Table Of Contents

Introduction

Online References: Link

YouTube: Link

1. Why Should I Take This Module?

Welcome to the Application Layer!

As you have learned, the transport layer is where data actually gets moved from one host to another. But before that can take place, there are a lot of details that have to be determined so that this data transport happens correctly. This is why there is an application layer in both the OSI and the TCP/IP models.

As an example, before there was streaming video over the internet, we had to watch home movies in a variety of other ways. Imagine that you videotaped some of your child's soccer games. Your parents, in another city, only have a video cassette player. You have to copy your video from your camera onto the right type of video cassette to send to them.

Your brother has a DVD player, so you transfer your video to a DVD to send to him. This is what the application layer is all about, making sure that your data is in a format that the receiving device can use. Let's dive in!

2. What Will I Learn To Do In This Module?

2A. Module Title

- Application Layer

2B. Module Objective

- Explain the operation of application layer protocols in providing support to end-user applications.

Topic Title	Topic Objective
Application, Presentation, and Session	Explain how the functions of the application layer, presentation layer, and session layer work together to provide network services to end user applications.
Peer-to-Peer	Explain how end user applications operate in a peer-to-peer network.
Web and Email Protocols	Explain how web and email protocols operate.
IP Addressing Services	Explain how DNS and DHCP operate.
File Sharing Services	Explain how file transfer protocols operate.

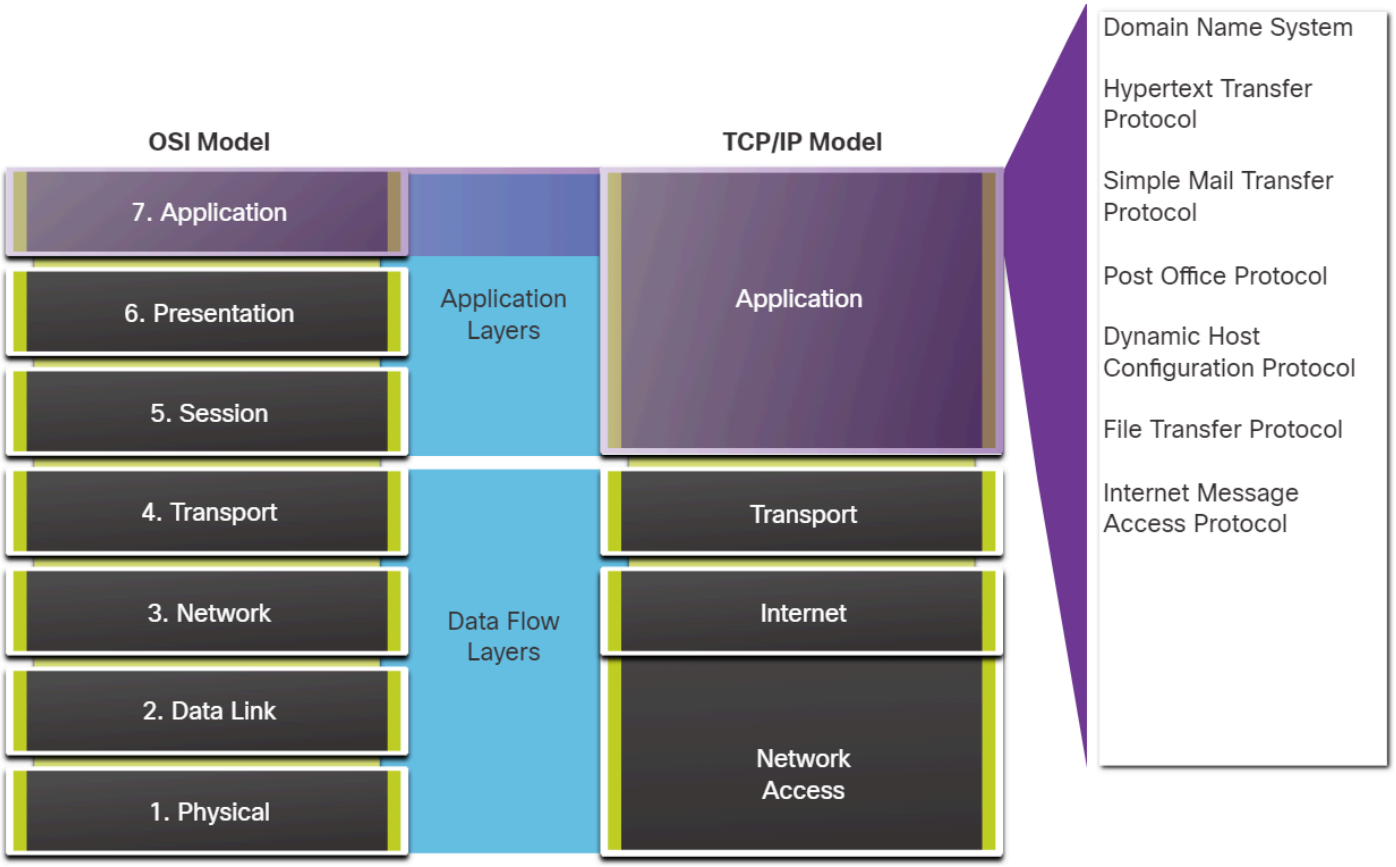
Application, Presentation, and Session

1. Application Layer

In the OSI and the TCP/IP models, the application layer is the closest layer to the end user. As shown in the figure, it is the application layer that provides the **interface** between the applications used to communicate, and the underlying network over which messages are transmitted. Application layer protocols are used to exchange data between programs running on the source and destination hosts.

Based on the TCP/IP model, the **upper three layers** of the OSI model (application, presentation, and session) define the functions of the TCP/IP application layer.

There are many application layer protocols, and new protocols are always being developed. Some of the most widely known application layer protocols include Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP), Internet Message Access Protocol (IMAP), and Domain Name System (DNS) protocol.



1A. Overview

In both the OSI (Open Systems Interconnection) and TCP/IP (Transmission Control Protocol/Internet Protocol) models, the **Application Layer** is the layer closest to the end-user.

This is where communication between users happens through applications. It acts as the interface between the user's applications (like a web browser or email client) and the network over which data travels.

The **Application Layer** is responsible for handling **data exchange** between programs running on two different devices, such as a computer and a server. The programs use predefined protocols to communicate effectively.

1B. Application Layer in OSI and TCP/IP Models

- **OSI Model:** The OSI model has seven layers, and the application layer is the topmost one. It defines the **user interface** and communication between applications.

- **TCP/IP Model:** The TCP/IP model has four layers, and the application layer combines the functionalities of the OSI model's **Application, Presentation, and Session layers**. It provides services directly to the user's applications.

1C. Functions of the Application Layer

- **Data Exchange:** It helps in exchanging data between applications across the network. For example, sending an email or downloading a web page.

- **Protocol Management:** The layer manages different protocols that define how data should be exchanged. These protocols include those for web browsing, file transfers, email, and more.

- **End-User Support:** It directly interacts with applications such as web browsers, email clients, and others to give the user a meaningful and understandable network interface.

1D. Key Application Layer Protocols

Hypertext Transfer Protocol (HTTP):

- Used for web browsing. It allows the exchange of web pages between a browser and a web server.
- **Example:** When you visit a website, your browser sends an HTTP request to the server. The server sends back an HTTP response containing the web page content, which is displayed in your browser.

File Transfer Protocol (FTP):

- Designed for file transfer between computers over a network. FTP allows users to upload, download, and manage files remotely.
- **Example:** If you want to upload a website's files to a web server, you can use FTP to transfer files from your computer to the hosting server.

Trivial File Transfer Protocol (TFTP):

- A simpler, lightweight version of FTP, mainly used for transferring small amounts of data between devices. It is commonly used for booting network devices or updating firmware.
- **Example:** Routers often use TFTP to download configuration files from a central server during startup.

Internet Message Access Protocol (IMAP):

- A protocol used by email clients to retrieve email messages from a mail server. Unlike older protocols (such as POP3), IMAP allows users to manage their mail directly on the server, so multiple devices can access the same mailbox.
- **Example:** When you access your email from your phone or computer using Gmail or Outlook, the mail client uses IMAP to sync your inbox.

Domain Name System (DNS) Protocol:

- DNS translates human-readable domain names (like www.google.com) into IP addresses that computers use to identify each other on the network.
- **Example:** When you type a web address (URL) into your browser, the DNS resolves the domain name into an IP address, allowing the browser to connect to the correct server.

1E. Relationship between the Application Layer and Other Layers

The application layer provides communication services directly to the user's application. Beneath it, other layers handle the details of data transportation. For example:

- The **Transport Layer** ensures reliable data transfer.
- The **Network Layer** handles routing data between different networks.
- The **Data Link Layer** manages communication between devices on the same network.

1F. Real-World Examples

Web Browsing:

- When you visit a website, your web browser uses the **HTTP/HTTPS** protocol (part of the application layer) to request web pages from the server. The server processes the request and responds with the requested page, which is then rendered in your browser.

Email:

- When you send or receive an email, the email client uses protocols like **SMTP (Simple Mail Transfer Protocol)** to send messages, and **IMAP** to retrieve and sync messages between the server and your device.

Remote File Access:

- You can use **FTP** to upload or download files to or from a server remotely. The file is transferred using the application layer, while lower layers handle the actual transmission over the network.

Network Booting:

- A router or network device may boot using a **TFTP** server. The device retrieves the necessary configuration or operating system image from the server during the boot process.

Resolving Web Addresses:

- When you type "www.example.com" in your browser, **DNS** converts that domain into an IP address so the browser can connect to the right web server.

Summary

The **Application Layer** is crucial for user-level interactions with the network. It provides the protocols that enable applications to exchange data effectively over a network. Common application layer protocols include **HTTP** for web browsing, **FTP** for file transfer, **IMAP** for email management, and **DNS** for resolving domain names. Each protocol is designed to handle a specific type of communication between networked applications.

2. Presentation and Session Layer

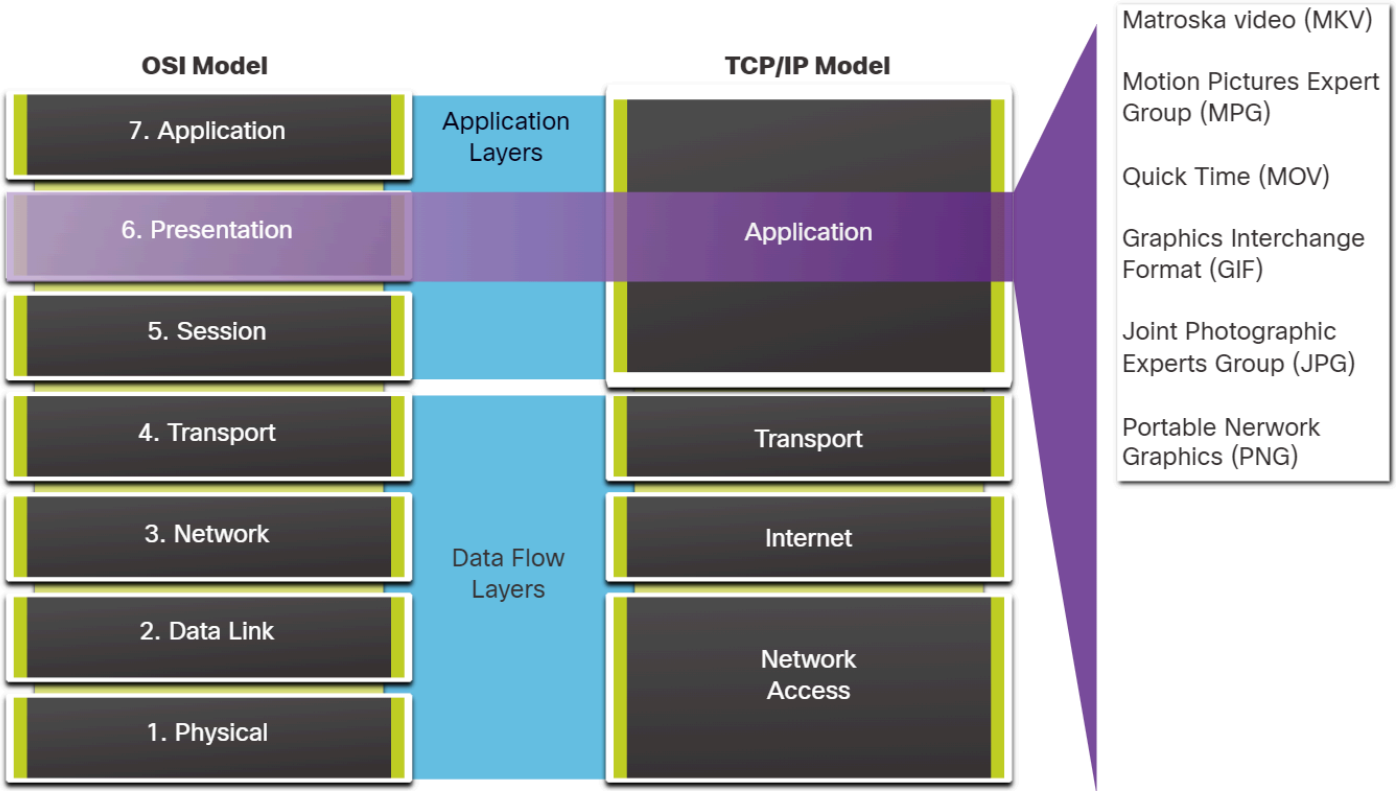
2A. Presentation Layer

The presentation layer has three primary functions:

- **Formatting, or presenting**, data at the source device into a compatible format for receipt by the destination device.
- **Compressing** data in a way that can be decompressed by the destination device.
- **Encrypting** data for transmission and decrypting data upon receipt.

As shown in the figure, the presentation layer formats data for the application layer, and it sets standards for file formats. Some well-known standards for video include Matroska Video (MKV), Motion Picture Experts Group (MPG), and QuickTime Video (MOV).

Some well-known graphic image formats are Graphics Interchange Format (GIF), Joint Photographic Experts Group (JPG), and Portable Network Graphics (PNG) format.



2B. Session Layer

As the name implies, **functions at the session layer** create and maintain dialogs between source and destination applications. The session layer handles the exchange of information to initiate dialogs, keep them active, and to restart sessions that are disrupted or idle for a long period of time.

2C. Presentation Layer (Layer 6 of the OSI Model)

The **Presentation Layer** is responsible for how data is formatted, compressed, and encrypted so it can be interpreted and used by the **Application Layer** (Layer 7) above it.

It ensures that data sent from one device can be read and understood by the receiving device, despite differences in data representation between systems. Here are the three main functions of the Presentation Layer:

i. Data Formatting (Translation)

- This involves converting data from one format to another to ensure compatibility between systems.
- Different systems may use different encoding formats for data, so the presentation layer translates the data into a format both systems can understand.
- For example, when sending a video file from one device to another, the presentation layer ensures that the receiving device can interpret the video format correctly.

Example:

- A computer that uses an ASCII encoding system sends data to another computer that uses EBCDIC encoding. The Presentation Layer translates the data from ASCII to EBCDIC, ensuring compatibility between the two systems.

ii. Data Compression:

- Compressing data reduces its size, making it faster to transmit over a network. At the receiving end, the presentation layer decompresses the data so it can be properly used by the application.

- Compression is especially important for multimedia files like videos and images, where large file sizes can slow down transmission.

- **Example**:
    - A video file in MP4 format is compressed before transmission, reducing its size. When the destination device receives the file, the presentation layer decompresses it so the video can be viewed in its original quality.

iii. Data Encryption/Decryption:

- To secure data during transmission, the presentation layer encrypts the data before it is sent and decrypts it upon receipt.

- Encryption is crucial when transmitting sensitive data, such as passwords, financial transactions, or private communications.

Example:

- When you log into a secure website, your password is encrypted by the presentation layer before it is sent over the network. The destination server decrypts it upon arrival to verify your identity.

2D Real-World Examples of Presentation Layer Functions

- **File Formats**: The presentation layer handles different file formats to ensure compatibility between systems.
    - Video formats: Matroska Video (MKV), Motion Picture Experts Group (MPG), QuickTime Video (MOV).
    - Image formats: Graphics Interchange Format (GIF), Joint Photographic Experts Group (JPG), Portable Network Graphics (PNG).

In short, the **Presentation Layer** ensures that data is in the proper format, size, and security level for the application layer to use effectively.

2E. Session Layer (Layer 5 of the OSI Model)

The **Session Layer** is responsible for establishing, managing, and terminating connections (sessions) between two communicating devices. It ensures that communication between two devices is synchronized, organized, and kept active as long as needed. It also helps in recovering communication sessions if interrupted.

Key functions of the Session Layer include:

i. Session Establishment

- Before two devices can start exchanging data, they need to establish a session or connection. The session layer handles this process.

- This process includes setting parameters such as who communicates first and how long the session will last.

Example:

- When you start a video call, the session layer establishes the connection between your device and the other party's device. It defines the rules for communication during the call.

iii. Session Maintenance (Dialog Control)

- The session layer manages the ongoing communication between devices. It ensures that the session remains active and synchronizes data exchange, keeping track of which side is sending or receiving data.
- The session layer can also handle full-duplex or half-duplex communication:
    - **Full-duplex**: Both devices can send and receive data simultaneously.
    - **Half-duplex**: Only one device can send or receive at a time.

Example:

- During a file transfer between two computers, the session layer ensures that both computers can send and receive data in an organized way, either simultaneously or one at a time.

iv. Session Termination

- Once communication is complete, the session layer properly terminates the session, ensuring that all data has been sent and received.
- Terminating the session prevents unnecessary use of network resources and ensures that new sessions can be started cleanly.

Example:

- When you end a video call, the session layer gracefully terminates the connection between both devices.

v. Session Recovery (Re-synchronization)

- If a session is interrupted due to network issues or one of the devices becoming temporarily unresponsive, the session layer can attempt to recover the session and resume communication without having to start over from scratch.

Example:

- If you lose internet connection during a video call, the session layer tries to re-establish the session once the connection is restored, allowing the call to resume where it left off.

2F. Real-World Example of the Session Layer

- **Online Banking**: When you log into an online banking website, a session is established between your browser and the bank's server. The session is maintained while you perform transactions, and it is terminated when you log out or after a period of inactivity.

In short, the **Session Layer** ensures that the communication session between devices is properly established, maintained, and terminated, making sure data flows smoothly and can be recovered if necessary.

In summary:

- The **Presentation Layer** (Layer 6) focuses on data formatting, compression, and encryption, ensuring the data is ready to be used by the application.

- The **Session Layer** (Layer 5) manages the creation, maintenance, and termination of communication sessions, ensuring smooth and organized data exchange between devices.

3. TCP/IP Application Layer Protocols

The TCP/IP application protocols specify the format and control information necessary for many common internet communication functions.

Application layer protocols are **used by both the source and destination** devices during a communication session.

For the communications to be successful, the application layer protocols that are implemented on the source and destination host must be **compatible**.

3A. Name System

i. DNS - Domain Name System (or Service)

- TCP, UDP 53
- Translates domain names, such as cisco.com, into IP addresses.

3B. Host Config

i. BOOTP - Bootstrap Protocol

- UDP client 68, server 67
- Enables a diskless workstation to discover its own IP address, the IP address of a BOOTP server on the network, and a file to be loaded into memory to boot the machine.
- BOOTP is being superseded by DHCP.

ii. DHCP - Dynamic Host Configuration Protocol

- UDP client 68, server 67
- Dynamically assigns IP addresses to be re-used when no longer needed.

3C. Email

i. SMTP - Simple Mail Transfer Protocol

- TCP 25
- Enables clients to send email to a mail server.
- Enables servers to send email to other servers.

ii. POP3 - Post Office Protocol

- TCP 110
- Enables clients to retrieve email from a mail server.
- Downloads the email to the local mail application of the client.

iii. IMAP - Internet Message Access Protocol

- TCP 143
- Enables clients to access email stored on a mail server.
- Maintains email on the server.

3D. File Transfer

i. FTP - File Transfer Protocol

- TCP 20 to 21
- Sets rules that enable a user on one host to access and transfer files to and from another host over a network.
- FTP is a reliable, connection-oriented, and acknowledged file delivery protocol.

ii. TFTP - Trivial File Transfer Protocol

- UDP client 69
- A simple, connectionless file transfer protocol with best-effort, unacknowledged file delivery.
- It uses less overhead than FTP.

3E. Web

i. HTTP - Hypertext Transfer Protocol

- TCP 80, 8080
- A set of rules for exchanging text, graphic images, sound, video, and other multimedia files on the World Wide Web.

ii. HTTPS - HTTP Secure

- TCP, UDP 443
- The browser uses encryption to secure HTTP communications
- Authenticates the website to which you are connecting your browser.

4. Check Your Understanding - Application, Session, Presentation

Check your understanding of the application, presentation, and session layers by choosing the BEST answer to the following questions.

Question 1: This layer of the OSI model is concerned with the protocols that exchange data between programs running on hosts.

(a) application

(b) transport

(c) network

(d) physical

Answer: **(a) -** The application layer of the OSI model is the layer that is closest to the end user. It provides an interface between application protocols and exchanging data between hosts.

Question 2: MKV, GIF, and JPG standards are associated with which OSI layer?

(a) application

(b) presentation

(c) session

(d) transport

Answer: **(b) -** The presentation layer is concerned with formatting and presenting data in a format that is compatible with the destination device. Examples of presentation layer standards are MKV, GIF, JPG, MOV, and PNG.

Question 3: Which two protocols belong in the OSI application layer?

(a) PNG

(b) DNS

(c) SMTP

(d) QuickTime

Answer: **(b & c) -** The application layer of the OSI model provides an interface between applications protocols exchanging data between hosts. Protocols at the application layer include DNS, HTTP, SMTP, FTP, and IMAP.

Question 4: These three OSI layers define the same functions as the TCP/IP model application layer.

(a) application

(b) presentation

(c) session

(d) transport

(e) network

(f) data link

Answer: **(a & b & c) -** The upper three OSI layers; application, presentation, and session, define the application layer functions of the TCP/IP model.

Question 5: This is a function of the OSI session layer.

(a) compress and decompress data

(b) provide an interface between applications

(c) format data for the application layer

(d) exchange of information to initiate dialogue between peers

Answer: **(d) -** The session layer of the OSI model creates and maintains the dialogues, or sessions, between two communicating hosts.

1. Client-Server Model

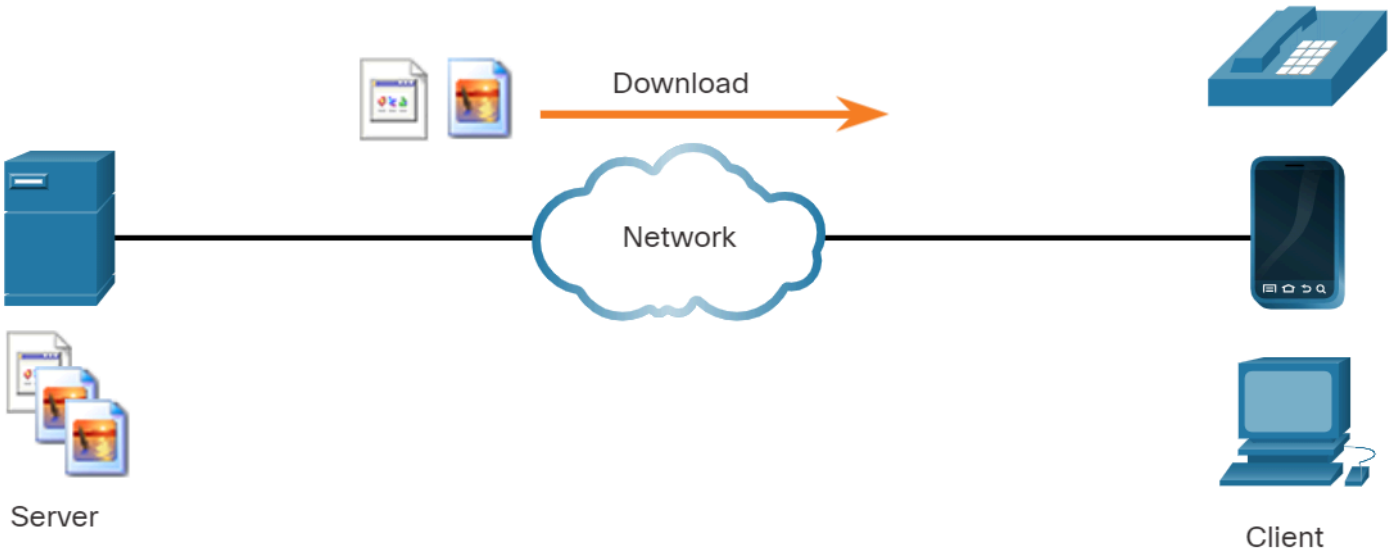
In the previous topic, you learned that TCP/IP application layer protocols implemented on both the source and destination host must be compatible. In this topic, you will learn about the client/server model and the processes used, which are in the application layer. The same is true for a peer-to-peer network. In the client/server model, the device requesting the information is called a client and the device responding to the request is called a server. The client is a hardware/software combination that people use to directly access the resources that are stored on the server.

Client and server processes are considered to be in the application layer. The client begins the exchange by requesting data from the server, which responds by sending one or more streams of data to the client. Application layer protocols describe the format of the requests and responses between clients and servers. In addition to the actual data transfer, this exchange may also require user authentication and the identification of a data file to be transferred.

One example of a client/server network is using the email service of an ISP to send, receive, and store email. The email client on a home computer issues a request to the email server of the ISP for any unread mail.

The server responds by sending the requested email to the client. Data transfer from a client to a server is referred to as an upload and data from a server to a client as a download.

As shown in the figure, files are downloaded from the server to the client.



2. Peer-to-Peer Networks

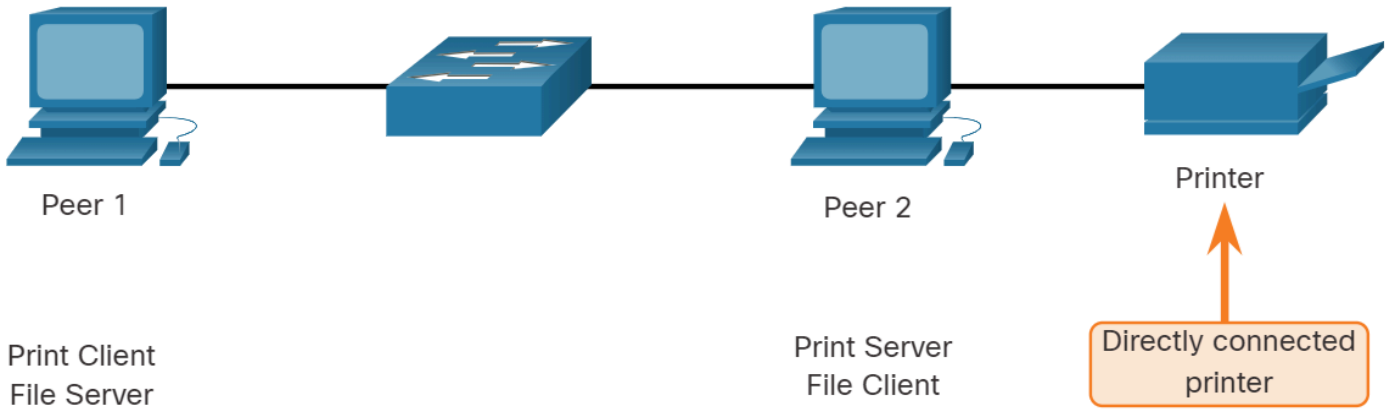
In the peer-to-peer (P2P) networking model, the data is accessed from a peer device without the use of a dedicated server.

The P2P network model involves two parts: P2P networks and P2P applications. Both parts have similar features, but in practice work quite differently.

In a P2P network, two or more computers are connected via a network and can share resources (such as printers and files) without having a dedicated server. Every connected end device (known as a peer) can function as both a server and a client. One computer might assume the role of server for one transaction while simultaneously serving as a client for another. The roles of the client and server are set on a per request basis.

In addition to sharing files, a network such as this one would allow users to enable networked games or share an internet connection.

In a peer-to-peer exchange, both devices are considered equal in the communication process. Peer 1 has files that are shared with Peer 2 and can access the shared printer that is directly connected to Peer 2 to print files. Peer 2 is sharing the directly connected printer with Peer 1 while accessing the shared files on Peer 1, as shown in the figure.

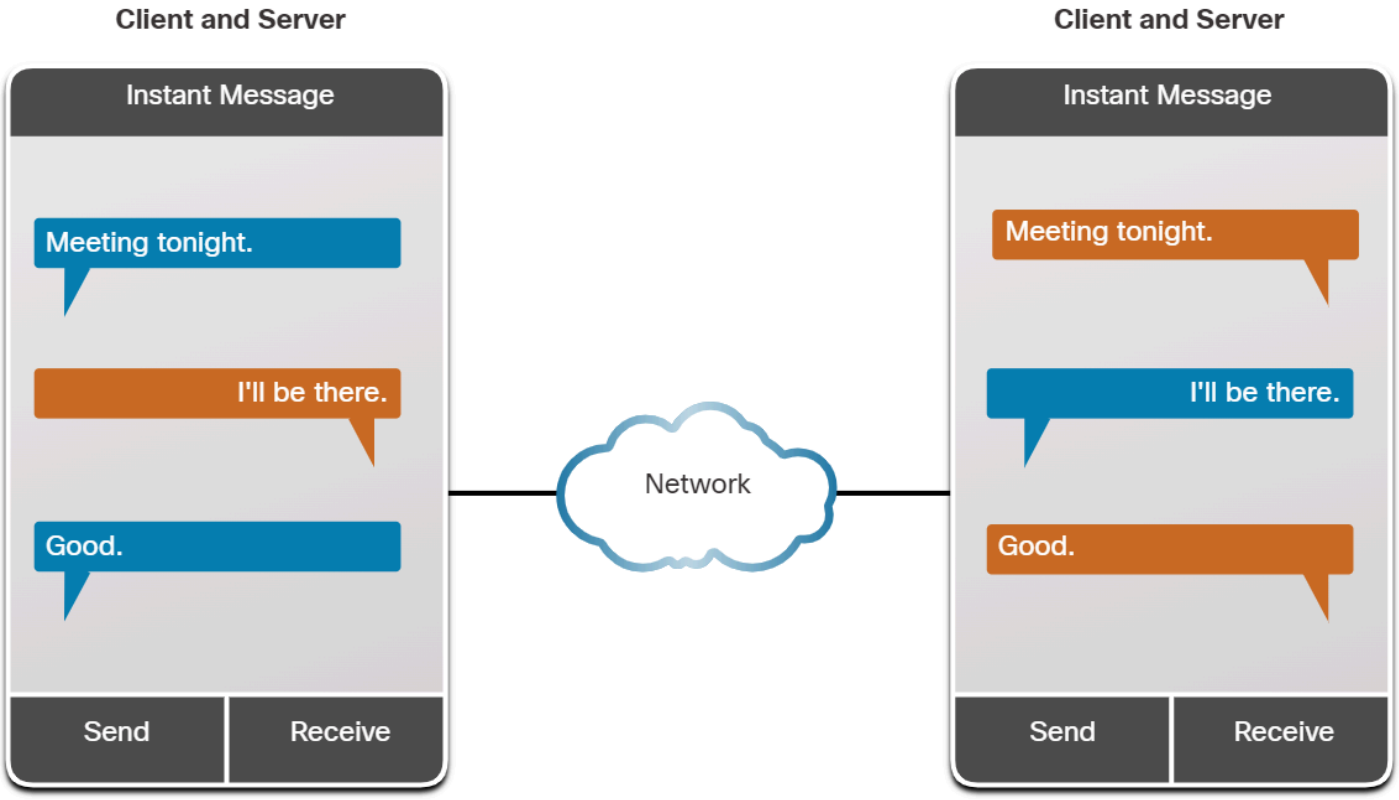


3. Peer-to-Peer Applications

A P2P application allows a device to act as **both a client and a server** within the same communication, as shown in the figure. In this model, every client is a server and every server is a client. P2P applications require that each end device provide a user interface and run a background service.

Some P2P applications use a **hybrid system** where resource sharing is decentralized, but the indexes that point to resource locations are stored in a centralized directory. In a hybrid system, each peer accesses an index server to get the location of a resource stored on another peer.

Both clients simultaneously initiate and receive messages.



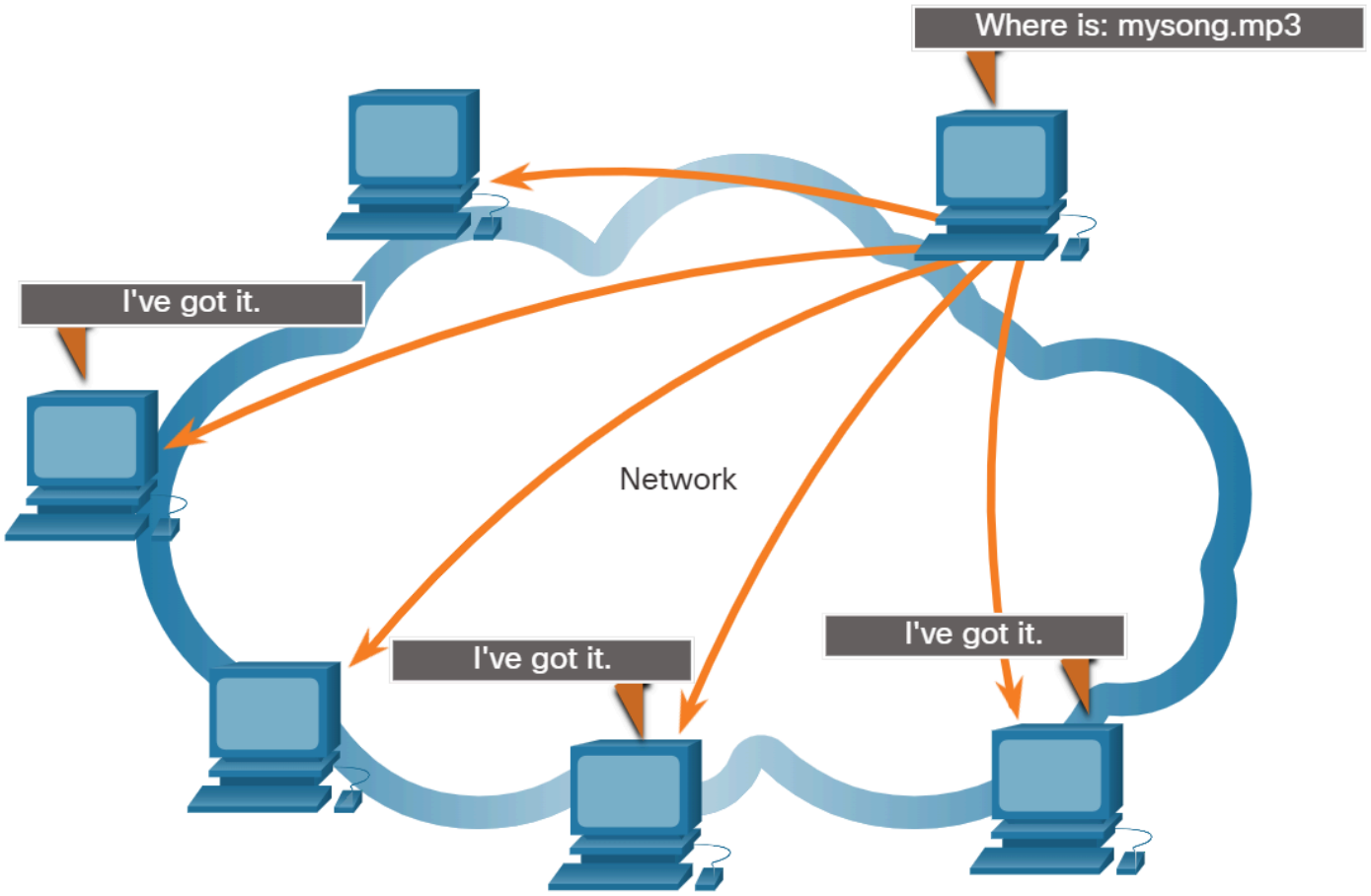
4. Common P2P Applications

With P2P applications, each computer in the network that is running the application can act as a client or a server for the other computers in the network that are also running the application. Common P2P networks include the following:

- BitTorrent
- Direct Connect
- eDonkey
- Freenet

Some P2P applications are based on the Gnutella protocol, where each user shares whole files with other users. As shown in the figure, Gnutella-compatible client software allows users to connect to Gnutella services over the internet, and to locate and access resources shared by other Gnutella peers. Many Gnutella client applications are available, including µTorrent, BitComet, DC++, Deluge, and emule.

Gnutella P2P applications search for shared resources on multiple peers.



Many P2P applications allow users to share pieces of many files with each other at the same time. Clients use a torrent file to locate other users who have pieces that they need so that they can then connect directly to them. This file also contains information about tracker computers that keep track of which users have specific pieces of certain files. Clients ask for pieces from multiple users at the same time. This is known as a swarm and the technology is called BitTorrent. BitTorrent has its own client. But there are many other BitTorrent clients including uTorrent, Deluge, and qBittorrent.

Note: Any type of file can be shared between users. Many of these files are copyrighted, meaning that only the creator has the right to use and distribute them. It is against the law to download or distribute copyrighted files without permission from the copyright holder. Copyright violation can result in criminal charges and civil lawsuits.

5. Check Your Understanding - Peer-to-Peer

Check your understanding of peer-to-peer by choosing the BEST answer to the following questions.

Question 1: True or false? The peer-to-peer networking model requires the implementation of a dedicated server for data access.

(a) True

(b) False

Answer: **(b) -** The correct answer is False. In the peer-to-peer model, clients can share resources without using a dedicated server.

Question 2: True or false? In a peer-to-peer network environment, every peer can function as both a client and a server.

(a) True

(b) False

Answer: **(a) -** The correct answer is True. A peer-to-peer network does not require a dedicated server because each peer can function as both a client and as a server.

Question 3: Which peer-to-peer application allows users to share pieces of many files with each other at the same time?

(a) Hybrid

(b) Gnutella

(c) BitTorrent

Answer: **(c) -** BitTorrent clients use a torrent file to locate other clients that are sharing pieces of needed files. In this way, many files can be shared between clients at the same time.

Question 4: Which of the following is a feature of the Gnutella protocol?

(a) Users can share whole files with other users.

(b) Users can share pieces of files with other users.

(c) Users can access an index server to get the location of resources shared by other users.

Answer: **(a) -** Gnutella is a peer-to-peer protocol that allows users to share whole files with other users.

Web and Email Protocols

1. Hypertext Transfer Protocol and Hypertext Markup Language

There are application layer-specific protocols that are designed for common uses such as web browsing and email. The first topic gave you an overview of these protocols. This topic goes into more detail.

When a web address or **Uniform Resource Locator (URL)** is typed into a web **browser**, the web browser establishes a **connection** to the web service. The web service is running on the server that is using the **HTTP protocol**. URLs and Uniform Resource Identifiers (URIs) are the names most people associate with web addresses.

To better understand how the web browser and web server interact, examine how a web page is opened in a browser. For this example, use the http://www.cisco.com/index.html URL.

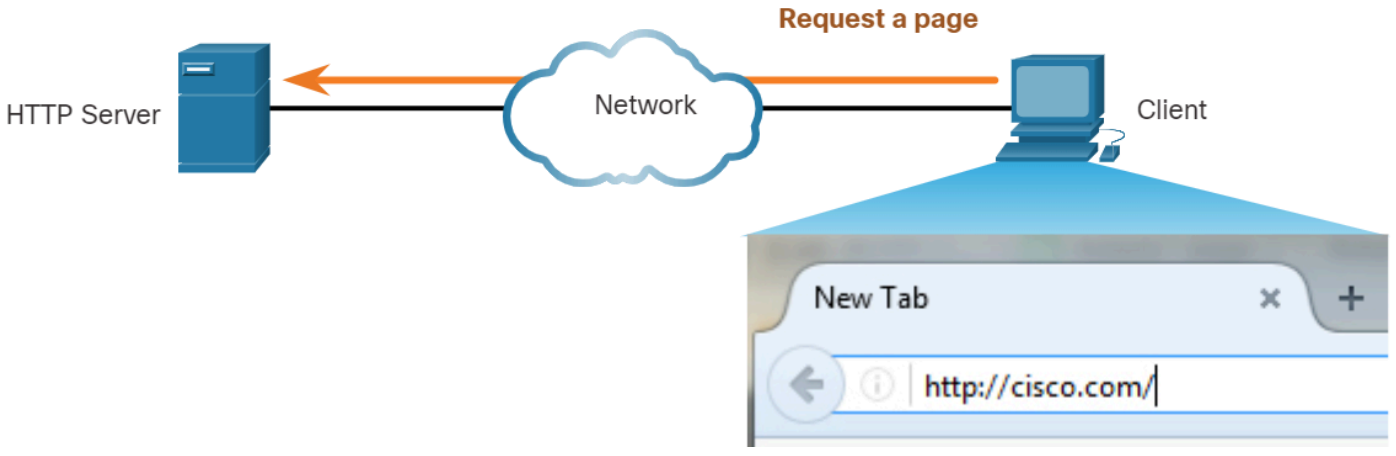
Step 1

The browser interprets the three parts of the URL:

- http (the protocol or scheme)
- www.cisco.com (the server name)
- index.html (the specific filename requested)

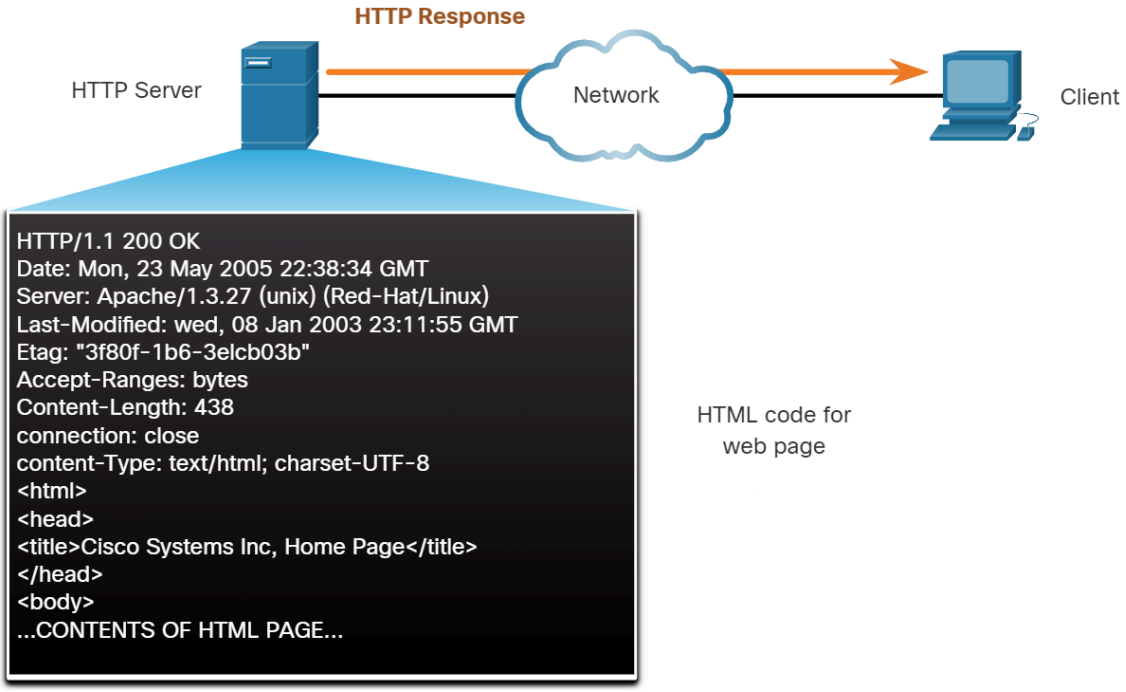
Step 2

- The browser then checks with a name server to convert www.cisco.com into a numeric IP address, which it uses to connect to the server. The client initiates an HTTP **request** to a server by sending a **GET** request to the server and asks for the index.html file.



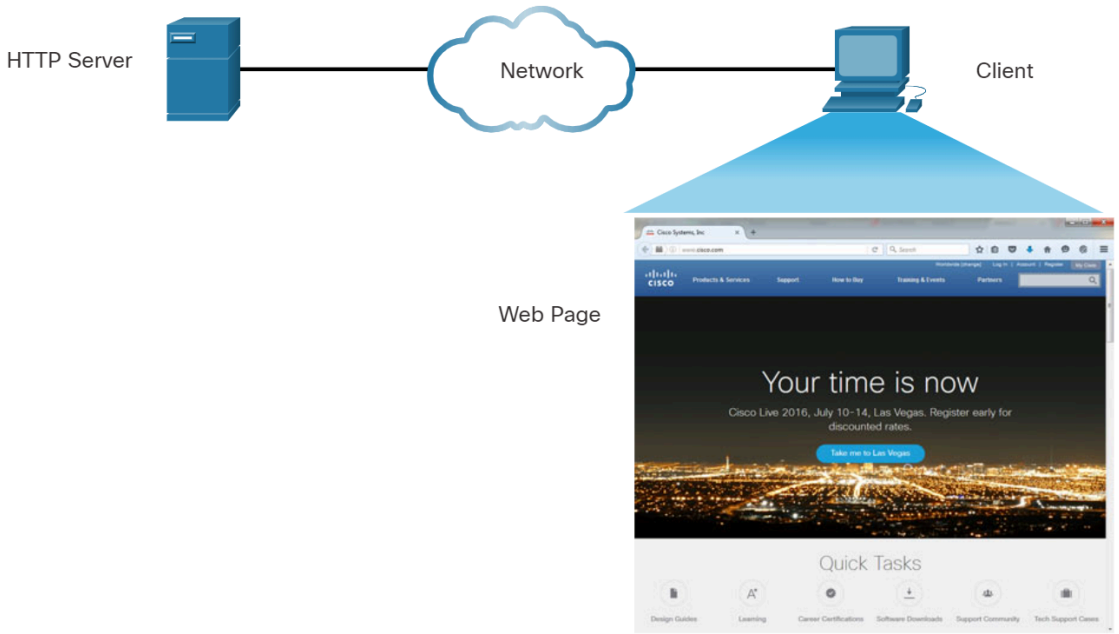
Step 3

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



Step 4

The browser **deciphers the HTML code** and formats the page for the browser window.

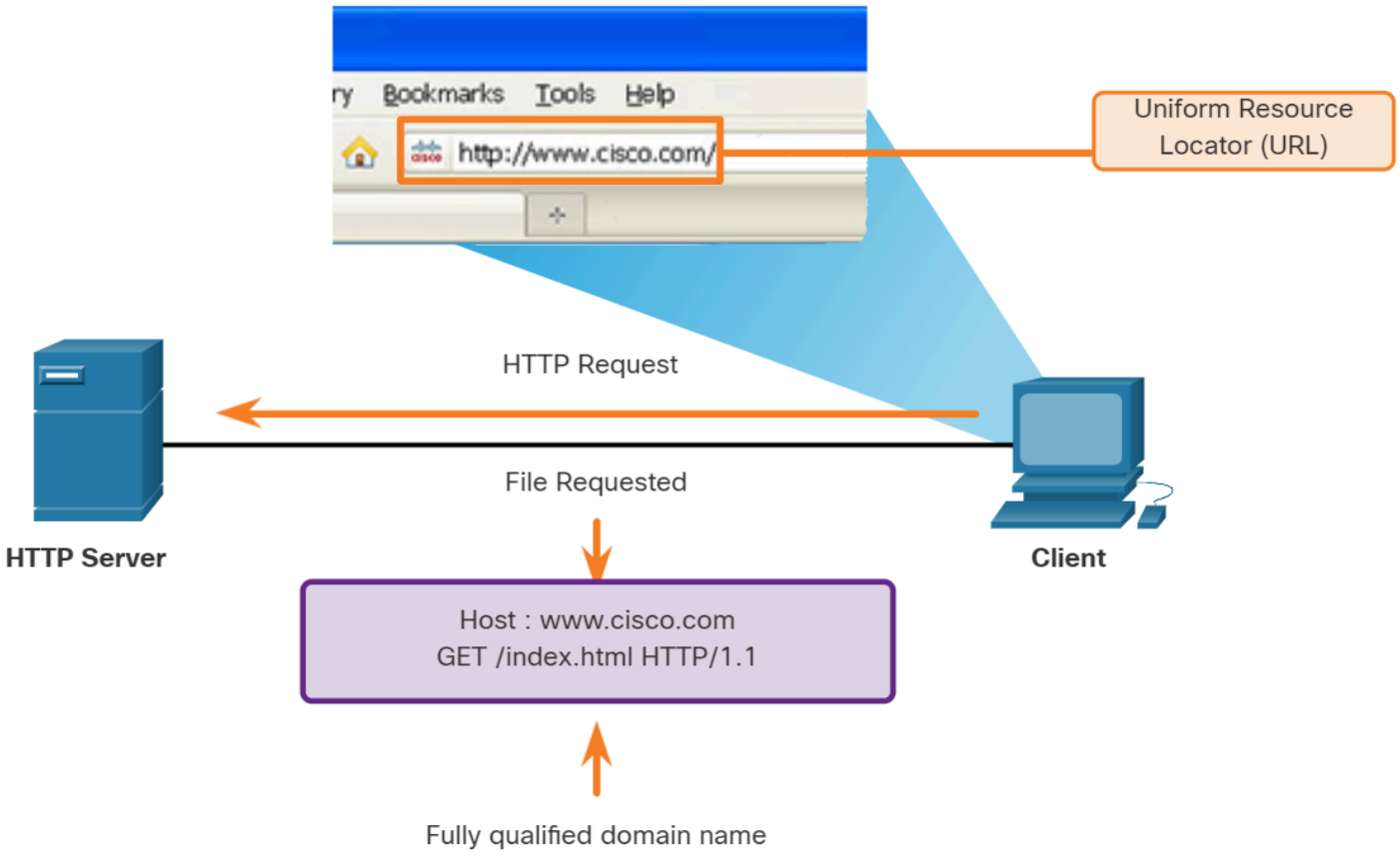


2. HTTP and HTTPS

HTTP is a request/response protocol. When a client, typically a web browser, sends a request to a web server, HTTP specifies the message types used for that communication. The **three** common message types are GET (see figure), POST, and PUT:

- **GET** - This is a client **request** for data. A client (web browser) sends the GET message to the webserver to request HTML pages.
- **POST** - This **uploads data files** to the web server, such as form data.
- **PUT** - This **uploads** resources or **content to the web** server, such as an image.

The figure depicts a client performing an HTTP request to an HTTP server. The file requested is a Fully Qualified Domain Name. The request uses a Get to retrieve the web page. The URL field is shown on the client computer as a http://www.cisco.com request.



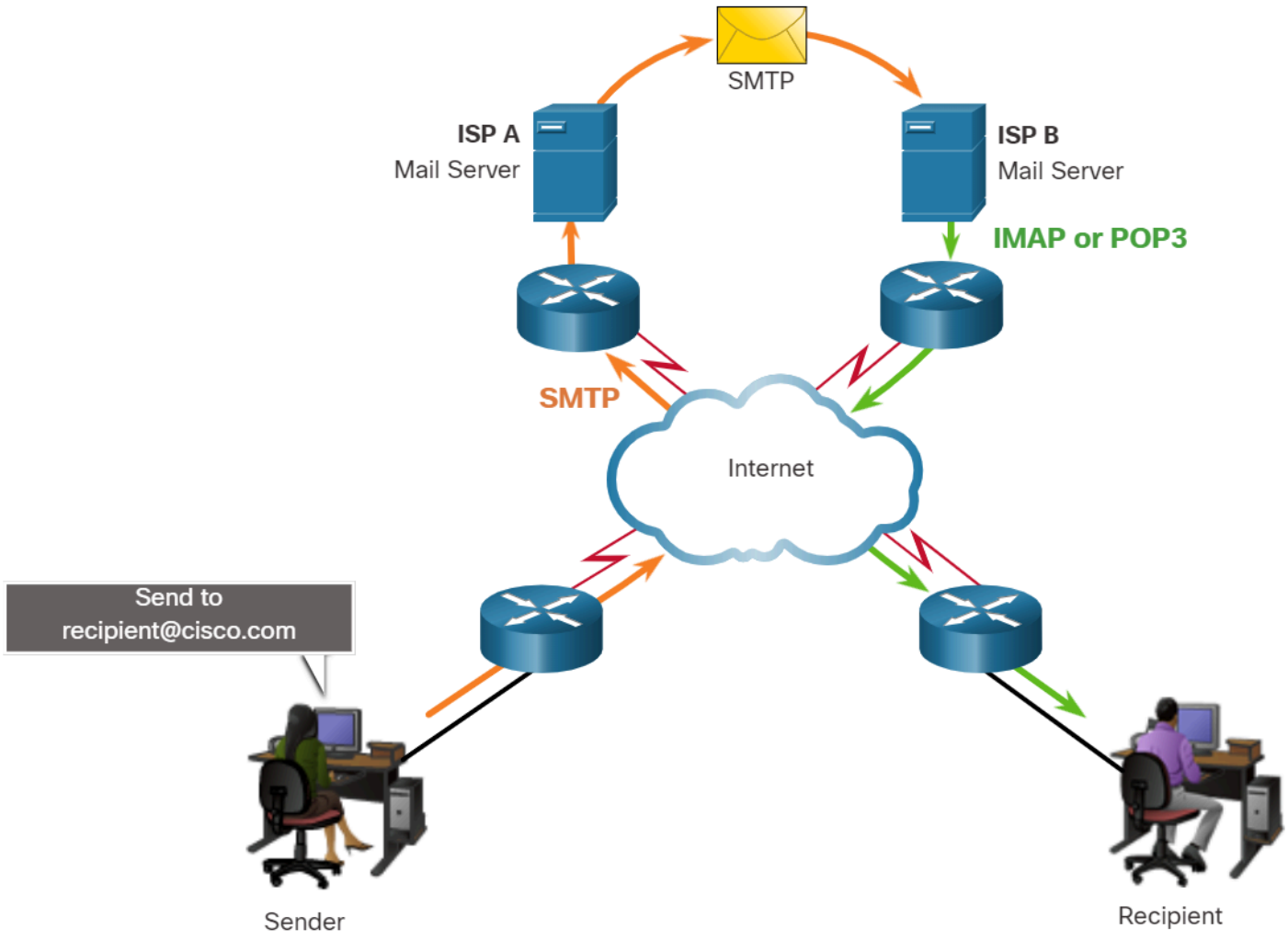
Although HTTP is remarkably flexible, it is not a secure protocol. The request messages send information to the server in plaintext that can be intercepted and read. The server responses, typically HTML pages, are also unencrypted.

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 server. HTTPS uses the same client request-server response process as HTTP, but the data stream is encrypted with Transport Layer Security (TLS) or its predecessor Secure Socket Layer (SSL) before being transported across the network.

3. Email Protocols

One of the primary services offered by an ISP is email hosting. To run on a computer or other end device, email requires several applications and services, as shown in the figure. Email is a **store-and-forward** method of sending, storing, and retrieving electronic messages across a network. Email messages are **stored** in databases on mail **servers**.

The figure depicts an email transaction from a sender using the SMTP protocol sending an email to recipient@cisco.com through an ISP mail server A arriving at the recipient's ISP mail server B and the recipient reading the email using either an IMAP or POP protocol.



Email clients communicate with mail servers to send and receive email. Mail servers communicate with other mail servers to transport messages from one domain to another. An email client does not communicate directly with another email client when sending the email. Instead, both clients rely on the mail server to transport messages.

Email supports three separate **protocols** for operation: Simple Mail Transfer Protocol (SMTP), Post Office Protocol (POP), and IMAP. The application layer process that sends mail uses SMTP. A client retrieves email using one of the two application layer protocols: POP or IMAP.

4. SMTP, POP, and IMAP

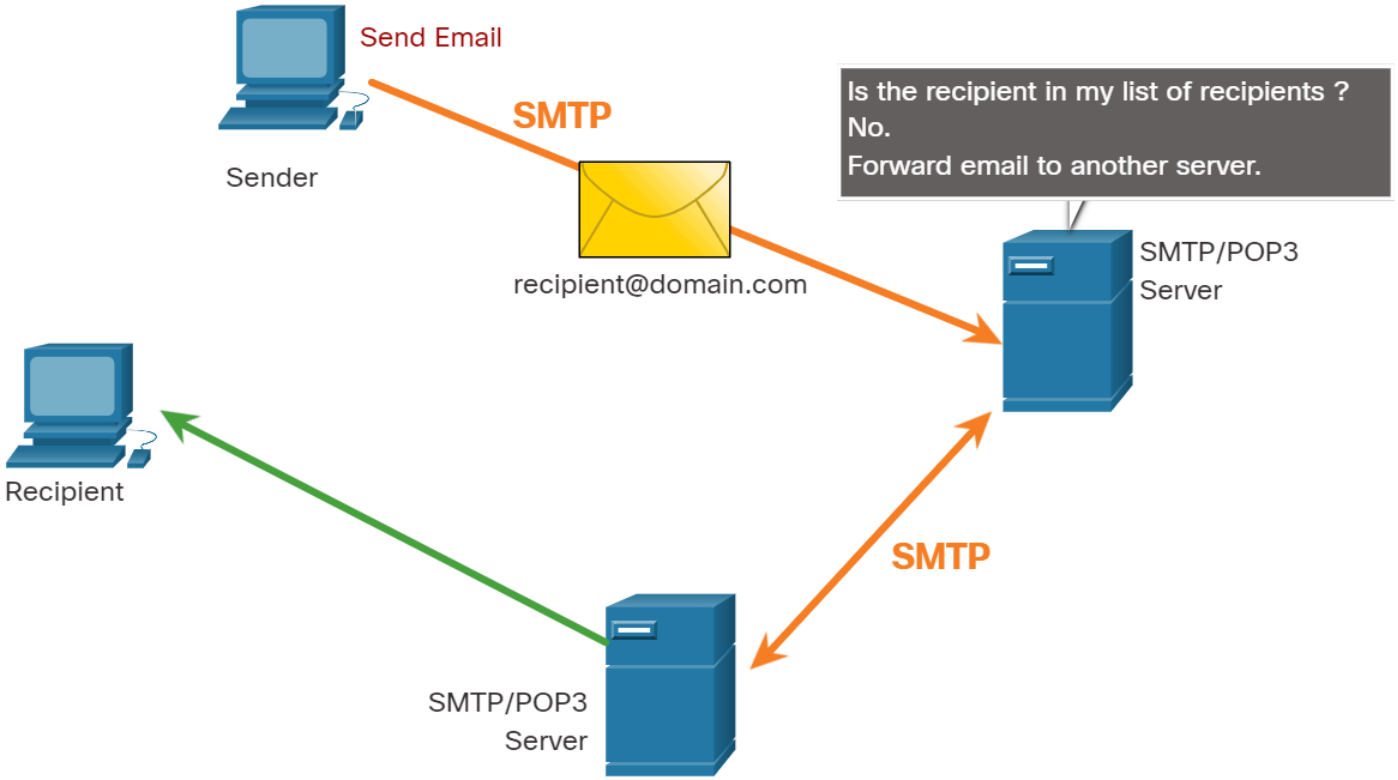
4A. SMTP

SMTP message formats require a message header and a message body. Although the message body can contain any amount of text, the message header must have a properly formatted recipient email address and a sender address.

When a client sends an email, the client SMTP process connects with a server SMTP process on well-known 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.

The destination email server may not be online or maybe busy when email messages are sent. Therefore, SMTP **spools** messages to be sent at a later time. 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.

This is a figure with a sender computer and a recipient computer. Two SMTP/POP3 servers are connected between the two. A mail message is sent from the sender's computer labeled recipient@domain.com using SMTP protocol. The first SMTP/POP3 receives the message from the sender and asks Is the recipient in my list of recipients? No. forward the email to another server. The second SMTP/POP3 server receives the message via the SMTP protocol and forwards the message to the recipient.



4B. POP

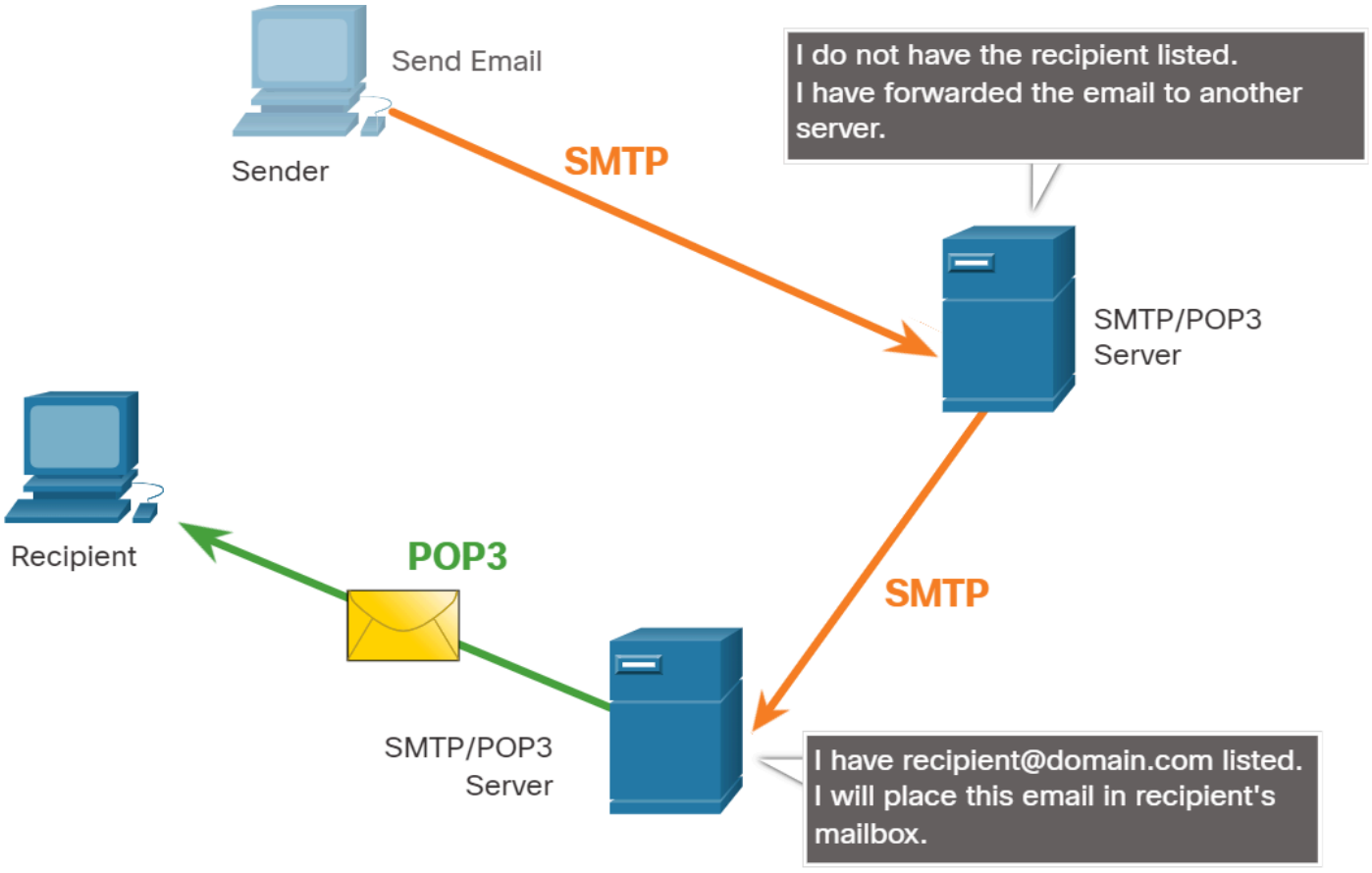
POP is used by an application to **retrieve** mail from a mail server. With POP, mail is downloaded from the server to the client and then **deleted** on the server. This is the default operation of POP.

The server starts the POP service by passively listening on TCP port **110** for client connection requests. When a client wants to make use of the service, it sends a **request** to establish a TCP connection with the server, as shown in the figure. When the connection is established, the **POP server sends a greeting**. The client and POP server then **exchange commands** and responses until the connection is closed or aborted.

With POP, email messages are downloaded to the client and removed from the server, so there is no centralized location where email messages are kept. Because **POP does not store messages**, it is not recommended for a small business that needs a centralized backup solution.

POP3 is the most commonly used version.

This is a figure with a sender computer and a recipient computer. Two SMTP/POP3 servers are connected between the two. A mail message is sent from the sender's computer labeled recipient@domain.com using SMTP protocol. The first SMTP/POP3 receives the message from the sender and asks Is the recipient in my list of recipients? No. forward the email to another server. The second SMTP/POP3 server receives the message via the SMTP protocol and states I have recipient@domain.com listed I will place this email in the recipients mailbox The recipient then reads the message using the POP3 protocol.

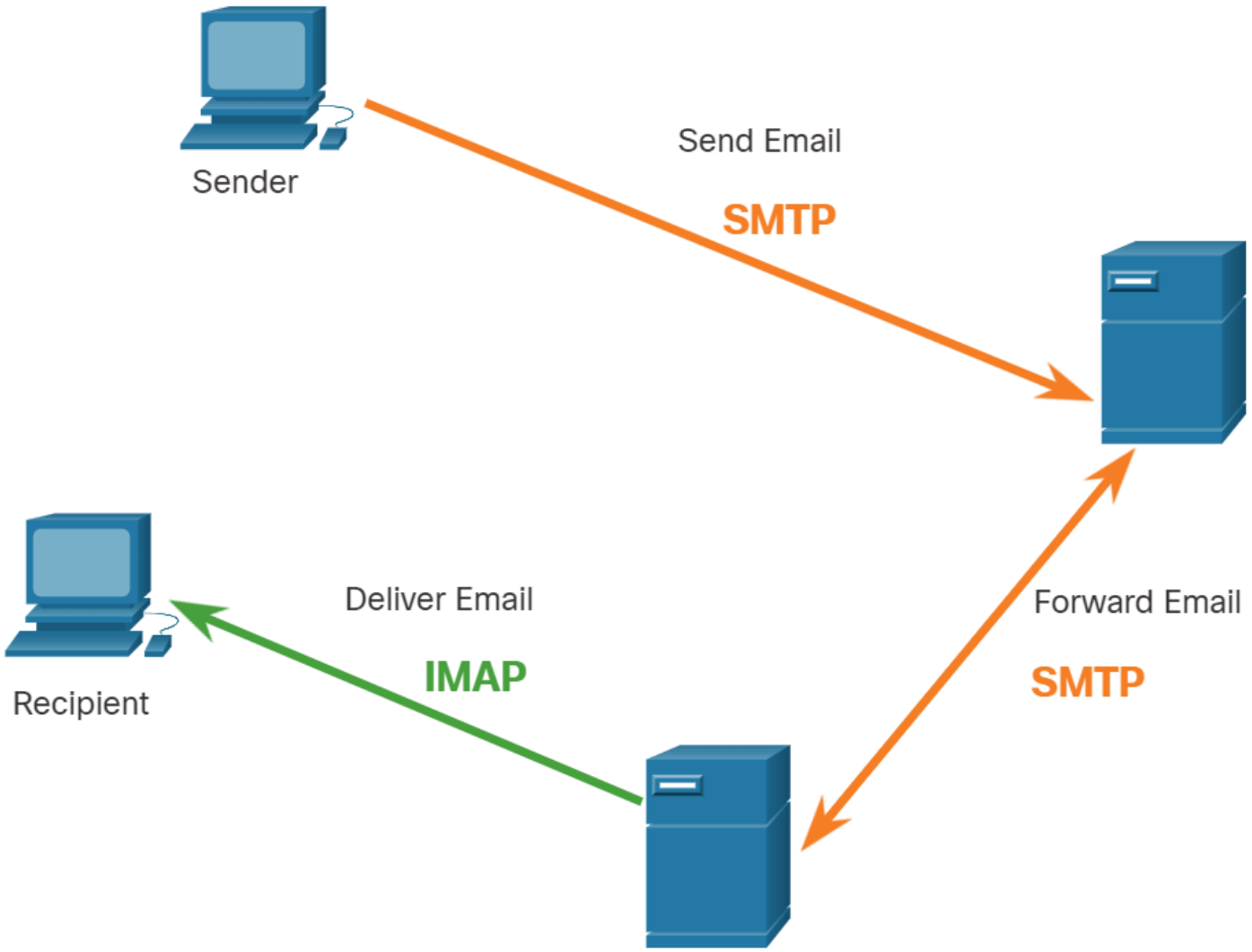


4C. IMAP

IMAP is another protocol that describes a method to retrieve email messages. Unlike POP, when the user connects to an IMAP-capable server, **copies** of the messages are downloaded to the client application, as shown in the figure. 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. That file structure is duplicated on the email client as well. When a user decides to delete a message, the server synchronizes that action and deletes the message from the server.

This is a figure with a sender computer and a recipient computer. Two SMTP/POP3 servers are connected between the two. The client computer uses the SMTP protocol to send a message through the two servers and the recipient computer receives the email via IMAP protocol.



5. Check Your Understanding - Web and Email Protocols

Check your understanding of web and email protocols by choosing the BEST answer to the following questions.

Question 1: This message type is used when uploading data files to a web server.

(a) GET

(b) POST

(c) PUT

Answer: **(b) -** HTTP uses the POST message to upload data files to a web server. The GET message is used by clients to request data and the PUT message is used to upload content such as images.

Question 2: This protocol is used by a web browser to establish a connection to a web server.

(a) HTTP

(b) SSL

(c) IMAP

(d) SMTP

Answer: **(a) -** Web browsers connect to web servers over HTTP. IMAP and SMTP are email protocols. SSL is an encryption protocol used with HTTPS.

Question 3: This protocol is used by a client to send emails to a mail server.

(a) POP

(b) SMTP

(c) IMAP

(d) HTTP

Answer: **(b) -** Email clients connect to SMTP servers over port 25 to send email. POP and IMAP are used by clients to receive email. HTTP is used between web browsers and web servers.

Question 4: Which is a feature of IMAP?

(a) It uploads email messages to a server.

(b) It listens passively on port 110 for client requests.

(c) It downloads a copy of email messages leaving the original on the server.

Answer: **(c) -** IMAP is a protocol for clients to retrieve copies of email messages from an IMAP server. The original messages remain on the server until manually deleted.

Question 5: True or false? HTTP is a secure protocol.

(a) True

(b) False

Answer: **(b) -** The correct answer is False. HTTP sends information in plaintext and is not considered secure. If security is desired, HTTP Secure (HTTPS) should be used.

IP Addressing Services

1. Domain Name System

There are other application layer-specific protocols that were designed to make it easier to obtain addresses for network devices. These services are essential because it would be very time-consuming to remember IP addresses instead of URLs or manually configure all of the devices in a medium to large network. The first topic in this module gave you an overview of these protocols. This topic goes into more detail about the IP addressing services, DNS and DHCP.

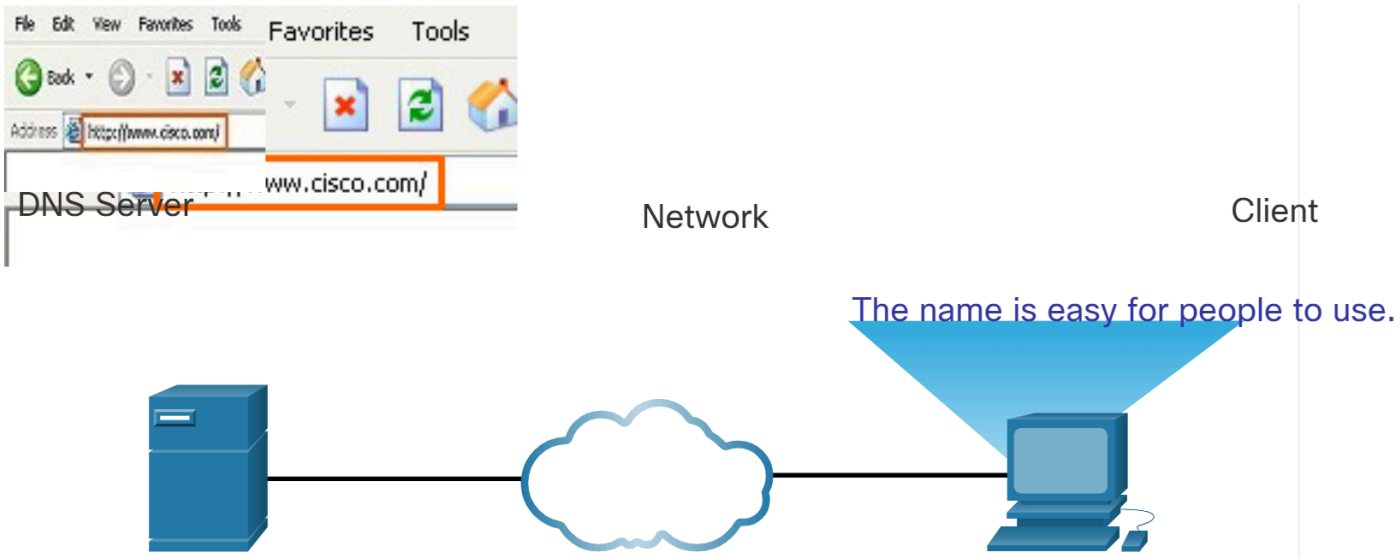
In data networks, devices are labeled with **numeric IP addresses** to send and receive data over networks. Domain names were created to convert the numeric address into a simple, recognizable name.

On the internet, fully-qualified domain names (FQDNs), such as http://www.cisco.com, are much **easier for people to remember** than 198.133.219.25, which is the actual numeric address for this server. If Cisco decides to change the numeric address of www.cisco.com, it is transparent to the user because the domain name remains the same. The new address is simply linked to the existing domain name and connectivity is maintained.

The DNS protocol defines an automated service that matches resource names with the required numeric network address. It includes the format for queries, responses, and data. The DNS protocol communications use a single format called a message. This message format is used for all types of client queries and server responses, error messages, and the transfer of resource record information between servers.

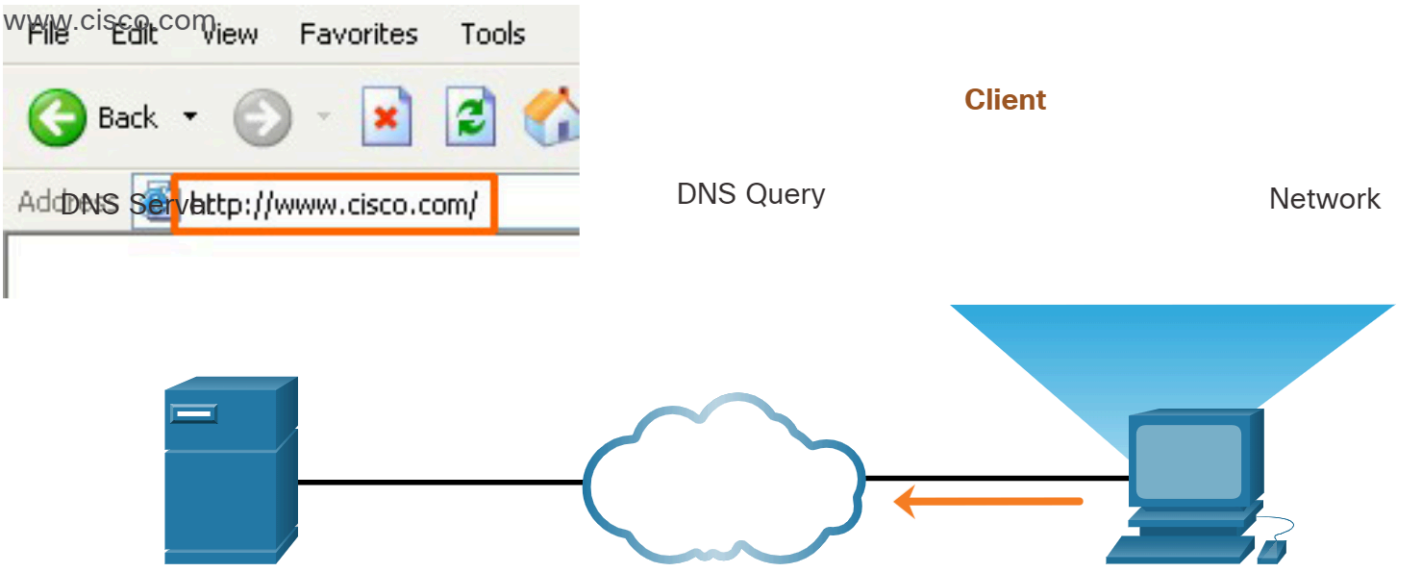
1A. Step 1

- The user types an FQDN into a browser application Address field.
- This is a figure with a client contacting a DNS server through the network with an FQDN typed in a browser URL field because the name of a website is easier for people to use.



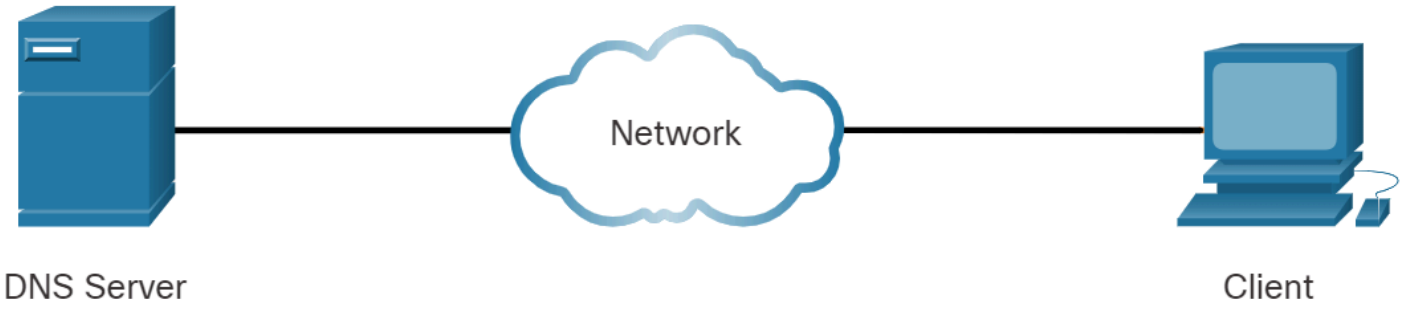
1B. Step 2

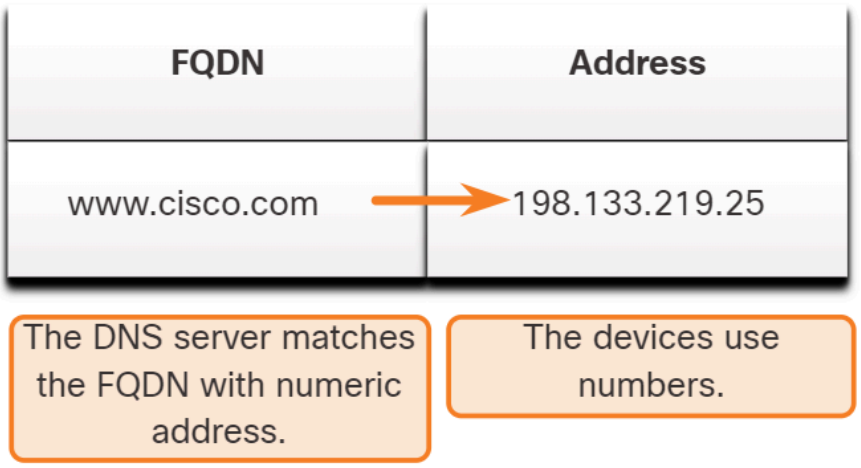
- A DNS query is sent to the designated DNS server for the client computer.
- This is a figure with a client sending a DNS query message to the DNS server for the URL www.cisco.com



1C. Step 3

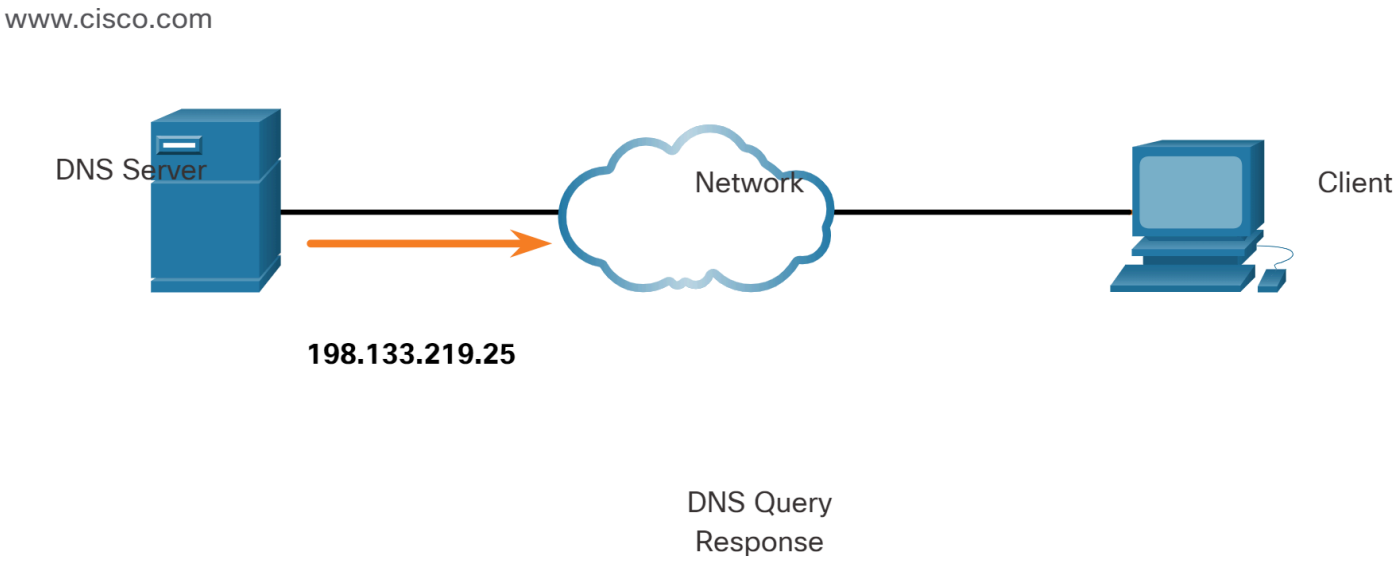
- The DNS server matches the FQDN with its IP address.
- This is a figure depicting the DNS server responding to the FQDN with the IP version 4 of the address of the website to the client computer.





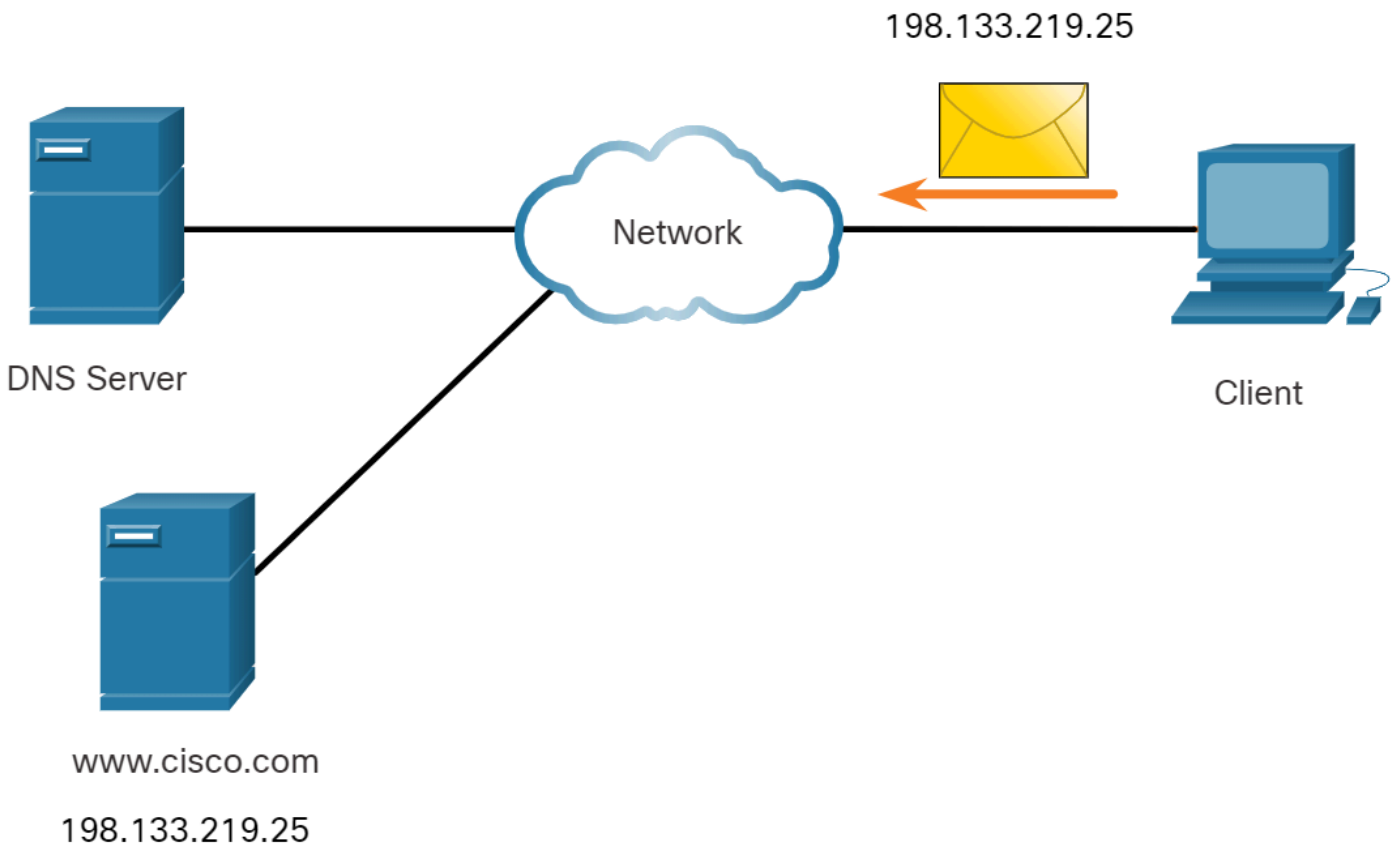
Step 4

- The DNS query response is sent back to the client with the IP address for the FQDN.
- This is a figure showing the DNS Query response message returning to the client computer with the FQDN and its IP version 4 address



Step 5

- The client computer uses the IP address to make requests to the server.
- this is a figure with the client computer using the IP version 4 address to contact the www.cisco.com server thru the network.



2. DNS Message Format

The DNS server **stores different types** of resource records that are used to resolve names. These records contain the name, address, and type of record. Some of these record types are as follows:

- **A** - An end device IPv4 address
- **NS** - An authoritative name server
- **AAAA** - An end device IPv6 address (pronounced quad-A)
- **MX** - A mail exchange record

When a client makes a query, the server DNS process first looks at its **own records** to resolve the name. If it is unable to resolve the name by using its stored records, it **contacts other servers** to resolve the name. After a match is found and returned to the original requesting server, the server temporarily stores the numbered address in the event that the same name is requested again.

The DNS client service on Windows PCs also stores previously resolved names in memory. The **ipconfig /displaydns** command displays all of the cached DNS entries.

As shown in the table, DNS uses the same message format between servers, consisting of a question, answer, authority, and additional information 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 **name server**
Answer	Resource Records **answering the question**
Authority	Resource Records pointing toward an **authority**
Additional	Resource Records holding **additional information**

3. DNS Hierarchy

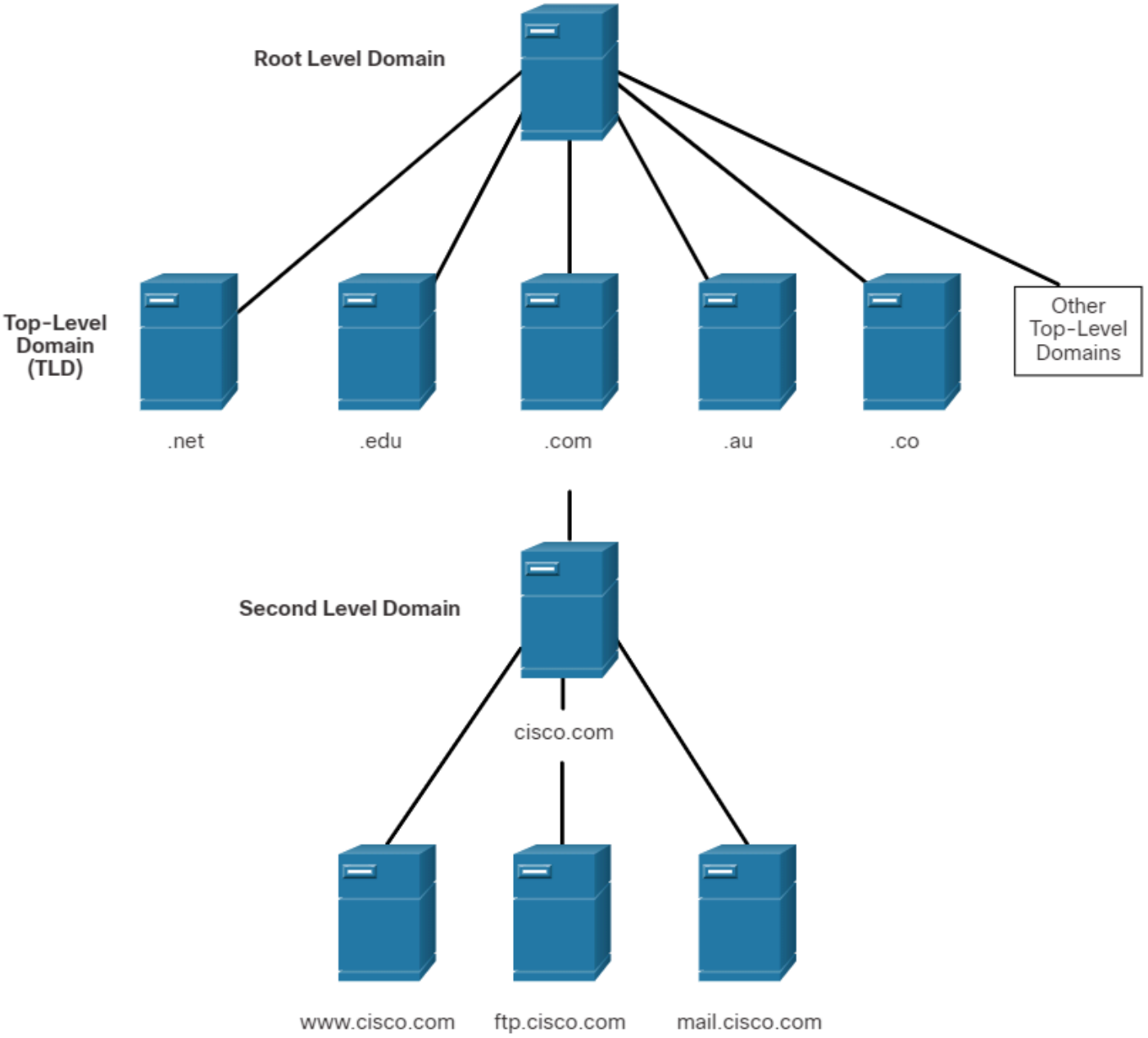
The DNS protocol uses a hierarchical system to create a database to provide name resolution, as shown in the figure. DNS uses domain names to form the hierarchy.

The naming structure is broken down into small, manageable zones. Each DNS server maintains a specific database file and is only responsible for managing name-to-IP mappings for that small portion of the entire DNS structure. When a DNS server receives a request for a name translation that is not within its DNS zone, the DNS server forwards the request to another DNS server within the proper zone for translation. DNS is scalable because hostname resolution is spread across multiple servers.

The different top-level domains represent either the type of organization or the country of origin. Examples of top-level domains are the following:

- **.com** - a business or industry
- **.org** - a non-profit organization
- **.au** - Australia
- **.co** - Colombia

The figure shows the DNS Hierachy tree. At the top is the Root Level Domain with the TOp-Level Domains(TLD) connected undererneath the Root Level Domainmain. The TLDs are .net, .edu, .com,.au, .co, and other top-level domains. Under the .com TLD is the Second Level domain www.cisco.com and under cisco.com are www.cisco.com, ftp.cisco.com, and mail.cisco.com.


Root Level Domain
Top-Level Domain (TLD)
.net
.edu
.com
.au
.co
Other Top-Level Domains
Second Level Domain
cisco.com
www.cisco.com
ftp.cisco.com
mail.cisco.com

4. The nslookup Command

When configuring a network device, one or more DNS Server addresses are provided that the DNS client can use for name resolution. Usually, the ISP provides the addresses to use for the DNS servers. When a user application requests to connect to a remote device by name, the requesting DNS client queries the name server to resolve the name to a numeric address.

Computer operating systems also have a utility called Nslookup that allows the user to manually query the name servers to resolve a given host name. This utility can also be used to troubleshoot name resolution issues and to verify the current status of the name servers.

In this figure, when the nslookup command is issued, the default DNS server configured for your host is displayed. The name of a host or domain can be entered at the nslookup prompt. The Nslookup utility has many options available for extensive testing and verification of the DNS process.

```
C:\Users> nslookup
Default Server:  dns-sj.cisco.com
Address:  171.70.168.183

> www.cisco.com
Server:  dns-sj.cisco.com
Address:  171.70.168.183
Name:    origin-www.cisco.com
Addresses:  2001:420:1101:1::a
          173.37.145.84
Aliases:  www.cisco.com

> cisco.netacad.net
Server:  dns-sj.cisco.com
Address:  171.70.168.183
Name:    cisco.netacad.net
Address:  72.163.6.223

>
```

5. Syntax Checker - The nslookup Command

Practice entering the nslookup command in both Windows and Linux

From the Windows command prompt, enter the nslookup command to begin a manual query of the name servers.

```
C:\>nslookup
Default Server: Unknown
Address: 10.10.10.1
```

The output lists the name and IP address of the DNS server configured in the client. Note that the DNS server address can be manually configured, or dynamically learned, through DHCP. You are now in nslookup mode. Enter the domain name www.cisco.com.

```
>www.cisco.com
Server:  UnKnown
Address:  10.10.10.1
Non-authoritative answer:
Name:    e2867.dsca.akamaiedge.net
Addresses:  2600:1404:a:395::b33
          2600:1404:a:38e::b33
          172.230.155.162
Aliases:  www.cisco.com
          www.cisco.com.akadns.net
          wwwds.cisco.com.edgekey.net
          wwwds.cisco.com.edgekey.net.globalredir.akadns.net
```

The output lists IP addresses related to www.cisco.com that the server 'e2867' currently has in its database. Notice that IPv6 addresses are also listed. In addition, various aliases are shown that will resolve to www.cisco.com.

Enter the exit command to leave nslookup mode and return to the Windows command line.

```
>exit
```

You can directly query the DNS servers by simply adding the domain name to the nslookup command. Enter nslookup www.google.com.

```
C:\>nslookup www.google.com
Server:  UnKnown
```

```
Address:  10.10.10.1
Non-authoritative answer:
Name:    www.google.com
Addresses:  2607:f8b0:4000:80f::2004
          172.217.12.36


========================================
```

You are now working from the Linux command prompt. The nslookup command is the same.

- Enter the nslookup command to begin a manual query of the name servers.
- Enter www.cisco.com at the > prompt.
- Enter the exit command to leave nslookup mode and return to the Linux command line.

```
user@cisconetacad$nslookup
Server: 127.0.1.1
Address: 127.0.1.1#53
>www.cisco.com
Non-authoritative answer:
www.cisco.com canonical name = www.cisco.com.akadns.net.
www.cisco.com.akadns.net canonical name = wwwds.cisco.com.edgekey.net.
wwwds.cisco.com.edgekey.net canonical name = wwwds.cisco.com.edgekey.net.globalredir.akadns.net.
wwwds.cisco.com.edgekey.net.globalredir.akadns.net canonical name = e144.dscb.akamaiedge.net.
Name: e144.dscb.akamaiedge.net
Address: 23.60.112.170
>exit
```

As in Windows, you can directly query the DNS servers by simply adding the domain name to the nslookup command. Enter nslookup www.google.com.

```
user@cisconetacad$nslookup www.google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name: www.google.com
```

```
Address: 172.217.6.164
Name: www.google.com
Address: 2607:f8b0:4000:812::2004
```

You successfully used the nslookup command to verify the status of domain names.

6. Dynamic Host Configuration Protocol

The Dynamic Host Configuration Protocol (DHCP) for IPv4 service automates the assignment of IPv4 addresses, subnet masks, gateways, and other IPv4 networking parameters. This is referred to as dynamic addressing. The alternative to dynamic addressing is static addressing. When using static addressing, the network administrator manually enters IP address information on hosts.

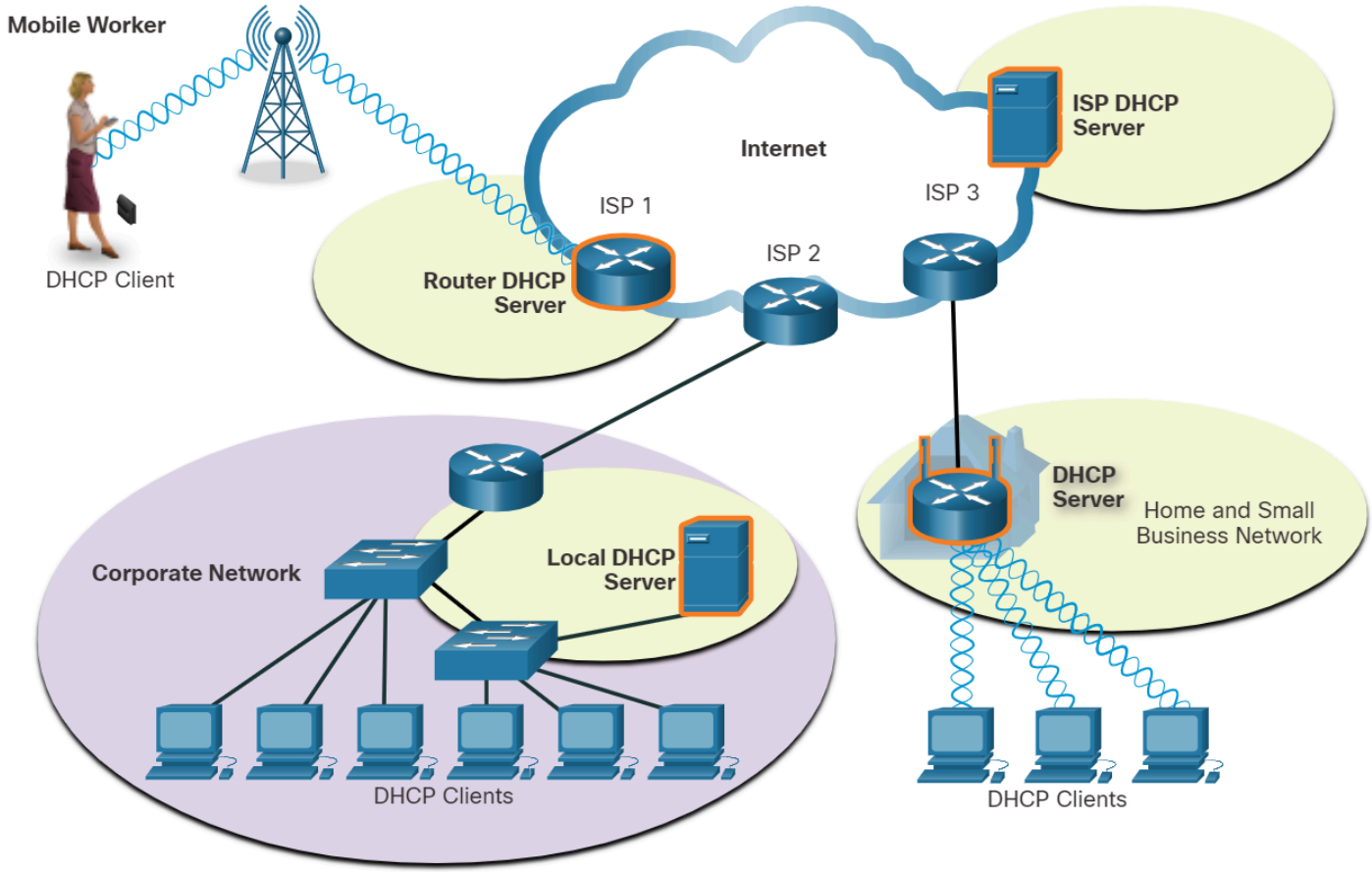
When a host connects to the network, the DHCP server is contacted, and an address is requested. The DHCP server chooses an address from a configured range of addresses called a pool and assigns (leases) it to the host.

On larger networks, or where the user population changes frequently, DHCP is preferred for address assignment. New users may arrive and need connections; others may have new computers that must be connected. Rather than use static addressing for each connection, it is more efficient to have IPv4 addresses assigned automatically using DHCP.

DHCP can allocate IP addresses for a configurable period of time, called a lease period. The lease period is an important DHCP setting, When the lease period expires or the DHCP server gets a DHCPRELEASE message the address is returned to the DHCP pool for reuse. Users can freely move from location to location and easily re-establish network connections through DHCP.

As the figure shows, various types of devices can be DHCP servers. The DHCP server in most medium-to-large networks is usually a local, dedicated PC-based server. With home networks, the DHCP server is usually located on the local router that connects the home network to the ISP.

The figure depicts an ISP DHCP server connected to the Internet with three ISP routers labelled ISP1, ISP2, and ISP3. Each ISP router is connected to a different network. ISP1 connects to a wireless antenna to a mobile worker who is the DCHP client. ISP2 is connected to a corporate network router which connects to a corporate LAN with its own local DHCP server connected to a swith connected to six DHCP clients. ISP3 is connected to a wireless DHCP server for a Home and Small Business network the three DHCP clients are connected.



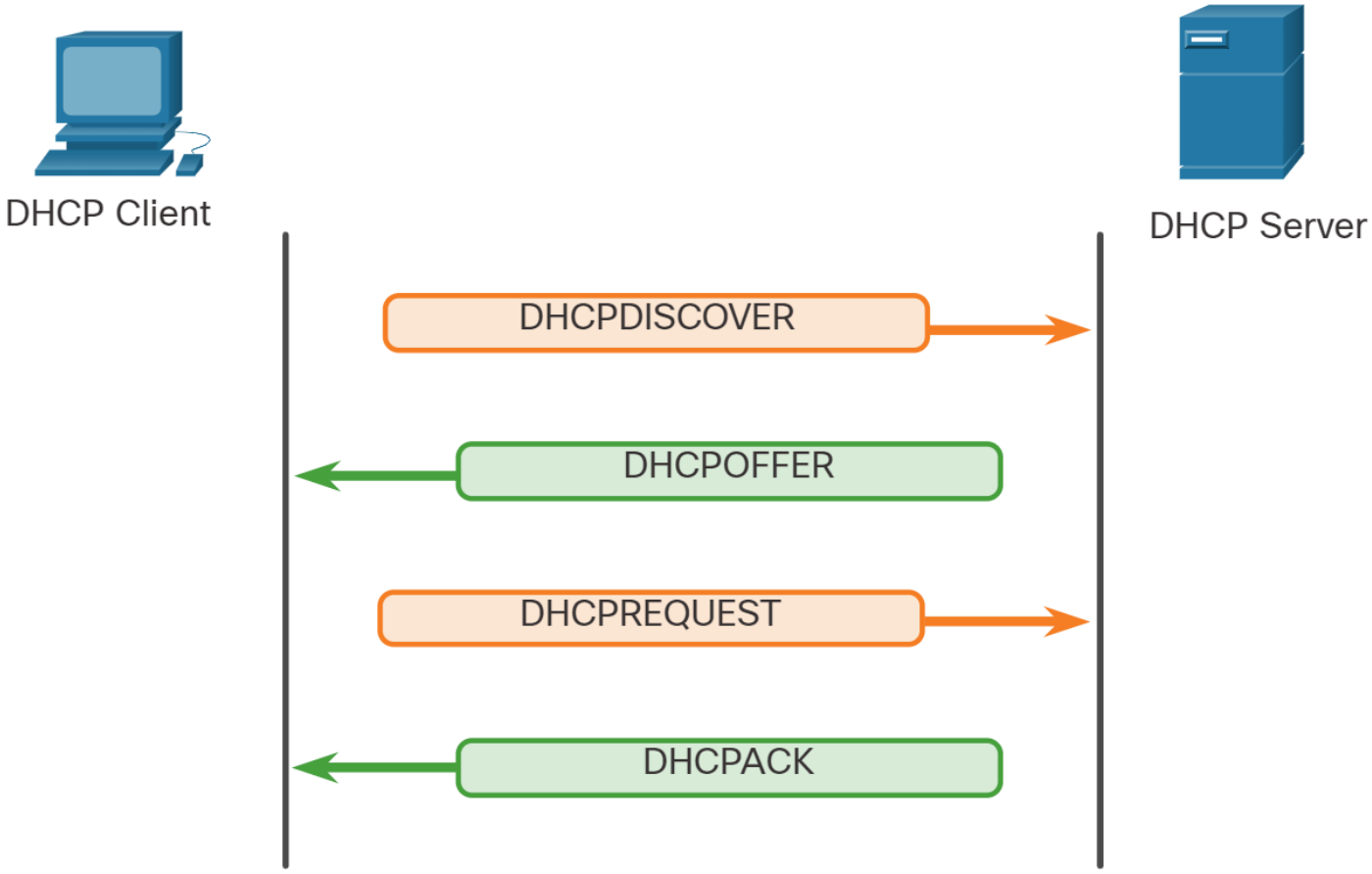
Many networks use both DHCP and static addressing. DHCP is used for general purpose hosts, such as end-user devices. Static addressing is used for network devices, such as gateway routers, switches, servers, and printers.

DHCP for IPv6 (DHCPv6) provides similar services for IPv6 clients. One important difference is that DHCPv6 does not provide a default gateway address. This can only be obtained dynamically from the Router Advertisement message of the router.

7. DHCP Operation

As shown in the figure, when an IPv4, DHCP-configured device boots up or connects to the network, the client broadcasts a DHCP discover (DHCPDISCOVER) message to identify any available DHCP servers on the network. A DHCP server replies with a DHCP offer (DHCPOFFER) message, which offers a lease to the client. The offer message contains the IPv4 address and subnet mask to be assigned, the IPv4 address of the DNS server, and the IPv4 address of the default gateway. The lease offer also includes the duration of the lease.

The figure shows a protocol ladder with a DHCP client on one side and a DHCP client on the other. The DHCP client sends a DHCPDISCOVER message to the DHCP Server. The DHCP server sends a DHCPOFFER message to the DHCP client. The DHCP client sends a DHCPREQUEST message in repoonse to the DHCPOFFER from the DHCP server. THE DHCP server sends a DHCPACK message back to the DHCP client. The process is called DORA.



The client may receive multiple DHCPOFFER messages if there is more than one DHCP server on the local network. Therefore, it must choose between them and send a DHCP request (DHCPREQUEST) message that identifies the explicit server and lease offer that the client is accepting. A client may also choose to request an address that had previously been allocated by the server.

Assuming that the IPv4 address requested by the client, or offered by the server, is still available, the server returns a DHCP acknowledgement (DHCPACK) message that acknowledges to the client that the lease has been finalized. If the offer is no longer valid, then the selected server responds with a DHCP negative acknowledgement (DHCPNAK) message. If a DHCPNAK message is returned, then the selection process must begin again with a new DHCPDISCOVER message being transmitted. After the client has the lease, it must be renewed prior to the lease expiration through another DHCPREQUEST message.

The DHCP server ensures that all IP addresses are unique (the same IP address cannot be assigned to two different network devices simultaneously). Most ISPs use DHCP to allocate addresses to their customers.

DHCPv6 has a set of messages that is similar to those for DHCPv4. The DHCPv6 messages are SOLICIT, ADVERTISE, INFORMATION REQUEST, and REPLY.

8. Lab - Observe DNS Resolution

8A. Objectives

Part 1: Observe the DNS Conversion of a URL to an IP Address

Part 2: Observe DNS Lookup Using the nslookup Command on a Web Site

Part 3: Observe DNS Lookup Using the nslookup Command on Mail Servers

8B. Background / Scenario

The Domain Name System (DNS) is invoked when you type a Uniform Resource Locator (URL), such as http://www.cisco.com, into a web browser. The first part of the URL describes which protocol is used. Common protocols are Hypertext Transfer Protocol (HTTP), Hypertext Transfer Protocol over Secure Socket Layer (HTTPS), and File Transfer Protocol (FTP).

DNS uses the second part of the URL, which in this example is www.cisco.com. DNS translates the domain name (www.cisco.com) to an IP address to allow the source host to reach the destination server. In this lab, you will observe DNS in action and use the nslookup (name server lookup) command to obtain additional DNS information.

8C. Required Resources

1 PC (Windows with internet and command prompt access)

8E. Part 1: Observe the DNS Conversion of a URL to an IP Address

a. Open a Windows command prompt.

b. At the command prompt, ping the URL for the Internet Corporation for Assigned Names and Numbers (ICANN) at **www.icann.org.** ICANN coordinates the DNS, IP addresses, top-level domain name system management, and root server system management functions. The computer must translate www.icann.org into an IP address to know where to send the Internet Control Message Protocol (ICMP) packets.

The first line of the output displays **www.icann.org** converted to an IP address by DNS. You should be able to see the effect of DNS, even if your institution has a firewall that prevents pinging, or if the destination server has prevented you from pinging its web server.

Note: If the domain name is resolved to an IPv6 address, use the command **ping -4 www.icann.org** to translate into an IPv4 address if desired.

```
C:\> ping www.icann.org

Pinging www.vip.icann.org [2620:0:2d0:200::7] with 32 bytes of data:
Reply from 2620:0:2d0:200::7: time=43ms
Reply from 2620:0:2d0:200::7: time=41ms
Reply from 2620:0:2d0:200::7: time=44ms
Reply from 2620:0:2d0:200::7: time=39ms

Ping statistics for 2620:0:2d0:200::7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 39ms, Maximum = 44ms, Average = 41ms
C:\> ping -4 www.icann.org

Pinging www.vip.icann.org [192.0.32.7] with 32 bytes of data:
Reply from 192.0.32.7: bytes=32 time=41ms TTL=241
Reply from 192.0.32.7: bytes=32 time=42ms TTL=241
Reply from 192.0.32.7: bytes=32 time=42ms TTL=241
Reply from 192.0.32.7: bytes=32 time=43ms TTL=241

Ping statistics for 192.0.32.7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 41ms, Maximum = 43ms, Average = 42ms
```

Record the IP addresses for www.icann.org.

- **192.0.32.7 and 2620:0:2d0:200::7**

c. Type the IPv4 addresses from step b into a web browser, instead of the URL. Enter **https://192.0.32.7** in the web browser. If your computer has an IPv6 address you can enter the IPv6 address. **https://[2620:0:2d0:200::7]** in the web browserd.

d. Notice that the ICANN home web page is displayed without using DNS.

Most humans find it easier to remember words, rather than numbers. If you tell someone to go to **www.icann.org**, they can probably remember that. If you told them to go to 192.0.32.7, they would have a difficult time remembering an IP address. Computers process in numbers. DNS is the process of translating words into numbers. Additionally, there is a second translation that takes place. Humans think in Base 10 numbers. Computers process in Base 2 numbers. The Base 10 IP address 192.0.32.7 in Base 2 numbers is 11000000.00000000.00100000.00000111. What happens if you cut and paste these Base 2 numbers into a browser?

The website does not display. The software code used in web browsers recognizes Base 10 numbers. It does not recognize Base 2 numbers.

e. At a command prompt, ping www.cisco.com.

Note: If the domain name is resolved to an IPv6 address, use the command **ping -4 www.cisco.com** to translate into an IPv4 address if desired.

```
C:\> ping www.cisco.com

Pinging origin-www.cisco.com [2600:1408:7:1:9300::90] with 32 bytes of data:
Reply from 2600:1408:7:1:9300::90: time=70ms
Reply from 2600:1408:7:1:9300::90: time=74ms
Reply from 2600:1408:7:1:9300::90: time=72ms
Reply from 2600:1408:7:1:9300::90: time=71ms

Ping statistics for 2600:1408:7:1:9300::90:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 70ms, Maximum = 74ms, Average = 71ms
C:\> ping -4 www.cisco.com

Pinging e2867.dsca.akamaiedge.net [172.230.155.162] with 32 bytes of data:
Reply from 172.230.155.162: bytes=32 time=7ms TTL=54
Reply from 172.230.155.162: bytes=32 time=6ms TTL=54
Reply from 172.230.155.162: bytes=32 time=7ms TTL=54
Reply from 172.230.155.162: bytes=32 time=6ms TTL=54

Ping statistics for 172.230.155.162:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 6ms, Maximum = 7ms, Average = 6ms
```

When you ping www.cisco.com, do you get the same IP address as the example? Explain.

Answer will vary depending on where you are geographically. Cisco hosts its web content on a series of mirror servers. This means that Cisco uploads the exact same content to geographically diverse (spread out all over the world) servers. When someone tries to reach www.cisco.com, the traffic is directed to the closest mirror server.

Type the IP address that you obtained when you pinged www.cisco.com into a browser. Does the website display? Explain.

The Cisco website does not display this. There are at least two possible explanations for this: 1. Some web servers are configured to accept IP addresses sent from a browser and some are not. 2. It may be a firewall rule in the Cisco security system that prohibits an IP address from being sent via a browser. Depending on the Web Browser you can also get a message saying the connection is not secure or there is a certificate error.

8F. Part 2: Observe DNS Lookup Using the nslookup Command on a Web Site

a. At the command prompt, type the nslookup command. Your result will be different than the example.

```
C:\> nslookup
Default Server: one.one.one.one
Address: 1.1.1.1

>
```

What is the default DNS server used?

- **Site dependent**

b. Notice how the command prompt changed to a greater than (>) symbol. This is the nslookup prompt. From this prompt, you can enter commands related to DNS. At the prompt, type ? to see a list of all the available commands that you can use in nslookup mode.

c. At the nslookup prompt, type www.cisco.com.

```
> www.cisco.com
Default Server:  one.one.one.one
Address:  1.1.1.1

Non-authoritative answer:
Name:    e2867.dsca.akamaiedge.net
Addresses:  2600:1404:a:395::b33
          2600:1404:a:38e:::b33
          172.230.155.162
Aliases:  www.cisco.com
          www.cisco.com.akadns.net
          wwwds.cisco.com.edgekey.net
          wwwds.cisco.com.edgekey.net.globalredir.akadns.net
```

What is the translated IPv4 address?

- **From a specific location, 172.230.155.162**.

Note: The IP address from your location will most likely be different because Cisco uses mirrored servers in various locations around the world.

Is it the same as the IP address shown with the ping command?

- **Yes**

Under addresses, in addition to the 172.230.155.162 IP address, there are the following numbers: 2600:1404:a:395::b33 and 2600:1404:a:38e:::b33. What are these?

- **IPv6 (IP version 6) IP addresses at which the website is reachable**.

d. At the nslookup prompt, type the IP address of the Cisco web server that you just found. You can use nslookup to get the domain name of an IP address if you do not know the URL.

```
> 172.230.155.162
Default Server:  one.one.one.one
Address:  1.1.1.1

Name:    a172-230-155-162.deploy.static.akamaitechnologies.com
Address:  172.230.155.162
```

You can use the nslookup tool to translate domain names into IP addresses. You can also use it to translate IP addresses into domain names. Using the nslookup tool, record the IP addresses associated with www.google.com.

Answers may vary. At the time of writing, the IP addresses are 2607:f8b0:4000:80f::2004 and 172.217.9.132.

```
> www.google.com
Server: one.one.one.one
Address: 1.1.1.1

Non-authoritative answer:
Name: www.google.com
Addresses: 2607:f8b0:4000:80f::2004
172.217.9.132
```

8G. Part 3: Observe DNS Lookup Using the nslookup Command on Mail Servers

a. At the nslookup prompt, type set type=mx to use nslookup to identify mail servers.

```
> set type=mx
```

b. At the nslookup prompt, type cisco.com.

```
> cisco.com
Server:  one.one.one.one
Address:  1.1.1.1

Non-authoritative answer:
cisco.com       MX preference = 20, mail exchanger = rcdn-mx-01.cisco.com
cisco.com       MX preference = 30, mail exchanger = aer-mx-01.cisco.com
cisco.com       MX preference = 10, mail exchanger = alln-mx-01.cisco.com
```

A fundamental principle of network design is redundancy (more than one mail server is configured). In this way, if one of the mail servers is unreachable, then the computer making the query tries the second mail server. Email administrators determine which mail server is contacted first by using MX preference. The mail server with the lowest MX preference is contacted first. Based upon the output above, which mail server will be contacted first when the email is sent to cisco.com?

- **rcdn-mx-01.cisco.com**

c. At the nslookup prompt, type exit to return to the regular PC command prompt.

d. At the PC command prompt, type ipconfig /all.

Write the IP addresses of all the DNS servers that your school uses.

- **Site-dependent**

8H. Reflection Question

What is the fundamental purpose of DNS?

- **DNS basically acts like the phonebook for the Internet. So DNS translates names to numbers. The numbers can be either IPv4 or IPv6**.

9. Check Your Understanding - IP Addressing Services

Check your understanding of DNS services by choosing the correct answer to the following questions.

Question 1: Which of the following DNS record types is used to resolve IPv6 addresses?

(a) A

(b) NS

(c) AAAA

(D) MX

Answer: **(c) -** DNS AAAA records are used to resolve names to IPv6 addresses.

Question 2: True or false? A DNS server that receives a request for a name resolution that is not within its DNS zone will send a failure message to the requesting client.

(a) True

(b) False

Answer: **(b) -** The correct answer is False. When a DNS server receives a name resolution request for a name not within its zone, the serve will forward the request to another DNS server.

Question 3: Which of the following is displayed by the nslookup utility?

(a) the configured default DNS server

(b) the IP address of the end device

(c) all cached DNS entries

Answer: **(a) -** By issuing the nslookup command, the default DNS server that is configured is displayed.

Question 4: Which of the following DNS resource record types resolves authoritative name servers?

(a) A

(b) NS

(c) AAAA

(D) MX

Answer: **(b) -** NS records resolve authoritative name servers. DNS A records resolve IPv4 addresses. AAAA records resolve IPv6 addresses, and MX records resolve mail exchange servers.

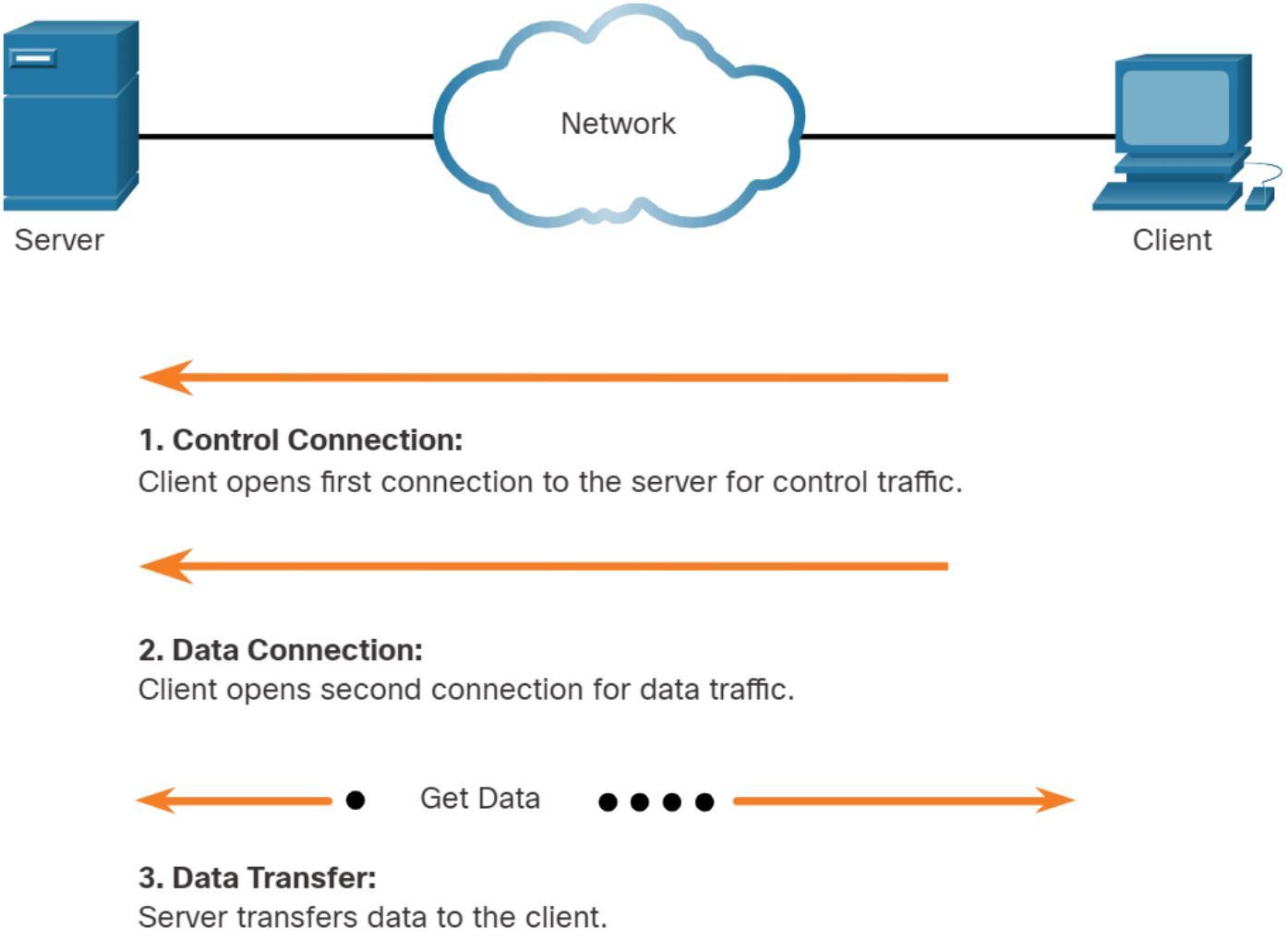
File Sharing Services

1. File Transfer Protocol

As you learned in previous topics, in the client/server model, the client can upload data to a server, and download data from a server, if both devices are using a file transfer protocol (FTP). Like HTTP, email, and addressing protocols, FTP is commonly used application layer protocol. This topic discusses FTP in more detail.

FTP was developed to allow for data transfers between a client and a server. An FTP client is an application which runs on a computer that is being used to push and pull data from an FTP server.

The figure depicts an FTP transaction between a client and a server. A client is contacting a server through a network. The first message from the client is a control connection: the client opens the first connection to the server for control traffic. The second message from the client is a data connection: the client opens a second connection for data traffic. Data can then be downloaded from the server or uploaded from the client.



Based on commands sent across the control connection, data can be downloaded from the server or uploaded from the client.

The client establishes the first connection to the server to control traffic using TCP port 21. The traffic consists of client commands and server replies.

The client establishes the second connection to the server for the actual data transfer using TCP port 20. This connection is created every time there is data to be transferred.

The data transfer can happen in either direction. The client can download (pull) data from the server, or the client can upload (push) data to the server.

2. Server Message Block

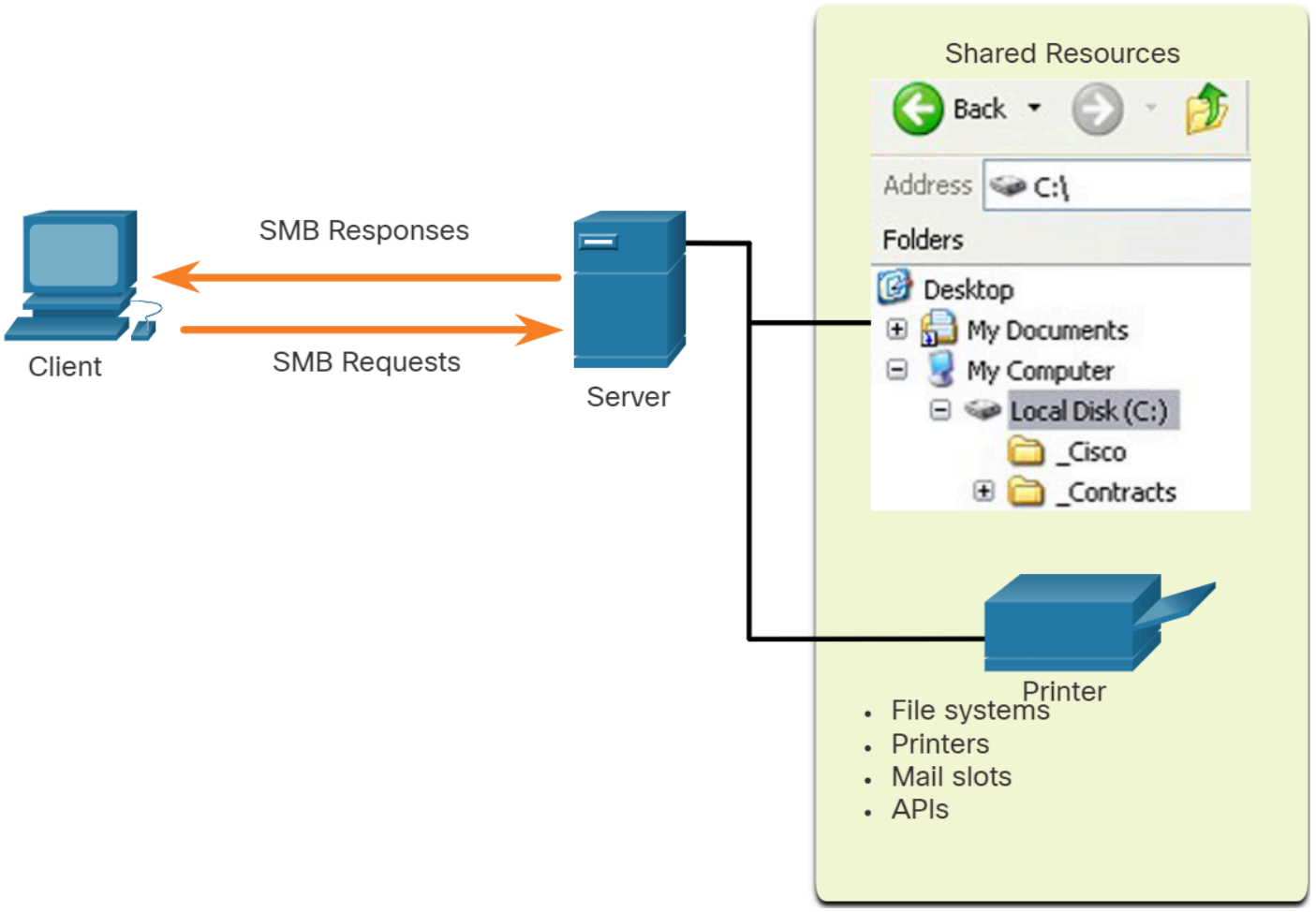
The Server Message Block (SMB) is a client/server file-sharing protocol that describes the structure of shared network resources, such as directories, files, printers, and serial ports. It is a request-response protocol. All SMB messages share a common format. This format uses a fixed-sized header, followed by a variable-sized parameter and a data component.

Here are three functions of SMB messages:

- Start, authenticate, and terminate sessions.
- Control file and printer access.
- Allow an application to send or receive messages to or from another device.

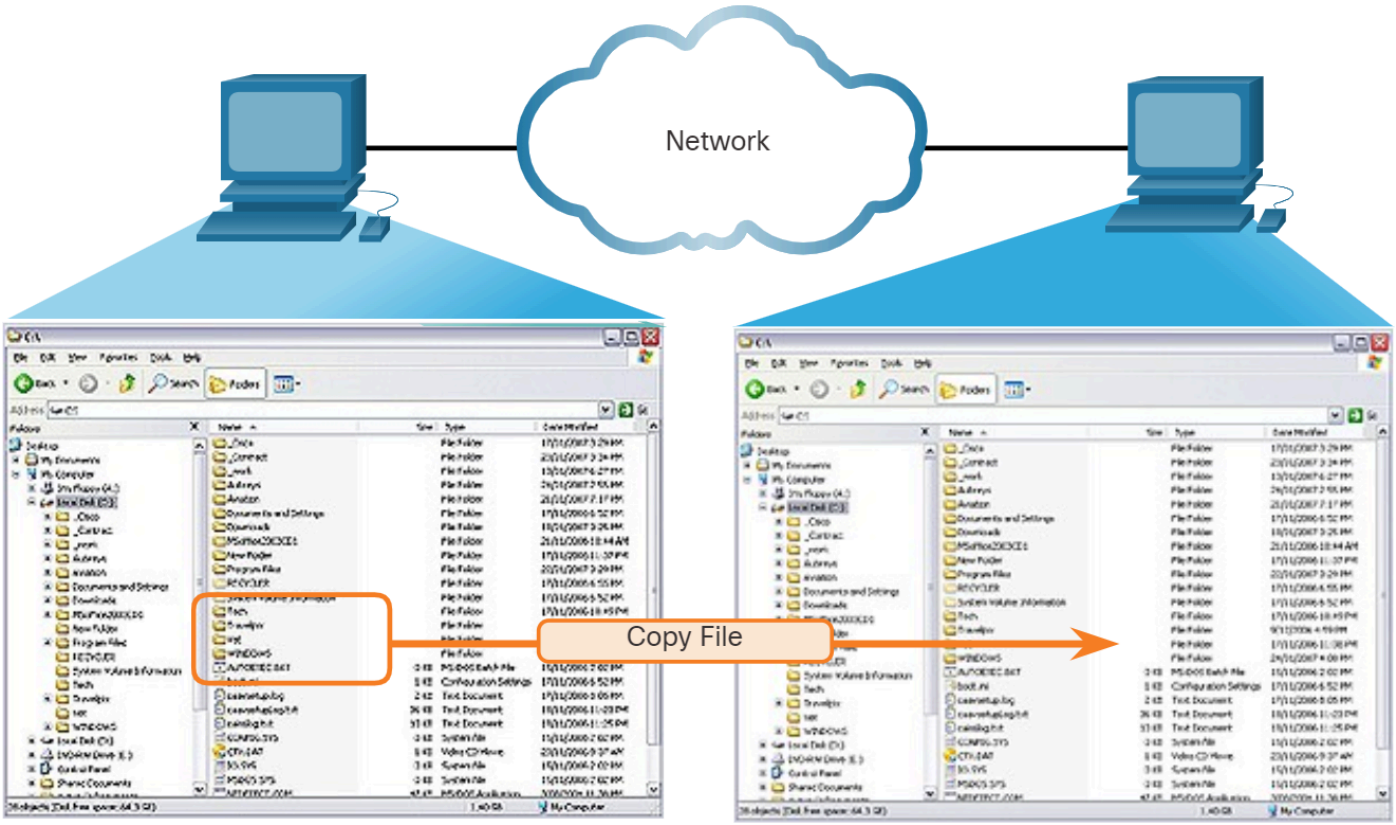
SMB file-sharing and print services have become the mainstay of Microsoft networking. With the introduction of the Windows 2000 software series, Microsoft changed the underlying structure for using SMB. In previous versions of Microsoft products, the SMB services used a non-TCP/IP protocol to implement name resolution. Beginning with Windows 2000, all subsequent Microsoft products use DNS naming, which allows TCP/IP protocols to directly support SMB resource sharing, as shown in the figure.

The first figure shows a Microsoft Windows shared resource of My Documents with a client request from a Server My Documents. The client sends an SMB request and receives an SMB response from the shared resource My Documents. Shared Resources include File systems, Printers shown as an icon, Mail slots, and APIs.



SMB is a client/server, request-response protocol. Servers can make their own resources available to clients on the network.

The SMB file exchange process between Windows PCs is shown in the next figure.



A file may be copied from PC to PC with Windows Explorer using the SMB protocol.

Unlike the file sharing supported by FTP, clients establish a long-term connection to servers. After the connection is established, the user of the client can access the resources on the server as though the resource is local to the client host.

The LINUX and UNIX operating systems also provide a method of sharing resources with Microsoft networks by using a version of SMB called SAMBA. The Apple Macintosh operating systems also support resource sharing by using the SMB protocol.

3. Check Your Understanding - File Sharing Services

Check your understanding of file sharing services by choosing the BEST answer to the following questions.

Question 1: How many connections are required by FTP between client and server?

(a) 1

(b) 2

(c) 3

(d) 4

Answer: **(b) -** FTP requires two connections between the client and the server. One connection is over port 21 for client commands and server replies. The other connection is over port 20 for data transfer.

Question 2: True or false? FTP data transfers take place from client to server (push) and from server to client (pull).

(a) True

(b) False

Answer: **(a) -** The correct answer is True. Data transfer over FTP can take place in either direction, uploads from client to server, or downloads from server to client.

Question 3: Which of these ports are used by FTP? (Choose two.)

(a) 20

(b) 21

(c) 25

(d) 110

Answer: **(a & b) -** Ports 20 and 21 are used by FTP.

Question 4: True or false? Resource sharing over SMB is only supported on Microsoft operating systems.

(a) True

(b) False

Answer: **(b) -** The correct answer is False. Resource sharing over SMB is also supported by Apple Macintosh. Linux and Unix operating systems use a version of SMB called SAMBA.

Module Practice and Quiz

1. What did I learn in this module?

1A. Application, Presentation, and Session

In the OSI and the TCP/IP models, the application layer is the closest layer to the end user. Application layer protocols are used to exchange data between programs running on the source and destination hosts. The presentation layer has three primary functions: formatting, or presenting, data at the source device into a compatible form for receipt by the destination device, compressing data in a way that can be decompressed by the destination device, and encrypting data for transmission and decrypting data upon receipt. The session layer creates and maintains dialogues between source and destination applications. The session layer handles the exchange of information to initiate dialogues, keep them active, and to restart sessions that are disrupted or idle for a long period of time. TCP/IP application layer protocols specify the format and control information necessary for many common Internet communication functions. These protocols are used by both the source and destination devices during a session. The protocols implemented on both the source and destination host must be compatible.

1B. Peer-to-Peer

In the client/server model, the device requesting the information is called a client and the device responding to the request is called a server. The client begins the exchange by requesting data from the server, which responds by sending one or more streams of data to the client. In a P2P network, two or more computers are connected via a network and can share resources without having a dedicated server. Every peer can function as both a server and a client. One computer might assume the role of server for one transaction while simultaneously serving as a client for another. P2P applications require that each end device provide a user interface and run a background service. Some P2P applications use a hybrid system where resource sharing is decentralized, but the indexes that point to resource locations are stored in a centralized directory. Many P2P applications allow users to share pieces of files with each other at the same time. Clients use a small file called a torrent file to locate other users who have pieces that they need so that they can connect directly to them. This file also contains information about tracker computers that keep track of which users have what pieces of which files.

1C. Web and Email Protocols

When a web address or URL is typed into a web browser, the web browser establishes a connection to the web service. The web service is running on the server that is using the HTTP protocol. HTTP is a request/response protocol. When a client, typically a web browser, sends a request to a web server, HTTP specifies the message types used for that communication. The three common message types are GET, POST, and PUT. For secure communication across the internet, HTTPS uses the same client request-server response process as HTTP, but the data stream is encrypted with SSL before being transported across the network. Email supports three separate protocols for operation: SMTP, POP, and IMAP. The application layer process that sends mail uses SMTP. A client retrieves email using POP or IMAP. SMTP message formats require a message header and a message body. While the message body can contain any amount of text, the message header must have a properly formatted recipient email address and a sender address. POP is used by an application to retrieve mail from a mail server. With POP, mail is downloaded from the server to the client and then deleted on the server. With IMAP, unlike POP, 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.

1D. IP Addressing Services

The DNS protocol matches resource names with the required numeric network address. The DNS protocol communications use a message format for all types of client queries and server responses, error messages, and the transfer of resource record information between servers. DNS uses domain names to form a hierarchy. Each DNS server maintains a specific database file and is only responsible for managing name-to-IP mappings for that small portion of the entire DNS structure. Computer OSs use Nslookup to allow the user to manually query the name servers to resolve a given host name. DHCP for IPv4 service automates the assignment of IPv4 addresses, subnet masks, gateways, and other IPv4 networking parameters. DHCPv6 provides similar services for IPv6 clients, except that it does not provide a default gateway address. When an IPv4, DHCP-configured device boots up or connects to the network, the client broadcasts a DHCPDISCOVER message to identify any available DHCP servers on the network. A DHCP server replies with a DHCPOFFER message, which offers a lease to the client. DHCPv6 has a set of messages that is similar to those for DHCPv4. The DHCPv6 messages are SOLICIT, ADVERTISE, INFORMATION REQUEST, and REPLY.

1E. File Sharing Services

An FTP client is an application which runs on a computer that is being used to push and pull data from an FTP server. The client establishes the first connection to the server to control traffic using TCP port 21. The client establishes the second connection to the server for the actual data transfer using TCP port 20. The client can download (pull) data from the server, or the client can upload (push) data to the server. Here are three functions of SMB messages: start, authenticate, and terminate sessions, control file and printer access, and allow an application to send or receive messages to or from another device. Unlike the file sharing supported by FTP, clients establish a long-term connection to servers. After the connection is established, the user the client can access the resources on the server as if the resource is local to the client host.

2. Module Quiz - Application Layer

Question 1: On a home network, which device is most likely to provide dynamic IP addressing to clients on the home network?

(a) a dedicated file server

(b) a home router

(c) an ISP DHCP server

(d) a DNS server

Answer: **(b) -** On a home network, a home router usually serves as the DHCP server. The home router is responsible for dynamically assigning IP addresses to clients on the home network. ISPs also use DHCP, but it usually assigns an IP address to the Internet interface of the home router, not the clients on the home network. In businesses, it is common to have a file or other dedicated server provide DHCP services to the network. Finally, a DNS server is responsible for finding the IP address for a URL, not for providing dynamic addressing to network clients.

Question 2: What part of the URL, http://www.cisco.com/index.html, represents the top-level DNS domain?

(a) .com

(b) www

(c) http

(d) index

Answer: **(a) -** The components of the URL http://www.cisco.com/index.htm are as follows:

- http = protocol
- www = part of the server name
- cisco = part of the domain name
- index = file name
- com = the top-level domain

Question 3: What are two characteristics of the application layer of the TCP/IP model? (Choose two.)

(a) responsibility for logical addressing

(b) responsibility for physical addressing

(c) the creation and maintenance of dialogue between source and destination applications

(d) closest to the end user

(e) the establishing of window size

Answer: **(c & d) -** The application layer of the TCP/IP model is the layer that is closest to the end user, providing the interface between the applications. It is responsible for formatting, compressing, and encrypting data, and is used to create and maintain dialog between source and destination applications.

Question 4: What message type is used by an HTTP client to request data from a web server?

(a) GET

(b) POST

(c) PUT

(d) ACK

Answer: **(a) -** HTTP clients send GET messages to request data from web servers.

Question 5: Which statement is true about FTP?

(a) The client can choose if FTP is going to establish one or two connections with the server.

(b) The client can download data from or upload data to the server.

(c) FTP is a peer-to-peer application.

(d) FTP does not provide reliability during data transmission.

Answer: **(b) -** FTP is a client/server protocol. FTP requires two connections between the client and the server and uses TCP to provide reliable connections. With FTP, data transfer can happen in either direction. The client can download (pull) data from the server or upload (push) data to the server.

Question 6: A wireless host needs to request an IP address. What protocol would be used to process the request?

(a) FTP

(b) HTTP

(c) DHCP

(d) ICMP

(e) SNMP

Answer: **(c) -** The DHCP protocol is used to request, issue, and manage IP addressing information. CSMA/CD is the access method used with wired Ethernet. ICMP is used to test connectivity. SNMP is used with network management and FTP is used for file transfer.

Question 7: Which TCP/IP model layer is closest to the end user?

(a) application

(b) internet

(c) network access

(d) transport

Answer: **(a) -** End users use applications to interact with and use the network. The application layer of the TCP/IP model is closest to the end user. Application layer protocols are used to communicate and exchange messages with other network devices and applications. The layers of the TCP/IP model are from top to bottom (memory aid – ATIN): application, transport, internet, network access

Question 8: Which three protocols or standards are used at the application layer of the TCP/IP model? (Choose three.)

(a) TCP

(b) HTTP

(c) MPEG

(d) GIF

(e) IP

(f) UDP

Answer: **(b & c & d) -** HTTP, MPEG, and GIF operate at the application layer of the TCP/IP model. TCP and UDP operate at the transport layer. IP operates at the internet layer.

Question 9: Which protocol uses encryption?

(a) DHCP

(b) DNS

(c) FTP

(d) HTTPS

Answer: **(d) -** HTTPS uses Secure Socket Layer (SSL) to encrypt traffic accessed from a web server.

Question 10: Why is DHCP preferred for use on large networks?

(a) Large networks send more requests for domain to IP address resolution than do smaller networks.

(b) DHCP uses a reliable transport layer protocol.

(c) It prevents sharing of files that are copyrighted.

(d) It is a more efficient way to manage IP addresses than static address assignment.

(e) Hosts on large networks require more IP addressing configuration settings than hosts on small networks.

Answer: **(d) -** Static IP address assignment requires personnel to configure each network host with addresses manually. Large networks can change frequently and have many more hosts to configure than do small networks. DHCP provides a much more efficient means of configuring and managing IP addresses on large networks than does static address assignment.

Question 11: Which two tasks can be performed by a local DNS server? (Choose two.)

(a) providing IP addresses to local hosts

(b) allowing data transfer between two network devices

(c) mapping name-to-IP addresses for internal hosts

(d) forwarding name resolution requests between servers

(e) retrieving email messages

Answer: **(c & d) -** Two important functions of DNS are to (1) provide IP addresses for domain names such as www.cisco.com, and (2) forward requests that cannot be resolved to other servers in order to provide domain name to IP address translation. DHCP provides IP addressing information to local devices. A file transfer protocol such as FTP, SFTP, or TFTP provides file sharing services. IMAP or POP can be used to retrieve an email message from a server.

Question 12: Which protocol can be used to transfer messages from an email server to an email client?

(a) SMTP

(b) POP3

(c) SNMP

(d) HTTP

Answer: **(b) -** SMTP is used to send mail from the client to the server but POP3 is used to download mail from the server to the client. HTTP and SNMP are protocols that are unrelated to email.

Question 13: When retrieving email messages, which protocol allows for easy, centralized storage and backup of emails that would be desirable for a small- to medium-sized business?

(a) IMAP

(b) POP

(c) SMTP

(d) HTTPS

Answer: **(a) -** IMAP is preferred for small-to medium-sized businesses as IMAP allows centralized storage and backup of emails, with copies of the emails being forwarded to clients. POP delivers the emails to the clients and deletes them on the email server. SMTP is used to send emails and not to receive them. HTTPS is not used for secure web browsing.

Question 14: Which application layer protocol is used to provide file-sharing and print services to Microsoft applications?

(a) HTTP

(b) SMTP

(c) DHCP

(d) SMB

Answer: **(d) -** SMB is used in Microsoft networking for file-sharing and print services. The Linux operating system provides a method of sharing resources with Microsoft networks by using a version of SMB called SAMBA.

Question 15: An author is uploading one chapter document from a personal computer to a file server of a book publisher. What role is the personal computer assuming in this network model?

(a) client

(b) master

(c) server

(d) slave

(e) transient

Answer: **(a) -** In the client/server network model, a network device assumes the role of server in order to provide a particular service such as file transfer and storage. The device requesting the service assumes the role of the client. In the client/server network model, a dedicated server does not have to be used, but if one is present, the network model being used is the client/server model. In contrast, the peer-to-peer network model does not have a dedicated server.