Network Protocols and Services

Md Manirul Islam
Director, Institute of Continuing Education
American International University-Bangladesh

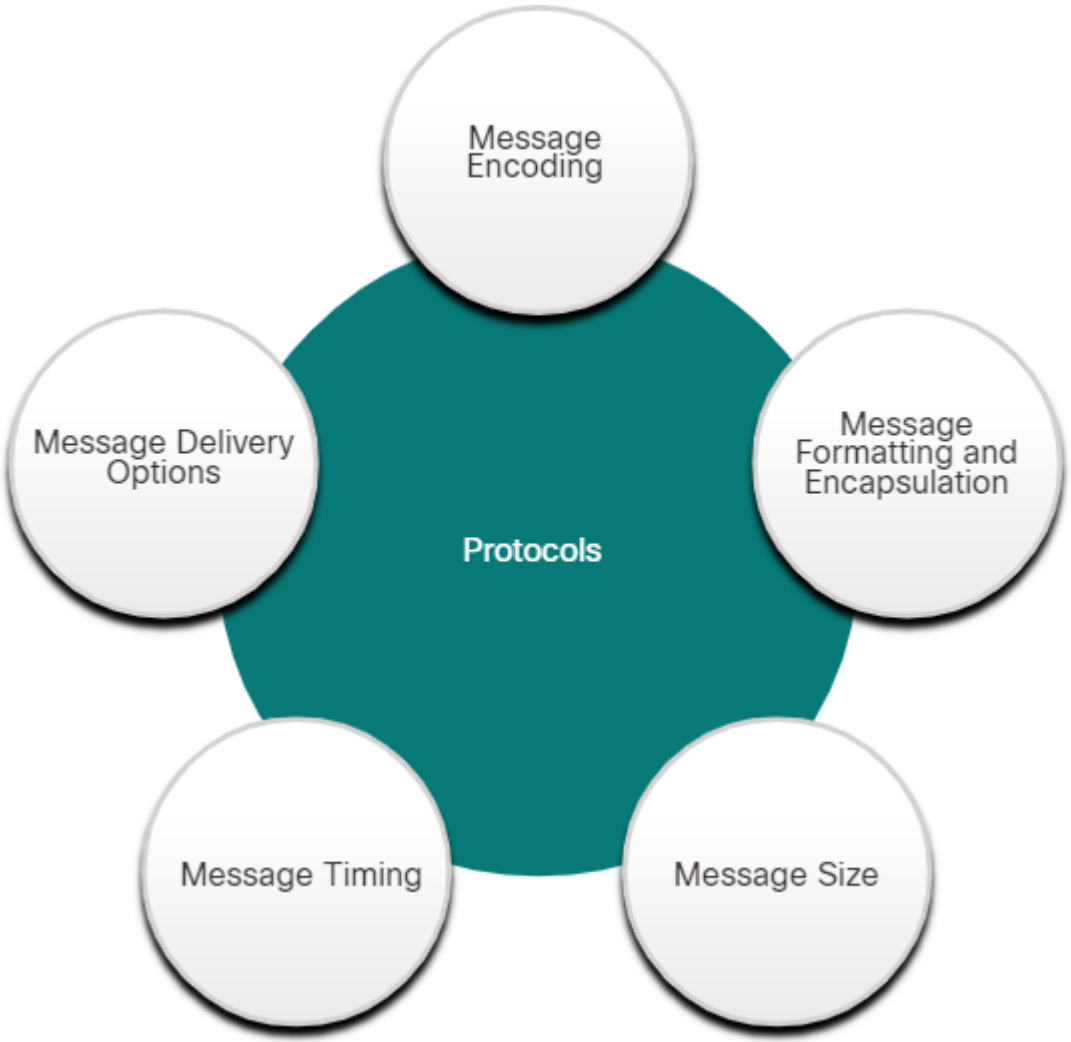
- Network Protocols
- Ethernet and Internet Protocols
- Connectivity Verification
- Address Resolution Protocol
- The Transport Layer
- Network Services

Network Protocols

Communications Protocols

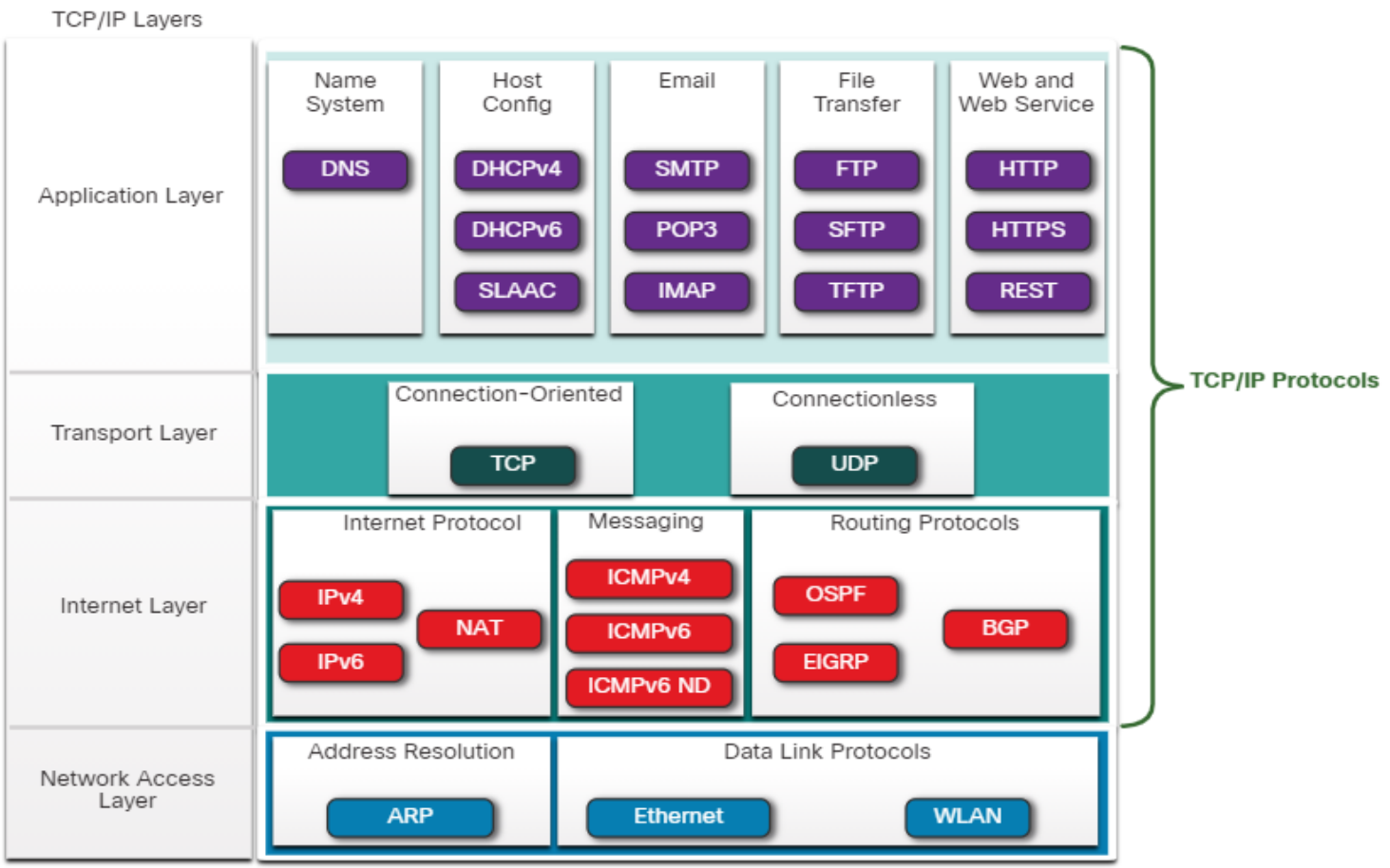
What are Protocols?

- Simply having a connection between end devices is not enough to enable communication. For communication to occur, devices must know “how” to communicate.
- Communication is governed by rules called protocols.
- These protocols are specific to the type of communication method occurring.
- Network protocols dictate the message encoding, formatting, encapsulation, size, timing, and delivery options.



The TCP/IP Protocol Suite

- TCP/IP has standardized the way the computers communicate and is the protocol suite used by the internet and the networks of today.
- TCP/IP protocols are specific to the application, transport, Internet, and network access layers.
- TCP/IP protocol suite is implemented on both the sending and receiving hosts to provide end-to-end delivery of messages over a network.

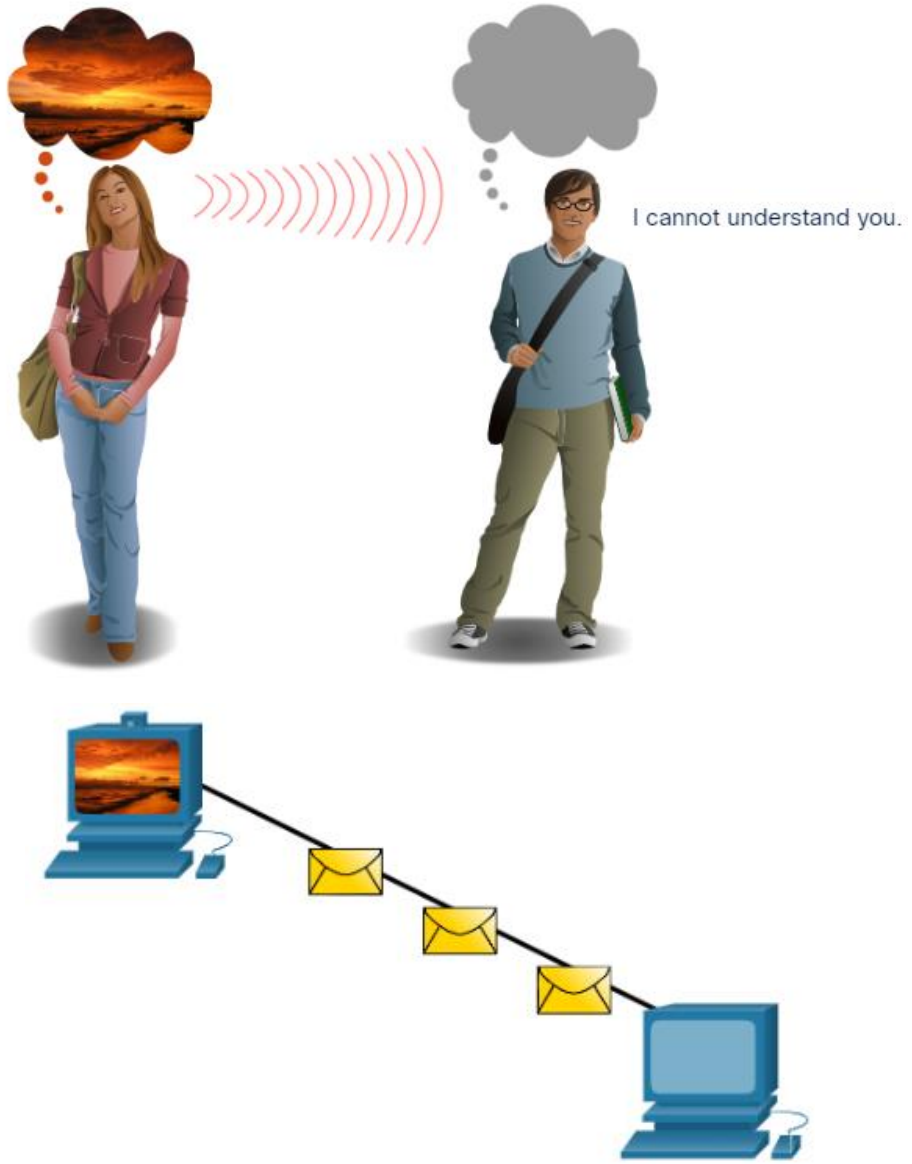


Message Formatting and Encapsulation

- When a message is sent from source to destination, it must use a specific format or structure. Message formats depend on the type of message and the channel that is used to deliver the message.
  - **Encapsulation** - process of placing one message format inside another message format.
  - **Decapsulation** - the reverse process of encapsulation.
- **Analogy**
  - A common example of requiring the correct format in human communications is when sending a letter. An envelope has the address of the sender and receiver, each located at the proper place on the envelope. If the destination address and formatting are not correct, the letter is not delivered.
  - Similar to sending a letter, a message that is sent over a computer network follows specific format rules for it to be delivered and processed. Internet Protocol (IP) is a protocol with a similar function to the envelope example.

Message Size

- Another rule of communication is **message size**.
- **Analogy**
  - When people communicate with each other, the messages that they send are usually broken into smaller parts or sentences.
  - These sentences are limited in size to what the receiving person can process at one time. It also makes it easier for the receiver to read and comprehend.
  - Likewise, when a long message is sent from one host to another over a network, it is necessary to break the message into smaller pieces. At the receiving host, the individual pieces of the message are reconstructed into the original message.



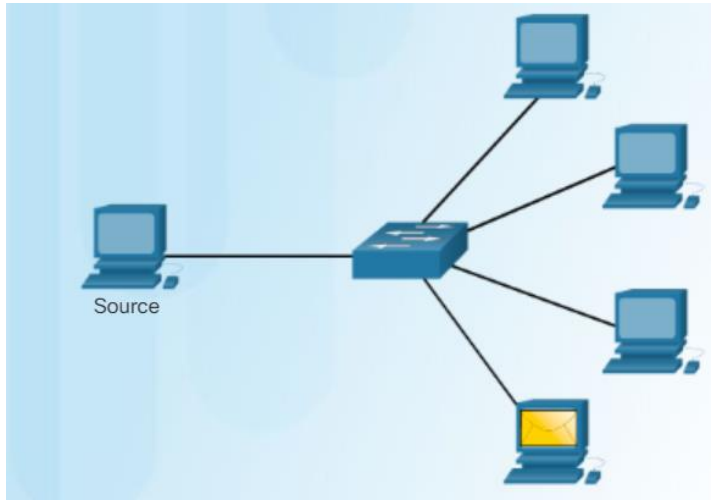
Message Timing

- Message timing includes the following:
  - **Flow Control -** Flow control defines how much information can be sent and the speed at which it can be delivered.
  - **Response Timeout -** Hosts on the network use network protocols that specify how long to wait for responses and what action to take if a response timeout occurs.
  - **Access method -** This determines when someone can send a message. When a device wants to transmit on a wireless LAN, it is necessary for the WLAN NIC to determine whether the wireless medium is available.

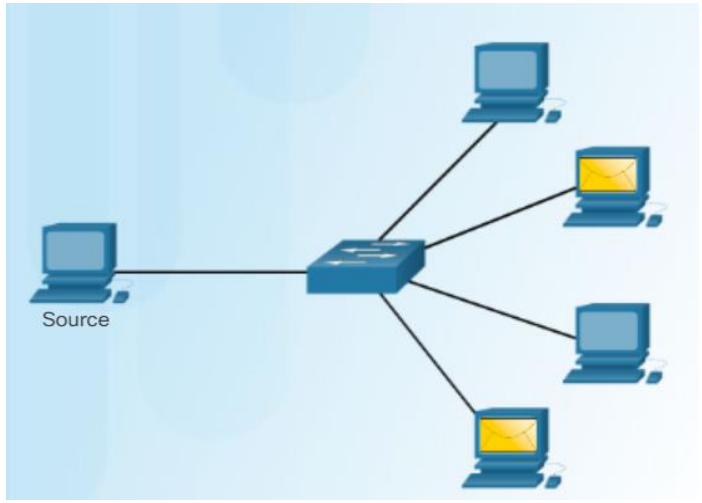
Unicast, Multicast, Broadcast

- A message can be delivered in different ways. Sometimes, a person wants to communicate information to a single individual. At other times, the person may need to send information to a group of people at the same time, or even to all people in the same area.

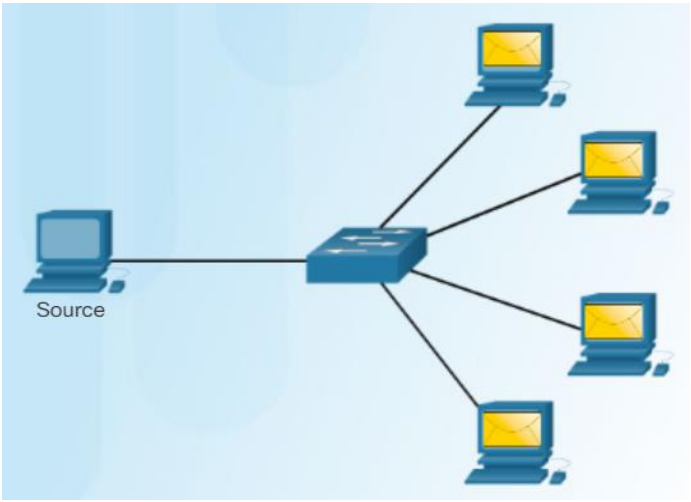
Unicast – one-to-one



Multicast – one-to-many

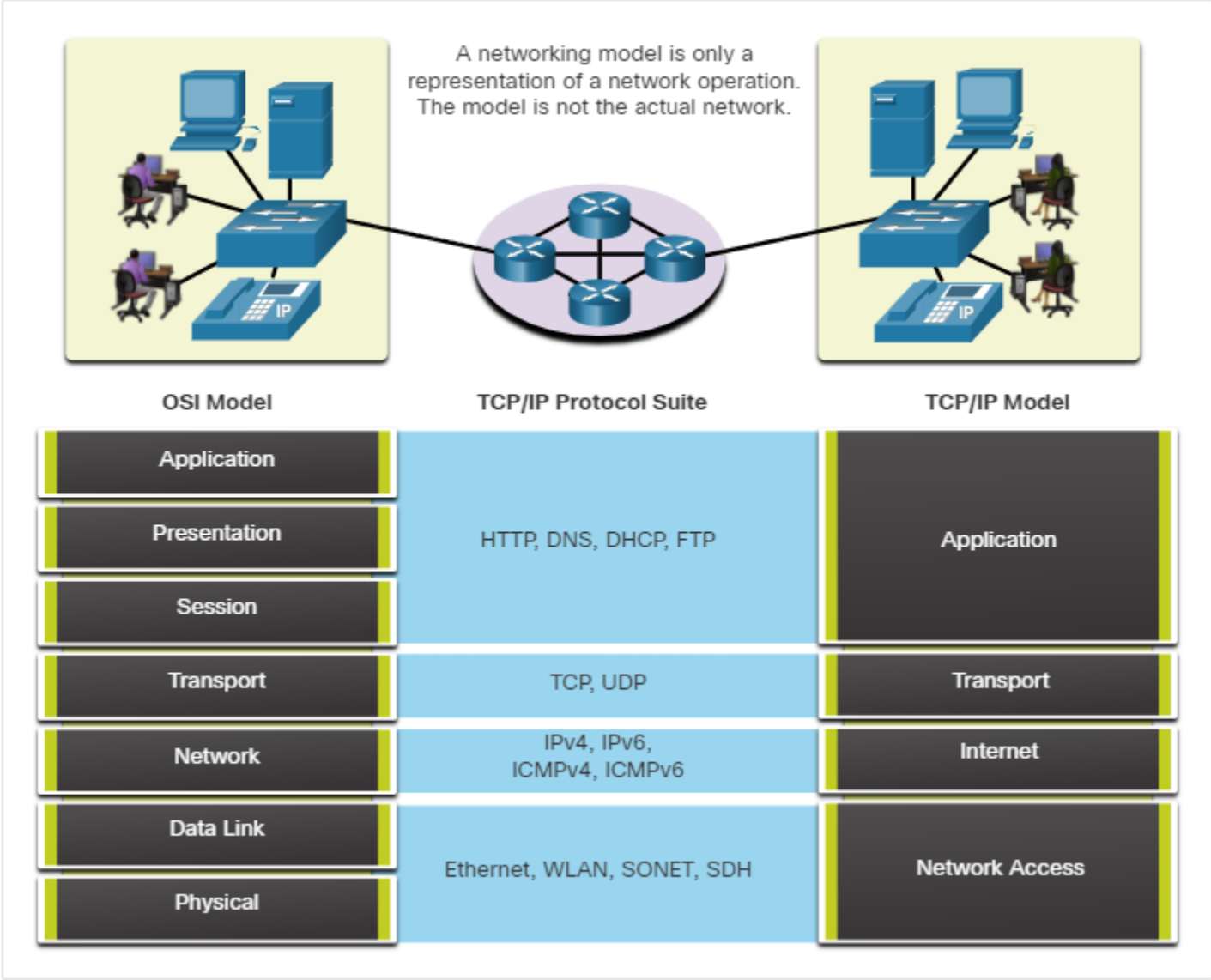


Broadcast – one-to-all



Reference Models

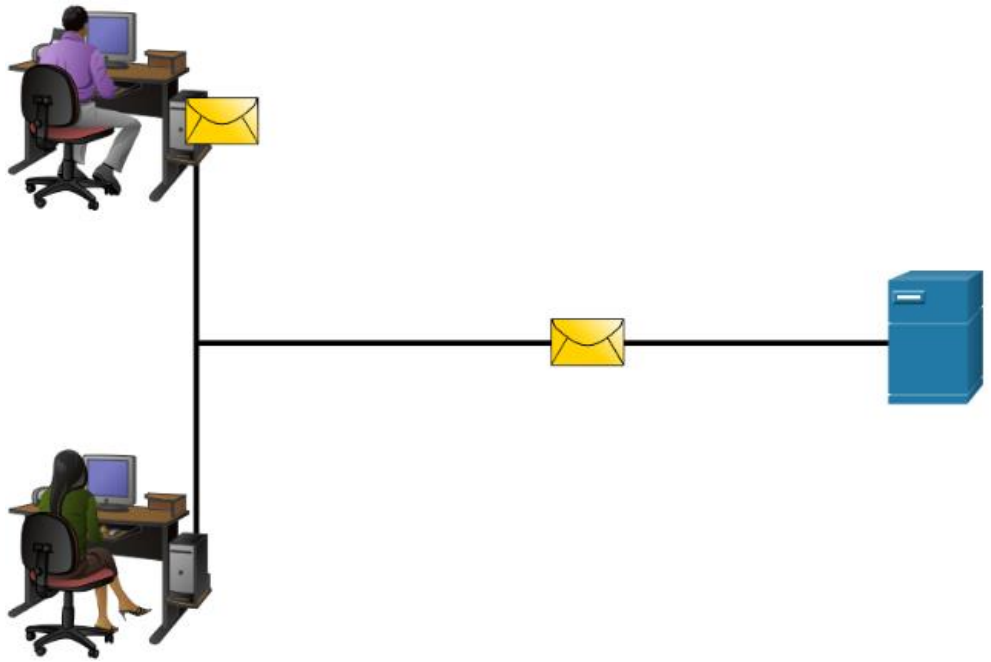
- A layered model is used to modularize the operations of a network into manageable layers.
- Two layered models that are used to describe network operations are:
  - **Open System Interconnection (OSI) Reference Model**
  - **TCP/IP Reference Model**
- The purpose of reference models is to define interoperability between network devices and software.



Data Encapsulation

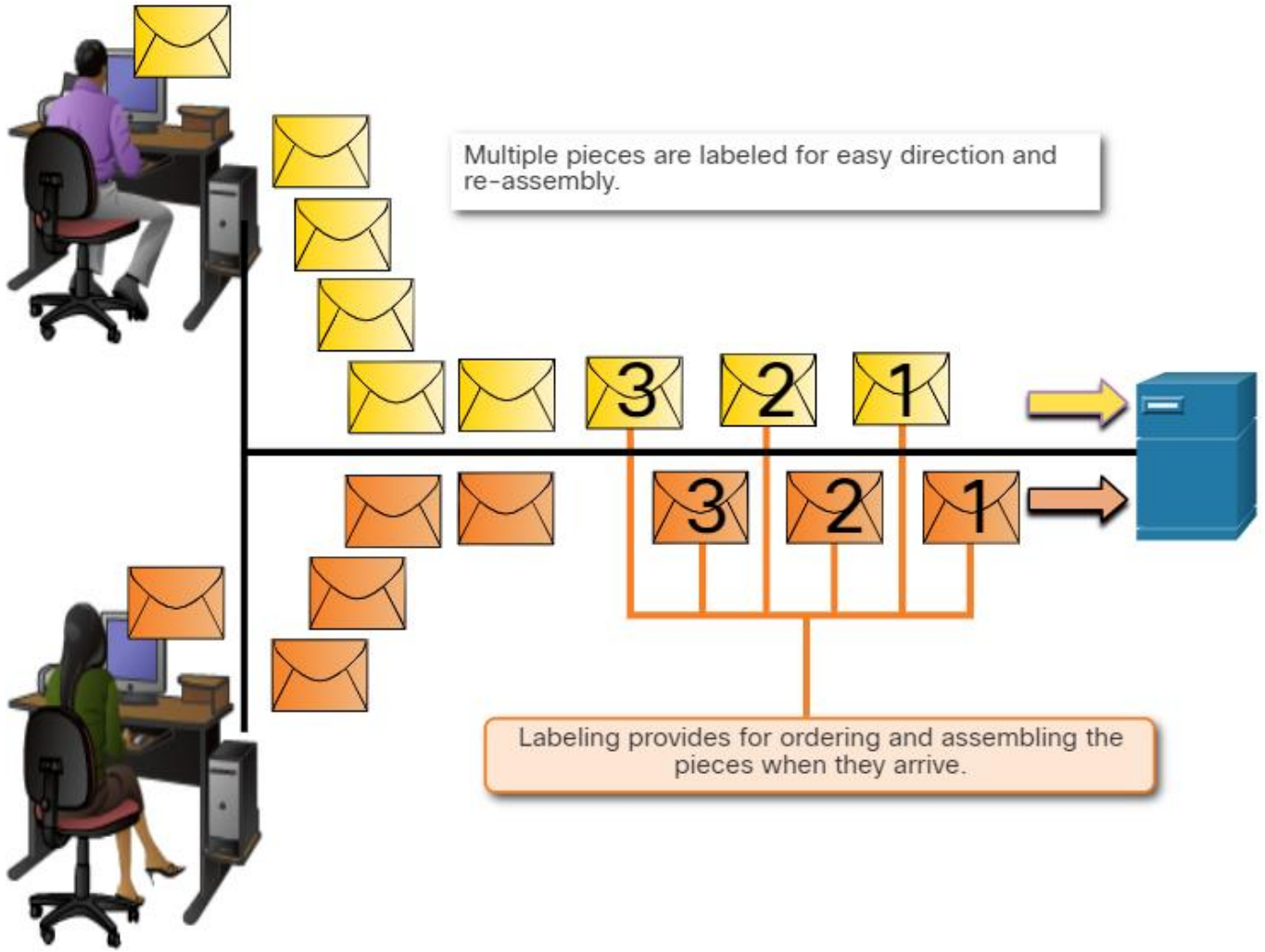
Segmenting Messages

- If large streams of data is sent across a network, it would result in delays. If any link in the interconnected network failed during the transmission, it will result in lost of complete message.
- Segmentation is the process of dividing a stream of data into smaller units for transmissions over the network.
- Segmenting messages has two primary benefits:
  - Increases speed
  - Increases efficiency



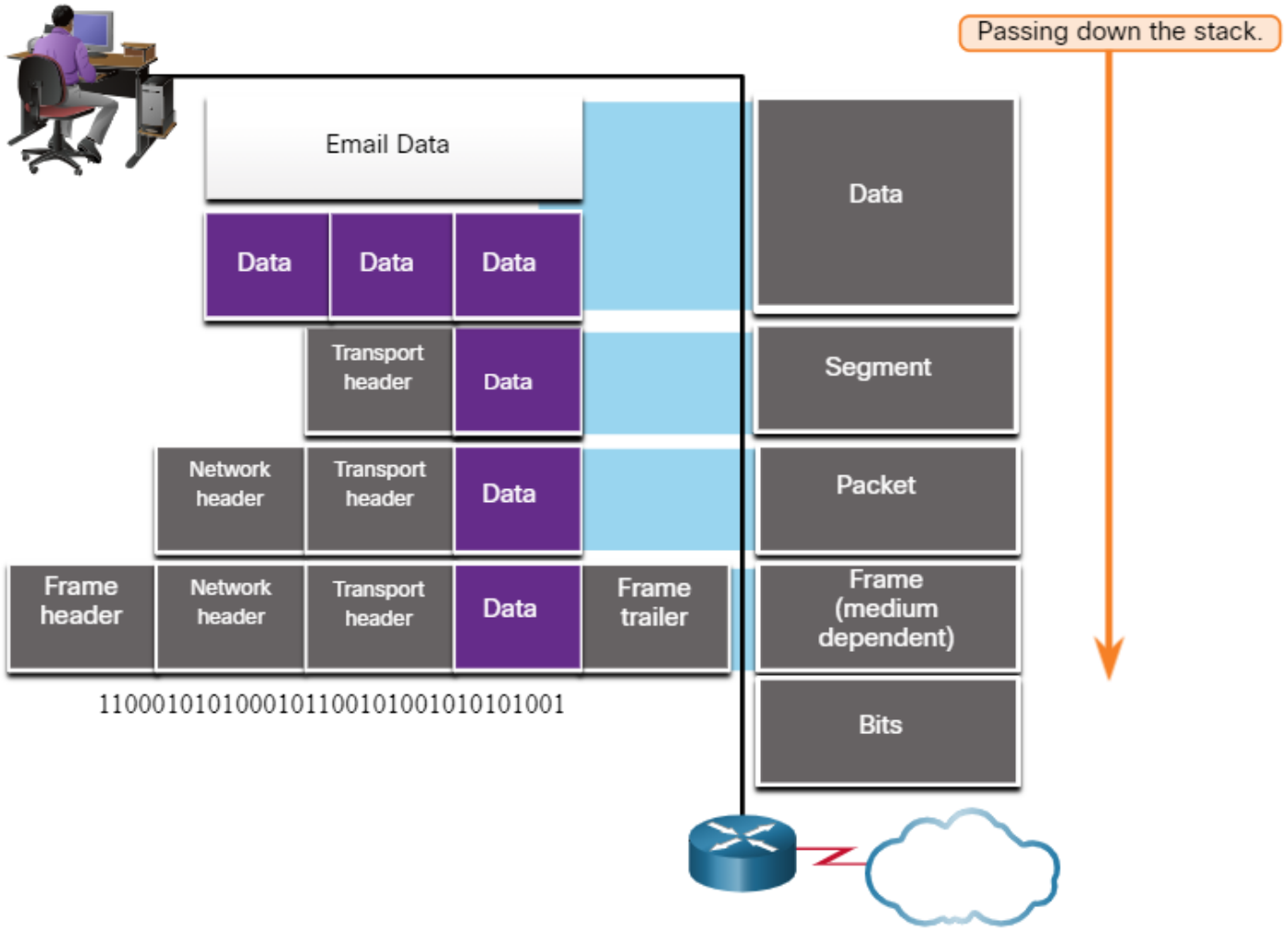
Sequencing

- While transmitting messages using segmentation and multiplexing, there is a possibility of data to reach the destination in a collapsed order.
- Each segment of the message must go through a sequencing process to ensure that it gets to the correct destination and can be reassembled similar to the content of the original message.
- TCP is responsible for sequencing the individual segments.



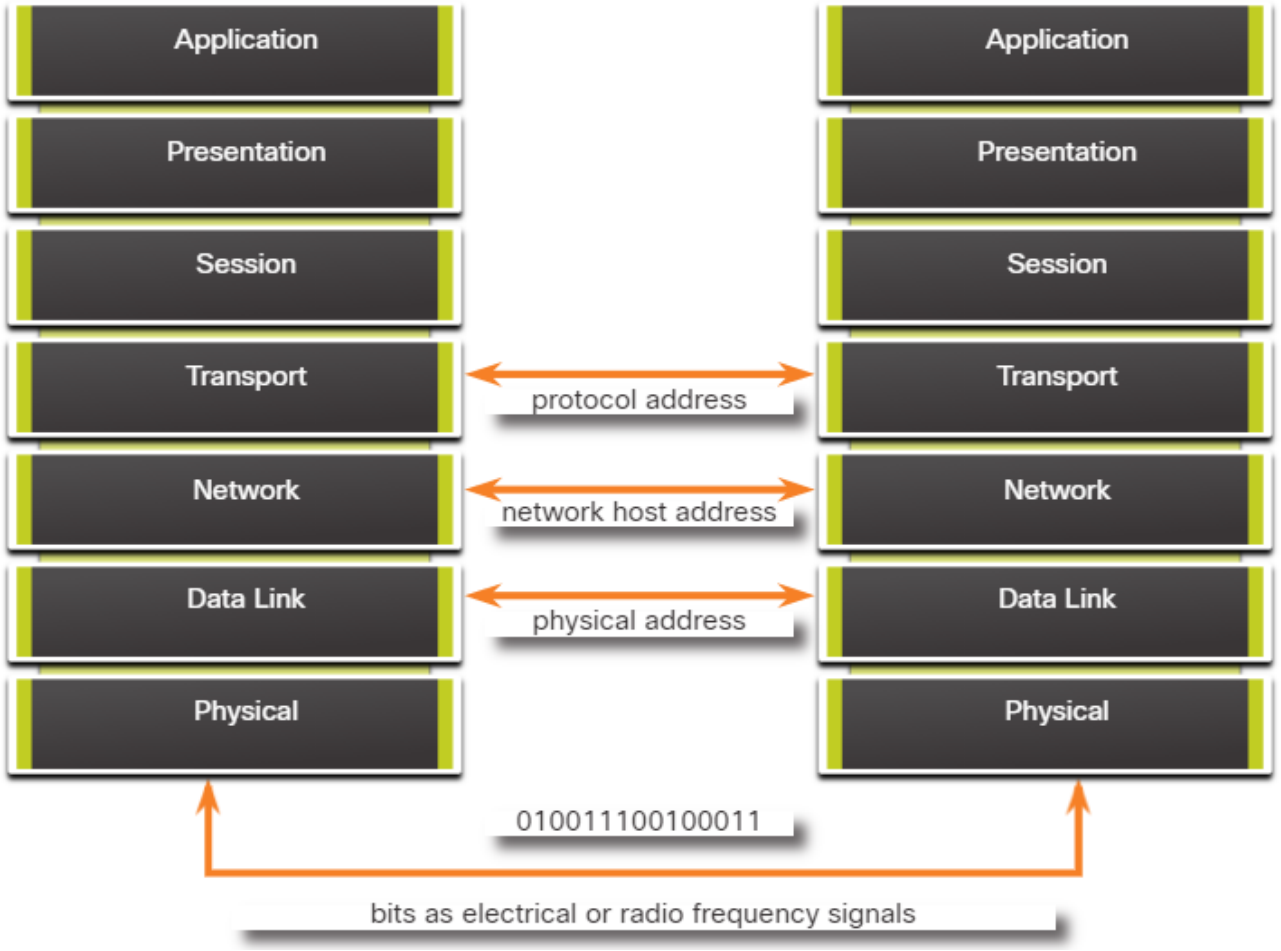
Protocol Data Units

- As application data is passed down the protocol stack on its way to be transmitted across the network media, various protocol information is added at each level.
- The form that a piece of data takes at any layer is called a Protocol Data Unit (PDU).
- At each stage of the process, a PDU has a different name to reflect its new functions.



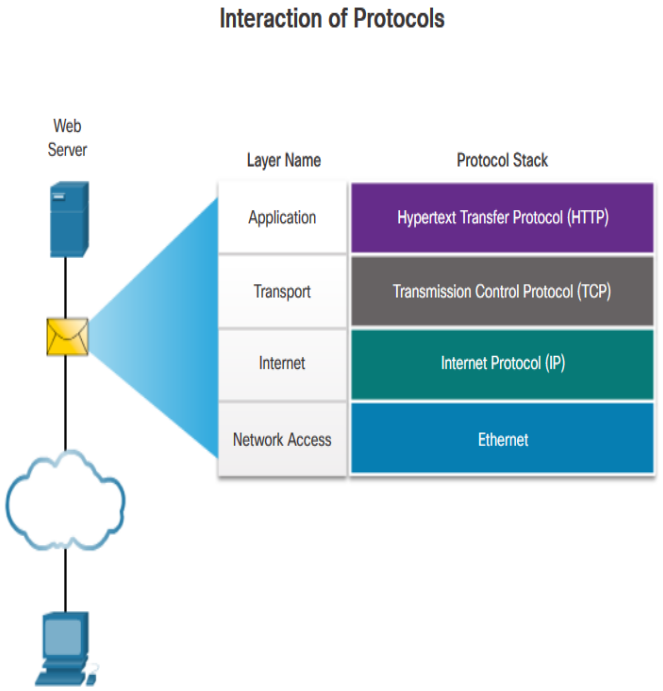
Three Addresses

- Network protocols require addresses to be used for network communication.
- The OSI transport, network, and data link layers use addressing in some form.
- The transport layer uses protocol addresses in the form of port numbers to identify network applications.
- The network layer specifies addresses that identify the networks that clients and servers are attached to.
- Data link layer specifies the devices on the local LAN that should handle data frames.
- All three addresses are required for client-server communication.



Scenario: Sending and Receiving a Web Page

- **HTTP** – This application protocol governs the way a web server and a web client interact.
- **TCP** – This transport protocol manages individual conversations. TCP divides the HTTP messages into smaller pieces, called segments. TCP is also responsible for controlling the size and rate at which messages are exchanged between the server and the client.
- **IP** – This is responsible for taking the formatted segments from TCP, encapsulating them into packets, assigning them the appropriate addresses, and delivering them to the destination host.
- **Ethernet** – This network access protocol is responsible for taking the packets from IP and formatting them to be transmitted over the media.

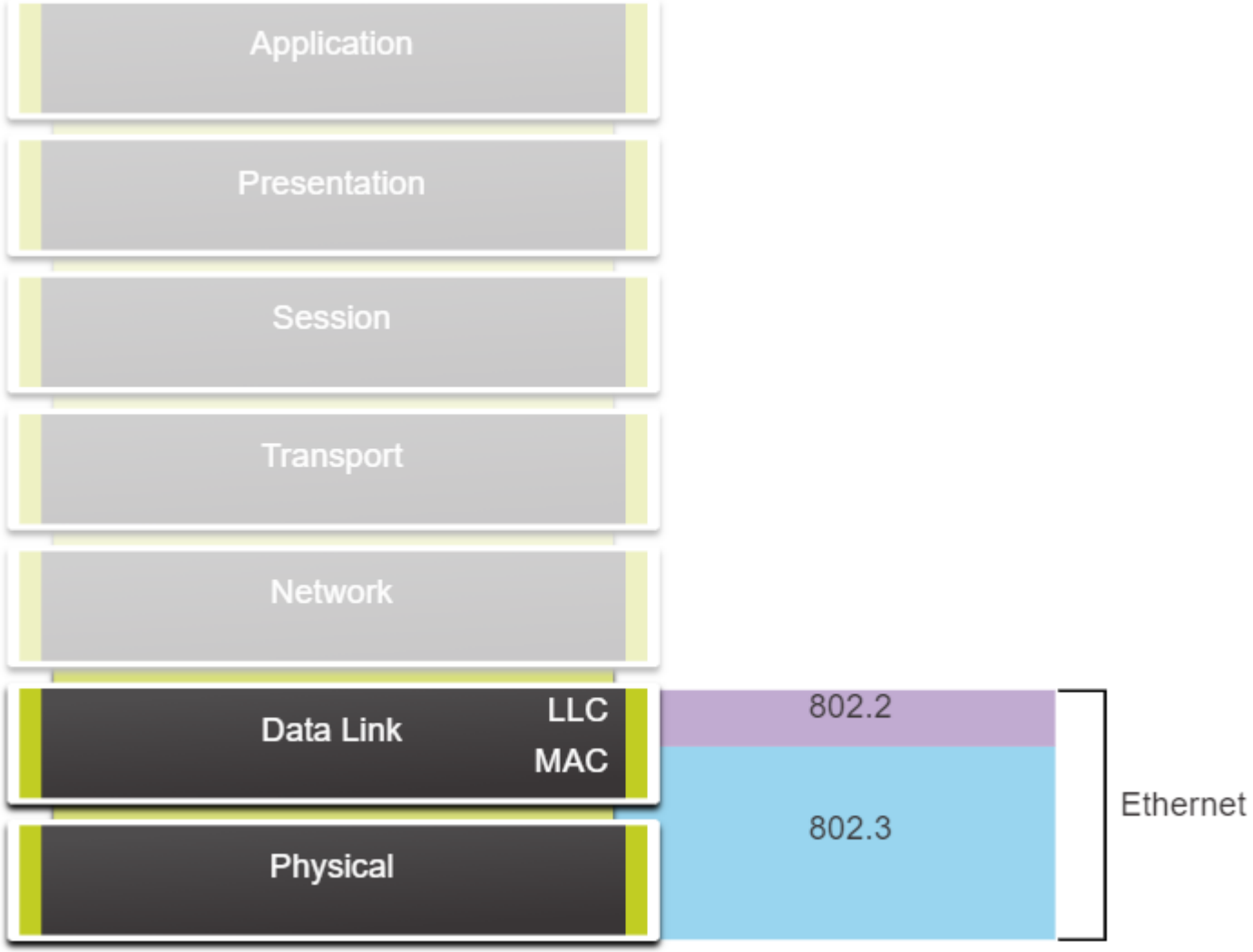


Ethernet and Internet Protocols

Ethernet

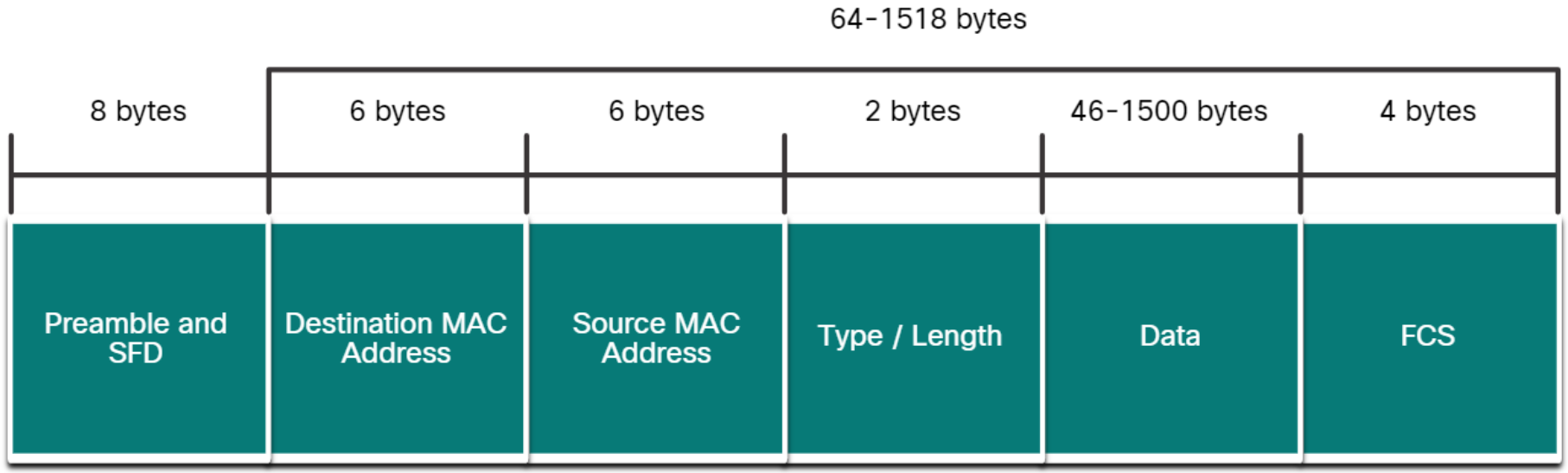
The Ethernet Protocol

- Unlike wireless, Ethernet uses wired communications, including twisted pair, fiber-optic links, and coaxial cables.
- Ethernet operates in the data link layer and physical layer.
- It is a family of networking technologies defined in the IEEE 802.2 and 802.3 standards.
- Ethernet supports data bandwidths from 10 Mbps to 100,000 Mbps (100 Gbps)



Ethernet Frame

- The minimum Ethernet frame size is 64 bytes, and the maximum is 1518 bytes.
- Two key identifiers
  - Destination MAC address
  - Source MAC address
- Any frame less than 64 bytes in length is considered a “collision fragment” or “runt frame” and is automatically discarded by receiving stations. Frames with more than 1500 bytes of data are considered “jumbo” or “baby giant frames”.

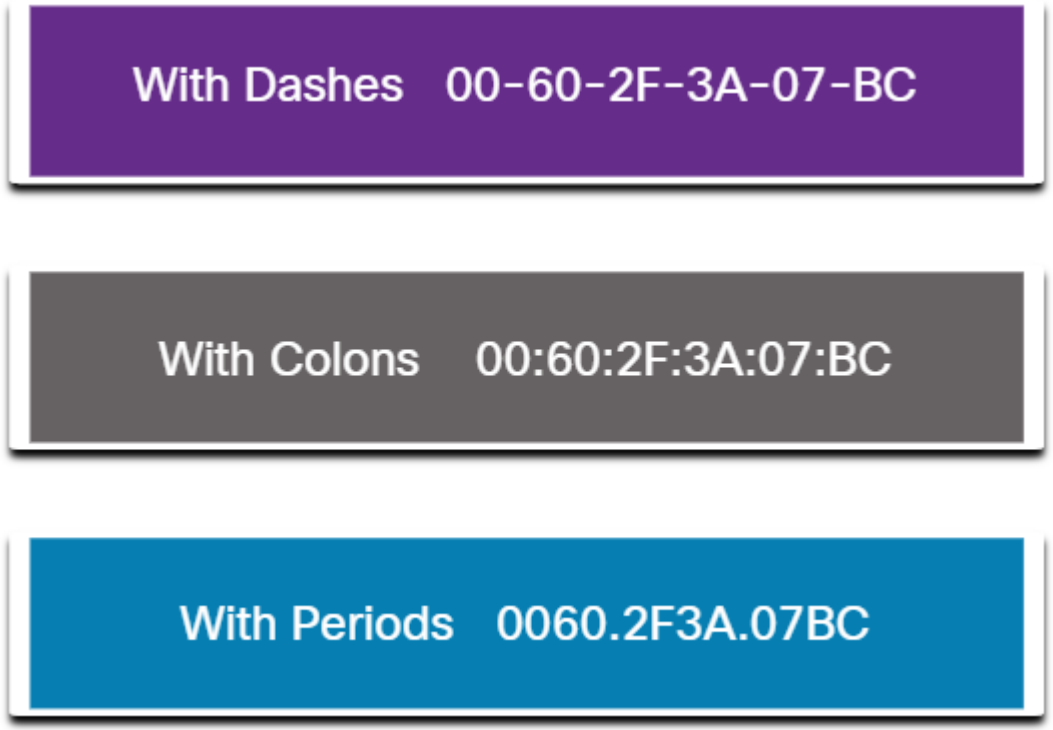


Ethernet Frame Fields

Field	Description
Preamble and Start Frame Delimiter	Used for synchronization between the sending and receiving devices.
Destination MAC Address	It is the identifier for the intended recipient. This address is used by Layer 2 to assist devices in determining if a frame is addressed to them. The address in the frame is compared to the MAC address in the device.
Source MAC Address	Identifies the originating NIC or interface of the frame.
Type / Length	Identifies the upper layer protocol encapsulated in the Ethernet frame.
Data Field	Contains the encapsulated data from a higher layer, an IPv4 packet.
Frame Check Sequence	Used to detect errors in a frame using Cyclic Redundancy Check (CRC).

MAC Address Format

- An Ethernet MAC address is a 48-bit binary value expressed as 12 hexadecimal digits.
- Depending on the device and the operating system, you will see various representations of MAC addresses.
- IPv6 addresses are another example of hexadecimal addressing.
- All data that travels on the network is encapsulated in Ethernet frames.
- A Cybersecurity analyst should be able to interpret the Ethernet data that is captured by protocol analyzers and other tools.

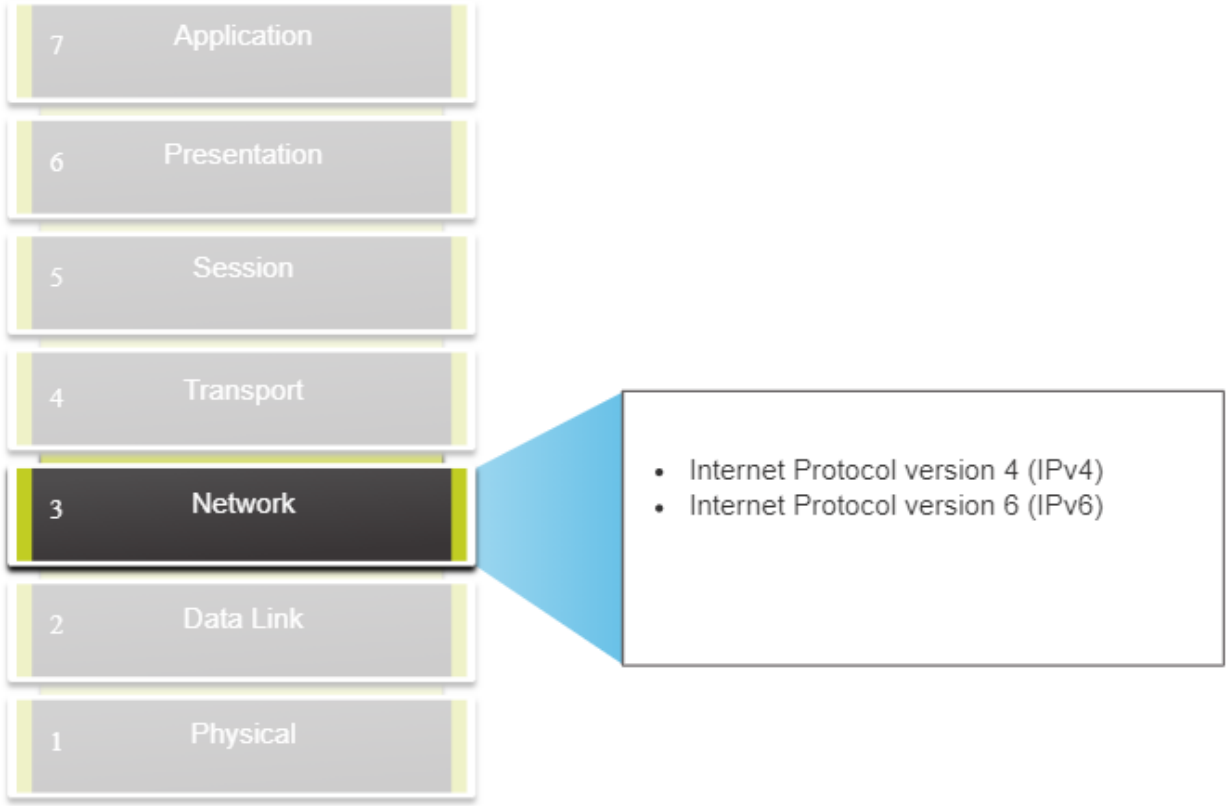


Different Representations of MAC Addresses

IPv4

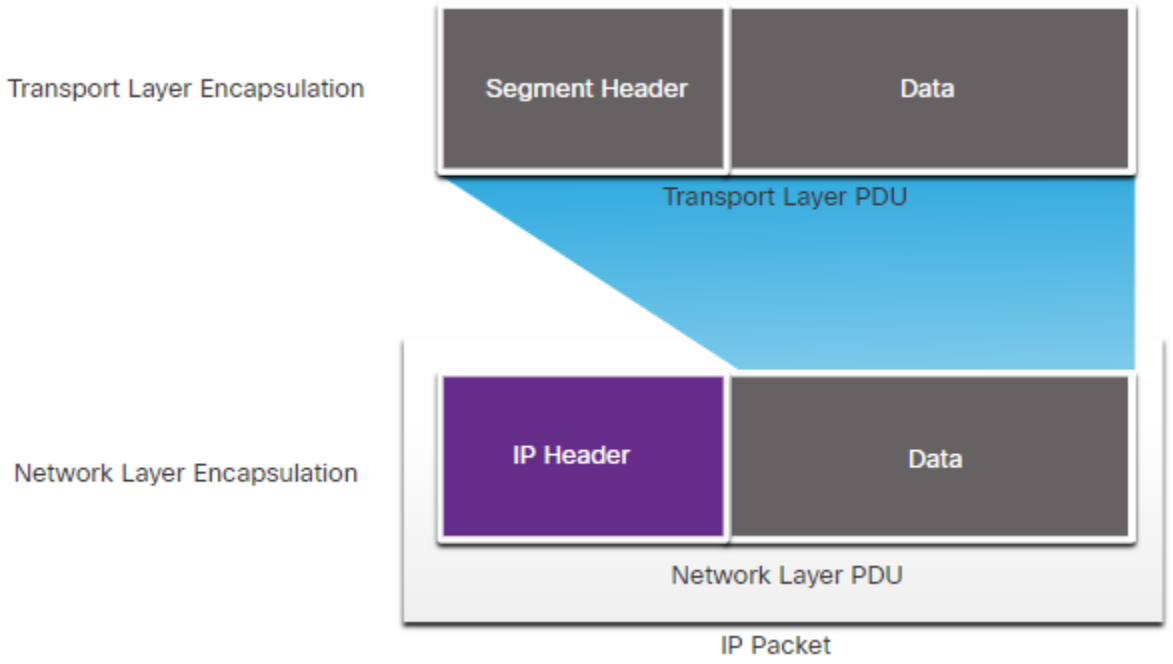
The Network Layer

- The network layer provides services to allow end devices to exchange data across networks.
- IPv4 and IPv6 are the principal network layer communication protocols.
- Basic operations of network layer protocol:
  - **Addressing end devices** - Configured with a unique IP address for identification
  - **Encapsulation** - Encapsulates the Protocol Data Unit (PDU) from the transport layer into a packet.
  - **Routing** - Select the best path and direct packets towards destination host.
  - **De-encapsulation** – Performed by the destination host.



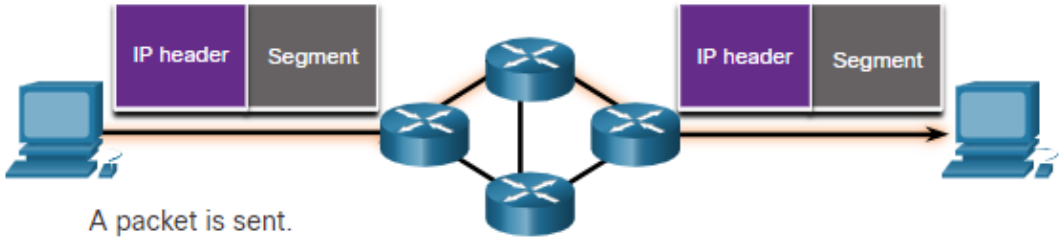
IP Encapsulation

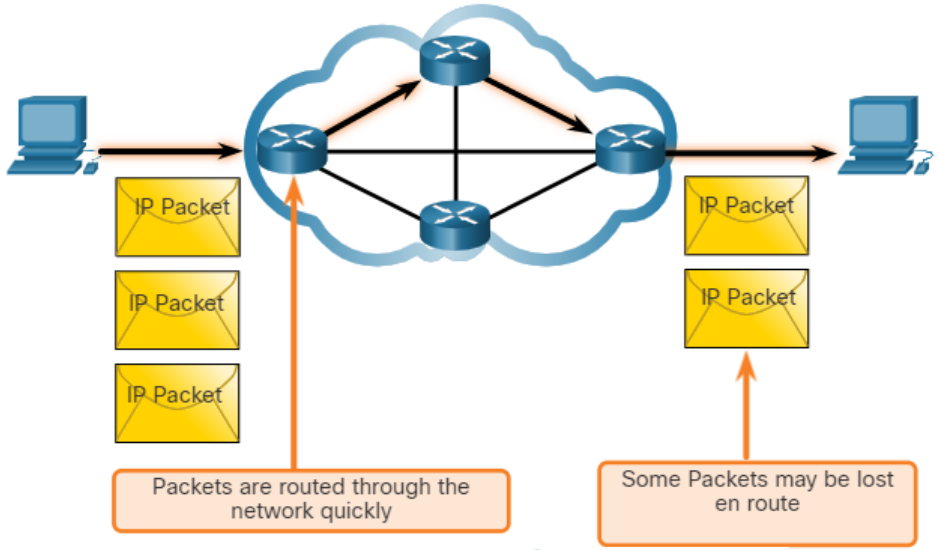
- IP encapsulates the transport layer segment or other data by adding an IP header. The IP header is used to deliver the packet to the destination host.
- IP addressing information remains the same from the time the packet leaves the source host until it arrives at the destination host, except when translated by the device performing Network Address Translation (NAT) for IPv4.
- The encapsulated transport layer PDU or other data, remains unchanged during the network layer processes.

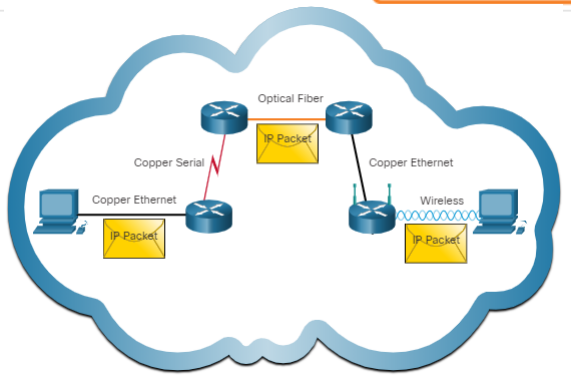


Characteristics of IP

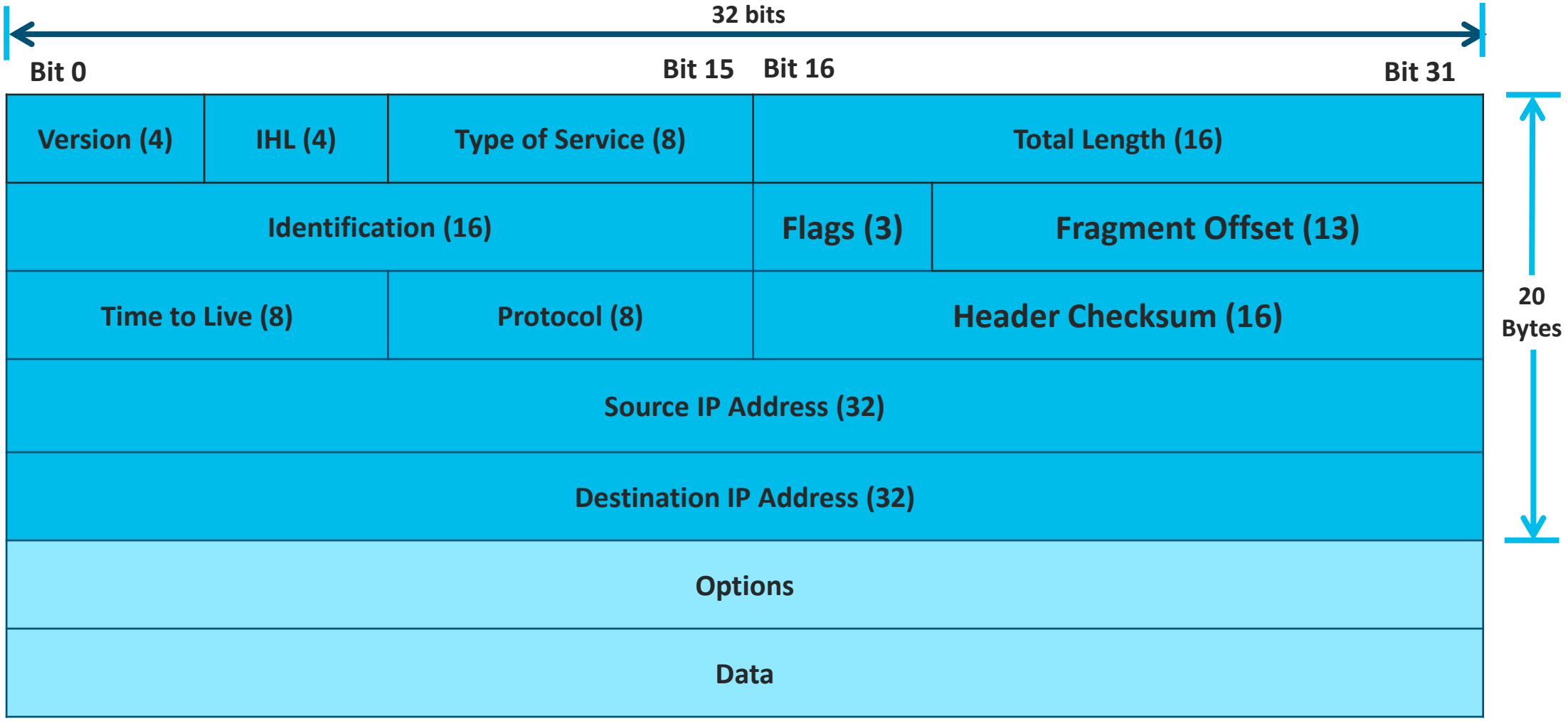
- IP was designed as a protocol with low overhead.
- IP provides the functions that are necessary to deliver a packet from a source to a destination over an interconnected system of networks.
- The basic characteristics of IP are as follows:
  - **Connectionless** - No dedicated end-to-end connection is created before data is sent.
  - **Best Effort** - IP protocol does not guarantee that all packets that are delivered are, in fact, received.
  - **Media Independent** - IP operates independently of the media (for example, copper, fiber-optic, or wireless) that carry the data at lower layers of the protocol stack.







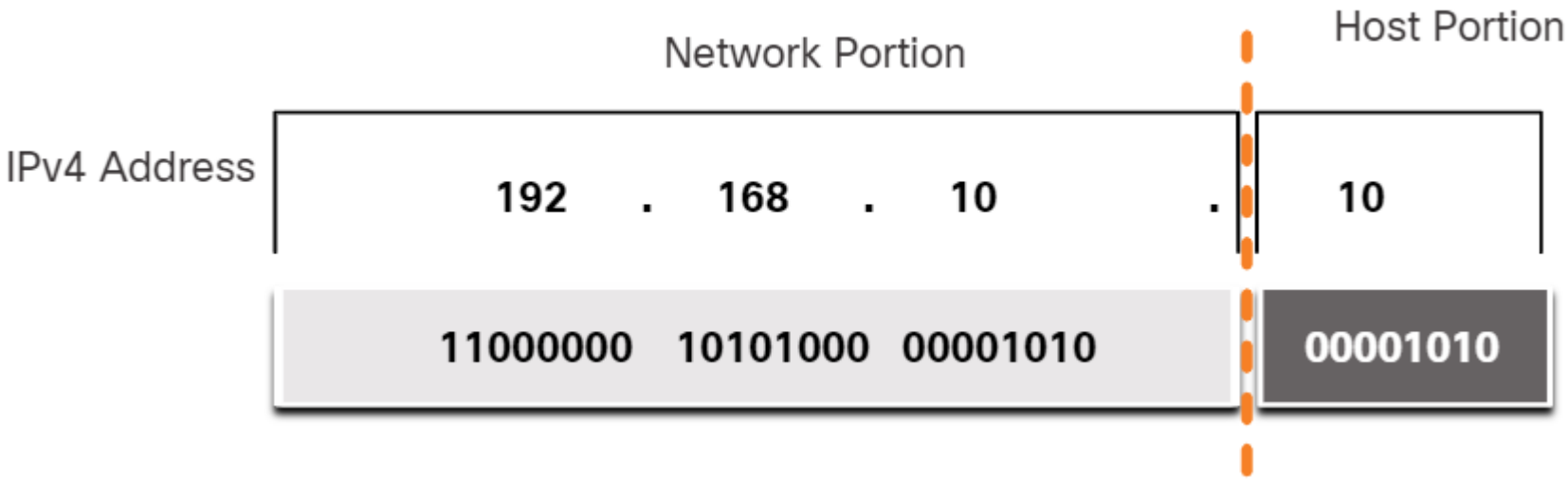
IPv4 Packet Header



The IPv4 Header

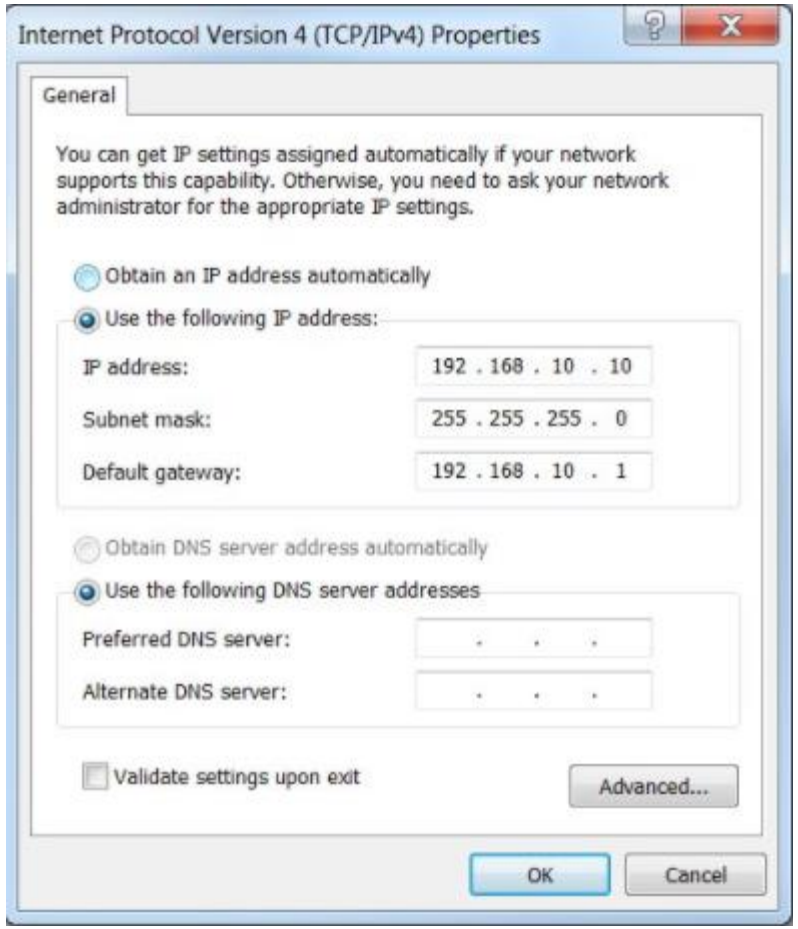
IPv4 Address Notation

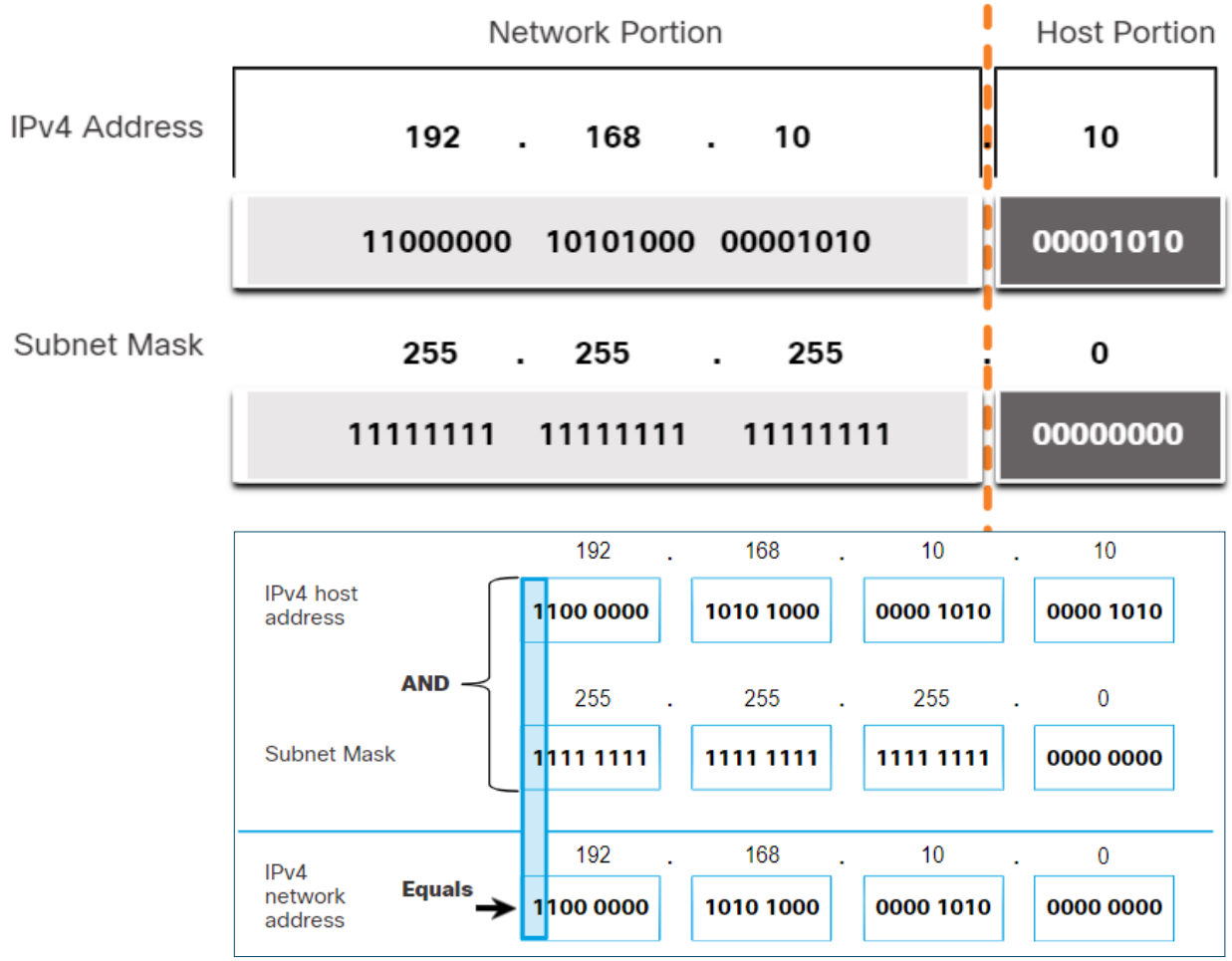
- An IPv4 address is a 32-bit hierarchical address expressed in dotted decimal format.
- An IPv4 address is made up of a network portion and a host portion.
- The bits within the network portion of the address must be identical for all devices that reside in the same network. The bits within the host portion of the address must be unique to identify a specific host within a network.
- But how do hosts know which portion of the 32-bits identifies the network and which identifies the host? That is the role of the subnet mask.



The Subnet Mask

- The subnet mask is used to identify the network portion in an IPv4 address.
- IP address is logically ANDed, bit by bit with subnet mask to determine the **network address** of the device.





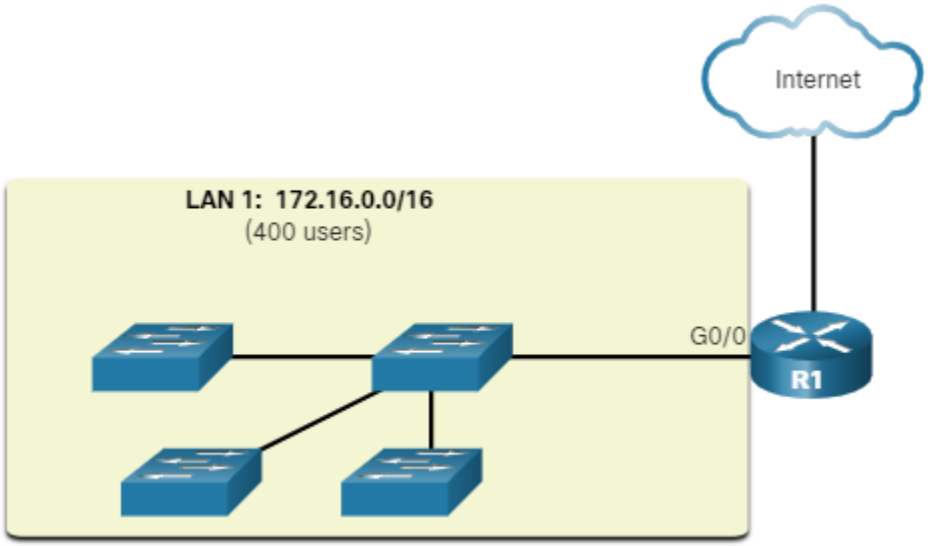
The Prefix Length

- The Prefix Length is an alternative method of identifying a subnet mask. The prefix length is the number of bits set to 1 in the subnet mask.
- It is written in “slash notation”, which is noted by a forward slash (/) followed by the number of bits set to 1. For example, 192.168.10.10 255.255.255.0 would be written as 192.168.10.10/24.

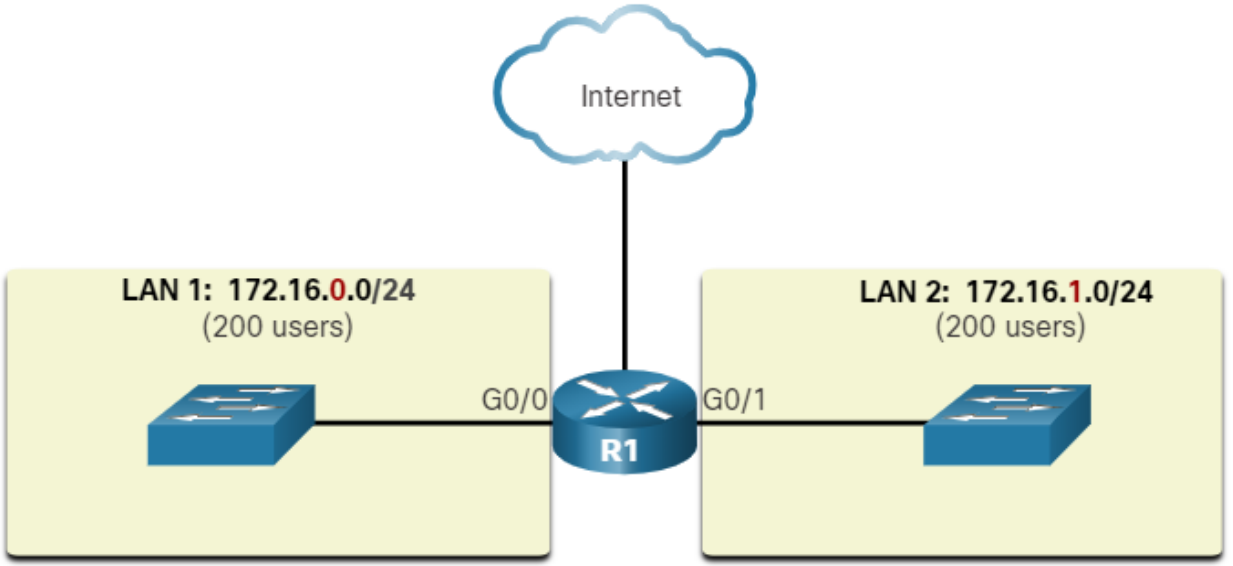
Subnet Mask	32-bit Address	Prefix Length
255.0.0.0	11111111.00000000.00000000.00000000	/8
255.255.0.0	11111111.11111111.00000000.00000000	/16
255.255.255.0	11111111.11111111.11111111.00000000	/24
255.255.255.128	11111111.11111111.11111111.10000000	/25
255.255.255.192	11111111.11111111.11111111.11000000	/26
255.255.255.224	11111111.11111111.11111111.11100000	/27
255.255.255.240	11111111.11111111.11111111.11110000	/28
255.255.255.248	11111111.11111111.11111111.11111000	/29
255.255.255.252	11111111.11111111.11111111.11111100	/30

Subnetting Broadcast Domains

- Subnetting takes a network space and divides it into smaller spaces called subnets.
- Subnetting creates smaller broadcast domains and reduces the overall network traffic to improves network performance.



A Large Broadcast Domain



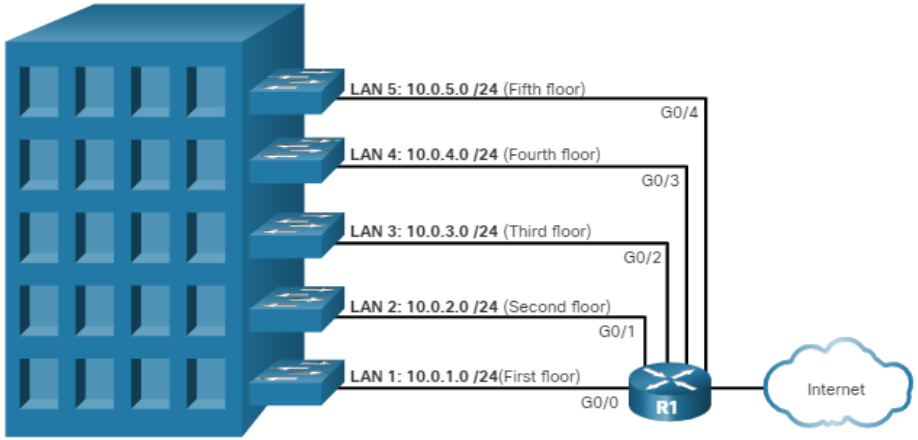
Smaller Broadcast Domains

- In the figure, for example, the 400 users in LAN 1 with network address 172.16.0.0 /16 have been divided into two subnets of 200 users each; 172.16.0.0 /24 and 172.16.1.0 /24. Broadcasts are only propagated within the smaller broadcast domains. Therefore, a broadcast in LAN 1 would not propagate to LAN 2.

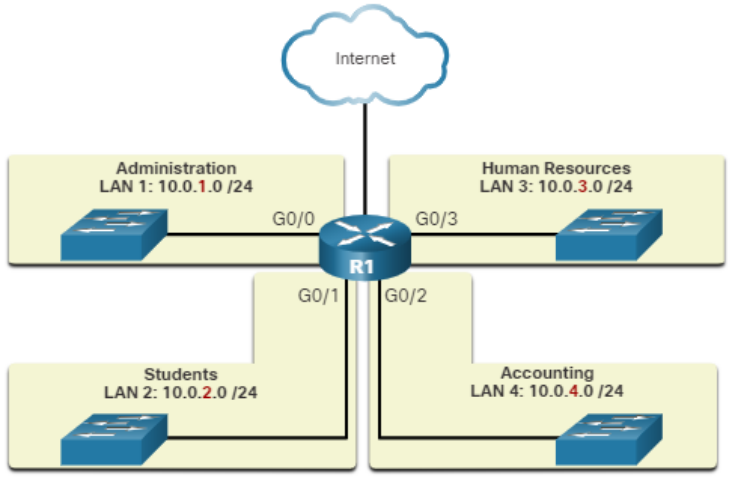
Subnetting the Network

- Network administrators can group devices and services into subnets that may be determined by a variety of factors.

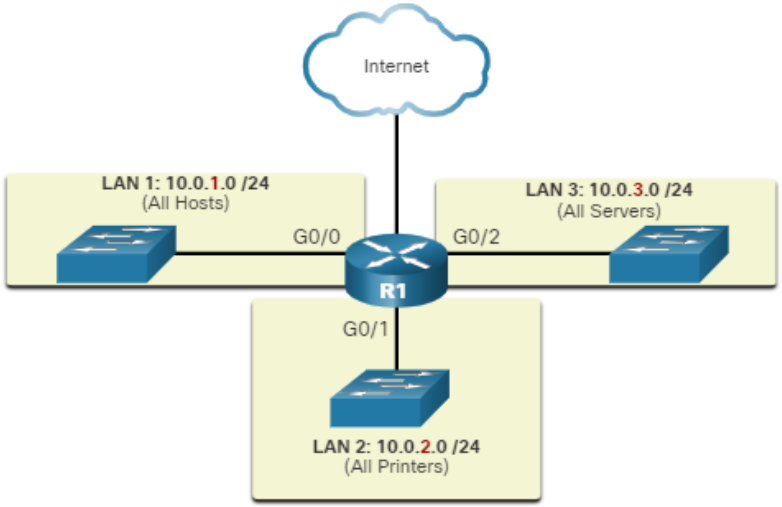
Location



By Department

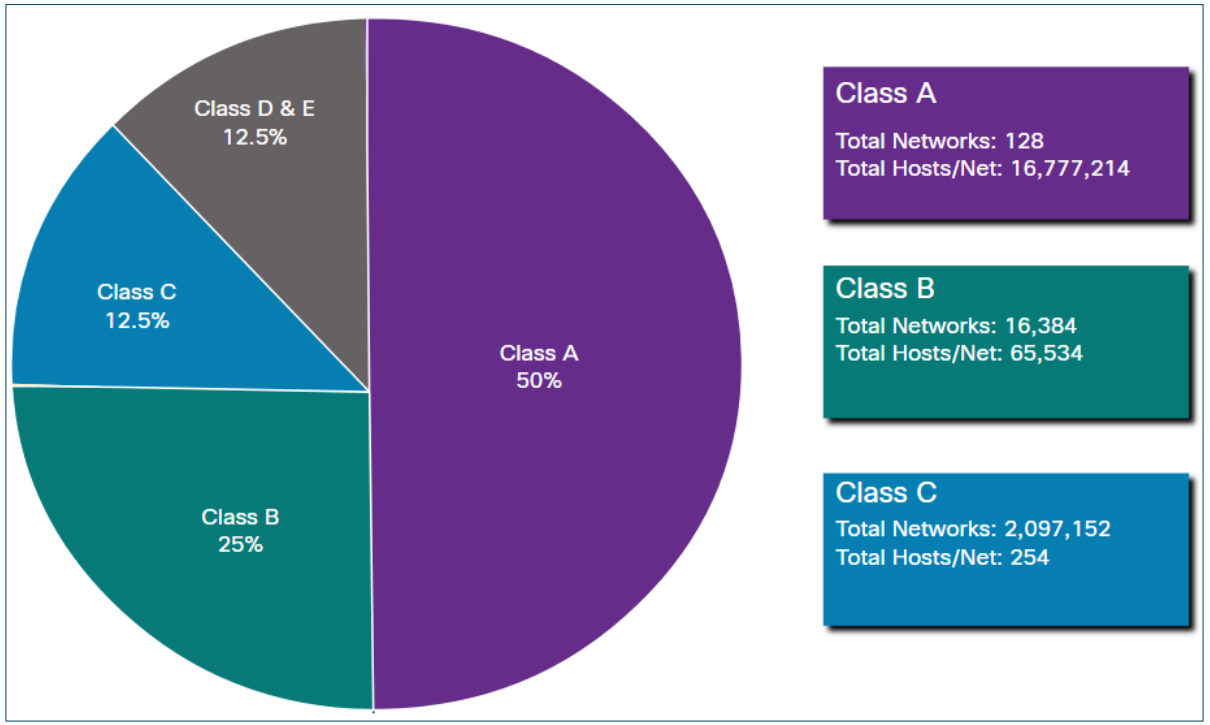


Device Type



IPv4 Address Classes and Default Subnet Mask

- The IPv4 addresses were based on the following classes:
  - **Class A** (0.0.0.0 – 127.255.255.255) Designed to support extremely large networks.
  - **Class B** (128.0.0.0 – 191.255.255.255) Designed to support moderate to large size network.
  - **Class C** (192.0.0.0 – 223.255.255.255) Designed to support small networks.
  - **Class D** (224.0.0.0 – 239.255.255.255) Multicast block.
  - **Class E** (240.0.0.0 – 255.255.255.255) Experimental address block.

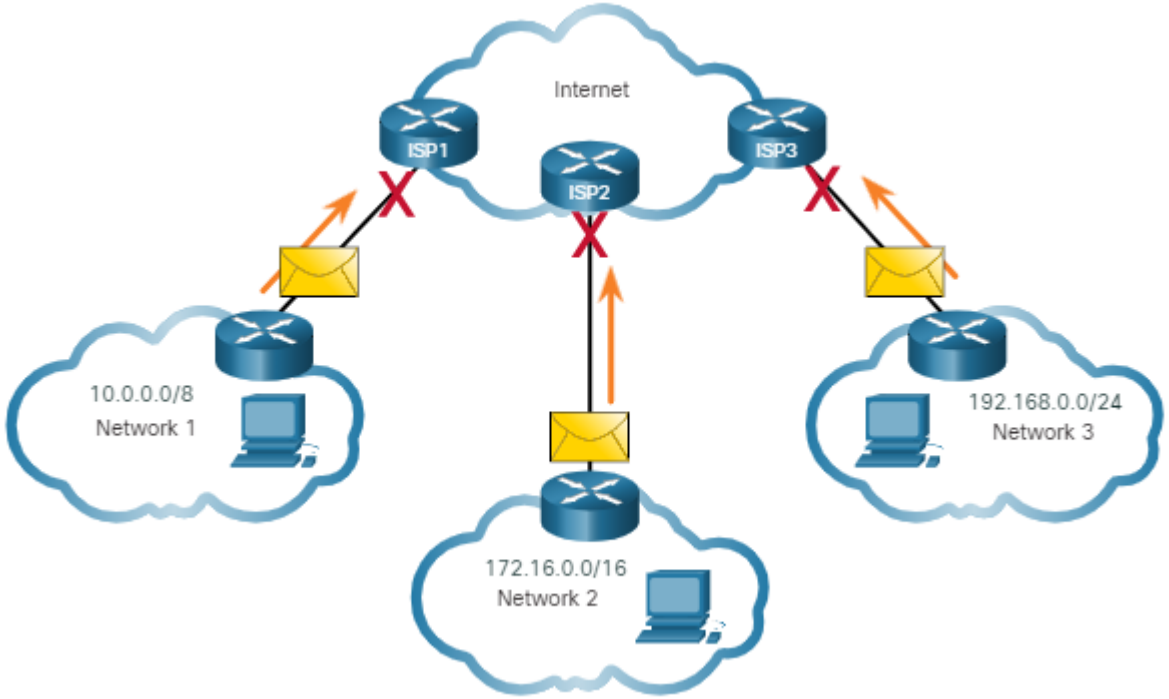


Class	Default Subnet Mask	Prefix Length
A	255.0.0.0	/8
B	255.255.0.0	/16
C	255.255.255.0	/24

Reserved Private Addresses

- In the mid-1990s, private IPv4 addresses were introduced because of the depletion of IPv4 address space.
- Private addresses are used by most organizations to assign IPv4 addresses to internal hosts and are not unique globally.
- Private addresses are not allowed on Internet and are filtered by internet routers.
- Network Address Translation (NAT) is used to translate between private IPv4 and public IPv4 addresses.

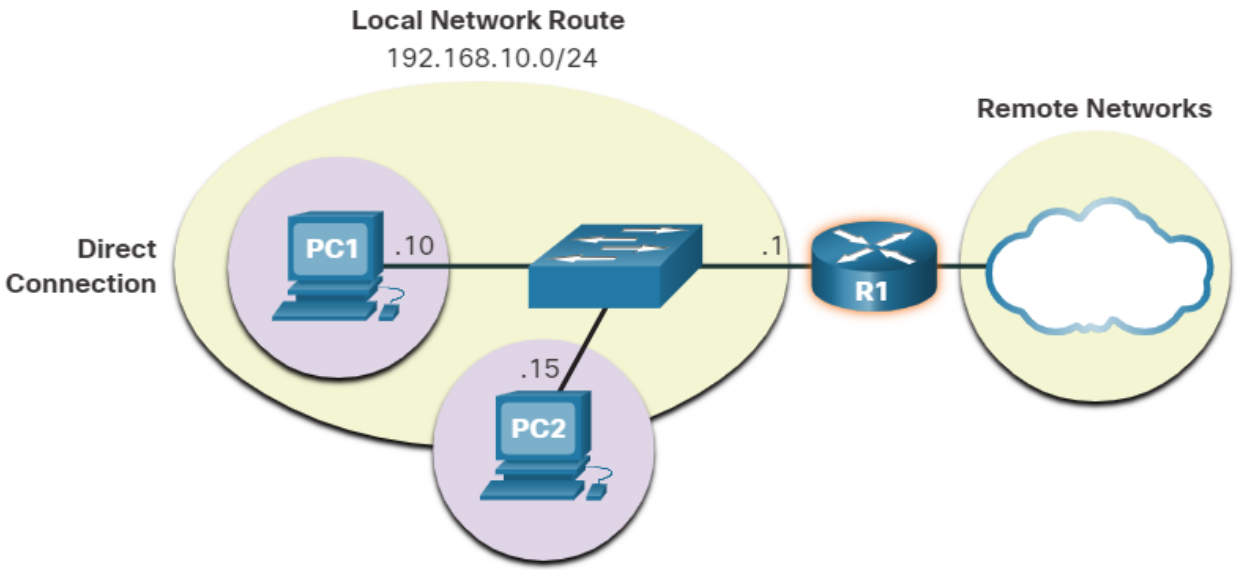
Class	Private Address Block	Private Address Range
A	10.0.0.0/8	10.0.0.0 – 10.255.255.255
B	172.16.0.0/12	172.16.0.0 – 172.31.255.255
C	192.168.0.0/16	192.168.0.0 – 192.168.255.255



Private Addresses cannot be Routed over the Internet

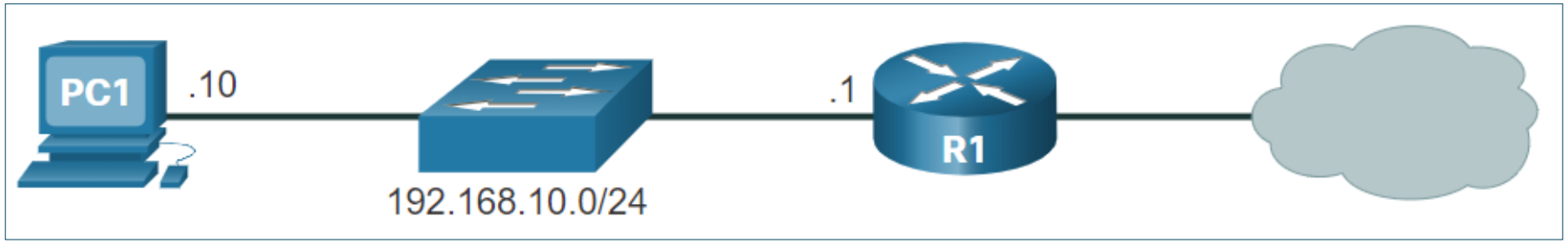
The Default Gateway

- A host can send a packet to: **Itself**, **Local host**, and **Remote host**.
- A default gateway, usually a router, is required to send traffic outside the local network.
- In IPv4, the host receives the IPv4 address of the default gateway either dynamically from DHCP server or configured manually.
- In IPv6, the router advertises the default gateway address, or the host can be configured manually.
- Having a default gateway configured creates a default route in the routing table of the PC.



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.

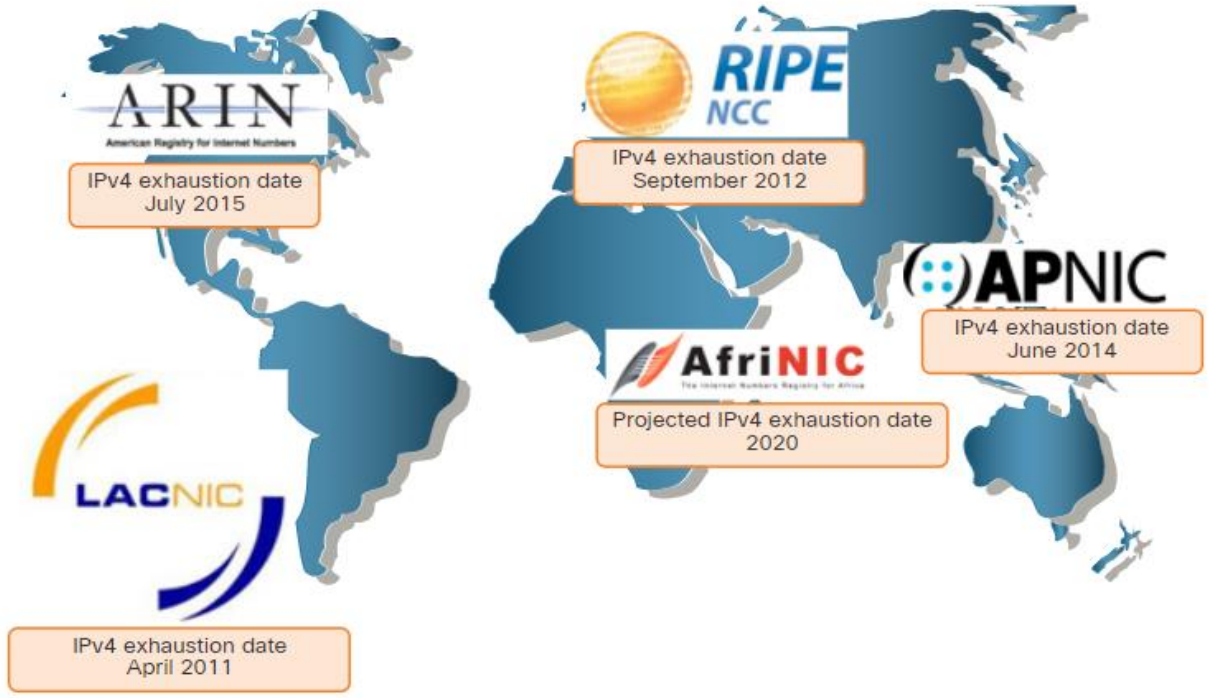



```
C:\Users\PC1> netstat -r
(output omitted)
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.10.1    192.168.10.10      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)
```

IPv6

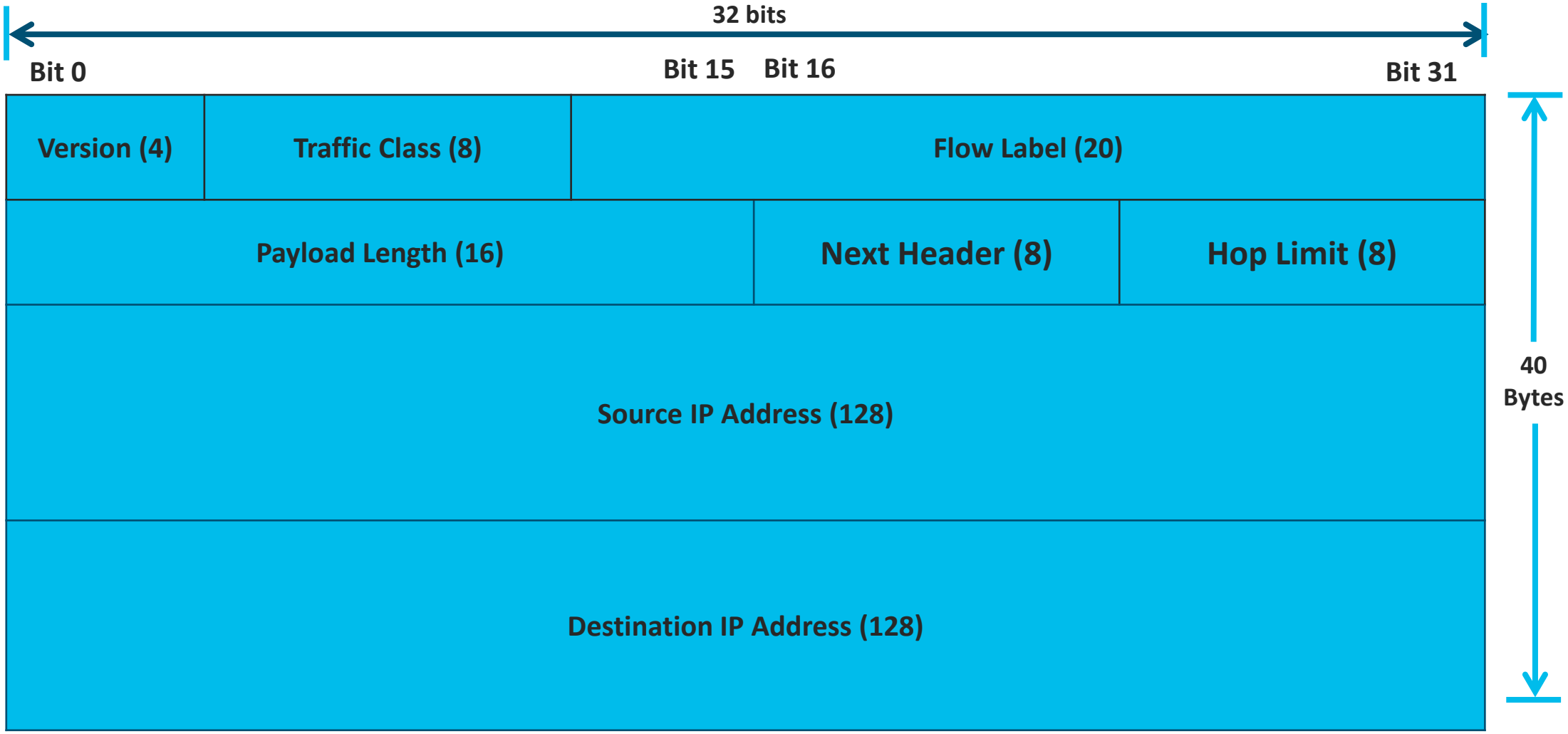
Need for IPv6

- IPv6 is designed to be the successor to IPv4.
- IPv6 has a larger 128-bit address space, providing 340 undecillion possible addresses.
- Mobile providers have been leading the way with the transition to IPv6.
- Most top ISPs and content providers such as YouTube, Facebook, and Netflix, have also made the transition.
- Many companies like Microsoft, Facebook, and LinkedIn are transitioning to IPv6-only internally.
- The depletion of IPv4 address space has been the motivating factor for moving to IPv6.
- Internet of Things (IoT) revolution is another key factor to transition to IPv6.



RIR IPv4 Exhaustion Dates

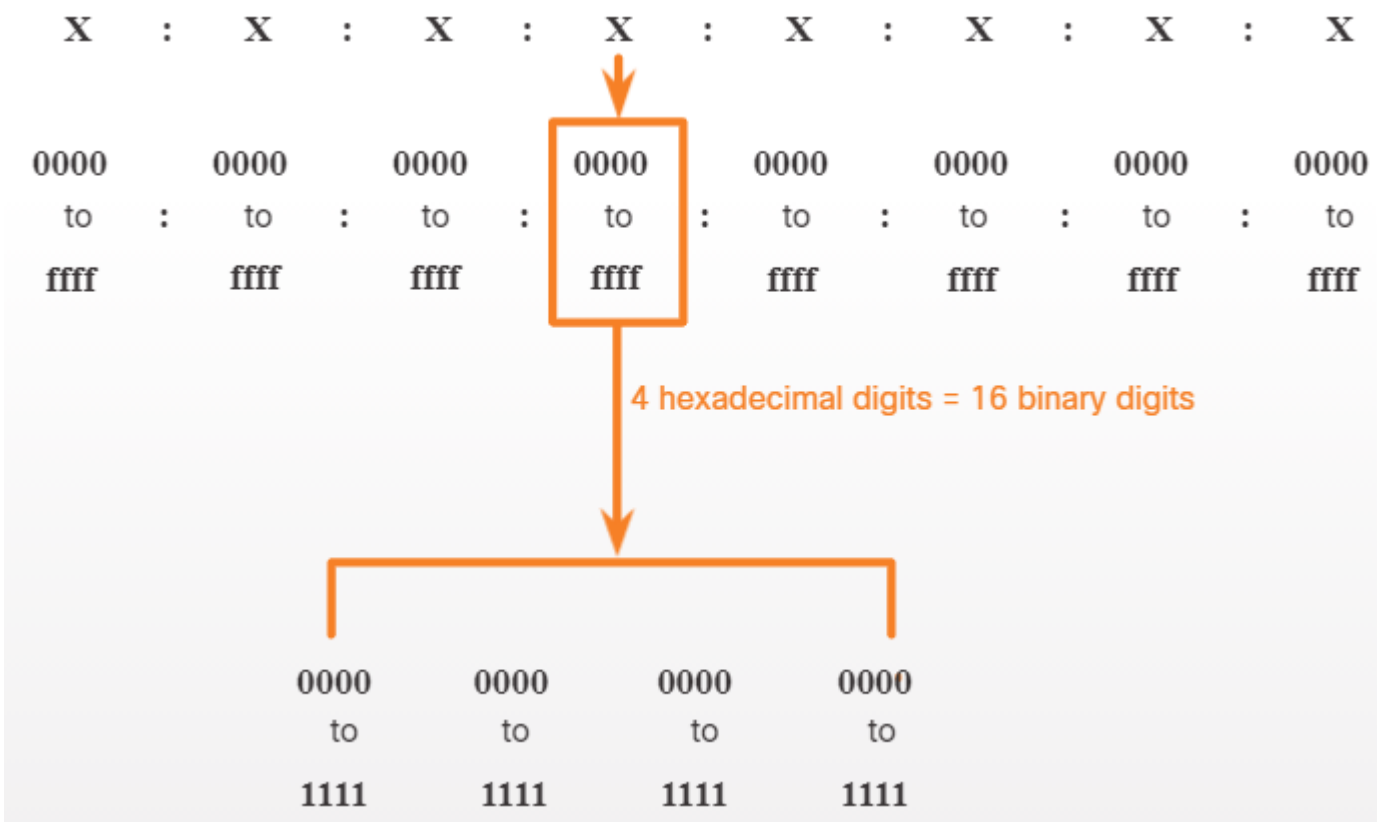
IPv6 Packet Header



The IPv6 Fixed Header

IPv6 Addressing Formats

- IPv6 addresses are **128 bits** in length and written as a string of **hexadecimal** values. For example: 2001:0DB8:0001:5270:0127:00AB:CAFE:0E1F /64
- In IPv6, a **Hextet** is the unofficial term used to refer to a segment of 16 bits, or four hexadecimal values.



Leading Zeroes and Double Colons

- Leading 0s (zeroes) in any Hextet can be omitted.

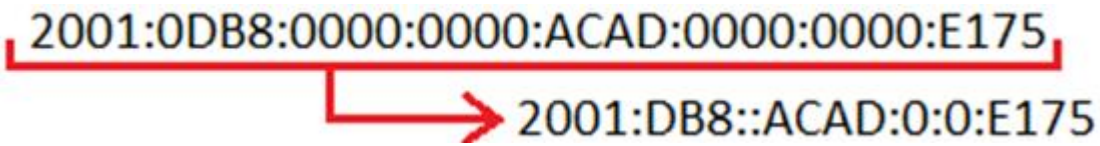
  Address **before** omission:

  2001:0DB8:0001:5270:0127:00AB:CAFE:0E1F /64

  Address **after** omission:

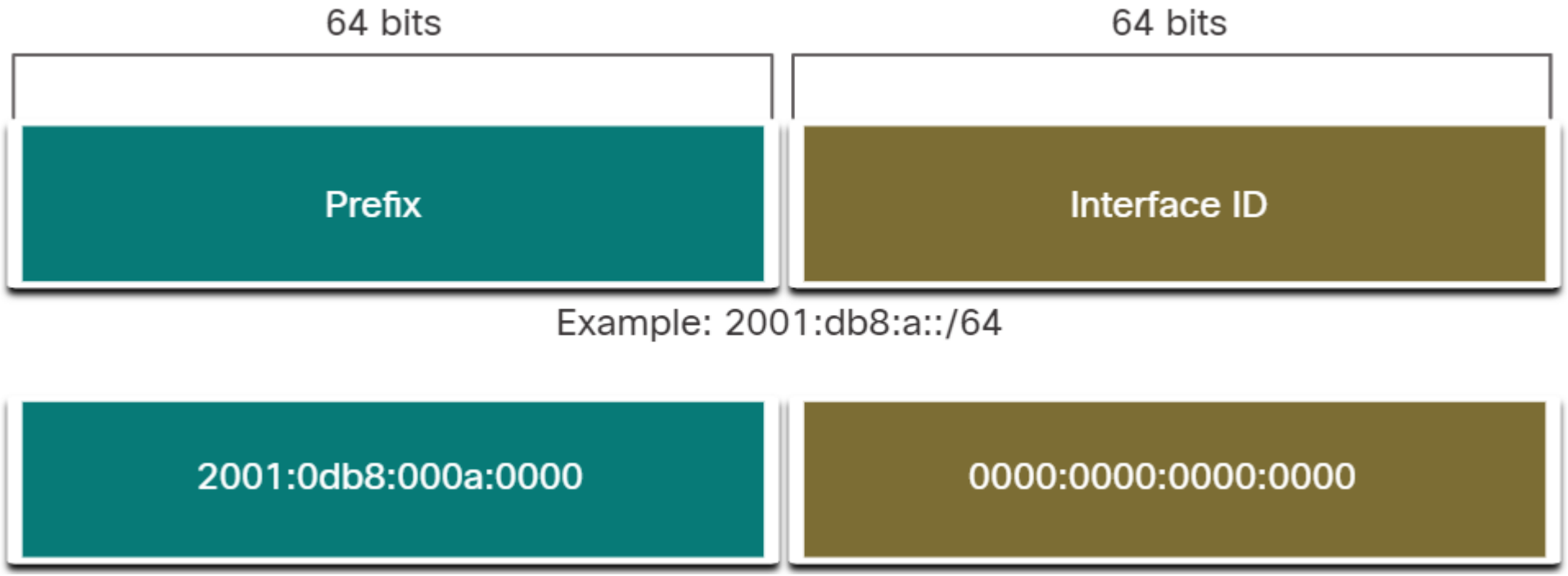
  2001:DB8:1:5270:127:AB:CAFE:E1F /64

- Contiguous Hextet of zeroes can be written as :: (Double Colon). Double Colon can only be used once in an IPv6 address. if it's used more than once the address could be ambiguous.



IPv6 Prefix Length

- In IPv6, the Prefix Length, represented in slash notation, is used to indicate the network portion of an IPv6 address.
- The prefix length can range from 0 to 128. The recommended IPv6 prefix length for LANs and most other types of networks is /64.



IPv6 Addressing Structure

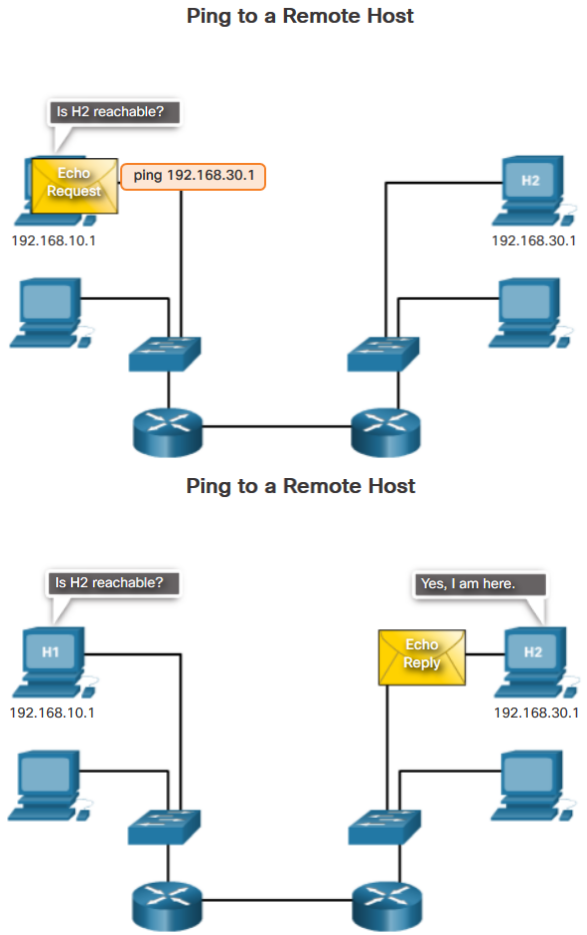
- The **Site Prefix or Global Routing Prefix** is the first 3 hextets or 48-bits of the address. It is assigned by the service provider.
- The **Subnet ID** Is the 4th hextet of the address.
- The **Interface ID** is the last 4 hextets or 64-bits of the address. It can be manually or dynamically assigned using the EUI-64 command (Extended Unique Identifier).
- The first (network) and last (broadcast) address may be assigned to an interface. An interface may contain more than one IPv6 address.
- There are no broadcast addresses, multicast is used instead.

Connectivity Verification

ICMP

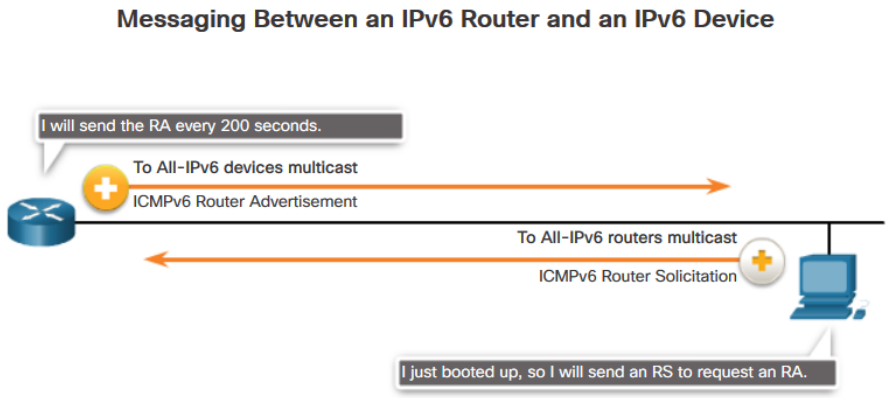
ICMPv4 Messages

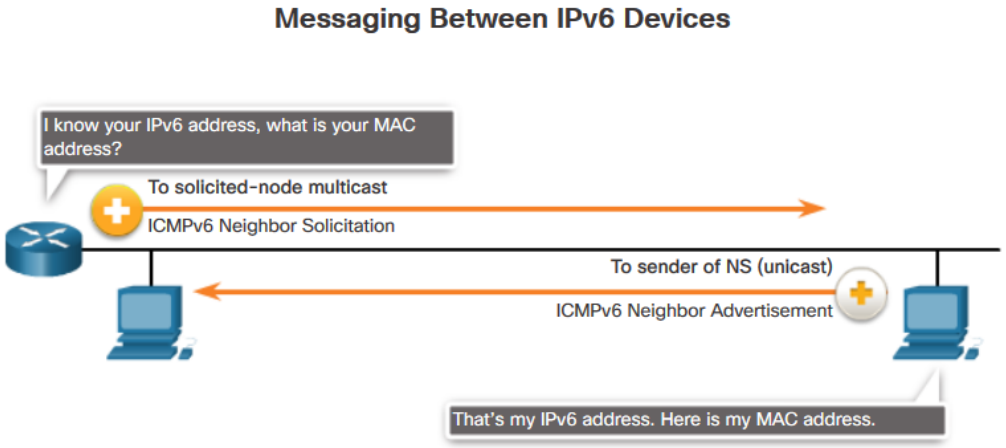
- Used to provide feedback and troubleshoot network problems.
- **Message types:**
  - **Host confirmation** – *echo request* and *echo reply* with the ping utility.
  - **Destination or service unreachable codes:**
    - **0** – net unreachable
    - **1** – host unreachable
    - **2** – protocol unreachable
    - **3** – port unreachable
  - **Time exceeded** – used by a router to indicate that a packet cannot be sent onward:
    - IPv4 is due to the time to live (TTL) field having a value of 0.
    - IPv6 does not have a TTL field but has a hop limit field instead.



ICMPv6 RS and RA Messages

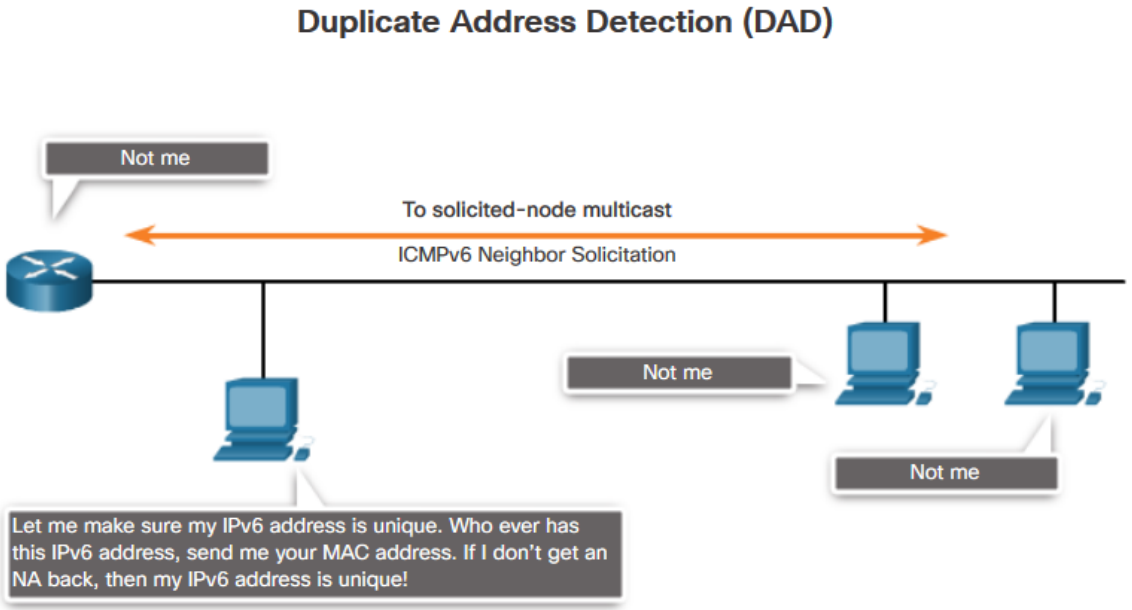
- ICMPv6 has new features and improved functionality not found in ICMPv4. ICMPv6 messages are encapsulated in IPv6.
- 4 new protocols as part of the Neighbor Discovery Protocol (ND or NDP):
- Messaging between IPv6 router and IPv6 device:
  - **Router Solicitation (RS)** – used between an IPv6 device and a router.
  - **Router Advertisement (RA)** – used between an IPv6 router and a device to provide addressing info using Stateless Address Autoconfiguration (SLAAC).
- Messaging between IPv6 devices:
  - **Neighbor Solicitation (NS) message**
  - **Neighbor Advertisement (NA) message**





IPv6 Duplicate Address Detection

- When a device is assigned a global unicast or link-local unicast address, the DAD is performed on the address to ensure that it is unique.
- To check the uniqueness of an address, the device will send an NS message with its own IPv6 address.
- If another device on the network has this address, it will respond with an NA message which will notify the sending device that the address is in use. If a corresponding NA message is not returned within a certain period of time, the unicast address is unique and acceptable for use.



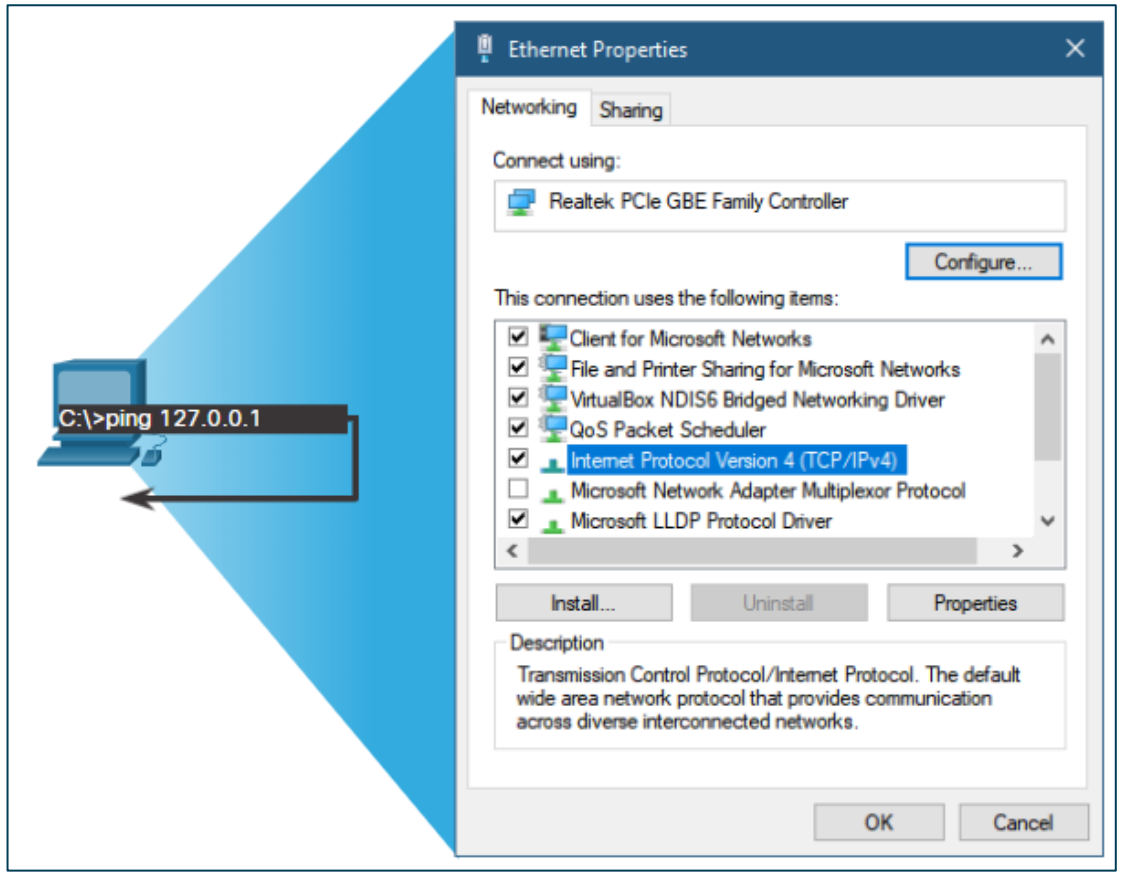
Ping and Traceroute Utility

Ping – Test Connectivity

- Ping is an IPv4 and IPv6 testing utility that uses ICMP echo request and echo reply messages to test connectivity between hosts.
- Type of connectivity tests performed with **ping** include the following:
  - Pinging the local loopback
  - Pinging the default gateway
  - Pinging the remote host

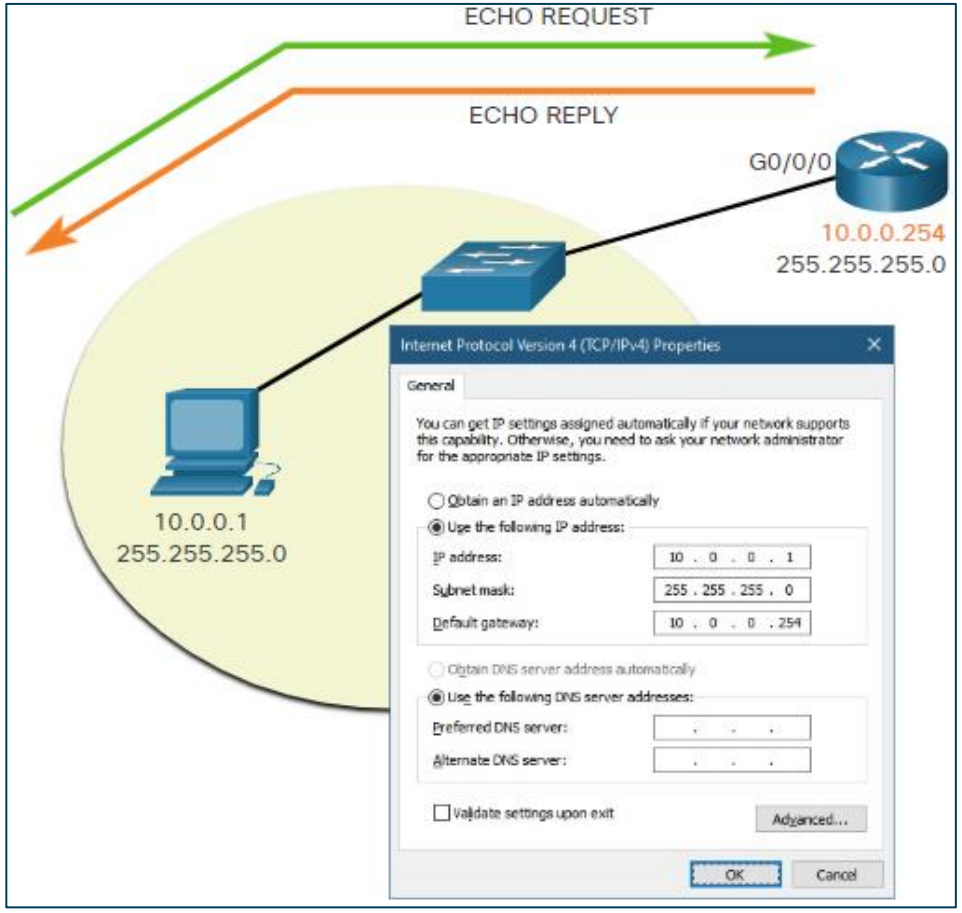
Ping the Loopback

- Ping can be used to test the internal configuration of IPv4 or IPv6 on the local host.
- To perform this test, **ping** the local loopback address of 127.0.0.1 for IPv4 (::1 for IPv6).
- Pinging the local host confirms that TCP/IP is installed and working on the local host.
- Pinging 127.0.0.1 causes a device to ping itself.



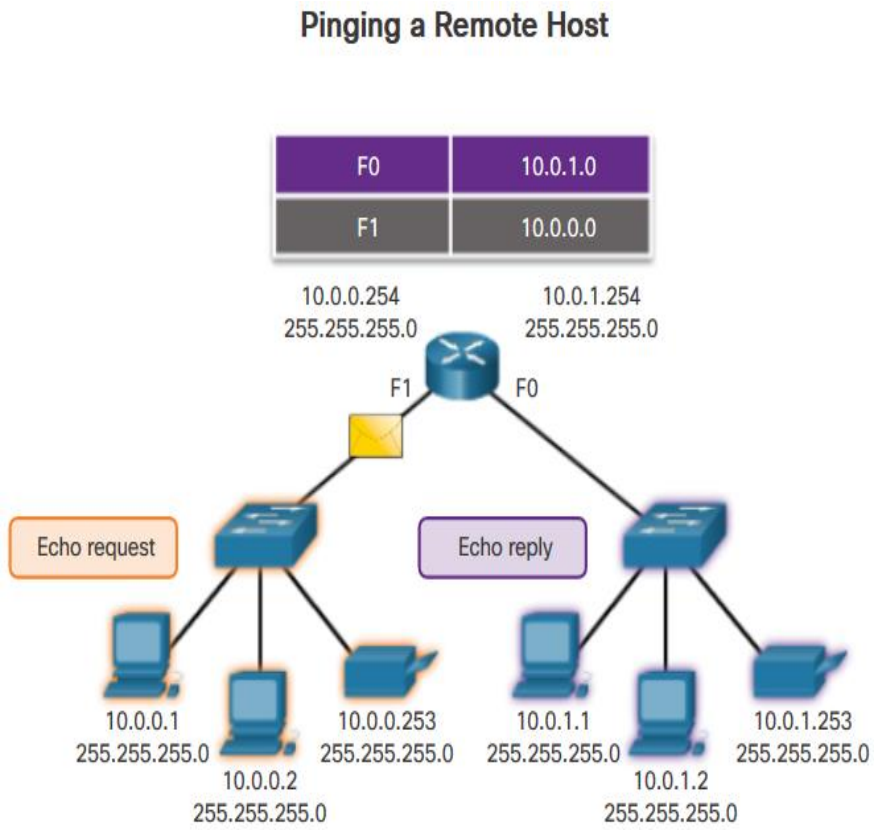
Ping the Default Gateway

- The **ping** can be used to test the ability of a host to communicate on the local network. This is done by pinging the IP address of the default gateway of the host.
- A successful **ping** to the default gateway indicates that the host and the router interface serving as the default gateway are both operational on the local network.
- The host pings its default gateway, sending an ICMP echo request. The default gateway sends an echo reply confirming connectivity.



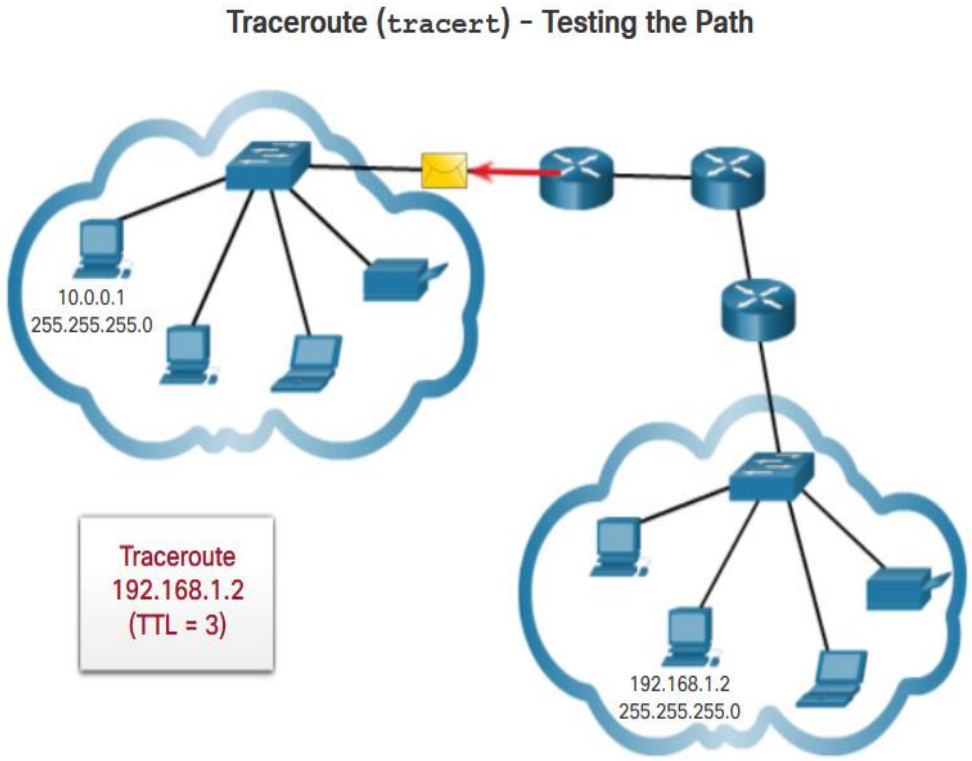
Ping a Remote Host

- Ping can also be used to test the ability of a local host to communicate across an internetwork.
- Successful ping across the internetwork confirms communication on the local network.
- It also confirms the operation of the router serving as the gateway, and the operation of all other routers that might be in the path between the local network and the network of the remote host.



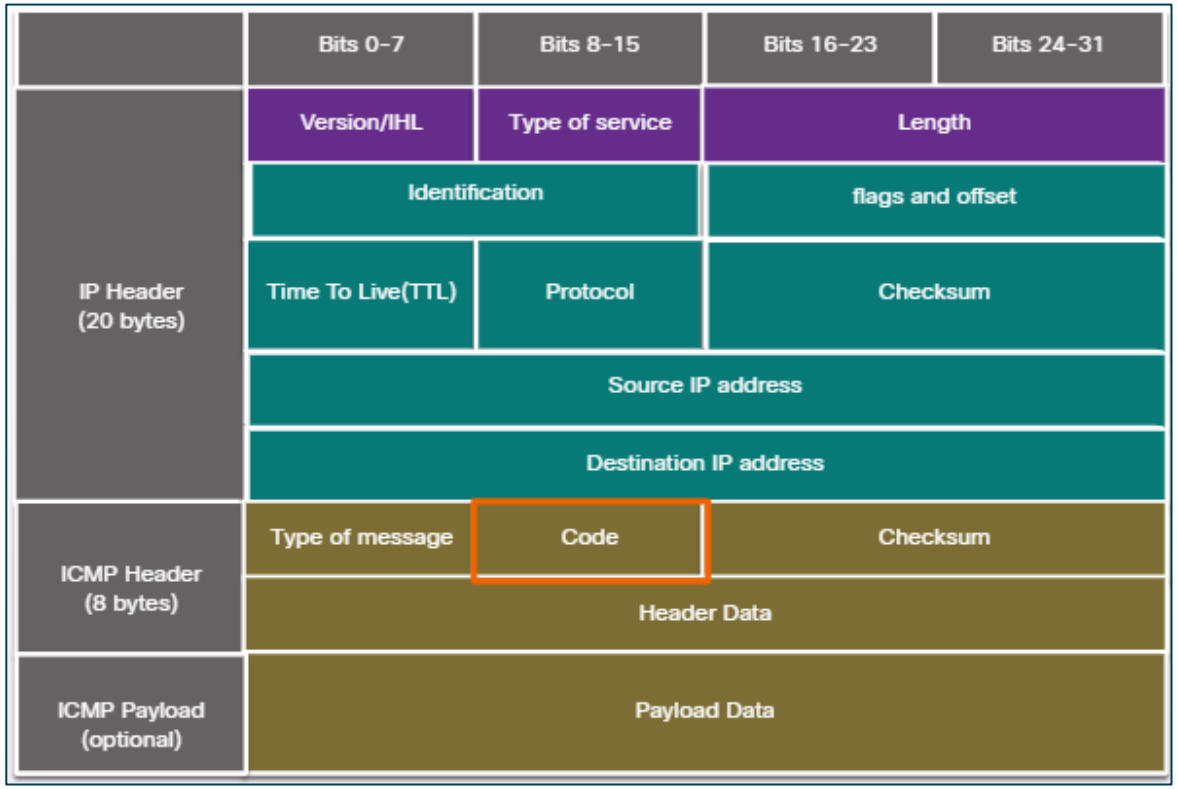
Traceroute – Testing the Path

- Traceroute provides information about the details of devices between the hosts.
- Generates a list of hops that were successfully reached along the path:
  - **Round trip Time (RTT)** – time for each hop along path.
  - **IPv4 TTL and IPv6 Hop Limit** - Traceroute makes use of a function of the TTL field in IPv4 and the Hop Limit field in IPv6 in the Layer 3 headers, along with the ICMP time exceeded message.
- After the final destination is reached, the host responds with either an ICMP port unreachable message or an ICMP echo reply message instead of the ICMP time exceeded message.



ICMP Packet Format

- ICMP is encapsulated directly into IP packets.
- ICMP acts as a data payload within the IP packet. It has a special header data field.
- It uses message codes to differentiate between different types of ICMP messages. These are some common message codes:
  - **0 –** Echo reply (response to a ping)
  - **3 –** Destination Unreachable
  - **5 –** Redirect (use another route to the destination)
  - **8 –** Echo request (for ping)
  - **11 –** Time Exceeded (TTL became 0)



Address Resolution Protocol

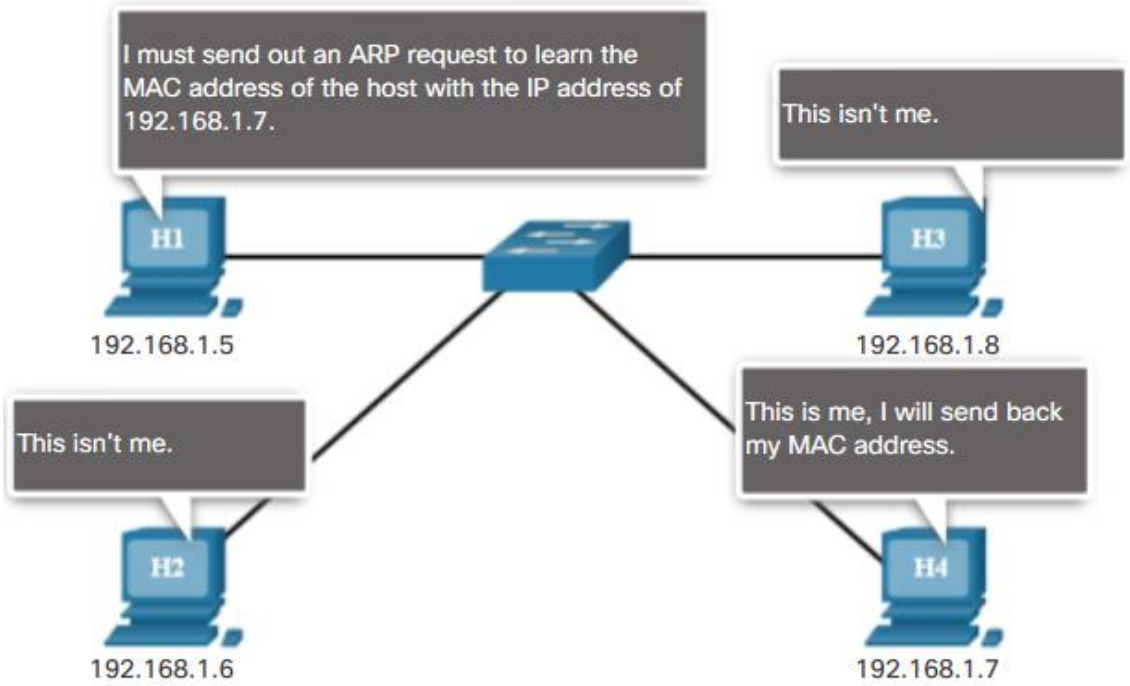
ARP Functions

ARP Functions

- When a packet is sent to the data link layer to be encapsulated into an Ethernet frame, the device refers to a table called **ARP table** or ARP cache in its RAM memory to find the MAC address that is mapped to the IPv4 address.
- The sending device will search its ARP table for a destination IPv4 address and a corresponding MAC address.
  - If the packet's destination IPv4 address is on the same network as the source IPv4 address, the device will search the ARP table for the destination IPv4 address.
  - If the destination IPv4 address is on a different network than the source IPv4 address, the device will search the ARP table for the IPv4 address of the default gateway.
- If the device locates the IPv4 address, its corresponding MAC address is used as the destination MAC address in the frame. If there is no entry is found, then the device sends an ARP request.

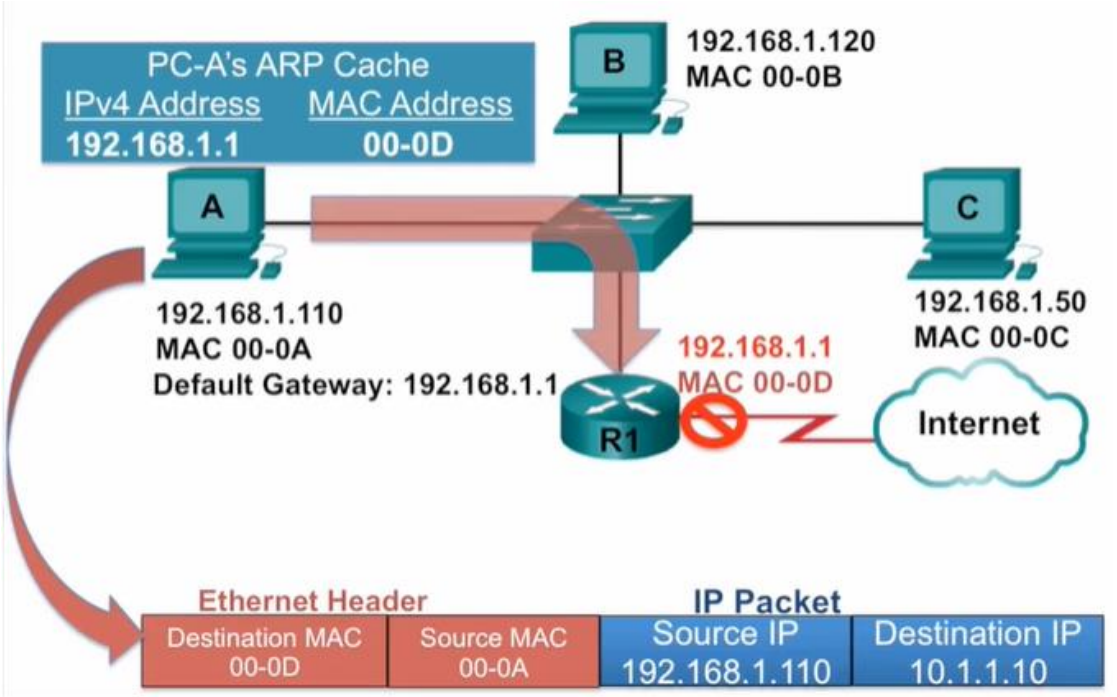
ARP Operation

- **ARP Request** - When a device needs to determine the MAC address mapped to the IPv4 address and no entry is found for the IPv4 address in its ARP table, then an ARP request is sent.
- **ARP Reply -** Only the device with the target IPv4 address associated with the ARP request will respond with an ARP reply.
- *IPv6 uses a similar process to ARP for IPv4, known as ICMPv6 Neighbor Discovery (ND). IPv6 uses neighbor solicitation and neighbor advertisement messages, similar to IPv4 ARP requests and ARP replies.*



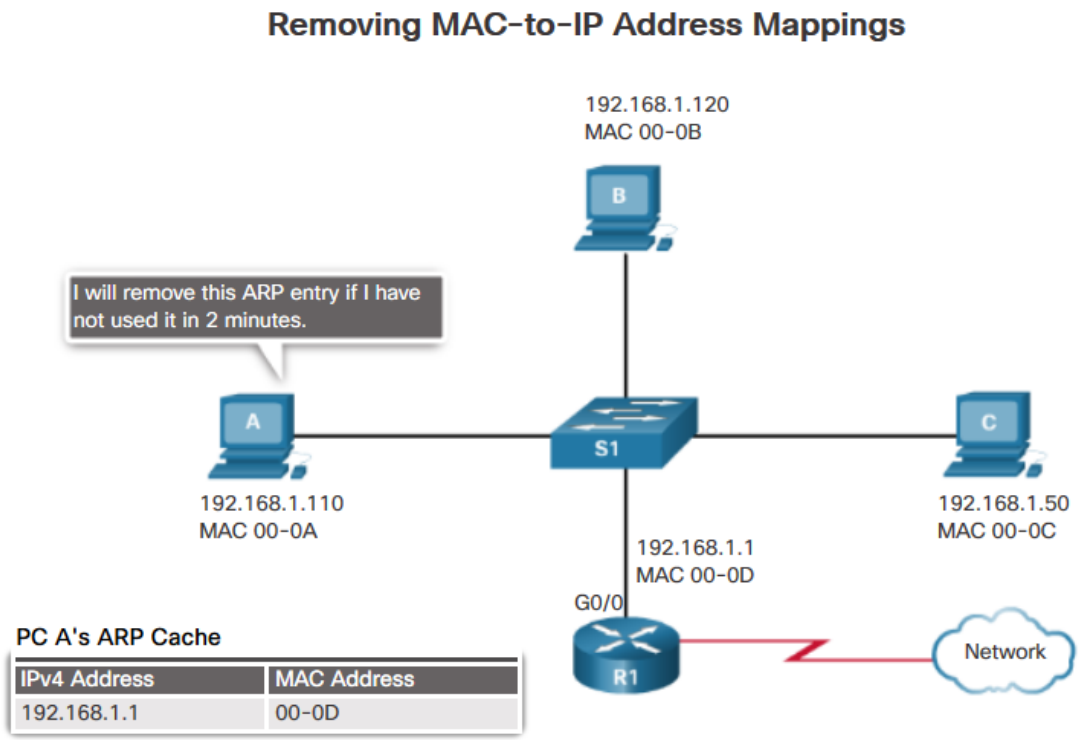
ARP Role in Remote Communication

- When the destination IPv4 address is not on the same network as the source IPv4 address, the source device needs to send the frame to its default gateway.
- Whenever a source device has a packet with an IPv4 address on another network, it will encapsulate that packet in a frame using the destination MAC address of the router.



Removing Entries from an ARP Table

- For each device, an ARP cache timer removes ARP entries that have not been used for a specified period of time.
- Commands may also be used to manually remove all or some of the entries in the ARP table.
- Network hosts and routers keep ARP Table
- After an entry has been removed, the process for sending an ARP request and receiving an ARP reply must occur again to enter the map in the ARP table.



ARP Tables on Networking Devices

On a Cisco router, the **show ip arp** command is used to display the ARP table.

```
R1# show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.10.1            -   a0e0.af0d.e140  ARPA   GigabitEthernet0/0/0
Internet  209.165.200.225          -   a0e0.af0d.e141  ARPA   GigabitEthernet0/0/1
Internet  209.165.200.226          1   a03d.6fe1.9d91  ARPA   GigabitEthernet0/0/1
R1#
```

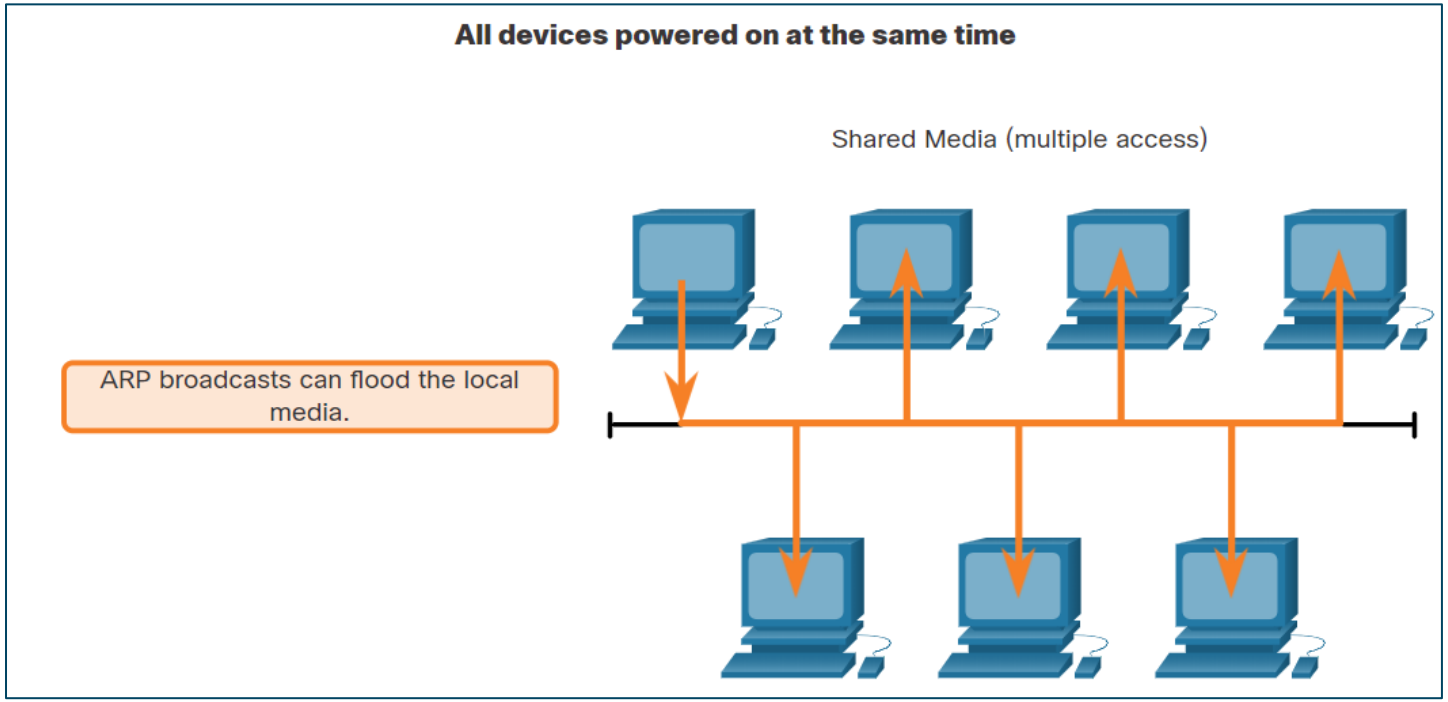
On a Windows 10 PC, the **arp –a** command is used to display the ARP table.

```
C:\Users\PC> arp -a
Interface: 192.168.1.124 --- 0x10
  Internet Address      Physical Address      Type
  192.168.1.1           c8-d7-19-cc-a0-86     dynamic
  192.168.1.101         08-3e-0c-f5-f7-77     dynamic
  192.168.1.110         08-3e-0c-f5-f7-56     dynamic
  192.168.1.112         ac-b3-13-4a-bd-d0     dynamic
  192.168.1.117         08-3e-0c-f5-f7-5c     dynamic
  192.168.1.126         24-77-03-45-5d-c4     dynamic
  192.168.1.146         94-57-a5-0c-5b-02     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
C:\Users\PC>
```

ARP Issues

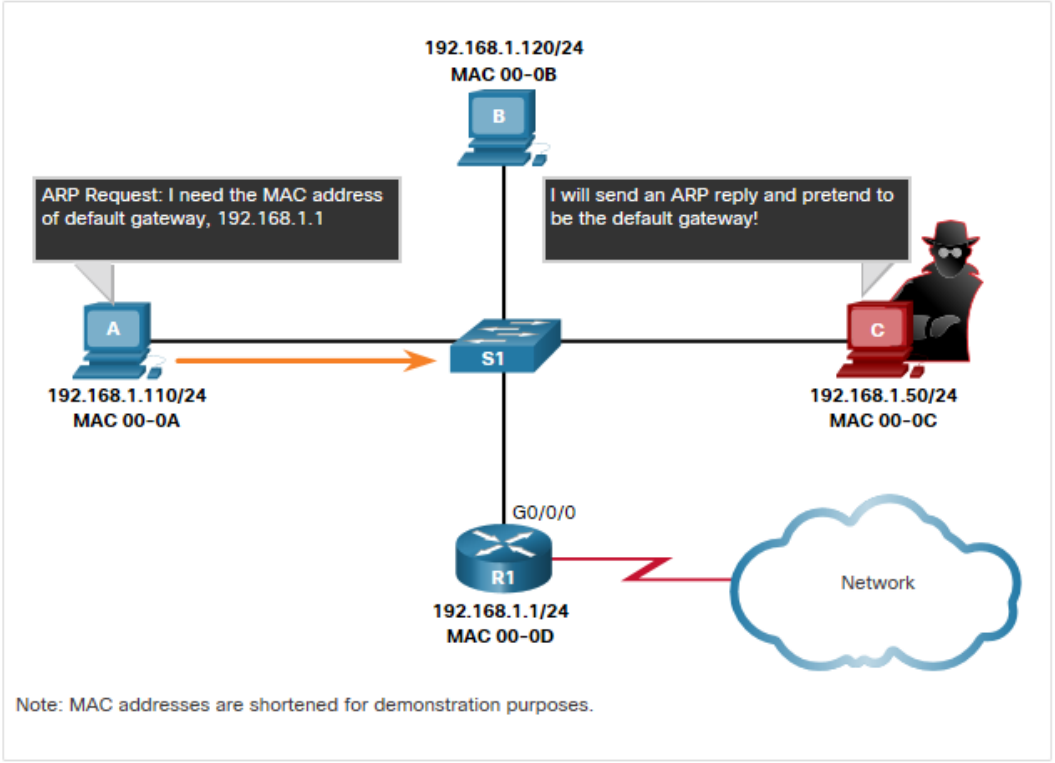
ARP Broadcasts

- As a broadcast frame, an ARP request is received and processed by every device on the local network.
- ARP Broadcasts could impact large networks.



ARP Spoofing

- The use of ARP can lead to a potential security risk in some cases.
- A threat actor uses ARP spoofing to perform an ARP poisoning attack.
  - It is a technique used by a threat actor to reply to an ARP request for an IPv4 address belonging to another device, such as the default gateway.
  - The threat actor sends an ARP reply with its own MAC address.The receiver of the ARP reply will add the wrong MAC address to its ARP table and send these packets to the threat actor.

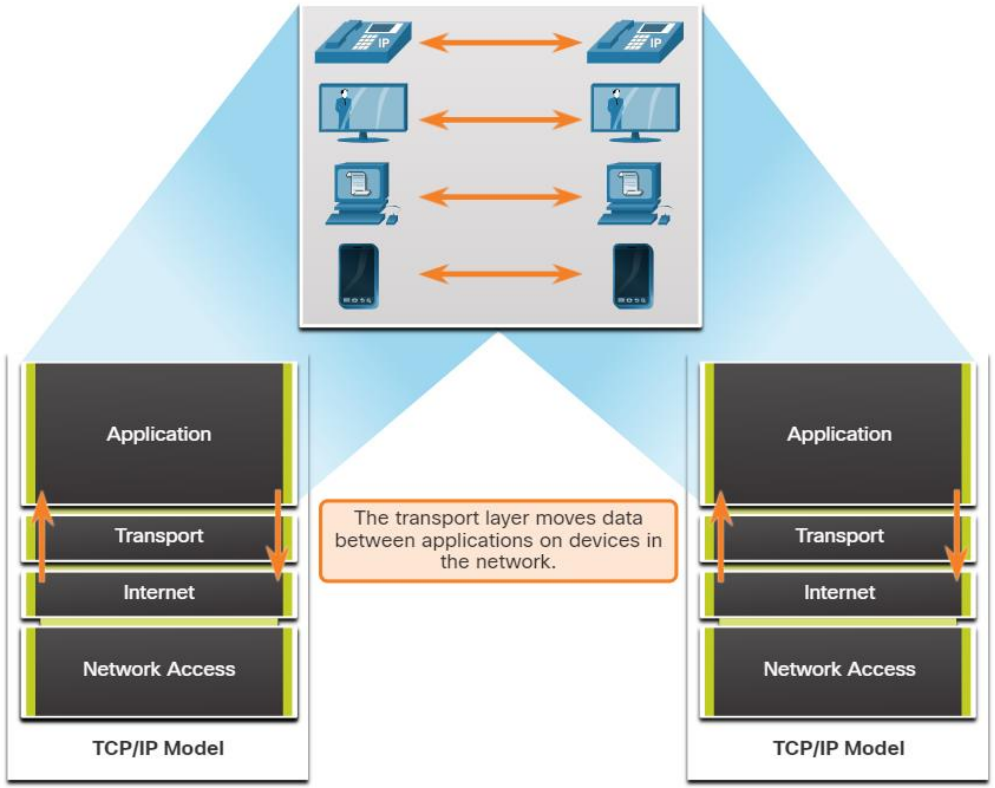


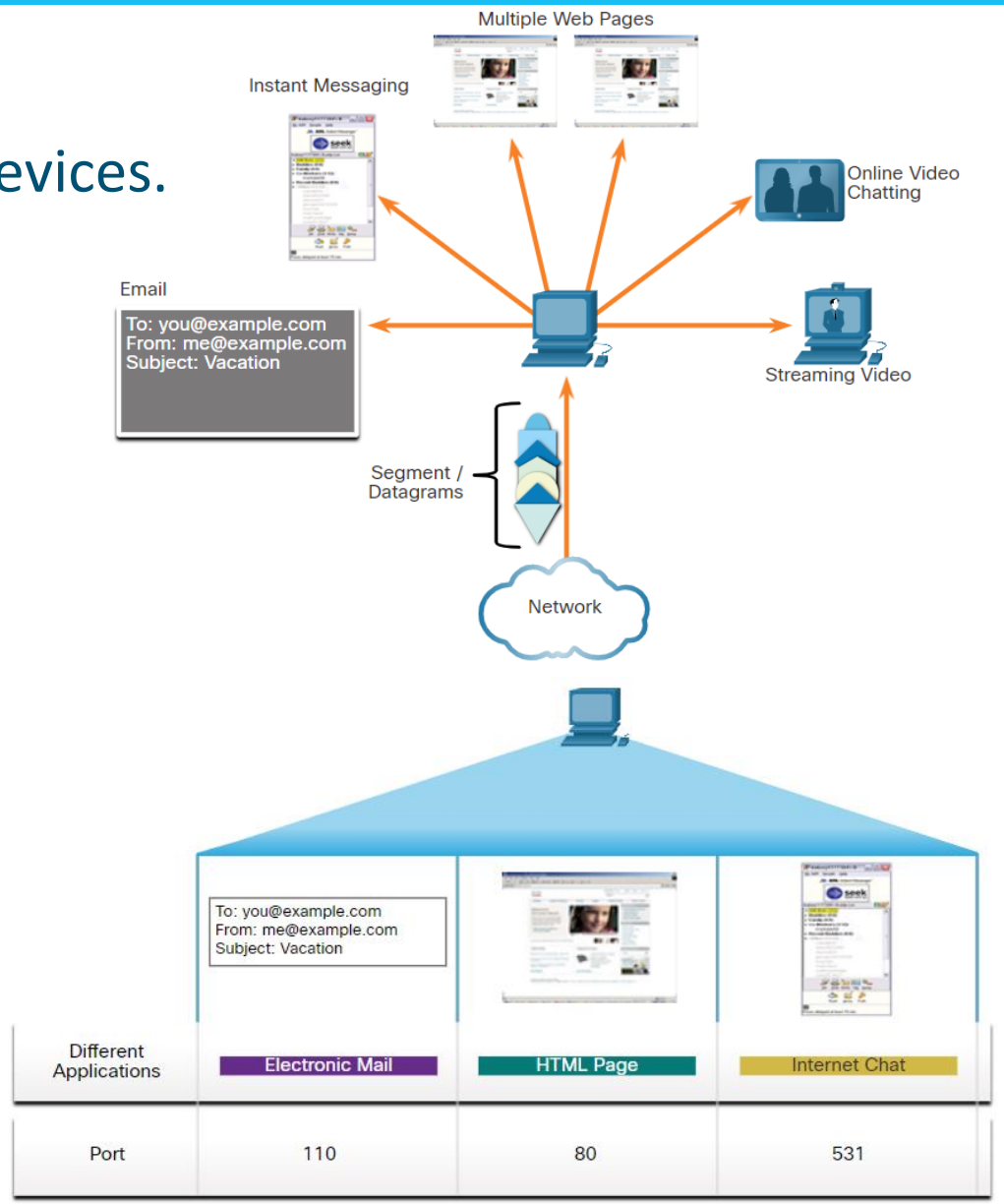
The Transport Layer

Transport Layer Characteristics

Role of the Transport Layer

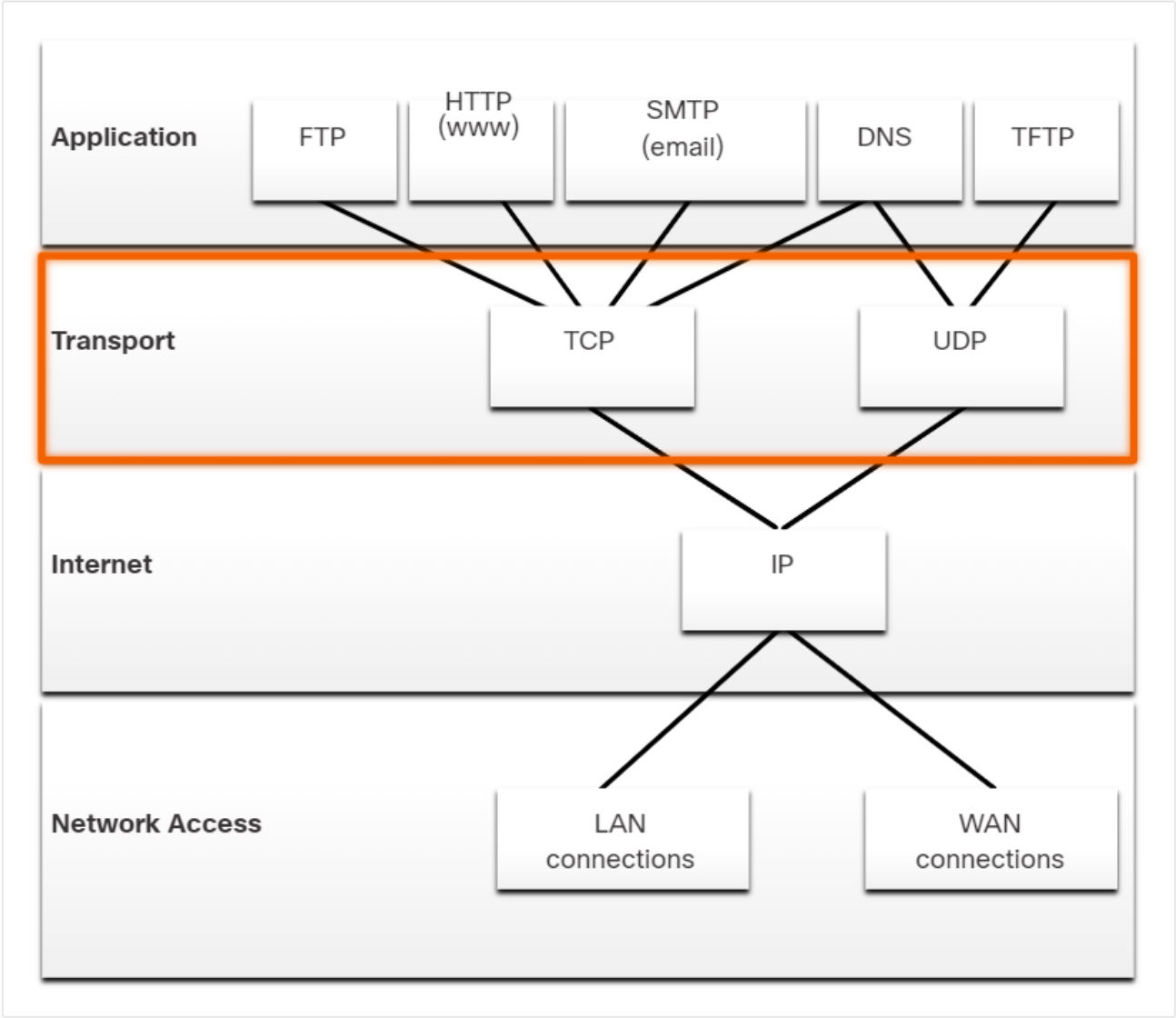
- Tracks individual conversations.
- Moves data between applications on network devices.
- Segments data and reassembles segments.
- Identifies applications using a port number.





Transport Layer Mechanisms

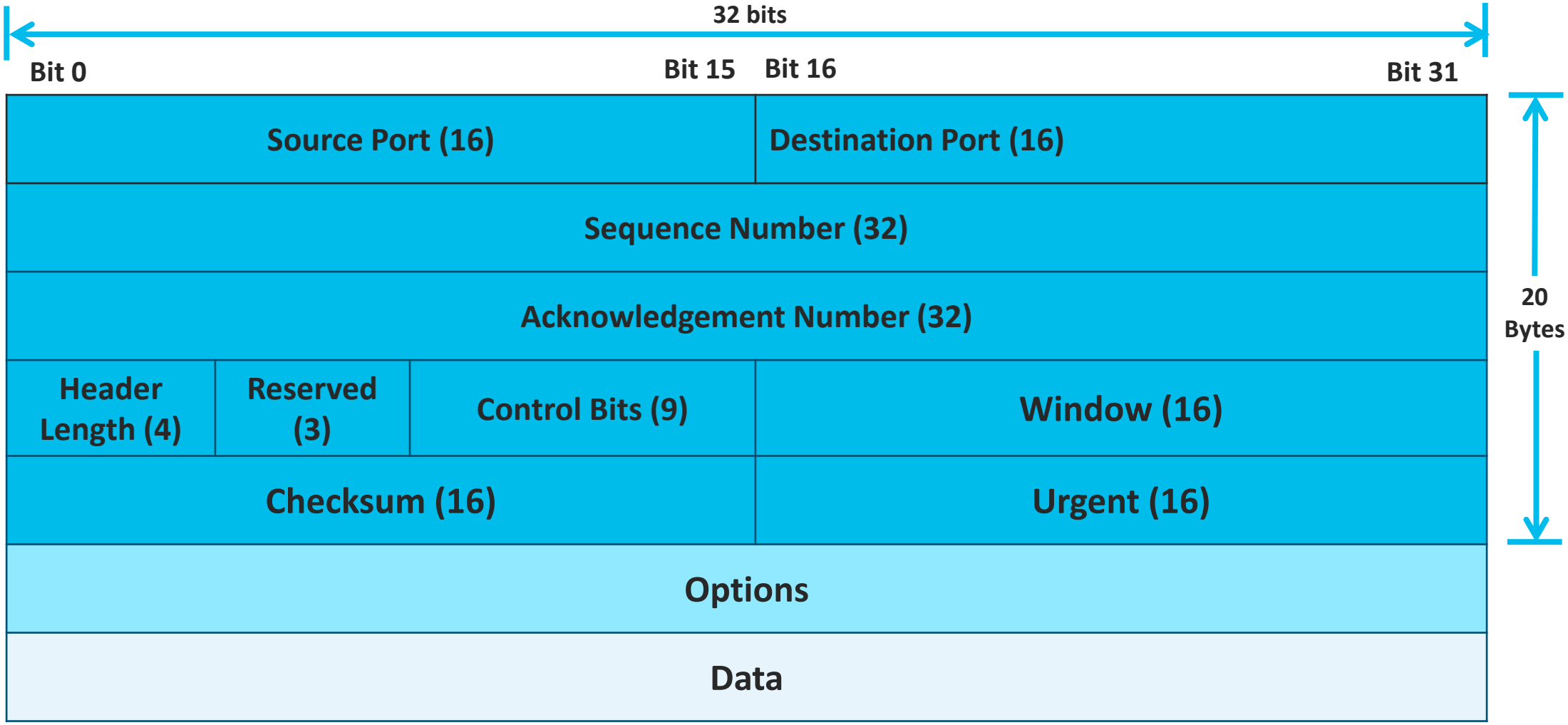
- Segmenting the data into smaller chunks enables many different communications, from many different users, to be interleaved (multiplexed) on the same network.
- The transport layer is also responsible for managing reliability requirements of a conversation.
- TCP/IP provides two transport layer protocols:
  - **Transmission Control Protocol (TCP)**
  - **User Datagram Protocol (UDP)**



Transmission Control Protocol (TCP)

- TCP is considered a reliable, full-featured transport layer protocol, which ensures that all of the data arrives at the destination.
- TCP includes fields which ensure the delivery of the application data. These fields require additional processing by the sending and receiving hosts.
- TCP transport is analogous to sending packages that are tracked from source to destination.
- In order to maintain the state of a conversation and track the information, TCP must first establish a connection between the sender and the receiver. This is why TCP is known as a connection-oriented protocol.
- TCP provides reliability and flow control using these basic operations:
  - Number and track data segments transmitted to a specific host from a specific application
  - Acknowledge received data
  - Retransmit any unacknowledged data after a certain amount of time
  - Sequence data that might arrive in wrong order
  - Send data at an efficient rate that is acceptable by the receiver

The TCP Header

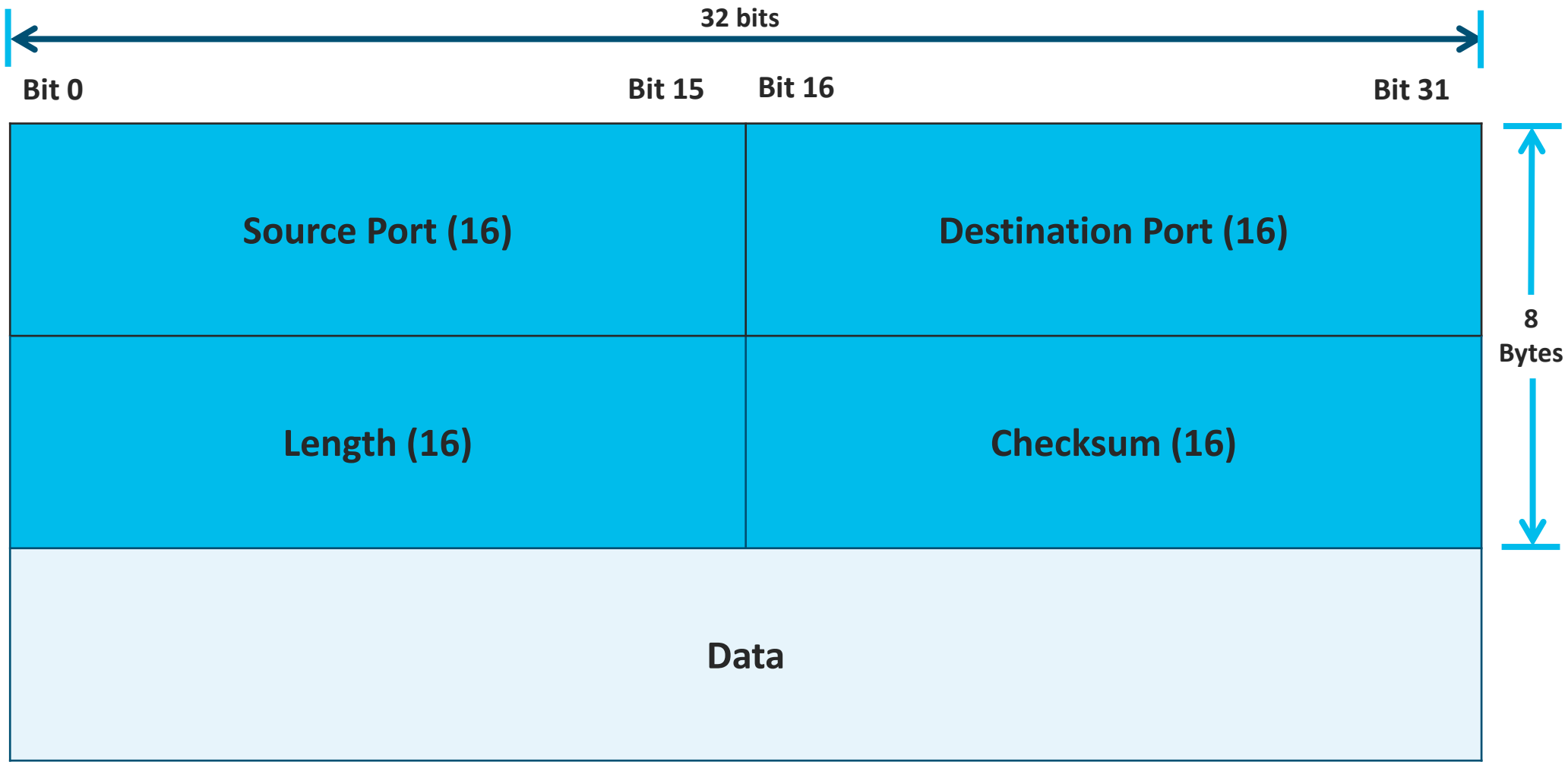


The TCP Header

User Datagram Protocol (UDP)

- UDP is a simpler transport layer protocol than TCP.
- It does not provide reliability and flow control, which means it requires fewer header fields.
- The sender and the receiver UDP processes do not have to manage reliability and flow control, this means UDP datagrams can be processed faster than TCP segments.
- UDP provides the basic functions for delivering datagrams between the appropriate applications, with very little overhead and data checking.
- UDP is a connectionless protocol. Because UDP does not provide reliability or flow control, it does not require an established connection.
- UDP is also known as a stateless protocol. Because UDP does not track information sent or received between the client and server.
- UDP is like placing a regular, nonregistered, letter in the mail. The sender of the letter is not aware of the availability of the receiver to receive the letter. Nor is the post office responsible for tracking the letter or informing the sender if the letter does not arrive at the final destination.

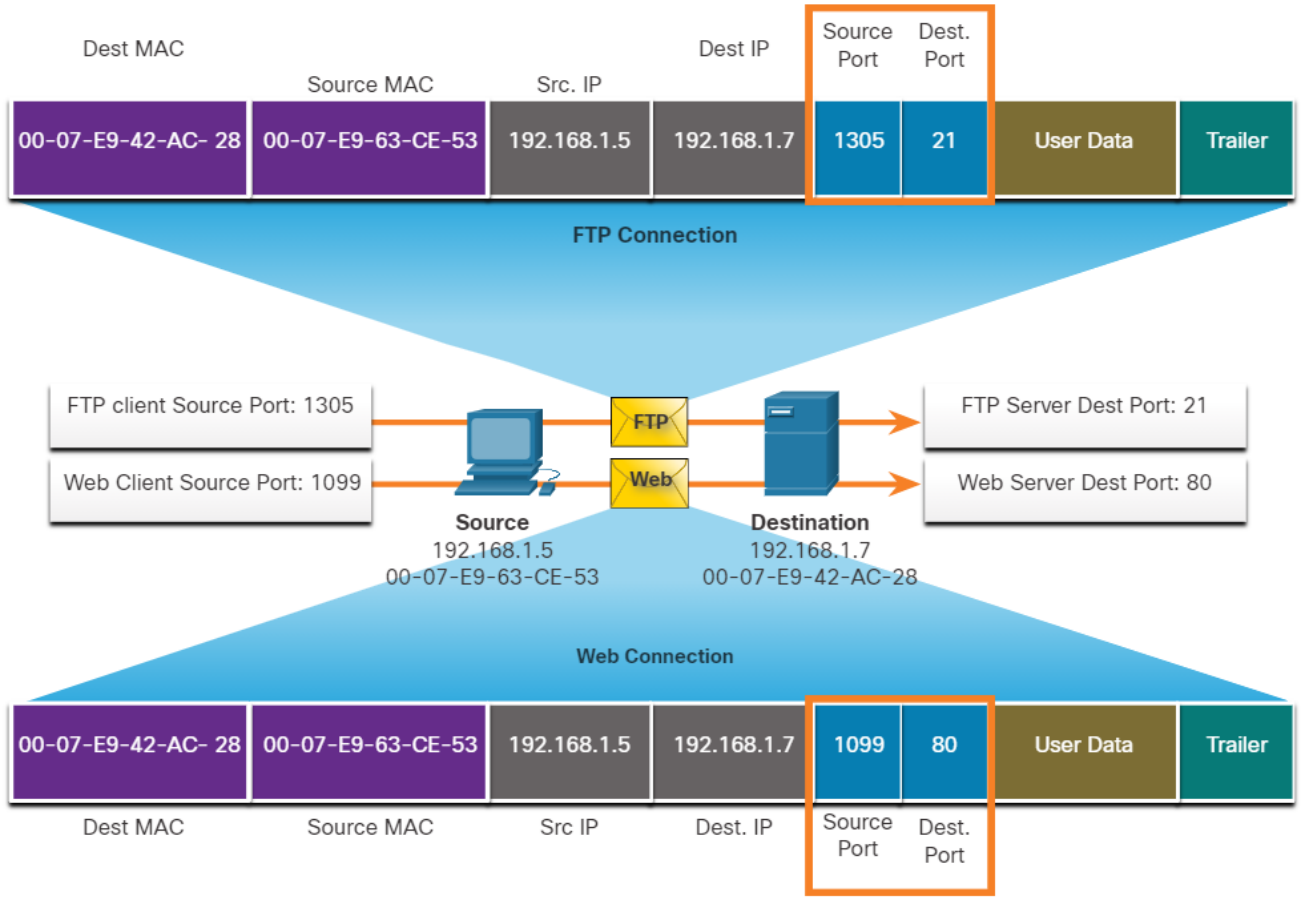
The UDP Header



The UDP Header

Socket Pairs

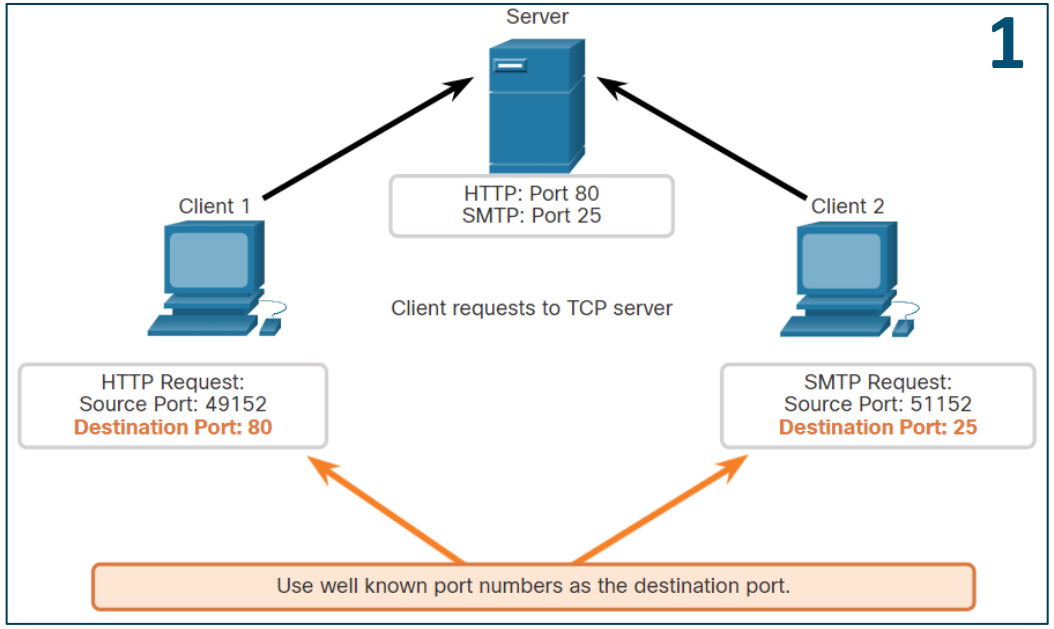
- The source and destination ports are placed within the segment. The segments are then encapsulated within an IP packet.
- The IP packet contains the IP address of the source and destination. The combination of the source IP address and source port number, or the destination IP address and destination port number is known as a **socket**.
- Sockets enable multiple processes, running on a client, to distinguish themselves from each other, and multiple connections to a server process to be distinguished from each other.

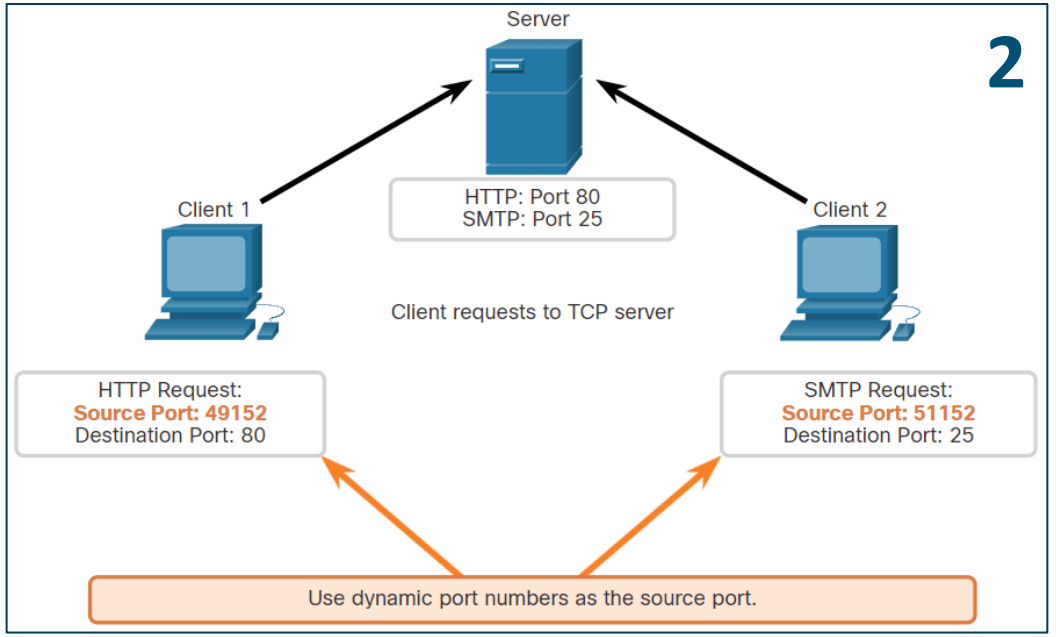


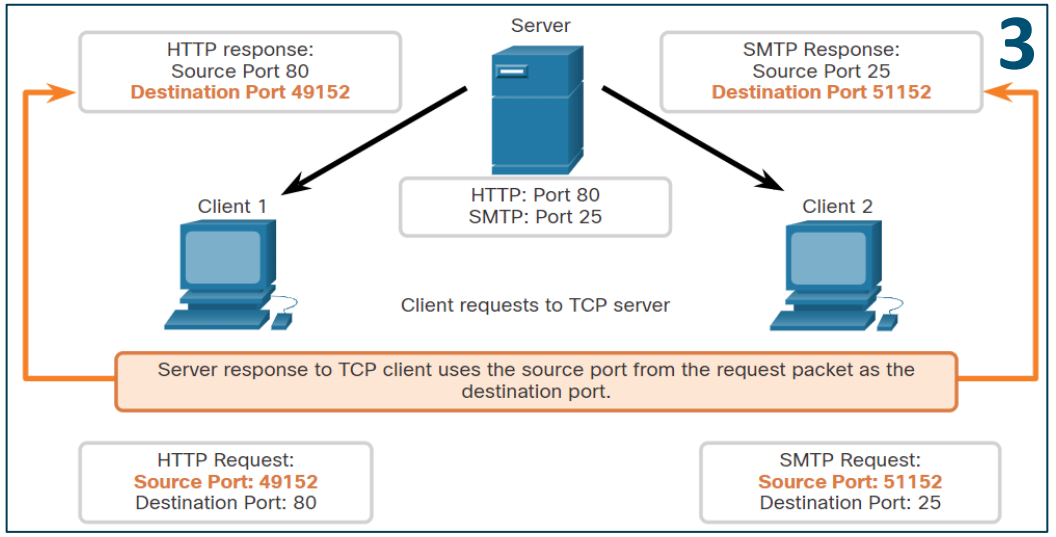
Transport Layer Session Establishment

TCP Server Processes

- Destination port numbers:
  - Uses well-known port numbers.
- Source port numbers:
  - Uses dynamic port numbers.
  - When establishing a connection with a server, the transport layer on the client establishes a source port to keep track of data sent from the server.

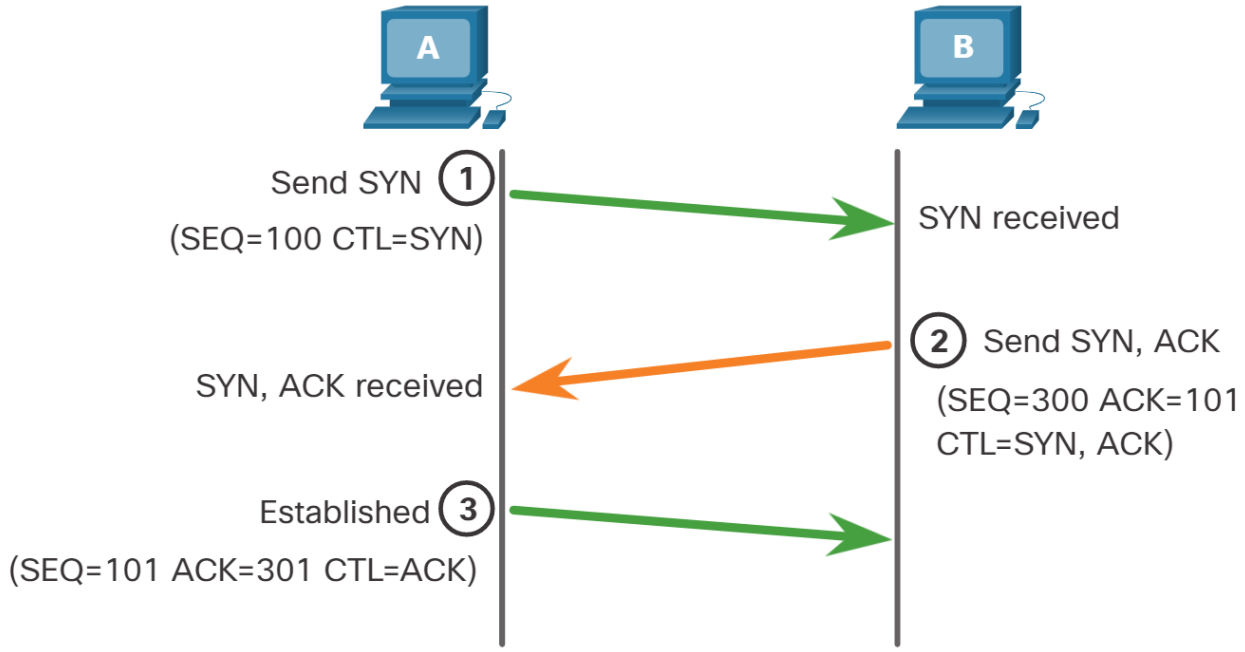






TCP Connection Establishment

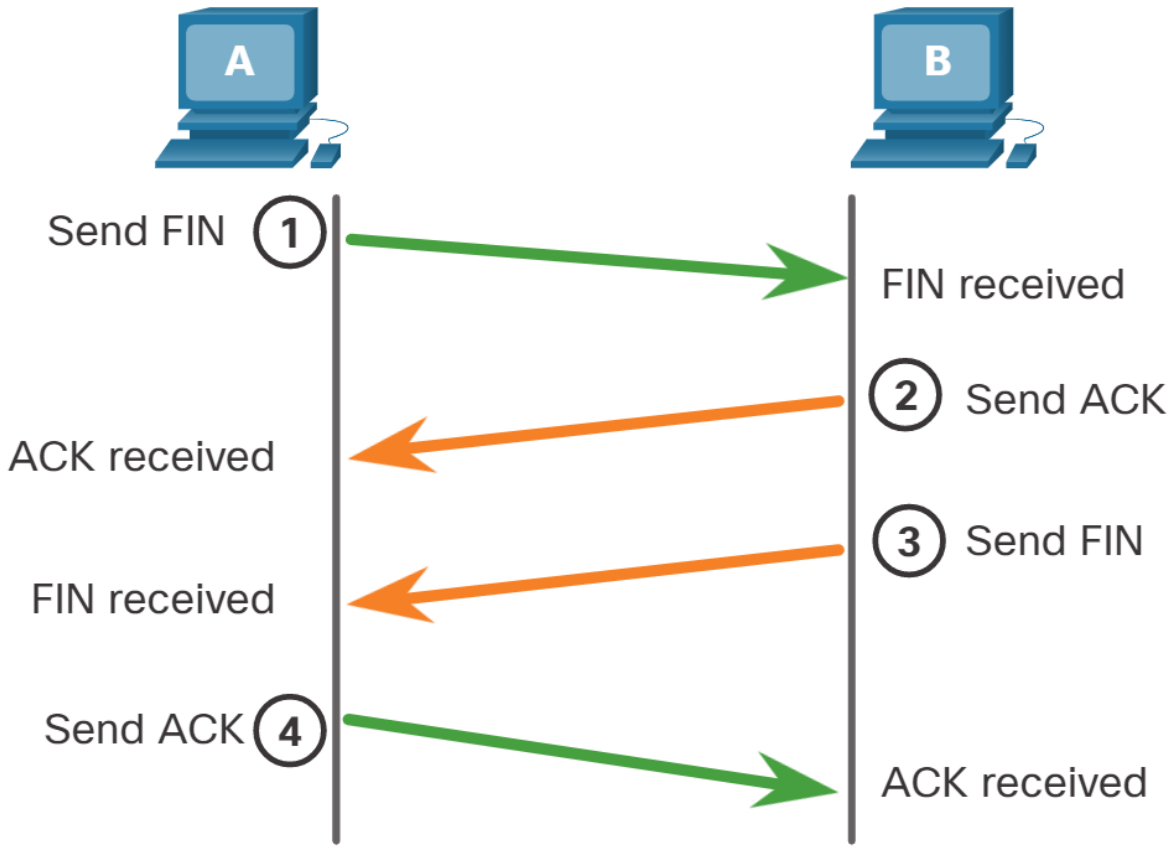
- In TCP connections, the host client establishes the connection with the server using the three-way handshake process.
- The three-way handshake validates that the destination host is available to communicate
- The TCP connection establishment steps are:
  - **Step 1. SYN**: The initiating client requests a client-to-server communication session with the server.
  - **Step 2. ACK and SYN**: The server acknowledges the client-to-server communication session and requests a server-to-client communication session.
  - **Step 3. ACK**: The initiating client acknowledges the server-to-client communication session.



TCP 3-way Handshake

Session Termination

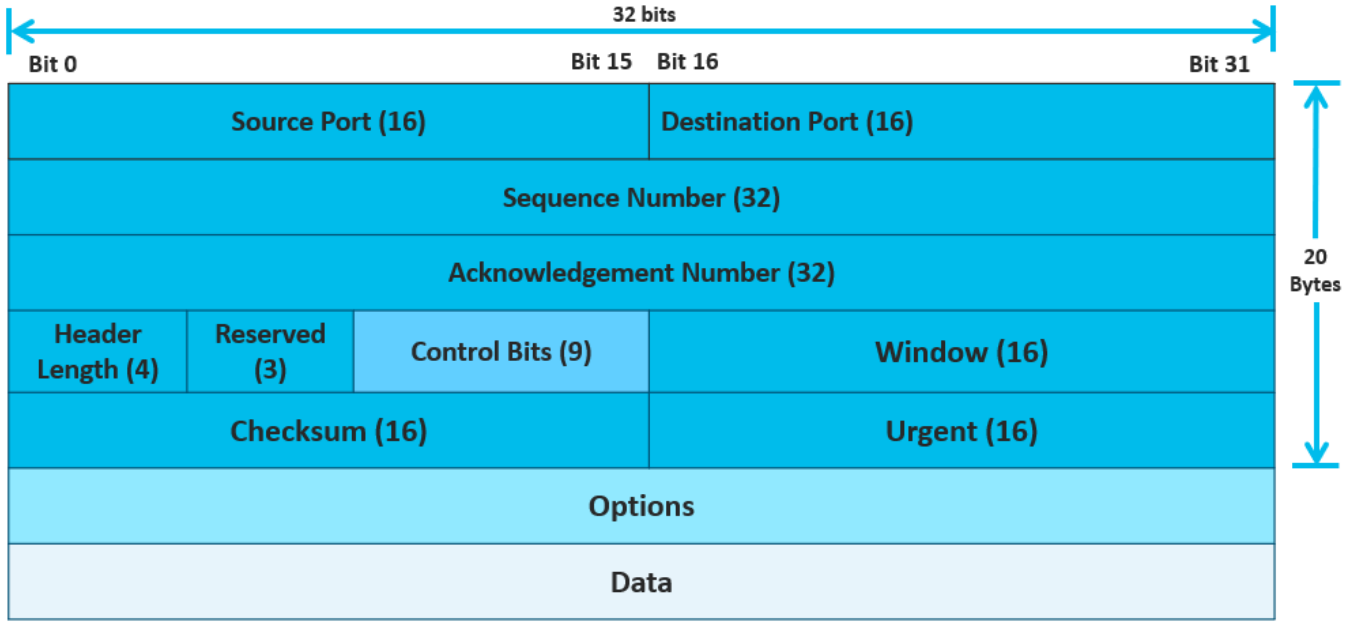
- To terminate a single conversation supported by TCP, four exchanges are needed to end both sessions. Either the client or the server can initiate the termination.
- The session termination steps are:
  - **Step 1. FIN**: When the client has no more data to send in the stream, it sends a segment with the FIN flag set.
  - **Step 2. ACK**: The server sends an ACK to acknowledge the receipt of the FIN to terminate the session from client to server.
  - **Step 3. FIN**: The server sends a FIN to the client to terminate the server-to-client session.
  - **Step 4. ACK**: The client responds with an ACK to acknowledge the FIN from the server.



TCP Three-way Handshake Analysis

The six bits in the Control Bits field of the TCP segment header are also known as flags. A flag is a bit that is set to either on or off. The six control bits flags are as follows:

- **URG** - Urgent pointer field significant
- **ACK** - Acknowledgment flag used in connection establishment and session termination
- **PSH** - Push function
- **RST** - Reset the connection when an error or timeout occurs
- **SYN** - Synchronize sequence numbers used in connection establishment
- **FIN** - No more data from sender and used in session termination



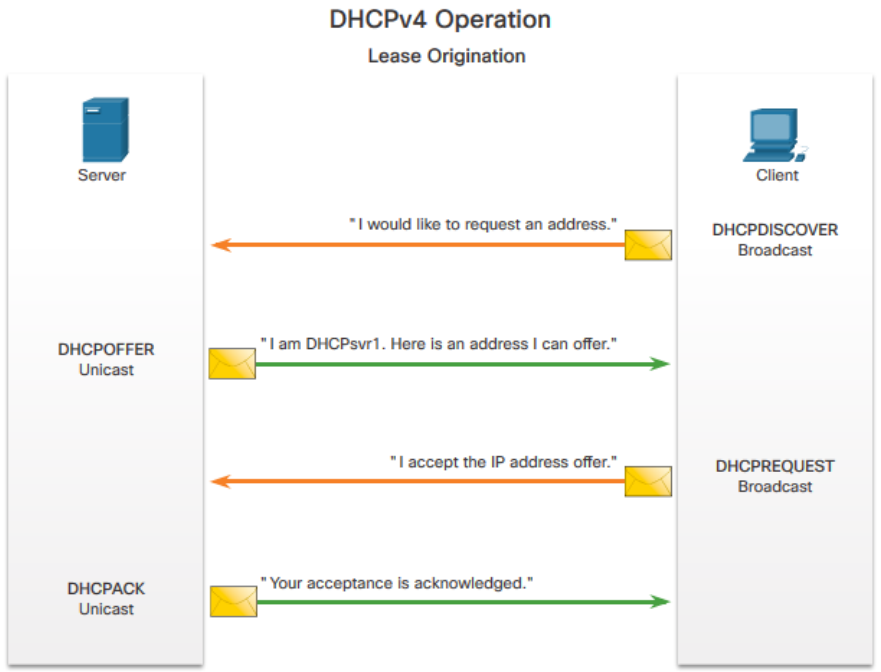
Network Services

DHCP

DHCP Overview

Dynamic Host Configuration Protocol (DHCP)

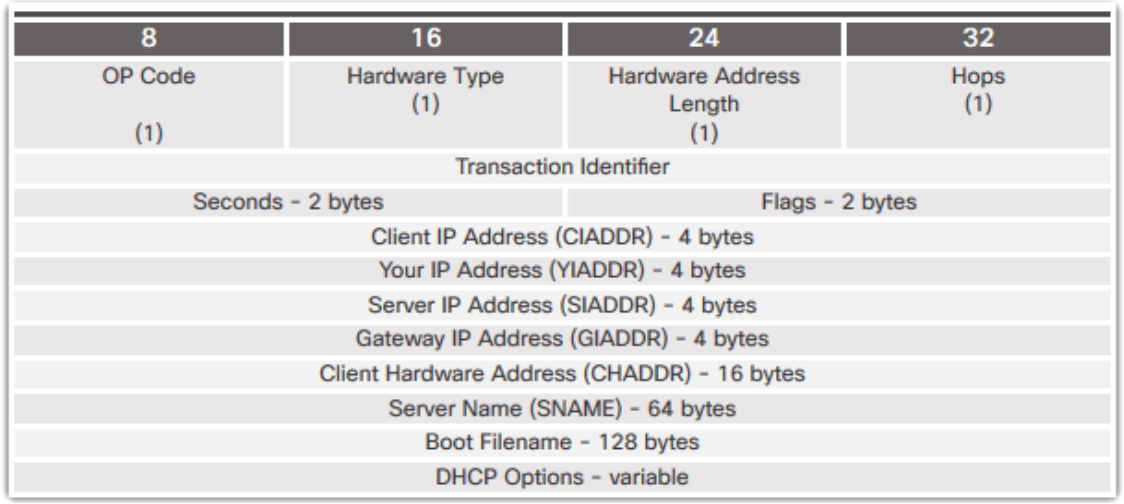
- Provides IP addressing information such as IP address, subnet mask, default gateway, DNS server IP address and domain name.
- Messages
  - **Discover**
  - **Offer**
  - **Request**
  - **Ack(nowledge)**
- If the IPv4 address requested by the client, or offered by the server, is still available, the server returns the DHCPACK message. If the offer is no longer valid, then the selected server responds with a DHCPNAK message. If a DHCPNAK message is returned, then the selection process begins again with a new DHCPDISCOVER message being transmitted.



DHCPv4 Message Format

The DHCPv4 messages are encapsulated within the UDP transport protocol.

A DHCP message contains the following fields:



8	16	24	32
OP Code (1)	Hardware Type (1)	Hardware Address Length (1)	Hops (1)
Transaction Identifier			
Seconds - 2 bytes		Flags - 2 bytes	
Client IP Address (CIADDR) - 4 bytes			
Your IP Address (YIADDR) - 4 bytes			
Server IP Address (SIADDR) - 4 bytes			
Gateway IP Address (GIADDR) - 4 bytes			
Client Hardware Address (CHADDR) - 16 bytes			
Server Name (SNAME) - 64 bytes			
Boot Filename - 128 bytes			
DHCP Options - variable			

- **Operation (OP) Code** - Specifies the general type of message.
- **Hardware Type** - Identifies the type of hardware used in the network.
- **Hardware Address Length** - Specifies the length of the address.
- **Hops** - Controls the forwarding of messages.
- **Transaction Identifier** - Used by the client to match the request with replies received from DHCPv4 servers.
- **Seconds** - Identifies the number of seconds elapsed since a client began attempting to acquire or renew a lease.
- **Flags** - Used by a client that does not know its IPv4 address when it sends a request.

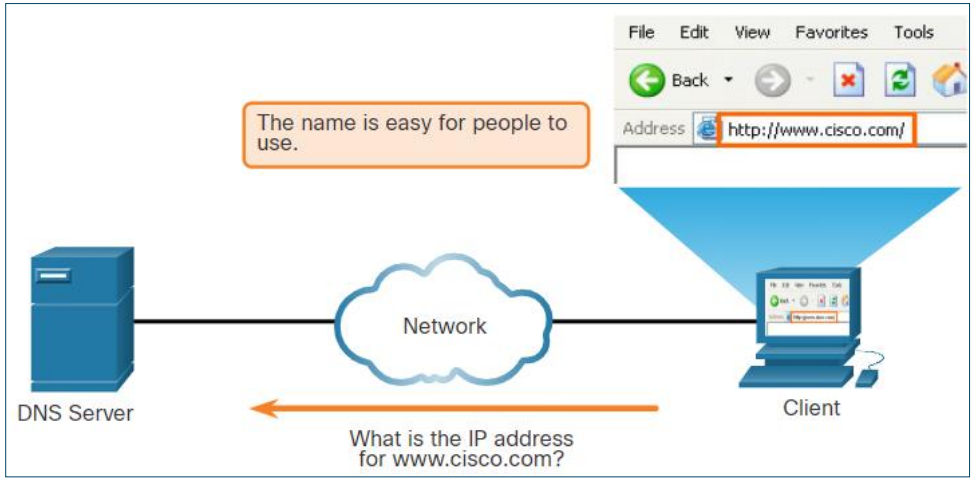
DHCPv4 Message Format

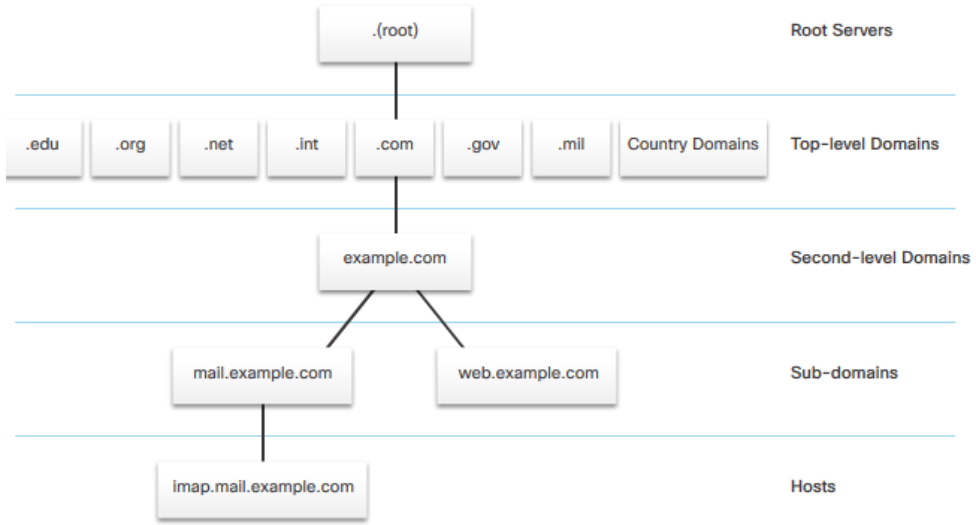
- **Client IP Address** - Used by a client during lease renewal when the address of the client is valid and usable, not during the process of acquiring an address.
- **Your IP Address** - Used by the server to assign an IPv4 address to the client.
- **Server IP Address** - Used by the server to identify the address of the server that the client should use for the next step in the bootstrap process.
- **Gateway IP Address** - Routes DHCPv4 messages when DHCPv4 relay agents are involved.
- **Client Hardware Address** - Specifies the physical layer of the client.
- **Server Name** - Used by the server sending a DHCPOFFER or DHCPACK message.
- **Boot Filename** - Optionally used by a client to request a particular type of boot file in a DHCPDISCOVER message.
- **DHCP Options** - Holds DHCP options, including several parameters required for basic DHCP operation.

DNS

DNS Overview

- Domain Name System (DNS) provides domain names and their associated IP addresses.
- The DNS system consists of a global hierarchy of distributed servers that contain databases of name to IP address mappings.
- Malicious DNS traffic can be detected through protocol analysis and the inspection of DNS monitoring information.
- The DNS consists of a hierarchy of generic top level domains (gTLD) which consist of .com, .net, .org, .gov, .edu, and numerous country-level domains, such as .br (Brazil), .es (Spain),.uk (United Kingdom).
- Second-level domains are represented by a domain name that is followed by a top-level domain.
- Subdomains are found at the next level of the DNS hierarchy and represent some division of the second-level domain.
- Finally, a fourth level can represent a host in a subdomain.

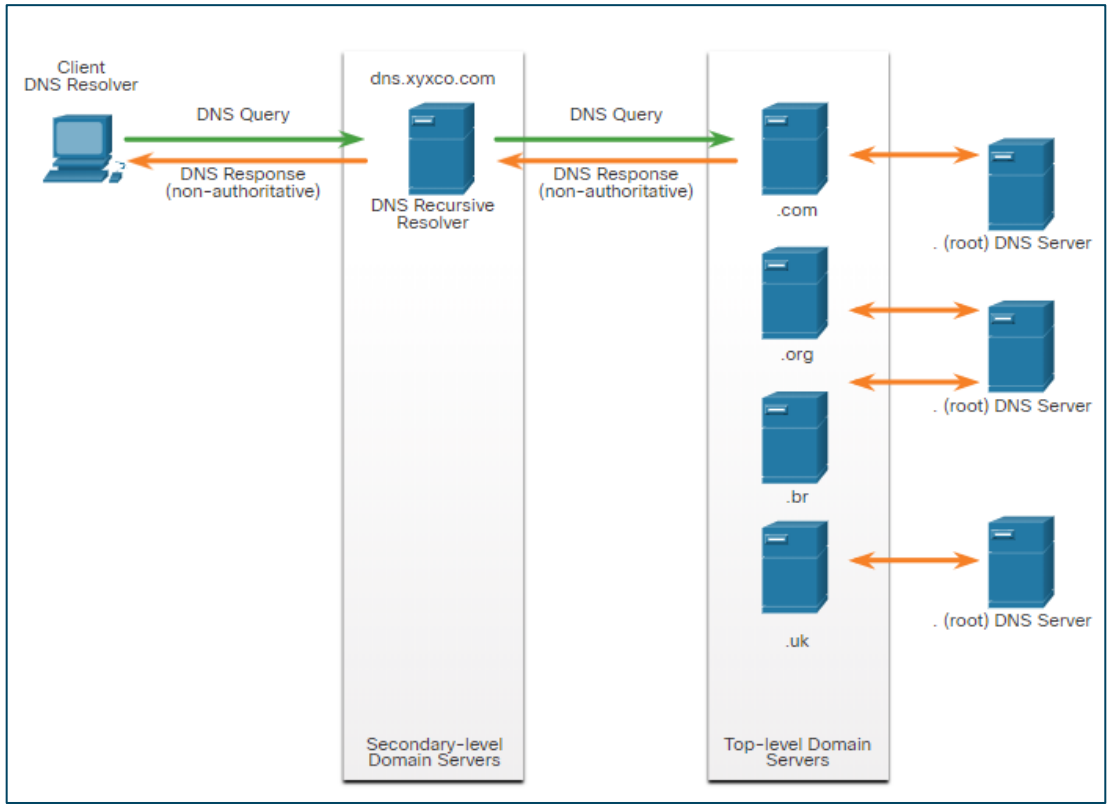




DNS Hierarchy

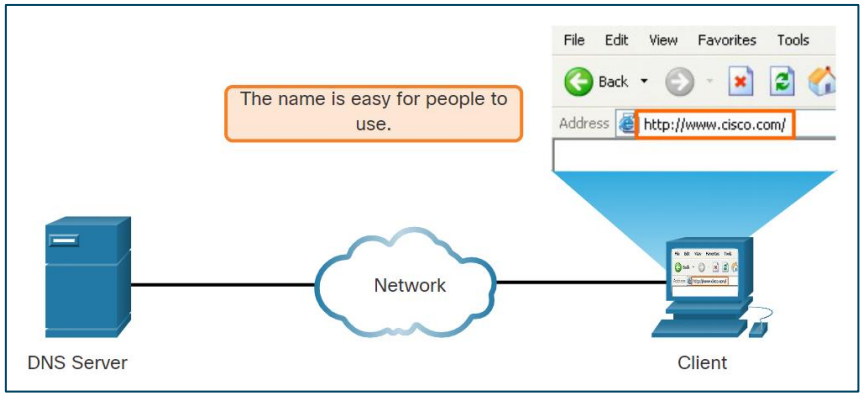
DNS Lookup Process

- To resolve a name to an IP address, the resolver, will first check its local DNS cache. If the mapping is not found, a query will be issued to the DNS server .
- If the mapping is not found there, the DNS server will query other higher-level DNS servers that are authoritative for the top-level domain in order to find the mapping. These are known as **recursive queries**.
- The **caching DNS servers** can resolve recursive queries without forwarding the queries to higher level servers.
- If a server requires data for a zone, it will request a transfer of that data from an authoritative server for that zone. The process of transferring DNS data between servers is known as **zone transfer**.

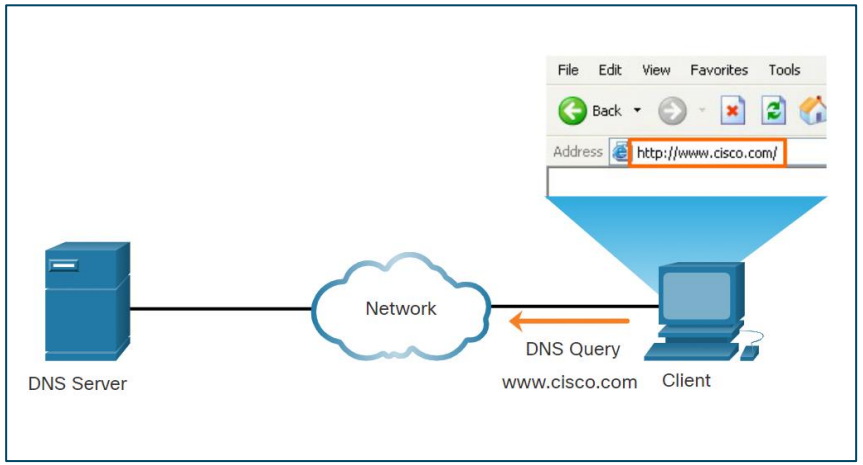


DNS Lookup Process (Cont'd)

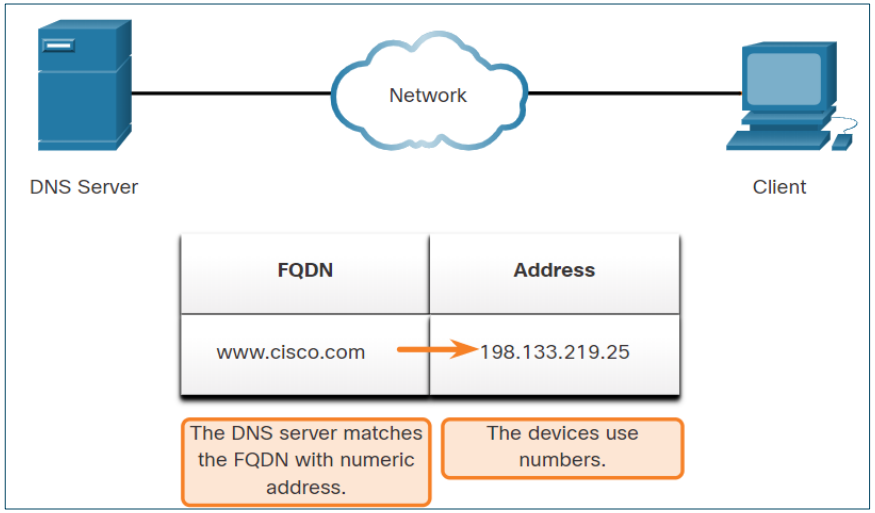
Steps involved in DNS resolution:



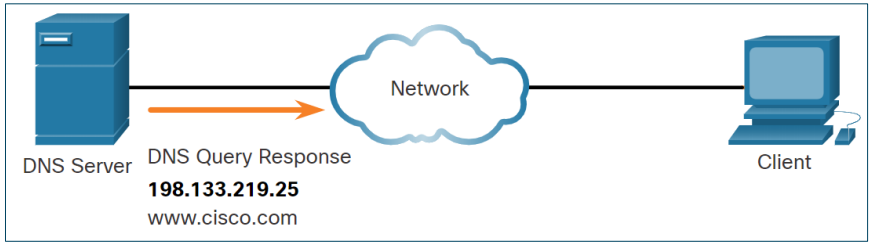
Step 1 - The user types an FQDN into a browser application Address field.



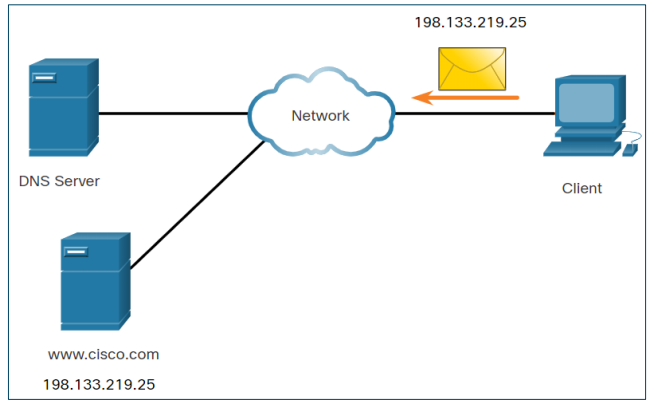
Step 2 - A DNS query is sent to the designated DNS server for the client computer.



Step 3 - The DNS server matches the FQDN with its IP address.



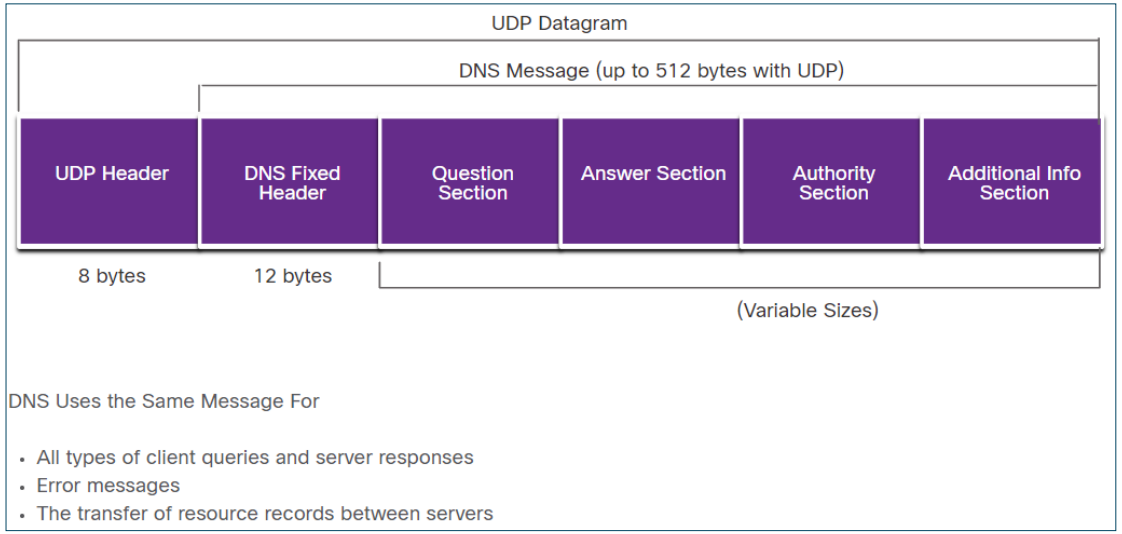
Step 4 - The DNS query response is sent back to the client with the IP address for the FQDN.



Step 5 - The DNS server matches the FQDN with its IP address.

DNS Message Format

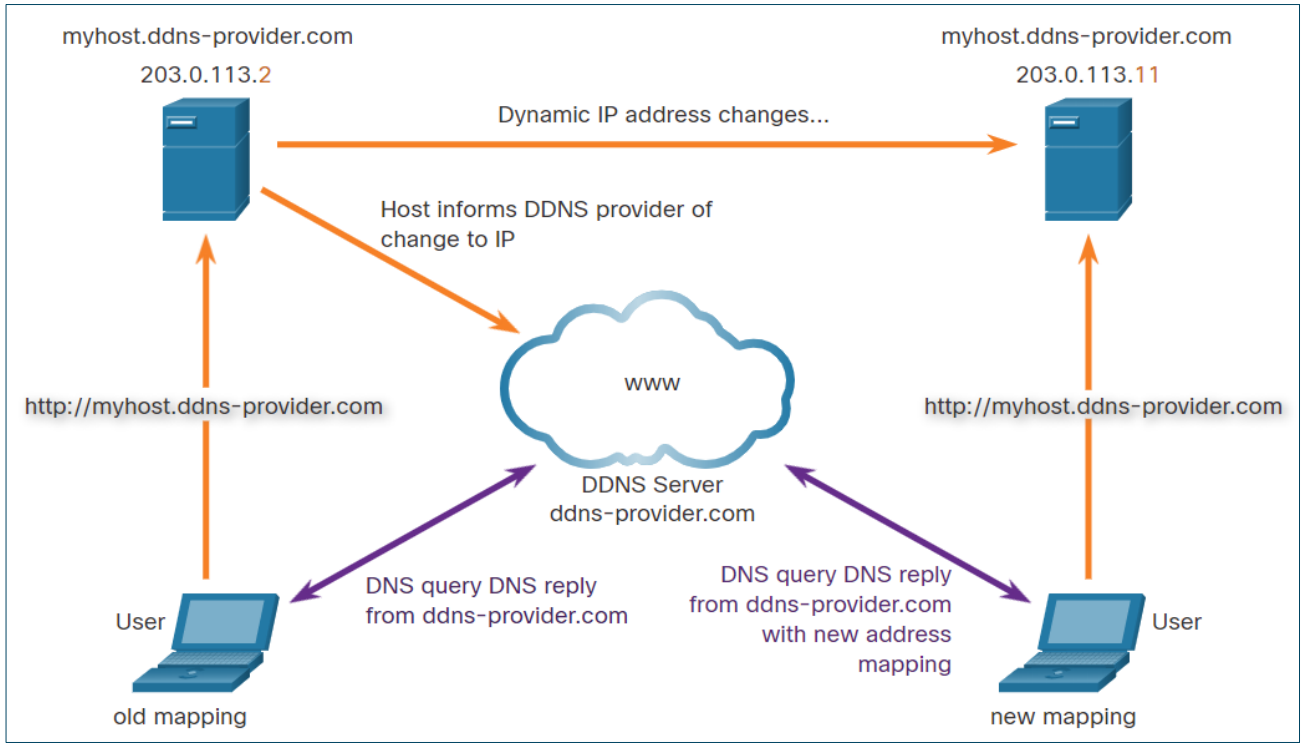
- DNS uses UDP port 53 for DNS queries and responses.
- If a DNS response exceeds 512 bytes, Dynamic DNS (DDNS) is used.
- The DNS protocol communications use a single format called a message.
- DNS uses the same message format for all types of client queries and server responses, error messages, and transfer of resource record information.



DNS message section	Description
Question	The question for the server. It contains the domain name to be resolved, the class of domain, and the query type.
Answer	The DNS resource record, or RR, for the query including the resolved IP address depending on the RR type.
Authority	Contains the RRs for the domain authority.
Additional	Relevant to query responses only. Consists of RRs that hold additional information that will make query resolution more efficient

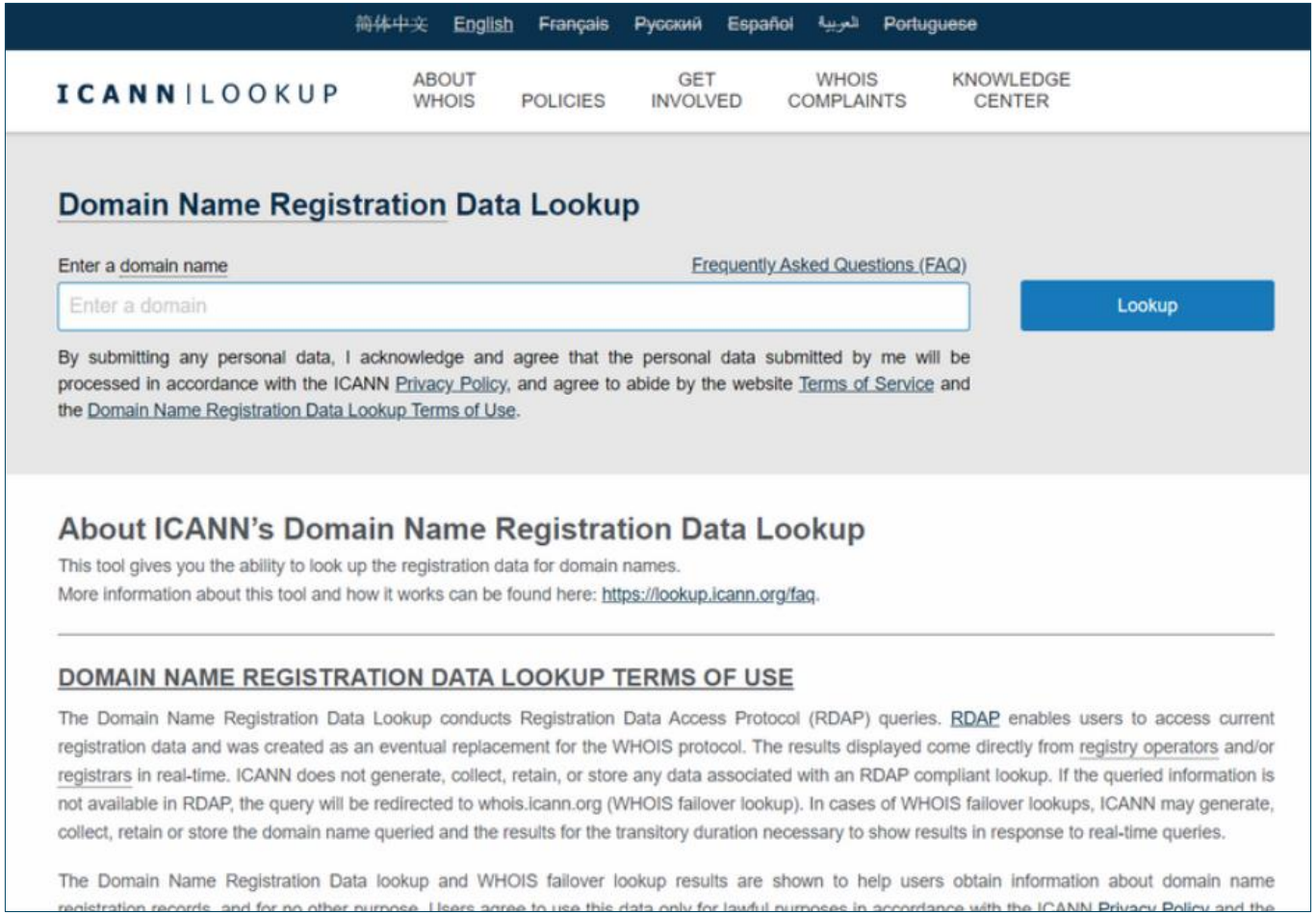
Dynamic DNS

- Dynamic DNS (DDNS) allows a user or organization to register an IP address with a domain name as in DNS.
- The subdomain is mapped to the IP address of the user's server, or home router connection to the internet.
- When a change is detected, the DDNS provider is immediately informed of the change and the mapping between the user's subdomain and the internet IP address is immediately updated.
- The DDNS provider service supplies that IP address to the resolver's second level DNS server. This DNS server, either at the organization or ISP, provides the DDNS IP address to the resolver.



The WHOIS Protocol

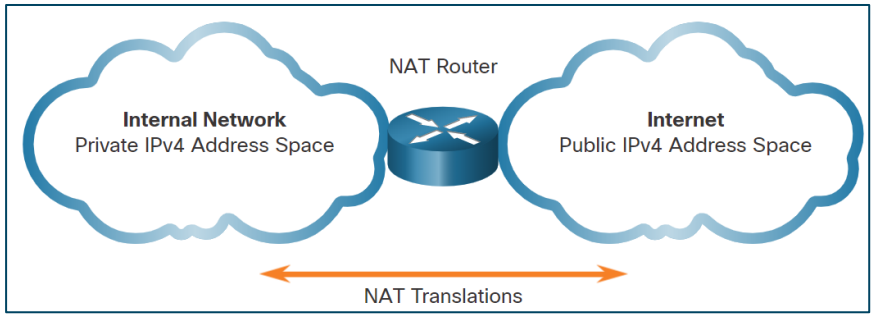
- WHOIS is a TCP-based protocol that is used to identify the owners of internet domains through the DNS system.
- The WHOIS application uses a query, in the form of a FQDN.
- WHOIS is a starting point for identifying potentially dangerous internet locations that may have been reached through the network.
- ICANN Lookup, an internet-based WHOIS tool, is used to obtain the registration record a URL.

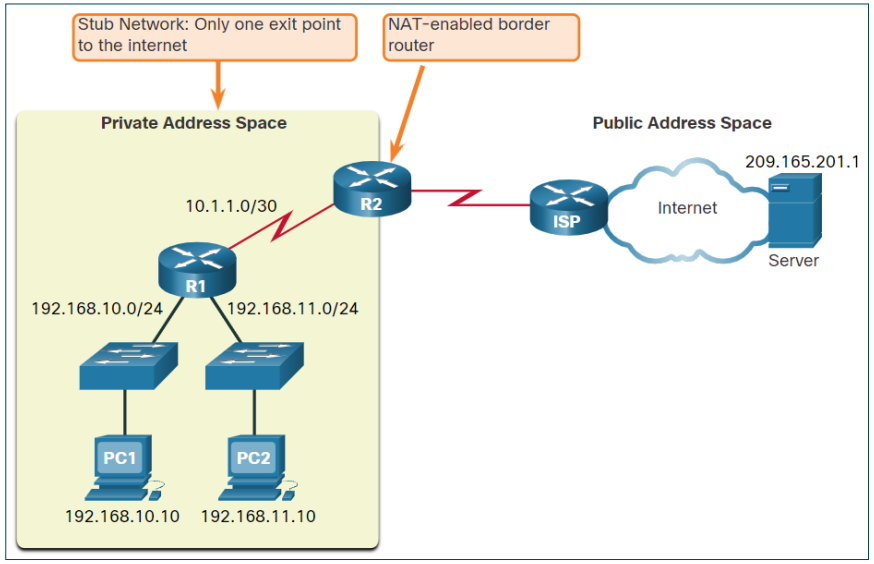


NAT

NAT Overview

- To allow a device with a private IPv4 address to access devices and resources outside the local network, the private address must be translated to a public address.
- NAT provides the translation of private addresses to public addresses.
- A single, public IPv4 address can be shared by thousands of devices, each configured with a unique private IPv4 address.
- The solution to the exhaustion of IPv4 address space and the limitations of NAT is the eventual transition to IPv6.
- NAT is used to conserve public IPv4 addresses.
- NAT-enabled routers can be configured with one or more valid public IPv4 addresses which are known as the NAT pool.
- To outside devices, all traffic entering and exiting the network appears to have a public IPv4 address from the provided pool of addresses.
- A NAT router typically operates at the border of a stub network.



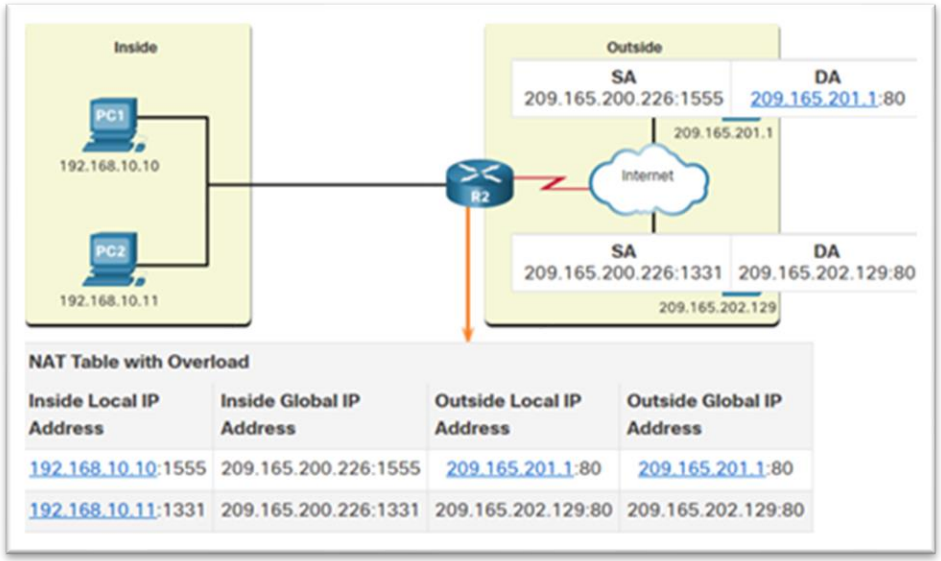


NAT Table

Inside Local	Inside Global	Outside Local	Outside Global
192.168.10.10	209.165.200.226	209.165.201.1	209.165.201.1

Port Address Translation

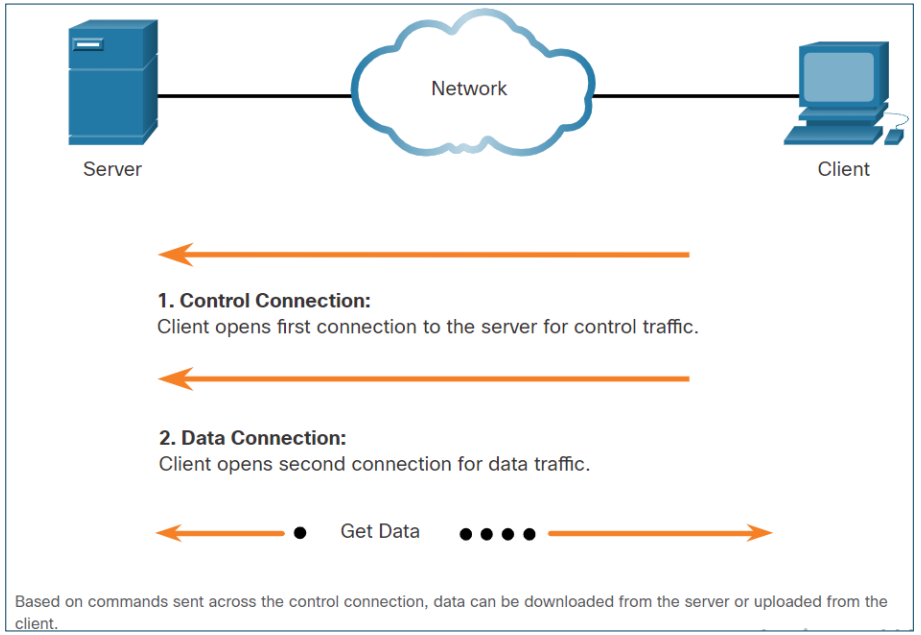
- Port Address Translation (PAT), also known as NAT overload, maps multiple private IPv4 addresses to a single public IPv4 address or a few addresses.
- When a device initiates a TCP/IP session, it generates a TCP or UDP source port value, or a specially assigned query ID for ICMP, to uniquely identify the session.
- PAT ensures that devices use a different TCP port number for each session with a server on the internet.
- PAT adds unique source port numbers to the inside global address to distinguish between translations.



File Transfer and Sharing Services

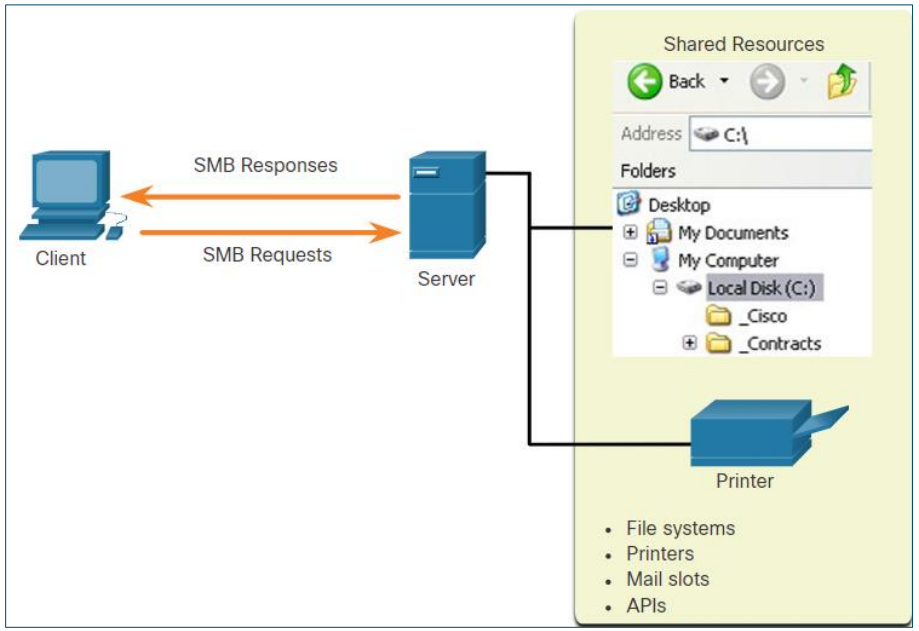
FTP and TFTP

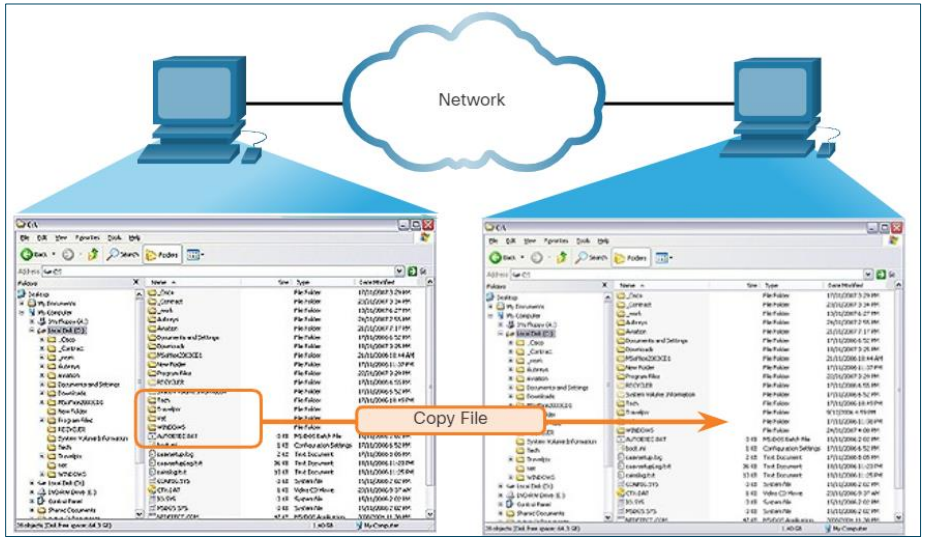
- File Transfer Protocol (FTP) allows data transfers between a client and a server.
- An FTP client runs on a computer and is used to push and pull data from an FTP server.
- FTP connections between the client and server:
  - **Control Connection**: The client opens the first connection to the server for control traffic.
  - **Data Connection**: The client opens the second connection to the server for data traffic.
- Trivial File Transfer Protocol (TFTP) is a simplified file transfer protocol that uses well-known UDP port number 69. TFTP is fast, but unreliable.



SMB

- **The Server Message Block (SMB)** is a client/server file sharing protocol that describes the structure of shared network resources.
- SMB is a client/server, request-response protocol.
- Servers can make their own resources available to clients on the network.
- SMB messages can start, authenticate, and terminate sessions, control file and printer access, and allow an application to send or receive messages to or from another device.
- SMB file sharing and print services have become the mainstay of Microsoft networking.
- A file may be copied from PC to PC with Windows Explorer using the SMB protocol.

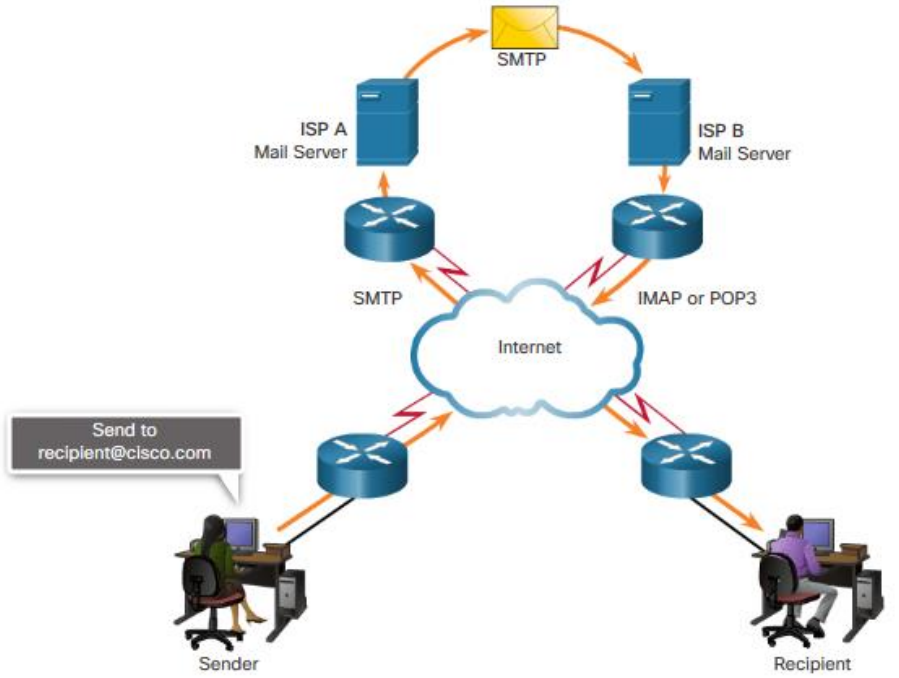




Email

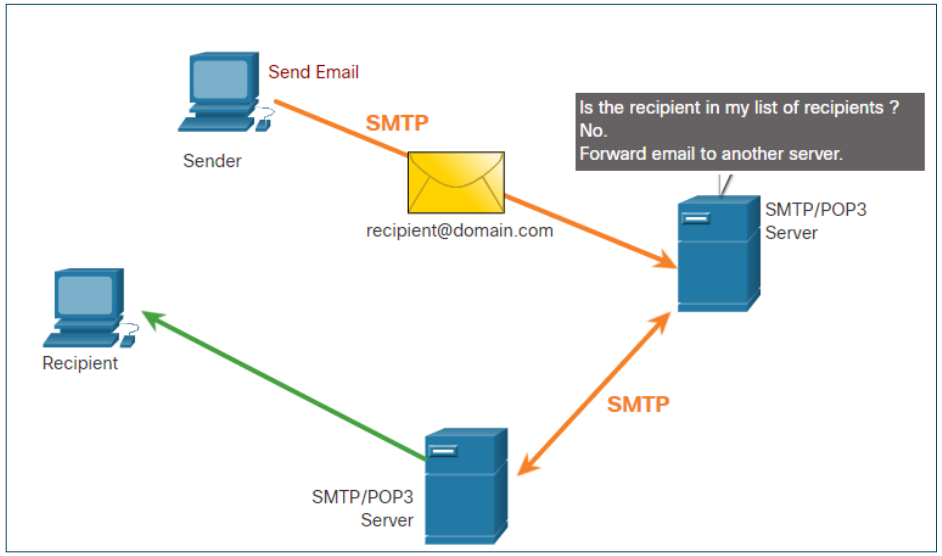
Email Overview

- Email supports three separate protocols for operation:
  - Simple Mail Transfer Protocol (SMTP)
  - Post Office Protocol version 3 (POP3)
  - Internet Message Access Protocol (IMAP)
- The application layer process that sends mail uses SMTP. A client retrieves email using one of the two application layer protocols: POP3 or IMAP.



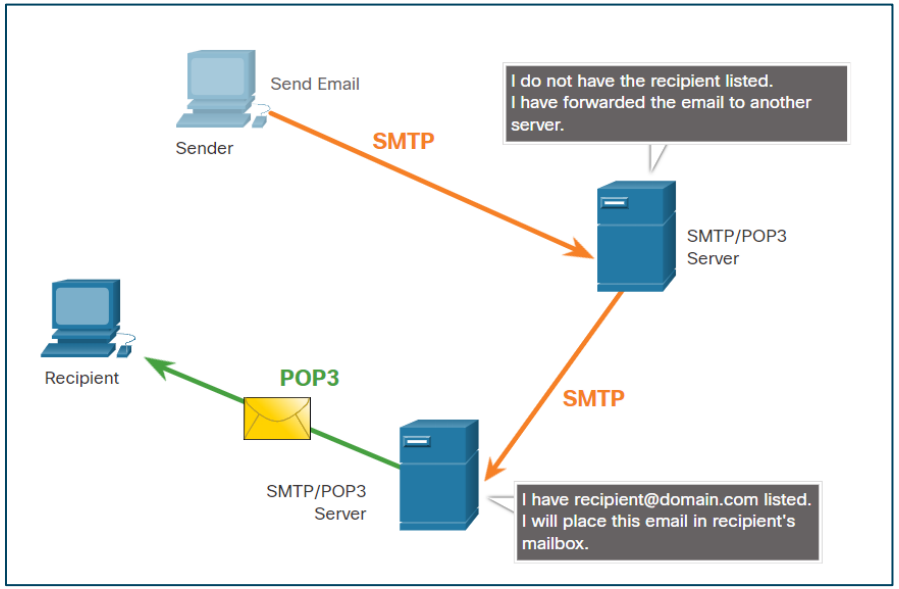
SMTP

- SMTP message formats require a message header and a message body.
- When a client sends an email, the client SMTP process connects with a server SMTP process on a well-known port 25.
- When the server receives the message, it either places the message in a local account, if the recipient is local, or forwards the message to another mail server for delivery.
- Periodically, the server checks the queue for messages and attempts to send them again. If the message is still not delivered after a predetermined expiration time, it is returned to the sender as undeliverable.



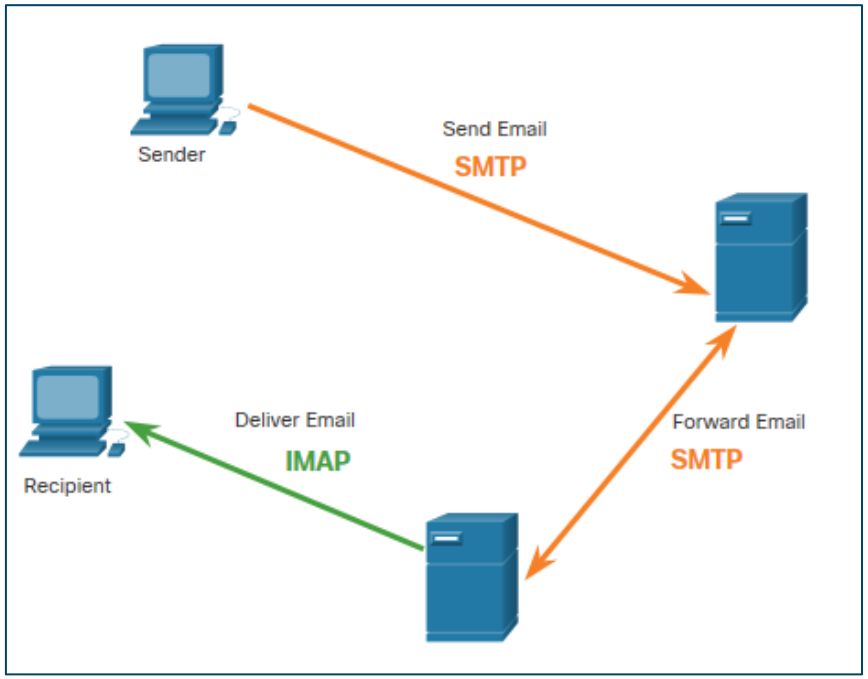
POP3

- POP3 is used by an application to retrieve a mail from a mail server.
- With POP3, email messages are downloaded to the client and removed from the server.
- The server starts the POP3 service by passively listening on TCP port 110 for client connection requests.
- The client sends a request to establish a TCP connection with the server.
- Once the connection is established, the POP3 server sends a greeting. The client and POP3 server then exchange commands and responses until the connection is closed or aborted.



IMAP

- IMAP is the protocol that describes a method to retrieve email messages.
- When the user connects to an IMAP-capable server, copies of the messages are downloaded to the client application. The original messages are kept on the server until manually deleted.
- Users view copies of the messages in their email client software.
- Users can create a file hierarchy on the server to organize and store mail.
- When a user decides to delete a message, the server synchronizes that action and deletes the message from the server.



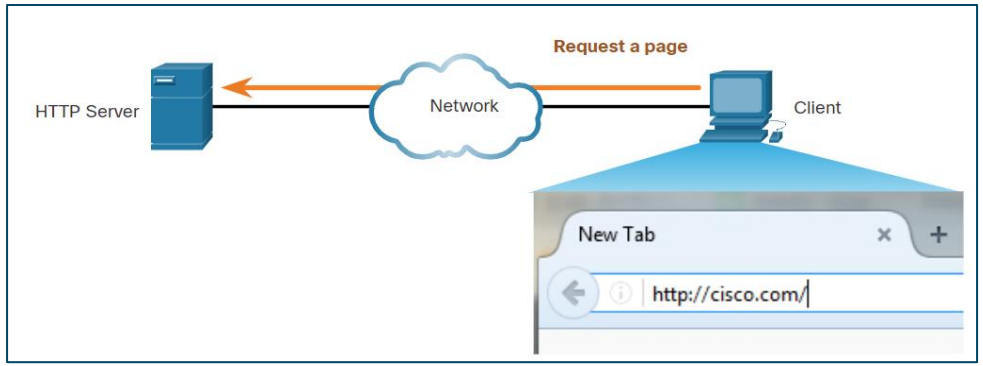
HTTP

HTTP Overview

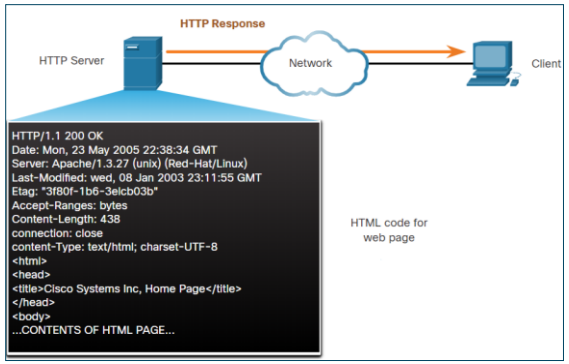
Hypertext Transfer Protocol (HTTP) :

- Port 80
- Governs the way a web server and client interact.
- TCP-based
- Has specific server responses.

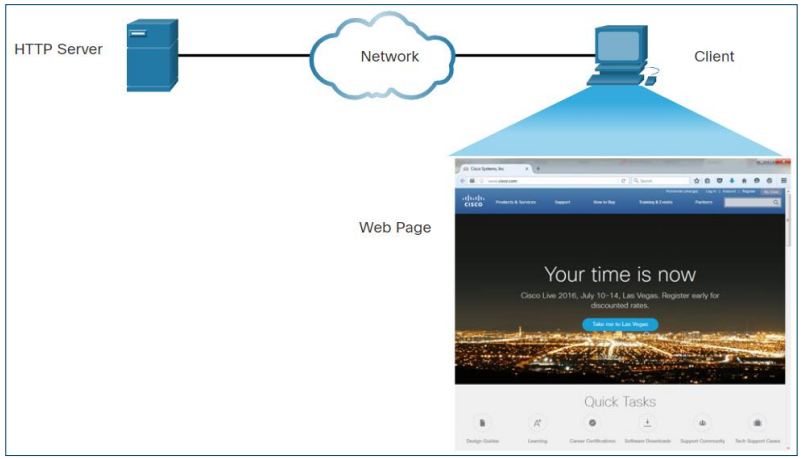
Steps:



Step 1: Client initiates HTTP request to server



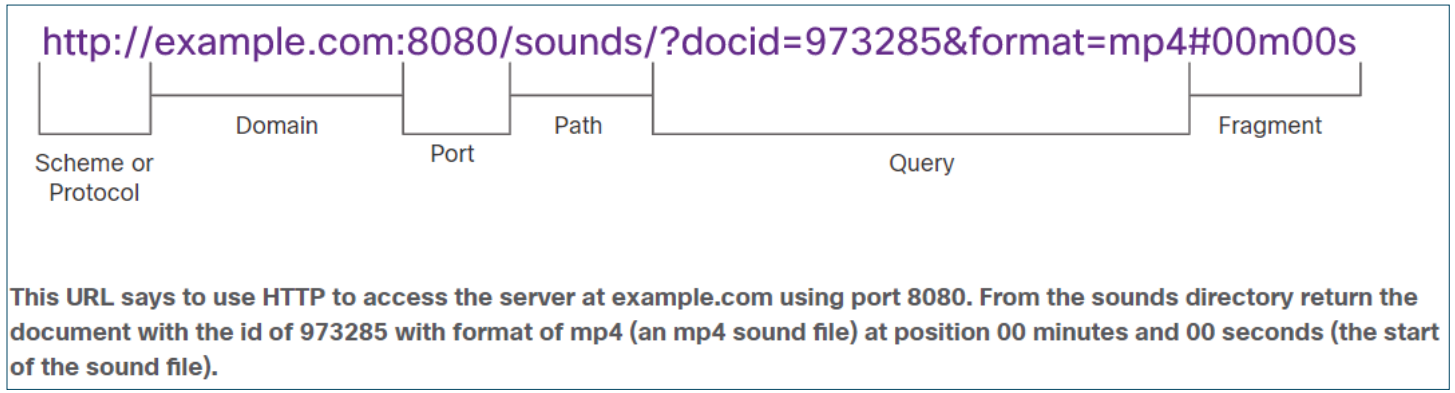
Step 2: In response to the request, the server sends the HTML code for this web page to the browser.



Step 3: Browser interprets HTML code and displays on webpage.

The HTTP URL

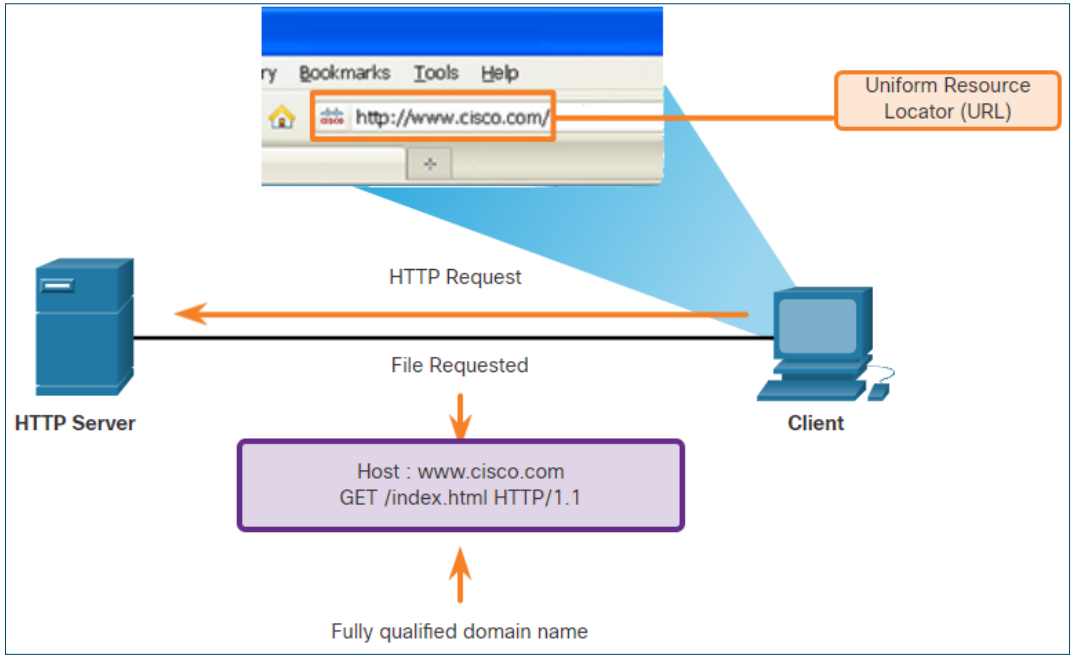
- HTTP URLs can specify the port on the server that should handle the HTTP methods.
- It can specify a query string and fragment.
- Query strings are preceded by a “?” character and typically consist of a series of name and value pairs.
- A fragment is preceded by a “#” character. It refers to a subordinate part of the resource that is requested in the URL.
- The parts of an HTTP URL are shown in the below figure:



This URL says to use HTTP to access the server at example.com using port 8080. From the sounds directory return the document with the id of 973285 with format of mp4 (an mp4 sound file) at position 00 minutes and 00 seconds (the start of the sound file).

HTTP Operation

- HTTP is a request/response protocol that uses TCP port 80.It is flexible but not a secure protocol.
- When a client sends a request to a web server, it will use one of the six methods specified by HTTP:
  - **GET** - A client request for data. A client (web browser) sends the GET message to the web server to request HTML pages.
  - **POST** - Submits data to be processed by a resource.
  - **PUT** - Uploads resources or content to the web server.
  - **DELETE** - Deletes the resource specified.
  - **OPTIONS** - Returns the HTTP methods that the server supports.
  - **CONNECT** - Requests that an HTTP proxy server forwards the HTTP TCP session to the desired destination.



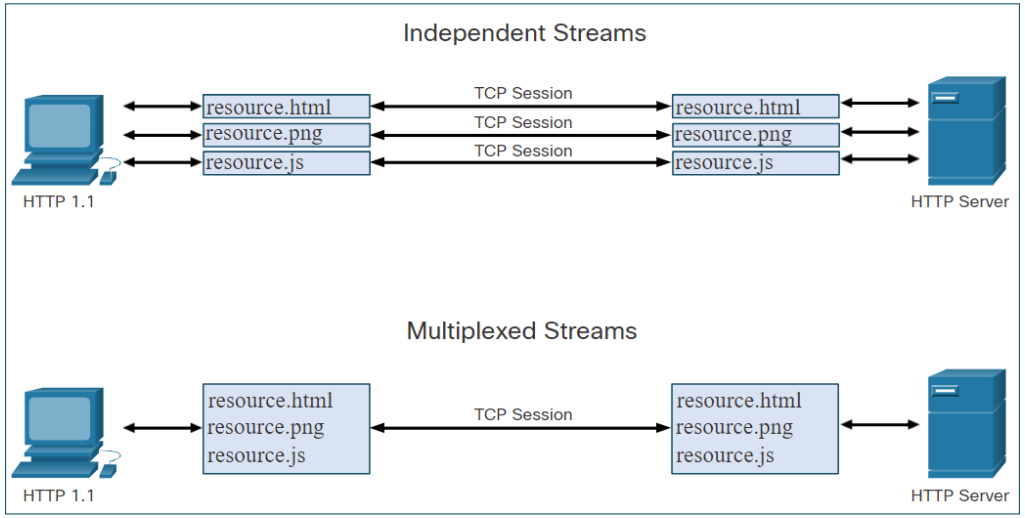
HTTP Status Codes

- The HTTP server responses are identified with various status codes that inform the host application of the outcome of client requests to the server. The codes are organized into five groups.
  - **1xx - Informational**
  - **2xx - Success**
  - **3xx - Redirection**
  - **4xx - Client Error**
  - **5xx - Server Error**

Code	Status	Meaning
1xx - Informational		
100	Continue	The client should continue with request. Server has verified that request can be fulfilled.
2xx - Success		
200	OK	The request completed successfully.
202	Accepted	The request has been accepted for processing, but processing is not completed.
4xx - Client Error		
403	Forbidden	The request is understood by the server, but the resource will not be fulfilled, possibly because the requester is not authorized to view the resource.
404	Not Found	The server cannot find the requested resource.

HTTP/2

- The purpose of HTTP/2 is to improve HTTP performance by addressing latency issues that existed in the HTTP 1.1 version of the protocol.
- HTTP/2 uses the same header format as HTTP 1.1 and uses the same status codes.
- Few important features of HTTP/2 that a cybersecurity analyst must be aware of:
  - Multiplexing
  - Server PUSH
  - A binary protocol
  - Header compression



HTTPS

- For secure communication across the internet, the HTTP Secure (HTTPS) protocol is used.
- HTTPS uses authentication and encryption to secure data as it travels between the client and the server.
- HTTPS uses the same client request-server response process as HTTP, but the data stream is encrypted with Secure Socket Layer (SSL), or Transport Layer Security (TLS), before being transported across the network.
- HTTPS/2 is specified to use HTTPS over TLS with the Application-Layer Protocol Negotiation (ALPN) extension for TLS 1.2 or newer.
- Confidential information is transmitted over the Internet using HTTPS.

Networking Academy

ice.aiub.edu

ice@aiub.edu

01630-665666