

Chapter 10: Application Layer

Introduction to Networks v5.1



Chapter Outline

10.0 Introduction

10.1 Application Layer Protocols

10.2 Well-Known Application
Layer Protocols and Services

10.3 Summary

Section 10.1:

Application Layer Protocols

Upon completion of this section, you should be able to:

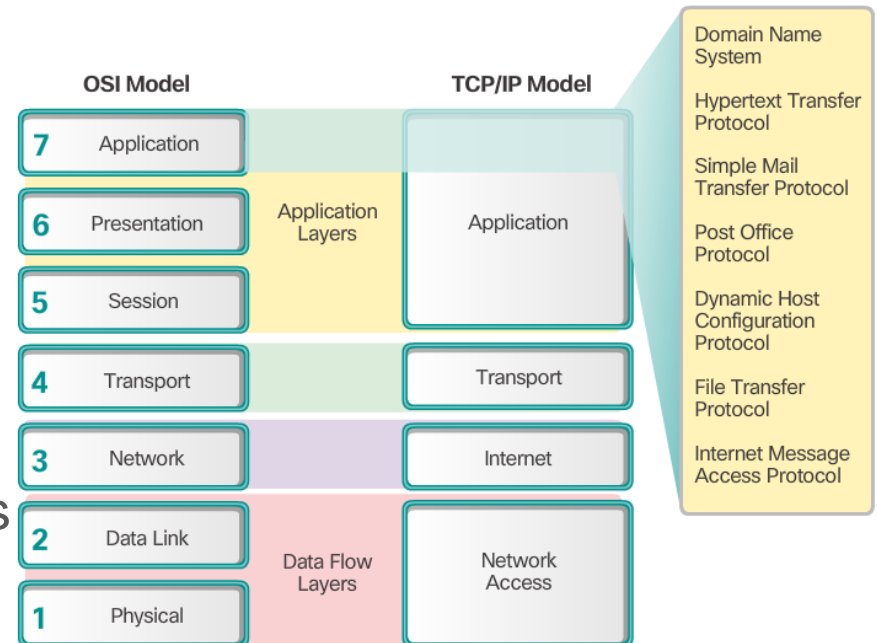
- Explain how the functions of the application layer, session layer, and presentation layer work together to provide network services to end user applications.
- Explain how common application layer protocols interact with end user applications.

Topic 10.1.1: Application, Presentation, and Session



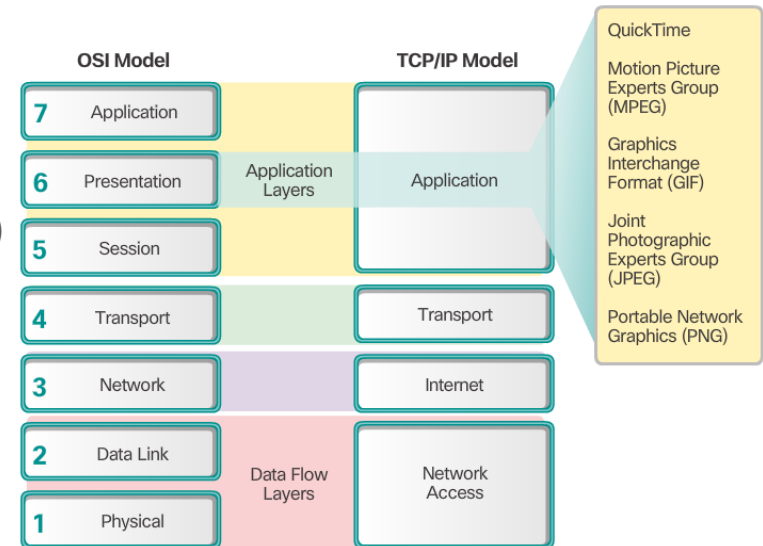
Application Layer

- The application layer is closest to the end user.
- Network applications enable users to send and receive data with ease.
- The application layer acts as interface between the applications and the underlying network.
- Application layer protocols help exchange data between programs running on the source and destination hosts.
- The TCP/IP application layer performs the functions of the upper three layers of the OSI model.
- Common application layer protocols include: HTTP, FTP, TFTP, DNS.



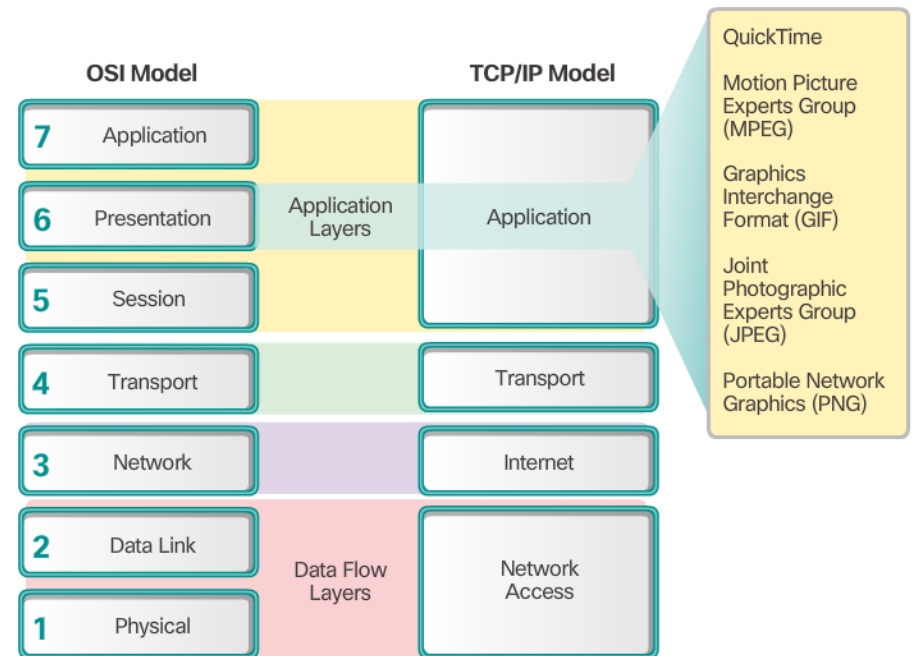
Presentation and Session Layer

- The presentation layer has three primary functions:
 - Format data
 - Compress data
 - Encrypt data
- Common standards for video include QuickTime and Motion Picture Experts Group (MPEG).
- Common graphic image formats are:
 - Graphics Interchange Format (GIF)
 - Joint Photographic Experts Group (JPEG)
 - Portable Network Graphics (PNG) format



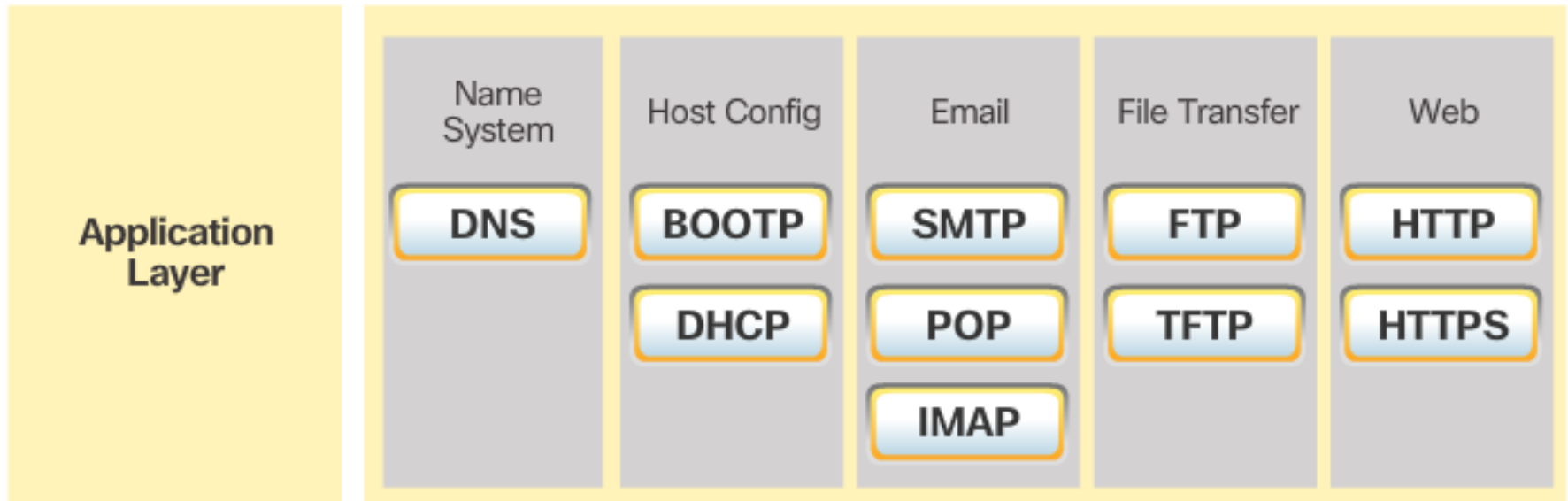
Presentation and Session Layer (cont.)

- The session layer creates and maintains 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.



TCP/IP Application Layer Protocols

- TCP/IP application protocols specify the format and control information necessary for common Internet functions.
- Application layer protocols must be implemented in both the source and destination devices.
- Application layer protocols implemented on the source and destination host must be compatible to allow communication.

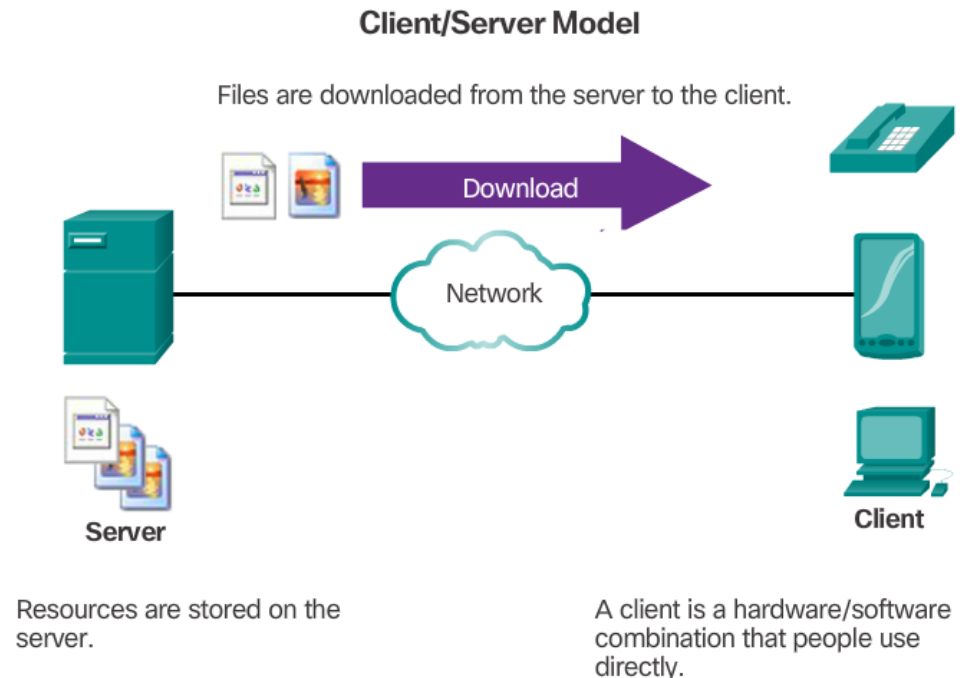


Topic 10.1.2: How Application Protocols Interact with End-User Applications



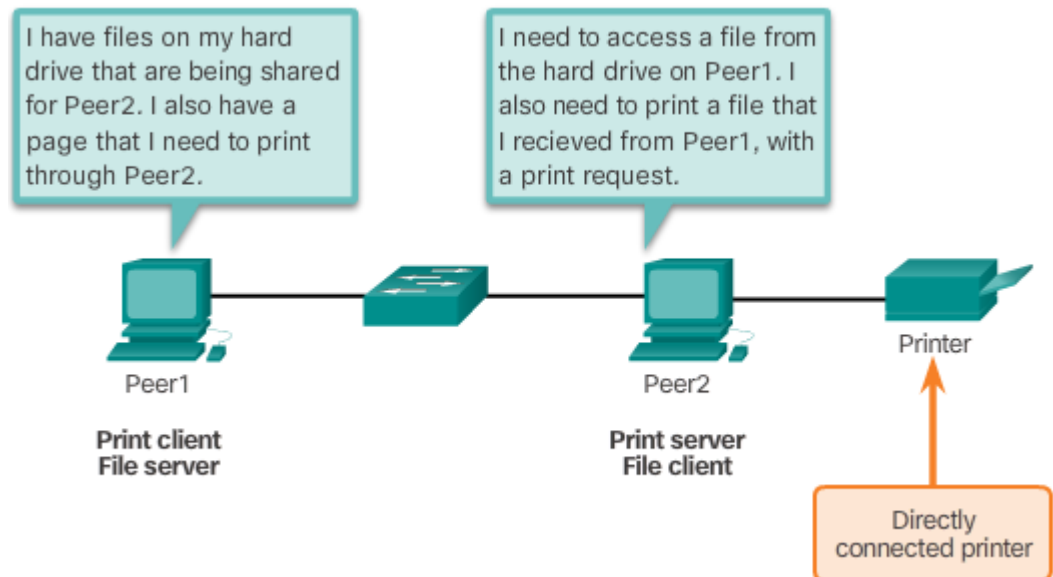
Client-Server Model

- The device requesting the information is called a client.
- The device responding to the request is called a server.
- Client and server processes are considered to be in the application layer.
- The client initiates the exchange by requesting data from the server.
- The server 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.
- The contents of the data exchange will depend of the application in use.
- Email is an example of a Client-Server interaction.



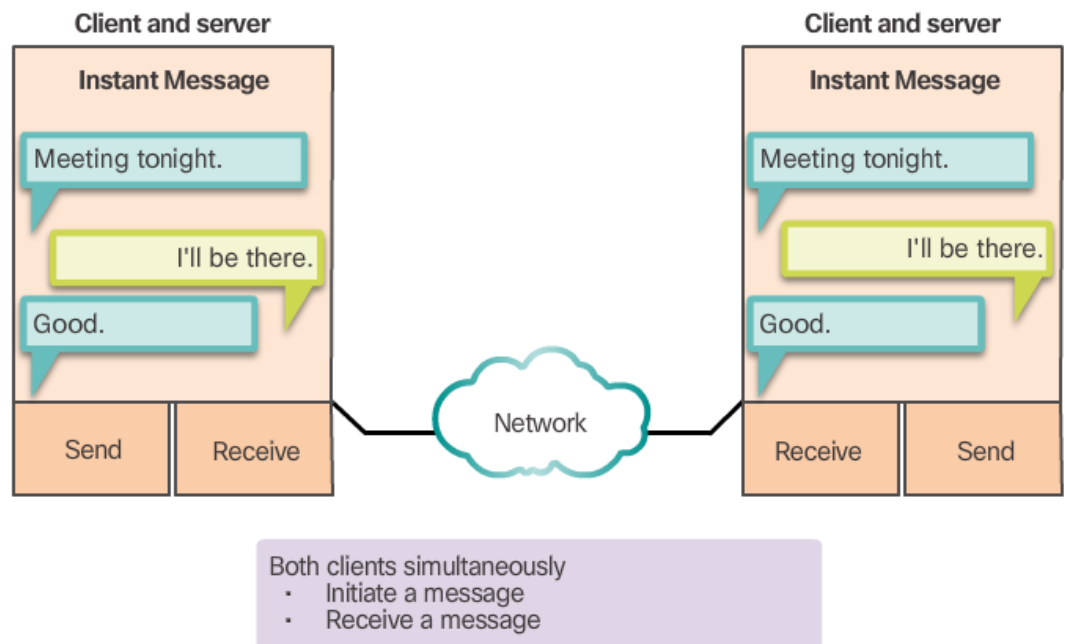
Peer-to-Peer Networks

- In the peer-to-peer (P2P) networking model, the data is accessed without the use of a dedicated server.
- Two or more computers can be connected to a P2P network to share resources.
- Every connected end device (a peer) can function as both a server and a client.
- The roles of client and server are set on a per request basis.



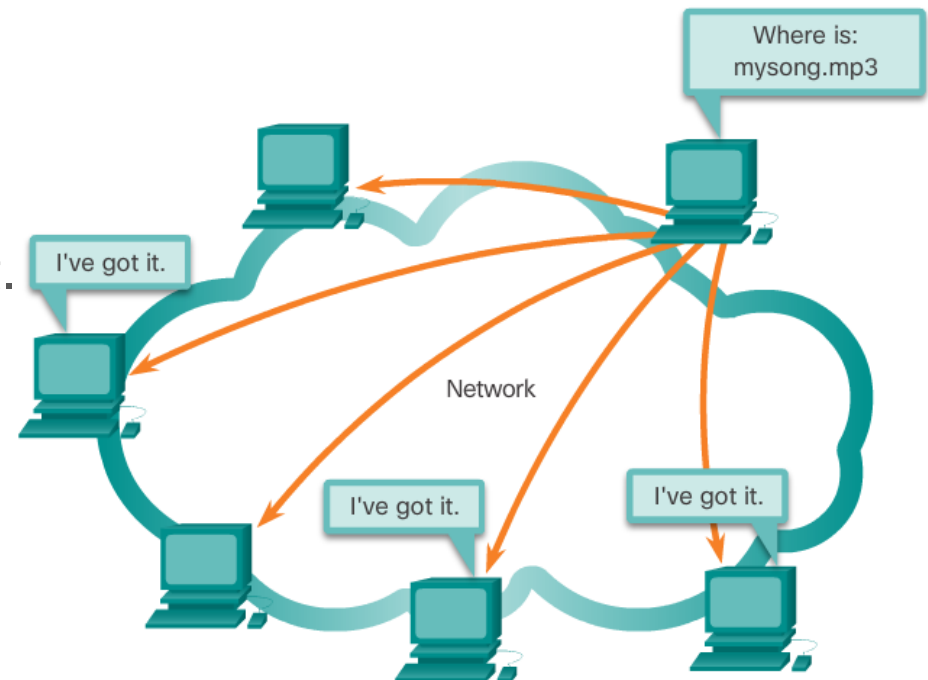
Peer-to-Peer Applications

- Some P2P applications use a hybrid system.
- In hybrid P2P, resource sharing is decentralized.
- 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.



Common P2P Applications

- Common P2P networks include: eDonkey, G2, BitTorrent, Bitcoin.
- Many P2P applications allow users to share pieces of many files with each other at the same time.
- A small torrent file contains information about the location of other users and tracker computers.
- Trackers are computers keeping track of the files hosted by users.
- This technology is called BitTorrent.
- There are many BitTorrent clients, including BitTorrent, uTorrent, Frostwire, and qBittorrent.



Section 10.2:

Well-Known Application Layer Protocols and Services

Upon completion of this section, you should be able to:

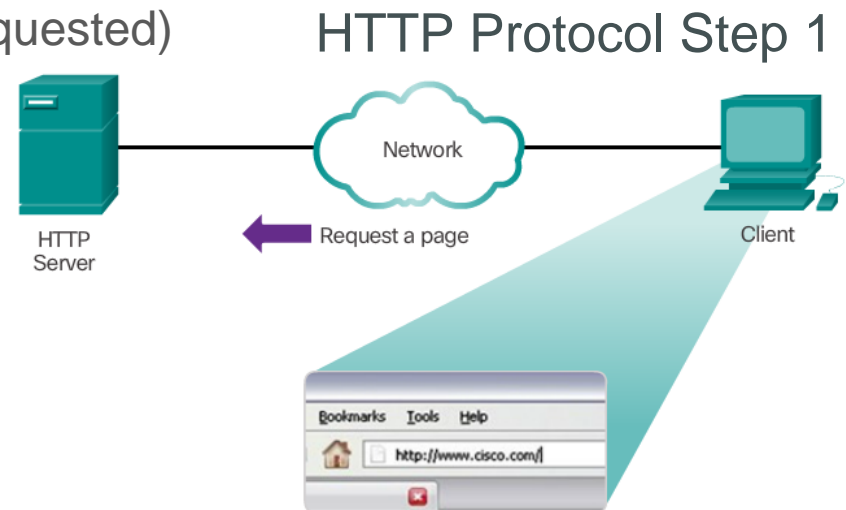
- Explain how web and email protocols operate.
- Explain how the IP addressing protocols operate.
- Explain how file transfer protocols operate.

Topic 10.2.1: Web and Email Protocols



Hypertext Transfer Protocol and Hypertext Markup Language

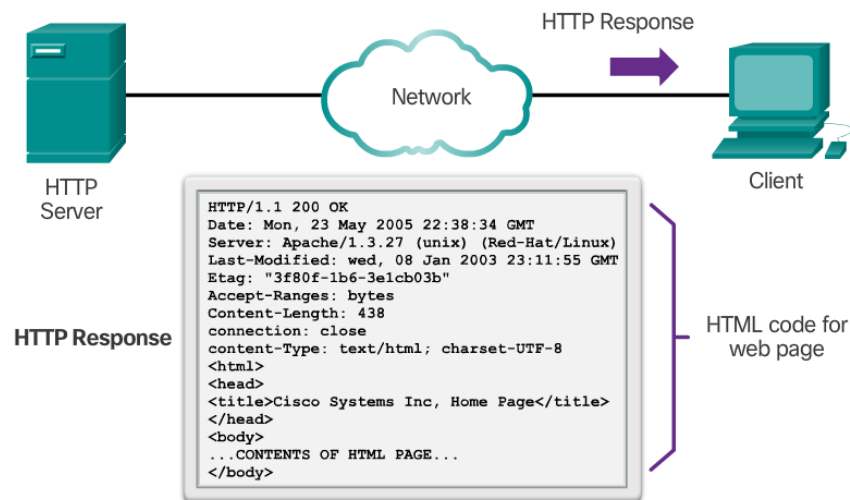
- A web address or uniform resource locator (URL) is a reference to a web server. A URL allows a web browser to establish a connection to that web server.
- URLs and Uniform Resource Identifier (URIs) are the names most people associate with web addresses.
- The URL <http://cisco.com/index.html> has three basic parts:
 - **http** (the protocol or scheme)
 - **www.cisco.com** (the server name)
 - **index.html** (the specific filename requested)
- Using DNS, the server name portion of the URL is then translated to the associated IP address before the server can be contacted.



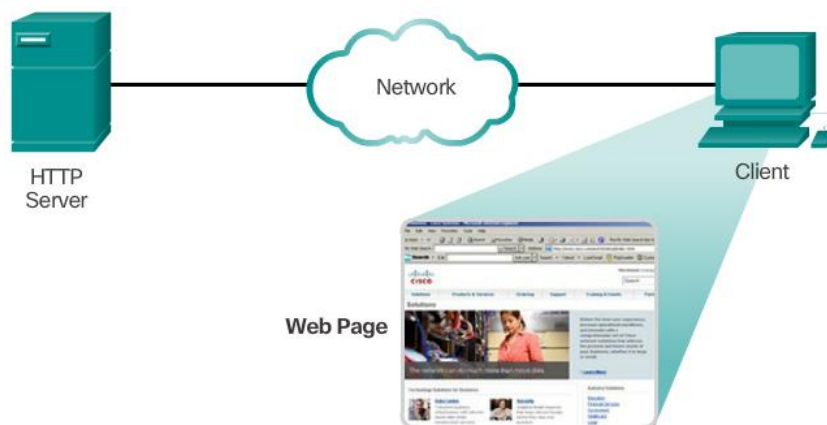
Hypertext Transfer Protocol and Hypertext Markup Language (cont.)

- The browser sends a GET request to the server's IP address and asks for the **index.html** file.
- The server sends the requested file to the client.
- The **index.html** was specified in the URL and contains the HTML code for this web page.
- The browser processes the HTML code and formats the page for the browser window based on the code in the file.

HTTP Protocol Step 2

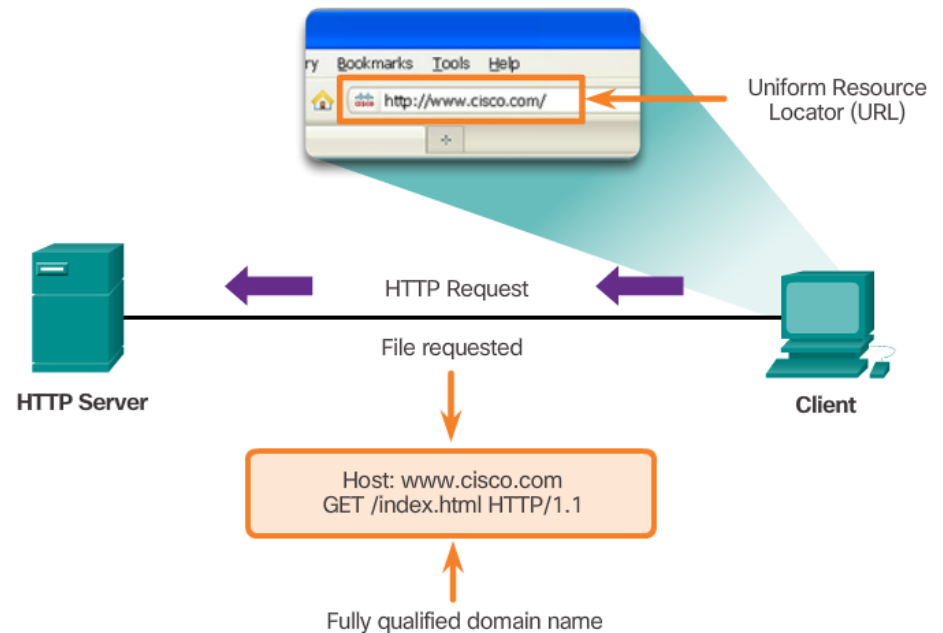


HTTP Protocol Step 3



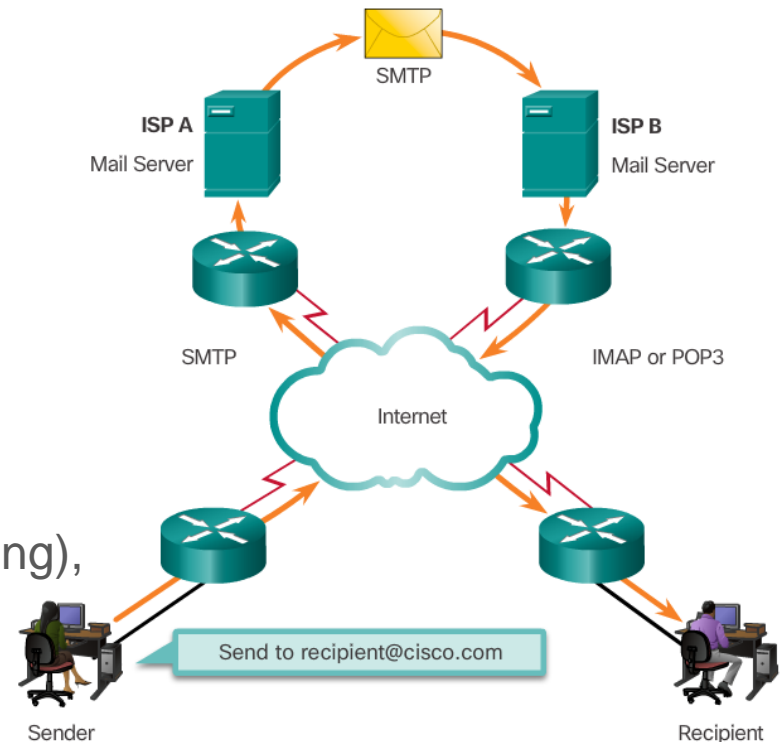
HTTP and HTTPS

- HTTP
 - Is a request/response protocol.
 - Has three common message types: GET, POST, PUT.
 - Is not secure. Messages can be intercepted.
- HTTPS uses authentication and encryption to secure data.



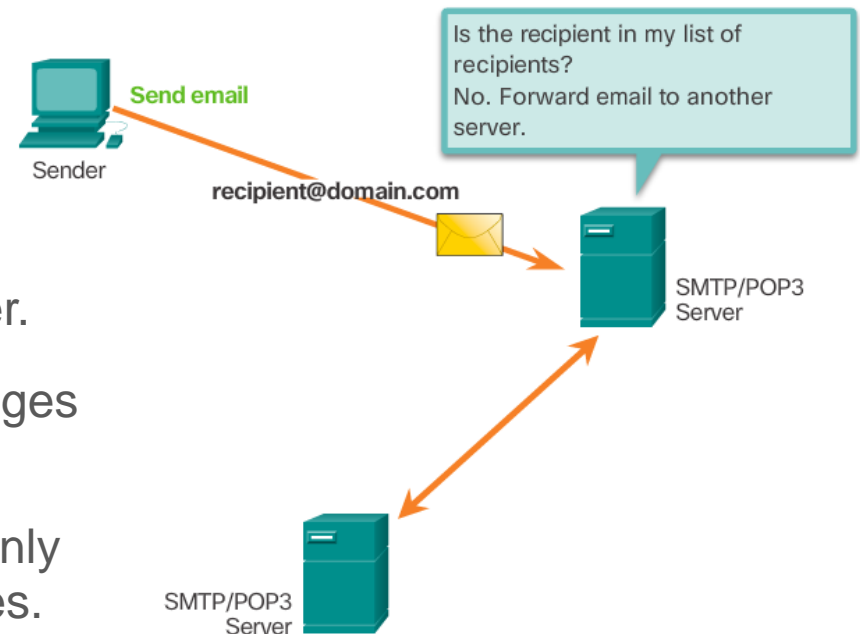
Email Protocols

- Email is a store-and-forward method of sending, storing, and retrieving electronic messages.
- Email messages are stored in databases on mail servers.
- 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.
- Email clients do not communicate directly when sending email.
- Email relies on three separate protocols for operation: SMTP (sending), POP (retrieving), IMAP (retrieving).



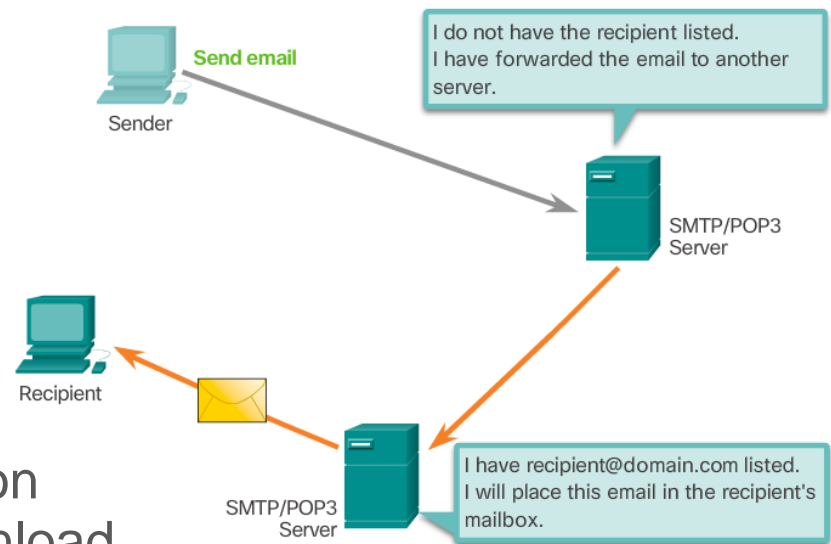
SMTP Operation

- SMTP message formats require a message header and body.
- The body can contain any amount of text.
- The header must have a properly formatted recipient email address and a sender address.
- An SMTP client sends an email by connecting to a SMTP server on port 25.
- The server receives the message and stores it message in a local mailbox or relays the message to another mail server.
- Users use email clients to retrieve messages stored on the server.
- IMAP and POP are two protocols commonly used by email clients to retrieve messages.



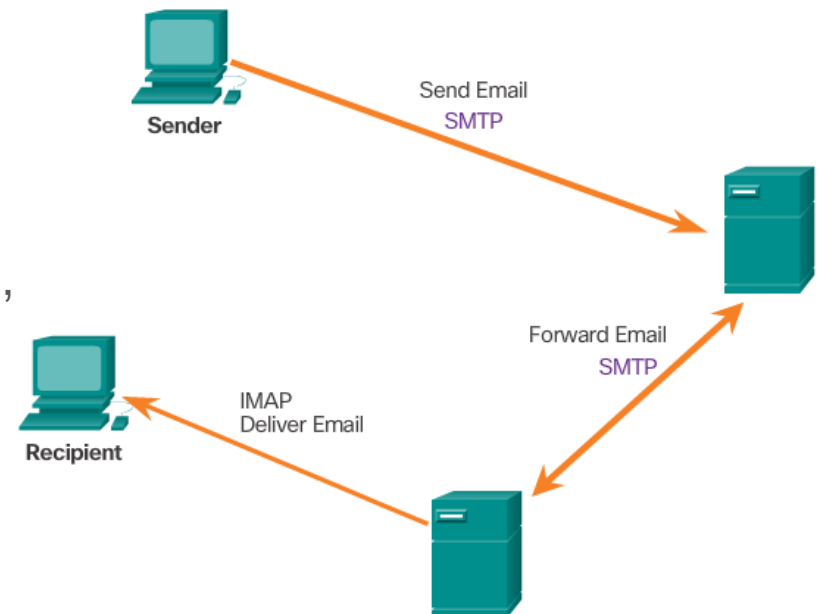
POP Operation

- Messages are downloaded from the server to the client.
- The server listens on port 110 TCP for client requests.
- Email clients direct their POP requests to mail servers on port TCP 110.
- The POP client and server exchange commands and responses until the connection is closed or aborted.
- POP allows for email messages to be downloaded to the client's device (computer or phone) and removed from the server.
- There is no centralized location where email messages are kept.
- A downloaded message resides on the device that triggered the download.



IMAP Operation

- IMAP is another protocol used to retrieve email messages.
- Allows for messages to be displayed to the user rather than downloaded.
- The original messages reside on the server until manually deleted by the user.
- Users view copies of the messages in their email client software.
- Users can create a folder hierarchy on the server to organize and store mail.
- That file structure is displayed on the email client.
- When a user decides to delete a message, the server synchronizes that action and deletes the message from the server.

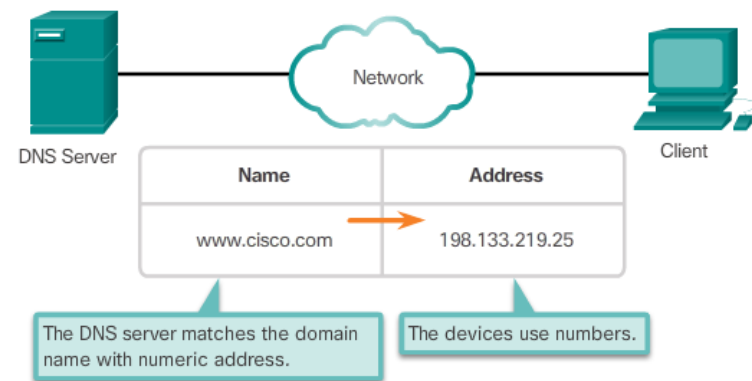
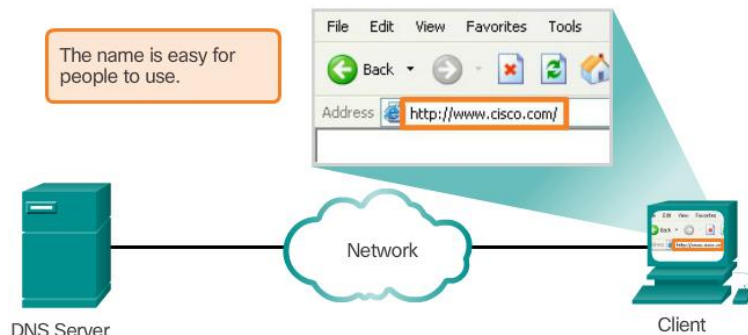


Topic 10.2.2: IP Addressing



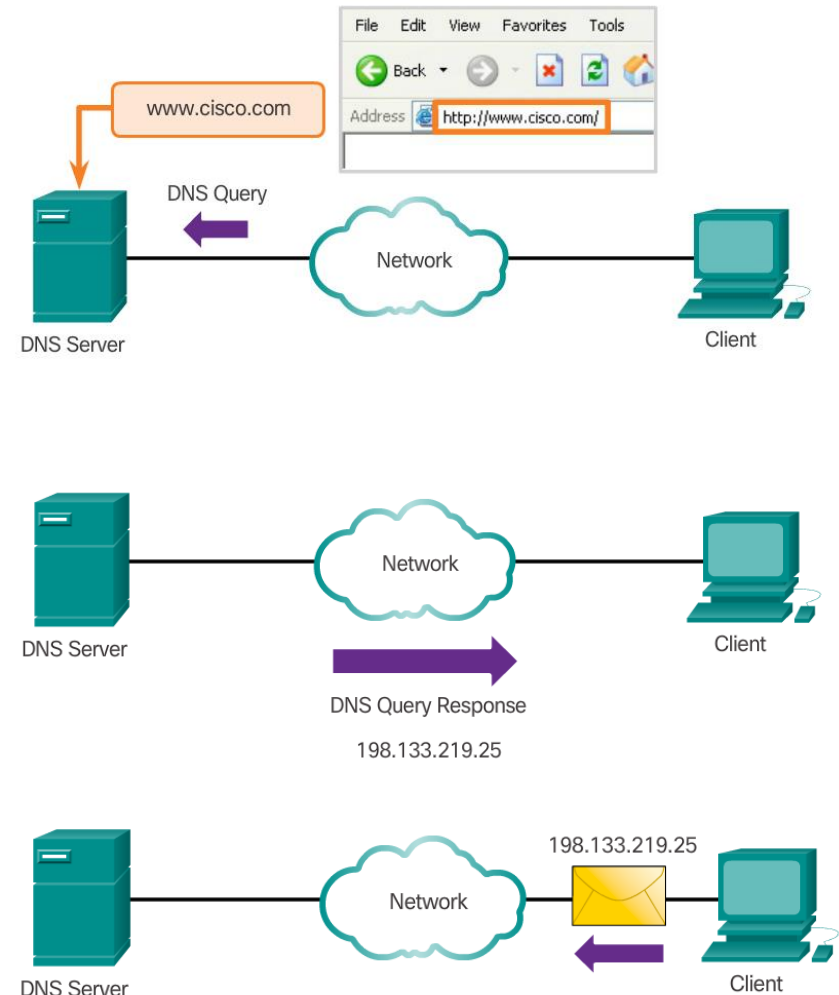
Domain Name Service

- While IP addresses are crucial for network communication, they are not easy to memorize.
- Domain names are created to make server addresses more user-friendly.
- Domain names such as <http://www.cisco.com> are user-friendly addresses associated with the IP address of a specific server.
- However, computers still need the actual numeric address before they can communicate.



Domain Name Service (cont.)

- The DNS protocol allows for the dynamic translation of a domain name into the correct IP address.
- The DNS protocol communications using a single format called a message.



DNS Message Format

- DNS supports different types of records. Some of these record types are:
 - **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
- DNS servers will first look at its own records to resolve the name. If the server is unable to resolve the name using its locally stored records, it relays the query to other servers.
- The response is then forwarded to the requesting client.
- The DNS Client service on Windows PCs also stores previously resolved names in memory.
- **ipconfig /displaydns** displays all of the cached DNS entries on Windows.

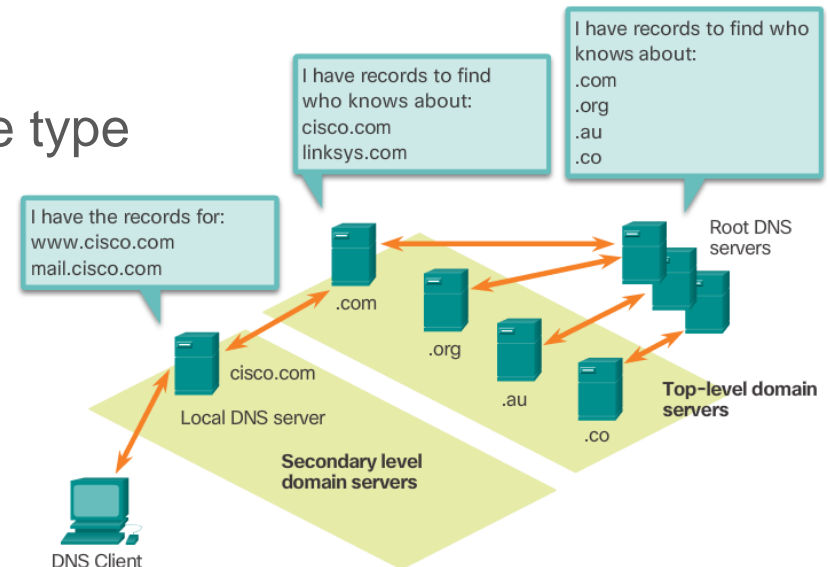
DNS uses the same message format for:

- all types of client queries and server responses
- error messages
- the transfer of resource record information between servers

Header	
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

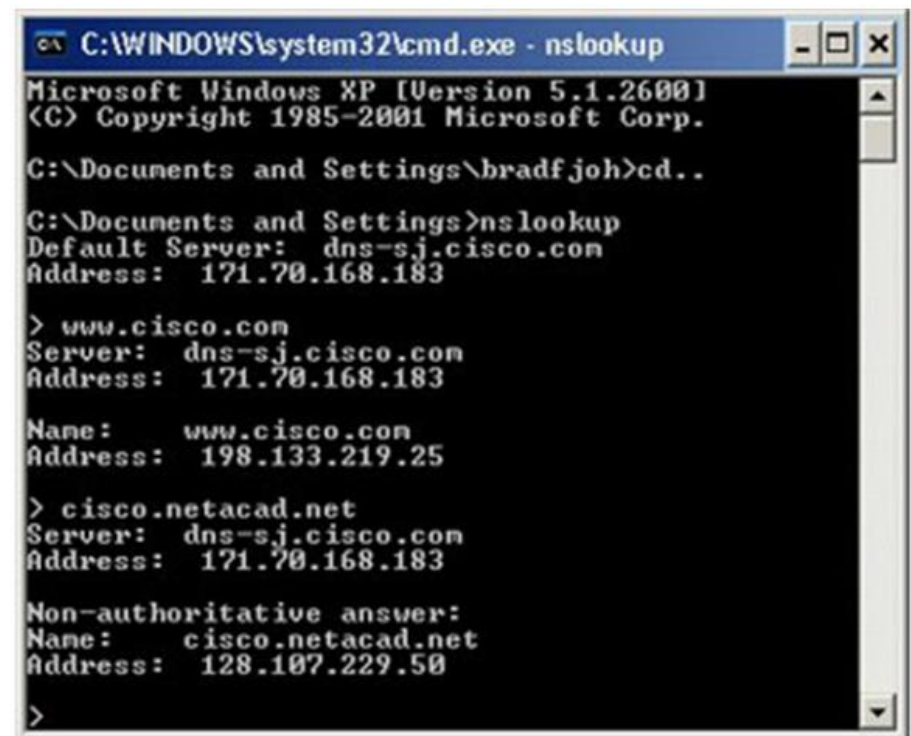
DNS Hierarchy

- The DNS protocol uses a hierarchical system, with the root at the top and branches below. The naming structure is broken down into small, manageable zones.
- Each DNS server is only responsible for managing name-to-IP mappings for that small portion of the DNS structure.
- Requests for zones not stored in a specific DNS server are forwarded to other servers for translation.
- Top-level domains represent either the type of domain or the country of origin. Examples of top-level domains are:
 - **.com** - a business or industry
 - **.org** - a non-profit organization
 - **.au** - Australia
 - **.co** - Colombia



The nslookup Command

- Allows the user to manually place DNS queries.
- It can also be used to troubleshoot name resolution issues.
- Has many options available for extensive testing and verification of the DNS process.



```
C:\WINDOWS\system32\cmd.exe - nslookup
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\bradfjoh>cd..

C:\Documents and Settings>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:    www.cisco.com
Address:  198.133.219.25

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

Non-authoritative answer:
Name:    cisco.netacad.net
Address:  128.107.229.50

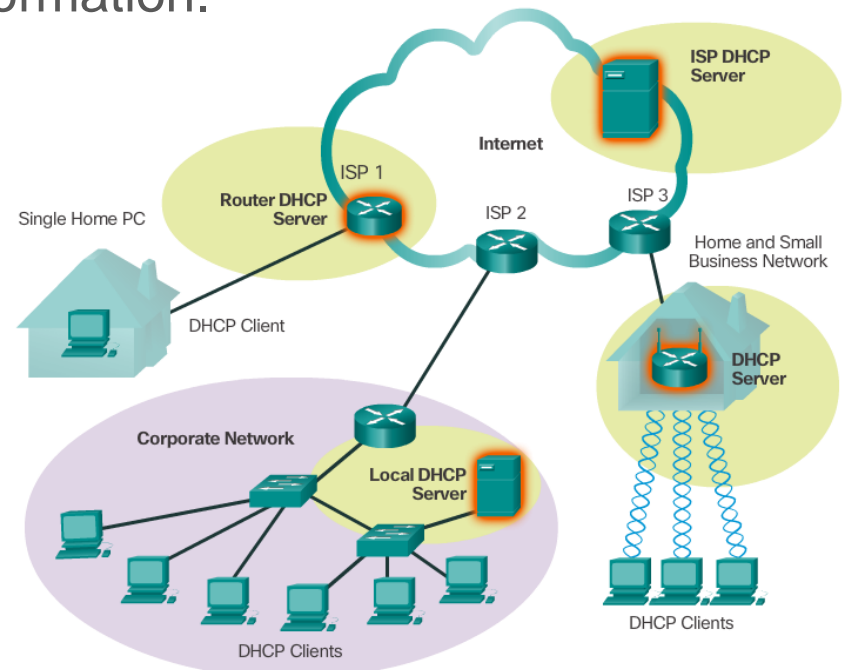
>
```

Topic 10.2.3: File Sharing Services



Dynamic Host Configuration Protocol

- Computers need network addresses to communicate over a network.
- Additional crucial information includes gateway address, subnet mask, and DNS server.
- Manually configuring end devices is not scalable. DHCP allows for automated distribution of network information.
- DHCP-distributed addresses are leased for a set period of time.
- Addresses are returned to the pool for reuse when no longer in use.
- DHCP supports IPv4 and DHCPv6 supports IPv6.



DHCP Operation

- A DHCP client goes through the following basic steps to request an IP:
 - The client broadcasts a DHCPDISCOVER.
 - A DHCP server replies with a DHCPOFFER message
 - The client sends a DHCPREQUEST message to the server it wants to use (in case of multiple offers).
- A client may also choose to request an address that it had previously been allocated by the server.
- The server returns a DHCPACK message to confirm the lease has been finalized.



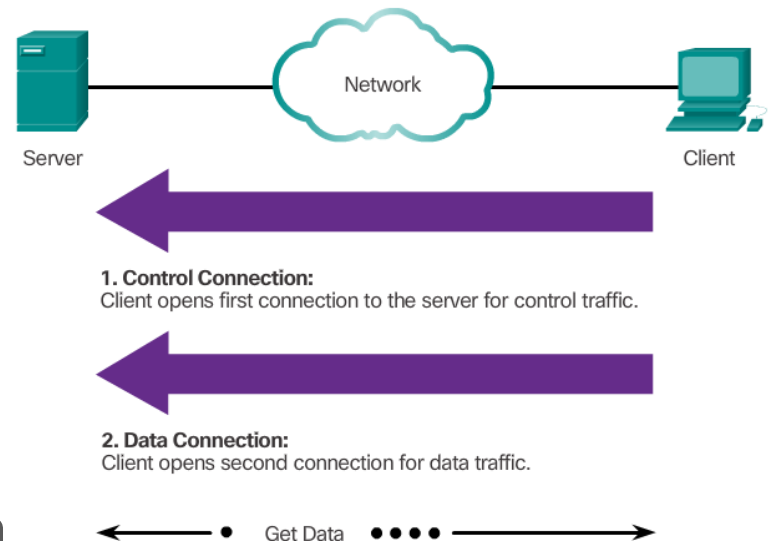
DHCP Operation (cont.)

- The server would respond with a DHCPNAK if the offer is no longer valid
- Leases must be renewed before its expiration through another DHCPREQUEST.
- DHCPv6 has a similar set of messages:
 - SOLICIT
 - ADVERTISE
 - INFORMATION REQUEST
 - REPLY



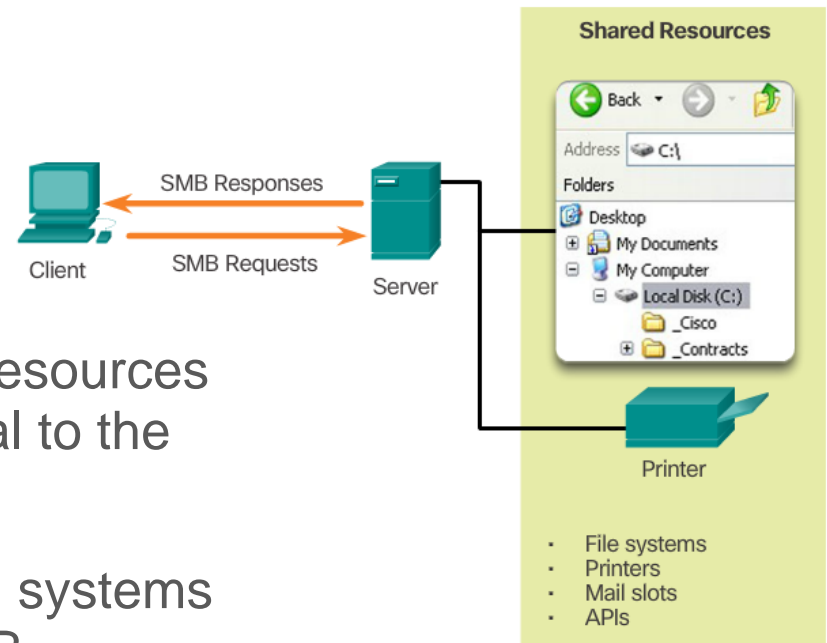
File Transfer Protocol

- FTP was developed to allow the transfer of files over the network.
- An FTP client is an application that runs on a client computer used to push and pull data from an FTP server.
- FTP requires two connections between the client and the server: one connection for commands and replies and another connection for the actual file transfer.
- The client initiates and establishes the first connection to the server for control traffic on TCP port 21.
- The client then establishes the second connection to the server for the actual data transfer on TCP port 20.
- The client can download (pull) data from the server or upload (push) data to the server.



Server Message Block

- SMB is a client/server file sharing protocol.
- All SMB messages share a common format.
- SMB file-sharing and print services have become the mainstay of Windows networking.
- Microsoft products now support TCP/IP protocols to directly support SMB resource sharing.
- After the connection is established, the user of the client can access the resources on the server as if the resource is local to the client host.
- The Mac, LINUX, and UNIX operating systems have their own implementation of SMB.



Section 10.3: Summary

Chapter Objectives:

- Explain the operation of the application layer in providing support to end-user applications.
- Explain how well-known TCP/IP application layer protocols and services operate.

Thank you.



Cisco Networking Academy
Mind Wide Open