Chapter 10: Application Layer

Introduction to Networks v6.0

Cisco | Networking Academy®
Mind Wide Open™

Chapter 10 - Sections & Objectives

10.0 Introduction

10.1 Application Layer Protocols

- 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.

10.2 Well-Known Application layer Protocols and Services

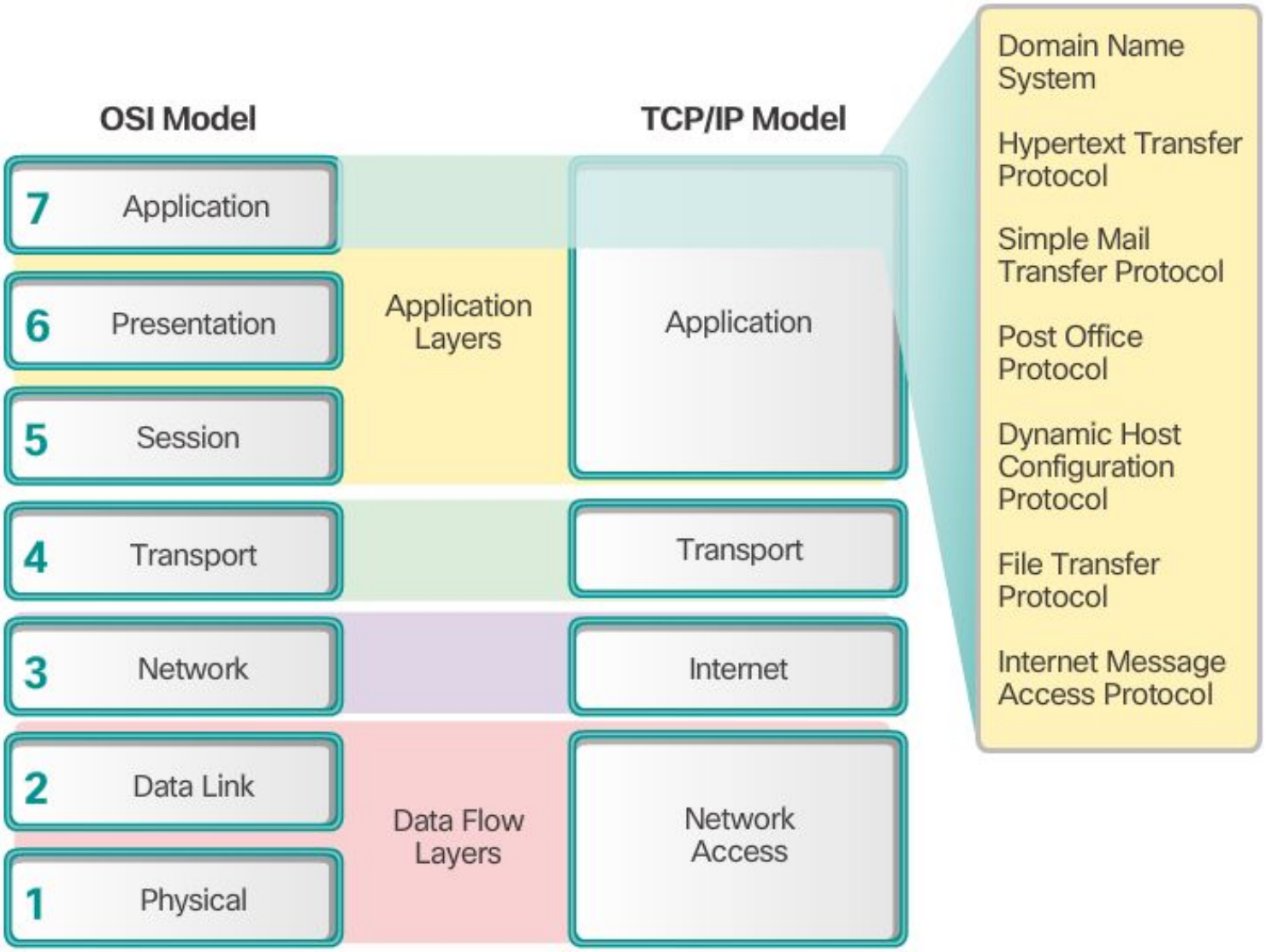
- Explain how web and email protocols operate.
- Explain how the IP addressing protocols operate.
- Explain how file transfer protocols operate.

10.3 Summary

10.1 Application Layer Protocols

Cisco | Networking Academy®
Mind Wide Open™

ISO/OSI and TCP/IP models

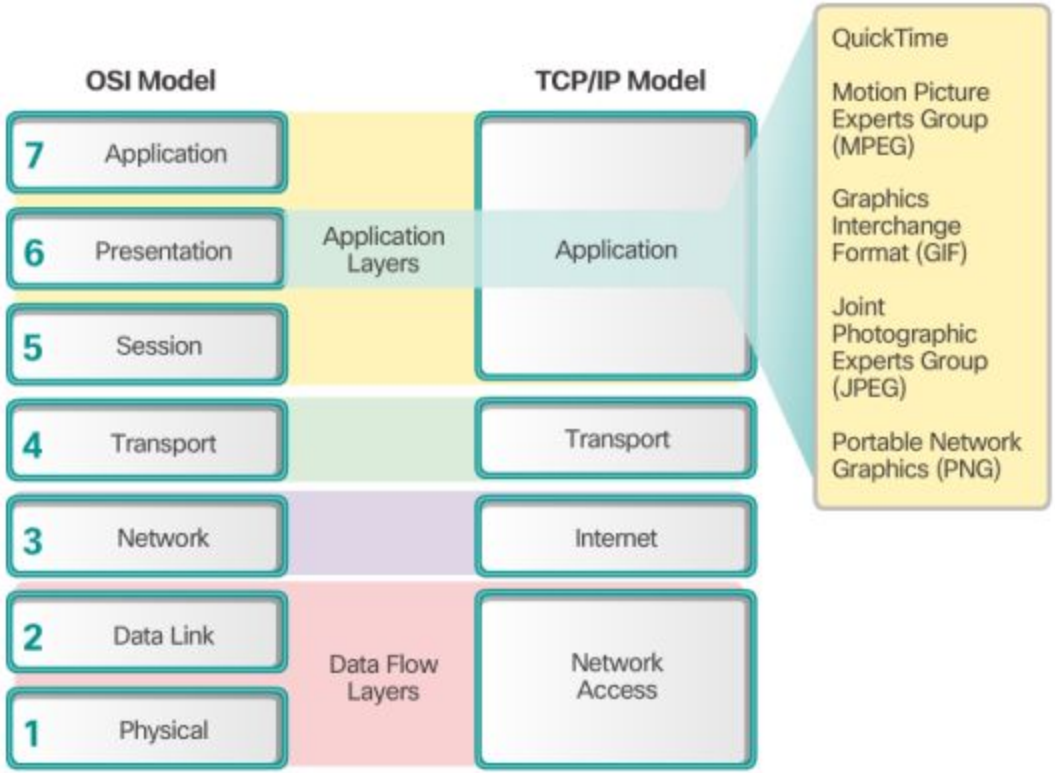


Application, Presentation, Session

- Application Layer
  - Closest to the end user.
  - 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 Layer

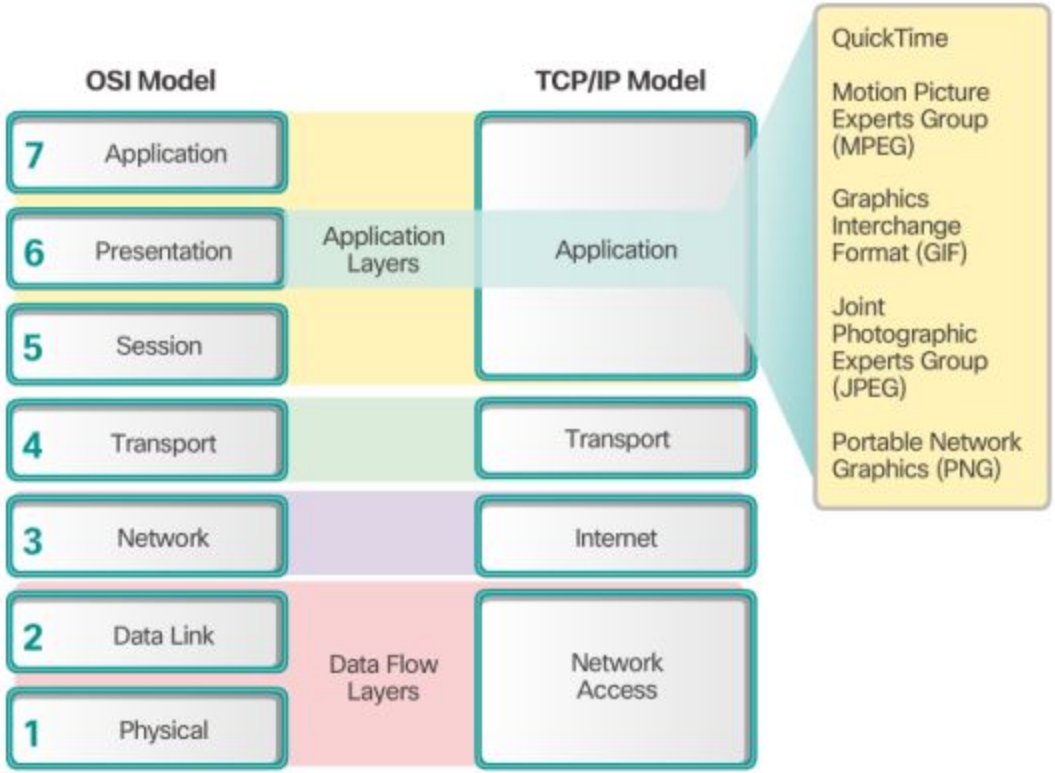
- Format (or present), compress and encrypt data
- The presentation layer formats data for the application layer, and it sets standards for file formats. Common standards for video include QuickTime and Motion Picture Experts Group (MPEG).
- Common graphic image formats are: GIF, JPEG and PNG



- Graphics Interchange Format (GIF)
- Joint Photographic Experts Group (JPEG)
- Portable Network Graphics (PNG) format

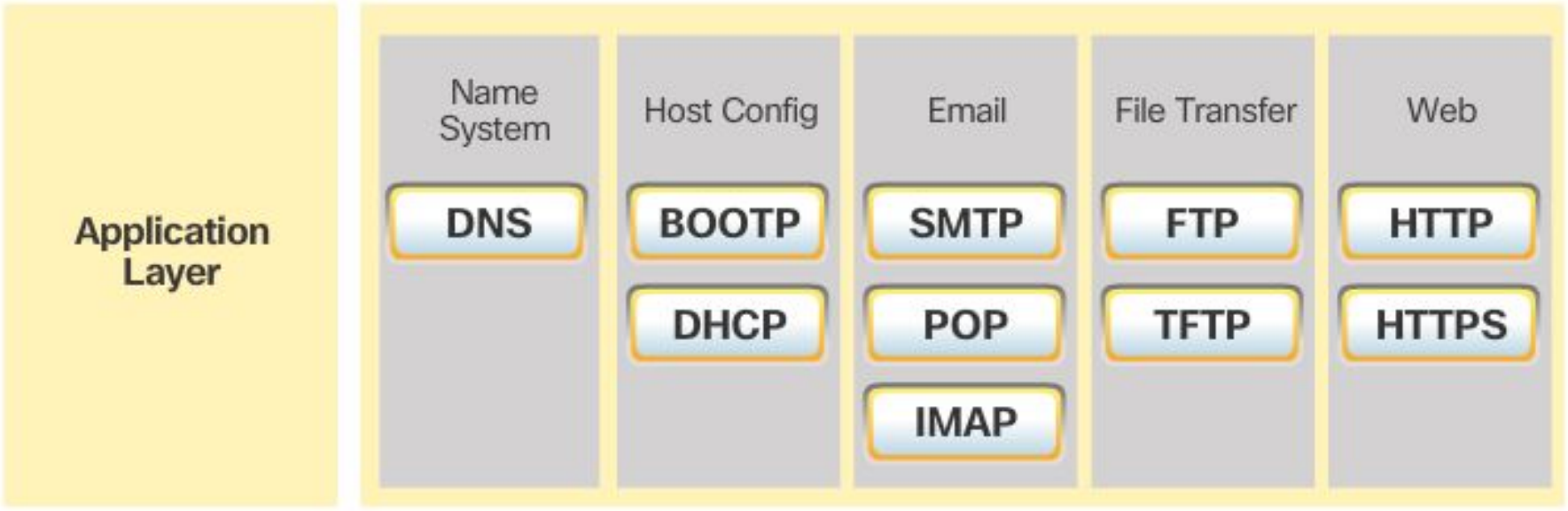
Session Layer

- 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.



TCP/IP Application Layer Protocols

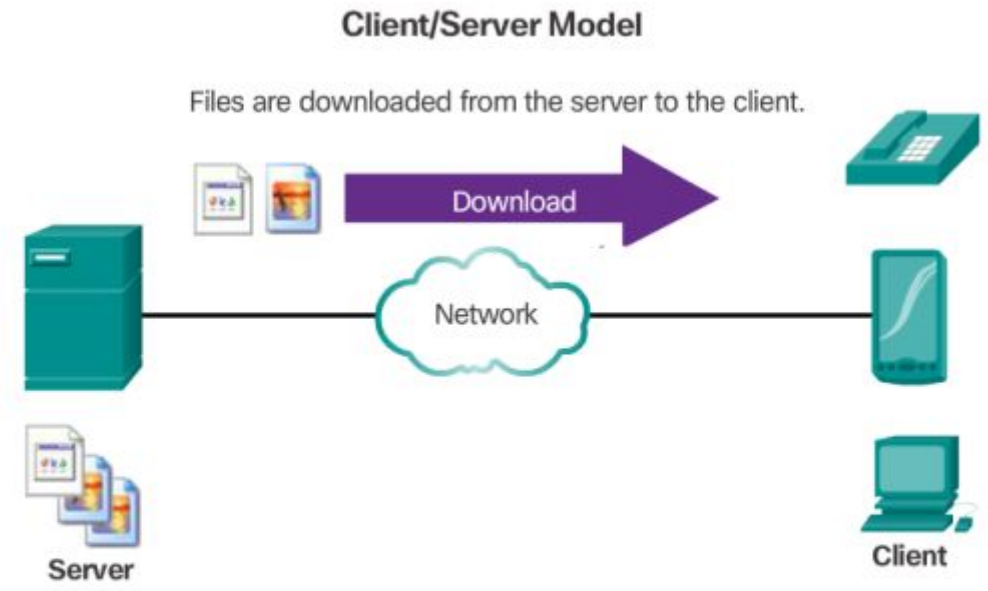
- TCP/IP application protocols specify the format and control information necessary for common Internet functions.
- Application layer protocols must be implemented in both the source and destination devices.
- Application layer protocols implemented on the source and destination host must be compatible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



How Application Protocols Interact with End-User Applications

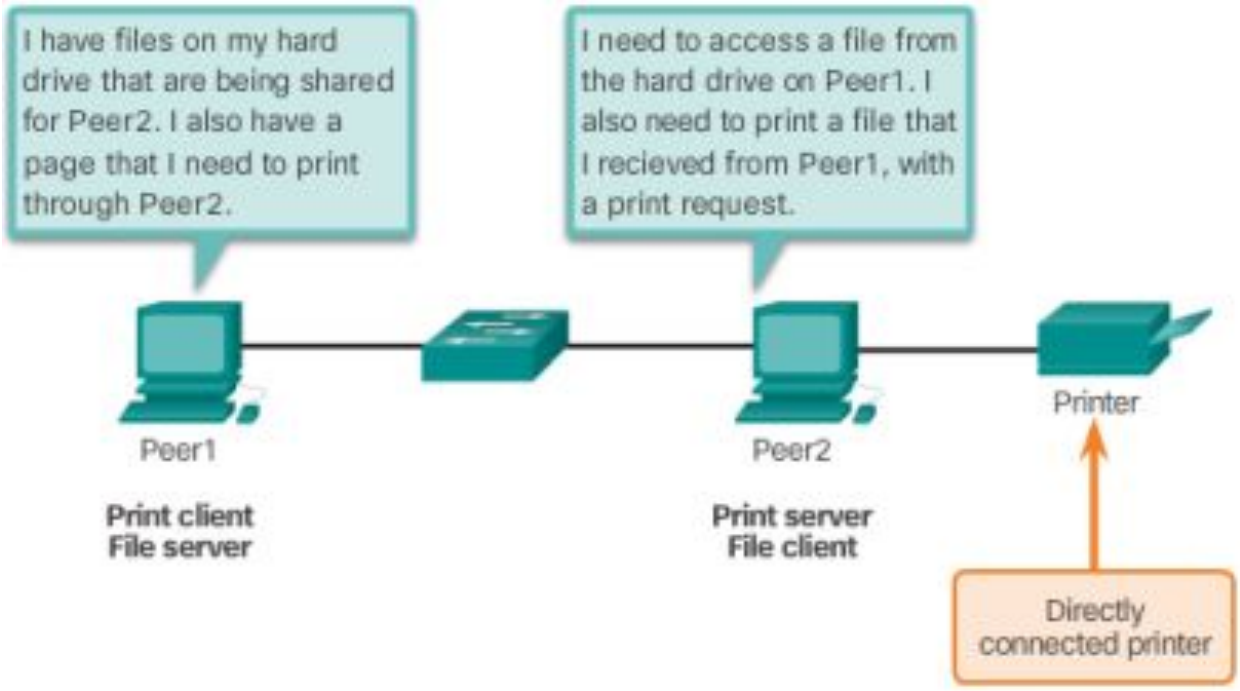
- Client-Server Model
  - Clients request information while servers provide it.
  - Client and server processes are considered to be in the application layer.
  - The contents of the data exchange will depend of the application in use.
  - Email is an example of a Client-Server interaction.

- 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.



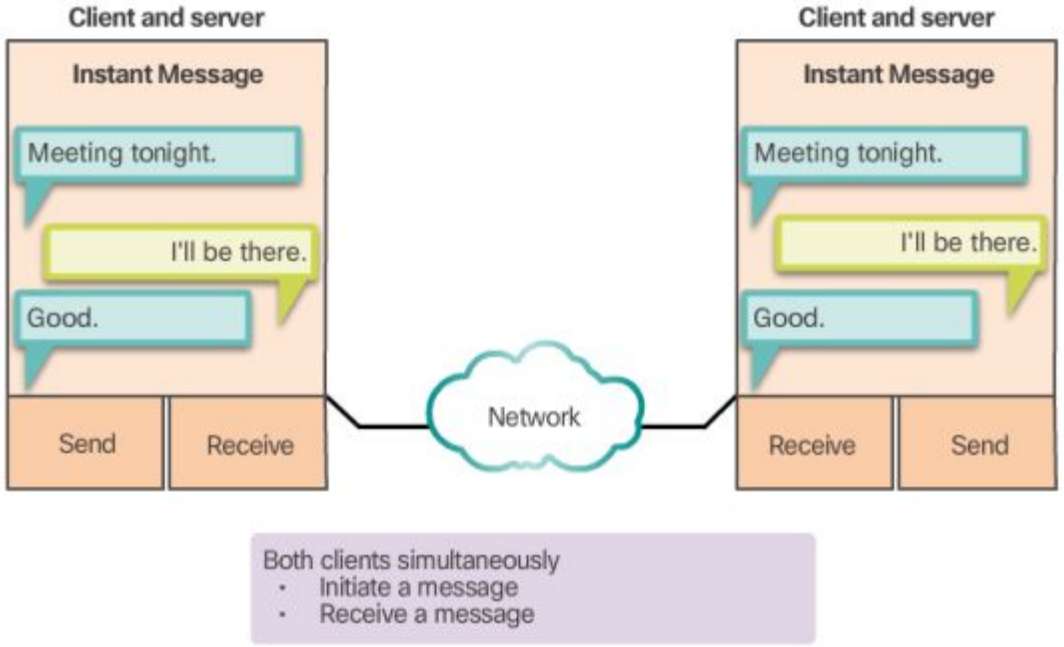
How Application Protocols Interact with End-User Applications

- Peer-to-Peer Networks
  - 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.



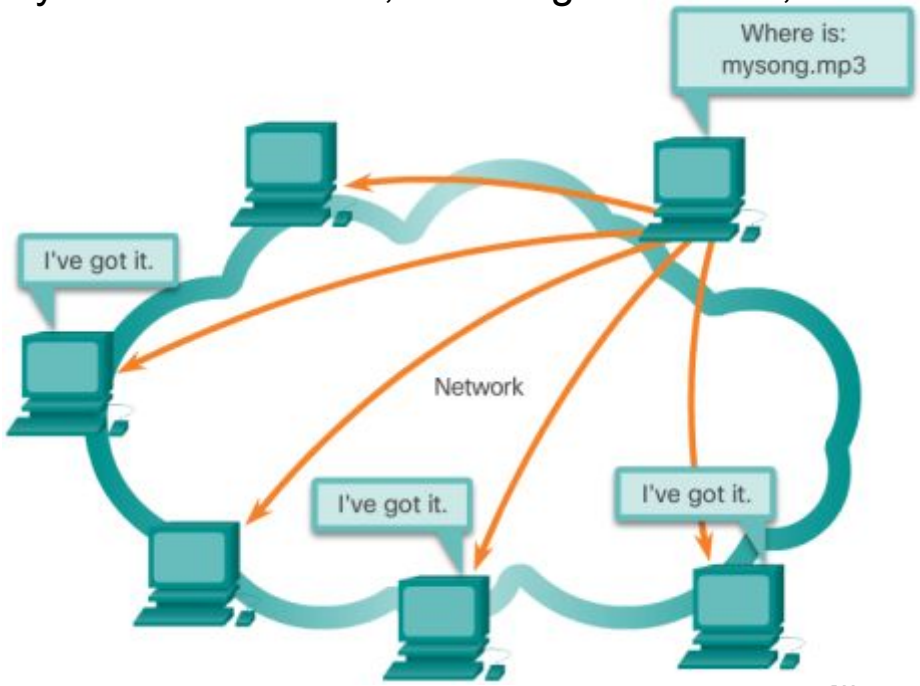
How Application Protocols Interact with End-User Applications (Cont.)

- Peer-to-Peer Applications
  - Some P2P applications use a hybrid system, where 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.
- 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.

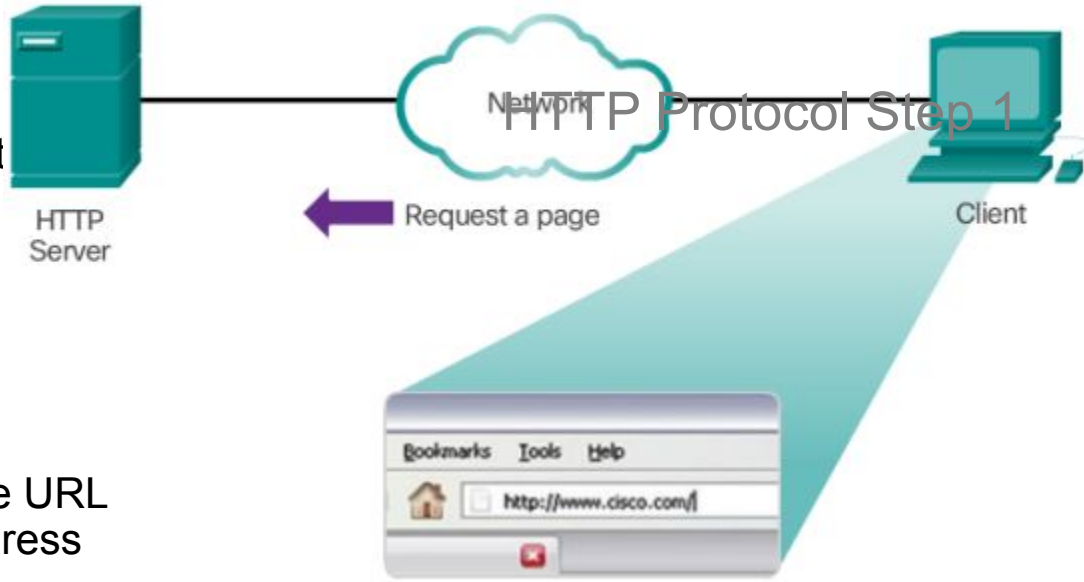


10.2 Well-Known Application Layer Protocols and Services

Cisco | Networking Academy®
Mind Wide Open™

Web Protocols

- Hypertext transfer Protocol and Hypertext Markup Language
- **URI** (Uniform Resource Identifier, RFC 2396) – Internet standard allowing resource identification, URI - URL or URN
- URLs and URIs are the names most people associate with web addresses.
- **URL** (Uniform Resource Locator, localisation) is a reference to a web server.
- 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 request



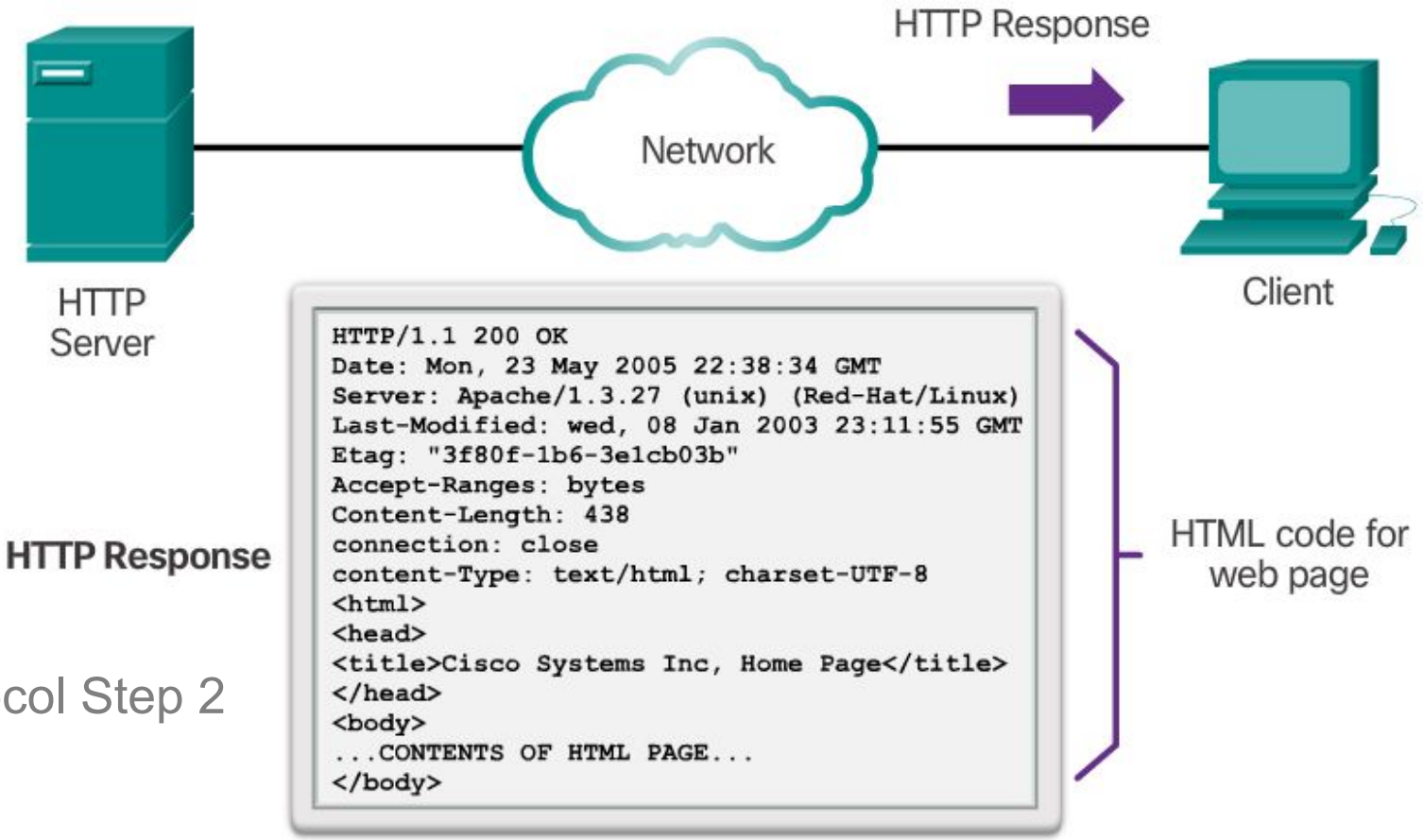
URN (Uniform Resource Name) – uniform name format

Using DNS, the server name portion of the URL is then translated to the associated IP address before the server can be contacted.

URI: http://www.domena.pl:8080/katalog1/plik1?parametr1=wartosc1&parametr2=wartosc2#tekst

HTTP and HTTPS (port 80, 443)

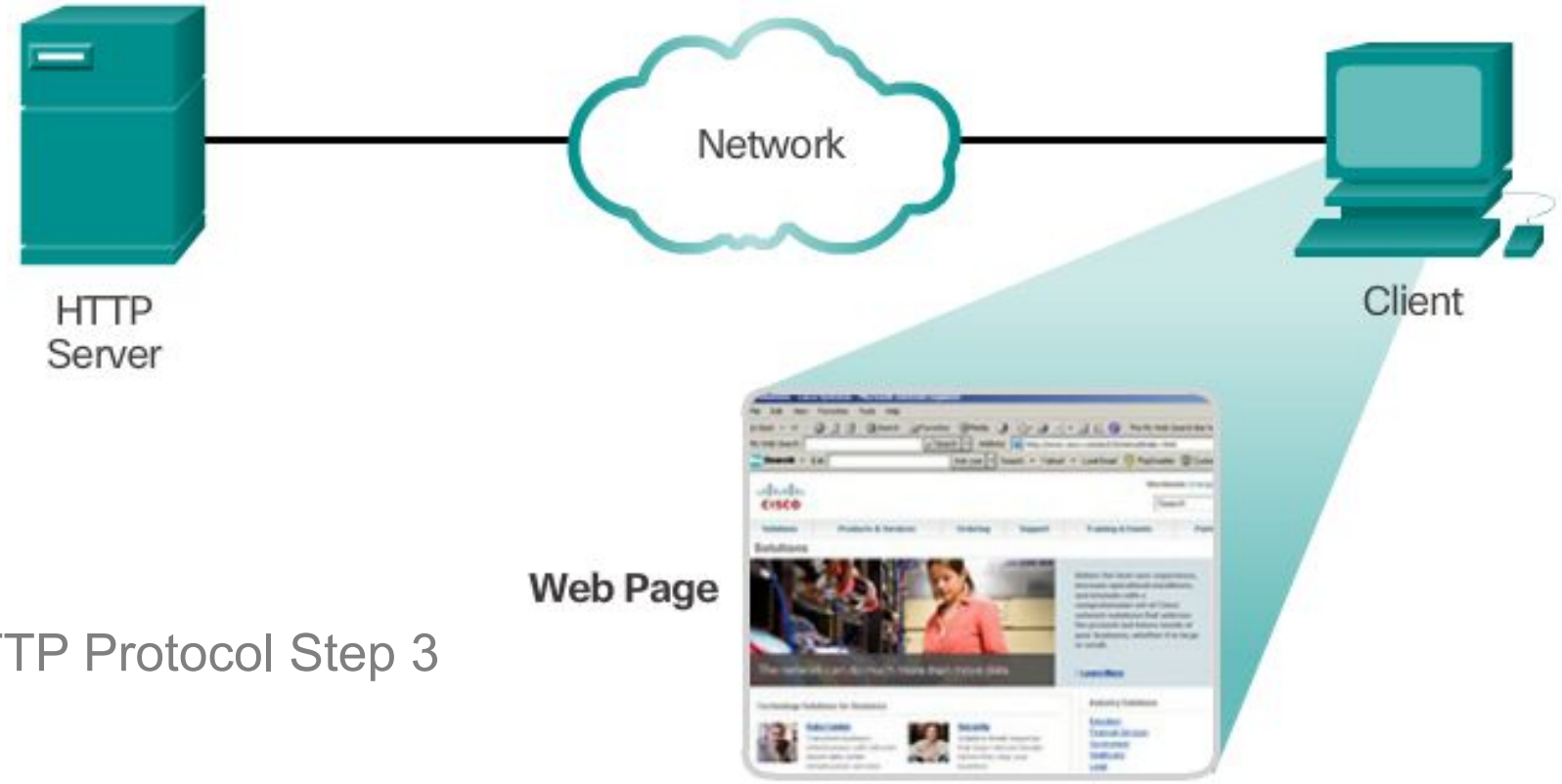
- The browser sends a GET request to the server's IP address and asks for the index.html file (step 1).
- The server sends the requested file to the client (step 2).
- The **index.html** was specified in the URL and contains the HTML code for this web page.



HTTP Protocol Step 2

HTTP and HTTPS

- The browser processes the HTML code and formats the page for the browser window based on the code in the file.



HTTP Protocol Step 3

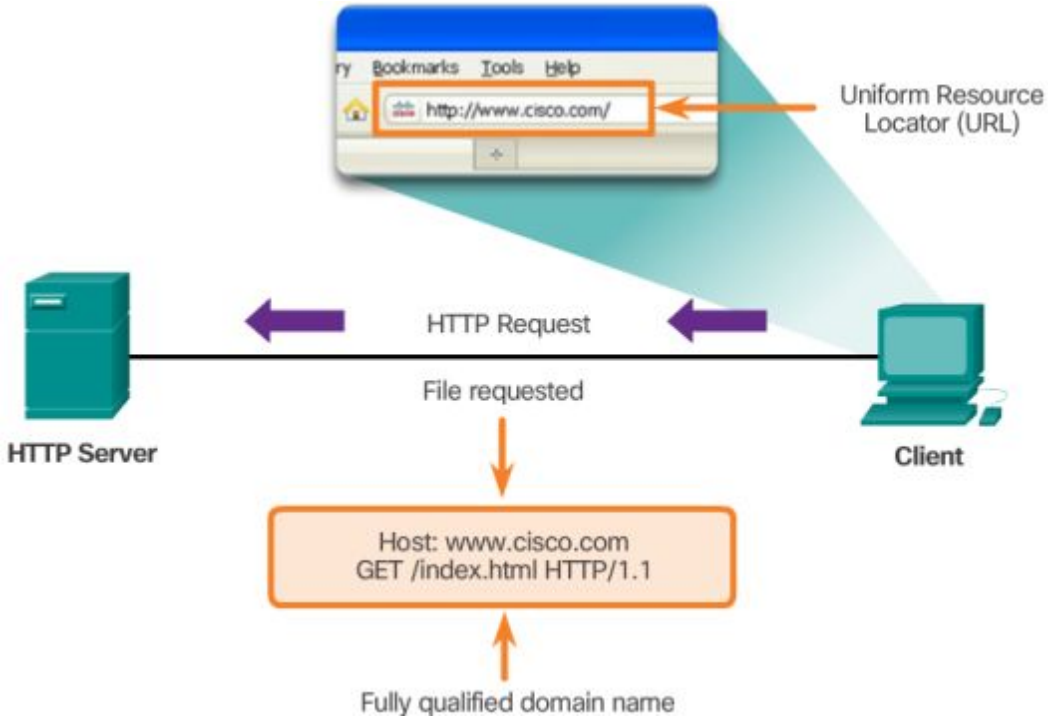
HTTP and HTTPS

HTTP

- is a request/response protocol,
- has three common message types: **GET** (download), **POST** (add new resource if we do not know destination (URL), modify and update a existing resource), **PUT** (create (id derives from client) or overwrite by new URL, **DELETE**),
- is not secure.

Messages can be captured.

HTTPS uses authentication and encryption to secure data.



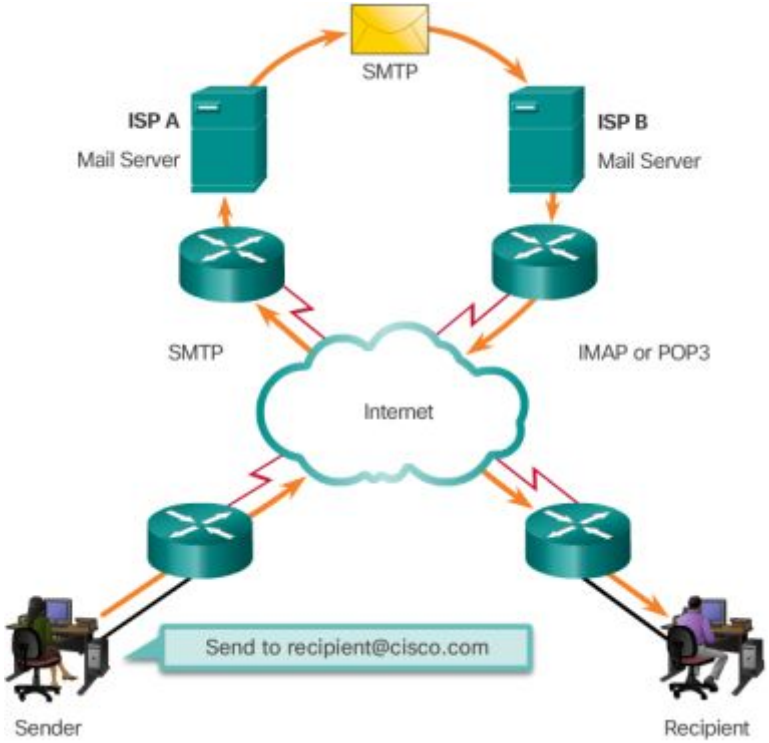
Email Protocols

- Email is a store-and-forward method of sending, storing, and retrieving electronic messages.
- Email messages are stored 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 relies on three separate protocols for operation:

SMTP (sending)

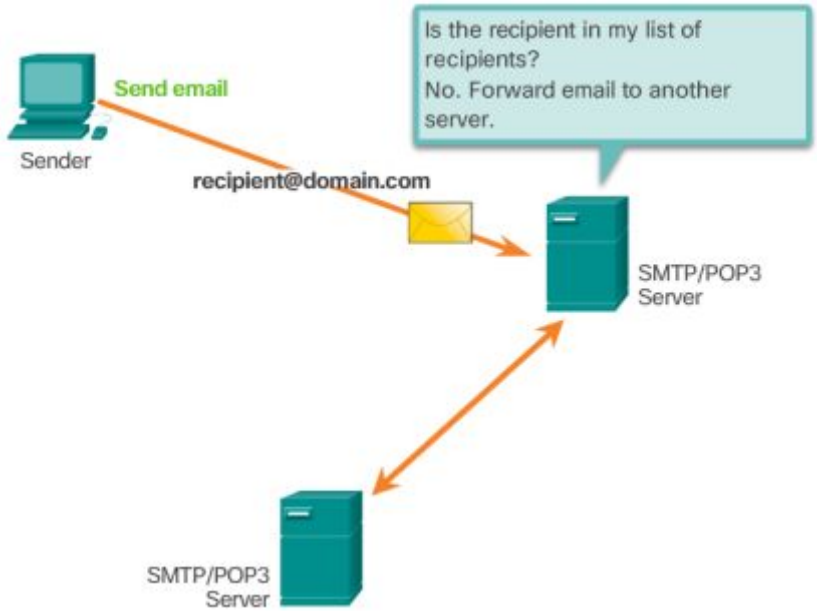
POP (retrieving) and IMAP (retrieving).



SMTP Operation

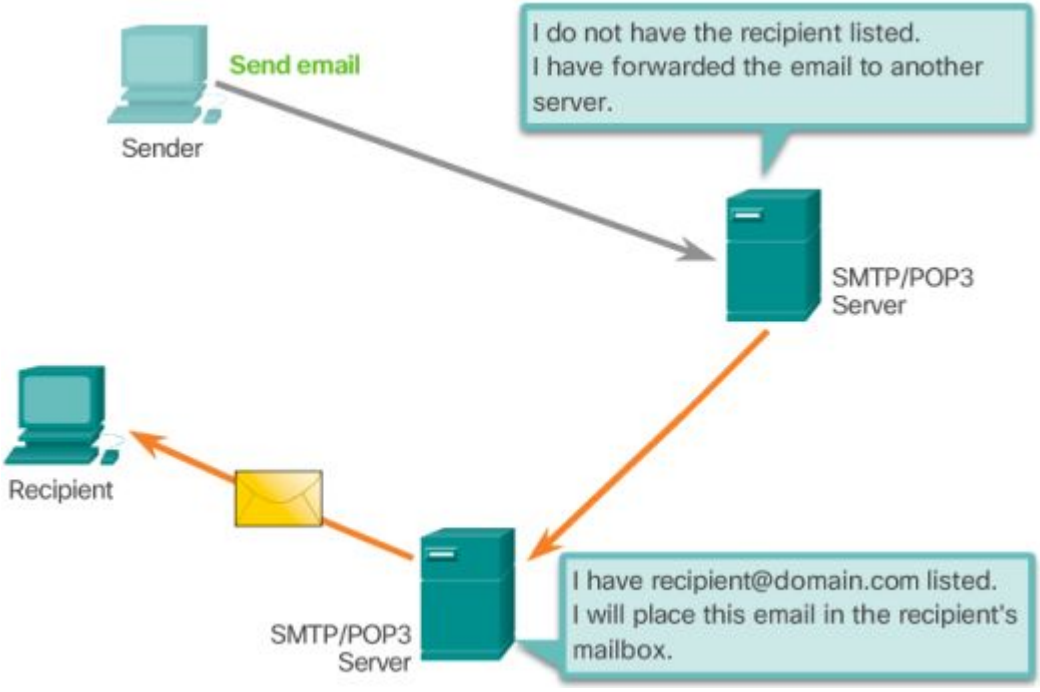
- SMTP message formats require a message **header** and **body**.
- The header must have a properly formatted recipient email address and a sender address.
- An SMTP client sends an email by connecting to a **SMTP server on port 25**.
- The server receives the message and stores it in a local mailbox 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.
- Email clients direct their POP requests to mail servers on **port TCP 110**.
- POP allows for email messages to be downloaded to the client's device (computer or phone) and removed from the server.
- A downloaded message resides on the device that triggered the download.

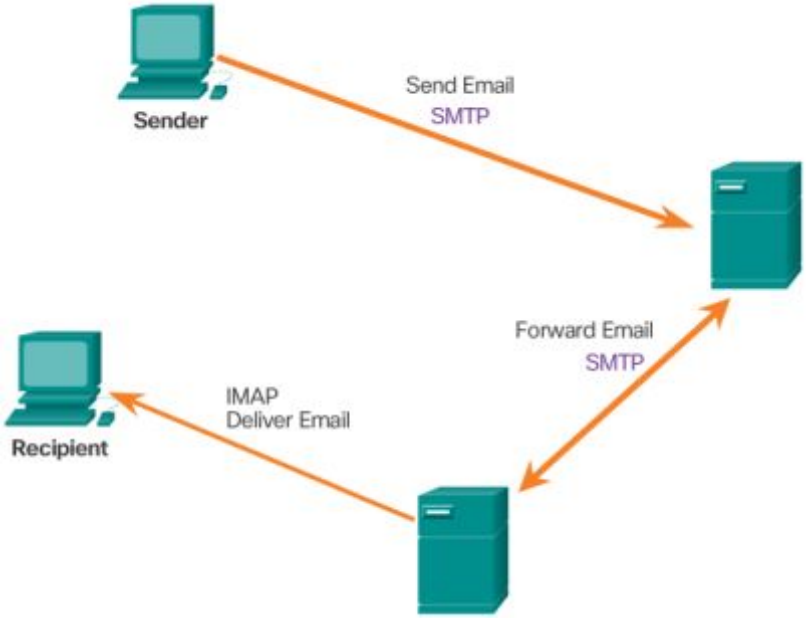


IMAP Operation

- IMAP is another protocol used to retrieve email messages (**port 143**).
- 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 (on the client device).
- Users view copies of the messages in their email client software.

Support folder hierarchy to organize and store mail. 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.

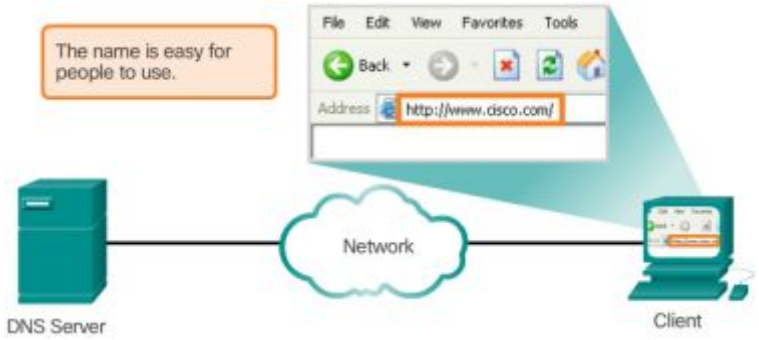


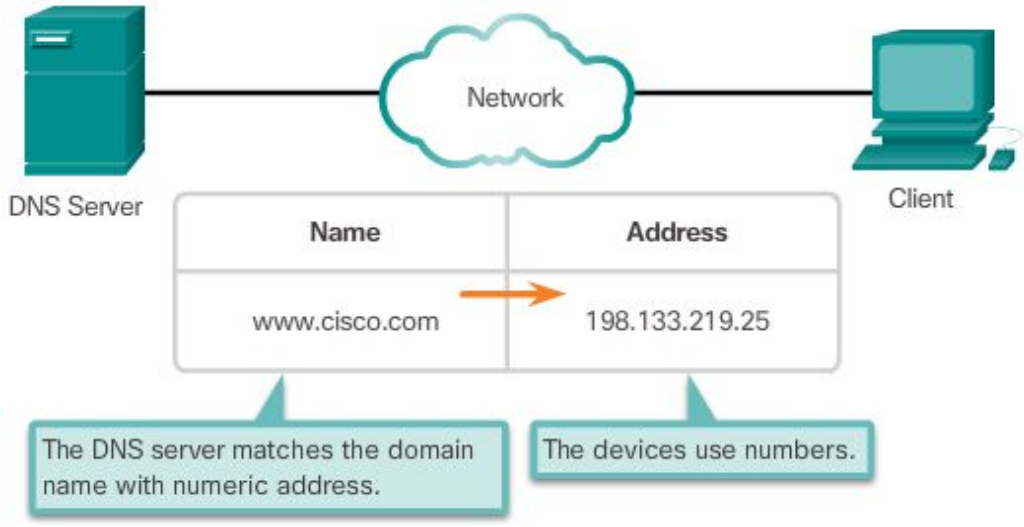
Email port numbers in the practice

Service	Port	Port SSL
SMTP	587 25 (deprecated)	465
POP3	110	995
IMAP	143	993

IP Addressing Services

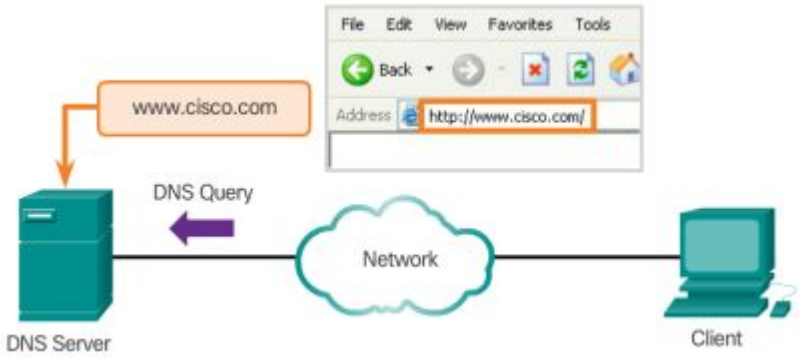
- Domain Name Service
  - IP addresses are not easy to memorize.
  - Domain names make server addresses more user-friendly.
  - Computers still need the actual numeric address before they can communicate.
  - The DNS protocol allows for the dynamic translation of a domain name into the associated IP address.





DNS

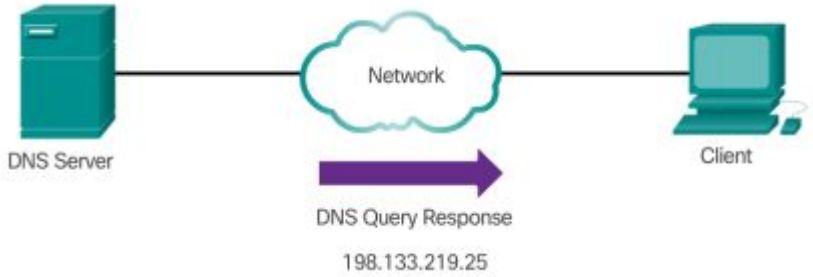
- The DNS protocol allows for the dynamic translation of a domain name into the correct IP address.
- The DNS protocol communications using a single format called a message.
- TCP and UDP **port 53**



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

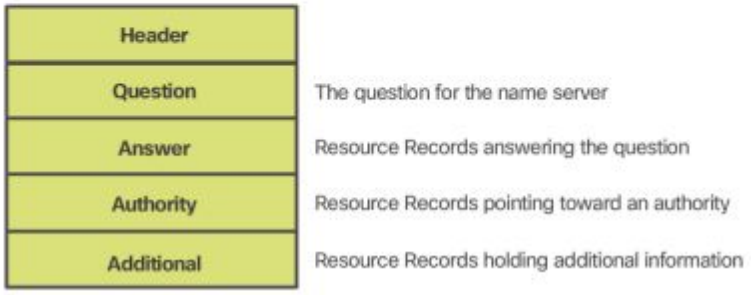


DNS Message Format

- 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
  - **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.

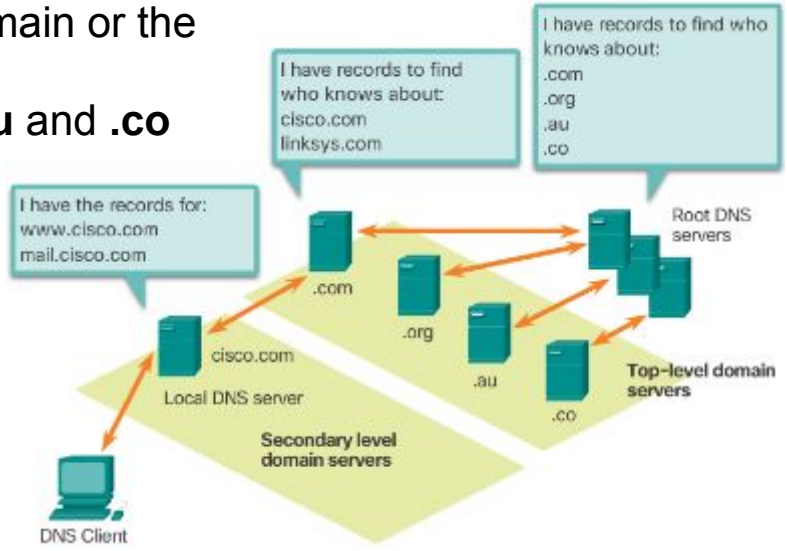
DNS uses the same message format for:

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

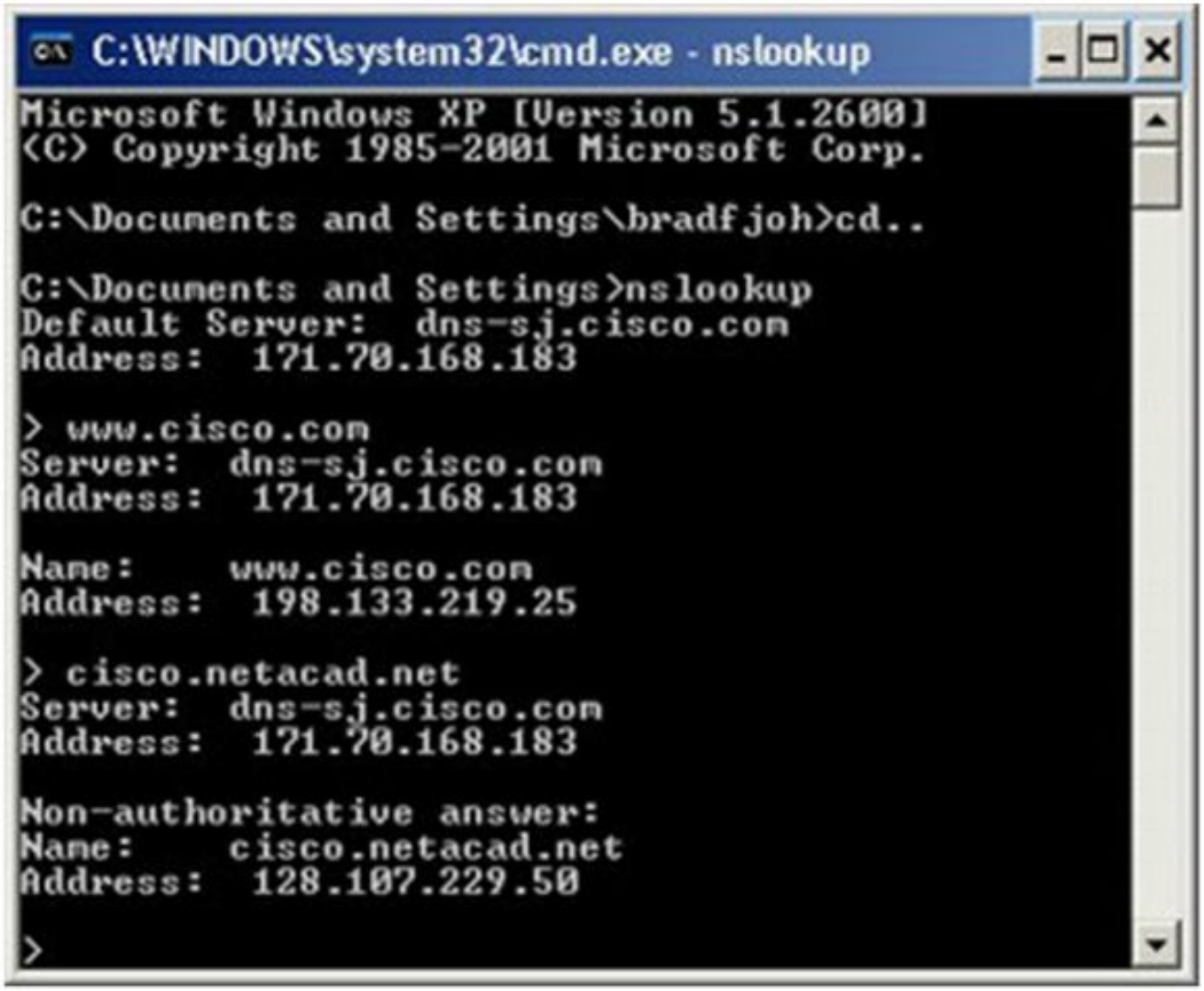


IP Addressing Services (Cont.)

- DNS Hierarchy
  - The DNS protocol uses a hierarchical system.
  - The naming structure is broken down into small, manageable zones.
  - Each DNS server is only responsible for managing name-to-IP mappings for a 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**, **.org**, **.au** and **.co**
- The nslookup Command
  - Use **nslookup** to place DNS queries.
  - Useful for DNS troubleshooting.

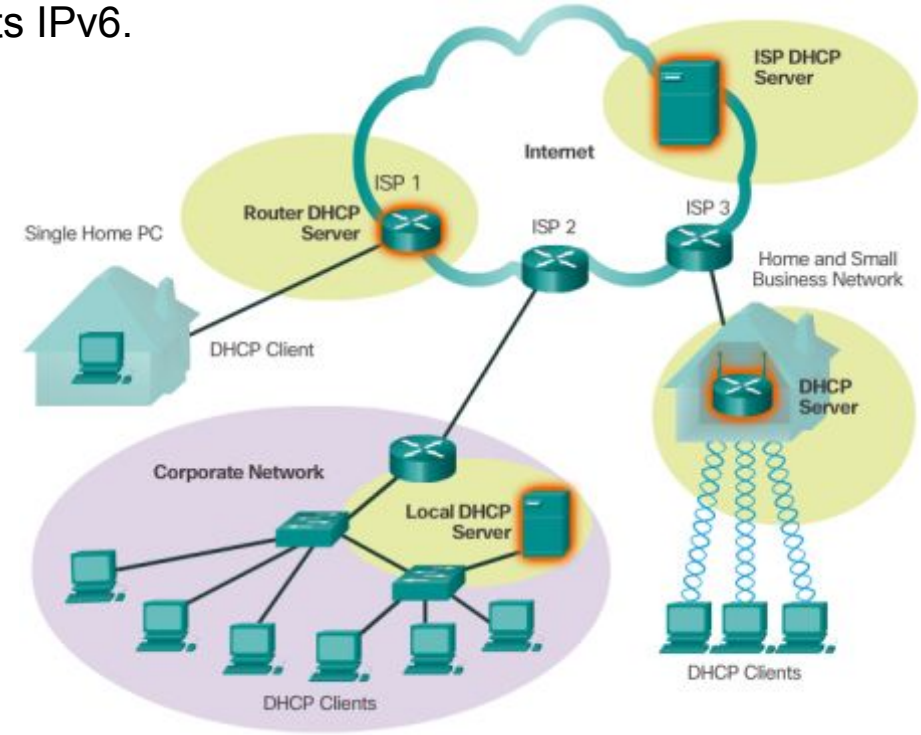


nslookup



IP Addressing Services (Cont.)

- Dynamic Host Configuration Protocol
  - Computers need network IP information to communicate over a network.
  - IP information include host and gateway addresses, mask, and DNS server.
  - DHCP allows for automated and scalable distribution of IP 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.



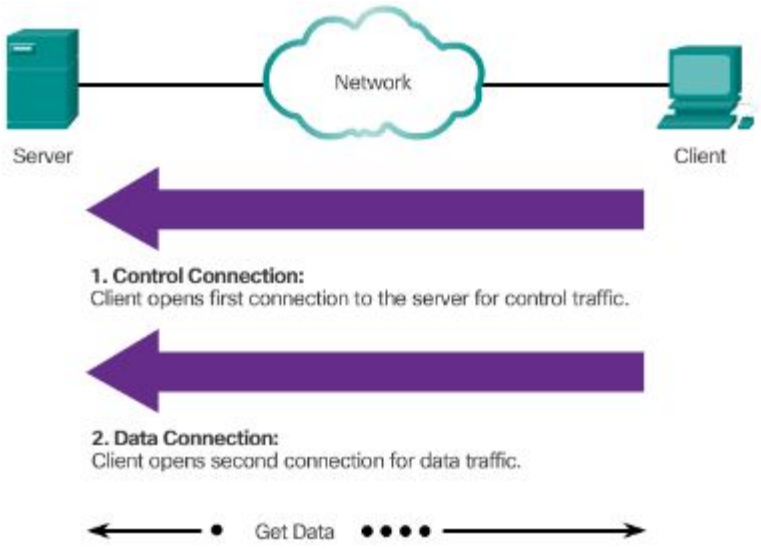
DHCP Operation

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

DHCP UDP
IPv4 client src port 68 and dest port 67
IPv6 client sends requests to dest port 547
and server sends to dest port 546

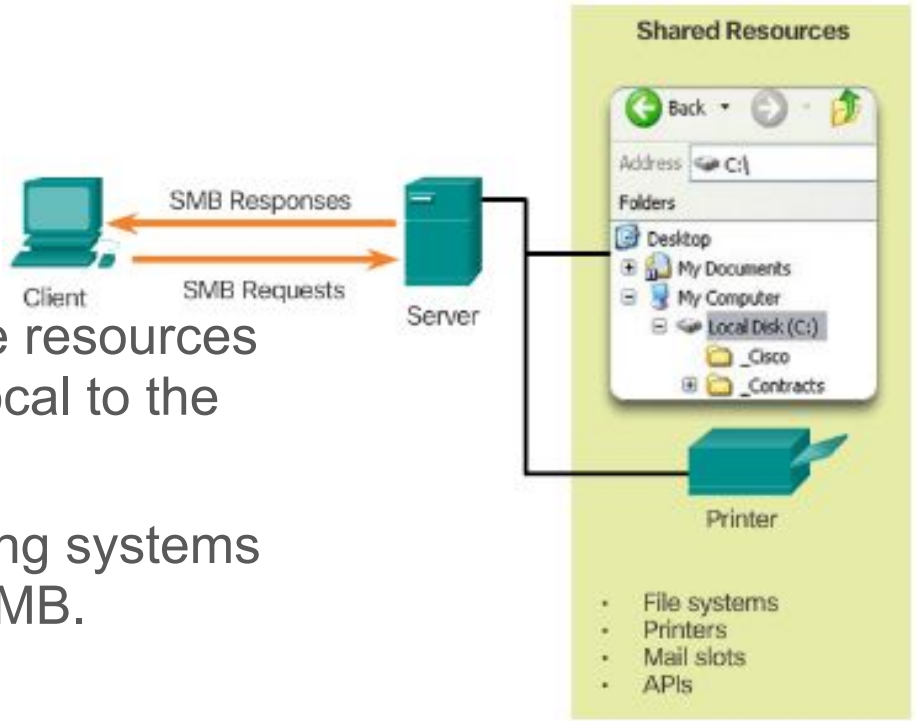
File Sharing Services

- 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.



File Sharing Services (Cont.)

- 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.



10.3 Summary

Cisco | Networking Academy®
Mind Wide Open™

Chapter Summary

Summary

- 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.

New Terms and Commands

- Hypertext Transfer Protocol (HTTP)
- File Transfer Protocol (FTP)
- Trivial File Transfer Protocol (TFTP)
- Internet Message Access Protocol (IMAP)
- Domain Name System (DNS)
- Simple Mail Transport Protocol (SMTP)
- Post Office Protocol (POP)
- Dynamic Host Configuration Protocol (DHCP)
- QuickTime and Motion Picture Experts Group (MPEG)
- Graphics Interchange Format (GIF)
- Joint Photographic Experts Group (JPEG)
- Portable Network Graphics (PNG)
- BOOTP
- HTTPS
- Client-server model
- Peer-to-peer network (P2P)
- P2P networks
- P2P applications
- Gnutella protocol
- BitTorrent
- Uniform Resource Locator (URL)
- Uniform Resource Identifier (URIs)
- Get
- Post
- Put
- HTTP Secure (HTTPS)
- Secure Socket Layer (SSL)
- Simple Mail Transfer Protocol (SMTP)
- Post Office Protocol (POP)

New Terms and Commands

- IMAP
- Port 25 (SMTP)
- TCP Port 110 (POP)
- Domain name
- DNS Protocol
- Record types: A, NS, AAAA, MX
- ipconfig /displaydns
- Top-level domains are: .com, .org, .au, .co
- 10.2.2.4
- Nslookup
- 10.2.2.5
- Dynamic Host Configuration Protocol (DHCP) for IPv4
- DHCPv6
- 10.2.2.6
- DHCP Discover
- DHCP Offer
- DHCP Request
- DHCP Acknowledgement
- DHCP Negative Acknowledgement
- DHCPv6: SOLICIT, ADVERTISE, INFORMATION REQUEST, and REPLY
- 10.2.3.1
- FTP daemon (FTPd)
- 10.2.3.2
- Server Message Block (SMB)