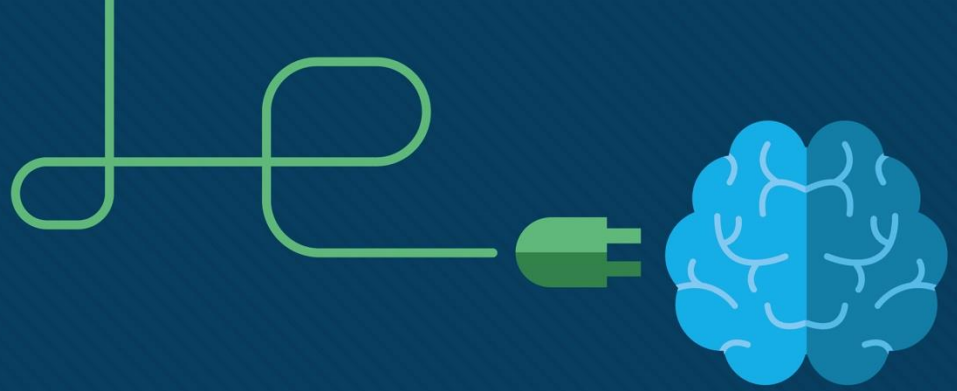


Chapter 4: Network Protocols and Services

CCNA Cybersecurity Operations v1.1

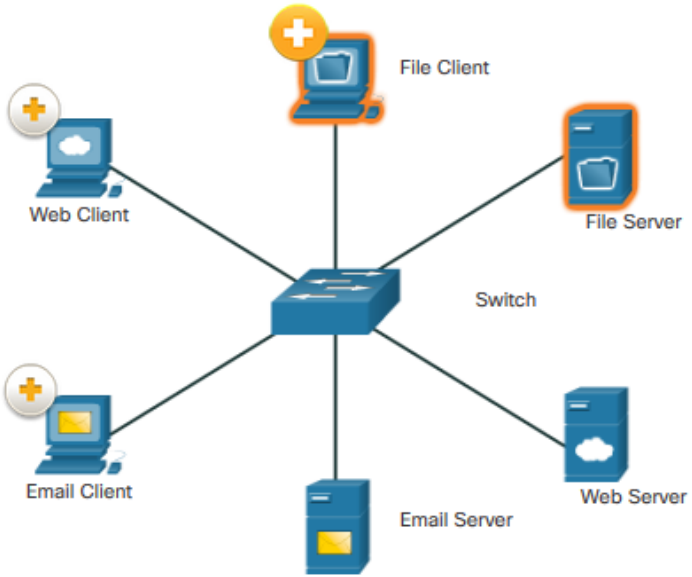
4.1 Network Protocols

Views of the Network

- Views of the network
  - Small home network
  - SOHO (Small Office/Home Office)
  - Medium to large networks
  - World-wide networks

Client-Server Communications

- File Client and Server communications
  - Server stores corporate and user files.
  - Client devices access these files or services with client software.
- Web Client Server
  - Web Server runs web server software and client uses browser software.
- Email Client-Server communications
  - Email Server runs email server software.

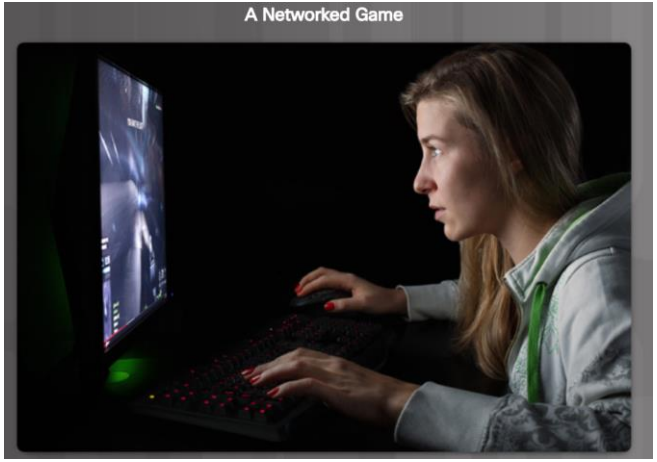


A Typical Session: Student

- A Typical Session: Student
  - Determine the origin of the traffic enter the network.
  - For example, Terry's data flows with the data of thousands of other users along a fiber-optic network that connects Terry's ISP with the several other ISPs, including the ISP that is used by the search engine company. Eventually, Terry's search string enters the search engine company's website and is processed by its powerful servers. The results are then encoded and addressed to Terry's school and her device.

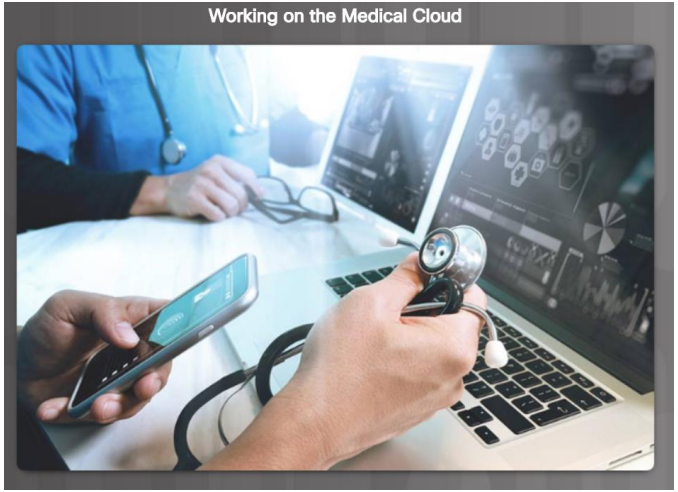
A Typical Session: Gamer

- A Typical Session: Gamer
  - Determine the origin of the traffic enter the network.
  - Michelle's network, like many home networks, connects to an ISP using a router and modem. These devices allow Michelle's home network to connect to a cable TV network that belongs to Michelle's ISP. The cable wires for Michelle's neighborhood all connect to a central point on a telephone pole and then connect to a fiber-optic network. This fiber-optic network connects many neighborhoods that are served by Michelle's ISP.



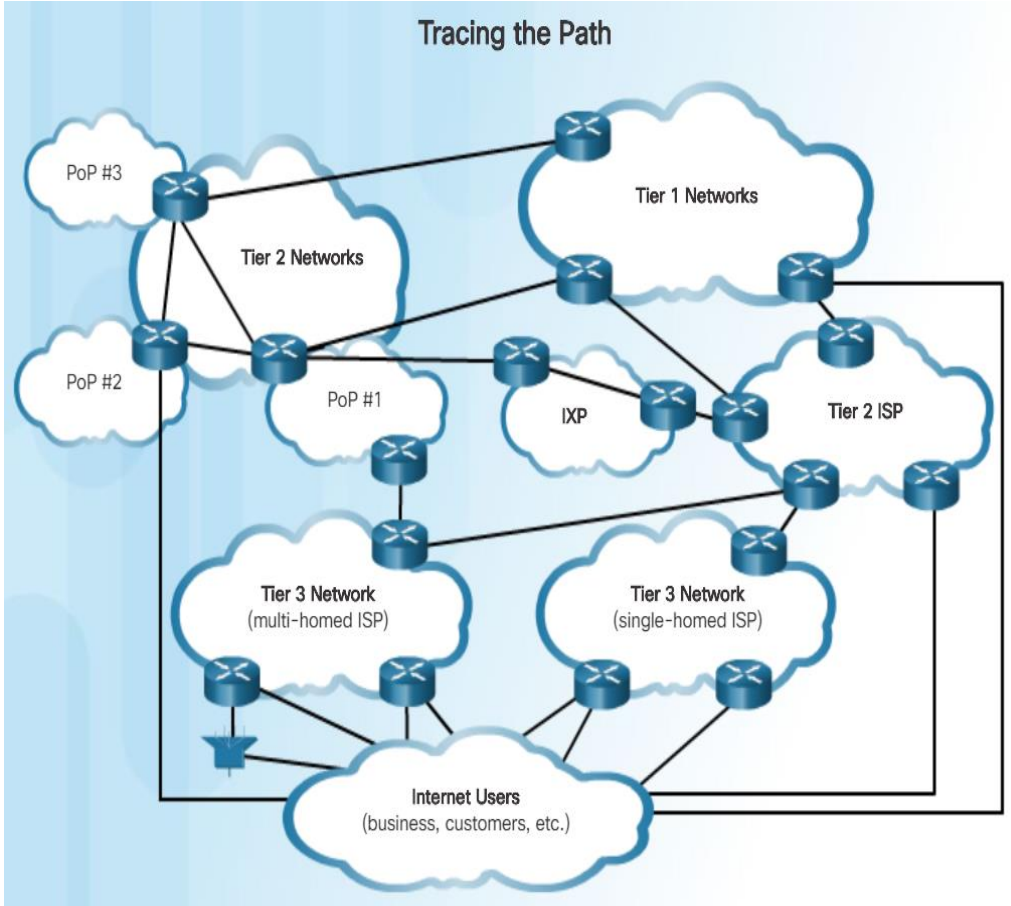
A Typical Session: Surgeon

- A Typical Session: Surgeon
  - Determine the origin of the traffic enter the network
  - Dr. Ismael Awad is an oncologist who performs surgery on cancer patients. He frequently needs to consult with radiologists and other specialists on patient cases. The hospital that Dr. Awad works for subscribes to a special service called a cloud. The cloud allows medical data, including patient x-rays and MRIs to be stored in a central location that is accessed over the Internet.



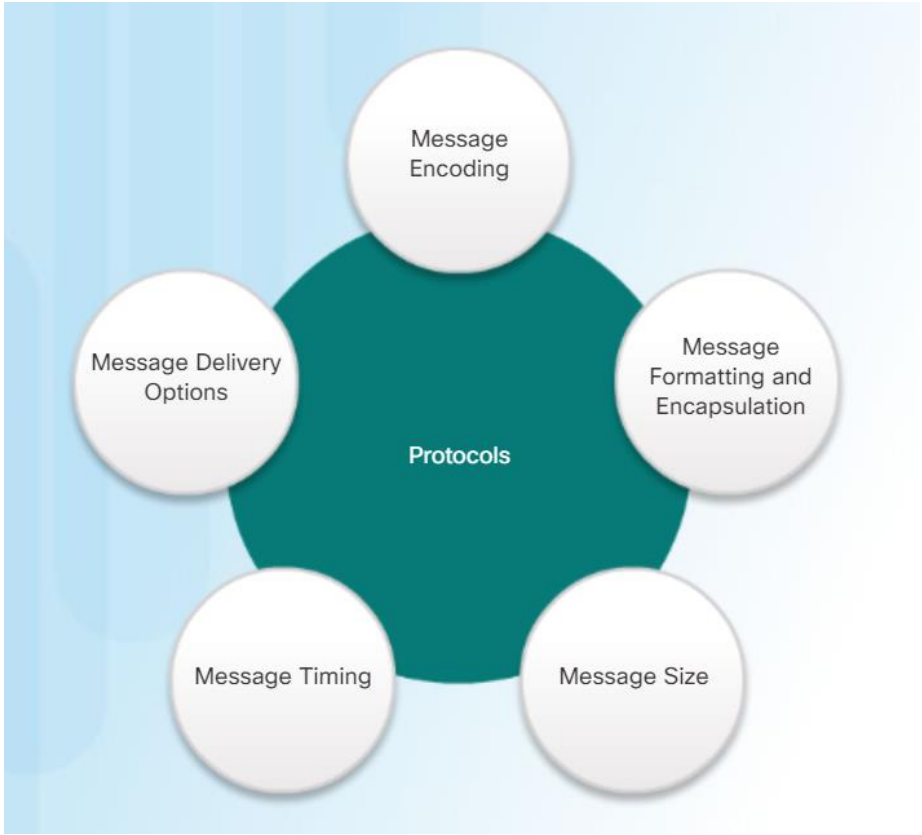
Tracing the Path

- Cybersecurity analysts must be able to determine the origin of traffic that enters the network, and the destination of traffic that leaves it. Understanding the path that network traffic takes is essential to this.
- Tier 1 Network and Tier 2 networks usually connect through an Internet Exchange Point (IXP).
- Larger networks connect to Tier 2 networks, usually through a Point of Presence (POP).
- Tier 3 ISPs connect homes and businesses to the Internet.



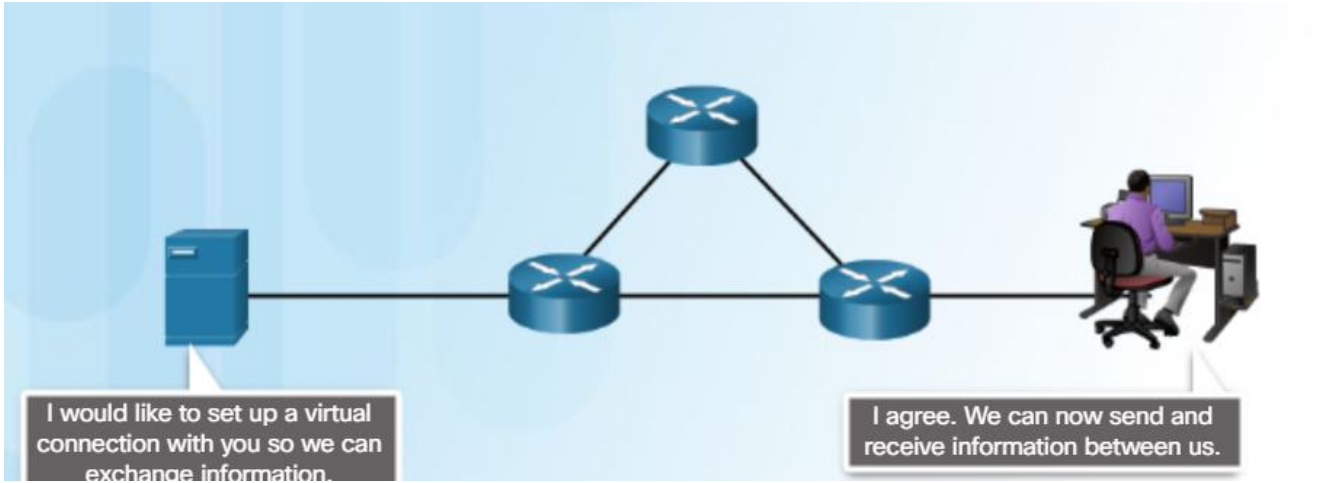
What are Protocols?

- Protocol – The rules of communications
  - Network protocols provide the means for computers to communicate on networks.
  - Network protocols dictate the message encoding, formatting, encapsulation, size, timing, and delivery options.



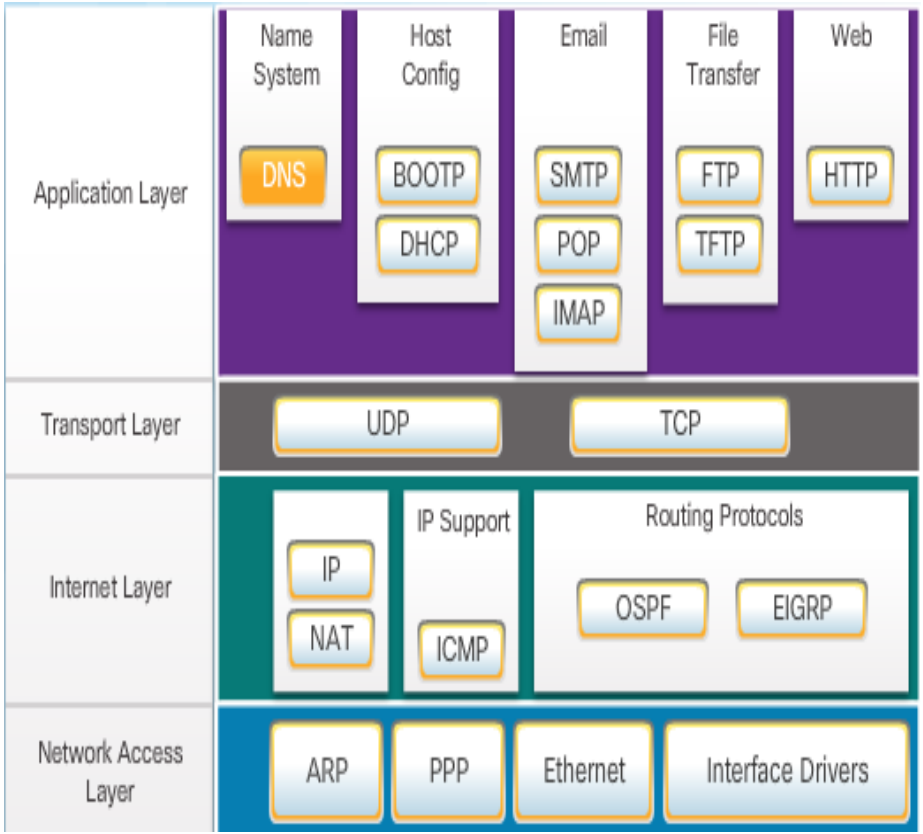
Network Protocol Suites

- Describe precise requirements and interactions.
- Define a common format and set of rules for exchanging messages between devices.
- Some common networking protocols are Hypertext Transfer Protocol (HTTP), Transmission Control Protocol (TCP), and Internet Protocol (IP).



TCP/IP Protocol Suite

- TCP/IP has standardized the way the computers communicate.
- 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.



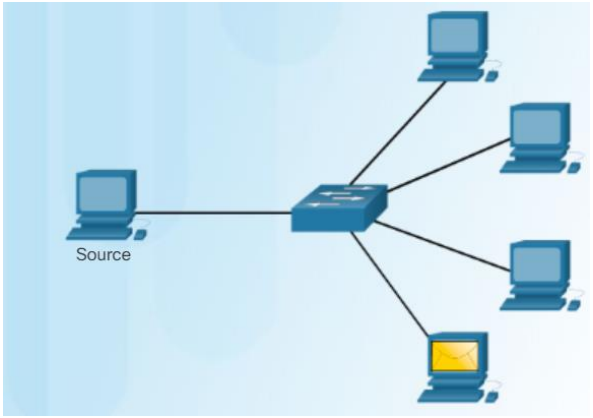
Format, Size, and Timing

- **Format**
  - **Encapsulation** - process of placing one message format inside another message format.
  - **Decapsulation** - the reverse process of encapsulation.
- **Size** – Message is broken up into many frames when sent, and reconstructed into the original message when received.
- **Timing** – includes the access method, flow control, and response timeout.

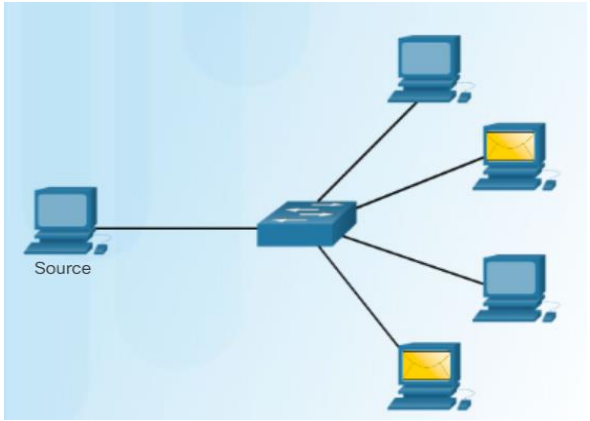
The email message and attachment are broken up into many frames and then sent on the network.

Unicast, Multicast, and Broadcast

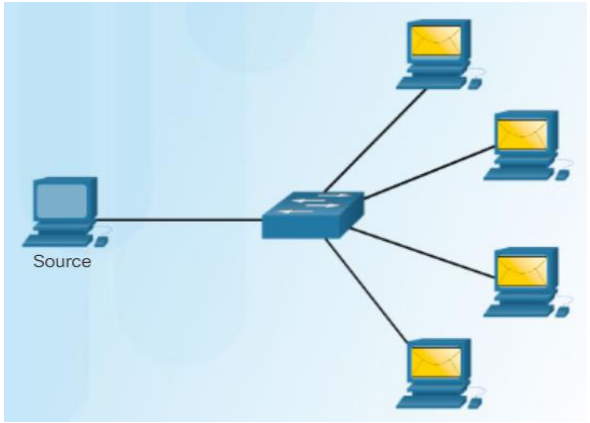
Unicast – one-to-one



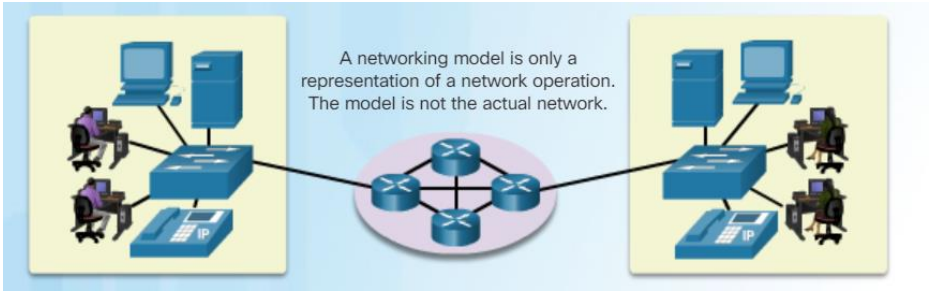
Multicast – one-to-many



Broadcast – one-to-all



Reference Models

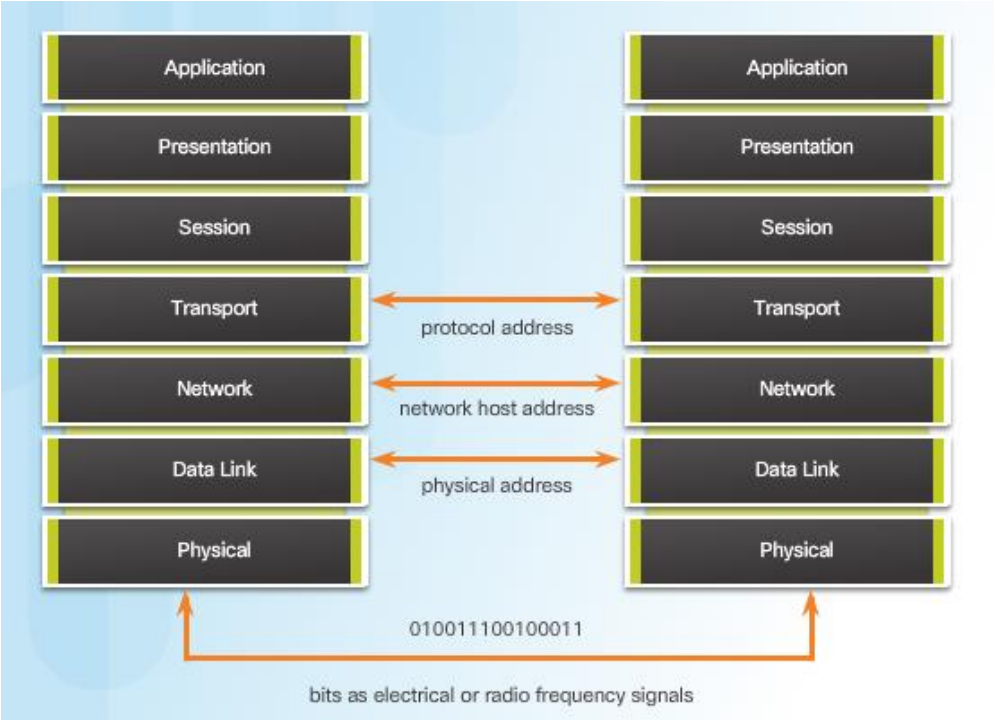


OSI Model		TCP/IP Protocol Suite	TCP/IP Model
7	Application	HTTP, DNS, DHCP, FTP	Application
6	Presentation		
5	Session		
4	Transport	TCP, UDP	Transport
3	Network	IPv4, IPv6, ICMPv4, ICMPv6	Internet
2	Data Link	PPP, Frame Relay, Ethernet	Network Access
1	Physical		

Three Addresses

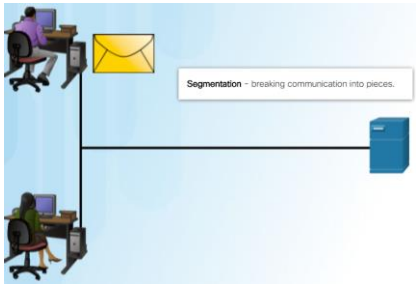
- Three important addresses:
  - Protocol address
  - Network host address
  - Physical address

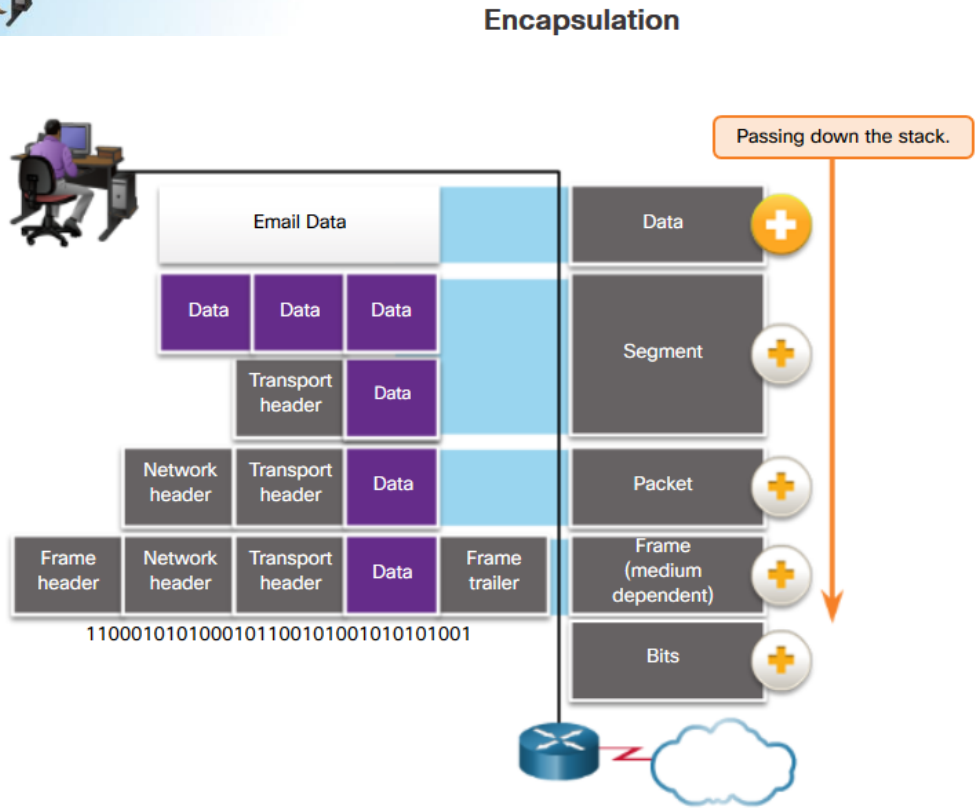
Addressing is used by the client to send requests and other data to a server. The server uses the client's address to return the requested data to the client that requested it.



Encapsulation

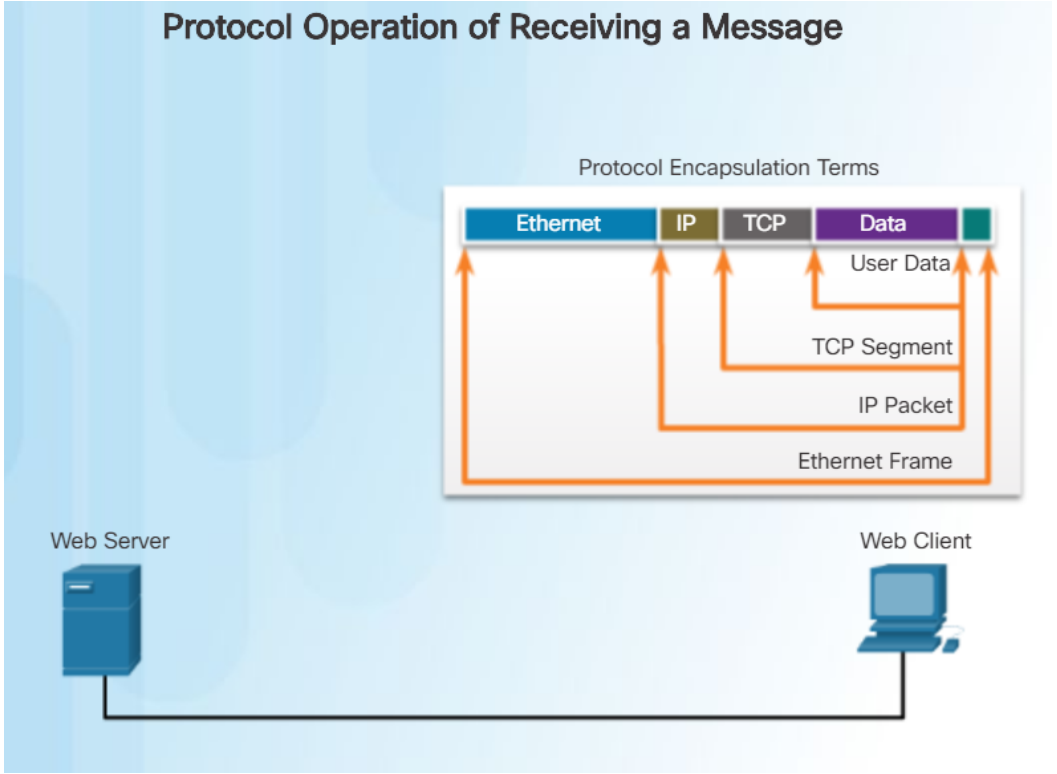
- This division of data into smaller pieces is called segmentation. Segmenting messages has two primary benefits:
  - **Segmentation**
  - **Multiplexing**
- The application data is encapsulated with various protocol information as it is passed down the protocol stack.
- The form that an encapsulated piece of data takes at any layer is called a protocol data unit (PDU).





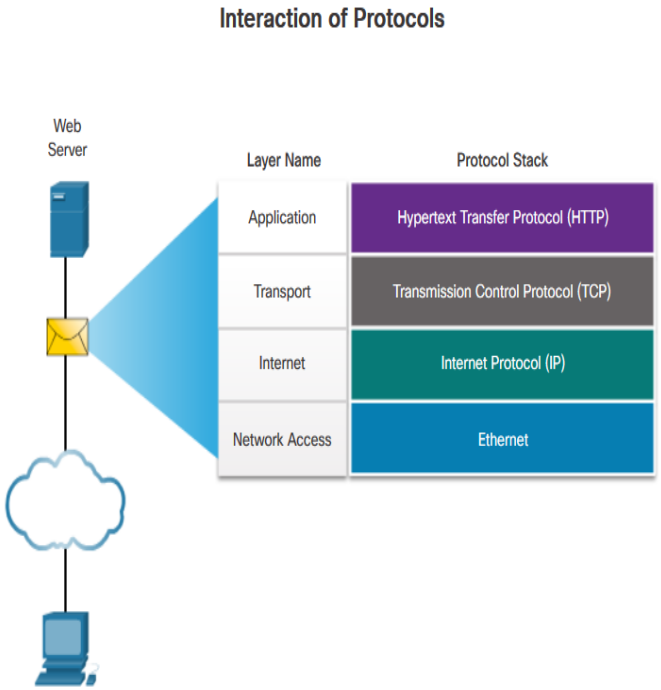
Encapsulation (Cont.)

- This process is reversed at the receiving host, and is known as de-encapsulation. The data is de-encapsulated as it moves up the stack toward the end-user application.



Scenario: Sending and Receiving a Web Page

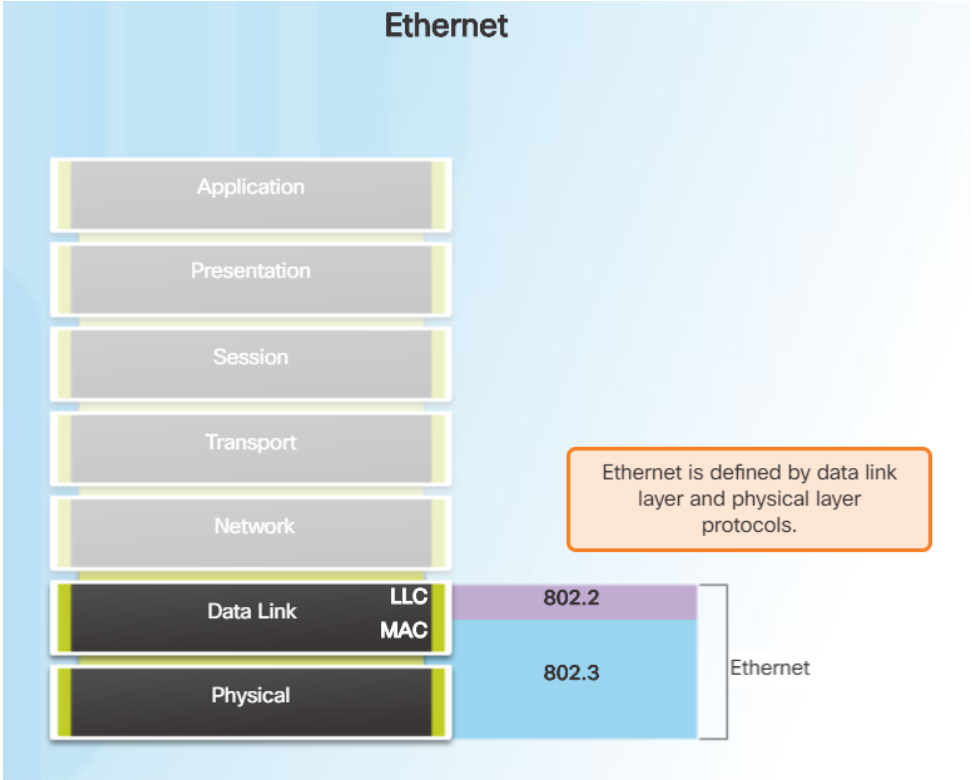
- **HTTP** – This application protocol governs the way a web server and a web client interact.
- **TCP** – This transport protocol manages individual conversations. TCP divides the HTTP messages into smaller pieces, called segments. TCP is also responsible for controlling the size and rate at which messages 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.



4.2 Ethernet and Internet Protocol (IP)

The Ethernet Protocol

- Operates at Layer 1 and 2
  - Defined by the IEEE 802.2 and 802.3 standards
  - Ethernet Sublayers
    - Logical Link Layer (LLC)
    - Media Access Control Layer (MAC)
- Ethernet responsibilities
  - Data encapsulation
  - Media access control

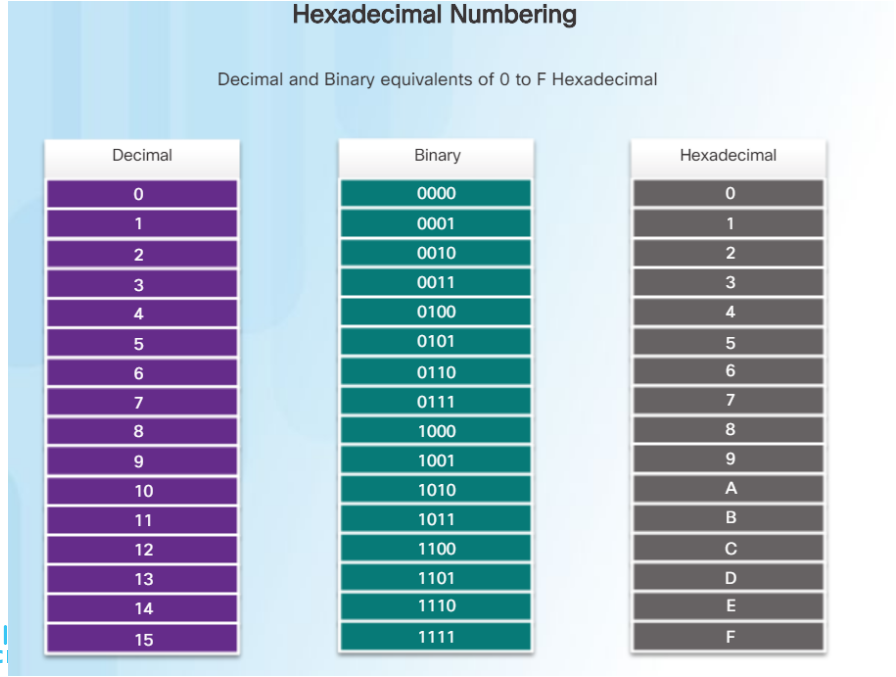


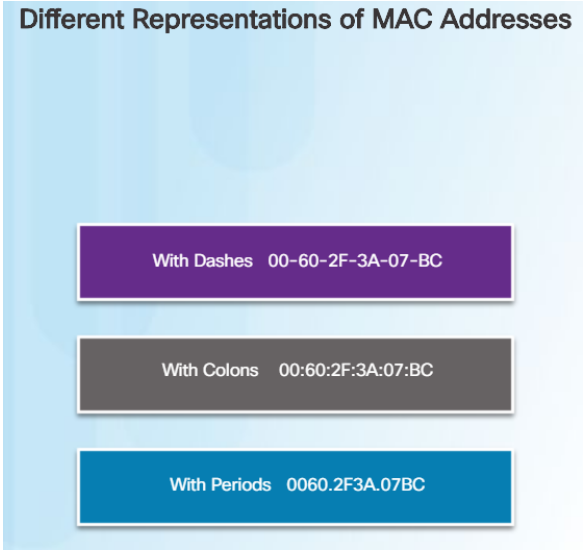
The Ethernet Frame

- Minimum Ethernet frame size 64 bytes
- Maximum Ethernet frame size 1518 bytes
- Two key identifiers
  - Destination MAC address
  - Source MAC address
- Uses hexadecimal

MAC Address Format

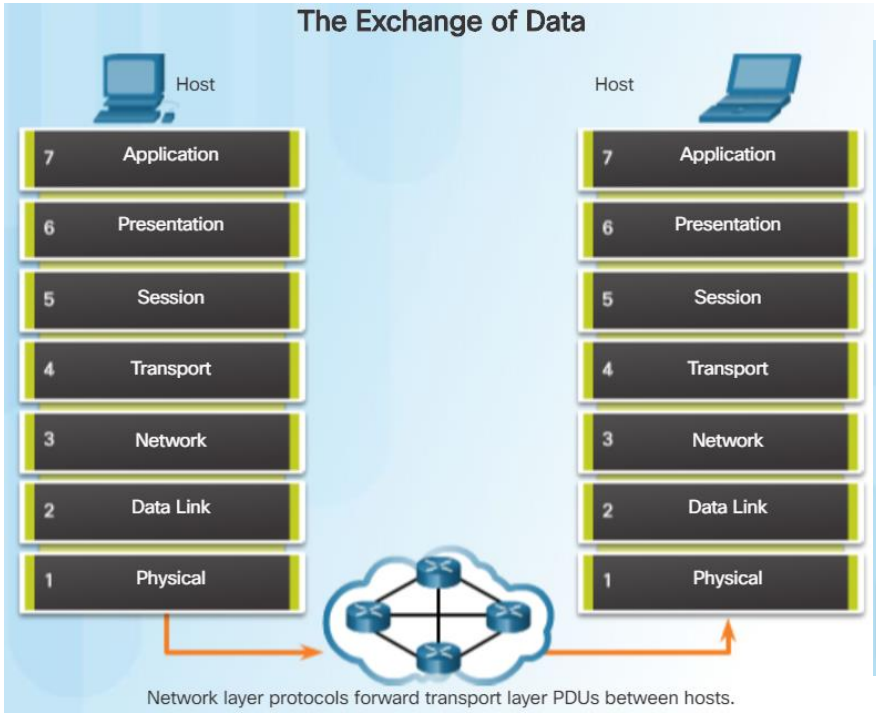
- Ethernet MAC address is 48-bit binary expressed as 12 hexadecimal digits.
  - Uses numbers 0 to 9 and letters A to F.
  - All data that travels on the network is encapsulated in Ethernet frames.

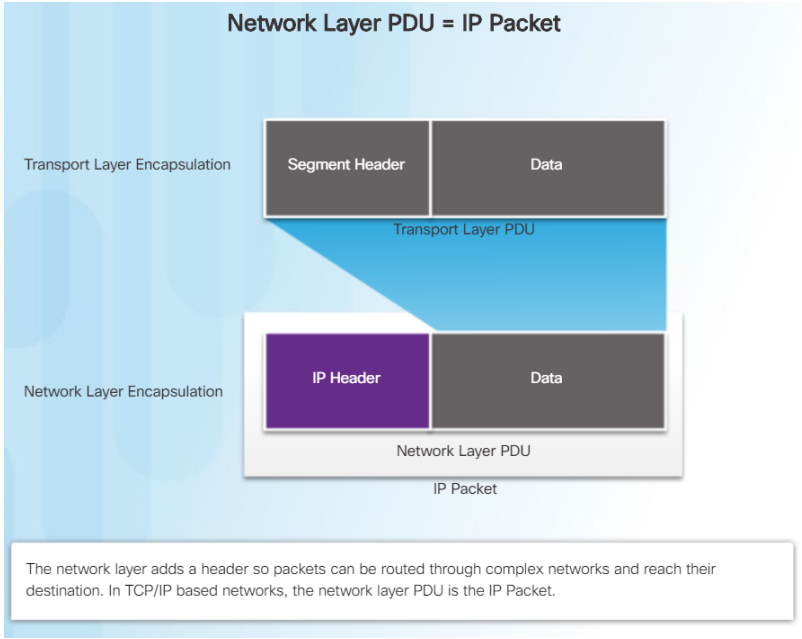




IPv4 Encapsulation

- IP encapsulates the transport layer segment by adding an IP header.

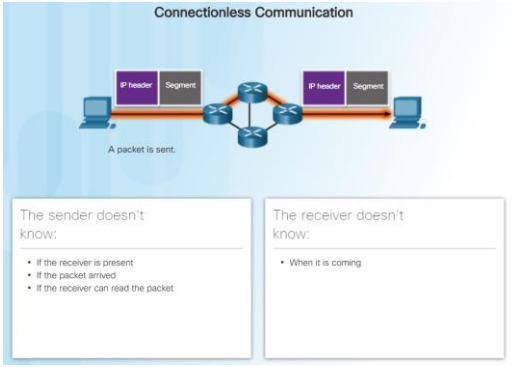


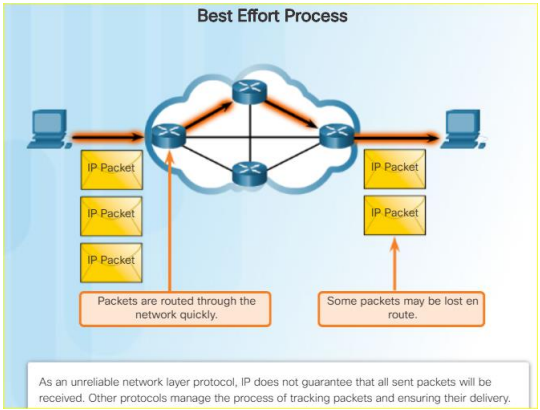


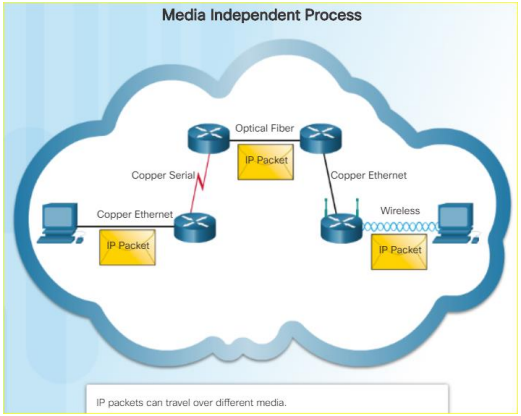
IPv4 Characteristics

IPv4 Characteristics

- **Connectionless** – no dedicated end-to-end connection is created before data is sent.
- **Unreliable (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 that carry the data at lower layers of the protocol stack.

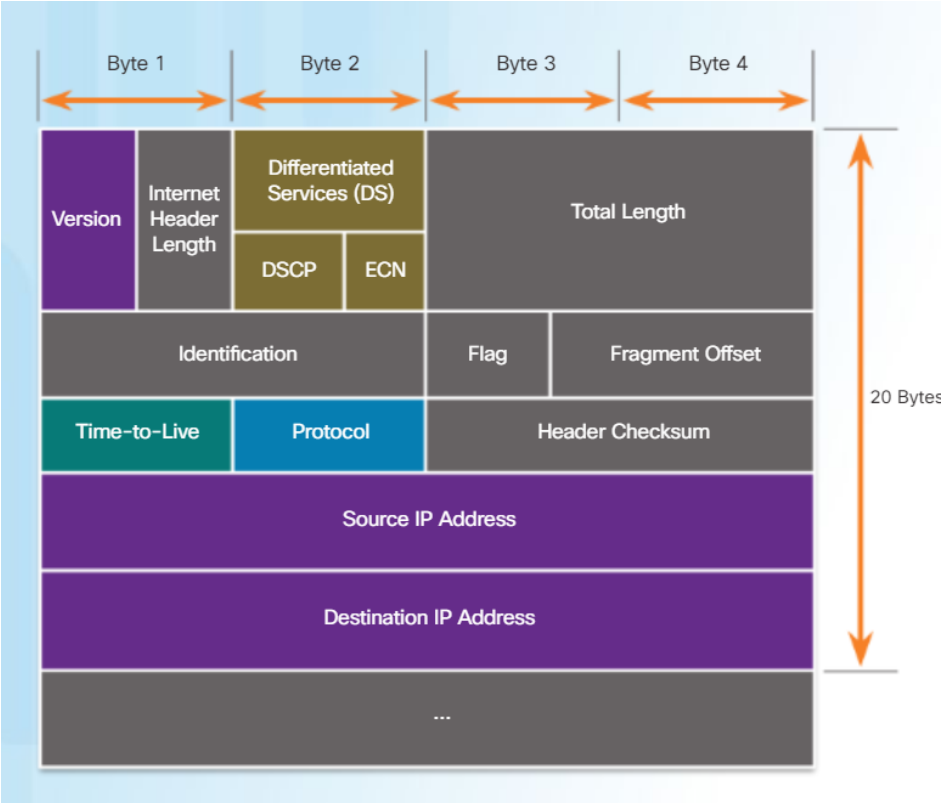






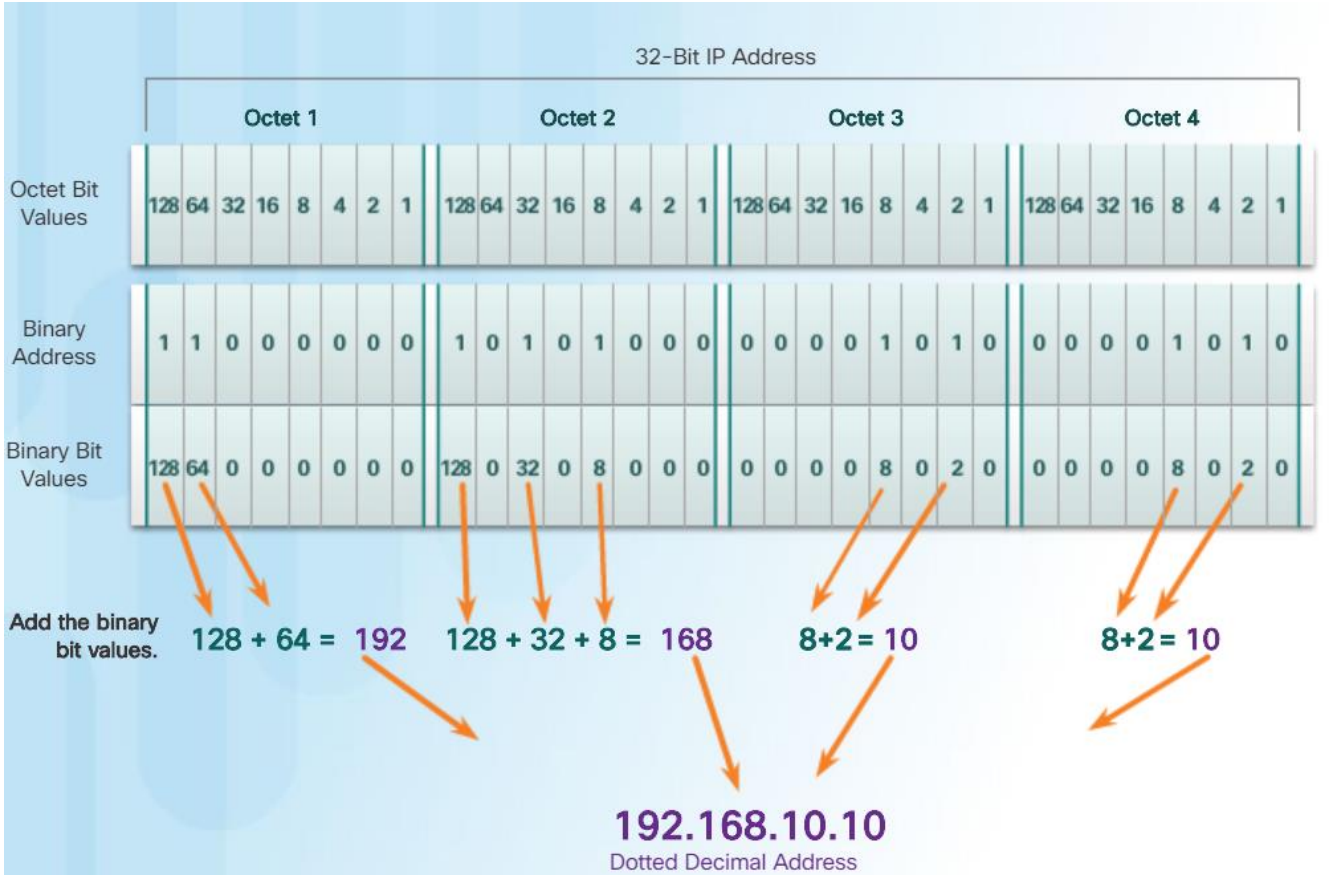
IPv4 Packet

- Packet header consists of fields containing important information about the packet.
- Fields contain binary numbers examined by the Layer 3 process.
- The binary values of each field identify various settings of the IP packet.
- Two most commonly referenced fields are the source and destination IP addresses.



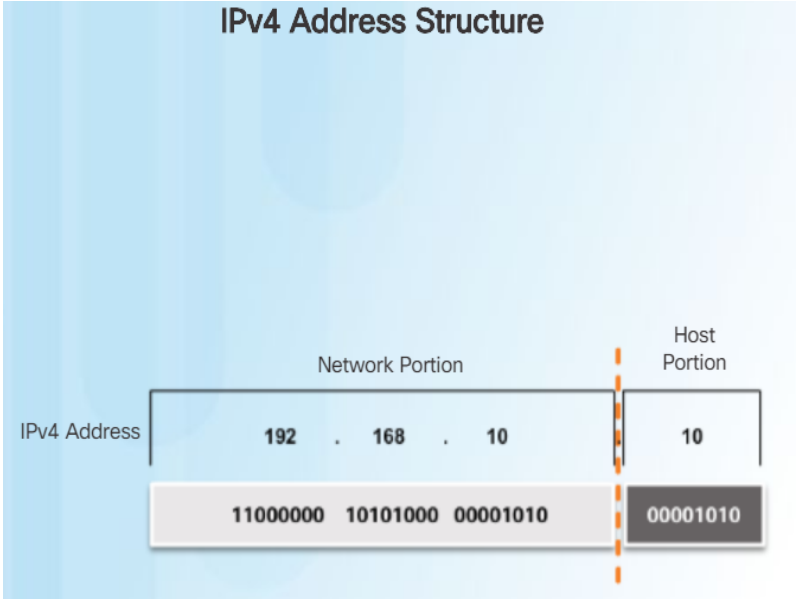
IPv4 Address Notation

- IP address is a series of 32 binary bits (ones and zeros).
- When a host is configured with an IPv4 address, it is entered as a dotted decimal number such as 192.168.10.10.
- The equivalent address in binary is 11000000.10101000.00001010.00001010



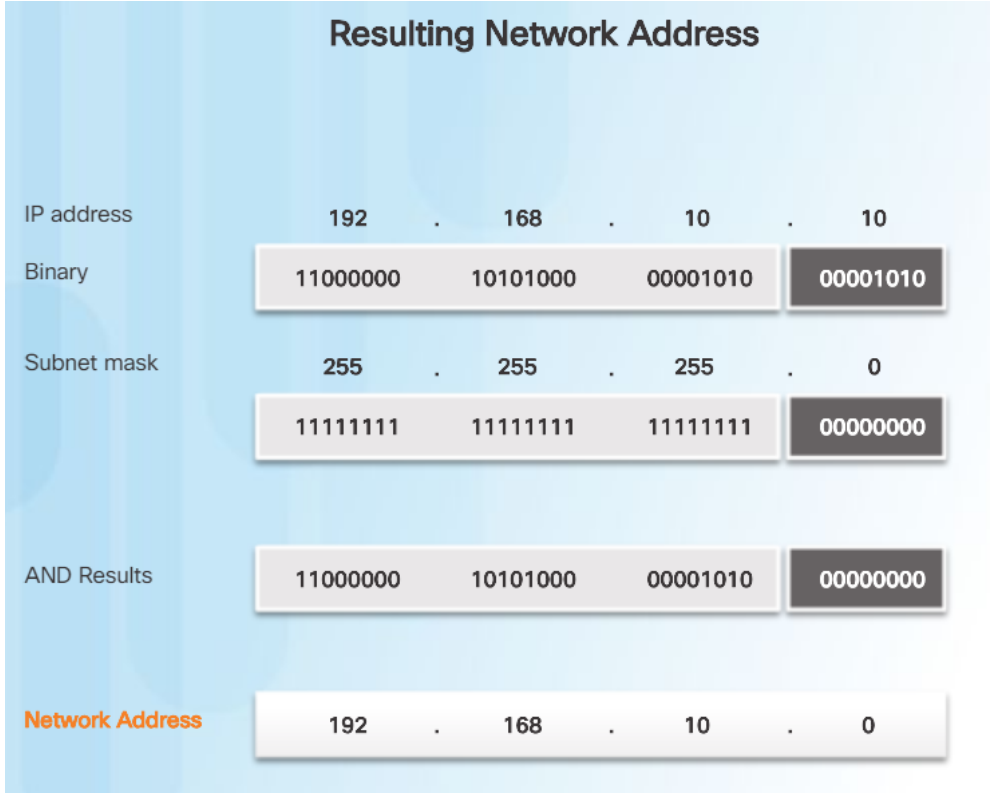
IPv4 Host Address Structure

- IPv4 address is a hierarchical address that is made up of a network portion and a host portion.
- 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.



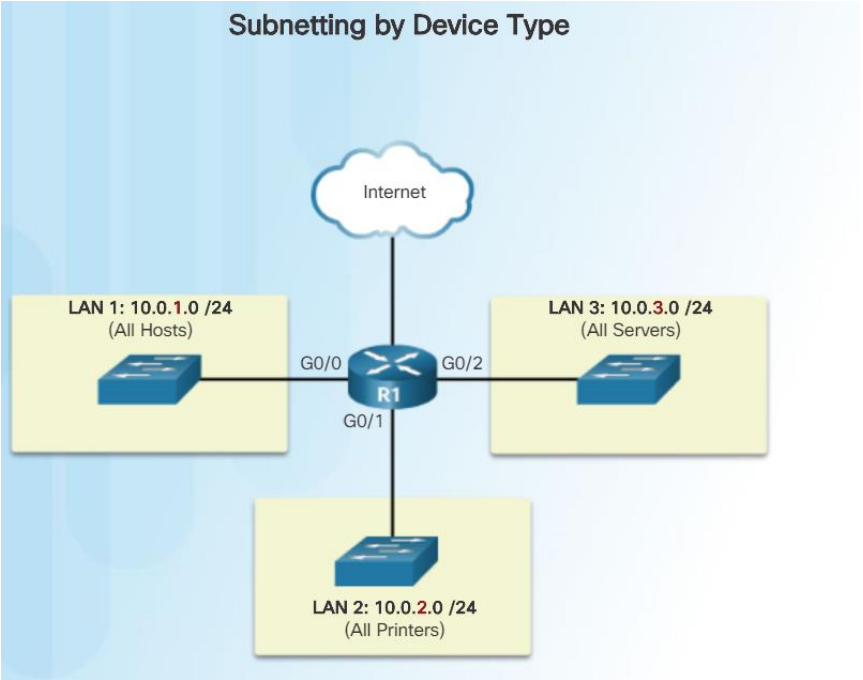
IPv4 Subnet Mask and Network Address

- Subnetting takes a network space and divides it into smaller spaces called subnets.
- Identifying network address of an IPv4host:
  - IP address is logically ANDed, bit by bit with subnet mask.
  - ANDing between the address and the subnet mask yields the network address.



Subnetting Broadcast Domains

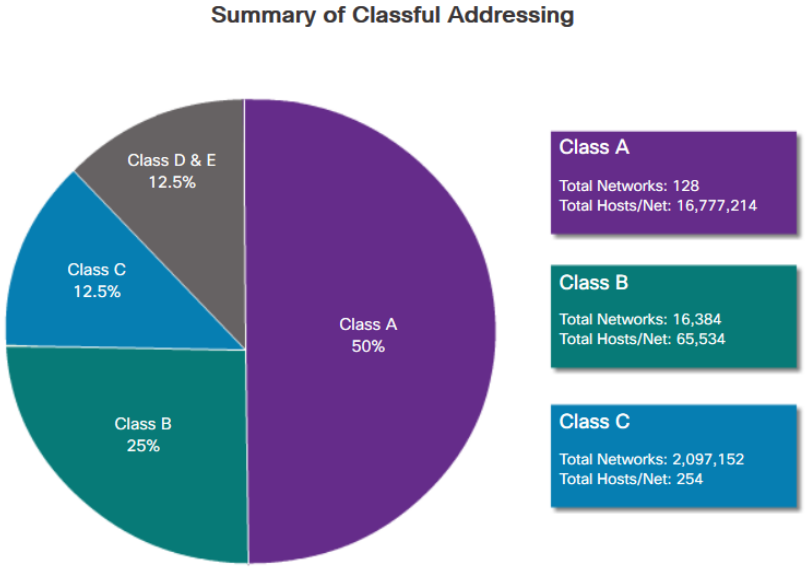
- Subnetting takes a network space and divides it into smaller spaces called subnets.
- Identifying network address of an IPv4 host:
  - IP address is logically ANDed, bit by bit with subnet mask.
  - ANDing between the address and the subnet mask yields the network address.



IPv4 Address Classes and Default Subnet Masks

Assigned Classes – A, B, C, D, and E

- **Class A** - Designed to support extremely large networks.
- **Class B** – Designed to support moderate to large networks.
- **Class C-** Designed to support small networks.
- **Class D -** Multicast block.
- **Class E -** Experimental address block.

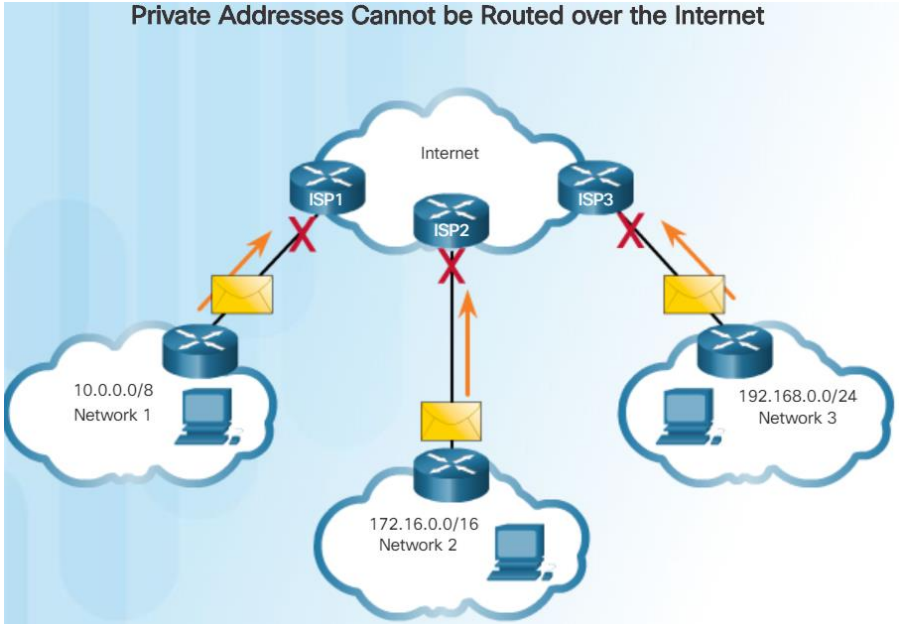


Private Internet Addresses are Defined in RFC 1918

Class	RFC 1918 Internal Address Range
A	10.0.0.0 - 10.255.255.255
B	172.16.0.0 - 172.31.255.255
C	192.168.0.0 - 192.168.255.255

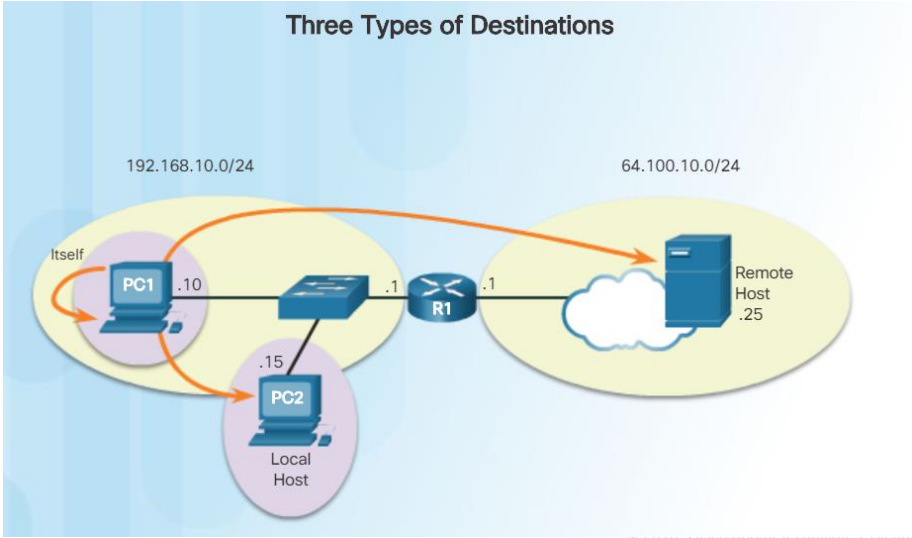
Reserved Private Addresses

- Blocks of addresses mostly used by organizations to assign IPv4 addresses to internal hosts.
- Not unique to any network.
- Not allowed on Internet and are filtered by internal router.
- Router usually connects the internal network to the ISP network.



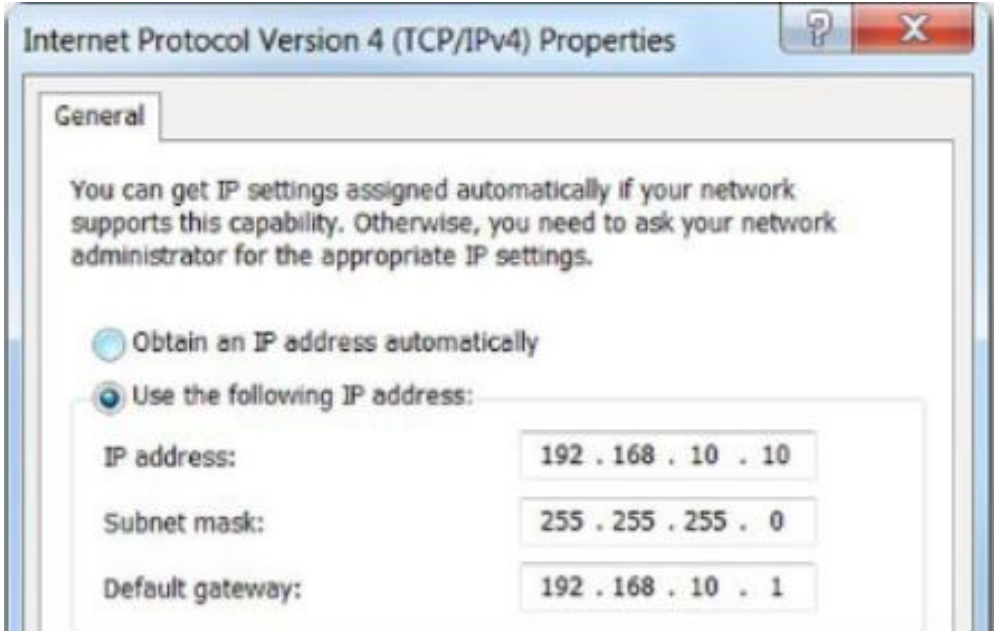
Host Forwarding Decision

- A host can send a packet to three types of destinations:
  - **Itself** - A host can ping itself by sending a packet to a special IPv4 address of 127.0.0.1. Pinging the loopback interface tests the TCP/IP protocol stack.
  - **Local host** - This is a host on the same local network.
  - **Remote host** - This is a host on a remote network. The hosts do not share the same network address.



Default Gateway

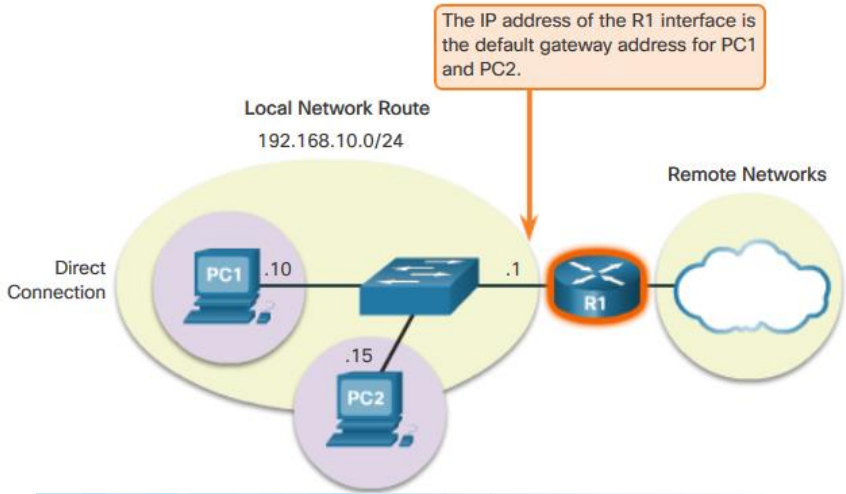
- Three dotted decimal IPv4 addresses must be configured when assigning an IPv4 configuration to host:
  - **IPv4 address** – Unique IPv4 address of the host.
  - **Subnet mask** - Used to identify the network/host portion of the IPv4 address.
  - **Default gateway** – Identifies the local gateway (i.e. local router interface IPv4 address) to reach remote networks.
- The default gateway is the network device that can route traffic to other networks. It is the router that can route traffic out of the local network.



Using the Default Gateway

A host's routing table will typically include a default gateway.

- The host receives the IPv4 address of the default gateway.
- IP addressing information:
  - Configured manually.
  - Obtained automatically/dynamically using Dynamic Host Configuration Protocol (DHCP).
  - Placed in computer's routing table.

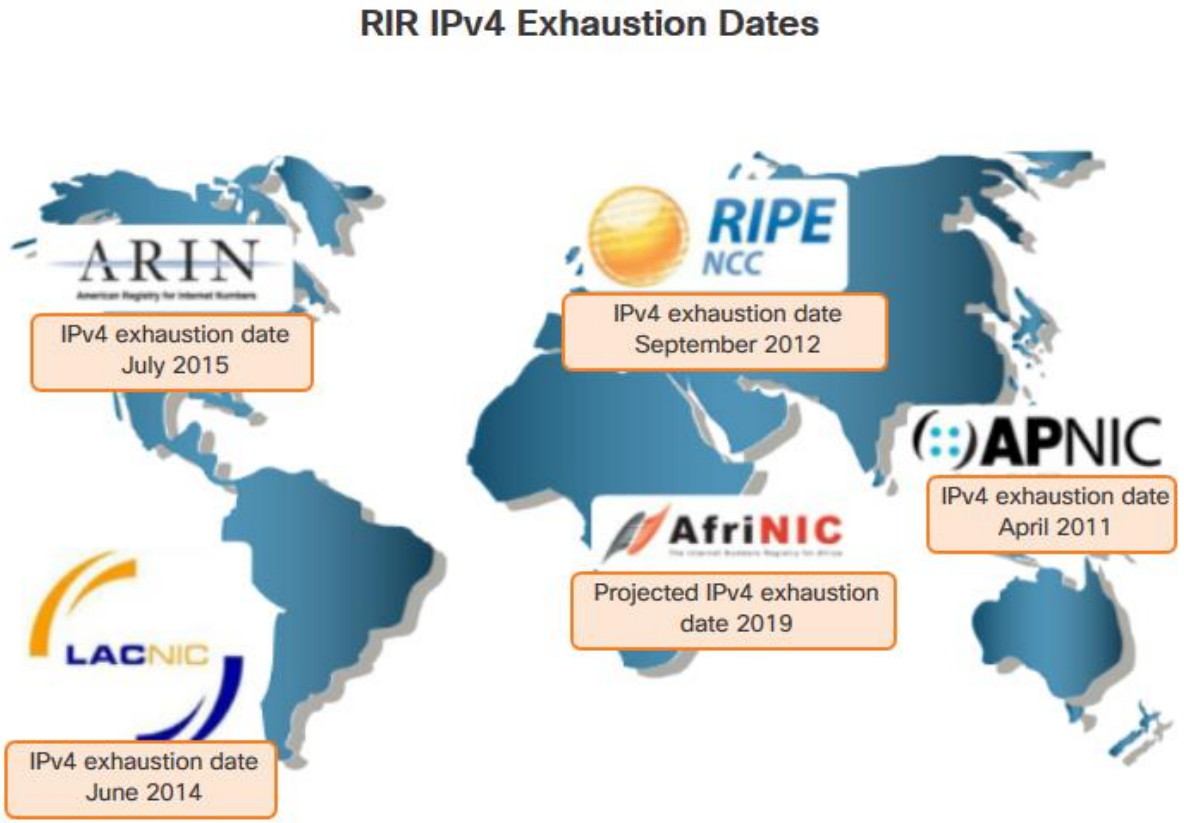


IPv4 Routing Table for PC1


```
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>
```

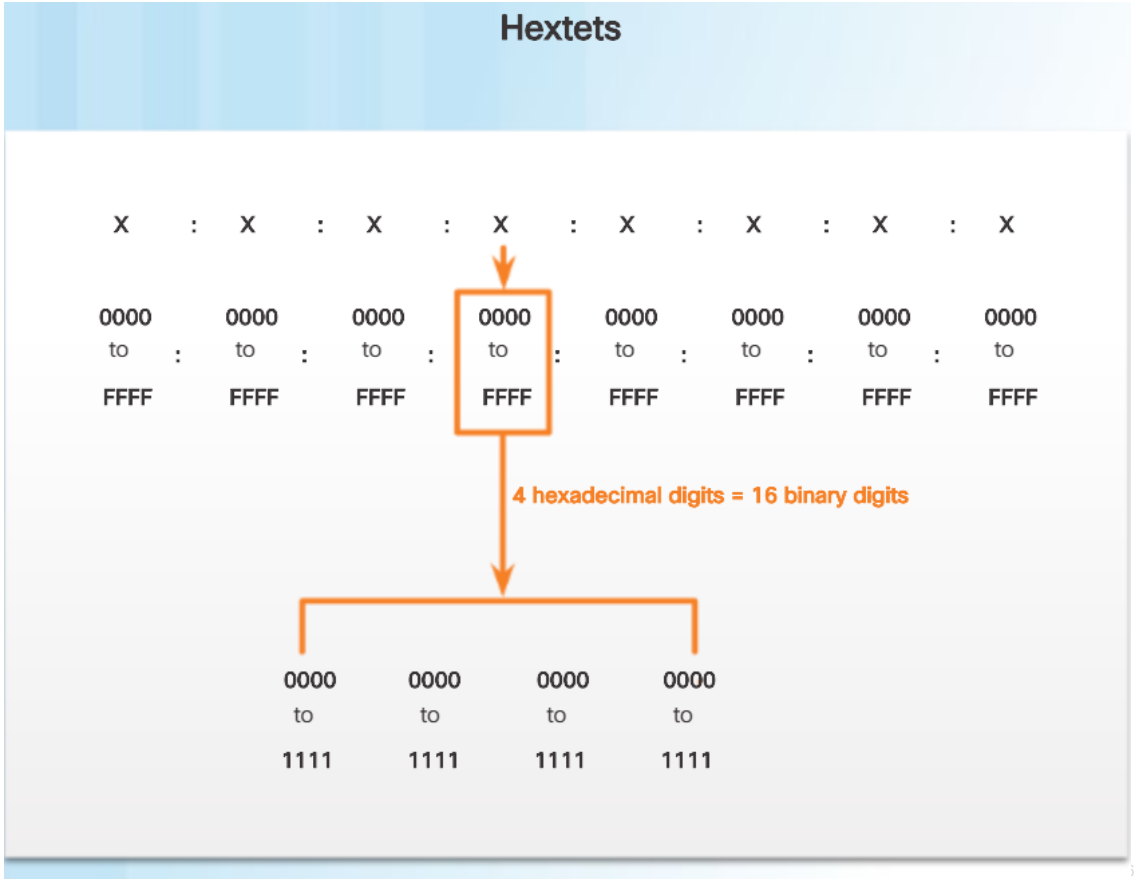
Need for IPv6

- The depletion of IPv4 address space has been the motivating factor for moving to IPv6.128-bit address space.
- Four out of the five Regional Internet Registries (RIRs) have run out of IPv4 addresses.



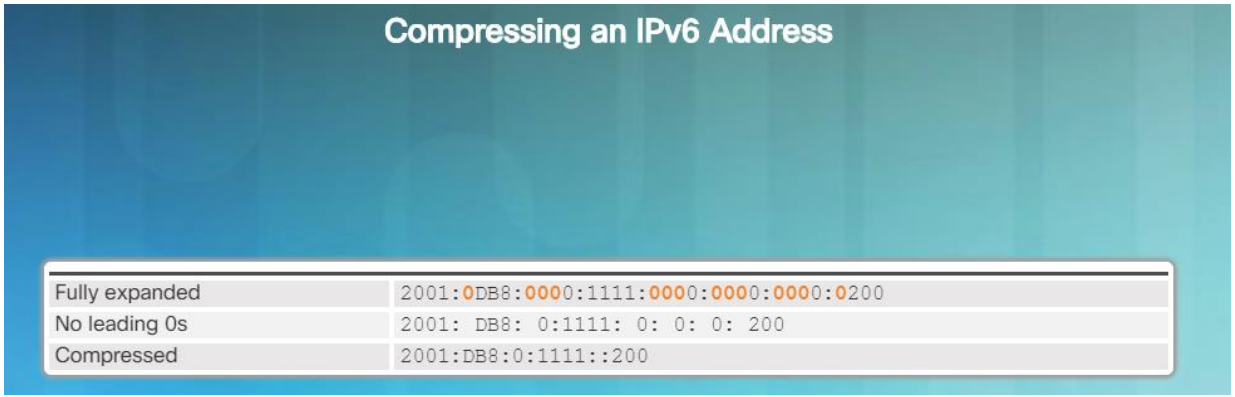
IPv6 Size and Representation

- 128-bit address space.
  - String of 32 hexadecimal values.
  - Every 4 bits represented by one hexadecimal digit.
  - Hextet is 16 bits or 4 hexadecimal digits.



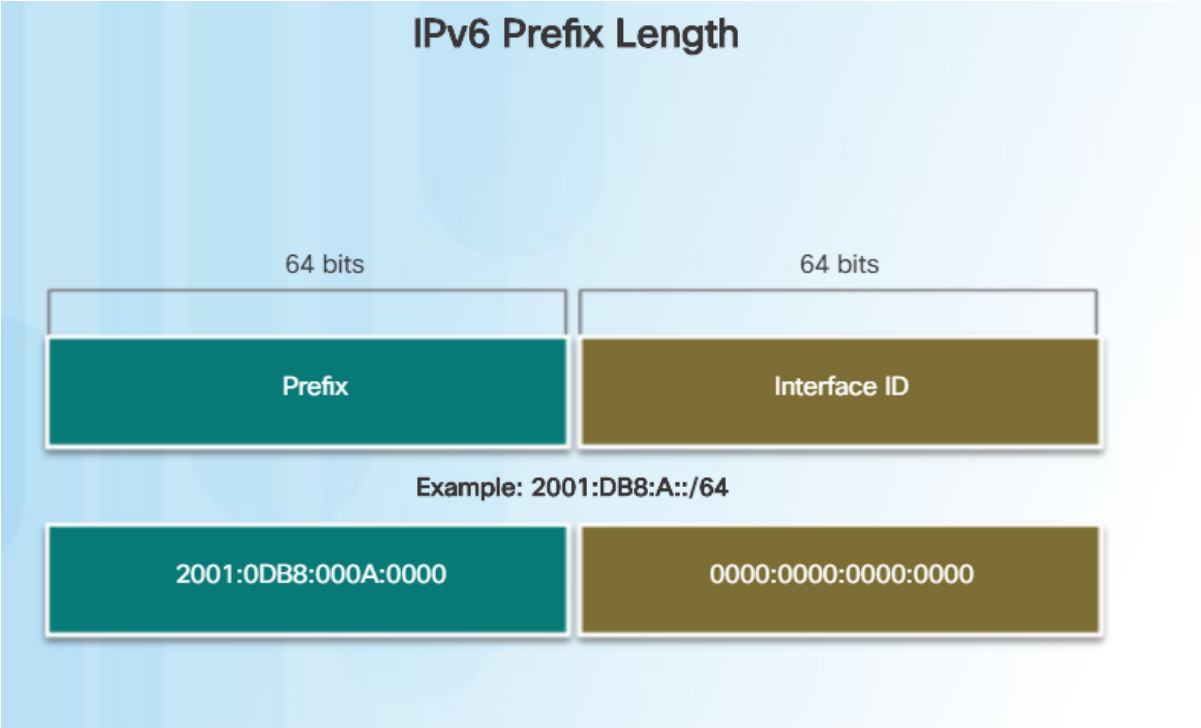
IPv6 Address Formatting

- IPv6 Addresses:
  - 128 bit address space.
  - Can remove leading zeros.
  - Can leave out 1 “all zeros” segment.
  - Two sections: Prefix and Interface ID.



IPv6 Prefix Length

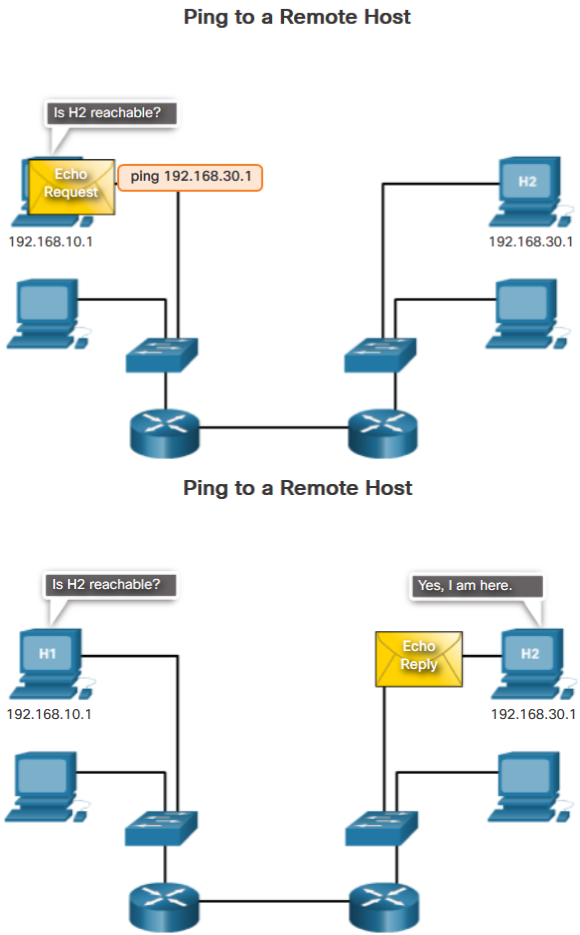
- IPv6 Prefix length does not use the dotted decimal subnet mask notation.
- The prefix length can range from 0 to 128.



4.3 Connectivity Verification

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

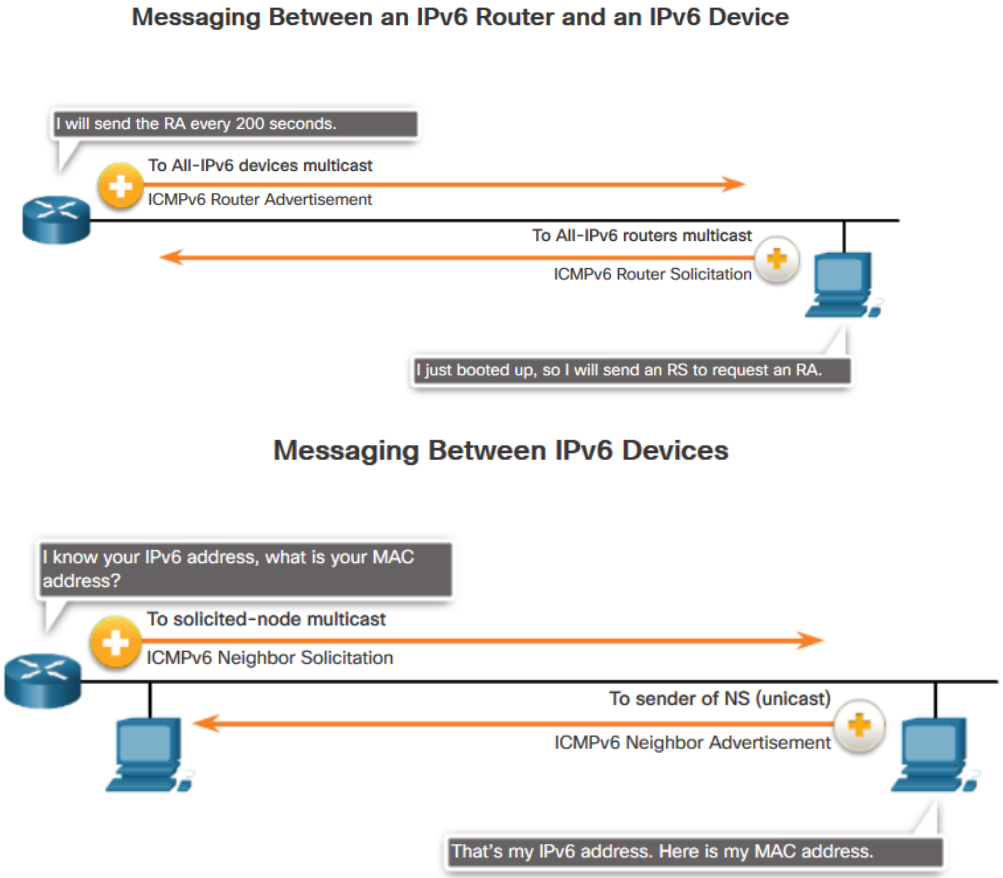
4 new protocols as part of the Neighbor Discovery Protocol (ND or NDP):

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:

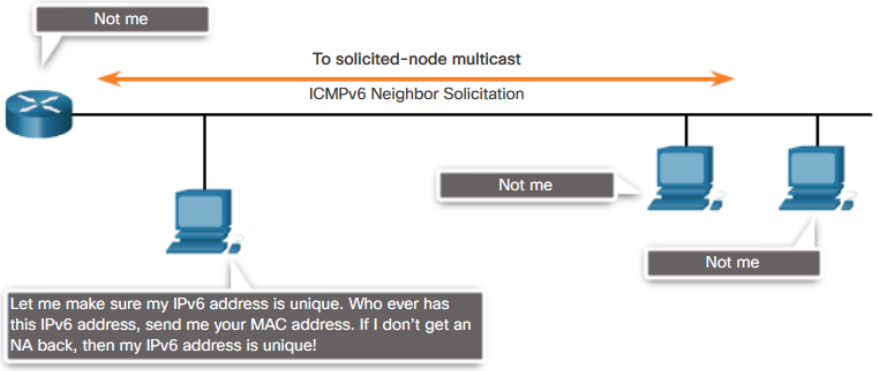
- **Neighbor Solicitation (NS) message**
- **Neighbor Advertisement (NA) message**



ICMPv6 and RA Messages (Cont.)

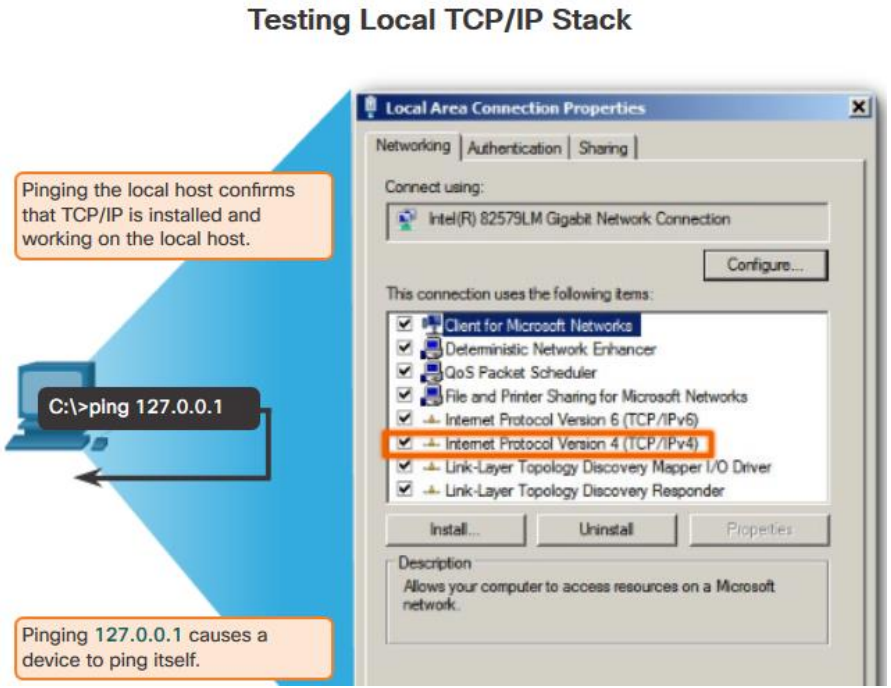
- IPv6 Duplicate Address Detection (DAD)
  - Not required, but recommended.
  - If another device on the network has the same global unicast or link-local unicast address, the device will respond with an NA message.

Duplicate Address Detection (DAD)



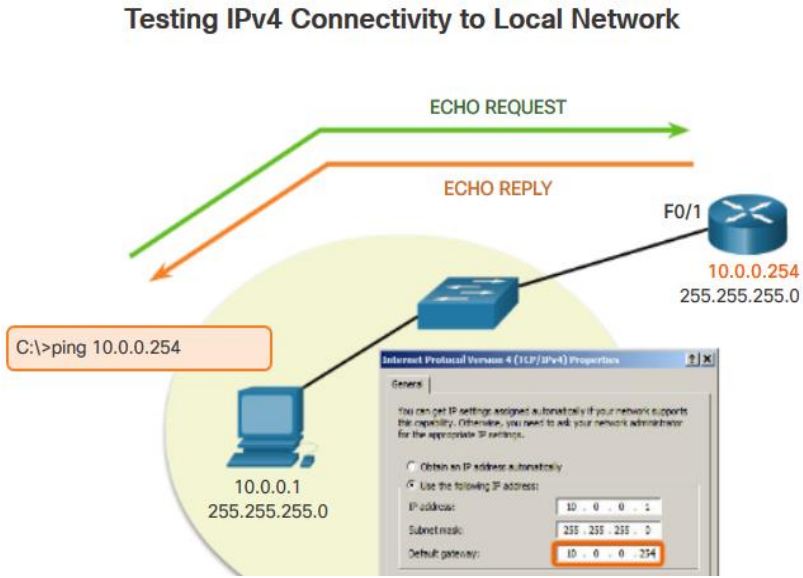
Ping – Testing and Local Stack

- Ping is a testing utility that uses ICMP echo request and echo reply messages to test connectivity between hosts.
- To test connectivity to another host on a network, an echo request is sent to the host address using the ping command.
- If the host at the specified address receives the echo request, it responds with an echo reply.



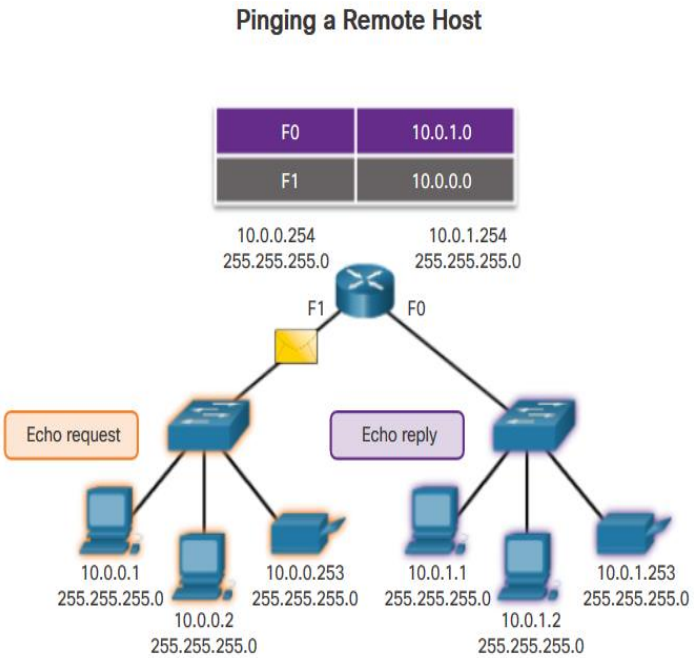
Ping – Testing Connectivity to Local LAN

- You can also use ping to test the ability of a host to communicate on the local network. This is generally done by pinging the IP address of the gateway of the host.
- A successful ping to the gateway indicates that the host and the router interface serving as the gateway are both operational on the local network.
- For this test, the gateway address is most often used because the router is normally always operational.



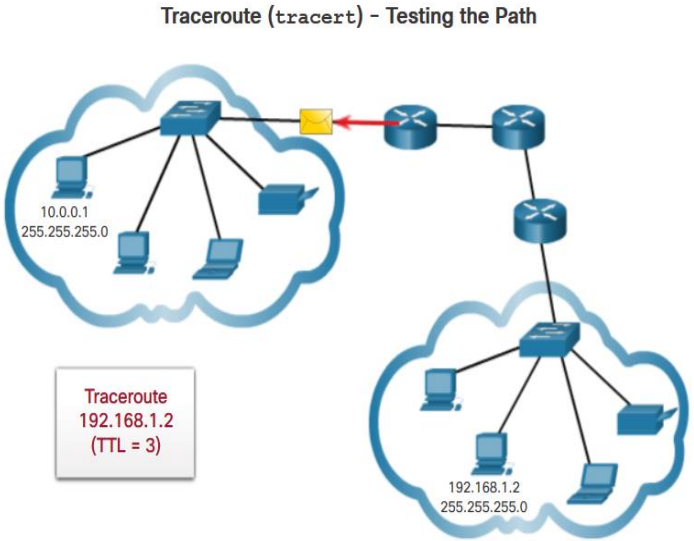
Ping – Testing Connectivity to Remote Host

- 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.



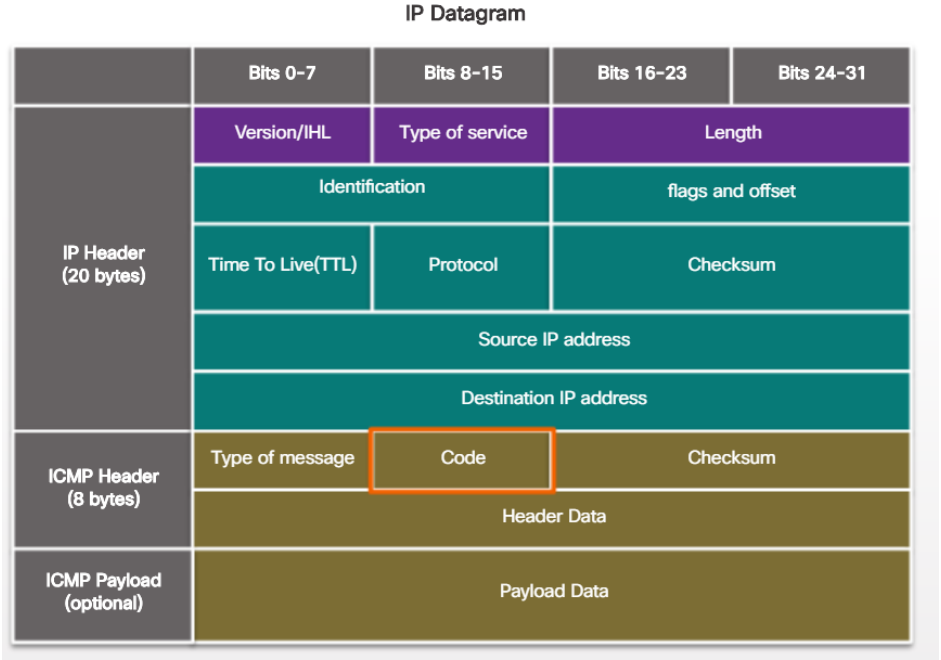
Traceroute- Testing the Path

- 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

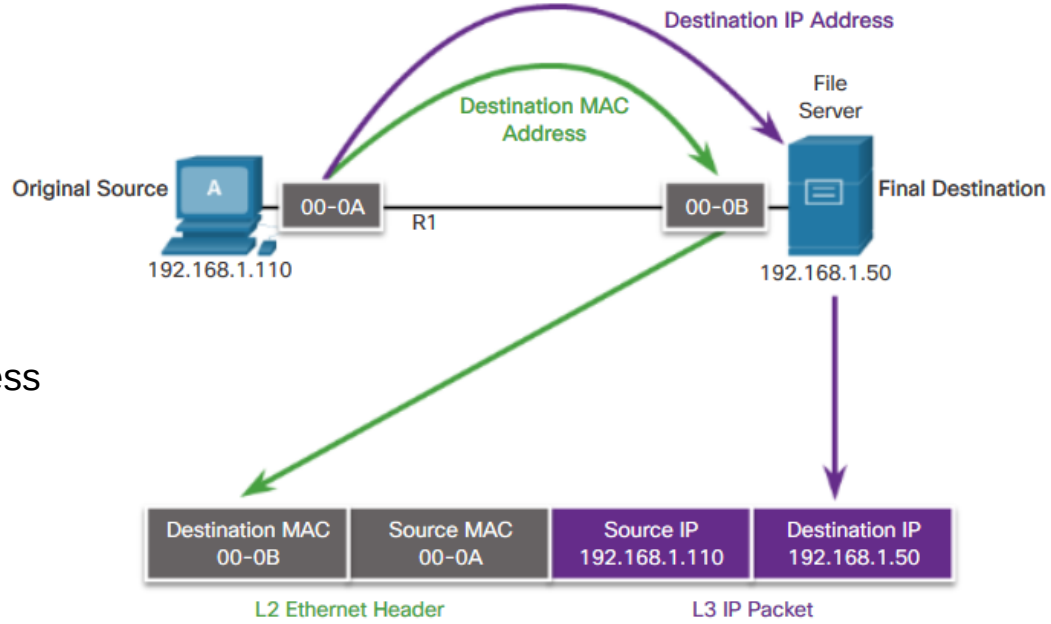
- ICPM is considered to be a Layer 3 protocol.
- ICMP acts as a data payload within the IP packet.
- It has a special header data field.
- These are some common message codes:
  - **0** – Echo reply (response to a ping)
  - **3** – Destination Unreachable
  - **5** – Redirect (use another route to your destination)
  - **8** – Echo request (for ping)
  - **11** – Time Exceeded (TTL became 0)



4.4 Address Resolution Protocol

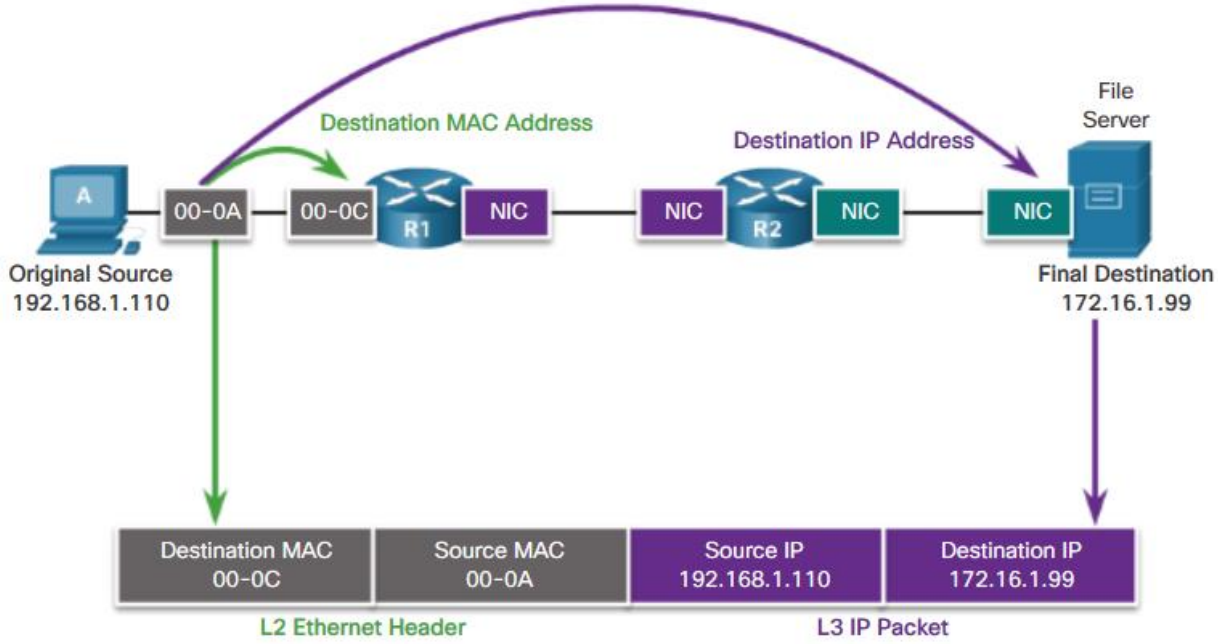
Destination on Same Network

- Two addresses assigned to an Ethernet device:
  - **MAC address** (Layer 2 physical address)
  - **IP address** (Layer 3 logical address)
- A device must have both addresses to communicate with another TCP/IP-based device:
  - Uses the source and destination MAC address
  - Uses the source and destination IP address



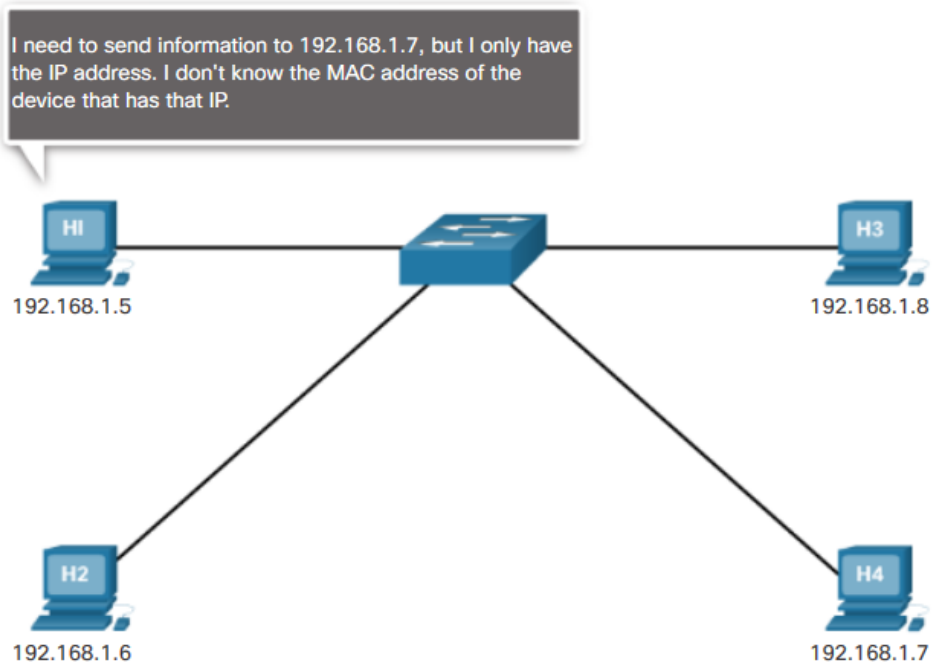
Destination on Remote Network

- When communicating with a device on a remote network, the destination MAC address is the MAC address of the Layer 3 device interface on the same network as the device originating the packet.



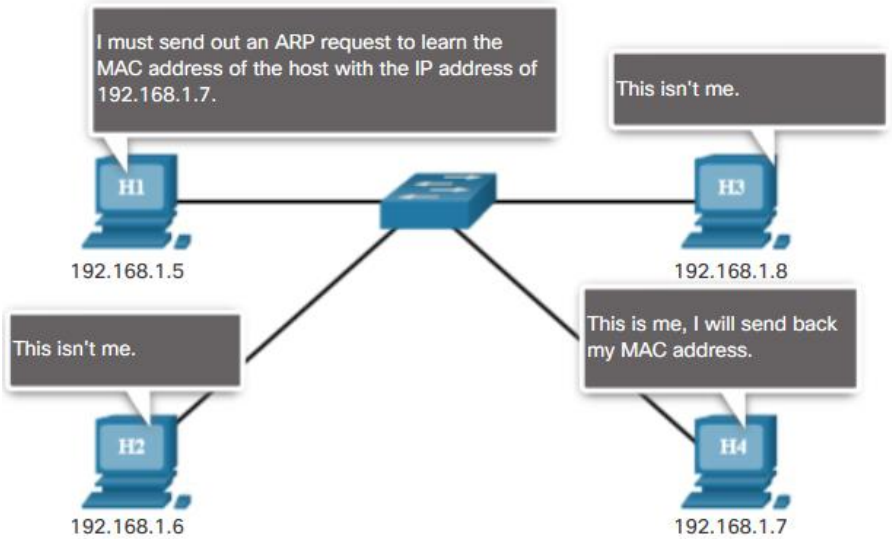
Introduction to ARP

- When a device sends an Ethernet frame, it contains these two addresses:
  - **Destination MAC address** - The MAC address of the Ethernet NIC, which will be either the MAC address of the final destination device or the router.
  - **Source MAC address** - The MAC address of the sender's Ethernet NIC.
- To determine the destination MAC address, the device uses ARP. ARP resolves IPv4 addresses to MAC addresses, and maintains a table of mappings.



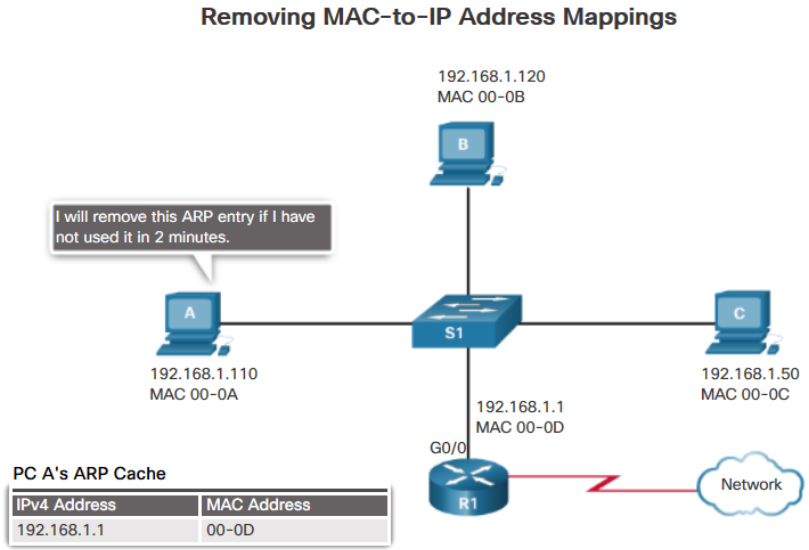
ARP Functions

- Used to resolve IPv4 addresses to MAC addresses.
- IPv4 and MAC address mappings kept in an ARP table.



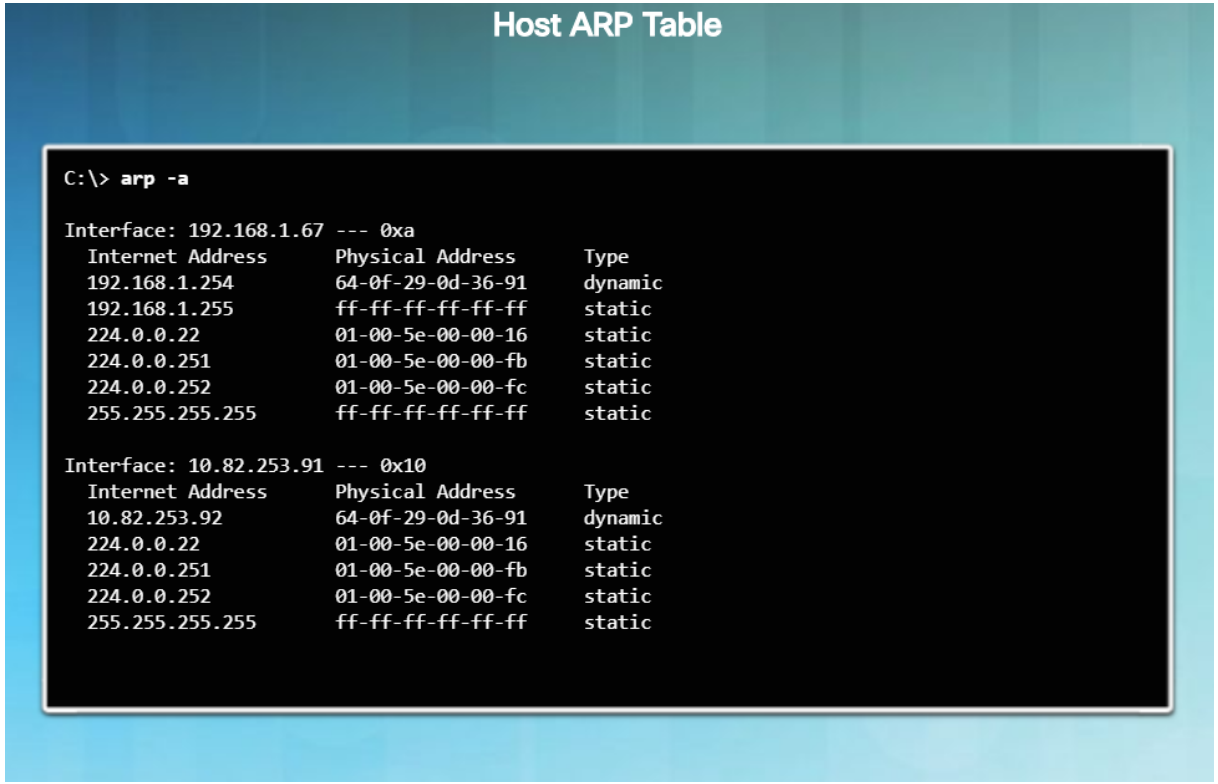
Removing Entries from an ARP Table

- 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 tables.



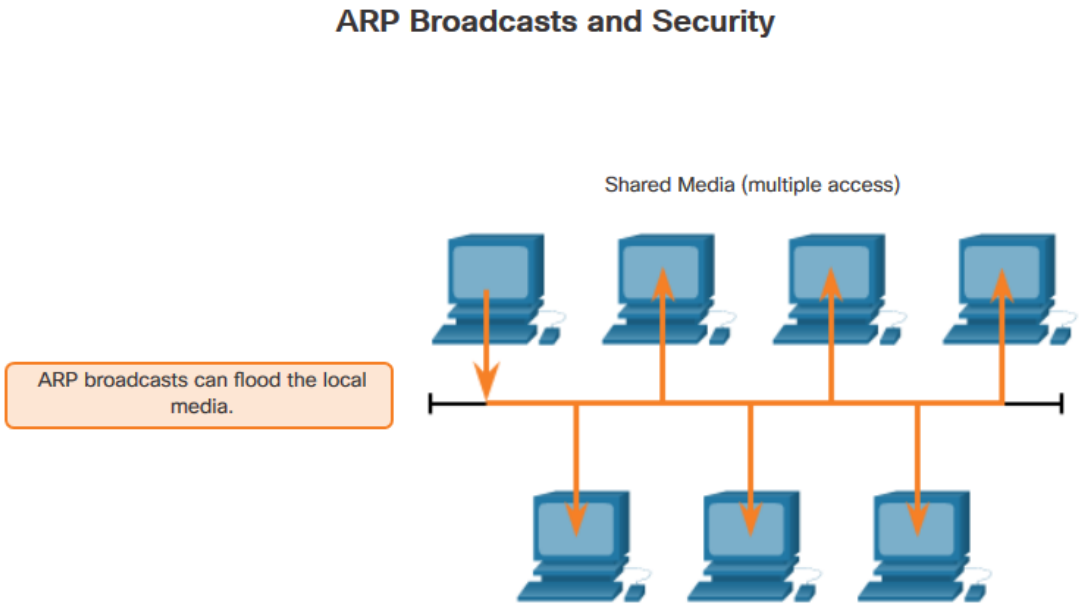
ARP Tables on Networking Devices

- Network hosts and routers keep ARP tables.
- Held in memory called ARP cache.
- Age out and removed from table.



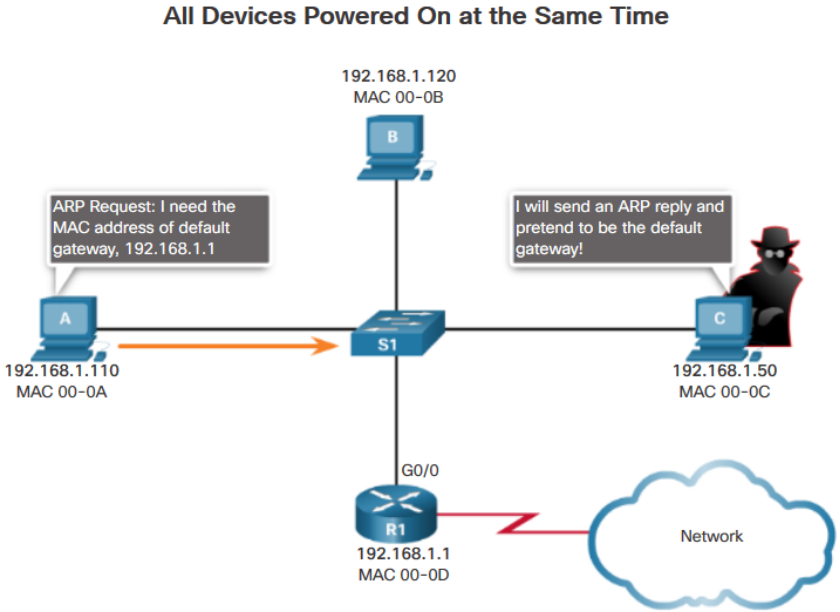
ARP Broadcasts

- ARP Broadcasts – could impact large networks.



ARP Spoofing

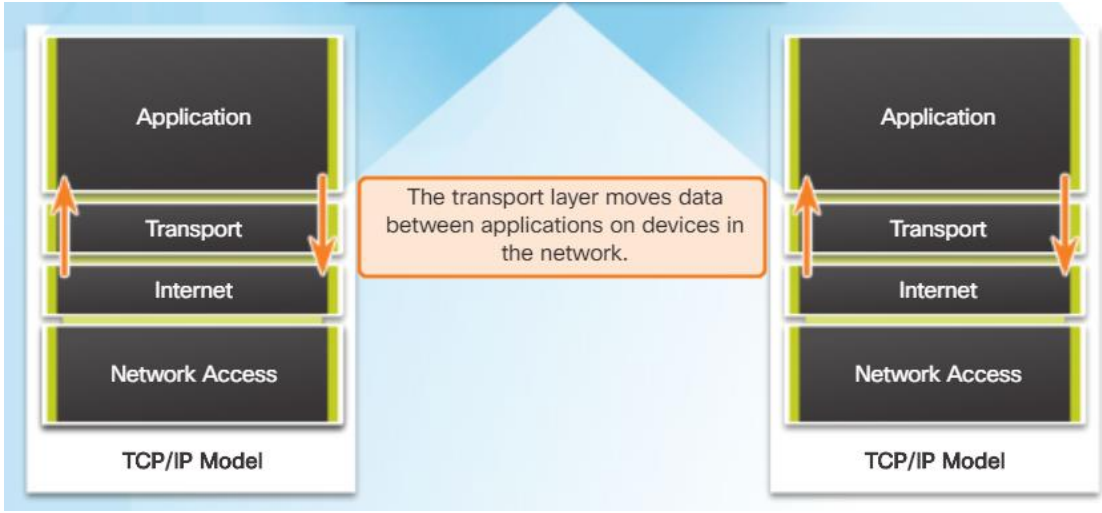
- ARP Spoofing (ARP poisoning) – security risk
  - This is a technique used by an attacker to reply to an ARP request for an IPv4 address belonging to another device, such as the default gateway.

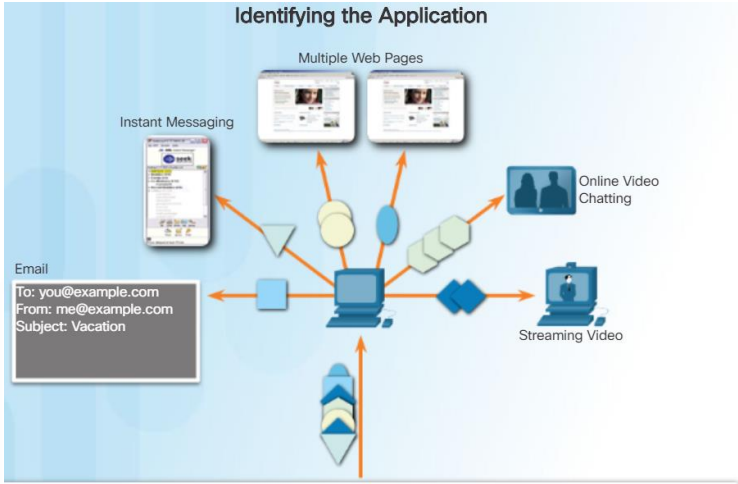


4.5 The Transport Layer

Transport Layer Protocol Role in Network Communication

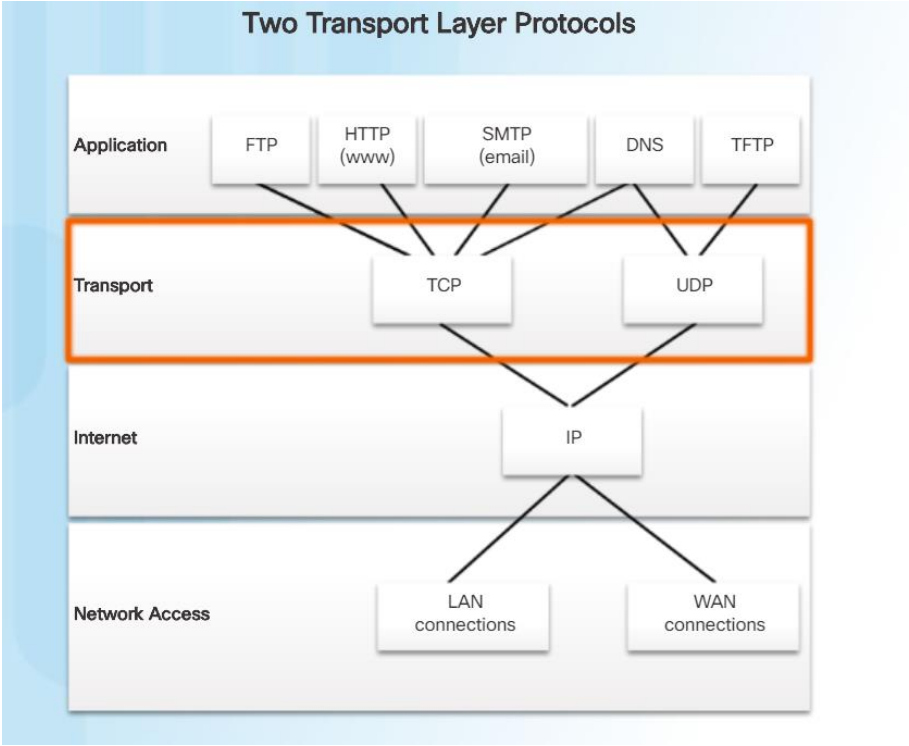
- Tracks individual conversations.
- Moves data between applications on network devices.
- Segments data and reassembles segments.
- Identifies applications using a port number.





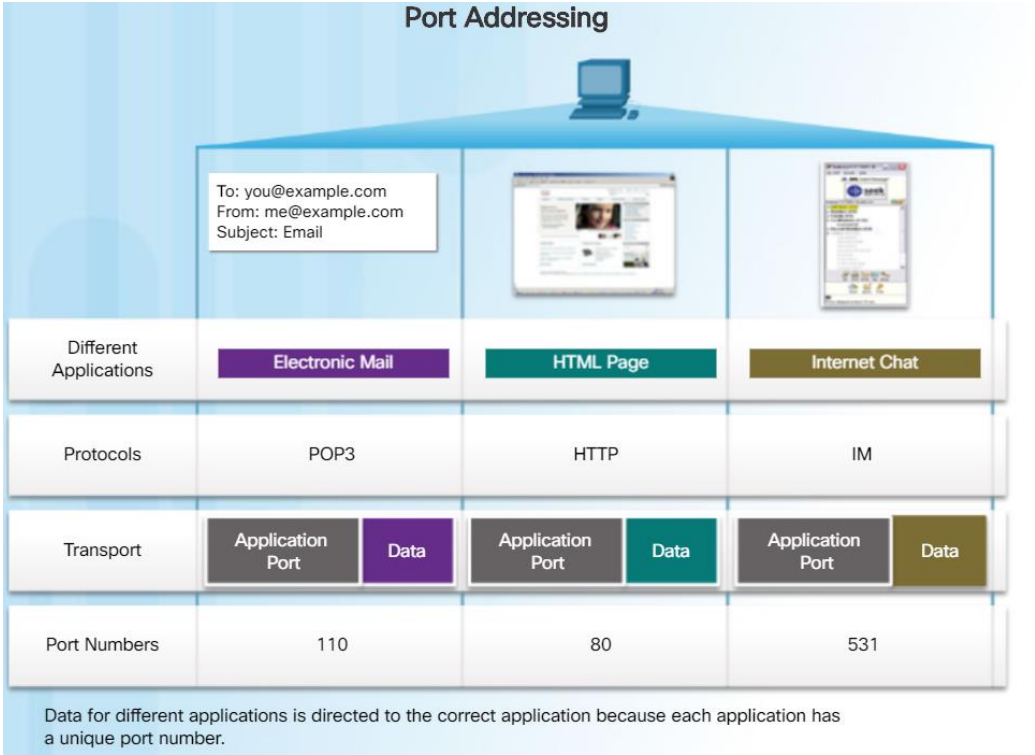
Transport Layer Mechanisms

- 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)**



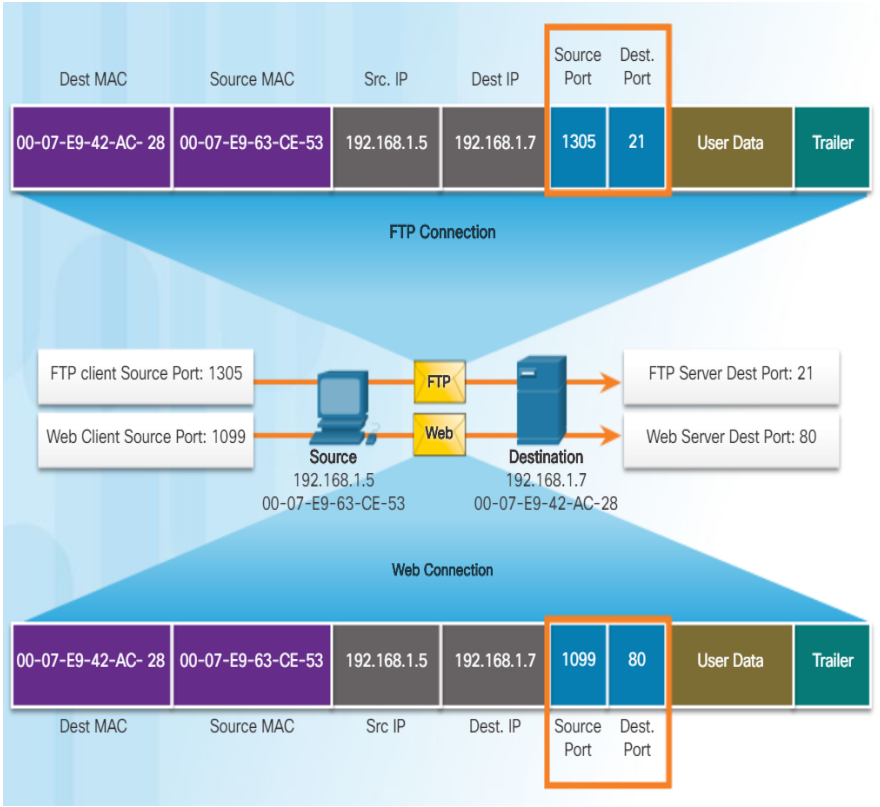
TCP Local and Remote Ports

- TCP and UDP manage these multiple simultaneous conversations by using header fields that can uniquely identify these applications. These unique identifiers are the port numbers:
  - The **source port number** is associated with the originating application on the local host.
  - The **destination port number** is associated with the destination application on the remote host.



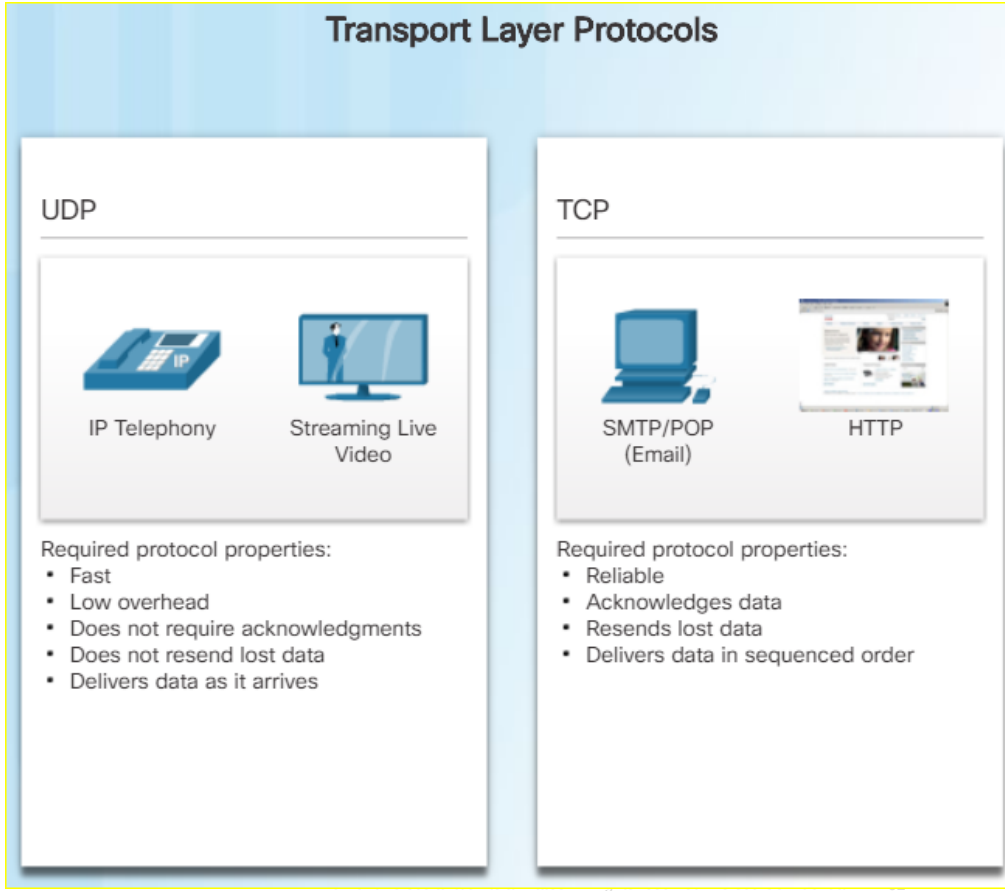
Socket Pairs

- 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**.
- The socket is used to identify the server and service being requested by the client.
- 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.



TCP versus UDP

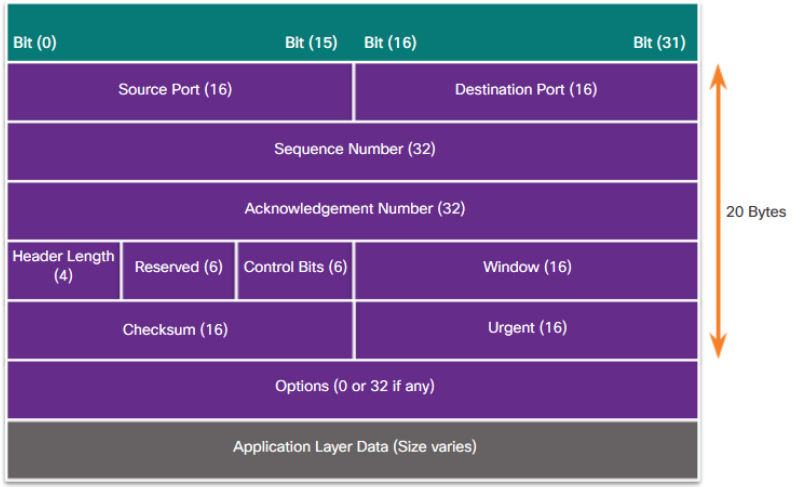
- TCP
  - Used for majority of the major TCP/IP protocols.
  - Reliable, acknowledges data, resends lost data, delivers data in sequenced order.
    - Examples: email, HTTP
- UDP
  - Fast, low overhead, does not require acknowledgments, does not resend lost data, delivers data as it arrives.
    - Examples: VoIP, streaming live videos



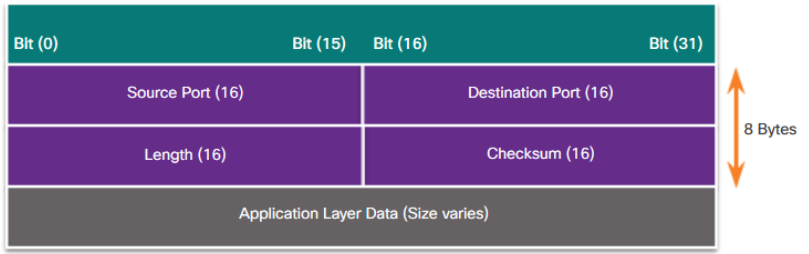
TCP and UDP Headers

- TCP
  - TCP is a stateful protocol. A stateful protocol is a protocol that keeps track of the state of the communication session.
  - To track the state of a session, TCP records which information it has sent and which information has been acknowledged.
  - The stateful session begins with the session establishment and ends when closed with the session termination.
- UDP
  - UDP is a stateless protocol, meaning neither the client, nor the server, is obligated to keep track of the state of the communication session.
  - If reliability is required when using UDP as the transport protocol, it must be handled by the application.

TCP Segment

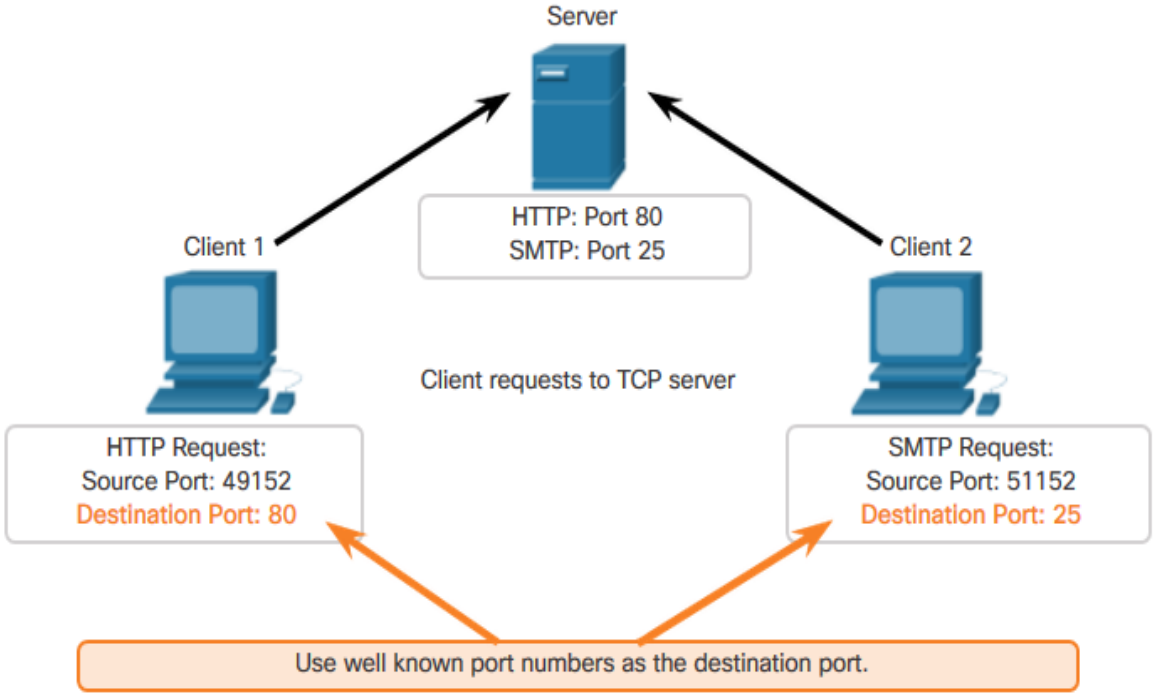


UDP Datagram



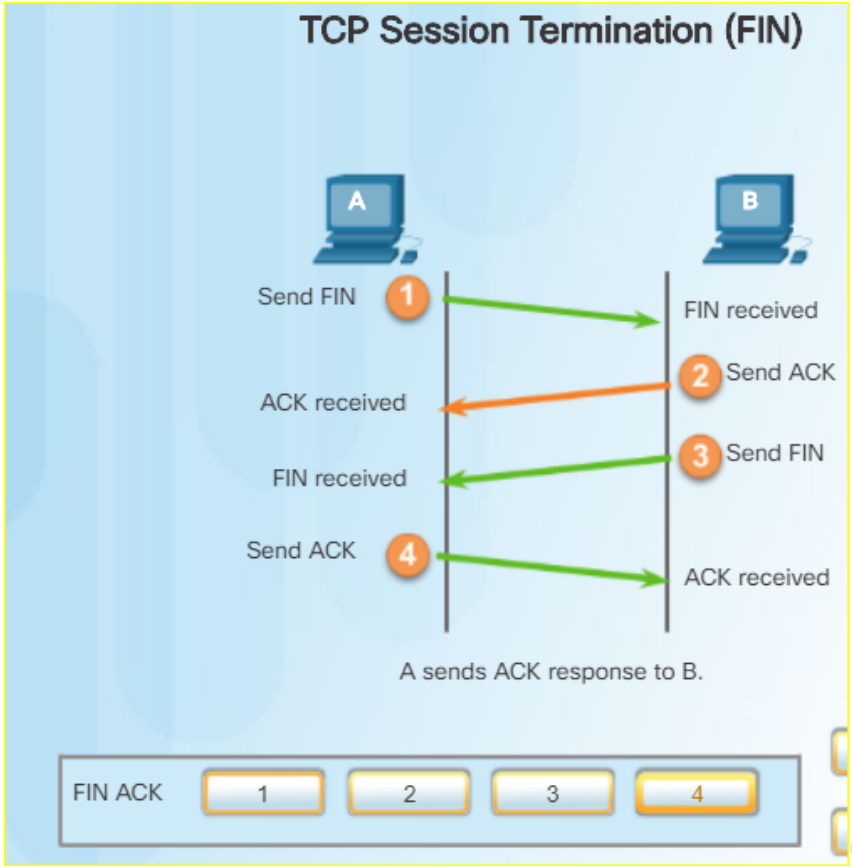
TCP Port Allocation

- 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.
  - Just as a server can have many ports open for server processes, clients can have many ports open for connections to multiple sockets.



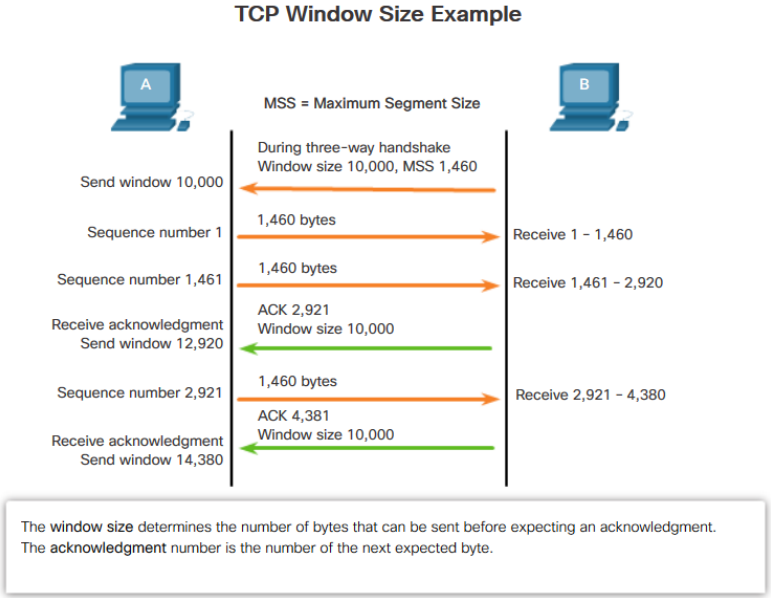
A TCP Session Part 1: Connection Establishment and Termination

- A TCP connection is established in three steps:
  1. The initiating client requests a client-to-server communication session with the server.
  2. The server acknowledges the client-to-server communication session and requests a server-to-client communication session.
  3. The initiating client acknowledges the server-to-client communication session.



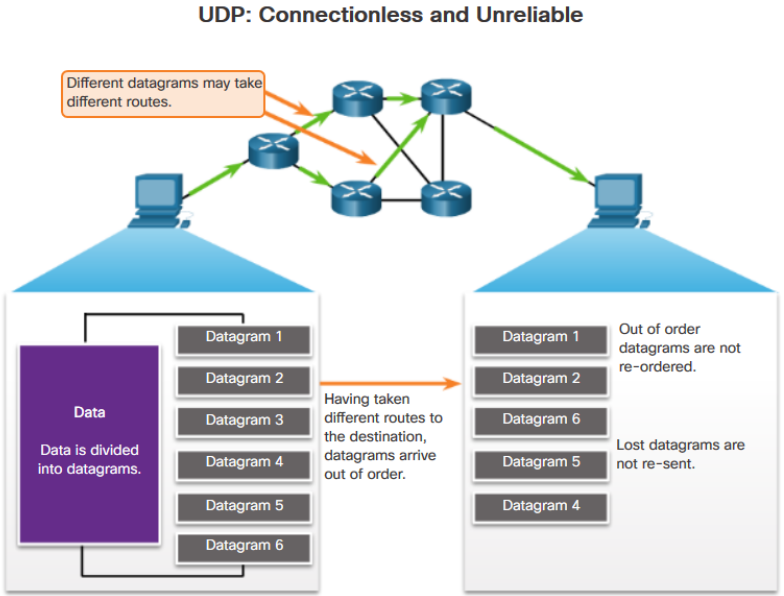
A TCP Session Part 2: Data Transfer

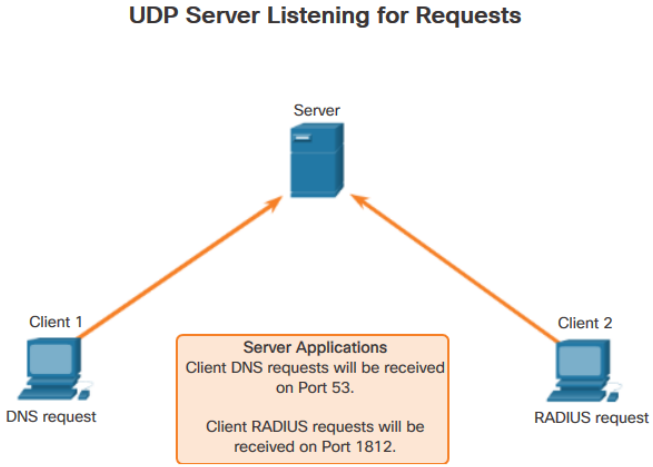
- **TCP Order Delivery:**
  - Segment sequence numbers indicate how to reassemble and reorder received segments.
  - The receiving TCP process places the data into a receiving buffer.
  - Out of order segments are held for later processing.
  - When the segments with the missing bytes arrive, these segments are processed in order.
- **Flow Control:**
  - Controls the amount of data that the destination can receive and process reliably by adjusting the rate of data flow.



UDP Session

- UDP Session:
  - Resembles the data in the order it was received.
  - Assigned well-known or registered port numbers.



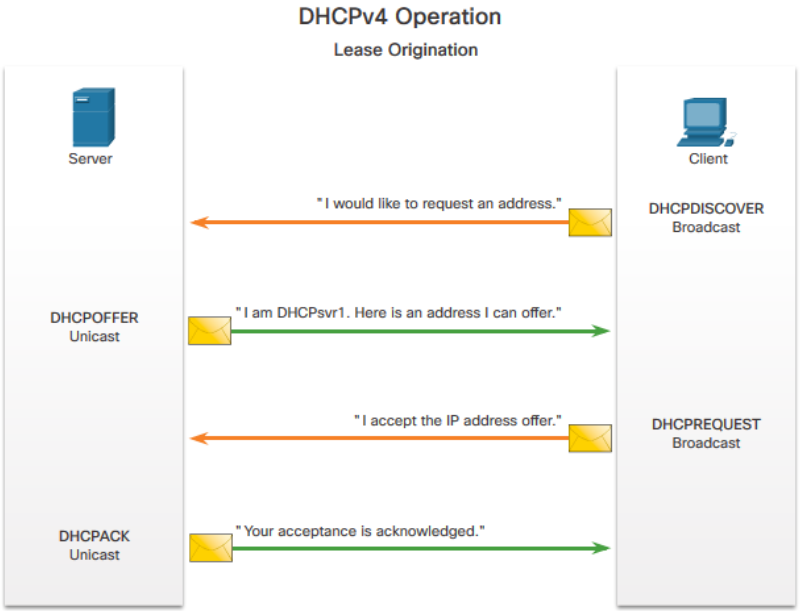


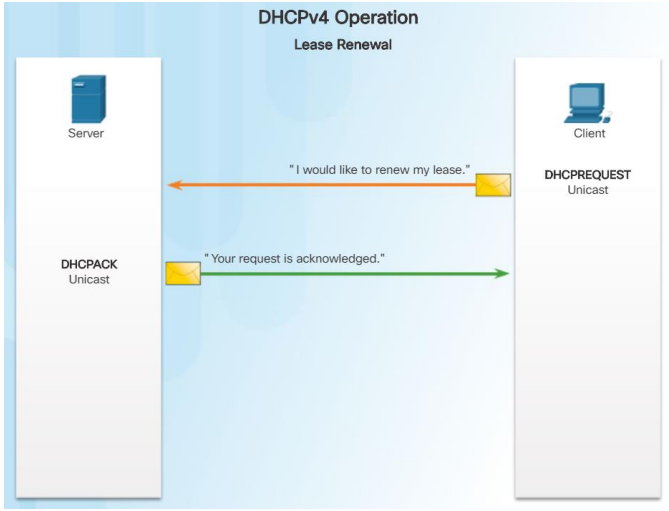
Client requests to servers have well-known port numbers as the destination port.

4.6 Network Services

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)

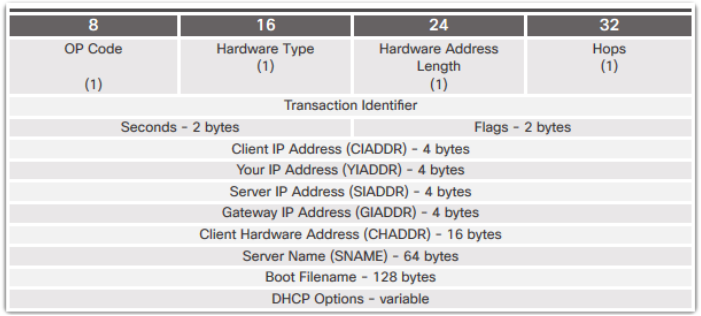




DHCPv4 Message Format

A DHCP message contains the following fields:

- **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.



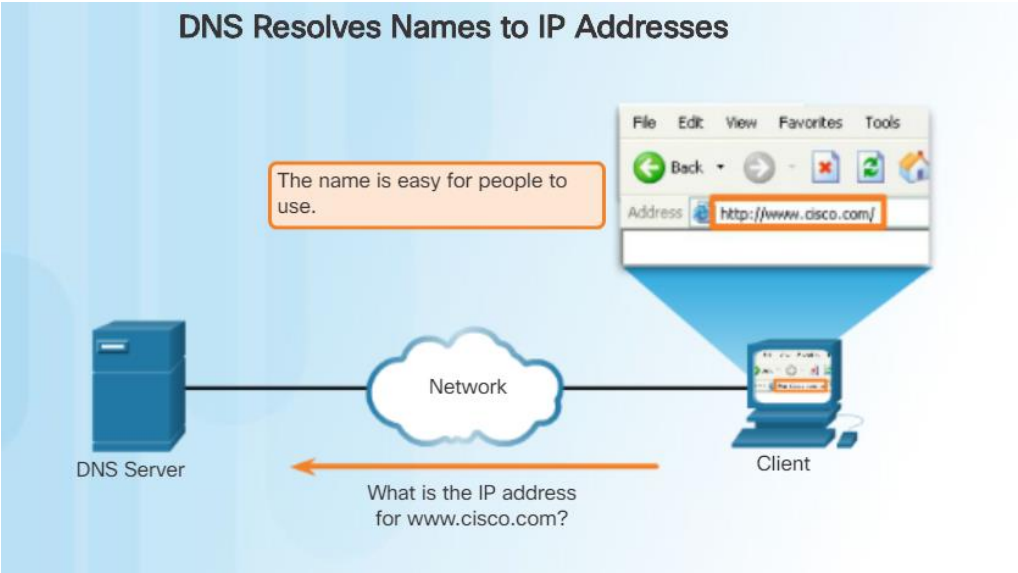
DHCPv4 Message Format (Cont.)

A DHCP message contains the following fields:

- **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.

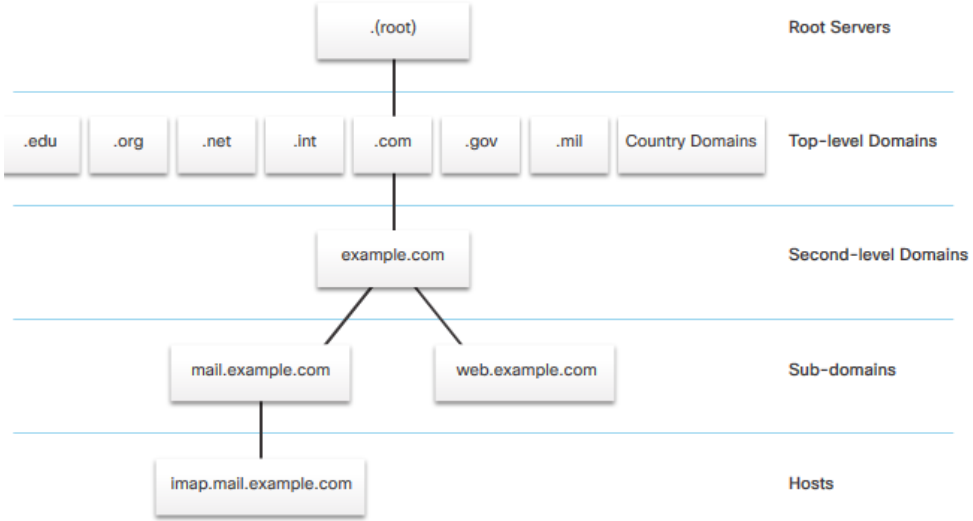
DNS Overview

- Dynamic Name System (DNS)
  - Manages and provides domain names and associated IP addresses.
  - Hierarchy of servers.
  - 90% of malicious software used to attack networks uses DNS to carry out attack campaigns.



DNS Domain Hierarchy

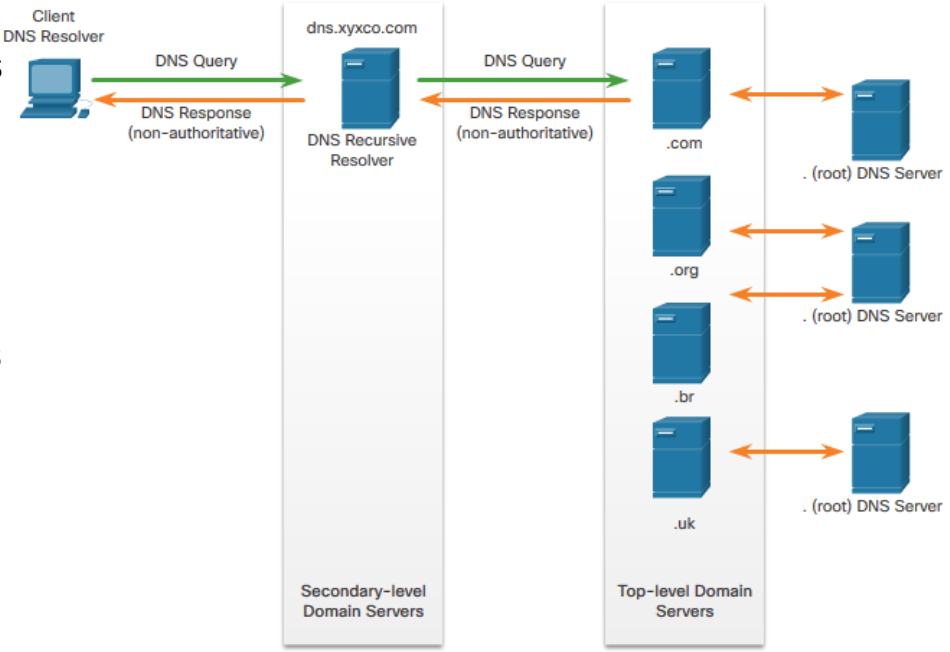
- Dynamic Name System (DNS)
  - The DNS consists of a hierarchy of generic top level domains (gTLD) which consist of .com, .net, .org, .gov, .edu, and numerous country-level domains, such as .br (Brazil), .es (Spain),.uk (United Kingdom).
  - Second-level domains are represented by a domain name that 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 Lookup Process

To understand DNS, cybersecurity analysts should be familiar with the following terms:

- **Resolver** - A DNS client that sends DNS messages to obtain information about the requested domain name space.
- **Recursion** - The action taken when a DNS server is asked to query on behalf of a DNS resolver.
- **Authoritative Server** - A DNS server that responds to query messages with information stored in Resource Records (RRs) for a domain name space stored on the server.
- **Recursive Resolver** - A DNS server that recursively queries for the information asked in the DNS query.

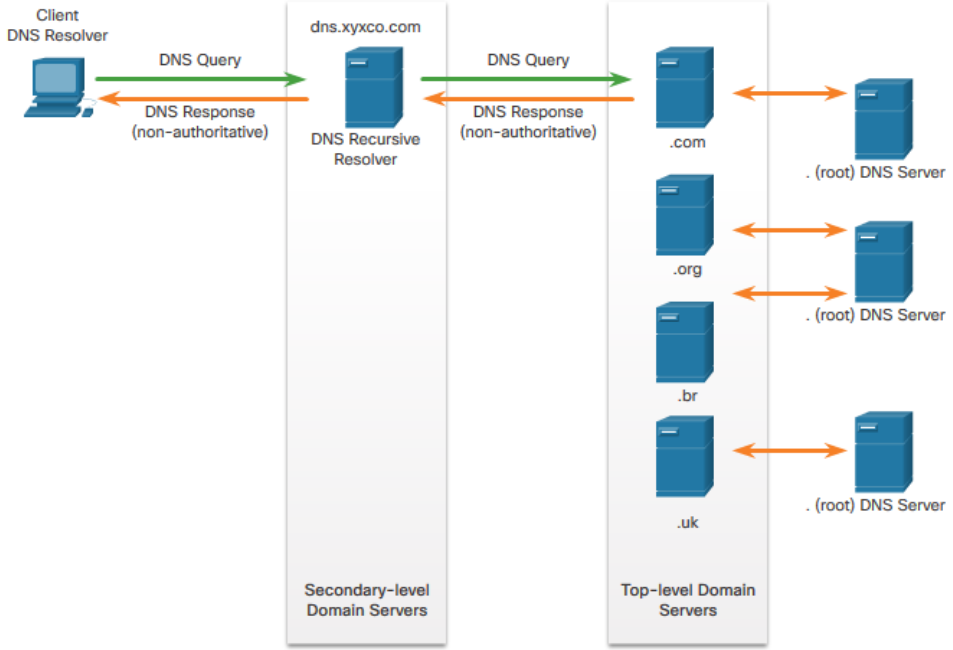


DNS Lookup Process (Cont.)

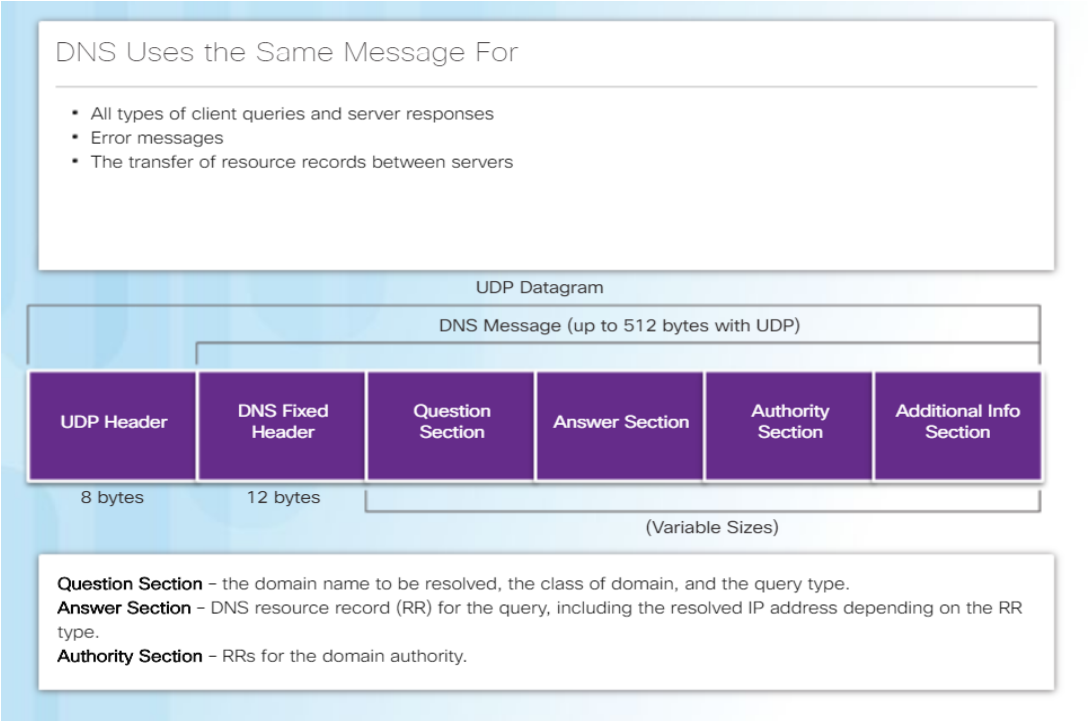
To understand DNS, cybersecurity analysts should be familiar with the following terms:

- **FQDN** - A Fully Qualified Domain Name is the absolute name of a device within the distributed DNS database.
- **RR** - A Resource Record is a format used in DNS messages that is composed of the following fields: NAME, TYPE, CLASS, TTL, RDLENGTH, and RDATA.
- **Zone** - A database that contains information about the domain name space stored on an authoritative server.

.

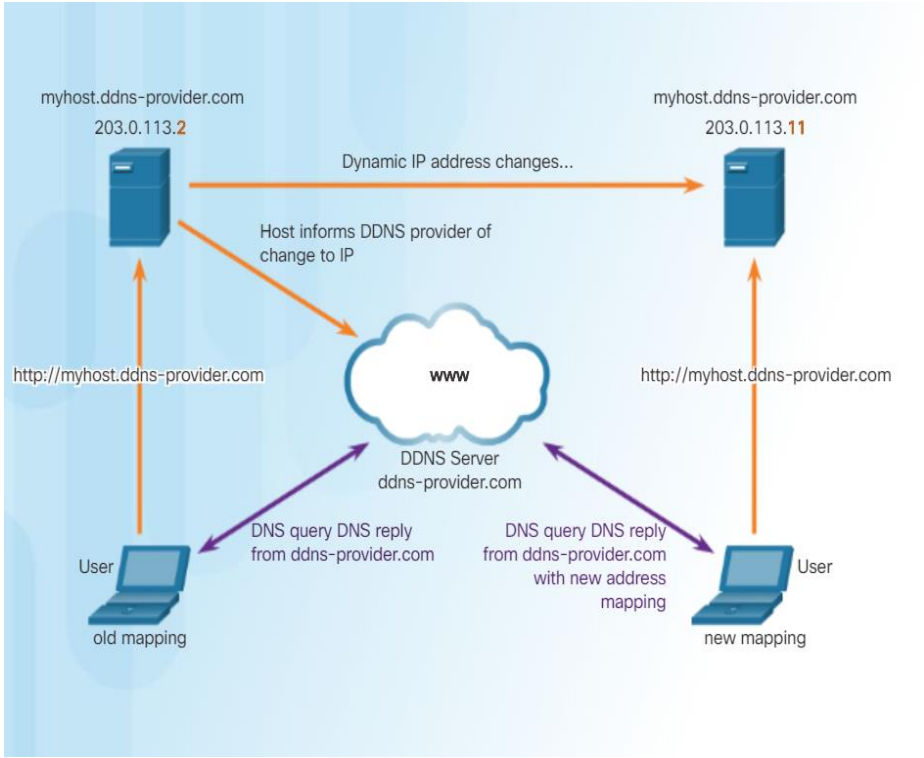


DNS Message Format



- DNS uses UDP port 53 for DNS queries and responses.
- DNS queries originate at a client and responses are issued from DNS servers.
- If a DNS response exceeds 512 bytes such as when Dynamic DNS (DDNS) is used, TCP port 53 is used to handle the message.
- DNS Record Types:
  - **A** - An end device IPv4 address
  - **NS** - An authoritative name server
  - **AAAA** - An end device IPv6 address
  - **MX** - A mail exchange record

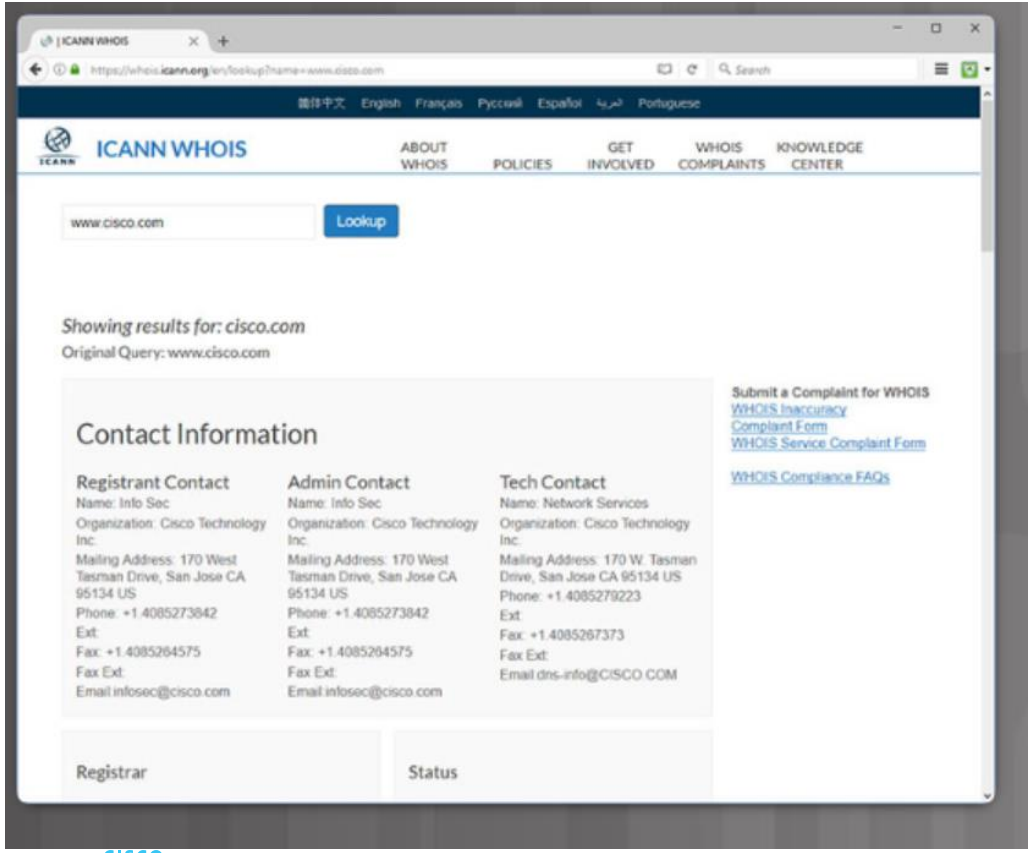
Dynamic DNS



Dynamic DNS (DDNS)

- Allows a user or organization to register an IP address with a domain name as in DNS.
- When the IP address of the mapping changes, the new mapping can be propagated through the DNS almost instantaneously.

The WHOIS Protocol

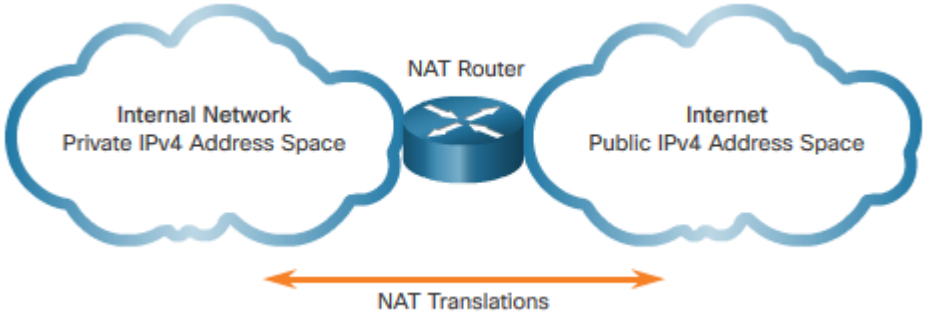


WHOIS Protocol:

- WHOIS is a TCP-based protocol that is used to identify the owners of Internet domains through the DNS system.

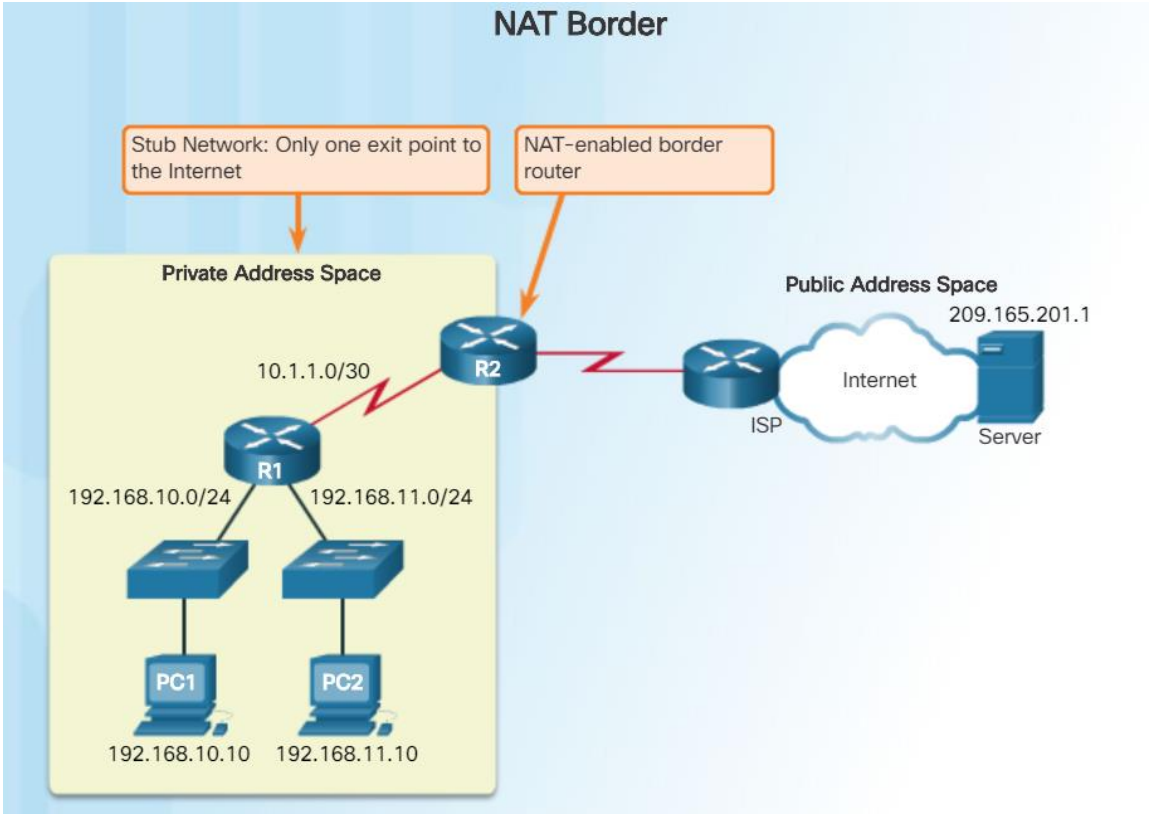
NAT – Overview

- Network Address Translation (NAT)
  - Not enough public IPv4 addresses to assign a unique address to each device connected to the Internet.
  - Private IPv4 addresses are used within an organization or site to allow devices to communicate locally.
  - Private IPv4 addresses cannot be routed over the Internet.
  - Used on border devices.



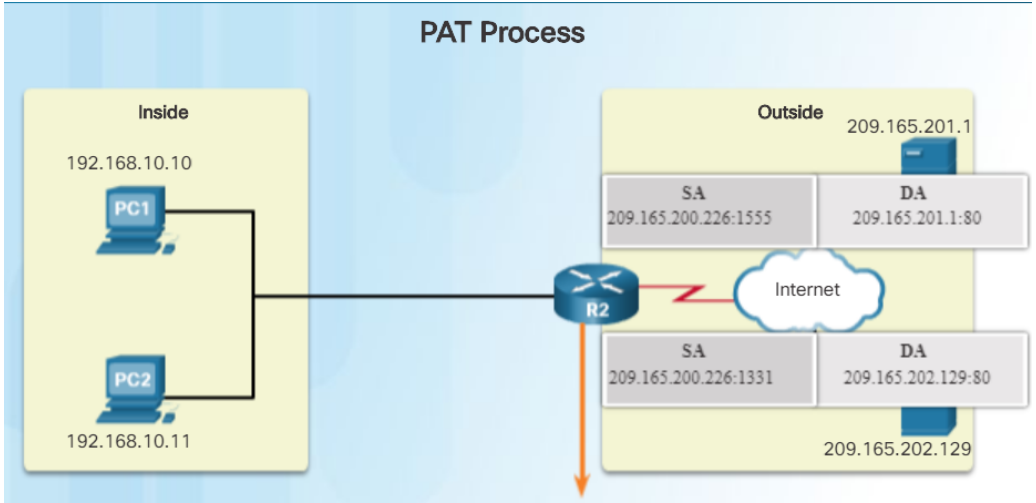
NAT – Enabled Routers

- Network Address Translation (NAT)
  - When an internal device sends traffic out of the network, the NAT-enabled router translates the internal IPv4 address of the device to a public address from 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.



Port Address Translation

- Port Address Translation (PAT)
  - One-to-many – Many internal address translations to one or more public IP addresses

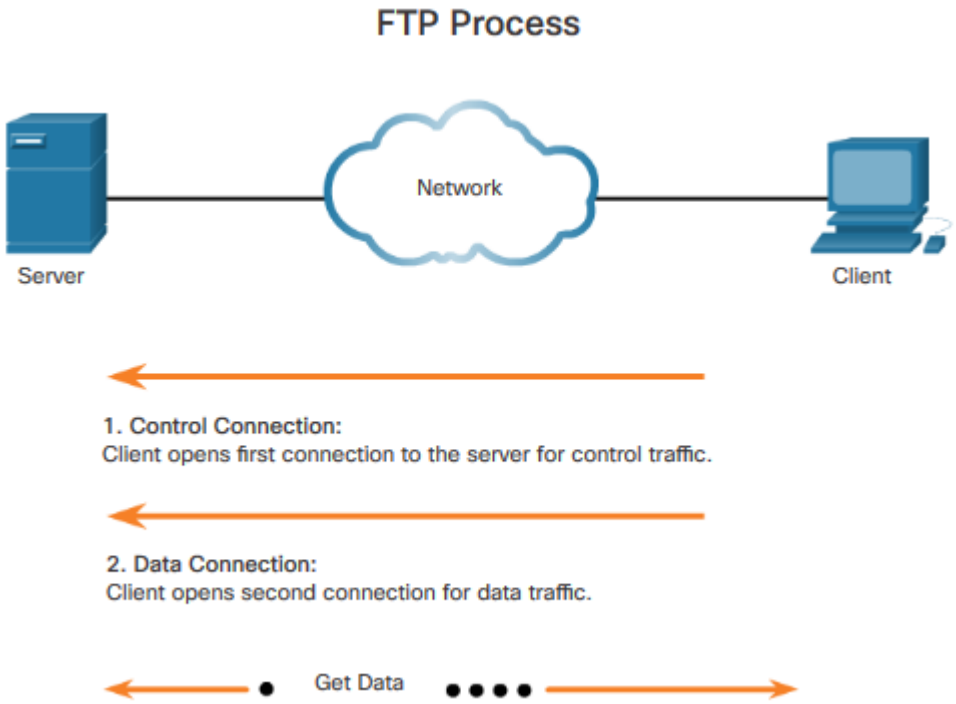


NAT Table with Overload

Inside Global IP Address	Inside Local IP Address	Outside Local IP Address	Outside Global IP Address
209.165.200.226:1555	192.168.10.10:1555	209.165.201.1:80	209.165.201.1:80
209.165.200.226:1331	192.168.10.11:1331	209.165.202.129:80	209.165.202.129:80

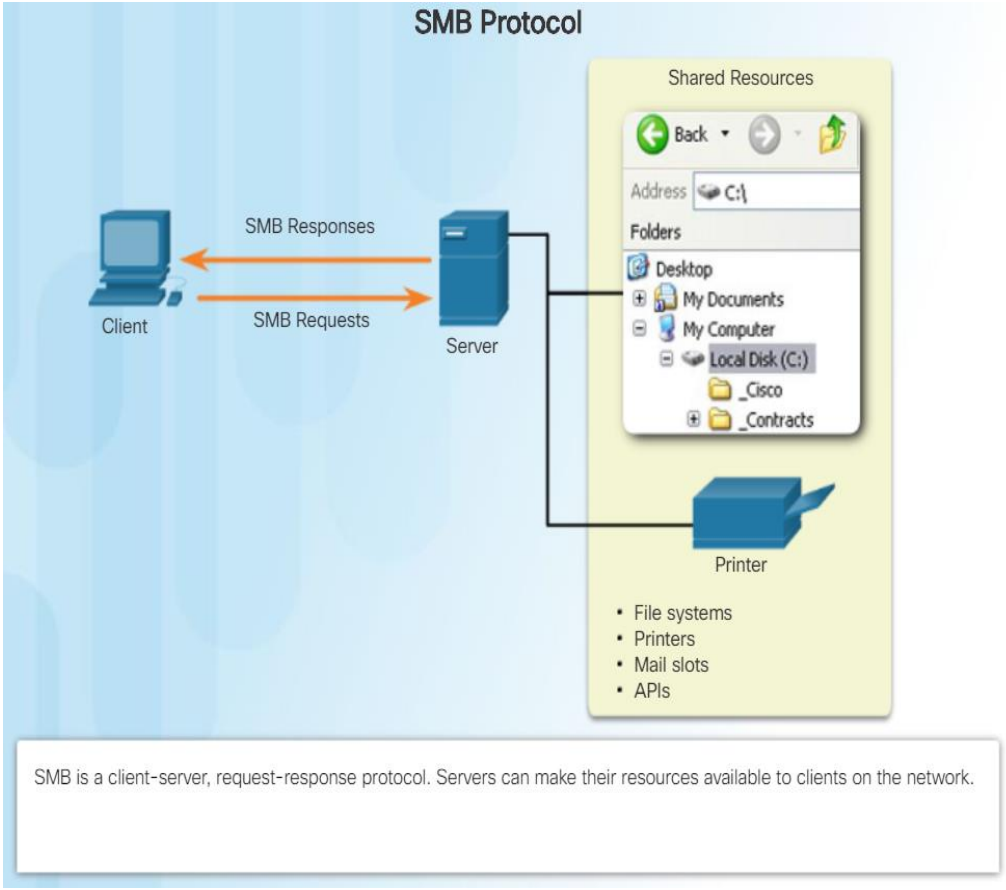
FTP and TFTP

- File Transfer Protocol (FTP)
  - TCP-based.
  - Used to push and pull data from a server.
- Trivial File Transfer Protocol (TFTP)
  - UDP-based.
  - Fast, but unreliable.
- Server Message Block (SMB)
  - Client/server-based file sharing protocol.



SMB

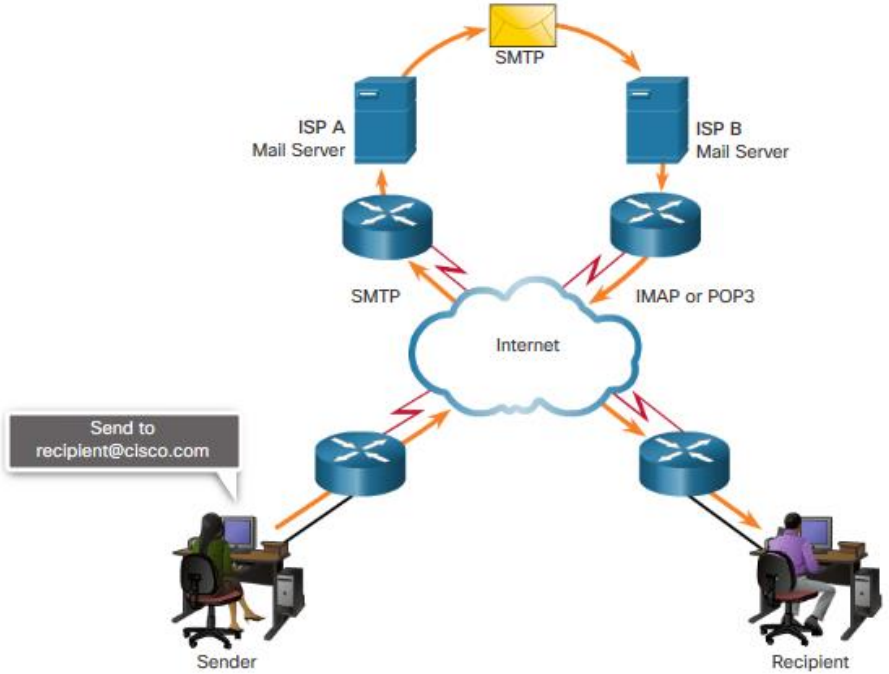
- Server Message Block (SMB)
  - Client/server-based file sharing protocol.
  - This format uses a fixed-sized header, followed by a variable-sized parameter and data component.
  - SMB messages can start, authenticate, and terminate sessions, control file and printer access, and allow an application to send or receive messages to or from another device.



Email Overview

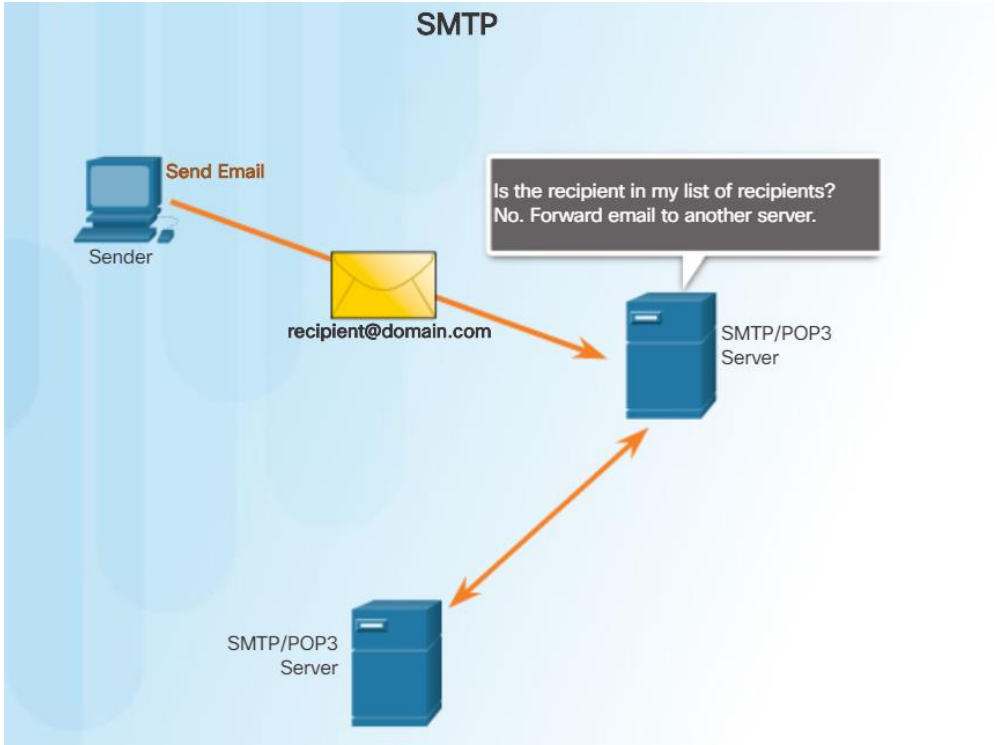
- Email supports three separate protocols for operation:
  - Simple Mail Transfer Protocol (SMTP)
  - Post Office Protocol version 3 (POP3)
  - IMAP

The application layer process that sends mail uses SMTP. A client retrieves email using one of the two application layer protocols: POP3 or IMAP.



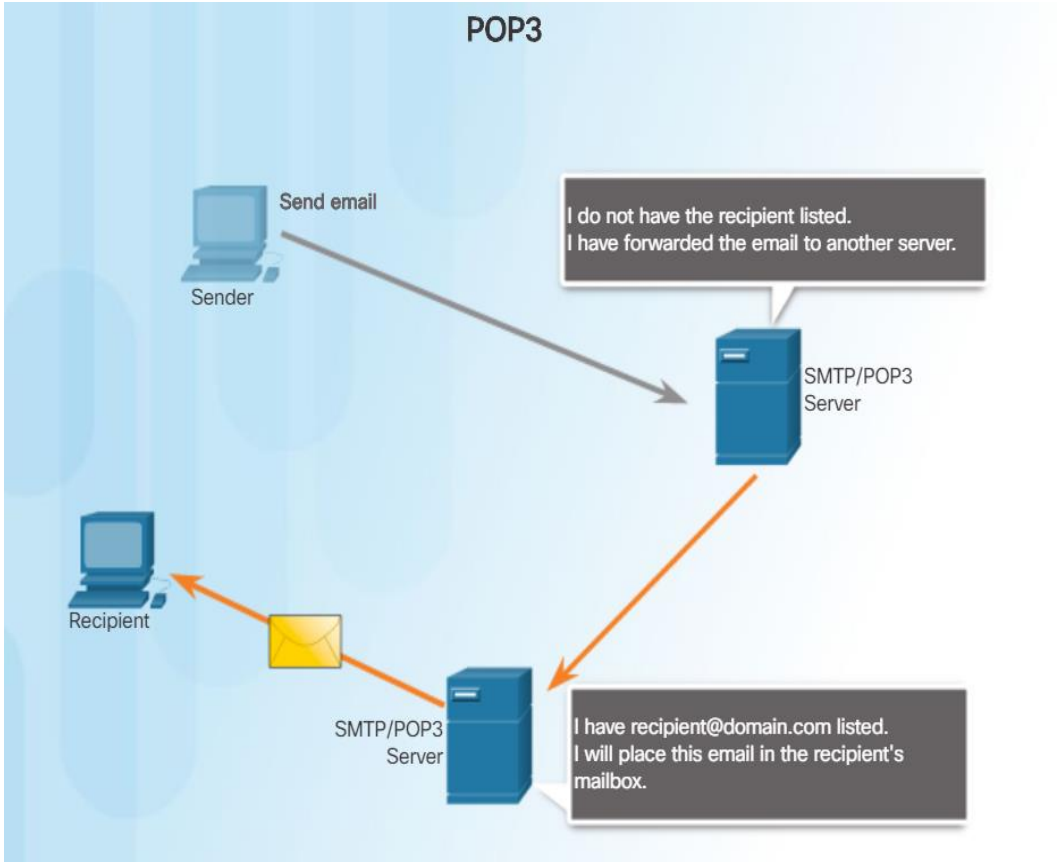
SMTP

- SMTP
  - Simple Mail Transfer Protocol (SMTP) – Port 25.
- After the connection is made, the client attempts to send the email to the server across the connection.
- 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.



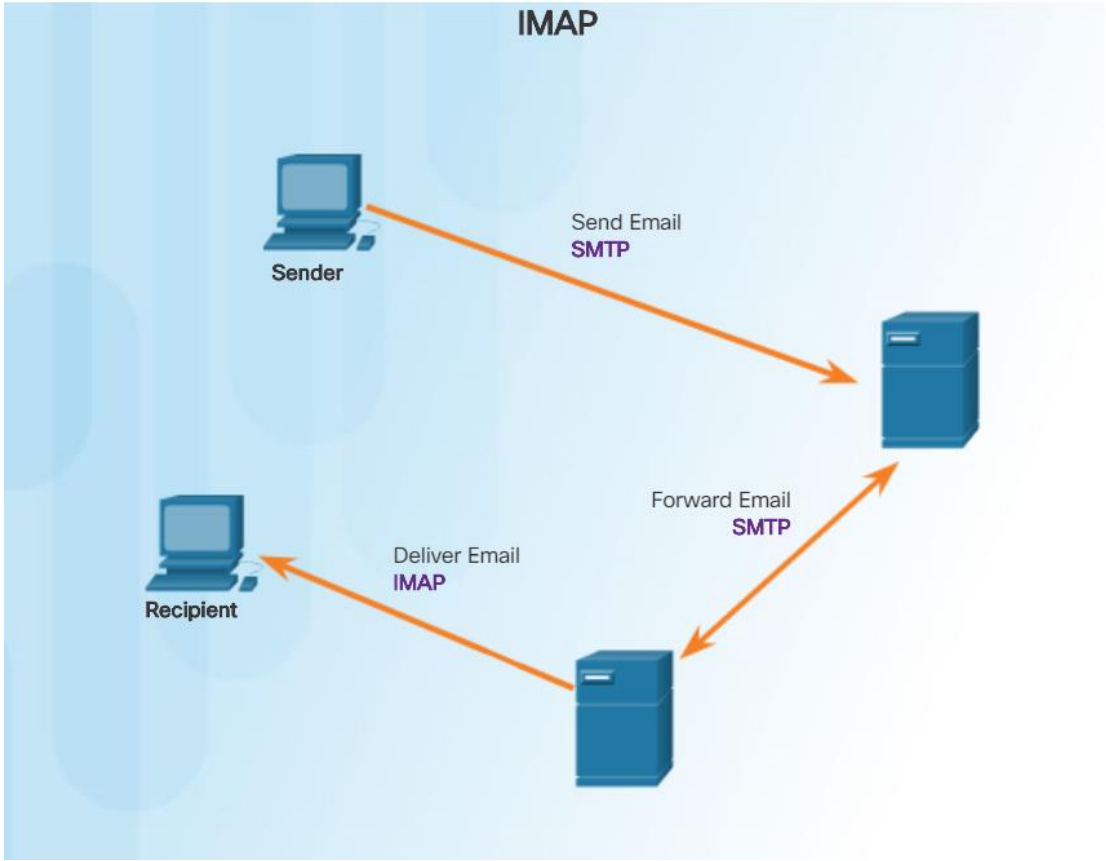
POP3

- With POP3, mail is downloaded from the server to the client and then deleted on the server.
- With POP3, email messages are downloaded to the client and removed from the server, so there is no centralized location where email messages are kept.



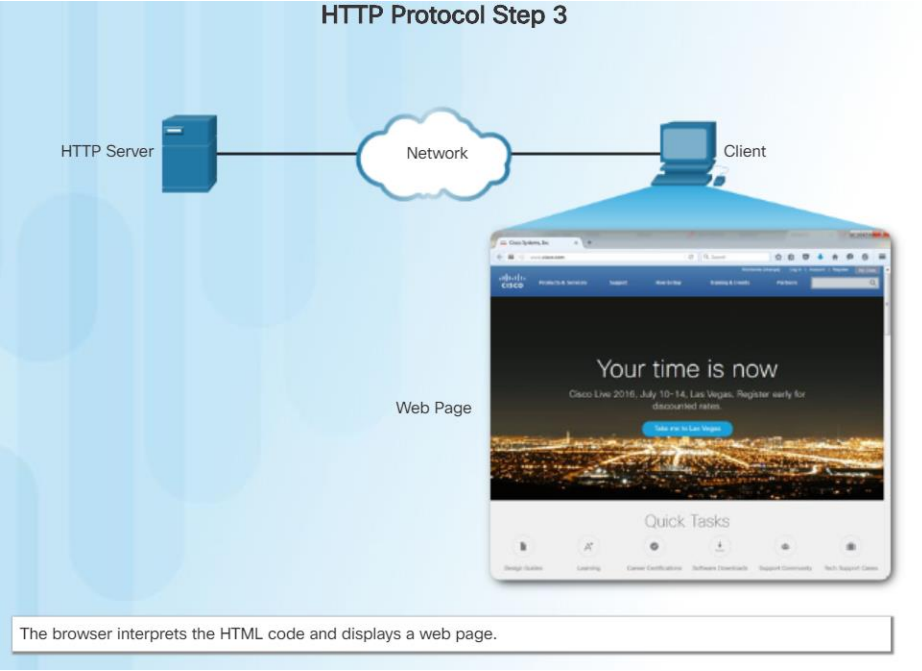
IMAP

- When a user connects to an IMAP-capable server, copies of the messages are downloaded to the client application.
- When a user decides to delete a message, the server synchronizes that action and deletes the message from the server.



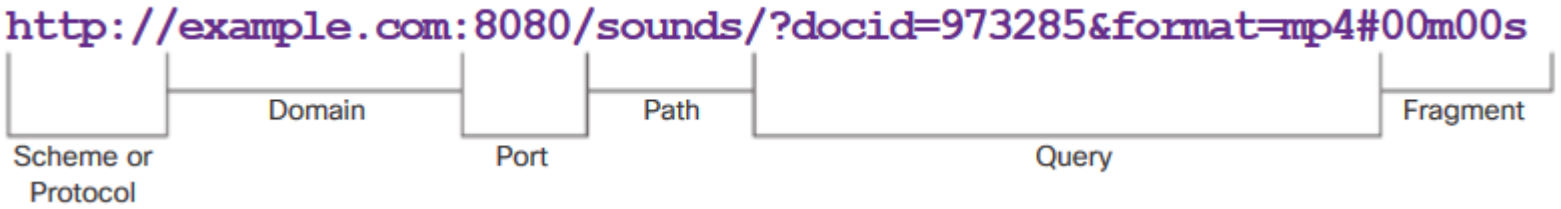
HTTP Overview

- Hypertext Transfer Protocol (HTTP) :
  - Port 80
  - Governs the way a web server and client interact.
  - TCP-based
  - Has specific server responses.
- Steps:
  1. Client initiates HTTP request to server.
  2. HTTP returns code for a webpage.
  3. Browser interprets HTML code and displays on webpage.



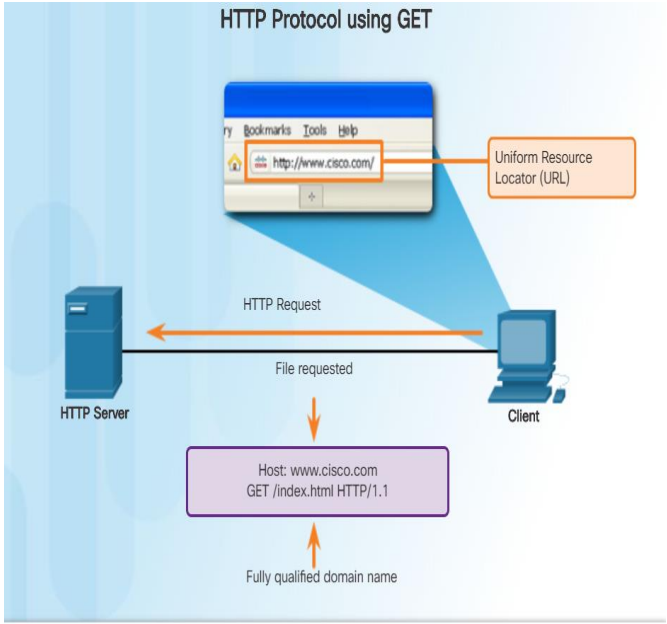
The HTTP URL

- HTTP URLs can also specify the port on the server that should handle the HTTP methods.
- In addition, it can specify a query string and fragment.
- Query string typically contains information that is not handled by the HTTP server process itself, but is instead handled by another process that is running on the server.



The HTTP Protocol

- HTTP is a request/response protocol that uses TCP port 80.
- When a client, typically a web browser, sends a request to a web server, it will use one of six methods that are specified by the HTTP protocol.
  - **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.



Entering 'http://www.cisco.com' in the address bar of a web browser generates the HTTP 'GET' message.

HTTP Status Code

- 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.


CISCO