Table Of Contents

Introduction

Online References: Link

YouTube: Link

1. Why Should I Take This Module?

Welcome to Network Layer!

By now you may have noticed that the modules in this course are progressing from the bottom up through the OSI model layers. At the network layer of the OSI model, we introduce you to communication protocols and routing protocols. Say you want to send an email to a friend who lives in another city, or even another country. This person is not on the same network as you. A simple switched network cannot get your message any further than the end of your own network. You need some help to keep this message moving along the path to your friend's end device. To send an email (a video, or a file, etc.) to anyone who is not on your local network, you must have access to routers. To access routers, you must use network layer protocols. To help you visualize these processes, this module contains two Wireshark activities. Enjoy!

2. What will I learn to do in this module?

Module Title: Network Layer

Module Objective: Explain how routers use network layer protocols and services to enable end-to-end connectivity.

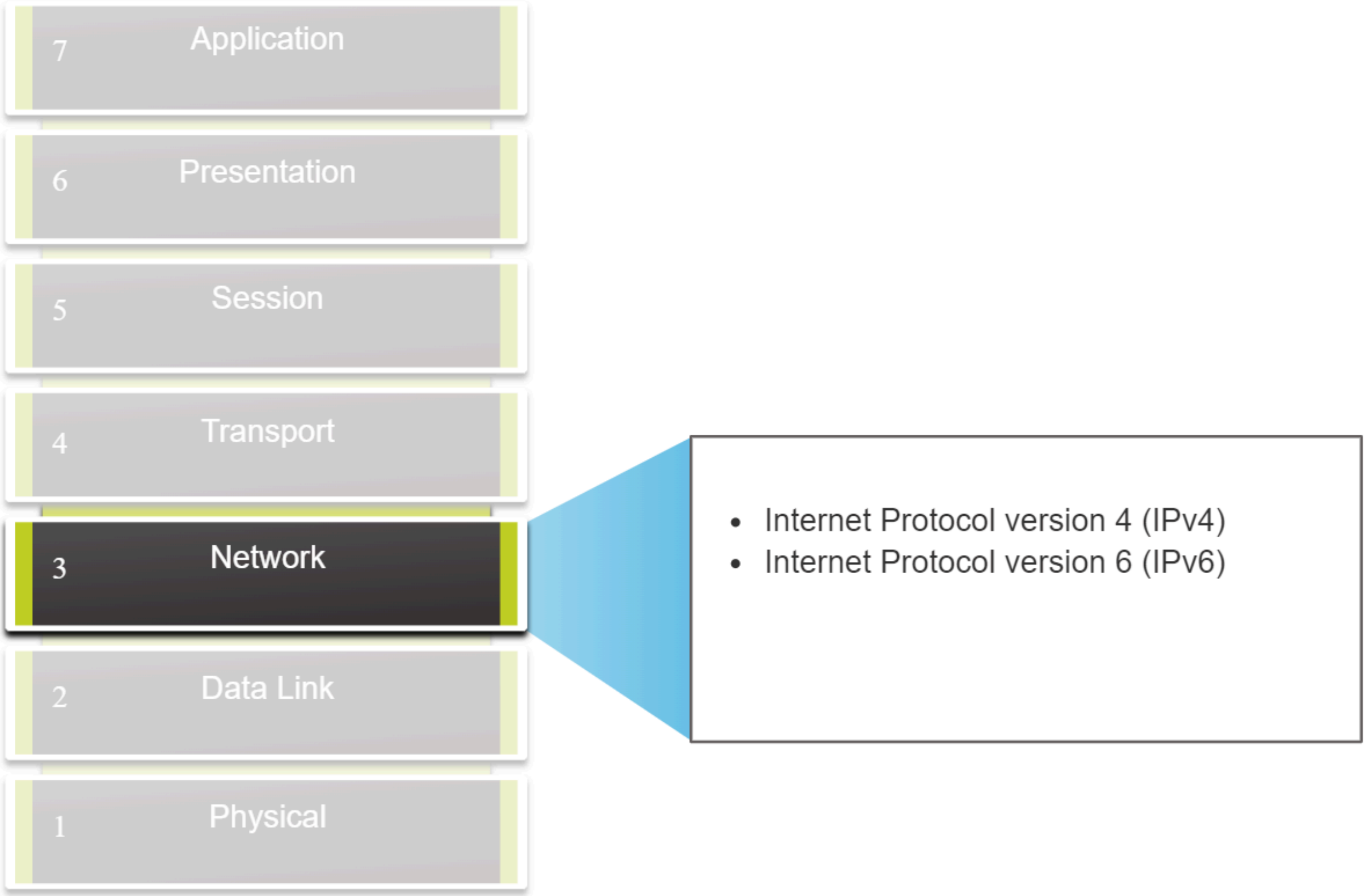
Topic Title	Topic Objective
Network Layer Characteristics	Explain how the network layer uses IP protocols for reliable communications.
IPv4 Packet	Explain the role of the major header fields in the IPv4 packet.
IPv6 Packet	Explain the role of the major header fields in the IPv6 packet.
How a Host Routes	Explain how network devices use routing tables to direct packets to a destination network.
Router Routing Tables	Explain the function of fields in the routing table of a router.

Network Layer Characteristics

1. The Network Layer

The network layer, or OSI Layer 3, provides services to allow end devices to exchange data across networks. As shown in the figure, IP version 4 (IPv4) and IP version 6 (IPv6) are the principle network layer communication protocols. Other network layer protocols include routing protocols such as Open Shortest Path First (OSPF) and messaging protocols such as Internet Control Message Protocol (ICMP).

1A. Network Layer Protocols



To accomplish end-to-end communications across network boundaries, network layer protocols perform four basic operations:

- **Addressing end devices** - End devices must be configured with a unique IP address for identification on the network.

- **Encapsulation** - The network layer encapsulates the protocol data unit (PDU) from the transport layer into a packet. The encapsulation process adds IP header information, such as the IP address of the source (sending) and destination (receiving) hosts. The encapsulation process is performed by the source of the IP packet.

- **Routing** - The network layer provides services to direct the packets to a destination host on another network. To travel to other networks, the packet must be processed by a router. The role of the router is to select the best path and direct packets toward the destination host in a process known as routing. A packet may cross many routers before reaching the destination host. Each router a packet crosses to reach the destination host is called a hop.

- **De-encapsulation** - When the packet arrives at the network layer of the destination host, the host checks the IP header of the packet. If the destination IP address within the header matches its own IP address, the IP header is removed from the packet. After the packet is de-encapsulated by the network layer, the resulting Layer 4 PDU is passed up to the appropriate service at the transport layer. The de-encapsulation process is performed by the destination host of the IP packet.

Unlike the transport layer (OSI Layer 4), which manages the data transport between the processes running on each host, network layer communication protocols (i.e., IPv4 and IPv6) specify the packet structure and processing used to carry the data from one host to another host. Operating without regard to the data carried in each packet allows the network layer to carry packets for multiple types of communications between multiple hosts.

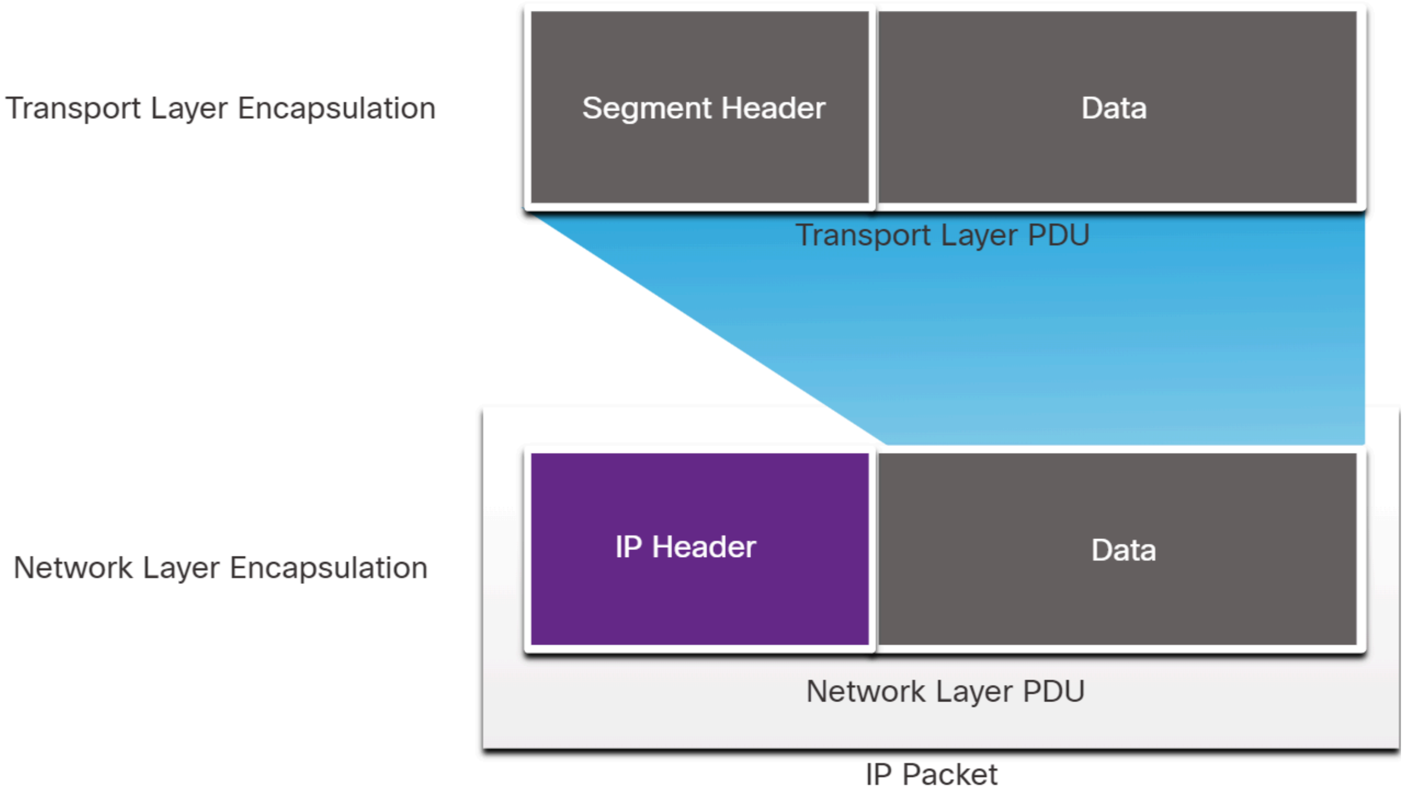
Click Play in the figure to view an animation that demonstrates the exchange of data.

2. IP Encapsulation

IP encapsulates the transport layer (the layer just above the network layer) segment or other data by adding an IP header. The IP header is used to deliver the packet to the destination host.

The figure illustrates how the transport layer PDU is encapsulated by the network layer PDU to create an IP packet.

The illustration shows the transport layer PDU being encapsulated into an IP packet. At the top of the graphic is the transport layer encapsulation. It shows the segment header followed by data. This comprises the transport layer PDU. This is passed down to the network layer for further encapsulation and becomes the data part of the network layer PDU. An IP header is added in front of the data to create the IP packet.



The process of encapsulating data layer by layer enables the services at the different layers to develop and scale without affecting the other layers. This means the transport layer segments can be readily packaged by IPv4 or IPv6 or by any new protocol that might be developed in the future.

The IP header is examined by Layer 3 devices (i.e., routers and Layer 3 switches) as it travels across a network to its destination. It is important to note, that the IP addressing information remains the same from the time the packet leaves the source host until it arrives at the destination host, except when translated by the device performing Network Address Translation (NAT) for IPv4.

Note: NAT is discussed in later modules.

Routers implement routing protocols to route packets between networks. The routing performed by these intermediary devices examines the network layer addressing in the packet header. In all cases, the data portion of the packet, that is, the encapsulated transport layer PDU or other data, remains unchanged during the network layer processes.

3. 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. The protocol was not designed to track and manage the flow of packets. These functions, if required, are performed by other protocols at other layers, primarily TCP at Layer 4.

These are the basic characteristics of IP:

- **Connectionless** - There is no connection with the destination established before sending data packets.
- **Best Effort** - IP is inherently unreliable because packet delivery is not guaranteed.
- **Media Independent** - Operation is independent of the medium (i.e., copper, fibre-optic, or wireless) carrying the data.

4. Connectionless

IP is connectionless, meaning that no dedicated end-to-end connection is created by IP before data is sent. Connectionless communication is conceptually similar to sending a letter to someone without notifying the recipient in advance. The figure summarizes this key point.

a packet, consisting of an IP header and segment, is sent from a source on one network to a destination on another network

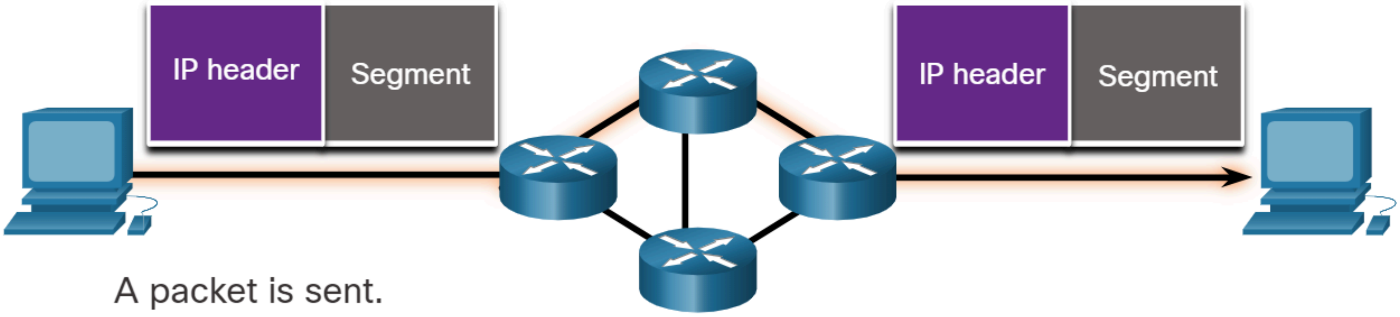
4A. Connectionless - Analogy

Mail box
Letter
Letter

A letter is sent.

Connectionless data communications work on the same principle. As shown in the figure, IP requires no initial exchange of control information to establish an end-to-end connection before packets are forwarded.

4B. Connectionless - Network

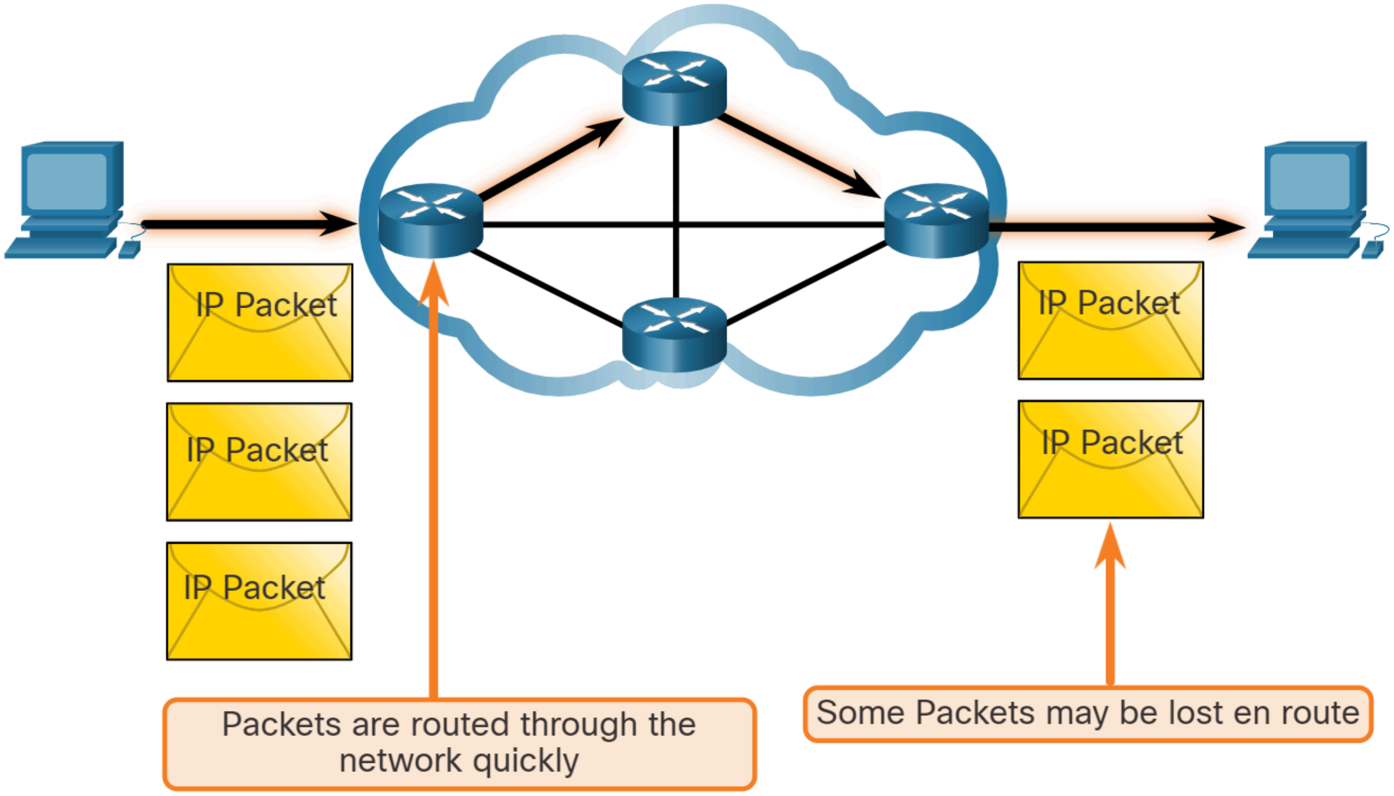


A packet is sent.

5. Best Effort

IP also does not require additional fields in the header to maintain an established connection. This process greatly reduces the overhead of IP. However, with no pre-established end-to-end connection, senders are unaware whether destination devices are present and functional when sending packets, nor are they aware if the destination receives the packet, or if the destination device is able to access and read the packet.

The IP protocol does not guarantee that all packets that are delivered are, in fact, received. The figure illustrates the unreliable or best-effort delivery characteristic of the IP protocol. The diagram shows a source on one network and a destination on another network. Between the two hosts is a cloud consisting of four routers in a mesh topology. Three IP packets leave the source host but only two arrive at the destination host. Text in the graphic reads: Packets are routed through the network quickly; Some Packets may be lost en route.


IP Packet
IP Packet
IP Packet
IP Packet
IP Packet
Packets are routed through the network quickly
Some Packets may be lost en route

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.

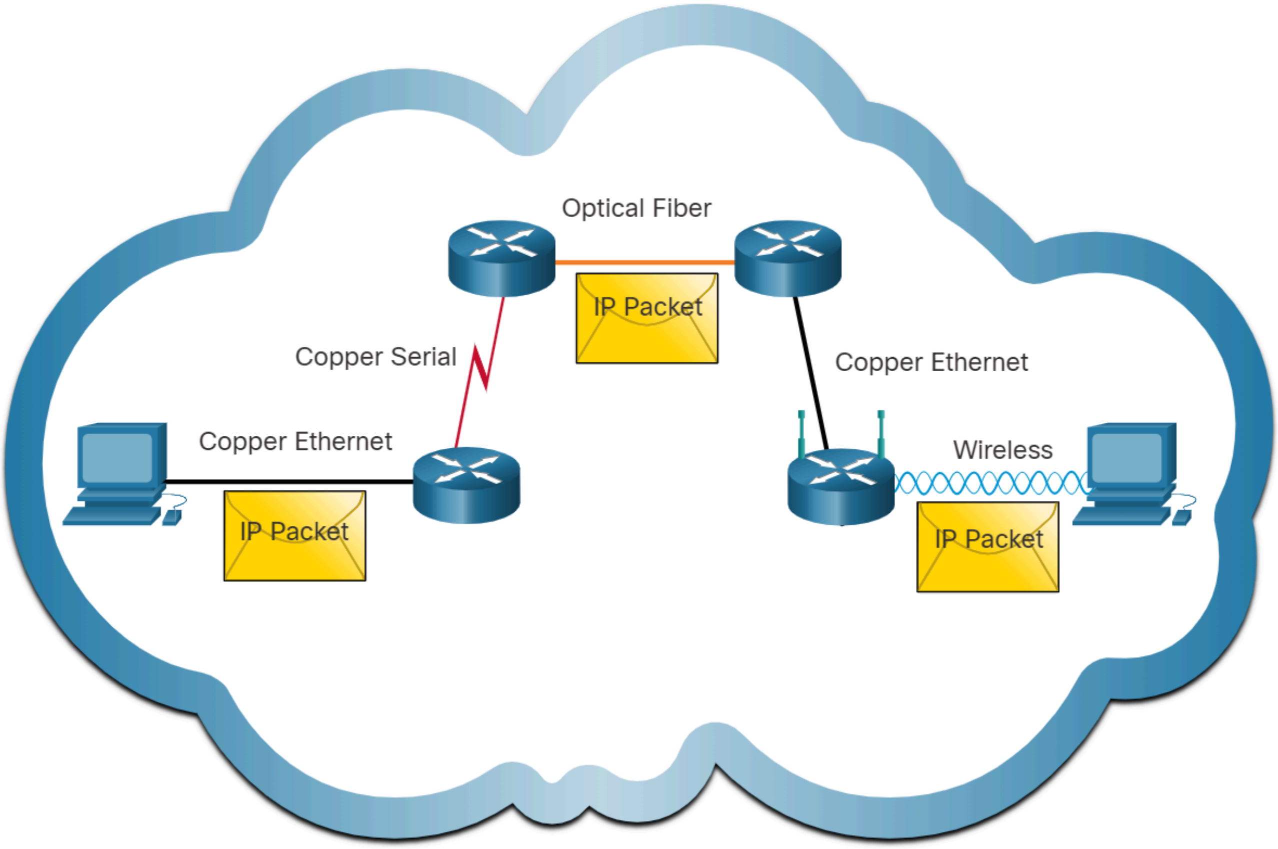
6. Media Independent

Unreliable 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, they do not contain information that can be processed to inform the sender whether delivery was successful. Packets may arrive at the destination corrupted, out of sequence, or not at all. IP provides no capability for packet retransmissions if errors occur.

If out-of-order packets are delivered, or packets are missing, then applications using the data, or upper-layer services, must resolve these issues. This allows IP to function very efficiently. In the TCP/IP protocol suite, reliability is the role of the TCP protocol at the transport layer.

IP operates independently of the media that carry the data at lower layers of the protocol stack. As shown in the figure, IP packets can be communicated as electronic signals over copper cable, as optical signals over fiber, or wirelessly as radio signals.

The diagram shows a network topology within a cloud with a packet travelling over various media types between two hosts. An IP packet is shown moving between a host and a router over a copper Ethernet connection. The first router is connected to second router via a copper serial connection. An IP packet is shown moving between the second router and a third router over an optical fiber connection. The third router is connected to a fourth router, which is a wireless router. An IP packet is shown moving between the fourth router and a host over a wireless connection.



IP packets can travel over different media.

The OSI data link layer is responsible for taking an IP packet and preparing it for transmission over the communications medium. This means that the delivery of IP packets is not limited to any particular medium.

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.

In some cases, an intermediate device, usually a router, must split up an IPv4 packet when forwarding it from one medium to another medium with a smaller MTU. This process is called fragmenting the packet, or fragmentation. Fragmentation causes latency. IPv6 packets cannot be fragmented by the router.

7. Check Your Understanding - IP Characteristics

Check your understanding of IP characteristics by choosing the correct answer to the following questions.

Question 1: Which OSI layer sends segments to be encapsulated in an IPv4 or IPv6 packet?

(a) data link layer

(b) network layer

(c) transport layer

(d) session layer

Answer: **(c) -** Transport layer PDUs, called segments, are encapsulated at the network layer by IPv4 and IPv6 into packets.

Question 2: Which layer is responsible for taking an IP packet and preparing it for transmission over the communications medium?

(a) physical layer

(b) network layer

(c) data link layer

(d) transport layer

Answer: **(c) -** The data link layer receives IP packets from the network layer and encapsulates them for transmission over the medium.

Question 3: What is the term for splitting up an IP packet when forwarding it from one medium to another medium with a smaller MTU?

(a) encapsulation

(b) fragmentation

(c) segmentation

(d) serialization

Answer: **(b) -** Fragmentation is the process of splitting up IP packets to travel over a medium with a smaller MTU.

Question 4: Which delivery method does not guarantee that the packet will be delivered fully without errors?

(a) connectionless

(b) best effort

(c) media independent

Answer: **(b) -** Best effort delivery does not guarantee packets will be delivered to the destination.

IPv4 Packet

1. IPv4 Packet Header

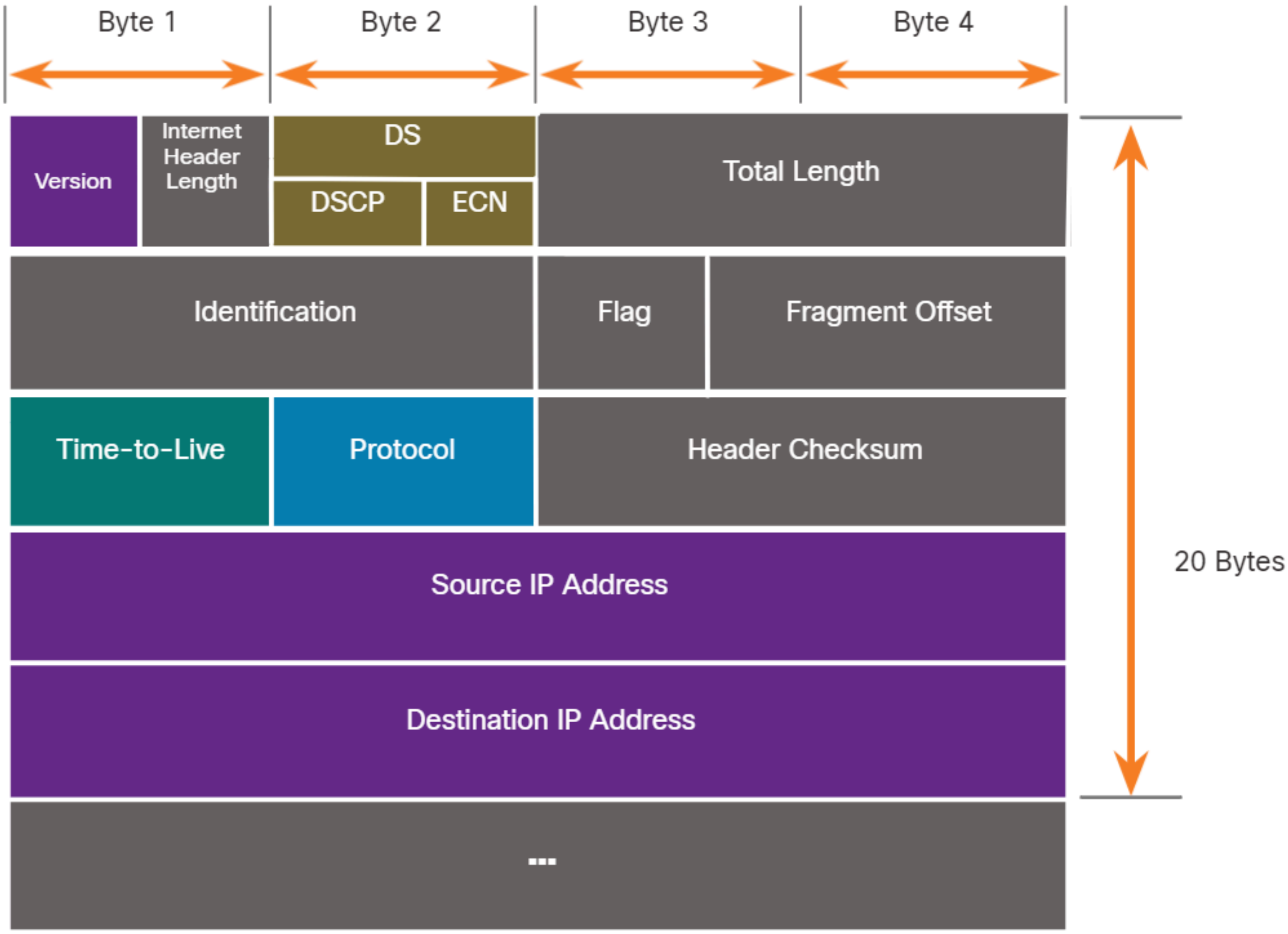
IPv4 is one of the primary network layer communication protocols. The IPv4 packet header is used to ensure that this packet is delivered to its next stop on the way to its destination end device.

An IPv4 packet header consists of fields containing important information about the packet. These fields contain binary numbers which are examined by the Layer 3 process.

2. IPv4 Packet Header Fields

The binary values of each field identify various settings of the IP packet. Protocol header diagrams, which are read left to right, and top down, provide a visual to refer to when discussing protocol fields. The IP protocol header diagram in the figure identifies the fields of an IPv4 packet.

2A. Fields in the IPv4 Packet Header



Significant fields in the IPv4 header include the following:

- **Version** – Contains a 4-bit binary value set to 0100 that identifies this as an IPv4 packet.

- **Differentiated Services or DiffServ (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. The six most significant bits of the DiffServ field are the differentiated services code point (DSCP) bits and the last two bits are the explicit congestion notification (ECN) bits.

- **Header Checksum** – This is used to detect corruption in the IPv4 header.

- **Time to Live (TTL)** – TTL contains an 8-bit binary value that is used to limit the lifetime of a packet. The source device of the IPv4 packet sets the initial TTL value. It is decreased by one each time the packet is processed by a router. If the TTL field decrements to zero, the router discards the packet and sends an Internet Control Message Protocol (ICMP) Time Exceeded message to the source IP address. Because the router decrements the TTL of each packet, the router must also recalculate the Header Checksum.

- **Protocol** – This field is used to identify the next level 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. Common values include ICMP (1), TCP (6), and UDP (17).

- **Source IPv4 Address** – This contains a 32-bit binary value that represents the source IPv4 address of the packet. The source IPv4 address is always a unicast address.

- **Destination IPv4 Address** – This contains a 32-bit binary value that represents the destination IPv4 address of the packet. The destination IPv4 address is a unicast, multicast, or broadcast address.

The two most commonly referenced fields are the source and destination IP addresses. These fields identify where the packet is coming from and where it is going. Typically, these addresses do not change while travelling from the source to the destination.

The Internet Header Length (IHL), Total Length, and Header Checksum fields are used to identify and validate the packet.

Other fields are used to reorder a fragmented packet. Specifically, the IPv4 packet uses Identification, Flags, and Fragment Offset fields to keep track of the fragments. A router may have to fragment an IPv4 packet when forwarding it from one medium to another with a smaller MTU.

The Options and Padding fields are rarely used and are beyond the scope of this module.

3. Video - Sample IPv4 Headers in Wireshark

Click Play in the figure to view a demonstration of examining IPv4 headers in a Wireshark capture.

4. Check Your Understanding - IPv4 Packet

Check your understanding of the IPv4 packet by choosing the correct answer to the following questions.

Question 1: What are the two most commonly referenced fields in an IPv4 packet header that indicate where the packet is coming from and where it is going? (Choose two.)

(a) destination IP address

(b) protocol

(c) Time to Live

(d) source IP address

(e) Differentiated Services (DS)

Answer: **(a & d) -** The IP header fields that identify where the packet originated and where it is going are Source IP Address and Destination IP Address.

Question 2: Which statement is correct about IPv4 packet header fields?

(a) The source and destination IPv4 addresses remain the same while travelling from source to destination.

(b) The Time to Live field is used to determine the priority of each packet.

(c) The Total Length and Header Checksum fields are used to reorder a fragmented packet.

(d) The Version field identifies the next level protocol.

Answer: **(a) -** The source and destination IP addresses in the IP packet do not change in route from source to destination.

Question 3: Which field is used to detect corruption in the IPv4 header?

(a) Header Checksum

(b) Time to Live

(c) Protocol

(d) Differentiated Services (DS)

Answer: **(a) -** The Header Checksum field in an IPv4 header is used to detect corrupt packets.

Question 4: Which field includes common values such as ICMP (1), TCP (6), and UDP (17)?

(a) Header Checksum

(b) Time to Live

(c) Protocol

(d) Differentiated Services (DS)

Answer: **(c) -** The protocol field identifies the upper layer protocol that is carried inside the IP packet. Common protocols are TCP, UDP, and ICMP.

IPv6 Packet

1. Limitations of IPv4

IPv4 is still in use today. This topic is about IPv6, which will eventually replace IPv4. To better understand why you need to know the IPv6 protocol, it helps to know the limitations of IPv4 and the advantages of IPv6.

Through the years, additional protocols and processes have been developed to address new challenges. However, even with changes, IPv4 still has three major issues:

- **IPv4 address depletion** - IPv4 has a limited number of unique public 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.

- **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.

- **Increased network complexity** – While NAT has extended the lifespan of IPv4 it was only meant as a transition mechanism to IPv6. NAT in its various implementation creates additional complexity in the network, creating latency and making troubleshooting more difficult.

2. IPv6 Overview

In the early 1990s, the Internet Engineering Task Force (IETF) grew concerned about the issues with IPv4 and began to look for a replacement. This activity led to the development of IP version 6 (IPv6). IPv6 overcomes the limitations of IPv4 and is a powerful enhancement with features that better suit current and foreseeable network demands.

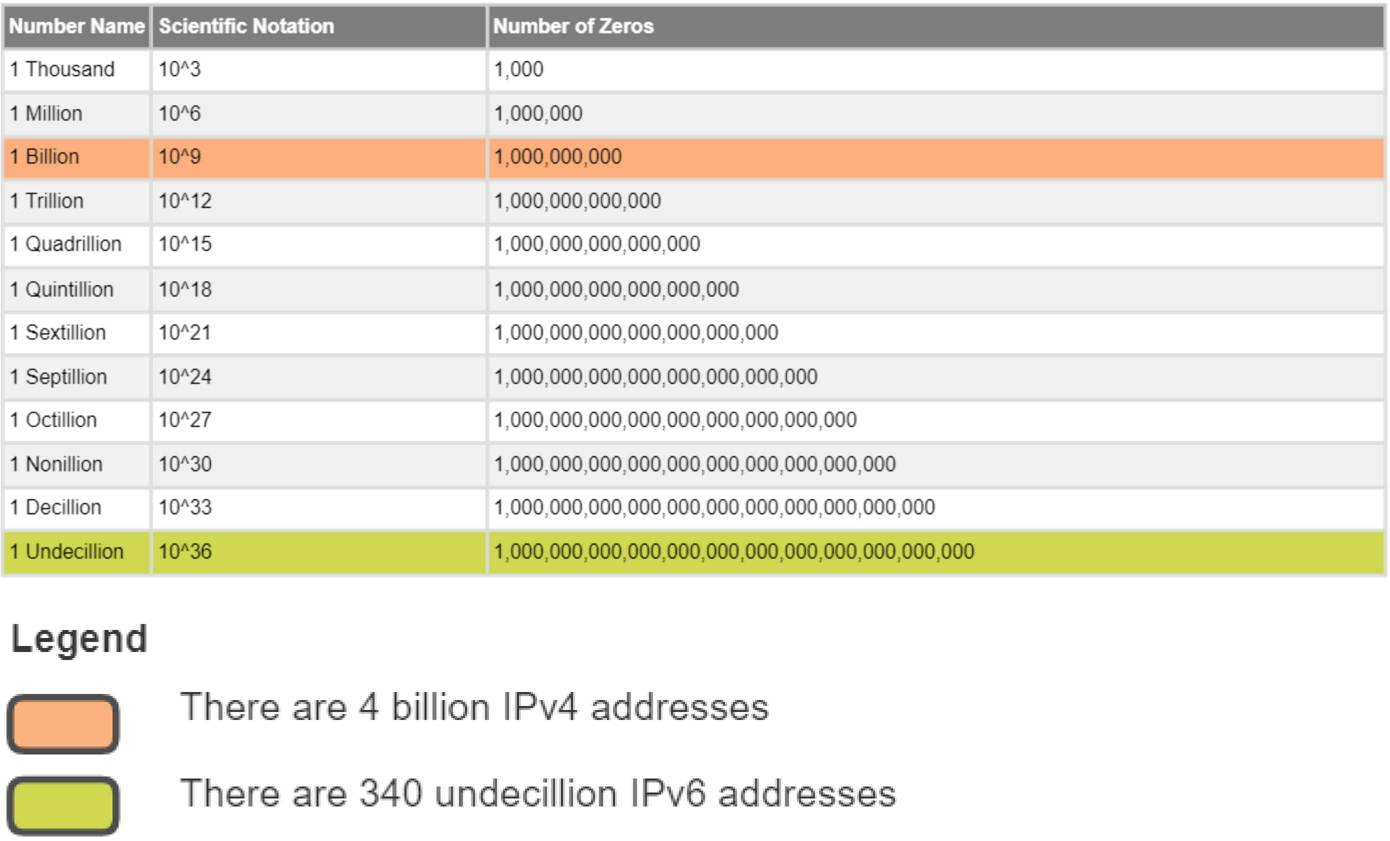
Improvements that IPv6 provides include the following:

- **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. This avoids some of the NAT-induced problems experienced by applications that require end-to-end connectivity.

The 32-bit IPv4 address space provides approximately 4,294,967,296 unique addresses. IPv6 address space provides 340,282,366,920,938,463,463,374,607,431,768,211,456, or 340 undecillion addresses. This is roughly equivalent to every grain of sand on Earth.

The figure provides a visual to compare the IPv4 and IPv6 address space.

2A. IPv4 and IPv6 Address Space Comparison



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

3. IPv4 Packet Header Fields in the IPv6 Packet Header

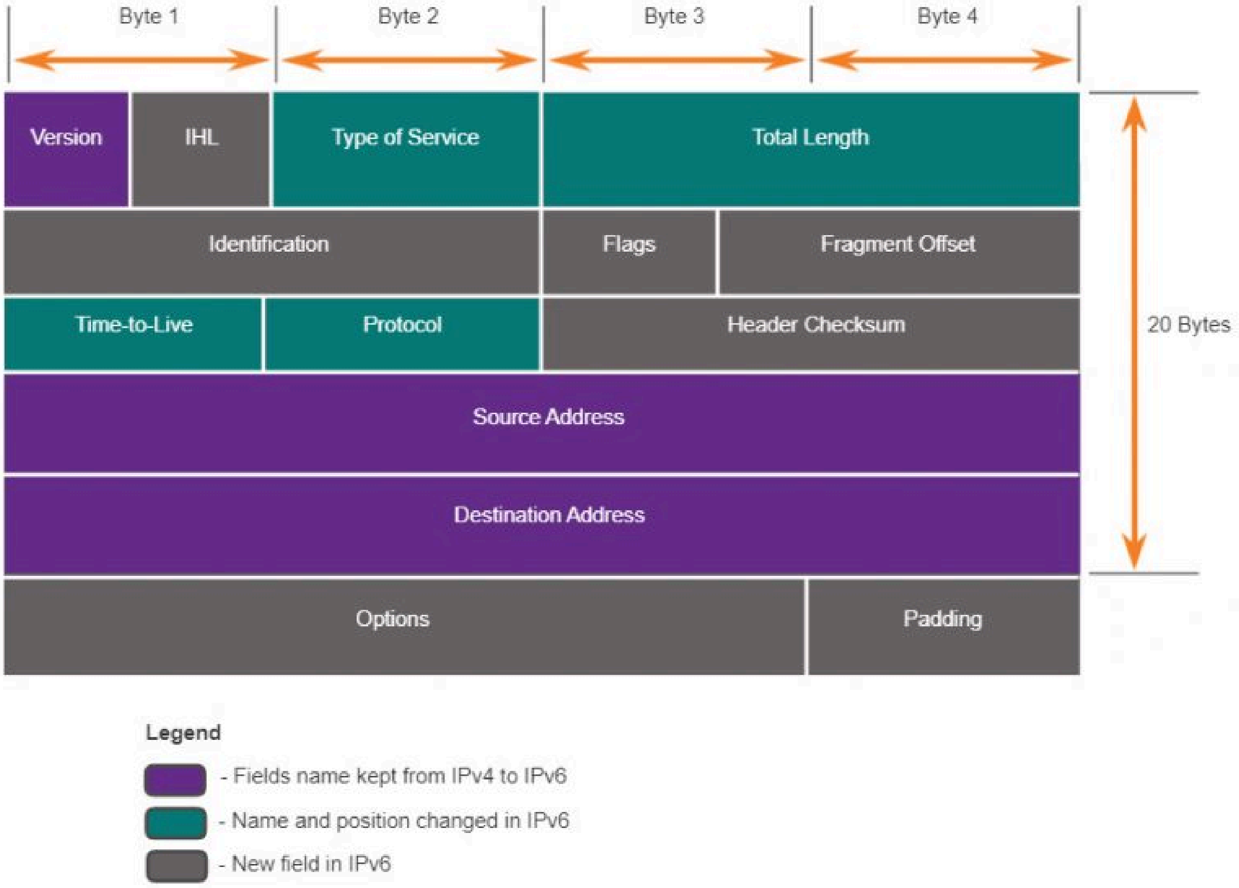
One of the major design improvements of IPv6 over IPv4 is the simplified IPv6 header.

For example, the IPv4 header consists of a variable length header of 20 octets (up to 60 bytes if the Options field is used) and 12 basic header fields, not including the Options field and Padding field.

For IPv6, some fields have remained the same, some fields have changed names and positions, and some IPv4 fields are no longer required, as highlighted in the figure.

The diagram shows an IPv4 packet header and indicates which fields kept the same name, which fields changed names and position, and which fields were not kept in IPv6. The fields that kept the same name are: version, source address, and destination address. The fields that changed names and positions are: type of service, total length, time-to-live, and protocol. The fields that were not kept in IPv6 are IHL, identification, flags, fragment offset, header checksum, options, and padding.

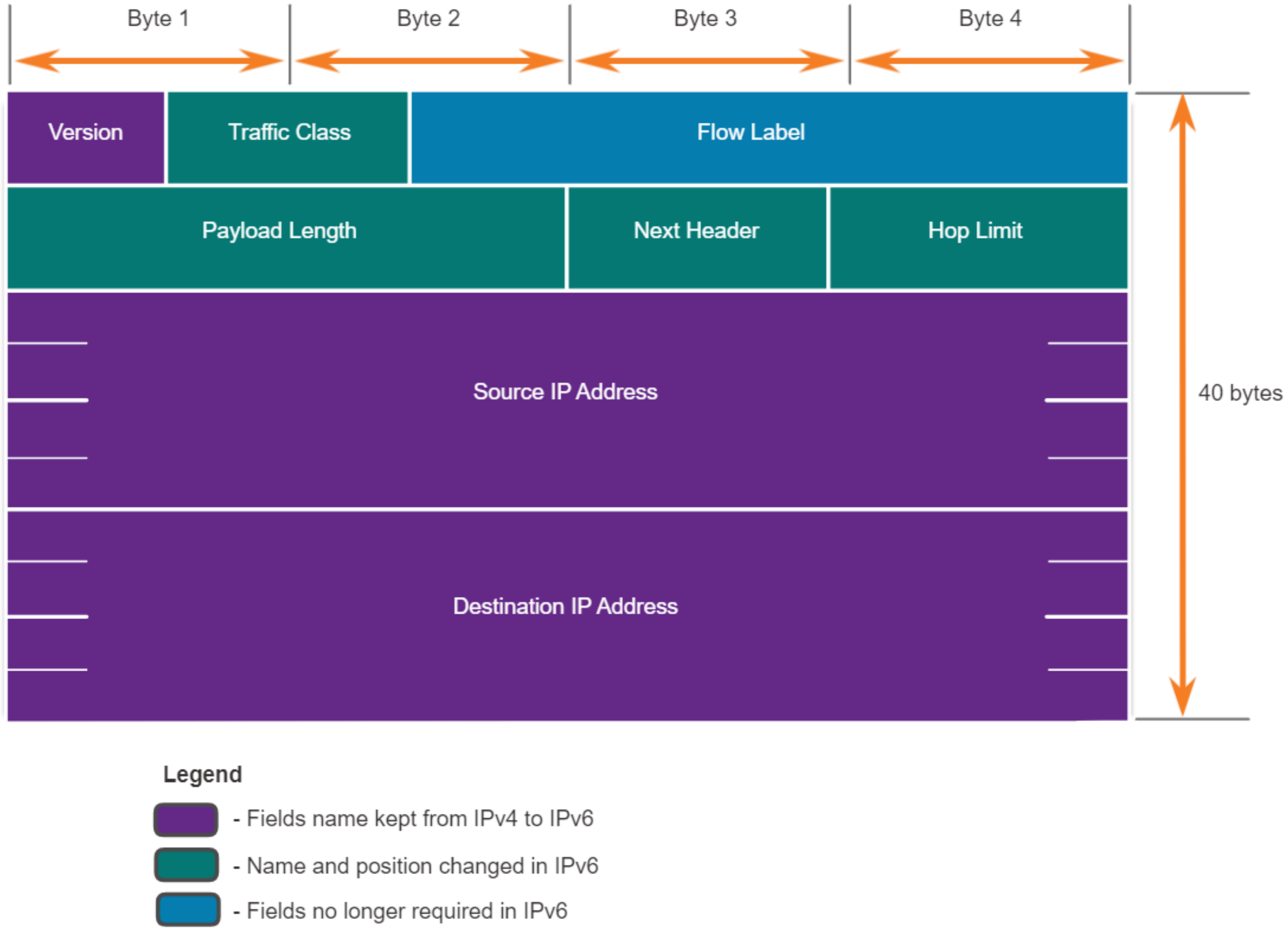
3A. IPv4 Packet Header



The figure shows IPv4 packet header fields that were kept, moved, changed, as well as those that were not kept in the IPv6 packet header. In contrast, the simplified IPv6 header shown the next figure consists of a fixed length header of 40 octets (largely due to the length of the source and destination IPv6 addresses).

The IPv6 simplified header allows for more efficient processing of IPv6 headers. The figure shows the IPv4 packet header fields that were kept or moved along with the new IPv6 packet header fields.

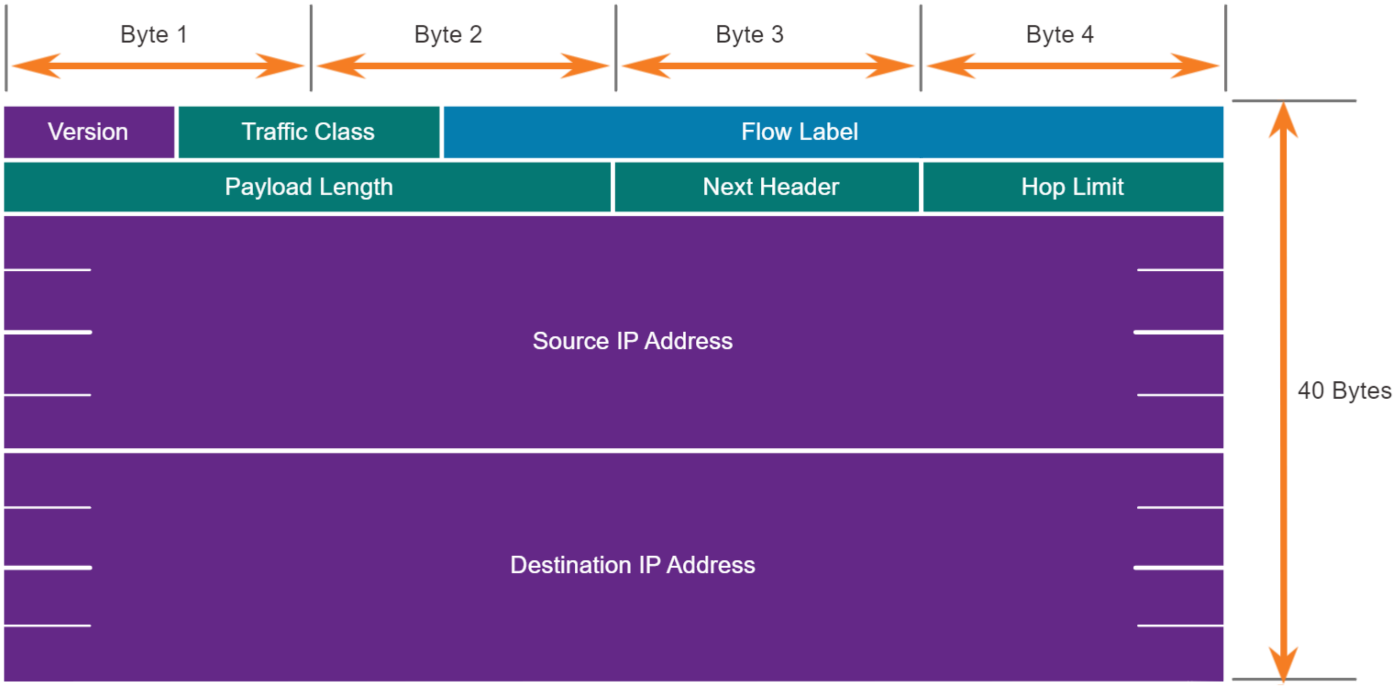
3B. IPv6 Packet Header



4. IPv6 Packet Header

The IP protocol header diagram in the figure identifies the fields of an IPv6 packet.

4A. Fields in the IPv6 Packet Header



The fields in the IPv6 packet header include the following:

- **Version** – This field contains a 4-bit binary value set to 0110 that identifies this as an IP version 6 packet.

- **Traffic Class** – This 8-bit field is equivalent to the IPv4 Differentiated Services (DS) field.

- **Flow Label** – This 20-bit field suggests that all packets with the same flow label receive the same type of handling by routers.

- **Payload Length** – This 16-bit field indicates the length of the data portion or payload of the IPv6 packet. This does not include the length of the IPv6 header, which is a fixed 40-byte header.

- **Next Header** – This 8-bit field is equivalent to the IPv4 Protocol field. It 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** – This 8-bit field replaces the IPv4 TTL field. This value is decremented by a value of 1 by each router that forwards the packet. When the counter reaches 0, the packet is discarded, and an ICMPv6 Time Exceeded message is forwarded to the sending host,. This indicates that the packet did not reach its destination because the hop limit was exceeded. Unlike IPv4, IPv6 does not include an IPv6 Header Checksum, because this function is performed at both the lower and upper layers. This means the checksum does not need to be recalculated by each router when it decrements the Hop Limit field, which also improves network performance.

- **Source IPv6 Address** – This 128-bit field identifies the IPv6 address of the sending host.

- **Destination IPv6 Address** – This 128-bit field identifies the IPv6 address of the receiving host.

An IPv6 packet may also contain extension headers (EH), which provide optional network layer information. Extension headers are optional and are placed between the IPv6 header and the payload. EHs are used for fragmentation, security, to support mobility and more.

Unlike IPv4, routers do not fragment routed IPv6 packets.

5. Video - Sample IPv6 Headers in Wireshark

Click Play in the figure to view a demonstration of examining IPv6 headers in a Wireshark capture.

6. Check Your Understanding - IPv6 Packet

Check your understanding of the IPv6 packet by choosing the correct answer to the following questions.

Question 1: Which three options are major issues associated with IPv4? (Choose three.)

(a) IP address depletion

(b) increased network complexity and Internet routing table expansion

(c) always on connections

(d) lack of end-to-end connectivity

(e) global and political boundaries

(f) too many IPv4 addresses available

Answer: **(a & b & d) -** IPv4 was standardized in the 1980s and has several technological limitations, such as lack of end-to-end connectivity and a depleted address space.

Question 2: Which two options are improvements provided by IPv6 as compared to IPv4? (Choose two.)

(a) header supports additional fields for complex packets

(b) increased the IP address space

(c) standardizes the use of NAT

(d) supports class-based networks

(e) uses a simpler header to provide improved packet handling

Answer: **(b & e) -** There are several technical improvements made to IPv6, two of which are a vastly larger IP address pool and a simplified protocol header.

Question 3: Which is true of the IPv6 header?

(a) it consists of 20 octets.

(b) it consists of 40 octets.

(c) it contains 8 header fields.

(d) it contains 12 header fields.

Answer: **(b & c) -** The IPv6 header is a fixed length of 40 octets and contains 8 header fields.

Question 4: Which is true of the IPv6 packet header?

(a) The Hop Limit field replaces the IPv4 Time to Live field.

(b) The Source and Destination IPv6 addresses change while travelling from source to destination.

(c) The Time to Live field replaces the DiffServ field.

(d) The Version field identifies the next header.

Answer: **(a) -** Several fields in the IPv6 header replaced fields in the IPv4 header. For example, the Hop Limit field replaced the IPv4 header Time to Live field.

How a Host Routes

1. Host Forwarding Decision

With both IPv4 and IPv6, packets are always created at the source host. The source host must be able to direct the packet to the destination host. To do this, host end devices create their own routing table. This topic discusses how end devices use routing tables.

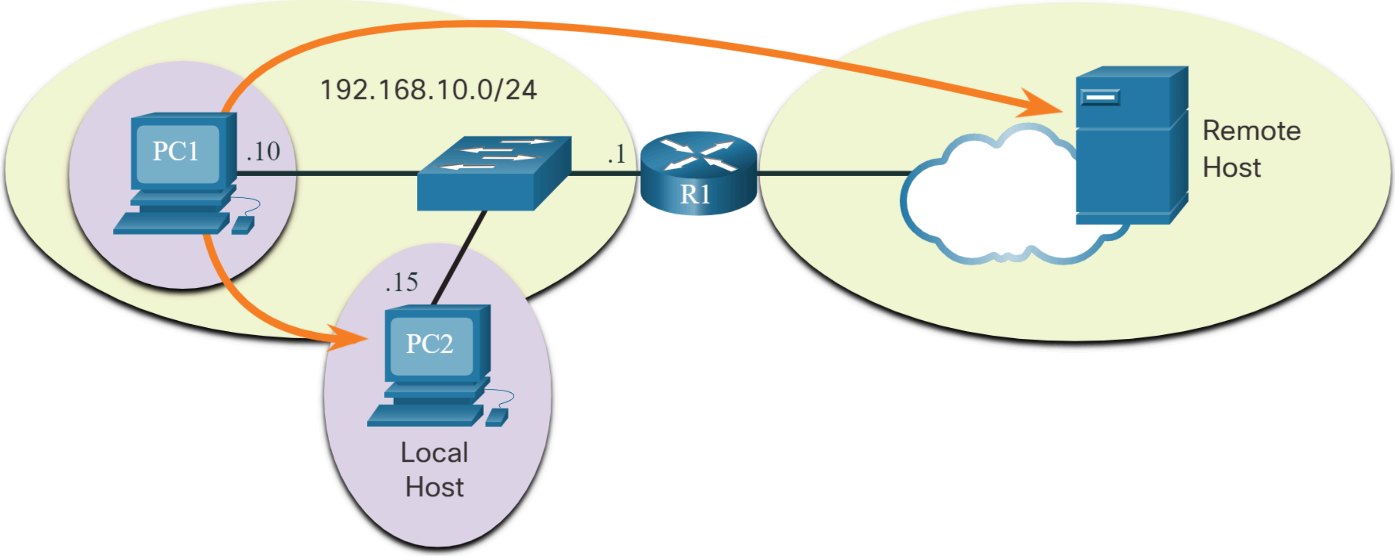
Another role of the network layer is to direct packets between hosts. A host can send a packet to the following:

- **Itself** - A host can ping itself by sending a packet to a special IPv4 address of 127.0.0.1 or an IPv6 address ::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 destination host that is on the same local network as the sending host. The source and destination hosts share the same network address.

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

The figure illustrates PC1 connecting to a local host on the same network, and to a remote host located on another network. The diagram shows a host, PC1, connecting to a local host, PC2, on the same network and to a remote host, a server, on another network. PC1 and PC2 are connected to a switch on network 192.168.10.0/24. PC1 has an address of .10 and PC2 has an address of .15. The switch is connected to a router, R1, at address .1. On the other side of the R1 is a connection to the cloud where the remote host resides.



Whether a packet is destined for a local host or a remote host is determined by the source end device. The source end device determines whether the destination IP address is on the same network that the source device itself is on. The method of determination varies by IP version:

- **In IPv4** - The source device uses its own subnet mask along with its own IPv4 address and the destination IPv4 address to make this determination.

- **In IPv6** - The local router advertises the local network address (prefix) to all devices on the network.

In a home or business network, you may have several wired and wireless devices interconnected together using an intermediary device, such as a LAN switch or a wireless access point (WAP). This intermediary device provides interconnections between local hosts on the local network. Local hosts can reach each other and share information without the need for any additional devices. If a host is sending a packet to a device that is configured with the same IP network as the host device, the packet is simply forwarded out of the host interface, through the intermediary device, and to the destination device directly.

Of course, in most situations we want our devices to be able to connect beyond the local network segment, such as out to other homes, businesses, and the internet. Devices that are beyond the local network segment are known as remote hosts. When a source device sends a packet to a remote destination device, then the help of routers and routing is needed. Routing is the process of identifying the best path to a destination. The router connected to the local network segment is referred to as the default gateway.

2. Default Gateway

The default gateway is the network device (i.e., router or Layer 3 switch) that can route traffic to other networks. If you use the analogy that a network is like a room, then the default gateway is like a doorway. If you want to get to another room or network you need to find the doorway.

On a network, a default gateway is usually a router with these features:

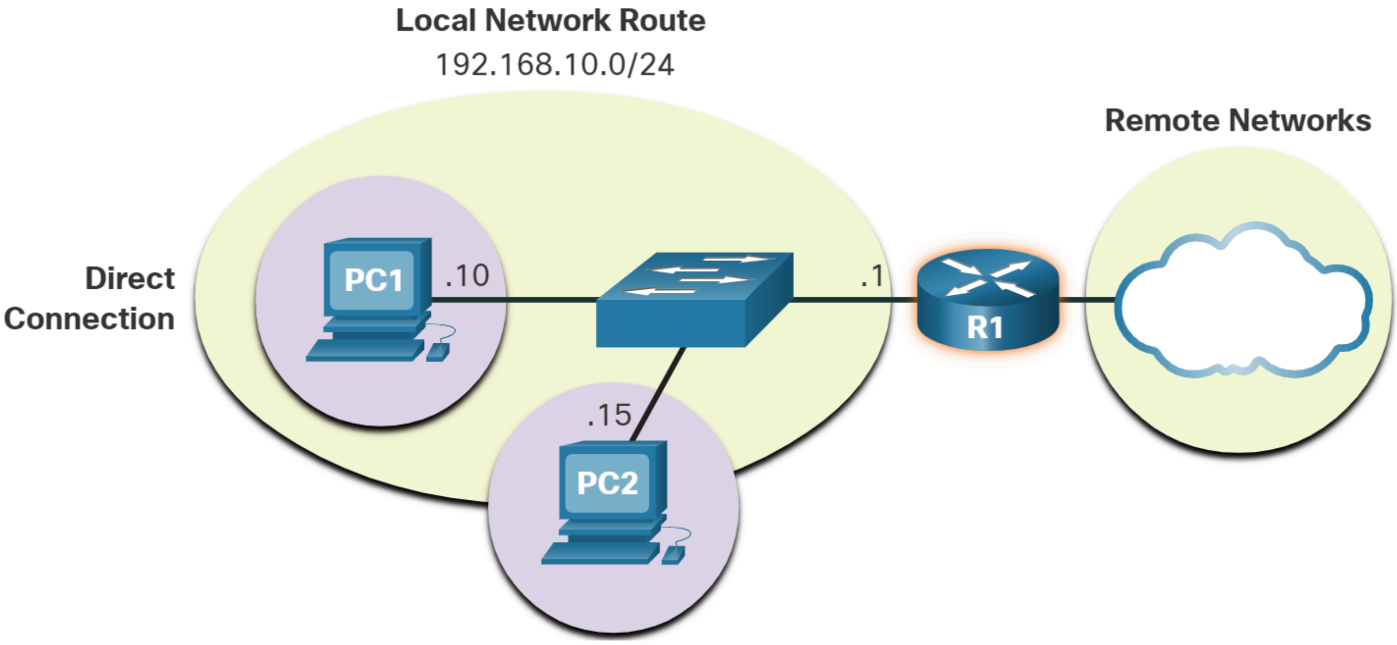
- It has a local IP address in the same address range as other hosts on the local network.
- It can accept data into the local network and forward data out of the local network.
- It routes traffic to other networks.

A default gateway is required to send traffic outside of the local network. Traffic cannot be forwarded outside the local network if there is no default gateway, the default gateway address is not configured, or the default gateway is down.

3. A Host Routes to the Default Gateway

A host routing table will typically include a default gateway. In IPv4, the host receives the IPv4 address of the default gateway either dynamically from Dynamic Host Configuration Protocol (DHCP) or configured manually. In IPv6, the router advertises the default gateway address or the host can be configured manually.

In the figure, PC1 and PC2 are configured with the IPv4 address of 192.168.10.1 as the default gateway. The diagram shows two hosts, PC1 and PC2, connected to a switch on network 192.168.10.0/24, the local network route. The switch is connected to a router, R1, which is then connected to the cloud representing remote networks. PC1 has an address of .10, PC2 has an address of .15, and the router interface to which the switch is connected has an address of .1. The PCs, the switch, and the router interface all have a direct connection.



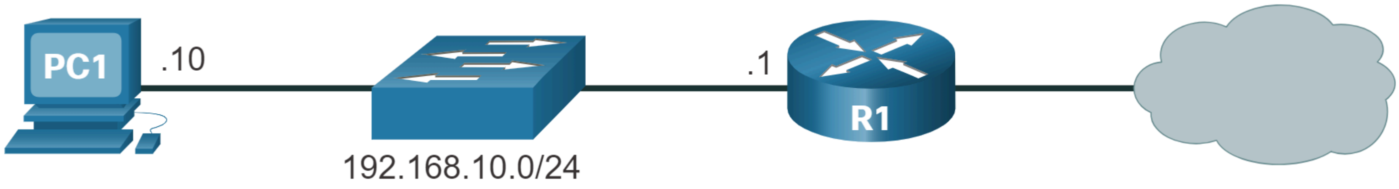
Having a default gateway configured creates a default route in the routing table of the PC. A default route is the route or pathway your computer will take when it tries to contact a remote network.

Both PC1 and PC2 will have a default route to send all traffic destined to remote networks to R1.

4. Host Routing Tables

On a Windows host, the **route print** or **netstat -r** command can be used to display the host routing table. Both commands generate the same output. The output may seem overwhelming at first, but is fairly simple to understand.

The figure displays a sample topology and the output generated by the **netstat –r** command. The diagram shows a network topology consisting of a host, PC1, connected to a switch on network 192.168.10.0/24. The switch is connected to a router, R1, which is then connected to the cloud. PC1 has an address of .10 and the router interface to which the switch is connected has an address of .1.



4A. 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)
```

Note: The output only displays the IPv4 route table.

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.

5. Check Your Understanding - How a Host Routes

Check your understanding of how a host routes by choosing the correct answer to the following questions.

Question 1: Which statement about host forwarding decisions is true?

(a) A host cannot ping itself.

(b) A remote destination host is on the same local network as the sending host.

(c) Local hosts can reach each other without the need of a router.

(d) Routing is enabled on switches to discover the best path to a destination.

Answer: **(c) -** A router is not needed to forward packets between local hosts on the network.

Question 2: Which default gateway statement is true?

(a) A default gateway is required to send packets to other hosts on the local network.

(b) The default gateway address is the IP address of a switch on a remote network.

(c) The default gateway address is the IP address of the router on the local network.

(d) Traffic can only be forwarded outside the local network if there is no default gateway.

Answer: **(c) -** The default gateway is the IP address of a router on the local network.

Question 3: Which two commands could be entered on a Windows host to view its IPv4 and IPv6 routing table? (Choose two.)

(a) netroute -l

(b) netstat -r

(c) print route

(d) route print

(e) print net

Answer: **(b & d) -** The commands netstat -r and route print will display the routing table of a Windows host.

Introduction to Routing

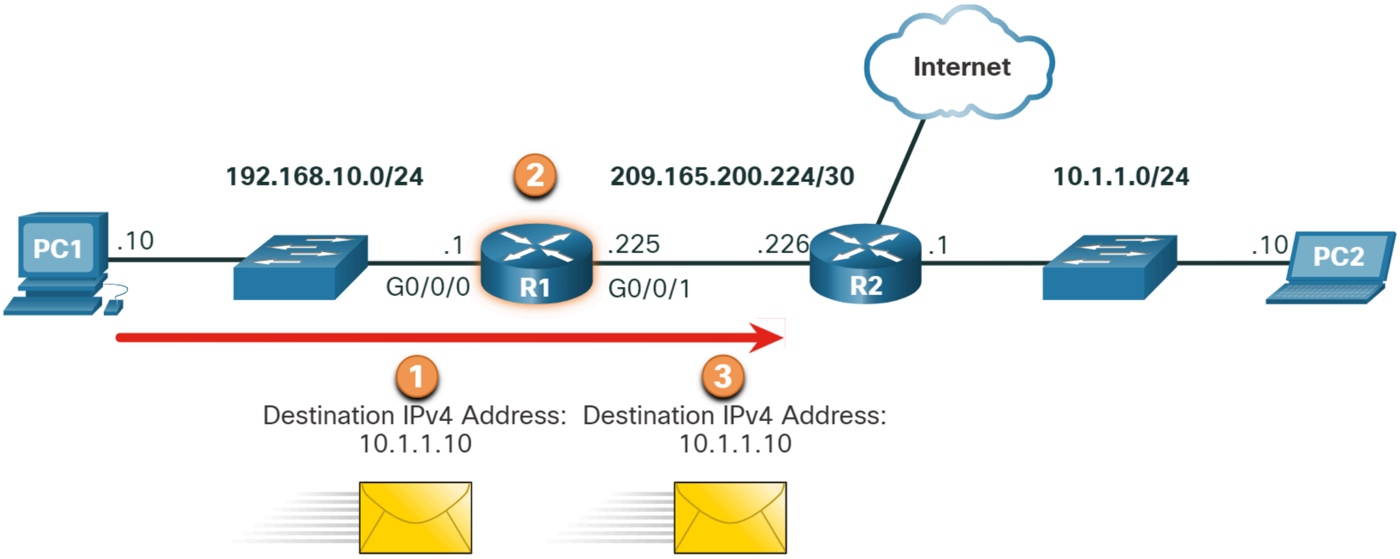
1. Router Packet Forwarding Decision

The previous topic discussed host routing tables. Most networks also contain routers, which are intermediary devices. Routers also contain routing tables. This topic covers router operations at the network layer. When a host sends a packet to another host, it consults its routing table to determine where to send the packet. If the destination host is on a remote network, the packet is forwarded to the default gateway, which is usually the local router.

What happens when a packet arrives on a router interface?

The router examines the destination IP address of the packet and searches its routing table to determine where to forward the packet. The routing table contains a list of all known network addresses (prefixes) and where to forward the packet. These entries are known as route entries or routes. The router will forward the packet using the best (longest) matching route entry.

The diagram is a network topology showing what happens to an IPv4 packet as it is routed between networks. Host PC1, with an address of .10, is connected to a switch on network 192.168.10.0/24 which is connected to the G0/0/0 interface of router R1 with an address of .1. Network 209.165.200.224/30 connects the G0/0/1 interface on R1, address .225, to another router, R2 at address .226. R2 is connected to a switch on network 10.1.1.0/24 to which host PC2, address .10, is connected. R2 also has a connection to the Internet cloud. A packet with destination IPv4 address 10.1.1.10 is sent from PC1 to R1. R1 then sends the packet with destination IPv4 address 10.1.1.10 to R2.



- Packet arrives on the Gigabit Ethernet 0/0/0 interface of router R1. R1 de-encapsulates the Layer 2 Ethernet header and trailer.
- Router R1 examines the destination IPv4 address of the packet and searches for the best match in its IPv4 routing table. The route entry indicates that this packet is to be forwarded to router R2.
- Router R1 encapsulates the packet into a new Ethernet header and trailer, and forwards the packet to the next hop router R2.

The following table shows the pertinent information from the R1 routing table.

1A. R1 Routing Table

Route	Next Hop or Exit Interface
192.168.10.0 /24	G0/0/0
209.165.200.224/30	G0/0/1
10.1.1.0/24	**via R2**
Default Route 0.0.0.0/0	via R2

2. IP Router Routing Table

The routing table of the router contains network route entries listing all the possible known network destinations.

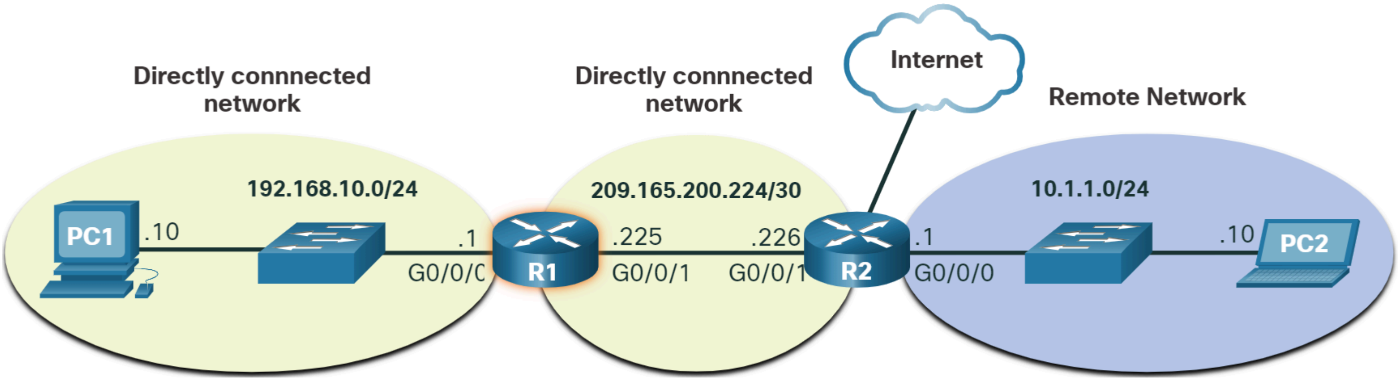
The routing table stores three types of route entries:

- **Directly connected networks** - These network route entries are active router interfaces. Routers add a directly connected route when an interface is configured with an IP address and is activated. Each router interface is connected to a different network segment. In the figure, the directly-connected networks in the R1 IPv4 routing table would be 192.168.10.0/24 and 209.165.200.224/30.

- **Remote networks** - These network route entries are connected to other routers. Routers learn about remote networks either by being explicitly configured by an administrator or by exchanging route information using a dynamic routing protocol. In the figure, the remote network in the R1 IPv4 routing table would be 10.1.1.0/24.

- **Default route** – Like a host, most routers also include a default route entry, a gateway of last resort. The default route is used when there is no better (longer) match in the IP routing table. In the figure, the R1 IPv4 routing table would most likely include a default route to forward all packets to router R2.

The figure identifies the directly connected and remote networks of router R1. The diagram is a network topology identifying directly connected networks and remote networks of a router. Host PC1, with an address of .10, is connected to a switch on network 192.168.10.0/24 which is connected to the G0/0/0 interface of router R1 with an address of .1. Network 209.165.200.224/30 connects the G0/0/1 interface on R1, address .225, to another router, R2 at address .226 on G0/0/1. R2 is connected to a switch on network 10.1.1.0/24 to which host PC2, address .10, is connected. R2 also has a connection to the Internet cloud. Networks 192.168.10.0/24 and 209.165.200.224/30 are shown as directly connected networks to R1 and network 10.1.2.0/24 (should this be 10.1.1.0/24?) is shown as a remote network to R2.



R1 has two directly connected networks:

- 192.168.10.0/24
- 209.165.200.224/30

R1 also has remote networks (i.e. 10.1.1.0/24 and the internet) that it can learn about.

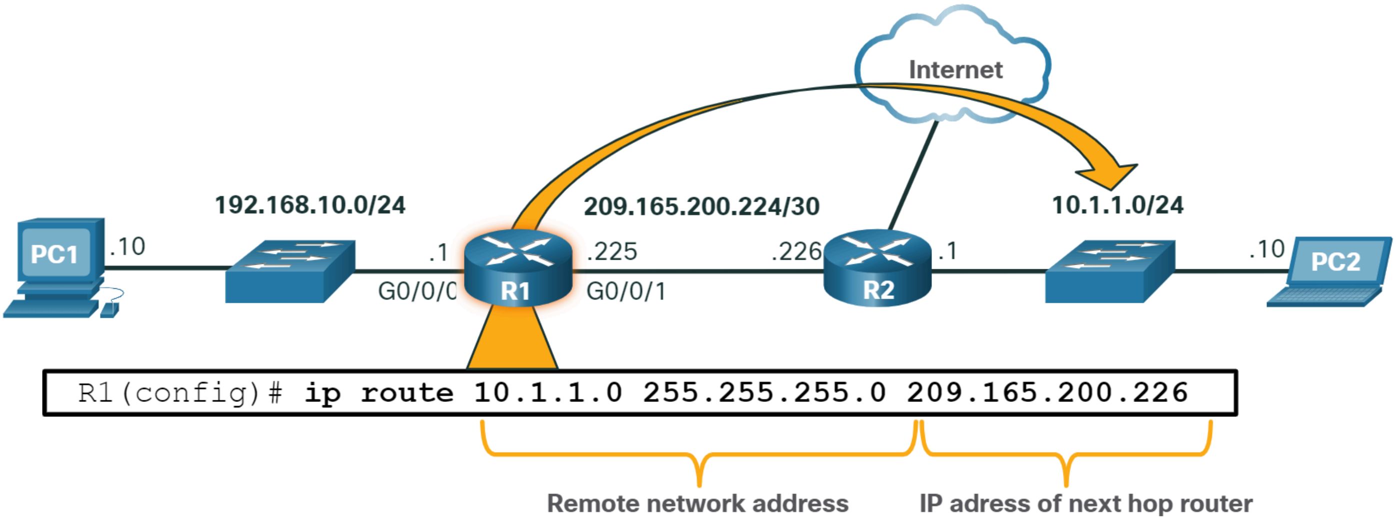
A router can learn about remote networks in one of two ways:

- **Manually** – Remote networks are manually entered into the route table using static routes.
- **Dynamically** – Remote routes are automatically learned using a dynamic routing protocol.

3. Static Routing

Static routes are route entries that are manually configured. The figure shows an example of a static route that was manually configured on router R1. The static route includes the remote network address and the IP address of the next hop router.

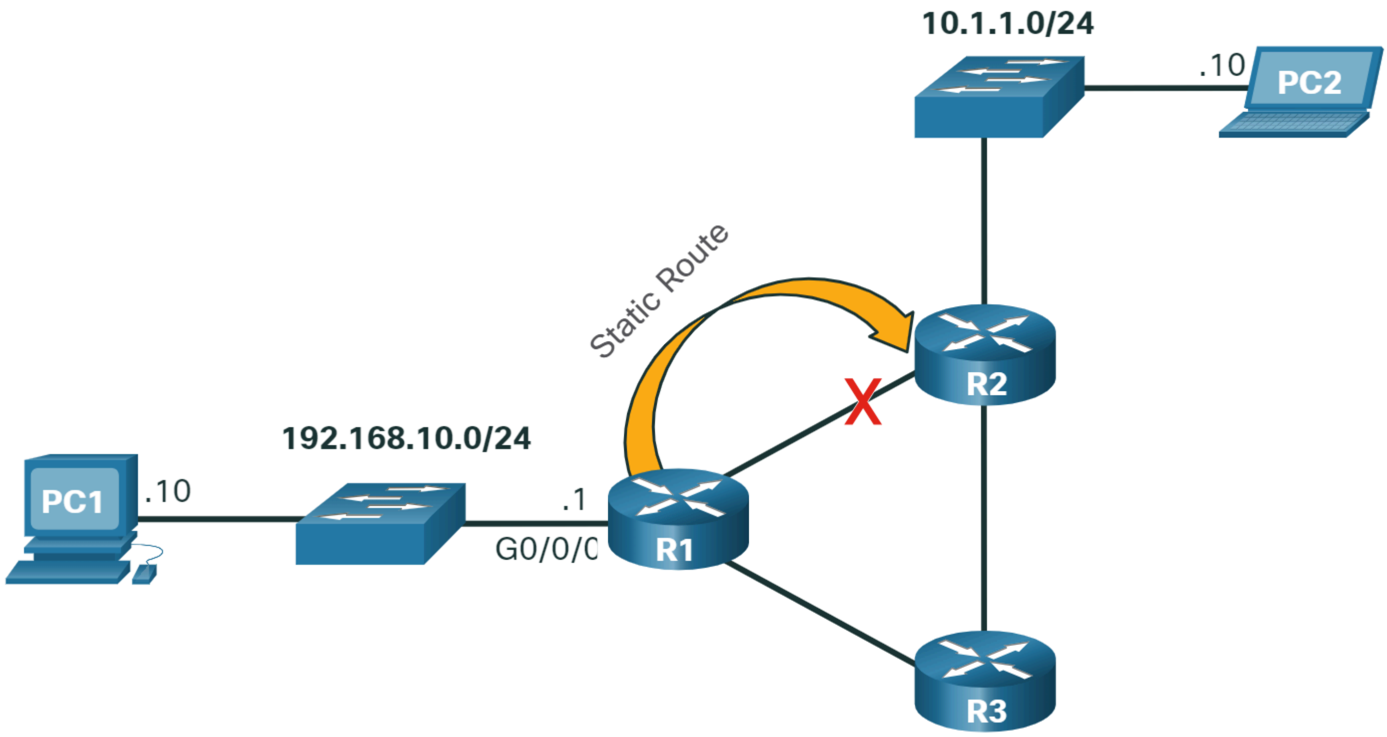
The diagram is a network topology showing a static route configuration to reach a remote network. Host PC1, with an address of .10, is connected to a switch on network 192.168.10.0/24 which is connected to the G0/0/0 interface of router R1 with an address of .1. Network 209.165.200.224/30 connects the G0/0/1 interface on R1, address .225, to another router, R2 at address .226. R2 has an interface with address .1 connected to a switch on network 10.1.1.0/24 to which host PC2, address .10, is connected. R2 also has a connection to the Internet cloud. A static route configuration on R1 to the network 10.1.1.0/24 reads: R1(config)#ip route 10.1.1.0 255.255.255.0 209.165.200.226. In the configuration, 10.1.1.0 255.255.255.0 is labeled remote network and 209.165.200.226 is labeled IP address of the next hop router.



```
R1(config)# ip route 10.1.1.0 255.255.255.0 209.165.200.226
```

R1 is manually configured with a static route to reach the 10.1.1.0/24 network. If this path changes, R1 will require a new static route.

If there is a change in the network topology, the static route is not automatically updated and must be manually reconfigured. For example, in the figure R1 has a static route to reach the 10.1.1.0/24 network via R2. If that path is no longer available, R1 would need to be reconfigured with a new static route to the 10.1.1.0/24 network via R3. Router R3 would therefore need to have a route entry in its routing table to send packets destined for 10.1.1.0/24 to R2.



If the route from R1 via R2 is no longer available, a new static route via R3 would need to be configured. A static route does not automatically adjust for topology changes.

Static routing has the following characteristics:

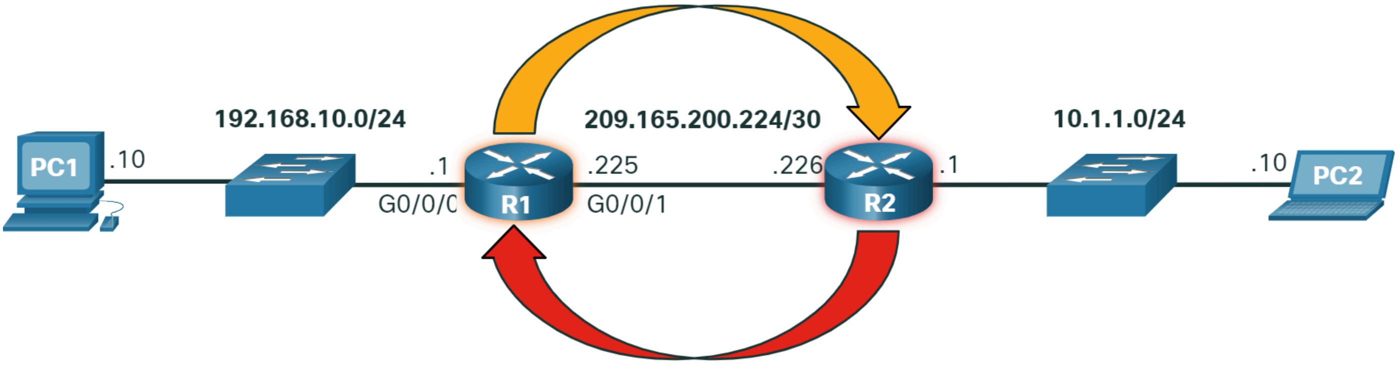
- A static route must be configured manually.
- The administrator needs to reconfigure a static route if there is a change in the topology and the static route is no longer viable.
- A static route is appropriate for a small network and when there are few or no redundant links.
- A static route is commonly used with a dynamic routing protocol for configuring a default route.

4. Dynamic Routing

A dynamic routing protocol allows the routers to automatically learn about remote networks, including a default route, from other routers. Routers that use dynamic routing protocols automatically share routing information with other routers and compensate for any topology changes without involving the network administrator. If there is a change in the network topology, routers share this information using the dynamic routing protocol and automatically update their routing tables.

Dynamic routing protocols include OSPF and Enhanced Interior Gateway Routing Protocol (EIGRP). The figure shows an example of routers R1 and R2 automatically sharing network information using the routing protocol OSPF.

The diagram is a network topology showing routers using dynamic routing protocols to exchange information. Host PC1, with an address of .10, is connected to a switch on network 192.168.10.0/24 which is connected to the G0/0/0 interface of router R1 with an address of .1. Network 209.165.200.224/30 connects the G0/0/1 interface on R1, address .225, to another router, R2 at address .226. R2 has an interface with address .1 connected to a switch on network 10.1.1.0/24 to which host PC2, address .10, is connected. Arrows show R1 and R2 sharing information with each other.

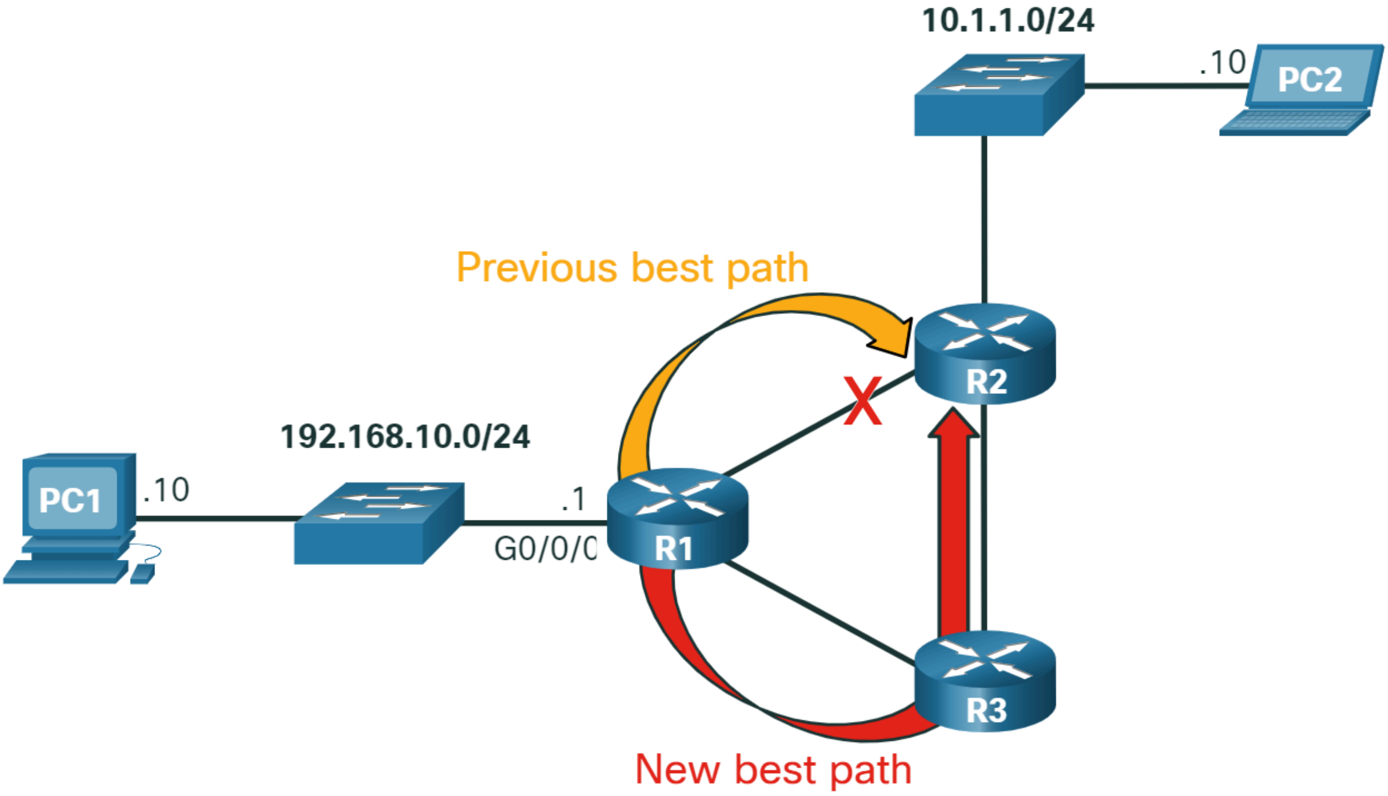


- R1 is using the routing protocol OSPF to let R2 know about the 192.168.10.0/24 network.
- R2 is using the routing protocol OSPF to let R1 know about the 10.1.1.0/24 network.

Basic configuration only requires the network administrator to enable the directly connected networks within the dynamic routing protocol. The dynamic routing protocol will automatically do as follows:

- Discover remote networks
- Maintain up-to-date routing information
- Choose the best path to destination networks
- Attempt to find a new best path if the current path is no longer available

When a router is manually configured with a static route or learns about a remote network dynamically using a dynamic routing protocol, the remote network address and next hop address are entered into the IP routing table. As shown in the figure, if there is a change in the network topology, the routers will automatically adjust and attempt to find a new best path.



R1, R2, and R3 are using the dynamic routing protocol OSPF. If there is a network topology change, they can automatically adjust to find a new best path.

Note: It is common for some routers to use a combination of both static routes and a dynamic routing protocol.

5. Video- IPv4 Router Routing Tables

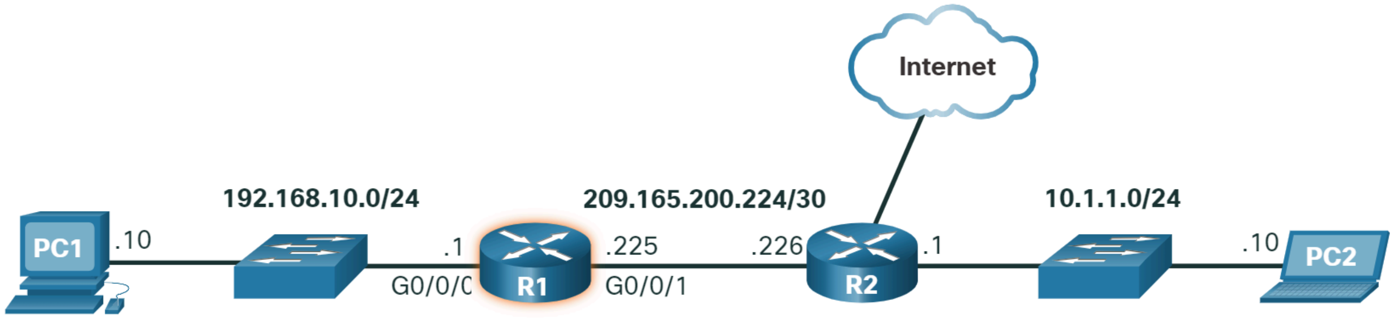
Unlike a host computer routing table, there are no column headings identifying the information contained in the routing table of a router. It is important to learn the meaning of the different items included in each entry of the routing table.

Click Play in the figure to view an introduction to the IPv4 routing table.

6. Introduction to an IPv4 Routing Table

Notice in the figure that R2 is connected to the internet. Therefore, the administrator configured R1 with a default static route sending packets to R2 when there is no specific entry in the routing table that matches the destination IP address. R1 and R2 are also using OSPF routing to advertise directly connected networks.

Host PC1, with an address of .10, is connected to a switch on network 192.168.10.0/24 which is connected to the G0/0/0 interface of router R1 with an address of .1. Network 209.165.200.224/30 connects the G0/0/1 interface on R1, address .225, to another router, R2 at address .226. R2 is connected to a switch on network 10.1.1.0/24 to which host PC2, address .10, is connected. R2 also has a connection to the Internet cloud.



```
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
       i - IS-IS, su - IS-IS summary, 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, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
Gateway of last resort is 209.165.200.226 to network 0.0.0.0
S*    0.0.0.0/0 [1/0] via 209.165.200.226, GigabitEthernet0/0/1
      10.0.0.0/24 is subnetted, 1 subnets
O        10.1.1.0 [110/2] via 209.165.200.226, 00:02:45, GigabitEthernet0/0/1
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, GigabitEthernet0/0/0
L        192.168.10.1/32 is directly connected, GigabitEthernet0/0/0
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.200.224/30 is directly connected, GigabitEthernet0/0/1
L        209.165.200.225/32 is directly connected, GigabitEthernet0/0/1
R1#
```

The **show ip route** privileged EXEC mode command is used to view the IPv4 routing table on a Cisco IOS router. The example shows the IPv4 routing table of router R1. At the beginning of each routing table entry is a code that is used to identify the type of route or how the route was learned. Common route sources (codes) include these:

- **L** - Directly connected local interface IP address
- **C** – Directly connected network
- **S** – Static route was manually configured by an administrator
- **O** - OSPF
- **D** - EIGRP

The routing table displays all of the known IPv4 destination routes for R1.

A directly connected route is automatically created when a router interface is configured with IP address information and is activated. The router adds two route entries with the codes **C** (i.e., the connected network) and **L** (i.e., the local interface IP address of the connected network). The route entries also identify the exit interface to use to reach the network. The two directly connected networks in this example are 192.168.10.0/24 and 209.165.200.224/30.

Routers R1 and R2 are also using the OSPF dynamic routing protocol to exchange router information. In the example routing table, R1 has a route entry for the 10.1.1.0/24 network that it learned dynamically from router R2 via the OSPF routing protocol.

A default route has a network address of all zeroes. For example, the IPv4 network address is 0.0.0.0. A static route entry in the routing table begins with a code of **S***, as highlighted in the example.

7. Check Your Understanding - Introduction to Routing

Check your understanding of the introduction to routing by choosing the correct answer to the following questions.

Question 1: What is the command used on a Cisco IOS router to view the routing table?

(a) netstart -r

(b) route print

(c) show ip route

(d) show routing table

Answer: **(c) -** The show ip route command is used to view the routing table on a Cisco router.

Question 2: What does a code of "O" indicate next to a route in the routing table?

(a) a directly connected route

(b) a route with an administrative distance of 0

(c) a gateway of last resort

(d) a route learned dynamically from OSPF

Answer: **(d) -** Codes at the beginning of each routing table entry are used to identify the type of route or how the route was learned. A code of "O" indicates the route was learned from OSPF.

Question 3: This type of route is also known as a gateway of last resort.

(a) static route

(b) remote route

(c) default route

(d) directly connected route

Answer: **(c) -** A default route is also known as a gateway of last resort.

Question 4: Which is a characteristic of static routes?

(a) They are manually configured.

(b) They are advertised to directly connected neighbors.

(c) They are appropriate when there are many redundant links.

(d) They automatically adjust to a change in network topology.

Answer: **(a) -** Static routes are manually configured and do not adjust to changes in the network topology and are not advertised to neighboring routers.

Question 5: True or False? A router can be configured with a combination of both static routes and a dynamic routing protocol.

(a) True

(b) False

Answer: **(a) -** The correct answer is True. Routers can be configured with static routes and with a dynamic routing protocol.

Module Practice and Quiz

1. What did I learn in this module?

1A. Network Layer Characteristics

The network layer (OSI Layer 3) provides services to allow end devices to exchange data across networks. IPv4 and IPv6 are the principle network layer communication protocols. The network layer also includes the routing protocol OSPF and messaging protocols such as ICMP. Network layer protocols perform four basic operations: addressing end devices, encapsulation, routing, and de-encapsulation. IPv4 and IPv6 specify the packet structure and processing used to carry the data from one host to another host. IP encapsulates the transport layer segment by adding an IP header, which is used to deliver the packet to the destination host. The IP header is examined by Layer 3 devices (i.e., routers) as it travels across a network to its destination. The characteristics of IP are that it is connectionless, best effort, and media independent. IP is connectionless, meaning that no dedicated end-to-end connection is created by IP before data is sent. The IP protocol does not guarantee that all packets that are delivered are, in fact, received. This is the definition of the unreliable, or best effort characteristic. IP operates independently of the media that carry the data at lower layers of the protocol stack.

1B. IPv4 Packet

An IPv4 packet header consists of fields containing information about the packet. These fields contain binary numbers which are examined by the Layer 3 process. The binary values of each field identify various settings of the IP packet. Significant fields in the IPv4 packet header include: version, DS, header checksum, TTL, protocol, and the source and destination IPv4 addresses.

1C. IPv6 Packet

IPv6 is designed to overcome the limitations of IPv4 including: IPv4 address depletion, lack of end-to-end connectivity, and increased network complexity. IPv6 increases the available address space, improves packet handling, and eliminates the need for NAT. The fields in the IPv6 packet header include: version, traffic class, flow label, payload length, next header, hop limit, and the source and destination IPv6 addresses.

1D. How a Host Routes

A host can send a packet to itself, another local host, and a remote host. In IPv4, the source device uses its own subnet mask along with its own IPv4 address and the destination IPv4 address to determine whether the destination host is on the same network. In IPv6, the local router advertises the local network address (prefix) to all devices on the network, to make this determination. The default gateway is the network device (i.e., router) that can route traffic to other networks. On a network, a default gateway is usually a router that has a local IP address in the same address range as other hosts on the local network, can accept data into the local network and forward data out of the local network, and route traffic to other networks. A host routing table will typically include a default gateway. In IPv4, the host receives the IPv4 address of the default gateway either dynamically via DHCP or it is configured manually. In IPv6, the router advertises the default gateway address, or the host can be configured manually. On a Windows host, the route print or netstat -r command can be used to display the host routing table.

1E. Introduction to Routing

When a host sends a packet to another host, it consults its routing table to determine where to send the packet. If the destination host is on a remote network, the packet is forwarded to the default gateway which is usually the local router. What happens when a packet arrives on a router interface? The router examines the packet's destination IP address and searches its routing table to determine where to forward the packet. The routing table contains a list of all known network addresses (prefixes) and where to forward the packet. These entries are known as route entries or routes. The router will forward the packet using the best (longest) matching route entry. The routing table of a router stores three types of route entries: directly connected networks, remote networks, and a default route. Routers learn about remote networks manually, or dynamically using a dynamic routing protocol. Static routes are route entries that are manually configured. Static routes include the remote network address and the IP address of the next hop router. OSPF and EIGRP are two dynamic routing protocols. The show ip route privileged EXEC mode command is used to view the IPv4 routing table on a Cisco IOS router. At the beginning of an IPv4 routing table is a code that is used to identify the type of route or how the route was learned. Common route sources (codes) include:

- **L** - Directly connected local interface IP address
- **C** - Directly connected network
- **S** - Static route was manually configured by an administrator
- **O** - Open Shortest Path First (OSPF)
- **D** - Enhanced Interior Gateway Routing Protocol (EIGRP)

2. Module Quiz - Network Layer

Question 1: Which command can be used on a Windows host to display the routing table?

(a) netstat -s

(b) show ip route

(c) netstat -r

(d) tracert

Answer: (c) - On a Windows host, either the route print or netstat -r commands can be used to display the host routing table. The show ip route command is used on a router to display its routing table. The netstat –s command is used to display per-protocol statistics. The tracert command is used to display the path that a packet travels to its destination.

Question 2: What information is added during encapsulation at OSI Layer 3?

(a) source and destination MAC

(b) source and destination application protocol

(c) source and destination port number

(d) source and destination IP address

Answer: (d) - IP is a Layer 3 protocol. Layer 3 devices can open the Layer 3 header to inspect the Layer 3 header which contains IP-related information including the source and destination IP addresses.

Question 3: How does the network layer use the MTU value?

(a) The network layer depends on the higher level layers to determine the MTU.

(b) The network layer depends on the data link layer to set the MTU, and adjusts the speed of transmission

(c) to accommodate it.

(d) The MTU is passed to the network layer by the data link layer.

(e) To increase speed of delivery, the network layer ignores the MTU.

Answer: (c) - The data link layer indicates to the network layer the MTU for the medium that is being used. The network layer uses that information to determine how large the packet can be when it is forwarded. When packets are received on one medium and forwarded on a medium with a smaller MTU, the network layer device can fragment the packet to accommodate the smaller size.

Question 4: Which characteristic describes an IPv6 enhancement over IPv4?

(a) IPv6 addresses are based on 128-bit flat addressing as opposed to IPv4 which is based on 32-bit hierarchical addressing.

(b) The IPv6 header is simpler than the IPv4 header is, which improves packet handling.

(c) Both IPv4 and IPv6 support authentication, but only IPv6 supports privacy capabilities.

(d) The IPv6 address space is four times bigger than the IPv4 address space.

Answer: **(b) -** IPv6 addresses are based on 128-bit hierarchical addressing, and the IPv6 header has been simplified with fewer fields, improving packet handling. IPv6 natively supports authentication and privacy capabilities as opposed to IPv4 that needs additional features to support those. The IPv6 address space is many times bigger than IPv4 address space.

Question 5: When a connectionless protocol is in use at a lower layer of the OSI model, how is missing data detected and retransmitted if necessary?

(a) Connectionless acknowledgements are used to request retransmission.

(b) Upper-layer connection-oriented protocols keep track of the data received and can request retransmission from the upper-level protocols on the sending host.

(c) Network layer IP protocols manage the communication sessions if connection-oriented transport services are not available.

(d) The best-effort delivery process guarantees that all packets that are sent are received.

Answer: **(b) -** When connectionless protocols are in use at a lower layer of the OSI model, upper-level protocols may need to work together on the sending and receiving hosts to account for and retransmit lost data. In some cases, this is not necessary, because for some applications a certain amount of data loss is tolerable.

Question 6: What was the reason for the creation and implementation of IPv6?

(a) to make reading a 32-bit address easier

(b) to relieve IPv4 address depletion

(c) to provide more address space in the Internet Names Registry

(d) to allow NAT support for private addressing

Answer: **(b) -** IPv4 addressing space is exhausted by the rapid growth of the Internet and the devices connected to the Internet. IPv6 expands the IP addressing space by increasing the address length from the 32 bits to 128 bits, which should provide sufficient addresses for future Internet growth needs for many years to come.

Question 7: Which statement accurately describes a characteristic of IPv4?

(a) All IPv4 addresses are assignable to hosts.

(b) IPv4 has a 32-bit address space.

(c) An IPv4 header has fewer fields than an IPv6 header has.

(d) IPv4 natively supports IPsec.

Answer: **(b) -** IPv4 has a 32-bit address space, providing 4,294,967,296 unique addresses, but only 3.7 billion are assignable, a limit due to address reservation for multicasting and testing. IPv4 does not provide native support for IPsec. IPv6 has a simplified header with fewer fields than IPv4 has.

Question 8: Which field in an IPv4 packet header will typically stay the same during its transmission?

(a) Flag

(b) Time-to-Live

(c) Packet Length

(d) Destination Address

Answer: **(d) -** The value in the Destination Address field in an IPv4 header will stay the same during its transmission. The other options might change during its transmission.

Question 9: When a router receives a packet, what information must be examined in order for the packet to be forwarded to a remote destination?

(a) destination MAC address

(b) source IP address

(c) destination IP address

(d) source MAC address

Answer: **(c) -** When a router receives a packet, it examines the destination address of the packet and uses the routing table to search for the best path to that network.

Question 10: Which field in an IPv6 packet is used by the router to determine if a packet has expired and should be dropped?

(a) TTL

(b) Hop Limit

(c) Address Unreachable

(d) No Route to Destination

Answer: **(b) -** ICMPv6, like IPv4, sends a Time Exceeded message if the router cannot forward an IPv6 packet because the packet has expired. However, the IPv6 packet does not have a TTL field. Instead, it uses the Hop Limit field to determine if the packet has expired.

Question 11: Which information is used by routers to forward a data packet toward its destination?

(a) source IP address

(b) destination IP address

(c) source data-link address

(d) destination data-link address

Answer: **(b) -** The destination IP address is the IP address for the receiving device. This IP address is used by routers to forward the packet to its destination.

Question 12: A computer has to send a packet to a destination host in the same LAN. How will the packet be sent?

(a) The packet will be sent to the default gateway first, and then, depending on the response from the gateway, it may be sent to the destination host.

(b) The packet will be sent directly to the destination host.

(c) The packet will first be sent to the default gateway, and then from the default gateway it will be sent directly to the destination host.

(d) The packet will be sent only to the default gateway.

Answer: **(b) -** If the destination host is in the same LAN as the source host, there is no need for a default gateway. A default gateway is needed if a packet needs to be sent outside the LAN.

Question 13: A router receives a packet from the Gigabit 0/0 interface and determines that the packet needs to be forwarded out the Gigabit 0/1 interface. What will the router do next?

(a) route the packet out the Gigabit 0/1 interface

(b) create a new Layer 2 Ethernet frame to be sent to the destination

(c) look into the ARP cache to determine the destination IP address

(d) look into the routing table to determine if the destination network is in the routing table

Answer: **(b) -** Once a router receives a packet and looks inside the header to determine the destination network, the router compares the destination network to the routing table to determine if the packet is to be routed or dropped. If routed, the router attaches a new Layer 2 header based on the technology that is used by the outgoing port that is used. The packet is then routed out the destination port as designated by the routing table. The ARP cache is used to match an IP address with a MAC address.

Question 14: Which IPv4 address can a host use to ping the loopback interface?

(a) 126.0.0.1

(b) 127.0.0.0

(c) 126.0.0.0

(d) 127.0.0.1

Answer: **(d) -** A host can ping the loopback interface by sending a packet to a special IPv4 address within the network 127.0.0.0/8.