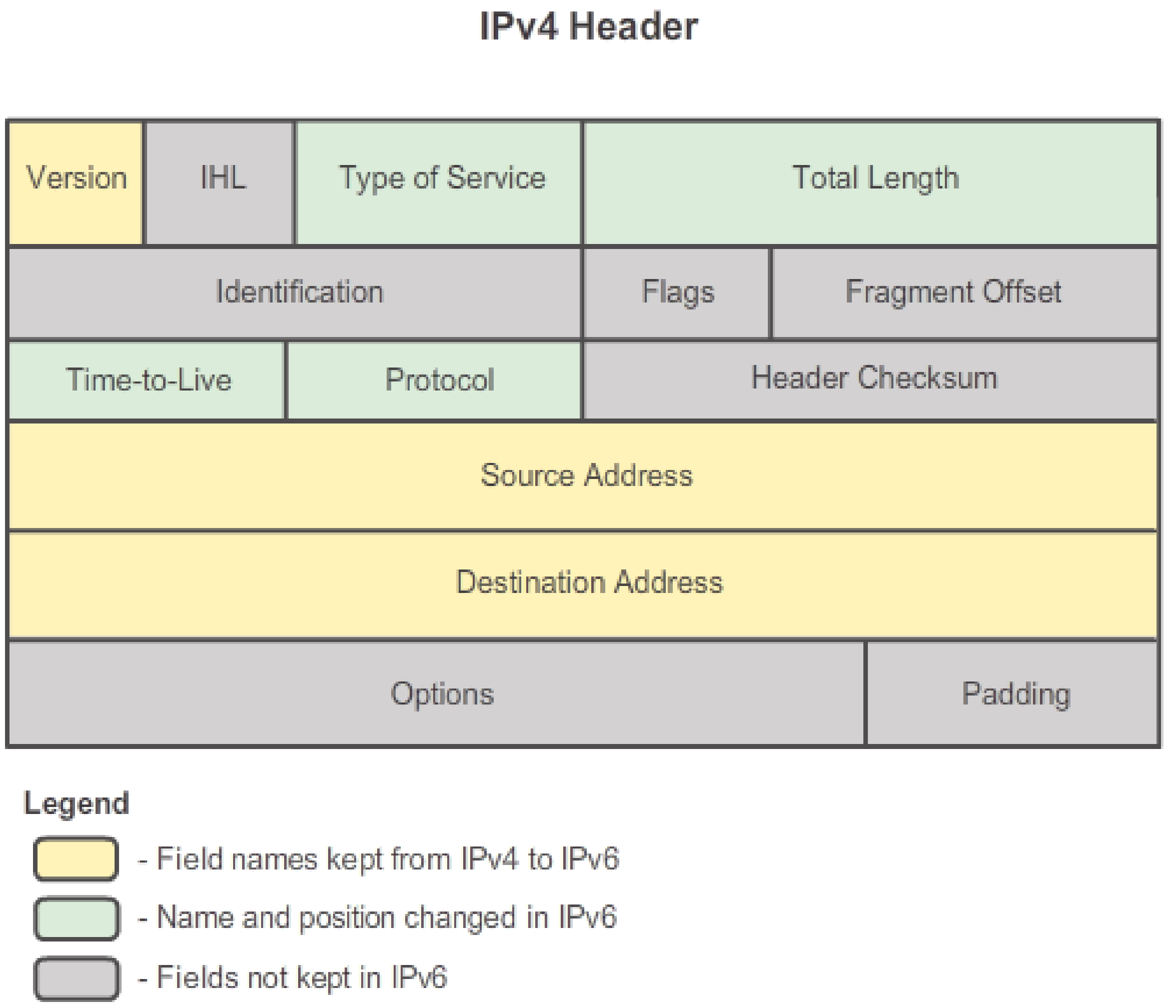
Legend

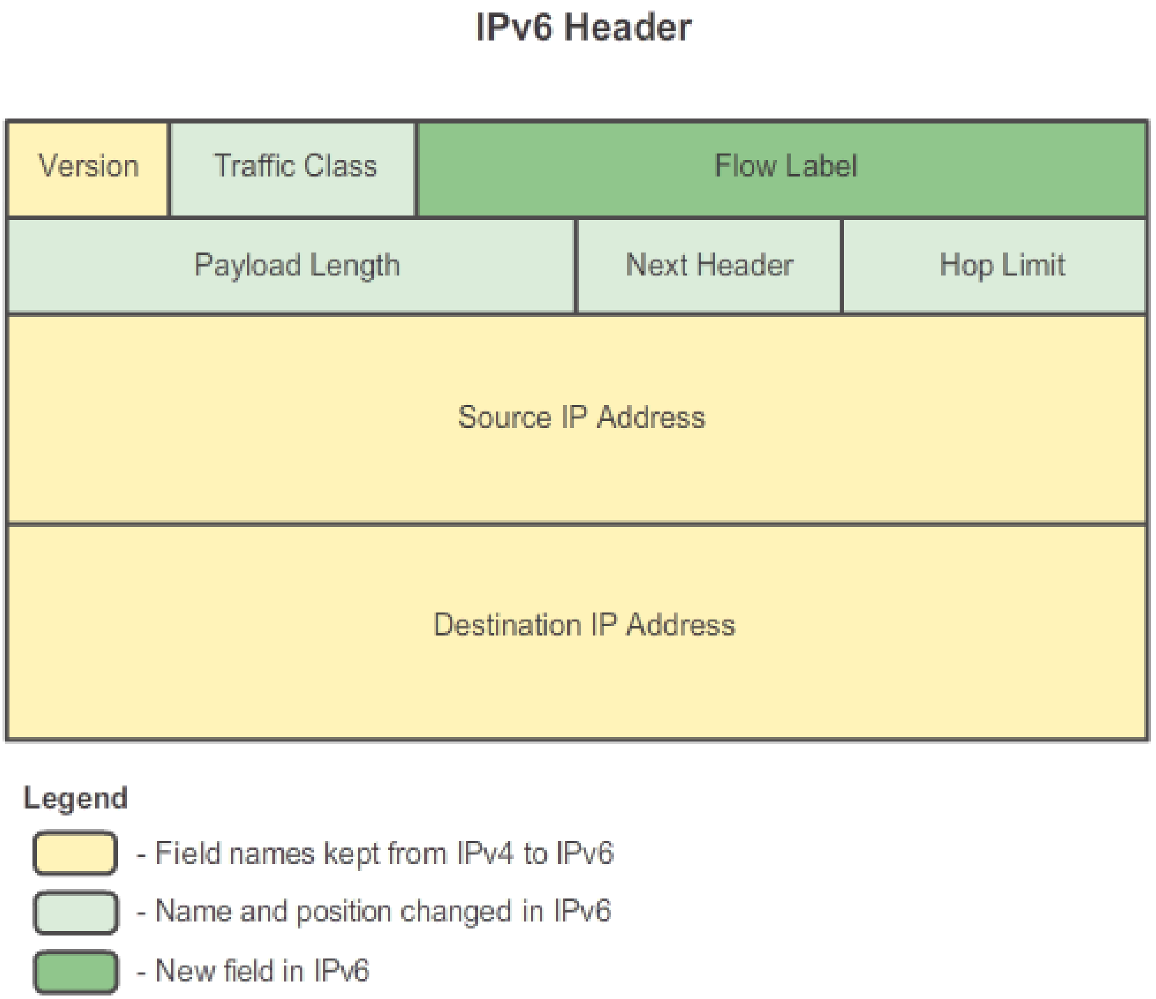
- There are 4 billion IPv4 addresses
- There are 340 undecillion IPv6 addresses

Improvements that IPv6 provides include:

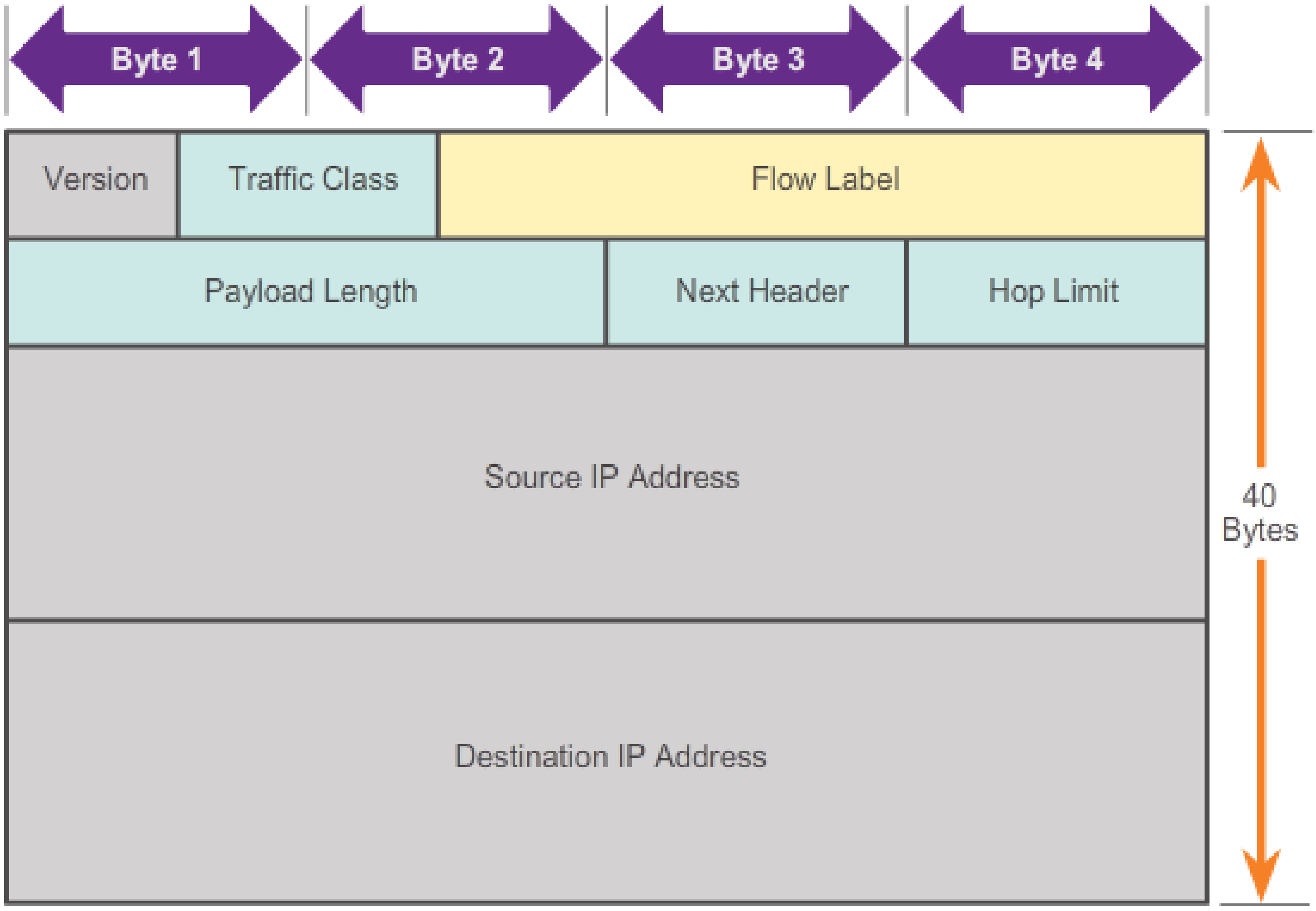
- Increased addresses
- Improved packet
- Eliminates the need for NAT
- Integrated security - IPv6 natively supports authentication and privacy capabilities

6.1.4.3 Encapsulating IPv6

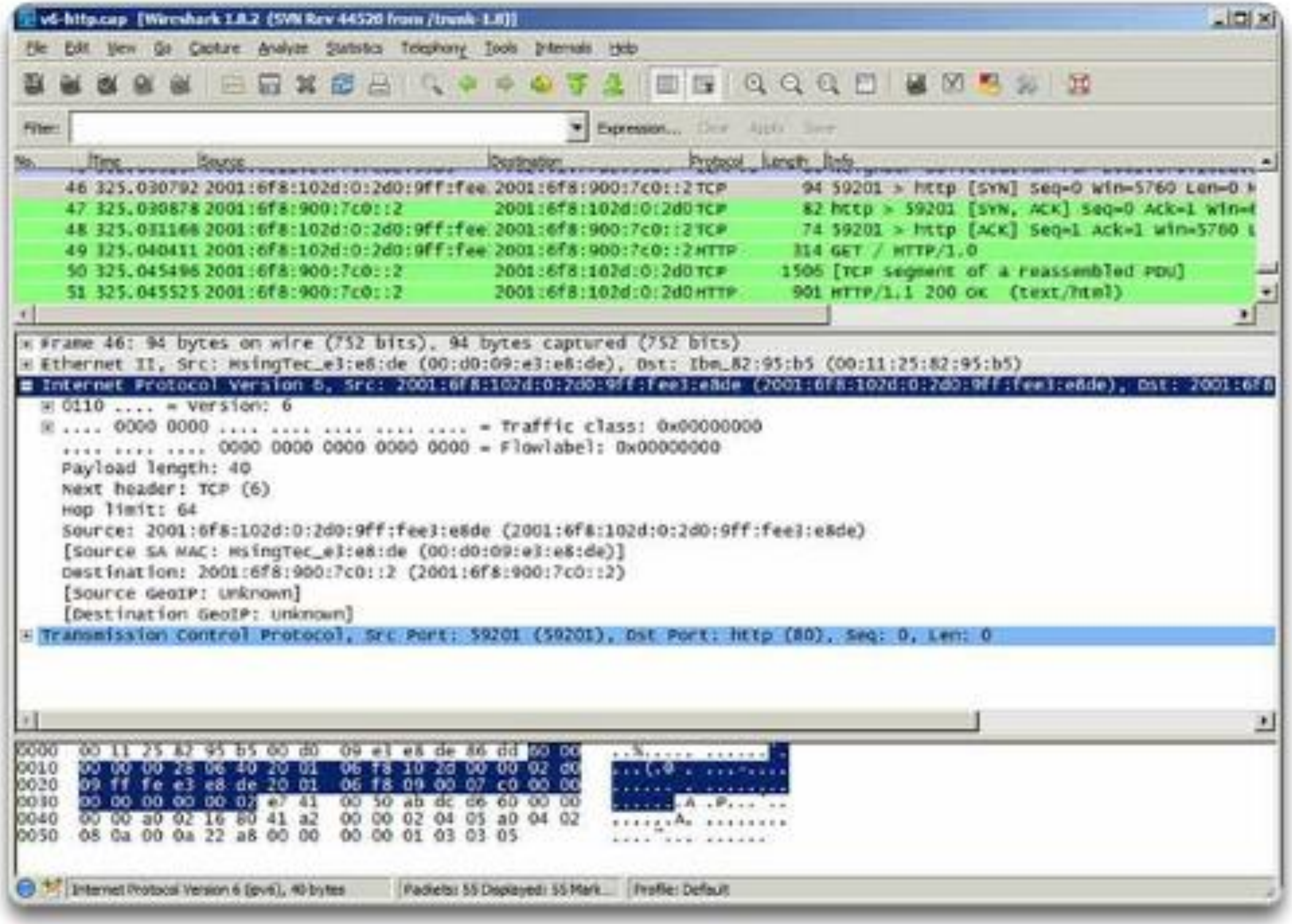




6.1.4.4 IPv6 Packet Header



6.1.4.5 Sample IPv6 Header



When viewing IPv6 Wireshark captures, notice that the IPv6 header has markedly fewer fields than an IPv4 header. This makes the IPv6 header easier and quicker for the router to process.

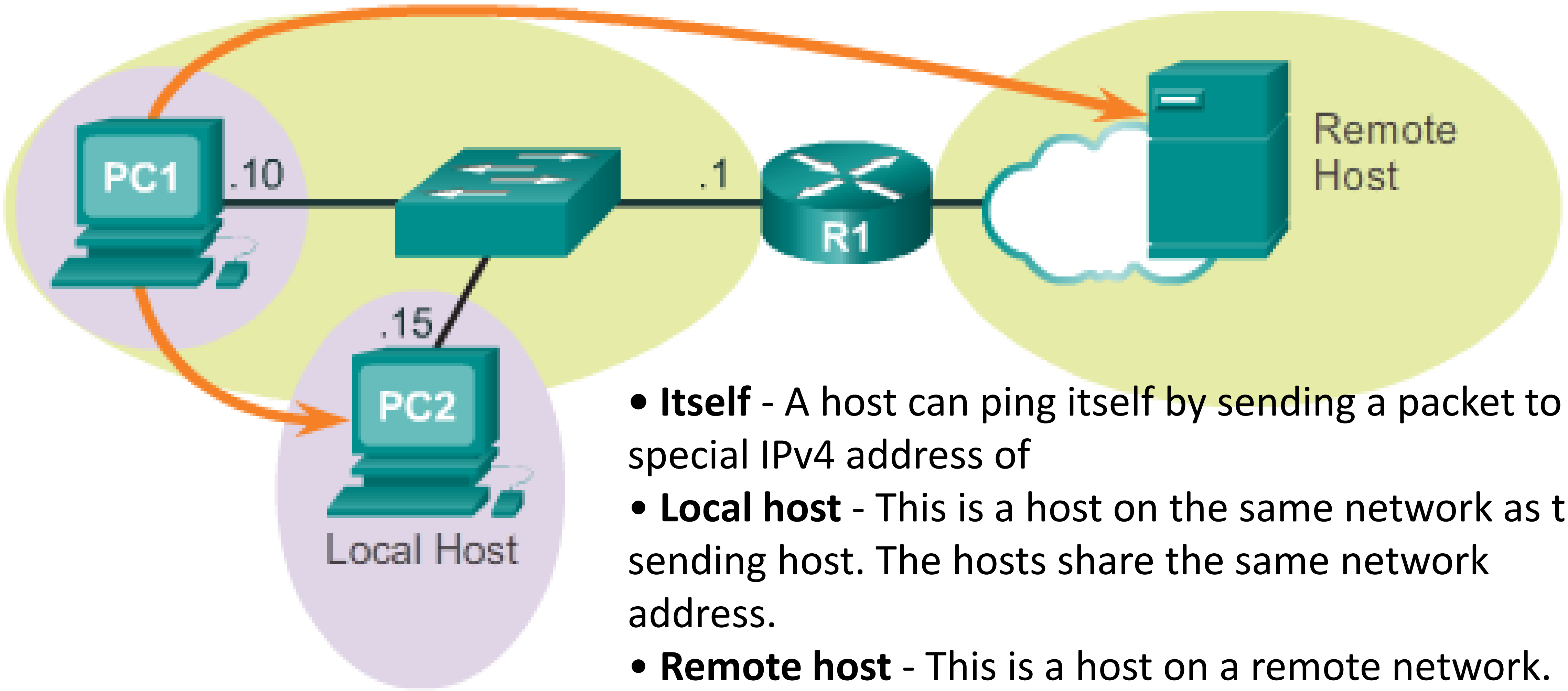
The IPv6 address itself looks very different. Because of the larger 128-bit IPv6 addresses, the hexadecimal numbering system is used to simplify the address representation. IPv6 addresses use colons to separate entries into a series of 16-bit hexadecimal blocks.

6.1.4.6 Activity - IPv6 Header Fields

IPv6 Header Fields

Version Is always set to 0110	**Payload Length** Identifies the packet fragment size
Traffic Class Classifies packets for congestion control	**Next Header** Identifies the application type to the upper-layer protocol
Flow Label Can be set to use the same pathway flow so that packets are not reordered upon delivery	**Hop Limit** When this value reaches 0, the sender is notified that the packet was not delivered

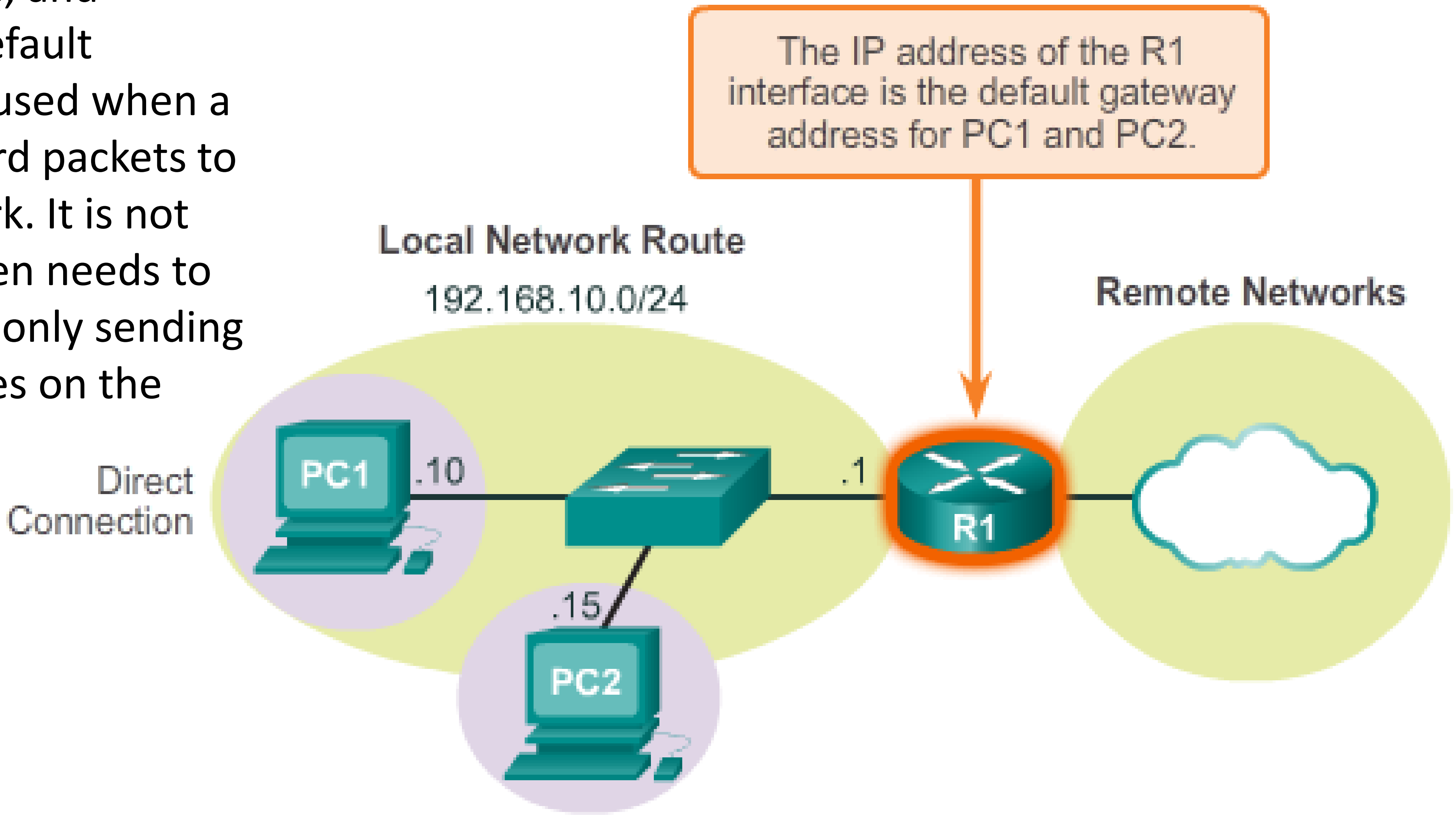
6.2.1.1 Host Forwarding Decision



- **Itself** - A host can ping itself by sending a packet to a special IPv4 address of
- **Local host** - This is a host on the same 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

It is important to note that the default route, and therefore, the default gateway, is only used when a host must forward packets to a remote network. It is not required, nor even needs to be configured, if only sending packets to devices on the local network



6.2.1.3 IPv4 Host Routing Table


```
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 –**
- **IPv4 Route Table –**
- **IPv6 Route Table -**

6.2.1.4 IPv4 Host Routing Entries


```
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>
```

To help simplify the output, the destination networks can be grouped into five sections as identified by the highlighted areas on the following slide:

0.0.0.0

The local default route; that is, all packets with destinations that do not match other specified addresses in the routing table are forwarded to the gateway. Therefore, all non-matching destination routes are sent to the gateway with IP address **192.168.10.1 (R1**) exiting from the interface with IP address 192.168.10.10. Note that the final destination address specified in the packet does not change; rather, the host simply knows to forward the packet to the gateway for further processing.

127.0.0.0 – 127.255.255.255

These loopback addresses all relate to the direct connection and provide services to the local host.

192.168.10.0 - 192.168.10.255

These addresses all relate to the host and local network. All packets with destination addresses that fall into this category will exit out of the 192.168.10.10 interface.

- 192.168.10.0 - The local network route address; represents all computers on the 192.168.10.x network.
- 192.168.10.10 - The address of the local host.
- 192.168.10.255 - The network broadcast address; sends messages to all hosts on the local network route.

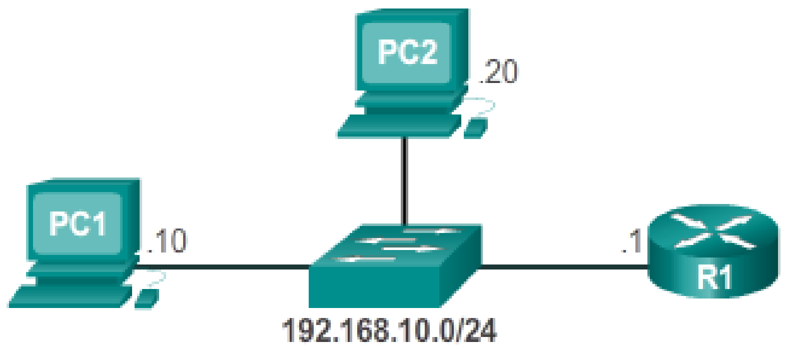
224.0.0.0

These are special multicast class D addresses reserved for use through either the loopback interface (127.0.0.1) or the host IP address (192.168.10.10).

255.255.255.255

The last two addresses represent the limited broadcast IP address values for use through either the loopback interface (127.0.0.1) or the host IP address (192.168.10.10). These addresses can be used to find a DHCP server before the local IP is determined

6.2.1.5 Sample IPv4 Host Routing Table

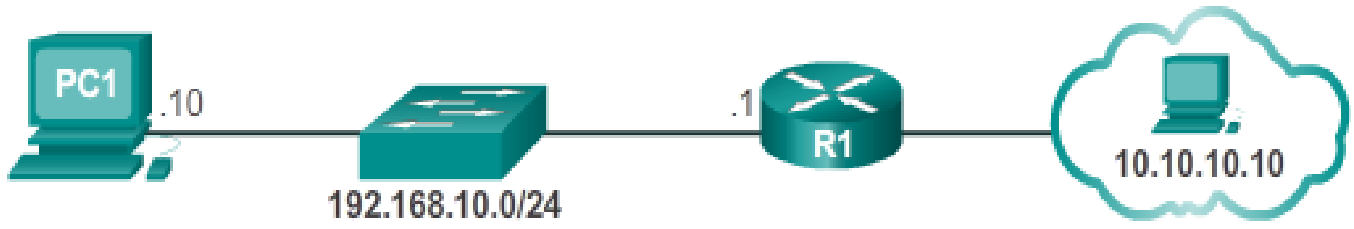



```
C:\Users\PC1> netstat -r

<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>
```

if PC1 wanted to send a packet to 192.168.10.20, it would:

1. Consult the IPv4 Route Table.
2. Match the destination IP address with the 192.168.10.0 Network Destination entry to reveal that the host is on the same network (On-link).
3. PC1 would then send the packet toward the final destination using its local interface (192.168.10.10).

6.2.1.5 Sample IPv4 Host Routing Table

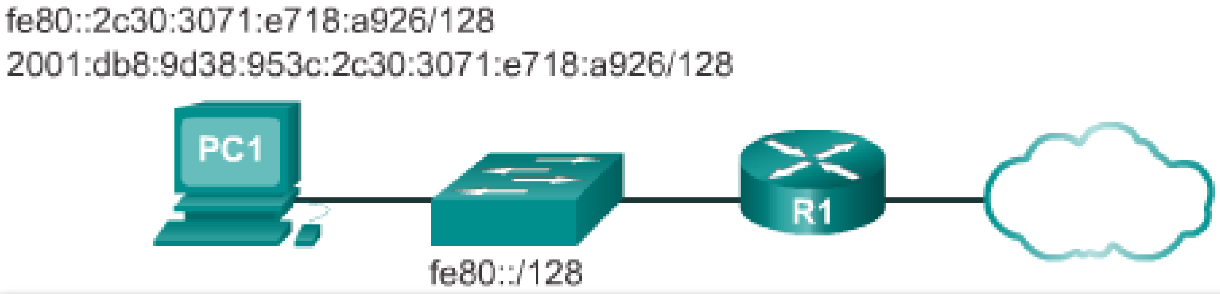



```
C:\Users\PC1> netstat -r

 <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>
```

If PC1 wanted to send a packet to a remote host located at 10.10.10.10, it would:

1. Consult the IPv4 Route Table.
2. Find that there is no exact match for the destination IP address.
3. Choose the local default route (0.0.0.0) to reveal that it should forward the packet to the 192.168.10.1 gateway address.
4. PC1 then forwards the packet to the gateway for using its local interface (192.168.10.10). The gateway device then determines the next path for the packet to reach the final destination address of 10.10.10.10.

6.2.1.6 Sample IPv6 Host Routing Table




```
C:\Users\PC1> netstat -r
<Output omitted>
IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
 16     58 ::/0                     On-link
  1    306 ::1/128                  On-link
 16     58 2001::/32                On-link
 16    306 2001:0:9d38:953c:2c30:3071:e718:a926/128
                                    On-link
 15    281 fe80::/64                On-link
 16    306 fe80::/64                On-link
 16    306 fe80::2c30:3071:e718:a926/128
                                    On-link
 15    281 fe80::b1ee:c4ae:a117:271f/128
                                    On-link
  1    306 ff00::/8                 On-link
 16    306 ff00::/8                 On-link
 15    281 ff00::/8                 On-link
===========================================================================
<Output omitted>
```

The IPv6 Route Table section displays four columns which identify:

- **If - Lists the interface** numbers from the Interface List section of the netstat –r command. The interface numbers correspond to the network capable interface on the host, including Ethernet, Wi-Fi, and Bluetooth adapters.
- **Metric** - Lists the cost of each route to a destination. Lower numbers indicate preferred routes.
- **Network Destination** - Lists the reachable networks.
- **Gateway** - Lists the address used by the local host to forward packets to a remote network destination. On-link indicates that the host is currently connected to it.

6.2.1.7 Activity - Identify Elements of a Host Routing Table Entry

Interactive Activity – Identify Elements of a Host Routing Table Entry

A partial host routing table entry is shown. Each section of the entry is identified by a circled letter above it.

Select the correct routing table entry segment for each output statement by clicking the appropriate column.

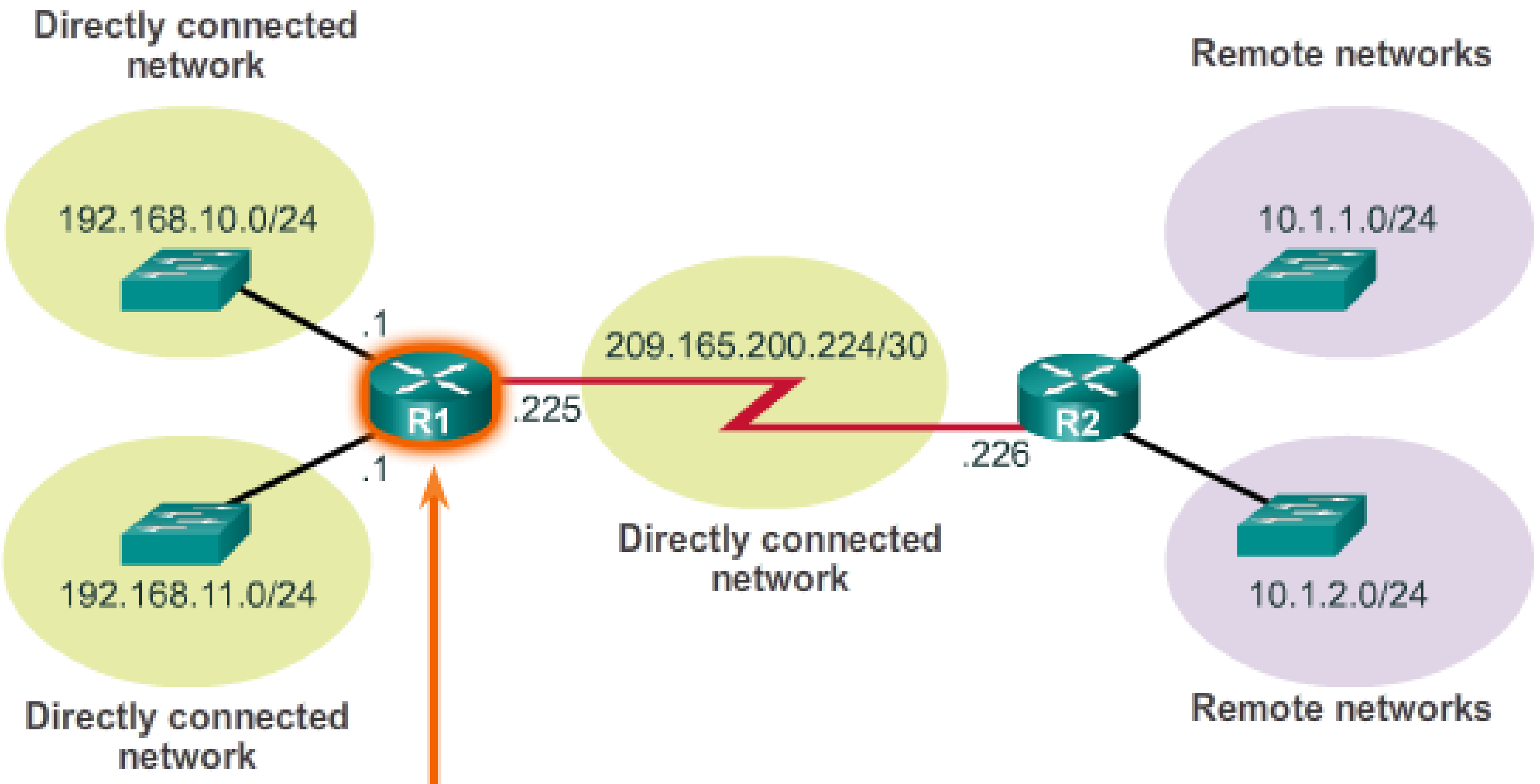
Correct

You have successfully chosen the correct host routing table entry as described.

```
C:\Documents and Settings\cisco>netstat -r
Route Table
===========================================================================
<Output omitted>
          A                  B                 C                D           E
===========================================================================
Active Routes:
Network Destination           Netmask          Gateway        Interface  Metric
          0.0.0.0             0.0.0.0      192.168.1.1    192.168.1.100      20
        127.0.0.0           255.0.0.0        127.0.0.1        127.0.0.1       1
      192.168.1.0       255.255.255.0    192.168.1.100    192.168.1.100      20
    192.168.1.100     255.255.255.255        127.0.0.1        127.0.0.1      20
```

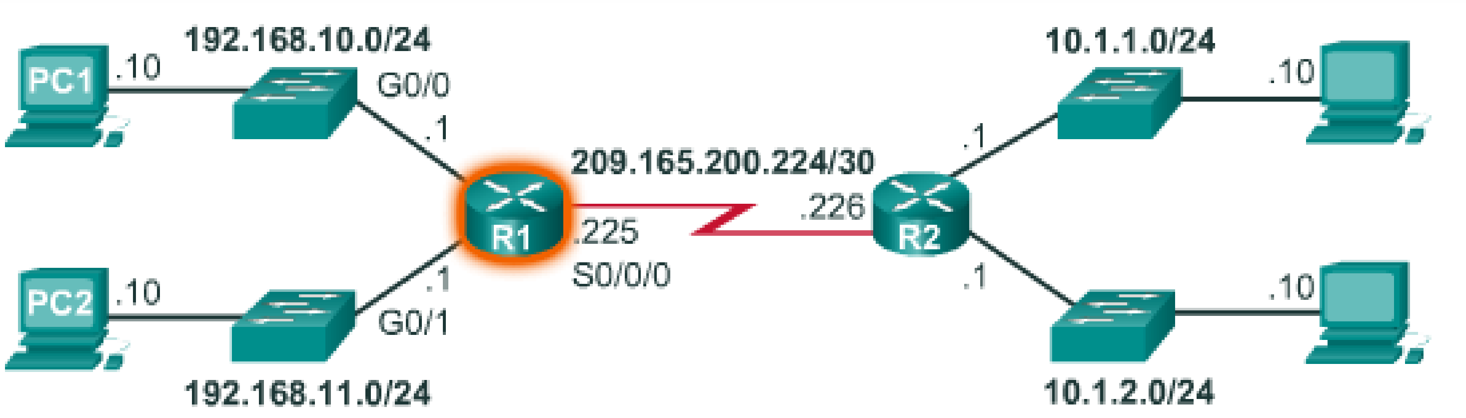
	A	B	C	D	E
1. The physical interface IP address used to send the packet to the gateway.				✓	
2. The route cost – lower numbers are best.					✓
3. The reachable networks available.	✓				
4. The network address is found in this column.	✓				

6.2.2.1 Router Packet Forwarding Decision



R1 has three directly connected networks: 192.168.10.0/24, 192.168.11.0/24, and 209.165.200.224/30. R1 also has two remote networks that it can learn about from R2: 10.1.1.0/24 and 10.1.2.0/24.

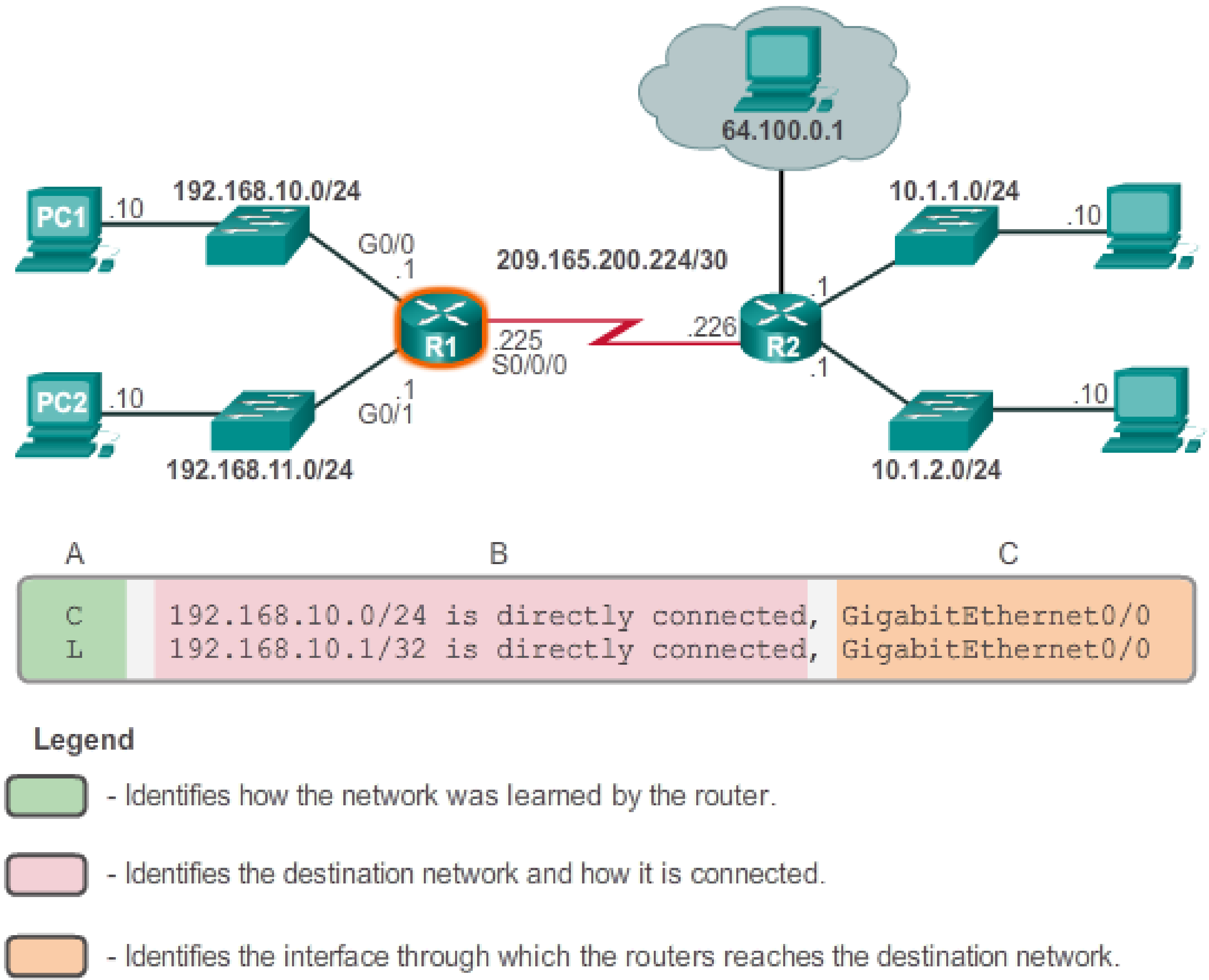
6.2.2.2 IPv4 Router Routing Table




```
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
     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
```

When a packet arrives at the router interface, the router examines the packet header to determine the destination network. If the destination network matches a route in the routing table, the router forwards the packet using the information specified in the routing table. If there are two or more possible routes to the same destination, the metric is used to decide which route appears on the routing table.

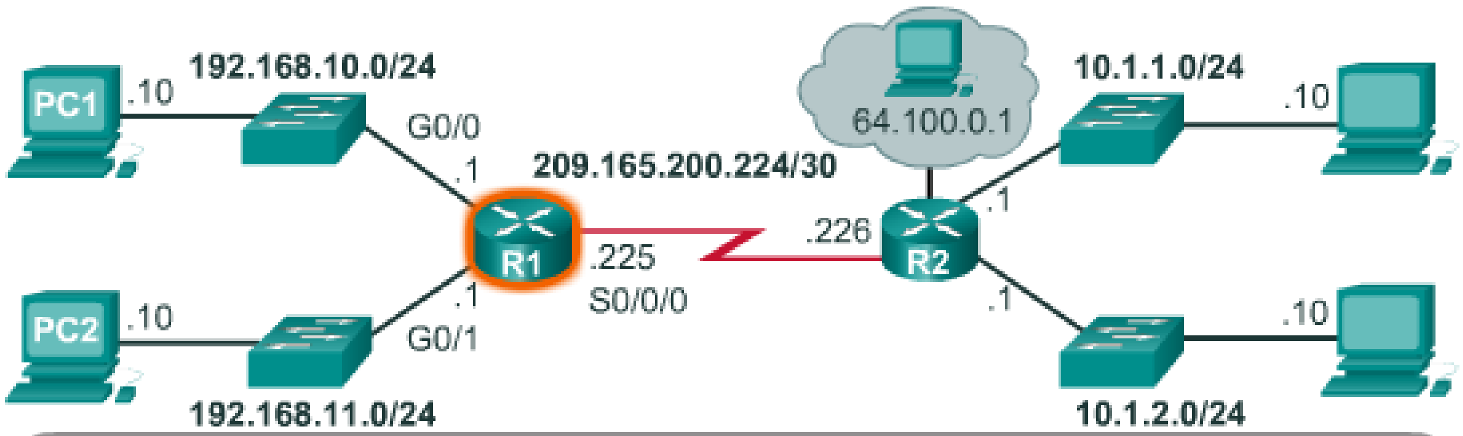
6.2.2.3 Directly Connected Routing Table Entries



The routing table stores information about both directly-connected and remote routes. As with directly connected networks, the route source identifies how the route was learned. For example, common codes for remote networks include:

- S - Identifies that the route was manually created by an administrator to reach a specific network. This is known as a static route.
- D - Identifies that the route was learned dynamically from another router using the Enhanced Interior Gateway Routing Protocol (EIGRP).
- O - Identifies that the route was learned dynamically from another router using the Open Shortest Path First (OSPF) routing protocol.

6.2.2.4 Remote Network Routing Table Entries

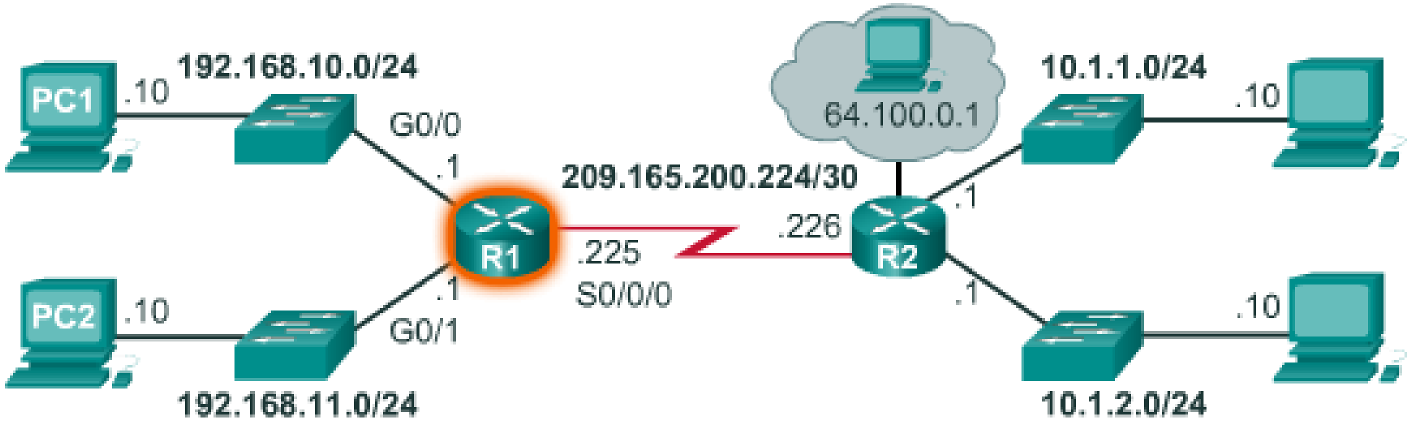


D 10.1.1.0/24 [90/2170112] via 209.165.200.226, 00:00:05, Serial0/0/0

Legend

- Identifies how the network was learned by the router.
- Identifies the destination network.
- Identifies the administrative distance (trustworthiness) of the route source.
- Identifies the metric to reach the remote network.
- Identifies the next hop IP address to reach the remote network.
- Identifies the amout of elapsed time since the route was last heard from.
- Identifies the outgoing interface on the router to reach the destination network.

6.2.2.5 Next-Hop Address




```
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

     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
```

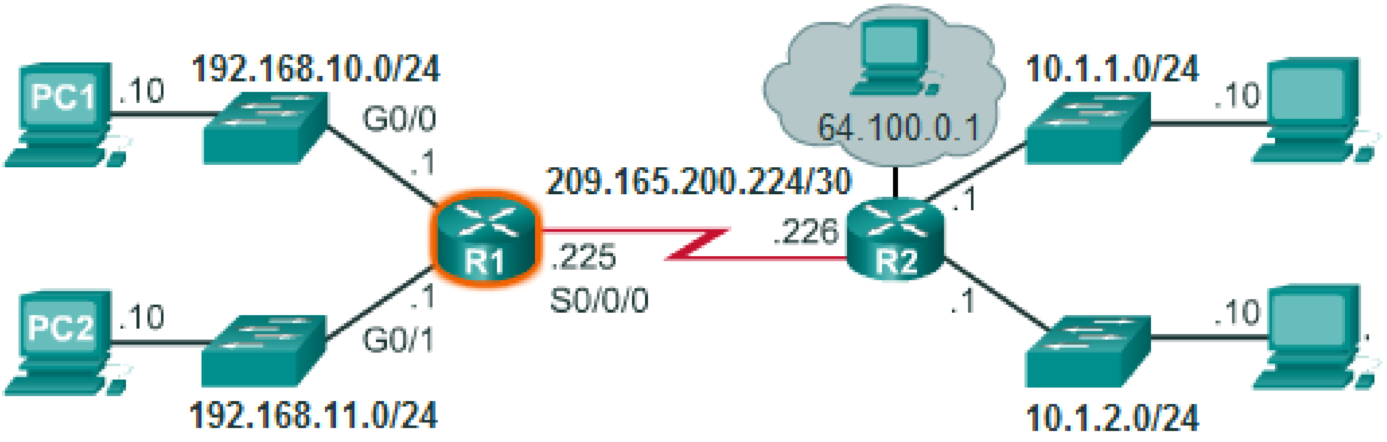
Packets cannot be forwarded by the router without a route for the destination network in the routing table.

If a route representing the destination network is not in the routing table, the packet is dropped (that is, not forwarded).

However, just as a host can use a default gateway to forward a packet to an unknown destination, a router can also be configured to use a default static route to create a Gateway of Last Resort.

The Gateway of Last Resort will be covered in more detail in the CCNA Routing course

6.2.2.6 Sample Router IPv4 Routing Table




```
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 209.165.200.226 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
```

The following examples illustrate how a host and a router make packet routing decisions by consulting their respective routing tables:

Follow the various routing tables and illustrations to learn how routing works

6.2.2.7 Activity - Identify Elements of a Router Routing Table Entry

Activity – Identify Elements of a Router Routing Table Entry

A partial **router** routing table entry is shown. Each section of the entry is identified by a circled letter above it.

Select the correct routing table entry section for each output.

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.						✓

Correct

You have successfully chosen the correct **router** routing entry as described.

6.2.2.8 Lab - View Host Routing Tables

6.3.1.1 A Router is a Computer

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

- **Branch** - Teleworkers, small business, and medium-size branch sites. Includes Cisco 800, 1900, 2900, and 3900 Integrated Series Routers (ISR) G2 (2nd generation).
- **WAN** - Large businesses, organizations, and enterprises. Includes the Cisco Catalyst 6500 Series Switches and the Cisco Aggregation Service Router (ASR) 1000.
- **Service Provider** - Large service providers. Includes Cisco ASR 1000, Cisco ASR 9000, Cisco XR 12000, Cisco CRS-3 Carrier Routing System, and 7600 Series routers.

The focus of CCNA certification is on the branch family of routers. The figure displays the Cisco 1900, 2900, and 3900 ISR G2 family of routers.

Regardless of their function, size or complexity, all router models are essentially computers. Just like computers, tablets, and smart devices, routers also require:

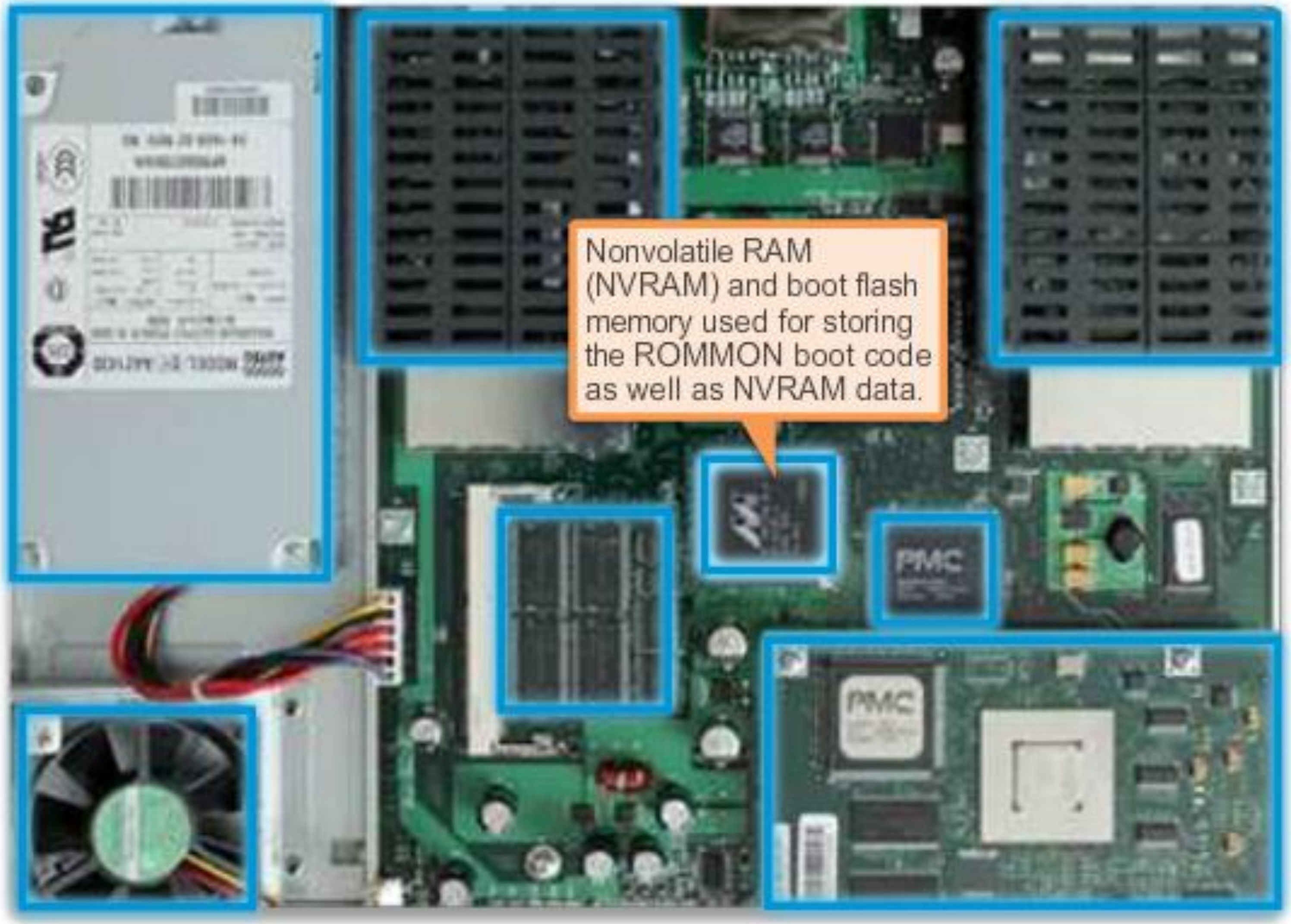
6.3.1.2 Router CPU and OS

The CPU requires an OS to provide routing and switching functions. The Cisco Internetwork Operating System (IOS) is the system software used for most Cisco devices regardless of the size and type of the device. It is used for routers, LAN switches, small wireless access points, large routers with dozens of interfaces, and many other devices.

6.3.1.3 Router Memory

Memory	Volatile / Non-Volatile	Stores
RAM	Volatile	• Running IOS • Running configuration file • IP routing and ARP tables • Packet buffer
ROM	Non-Volatile	• Bootup instructions • Basic diagnostic software • Limited IOS
NVRAM	Non-Volatile	• Startup configuration file
Flash	Non-Volatile	• IOS • Other system files

6.3.1.4 Inside a Router

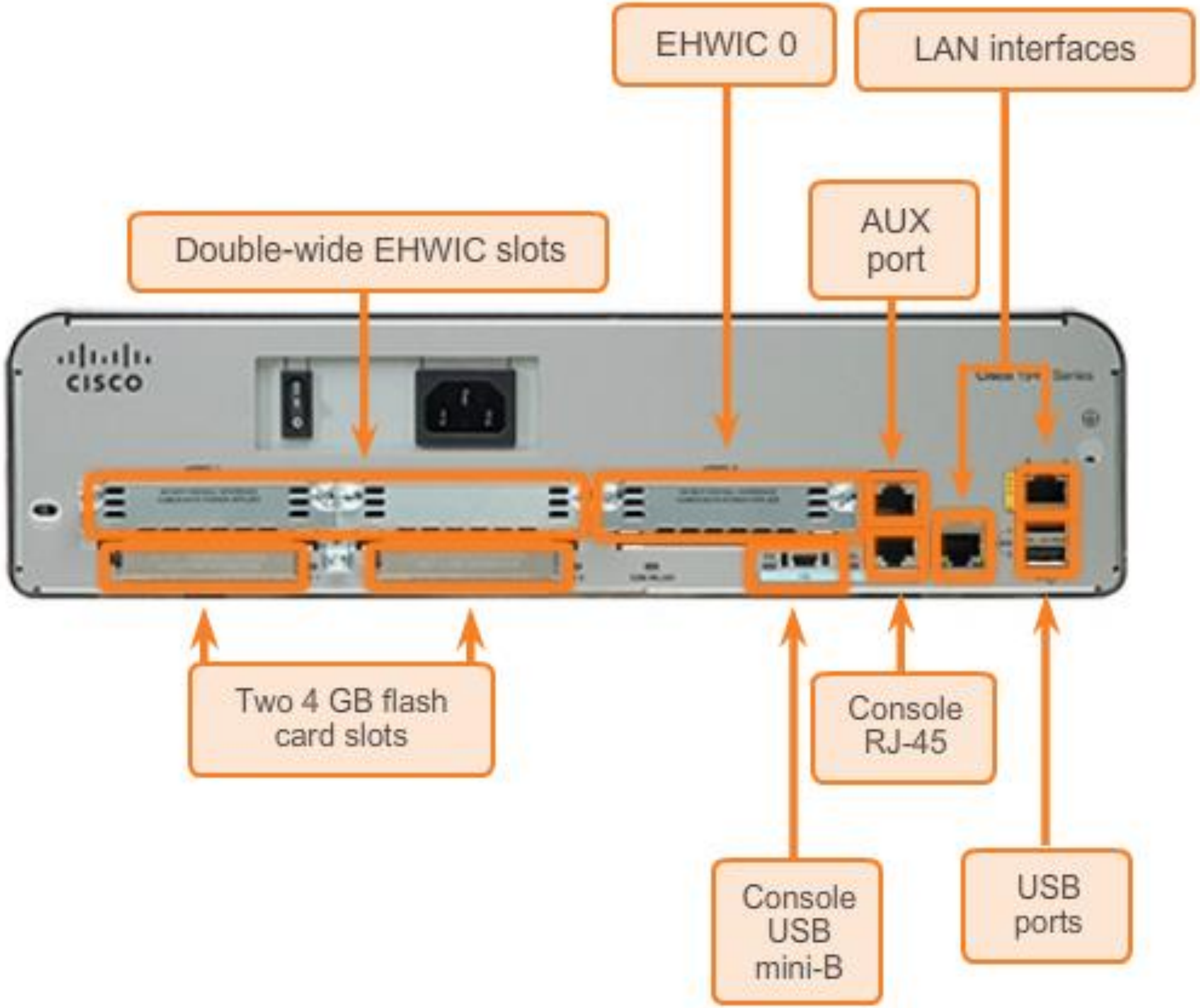


Click the highlighted areas for more information.

Although there are several different types and models of routers, every router has the same general hardware components.

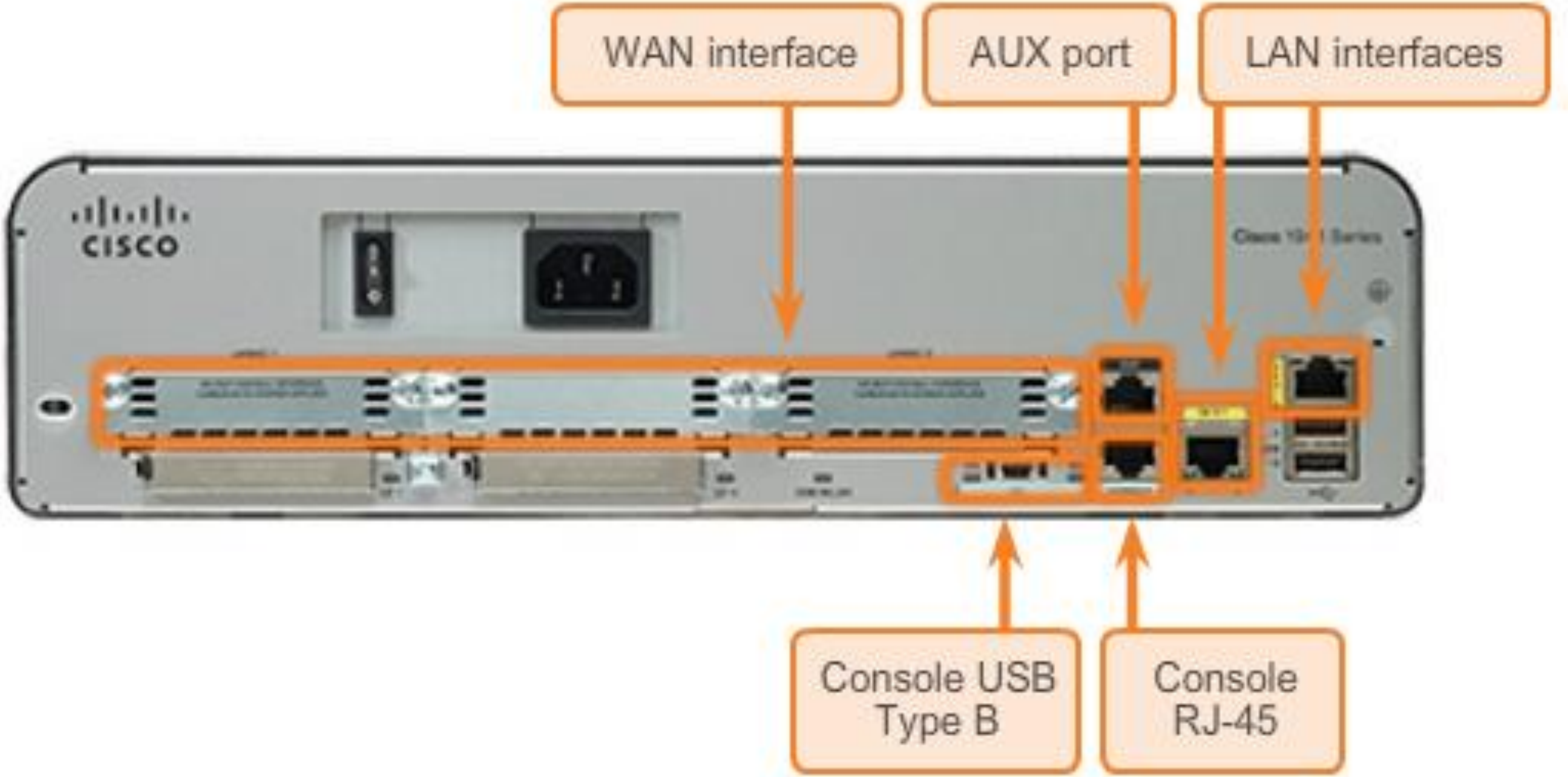
The figure shows the inside of a Cisco 1841 first generation ISR. Click the components to see a brief description of the components.

6.3.1.5 Router Backplane

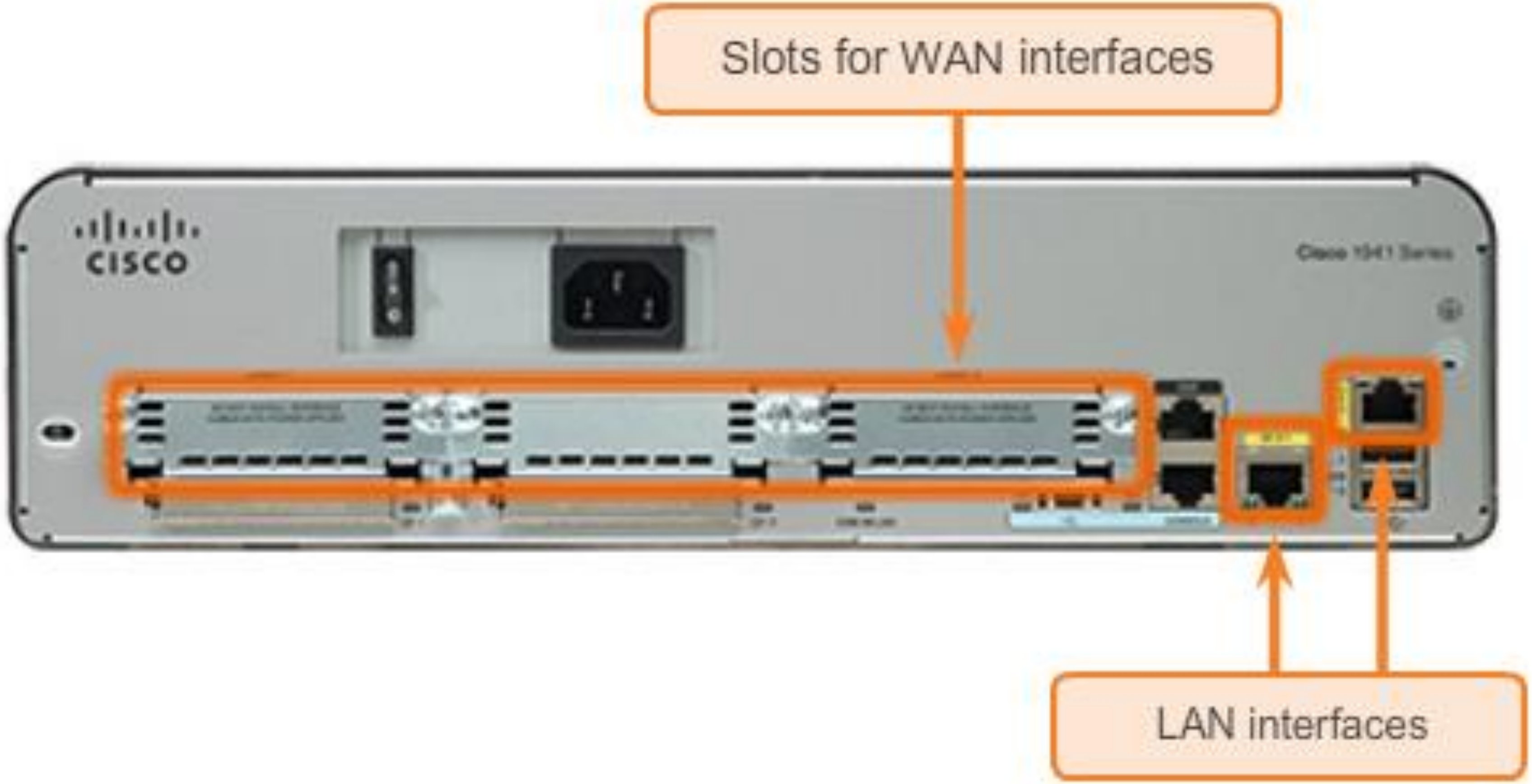


- *Enhanced high-speed WAN interface card (EHWIC) slots - Two slots that provide modularity and flexibility by enabling the router to support different types of interface modules, including Serial, digital subscriber line (DSL), switch port, and wireless.*

6.3.1.6 Connecting to a Router



6.3.1.7 LAN and WAN Interfaces



- **Console** - Uses a low speed serial or USB connection to provide direct connect, out-of-band management access to a Cisco device.
- **Telnet or SSH** - Two methods for remotely accessing a CLI session across an active network interface.
- **AUX port** - Used for remote management of the router using a dial-up telephone line and modem.

6.3.1.8 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.

6.3.1.9 Lab - Exploring Router Physical Characteristics

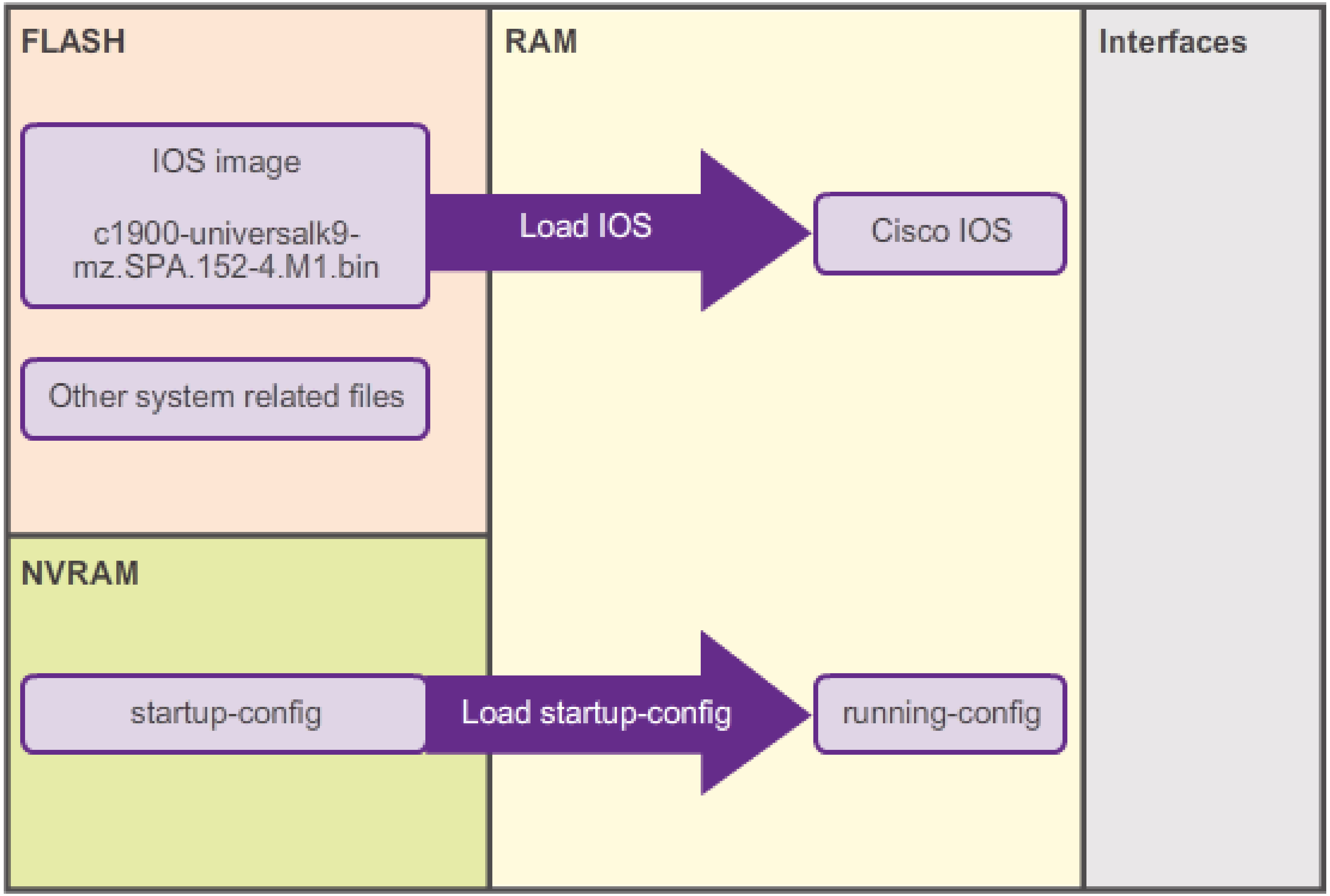
6.3.1.10 Packet Tracer - Exploring Internetworking Devices

Exploring Internetworking Devices

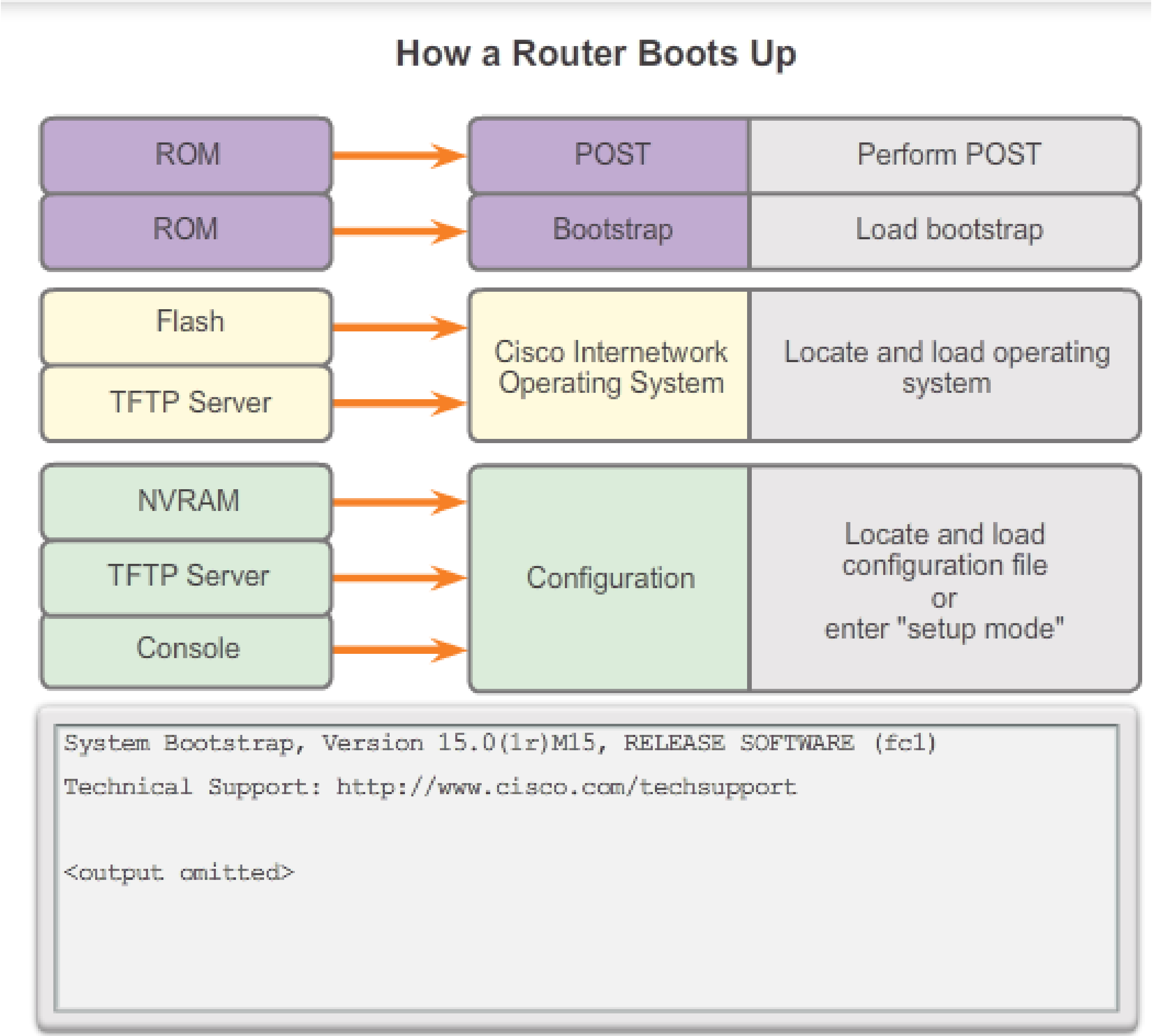
6.3.2.1 Cisco IOS

- The IOS file itself is several megabytes in size and similar to Cisco IOS switches, is stored in flash memory.
- Using flash allows the IOS to be upgraded to newer versions or to have new features added.
- During bootup, the IOS is copied from flash memory into RAM.
- DRAM is much faster than flash; therefore, copying the IOS into RAM increases the performance of the device.

6.3.2.2 Bootset Files



6.3.2.3 Router Bootup Process



The curriculum illustrates the step by step process of booting up

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
```

You can use the show version command to verify and troubleshoot some of the basic hardware and software components of the router. The 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 Router Boot Process

6.3.2.6 Activity - The Router Boot Process

The Router Boot Process

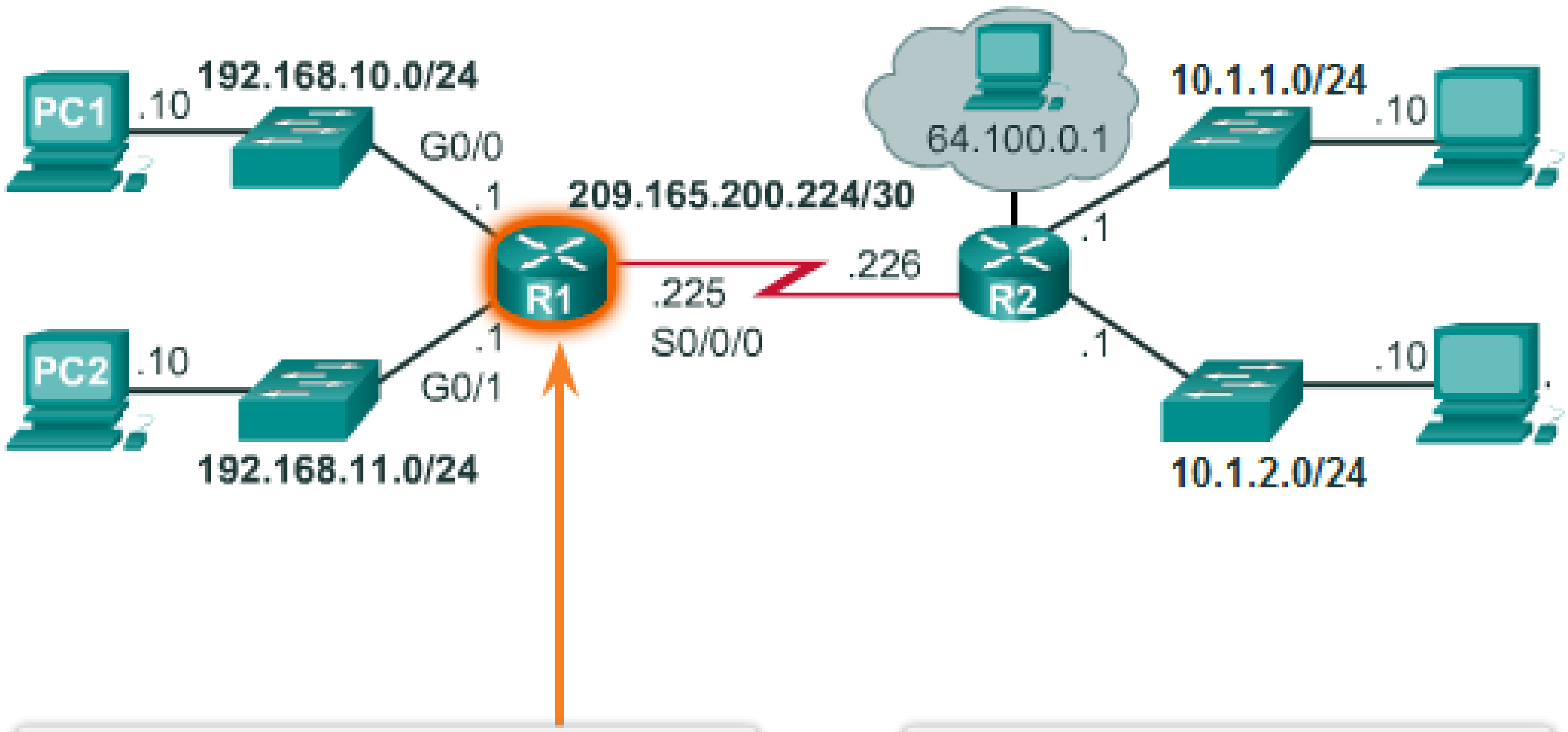
Perform POST (hardware check – performed by built-in ROM chip)

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)

6.4.1.1 Router Configuration Steps

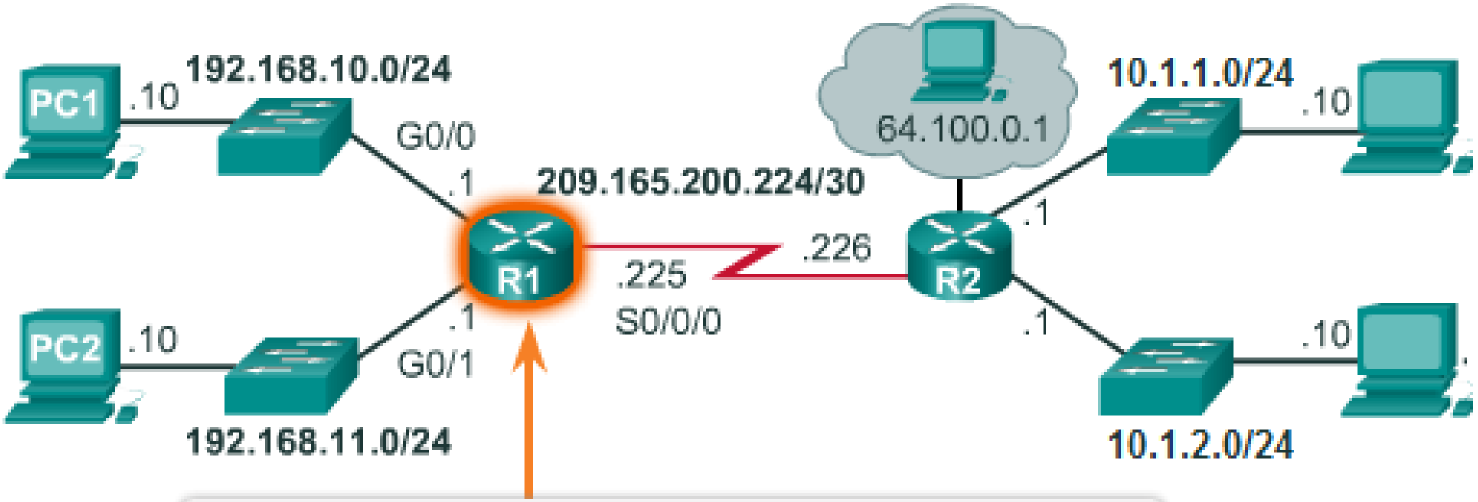



```
Router>enable
Router#configure terminal
Enter configuration
commands, one per line.
End with CNTL/Z.
Router(config)#hostname R1
R1(config)#
```

OR

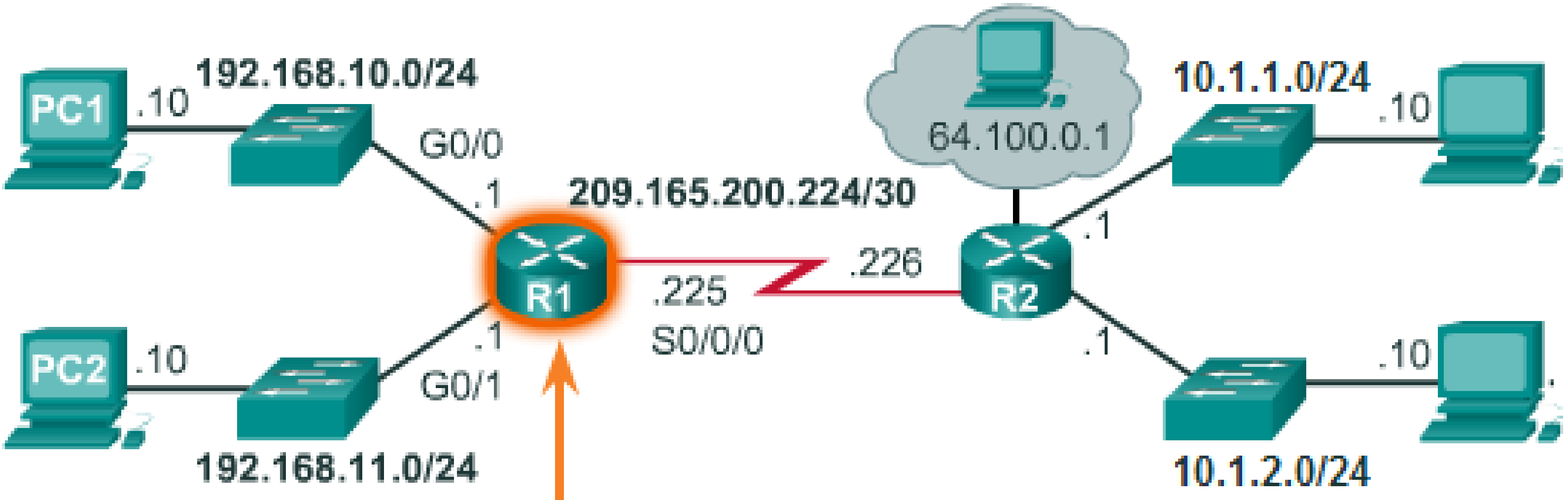
```
Router>en
Router#conf t
Enter configuration
commands, one per line.
End with CNTL/Z.
Router(config)#ho R2
R2(config)#
```

6.4.1.1 Router Configuration Steps



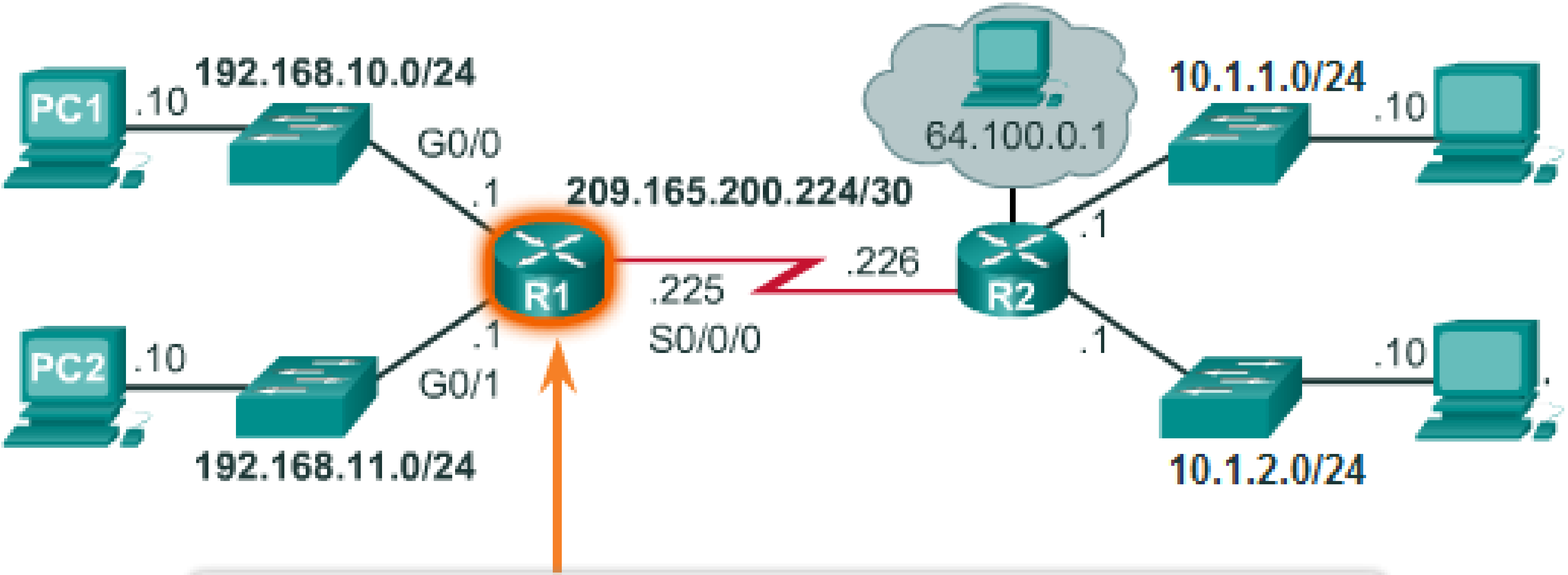

```
R1(config)#enable secret class
R1(config)#
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#
R1(config)#service password-encryption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

6.4.1.1 Router Configuration Steps



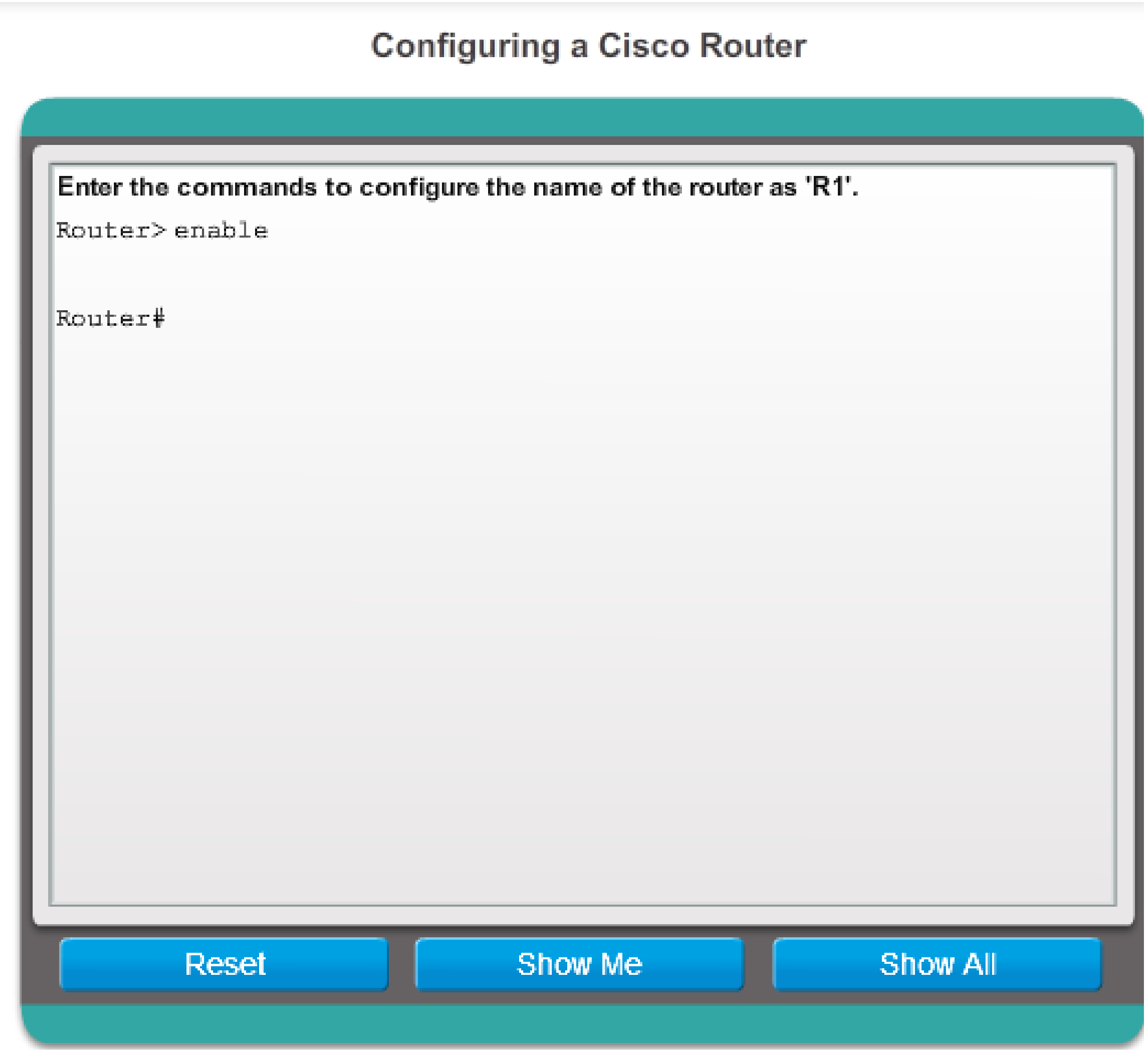

```
R1(config)#banner motd #
Enter TEXT message.  End with the character '#'.

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

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

R1(config)#
```

6.4.1.1 Router Configuration Steps

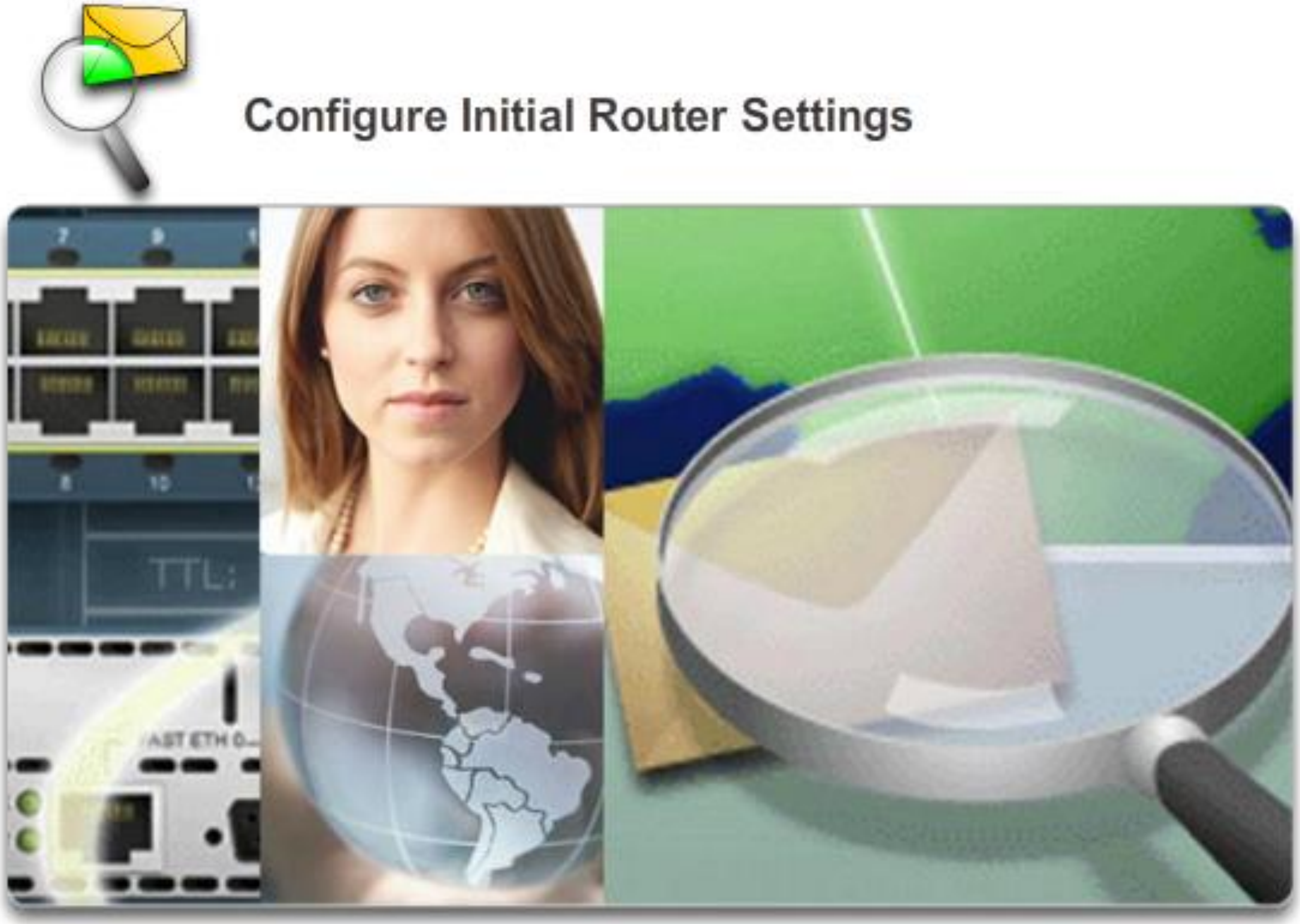



```
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

6.4.1.1 Router Configuration Steps

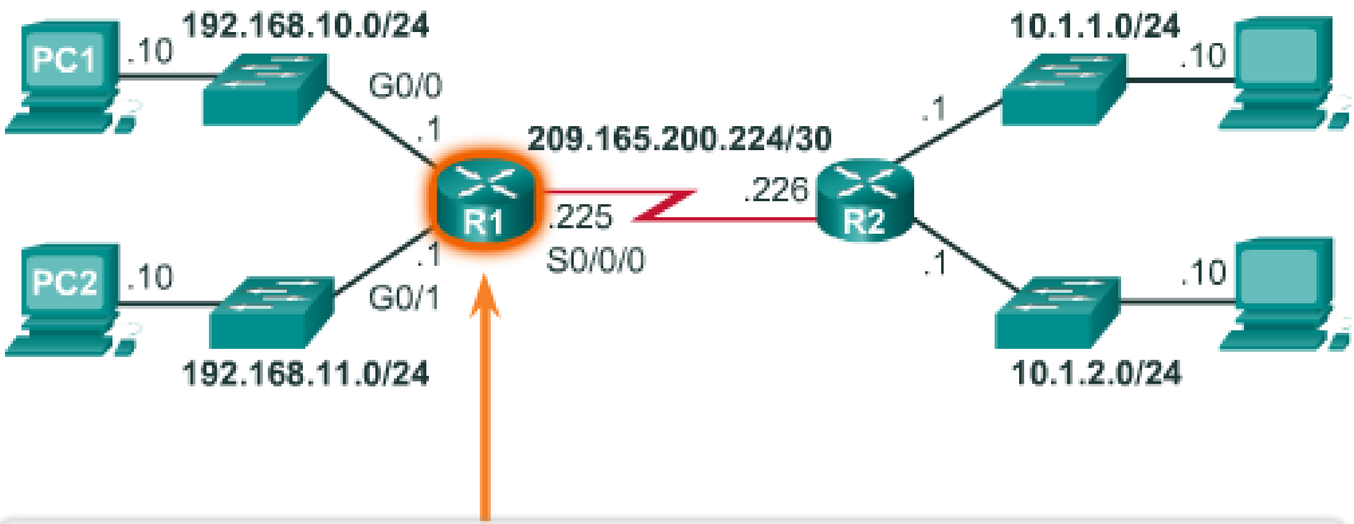


6.4.1.2 Packet Tracer - Configure Initial Router Settings



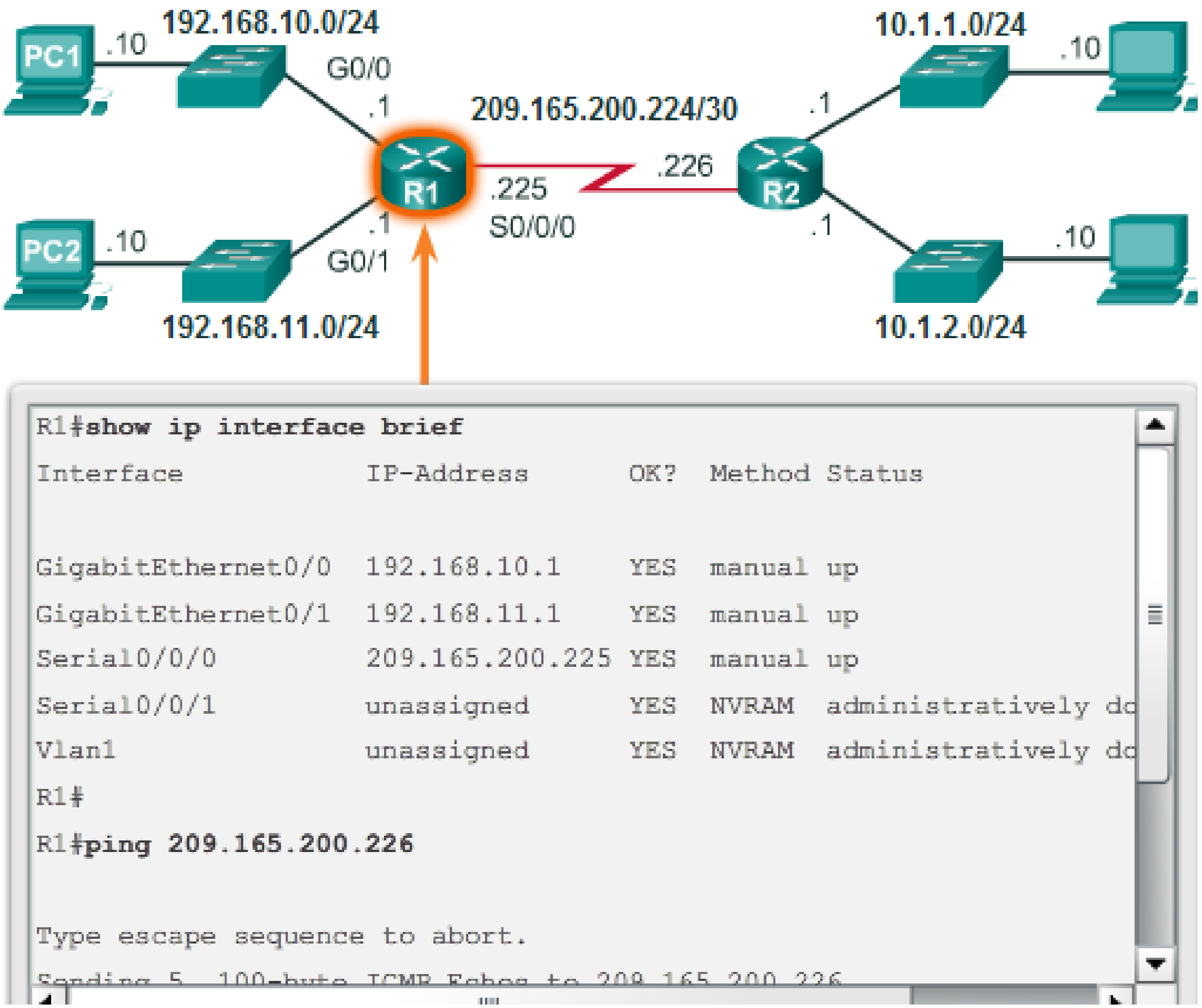
In this activity, you will perform basic router configurations. You will secure access to the CLI and console port using encrypted and plain text passwords. You will also configure messages for users logging into the router. These banners also warn unauthorized users that access is prohibited. Finally,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

6.4.2.1 Configure LAN 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
```

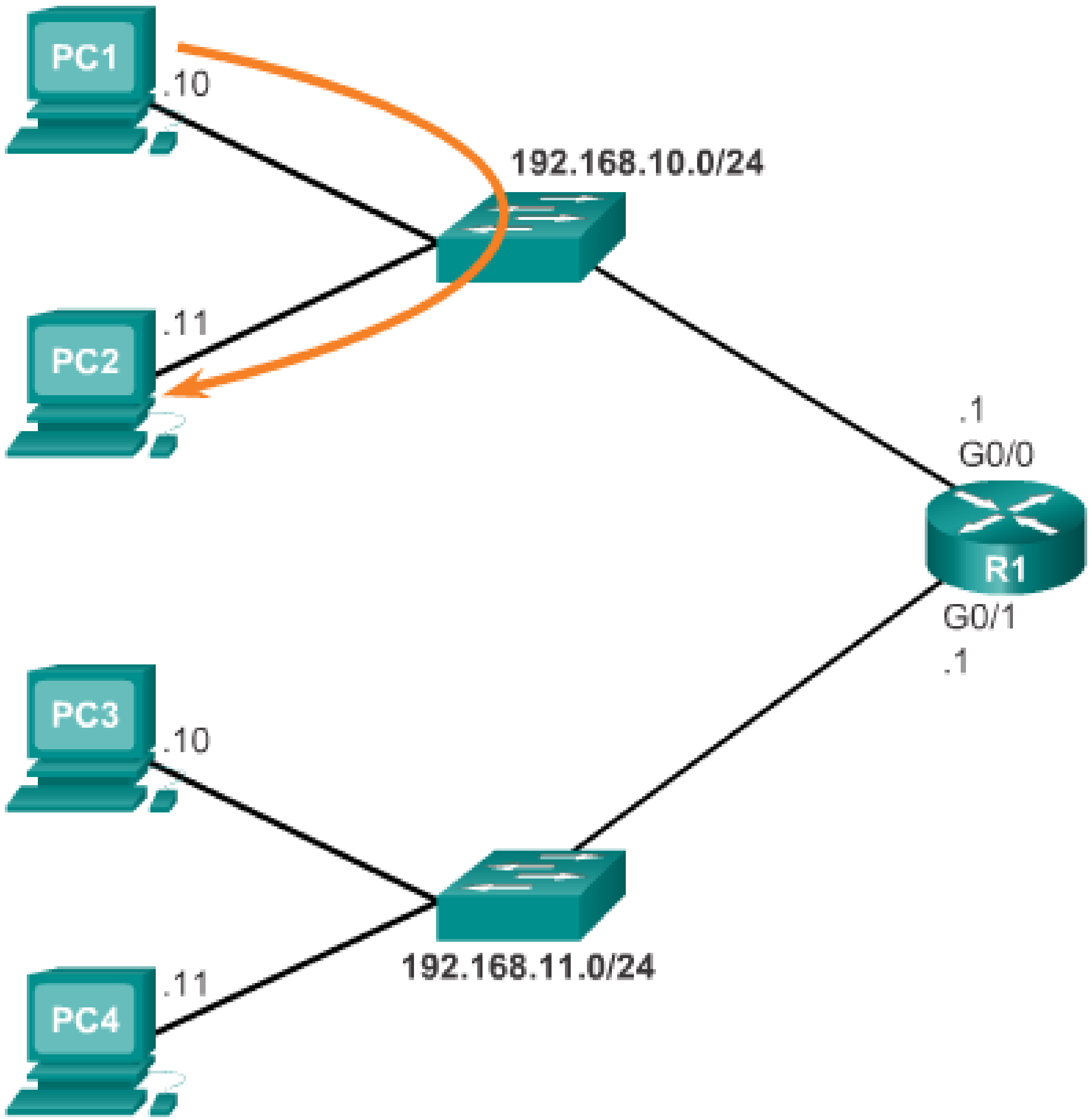
6.4.2.2 Verify Interface Configuration

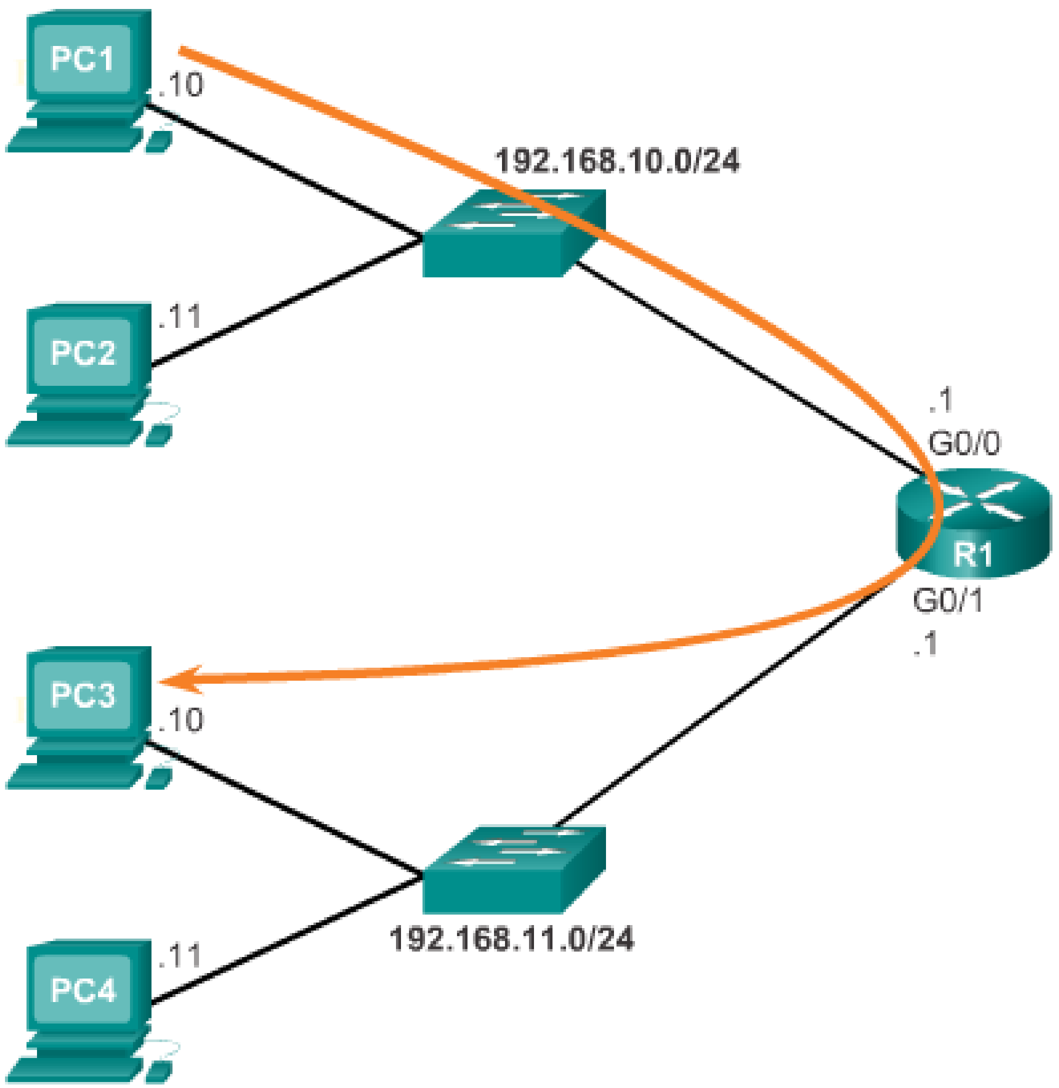


Other interface verification commands include:

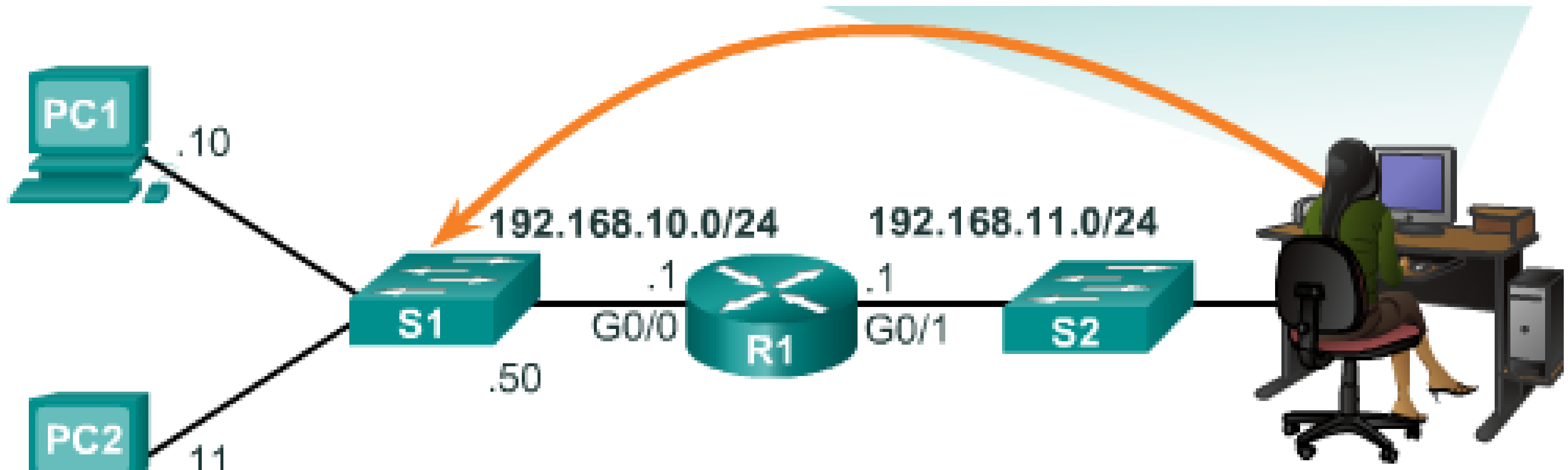
- **show ip route** - Displays the contents of the IPv4 routing table stored in RAM.
- **show interfaces** - Displays statistics for all interfaces on the device.
- **show ip interface** - Displays the IPv4 statistics for all interfaces on a router.

6.4.3.1 Default Gateway on a Host





6.4.3.2 Default Gateway on 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.

A default gateway is used by all devices that require the use of a router to determine the best path to a remote destination. End devices require default gateway addresses, but so do intermediate devices, such as the Cisco IOS switch.

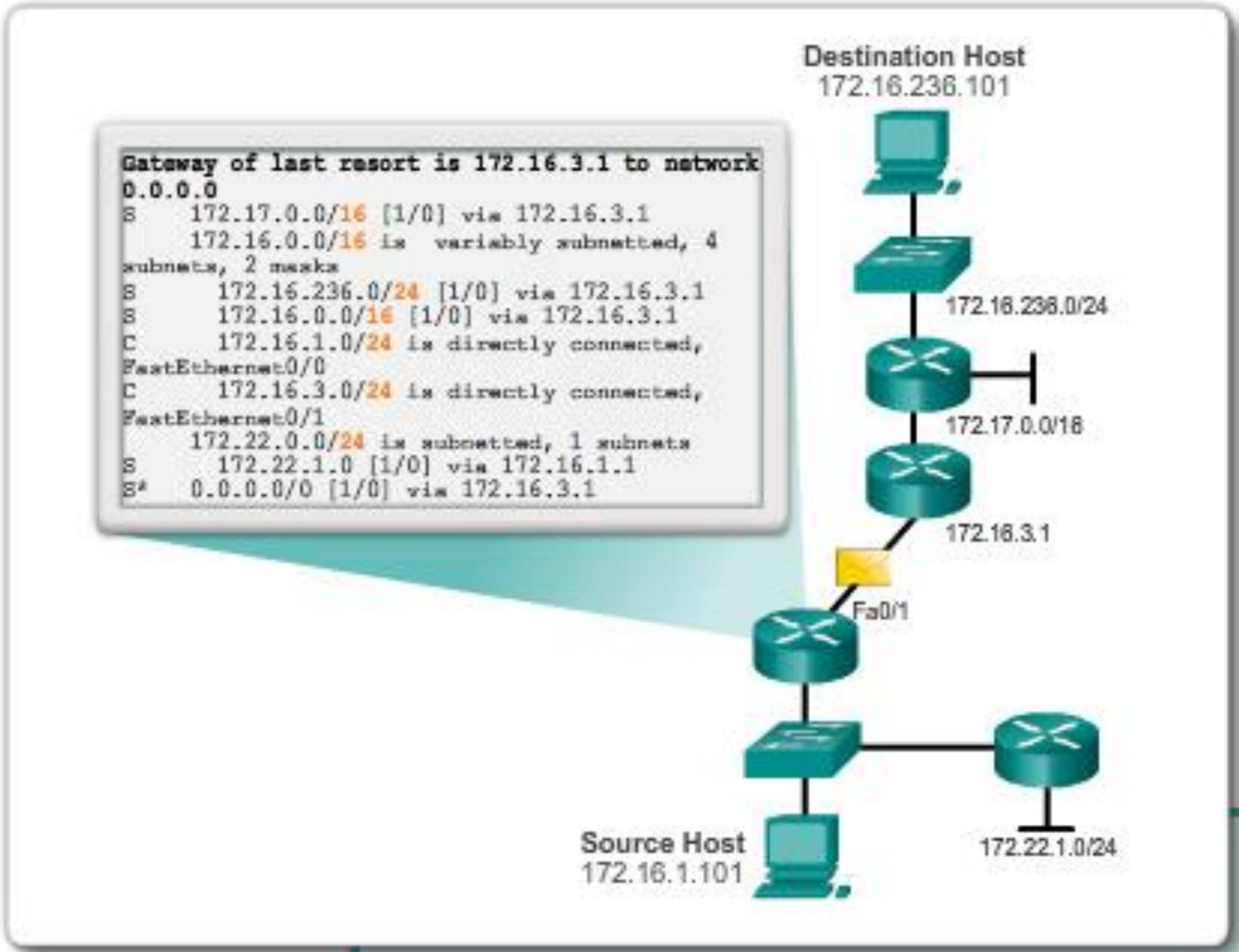
The IP address information on a switch is only necessary to manage the switch remotely. In other words, to be able to telnet to the switch, the switch must have an IP address to Telnet to. If the switch is only accessed from devices within the local network, only an IP address is required.

6.4.3.3 Packet Tracer - Connect a Router to a LAN

6.4.3.4 Packet Tracer - Troubleshooting Default Gateway Issues

6.4.3.5 Lab - Initializing and Reloading a Router and Switch

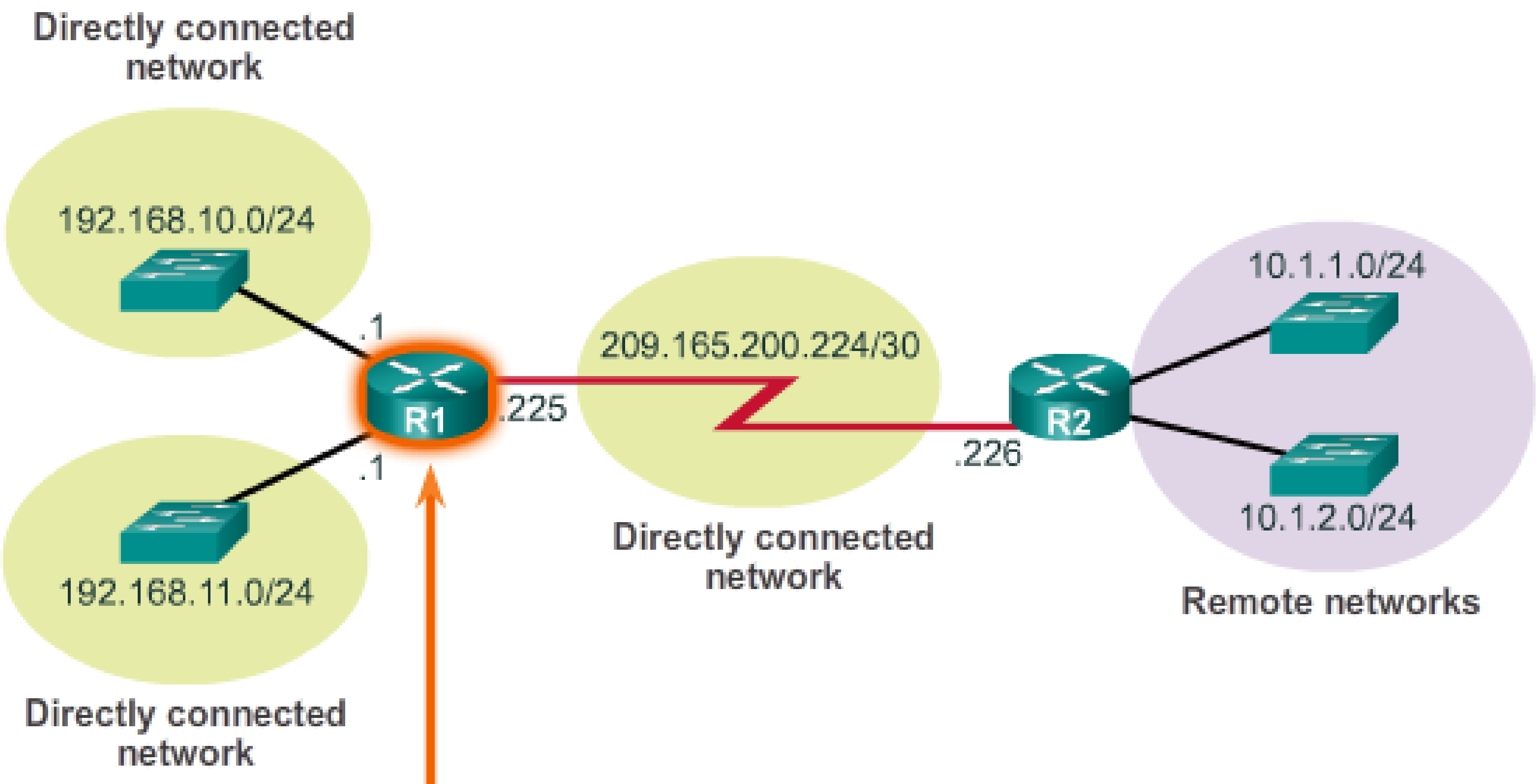
6.5.1.1 Class Activity – Can You Read This Map?



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

6.5.1.2 Packet Tracer - Skills Integration Challenge

6.5.1.3 Summary



R1 has three directly connected networks: 192.168.10.0/24, 192.168.11.0/24, and 209.165.200.224/30. R1 also has two remote networks that it can learn about from R2: 10.1.1.0/24 and 10.1.2.0/24.

6.5.1.3 Summary

Summary

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: IP addressing for end devices, encapsulation, routing, and de-encapsulation.

The Internet is largely based on IPv4, which is still the most widely-used network layer protocol. An IPv4 packet contains the IP header and the payload. However, IPv4 has a limited number of unique public IP addresses available. This led to the development of IP version 6 (IPv6). The IPv6 simplified header offers several advantages over IPv4, including better routing efficiency, simplified extension headers, and capability for per-flow processing. Plus, IPv6 addresses are based on 128-bit hierarchical addressing as opposed to IPv4 with 32 bits. This dramatically increases the number of available IP addresses