Elk Technologies
https://elktech.org
Scott Stephenson

Module 15: Application Layer

Introduction to Networks

Cisco | Networking Academy®
Mind Wide Open™

Module Objectives

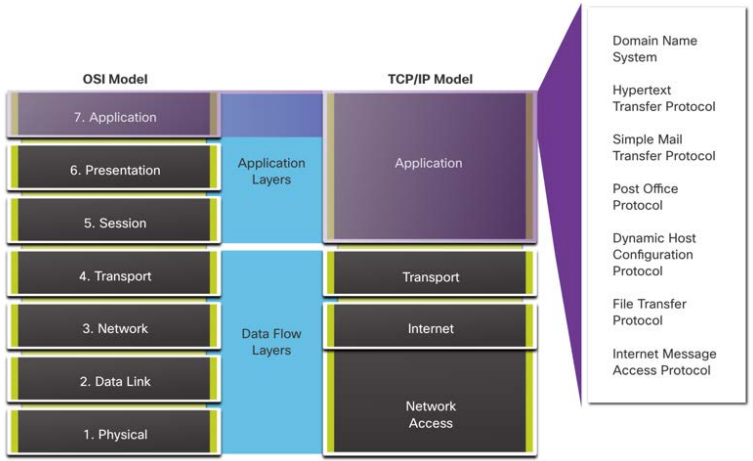
- Module Title: Application Layer
- Module Objective: Explain the operation of application layer protocols in providing support to end-user applications.

Topic Title	Topic Objective
15.1 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.
15.2 Peer-to-Peer	Explain how end user applications operate in a peer-to-peer network.
15.3 Web and Email Protocols	Explain how web and email protocols operate.
15.4 IP Addressing Services	Explain how DNS and DHCP operate.
15.5 File Sharing Services	Explain how file transfer protocols operate.

15.1 Application, Presentation, and Session

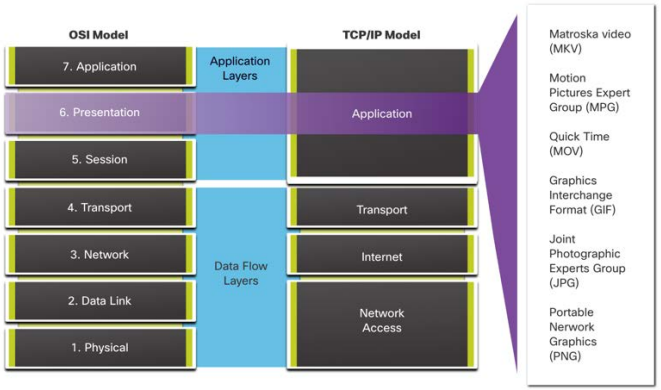
Application Layer

- The upper three layers of the OSI model (application, presentation, and session) define functions of the TCP/IP application layer.
- The application layer provides the interface between the applications used to communicate, and the underlying network over which messages are transmitted.
- Closest to the end user.
- Protocols help exchange data between programs running on the source and destination hosts.
- Some of the most widely known application layer protocols include HTTP, FTP, TFTP, POP3, IMAP, DHCP, and DNS.



Presentation Layer

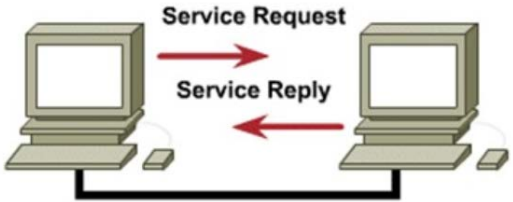
- The presentation layer has three primary functions:
  - **Formatting**, or presenting, data at the source device into a compatible format for receipt by the destination device (**Syntax**).
  - **Compressing** data in a way that can be decompressed by the destination device.
  - **Encrypting** data for transmission and decrypting data upon receipt.
- Common standards for video include QuickTime and Motion Picture Experts Group (MPEG).
- Common graphic image formats are: GIF, JPEG and PNG.



Session Layer

- The session layer functions:
  - It creates and maintains dialogs between source and destination applications.
  - It 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.

- Network File System (NFS)
- Structured Query Language (SQL)
- Remote-Procedure Call (RPC)
- X Window System
- AppleTalk Session Protocol (ASP)
- DNA Session Control Protocol (SCP)



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.

Name System
DNS - Domain Name System (or Service)

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

Host Config
DHCP - Dynamic Host Configuration Protocol

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

Web
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

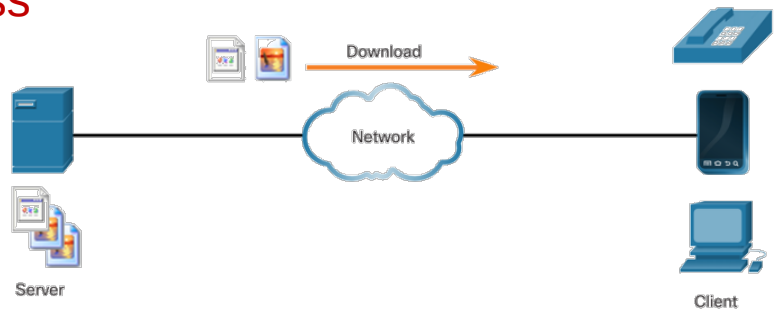
Common TCP and UDP Port Addressing

Destination Port	Protocol	Used By	Definition
20 & 21	FTP	TCP	File Transfer Protocol (20 for data; 21 for control)
22	SSH	TCP	Secure Shell
23	TELNET	TCP	TELetype NETwork
25 or 465 or 587	SMTP	TCP	Simple Mail Transfer Protocol
53	DNS	Both	Domain Name Service
67	DHCP Server	UDP	Dynamic Host Configuration Protocol (server)
68	DHCP Client	UDP	Dynamic Host Configuration Protocol (client)
69	TFTP	UDP	Trivial File Transfer Protocol
80	HTTP	TCP	Hypertext Transfer Protocol
110 or 995	POP3	TCP	Post Office Protocol version 3
143 or 993	IMAP4	TCP	Internet Message Access Protocol version 4
443	HTTPS	TCP	Hypertext Transfer Protocol Secure
3389	RDP	TCP	Remote Desktop Protocol
161 & 162	SNMP	UDP	Simple Network Management Protocol

15.2 Peer-to-Peer

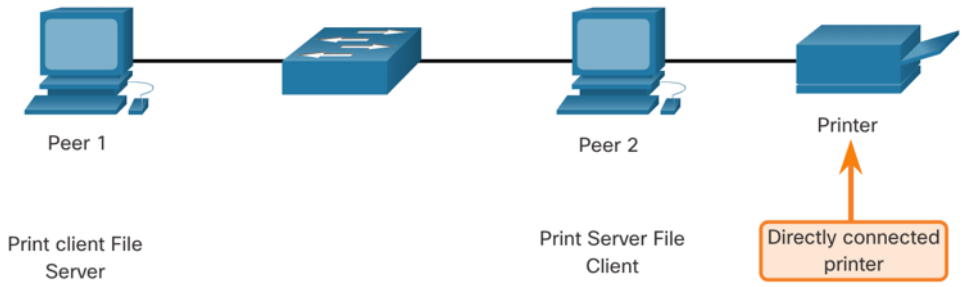
Client-Server Model

- Client and server processes are considered to be in the application layer.
- 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.
- Application layer protocols describe the format of the requests and responses between clients and servers.
- Examples:
  - A workstation initiates a DNS request when the user types www.cisco.com in the address bar of a web browser.
  - A client must login to a domain to gain access to resources and security credentials.
  - Email is an example of a Client-Server interaction.



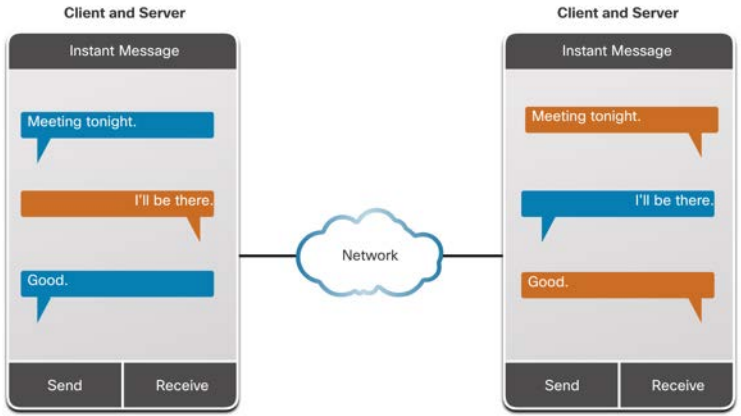
Peer-to-Peer Networks

- In a peer-to-peer (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 or centralized resources.
- 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 client and server are set on a per request basis.



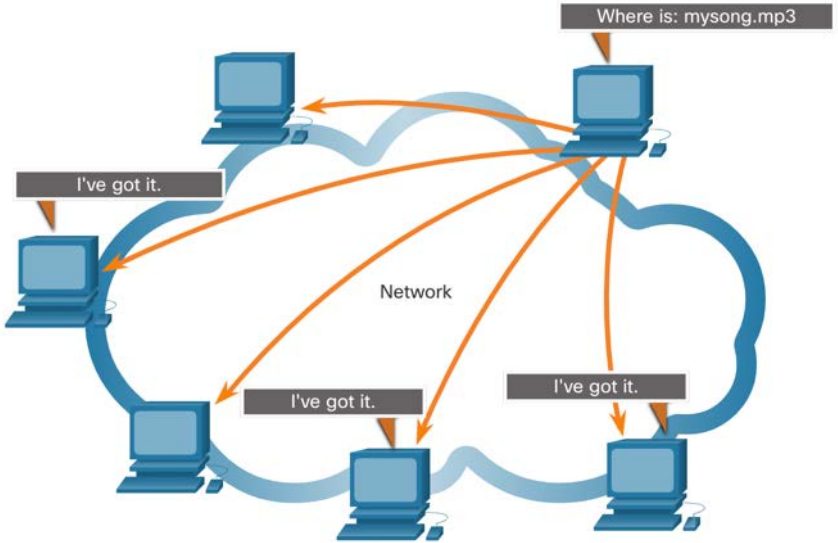
Peer-to-Peer Applications

- A P2P application allows a device to act as both a client and a server within the same communication.
- Some P2P applications use a hybrid system where each peer accesses an index server to get the location of a resource stored on another peer.
- Gnutella protocol – A decentralized file sharing protocol that defines the way distributed nodes communicate over a peer-to-peer (P2P) network.
  - Wireshare
  - Bearshare
  - Shareaza



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
  - Bitcoin
  - LionShare
  - Direct Connect
  - eDonkey
  - eMule
  - Freenet



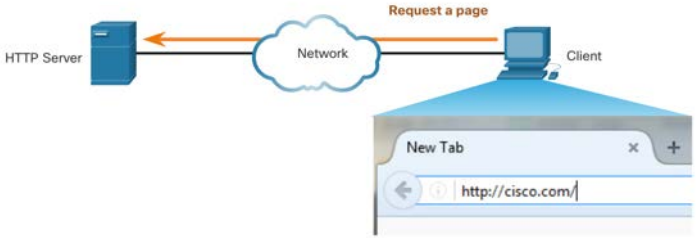
15.3 Web and Email Protocols

Hypertext Transfer Protocol and Hypertext Markup Language

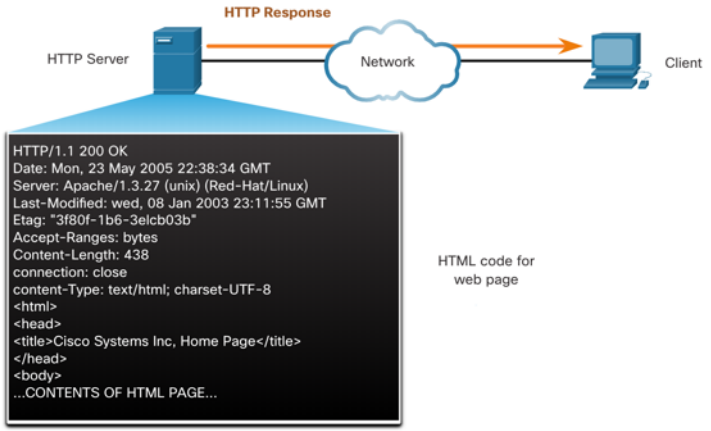
- When a web address or **Uniform Resource Locator** (URL) is typed into a web browser, the web browser establishes a connection to the web service. The web service is running on the server that is using the HTTP protocol.
- To better understand how the web browser and web server interact, examine how a web page is opened in a browser.
- Step 1 – The browser interprets the three parts of the URL:
  - http (the protocol or scheme)
  - www.cisco.com (the server name)
    - www is a folder on the server
  - index.html (the specific filename requested)

Hypertext Transfer Protocol and Hypertext Markup Language

- **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.

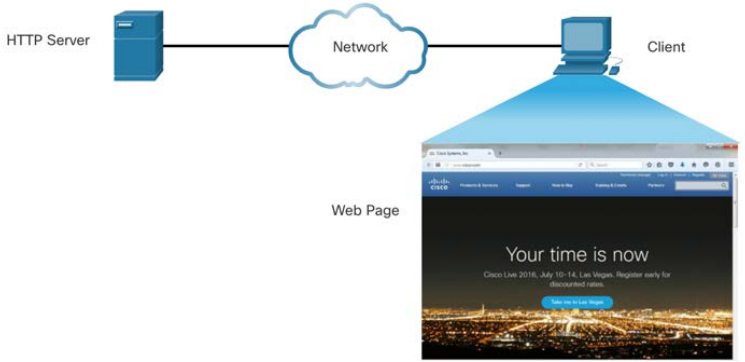


- **Step 3** – In response to the request, the server sends the HTML code for this web page to the browser.



Hypertext Transfer Protocol and Hypertext Markup Language

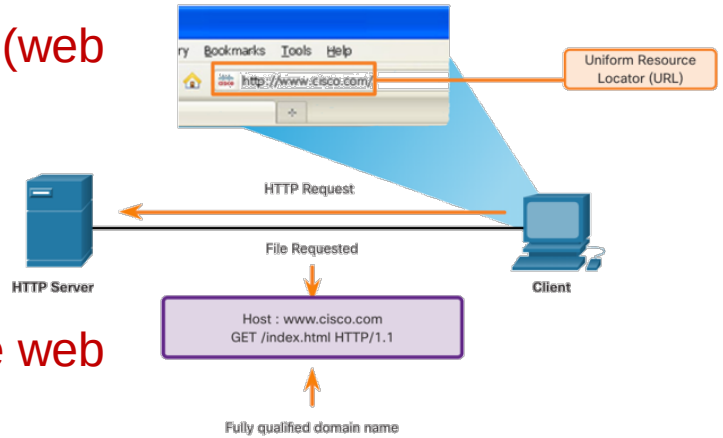
- **Step 4** – The browser deciphers the HTML code and formats the page for the browser window.



- **Hypertext Transfer Protocol** (HTTP) TCP 80, 8080 - Set of rules for exchanging text, graphic images, etc. on the World Wide Web.
  - HTTP is not secure. Messages can be intercepted.
- **Hypertext Transfer Protocol Secure** (HTTPS) TCP, UDP 443 – Uses encryption and authentication to secure communication.

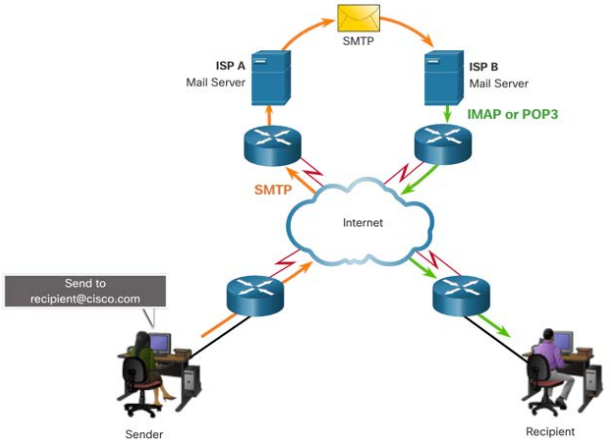
HTTP and HTTPS

- HTTP is a request/response protocol that specifies the message types used for that communication.
- The three common message types are:
  - **GET** - This is a client request for data. A client (web browser) sends the GET message to the web server 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.



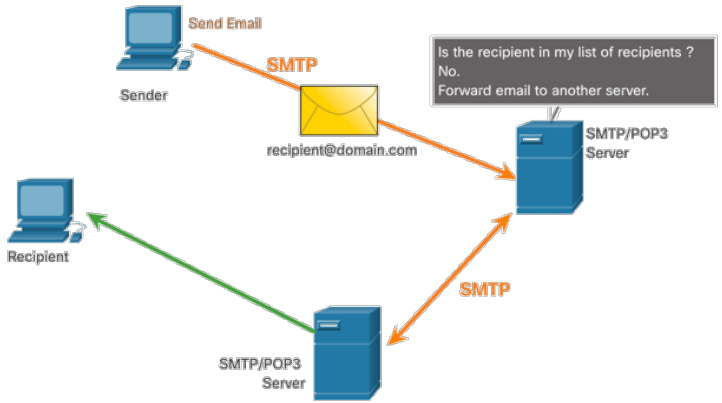
Email Protocols

- 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.
- 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.
- The email protocols used for operation are:
  - **Simple Mail Transfer Protocol** (SMTP) – used to send mail.
  - **Post Office Protocol** (POP3) & **Internet Message Access Protocol** (IMAP) – used for clients to receive mail.



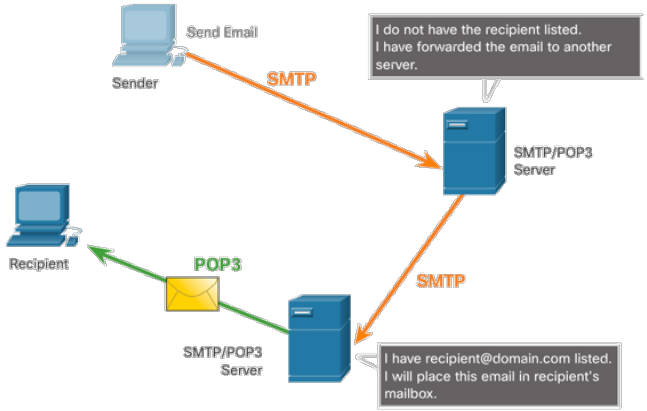
Simple Mail Transfer Protocol

- Used for the transfer of mail messages and attachments to and between servers.
- When a client sends 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 may be busy. If so, SMTP spools messages to be sent at a later time.
- SMTP message formats require a message header (recipient email address & sender email address) and a message body.
- DNS may be used to locate the mail server.



Post Office Protocol Version 3

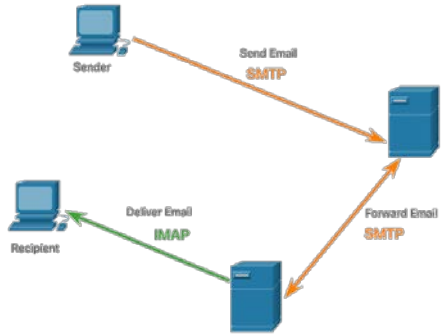
- POP3 is used by an application to retrieve mail from a mail server. When mail is downloaded from the server to the client using POP the messages are then deleted on the server.
  - The server starts the POP service by passively listening on TCP port 110 for client connection requests.
  - When a client wants to make use of the service, it sends a request to establish a TCP connection with the server.
  - 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.



- Since POP does not store messages, it is not recommended for small businesses that need a centralized backup solution.

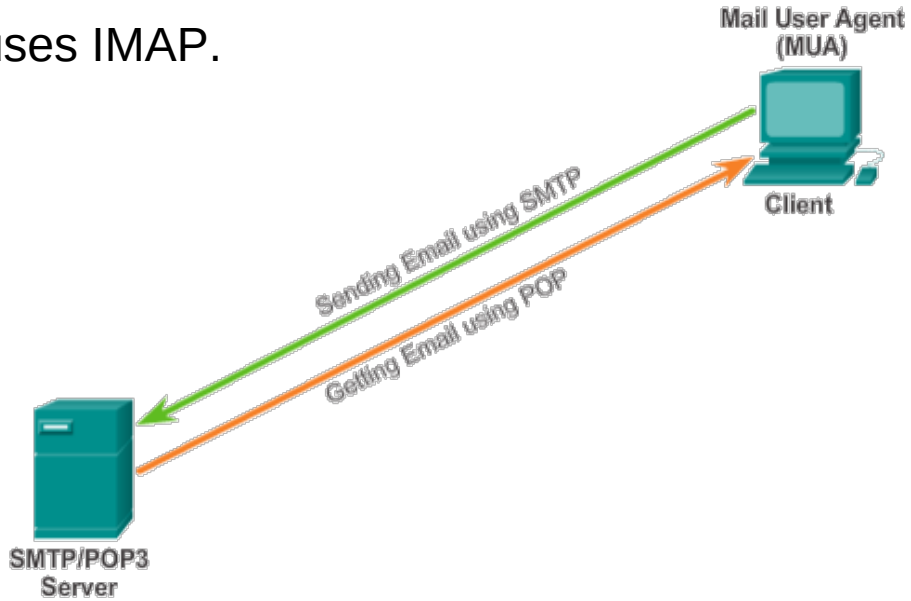
Internet Message Access Protocol

- IMAP is another protocol that describes a method to retrieve email messages.
- Unlike POP, when a user connects to an IMAP server, copies of the messages are downloaded to the client application. The original messages are kept on the server until manually deleted.
- Allows for easy, centralized storage and backup of emails.
- Allows for messages to be displayed to the user rather than downloaded.
- Original messages are kept on the server until manually deleted.
- Users view copies of the messages in their email client software.
- Uses port TCP 143.
- Support folder hierarchy to organize and store mail.
- When a user decides to delete a message, the server synchronizes that action and deletes the message from the server.



SMTP, POP, and IMAP

- Typically use an application called a **Mail User Agent** (email client).
- Email client provides the functionality of both protocols within one application.
- Clients send e-mails to a server using SMTP and receive e-mails using POP3 or IMAP.
- Web mail typically uses IMAP.



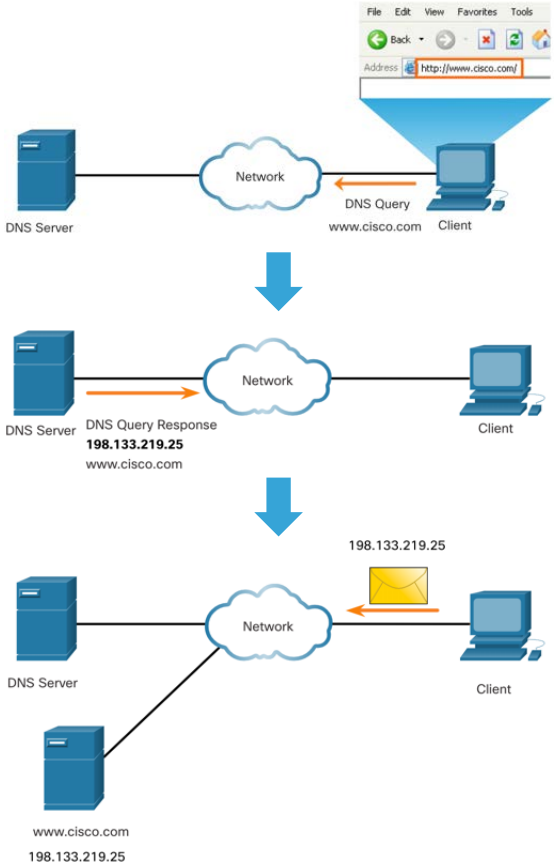
TCP/IP Application Layer Protocols

- **Telnet** - a terminal emulation protocol used to provide remote access to servers and networking devices.
- **Bootstrap Protocol** (BOOTP) - a precursor to the DHCP protocol, a network protocol used to obtain IP address information during bootup.

15.4 IP Addressing Services

Domain Name Service

- Domain names were created to convert the numeric IP addresses into a simple, recognizable name.
- **Fully-qualified domain names** (FQDNs), such as http://www.cisco.com, are much easier for people to remember than 198.133.219.25.
- 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 allows for the dynamic translation of a domain name into the associated IP address
- Uses port TCP and UDP 53.



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 that maps a domain name to a list of mail exchange servers.
- 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.

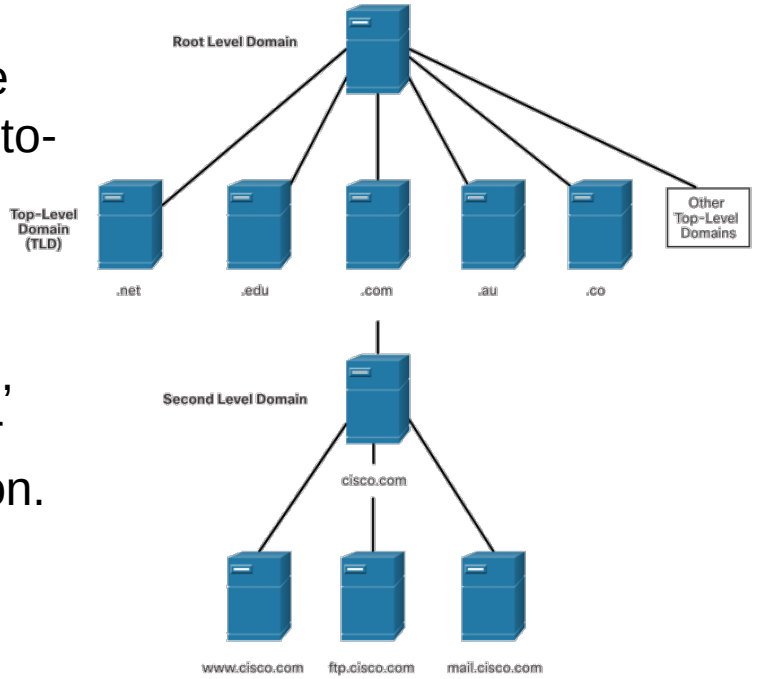
DNS Message Format

- 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

DNS Hierarchy

- DNS uses a hierarchical system to create a database to provide name resolution.
- 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.
- Examples of top-level domains:
  - .com - a business or industry
  - .org - a non-profit organization
  - .au - Australia



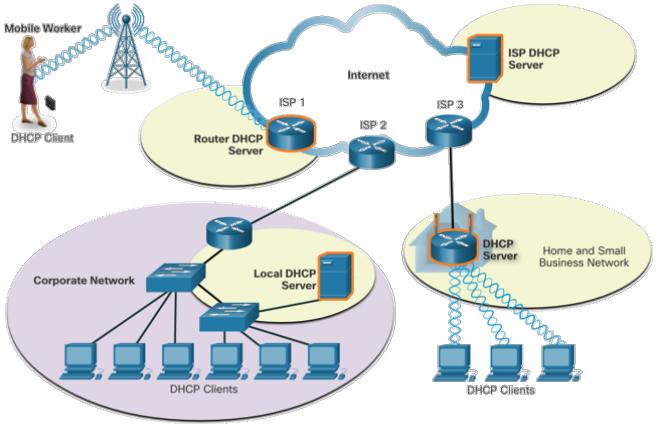
The nslookup Command

- **nslookup** is a computer operating system utility that allows a user to manually query the DNS servers configured on the device 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.
- 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.

```
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
>
```

Dynamic Host Configuration Protocol

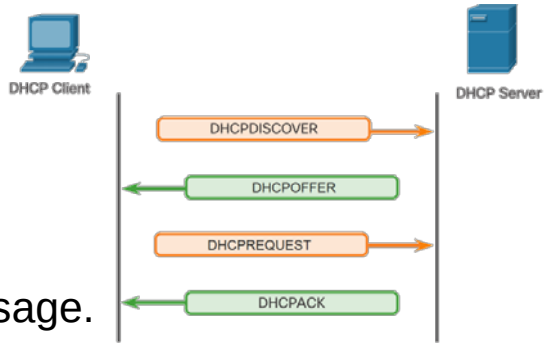
- The Dynamic Host Configuration Protocol (DHCP) for IPv4 service automates the assignment of IPv4 addresses, subnet masks, gateways, and other IPv4 networking parameters.
- DHCP is considered dynamic addressing compared to static addressing. Static addressing is manually entering IP address information.



- 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.
- 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. However, DHCPv6 does not provide a default gateway address. This can only be obtained dynamically from the Router Advertisement message of the router.

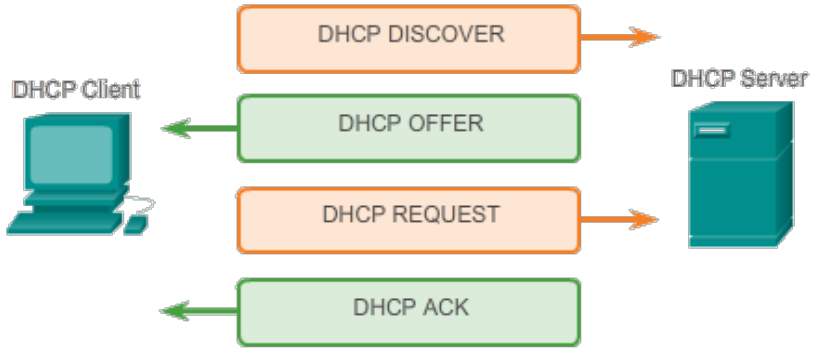
DHCP Operation

- The DHCP Process:
  1. 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.
  2. A DHCP server replies with a DHCP offer (**DHCPOFFER**) message, which offers a lease to the client. (If a client receives more than one offer due to multiple DHCP servers on the network, it must choose one.)
  3. The client sends a DHCP request (**DHCPREQUEST**) message that identifies the explicit server and lease offer that the client is accepting.
  4. The server then returns a DHCP acknowledgment (**DHCPACK**) message that acknowledges to the client that the lease has been finalized.
  5. If the offer is no longer valid, then the selected server responds with a DHCP negative acknowledgment (**DHCPNAK**) message and the process must begin with a new DHCPDISCOVER message.



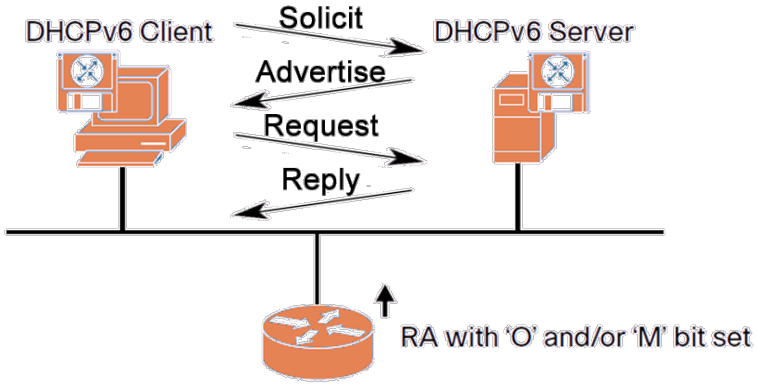
DHCP Operation

- A PC uses DHCPDISCOVER and DHCPREQUEST to broadcast messages when communicating with a DHCP server.
- A DHCP Discover message:
  - The destination IP address is 255.255.255.255
  - The source MAC address is FF-FF-FF-FF-FF-FF
  - The message comes from a server offering an IP address
  - The message comes from a client seeking an IP address
  - All hosts receive the message, but only a DHCP server replies



DHCPv6

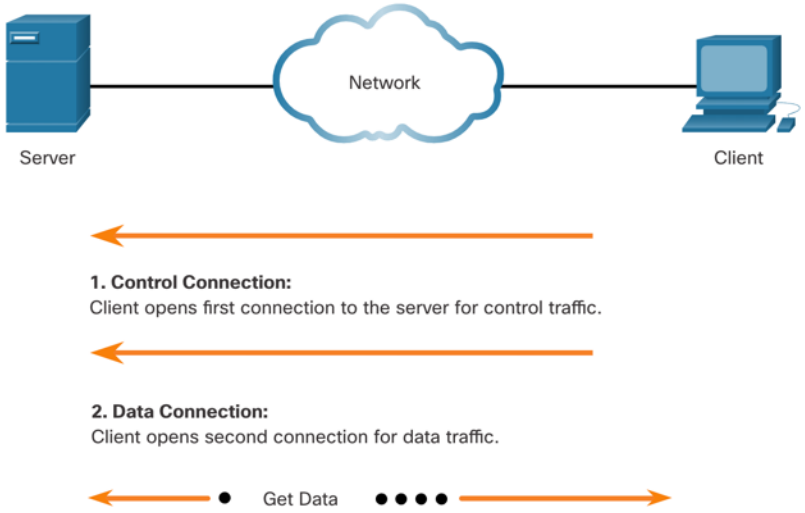
- DHCPv6 has a set of messages that is similar to those for DHCPv4.
- DHCPv6 uses UDP port number 546 for clients and port number 547 for servers.
- The DHCPv6 messages are:
  - SOLICIT
  - ADVERTISE
  - INFORMATION REQUEST
  - REPLY
- Router Advertisement bit:
  - M - Managed Address Configuration Flag – When set, it indicates that addresses are available via Stateful DHCPv6.
  - O - Other Configuration Flag – When set, it indicates that other configuration information is available via Stateless DHCPv6.



15.5 File Sharing Services

File Transfer Protocol

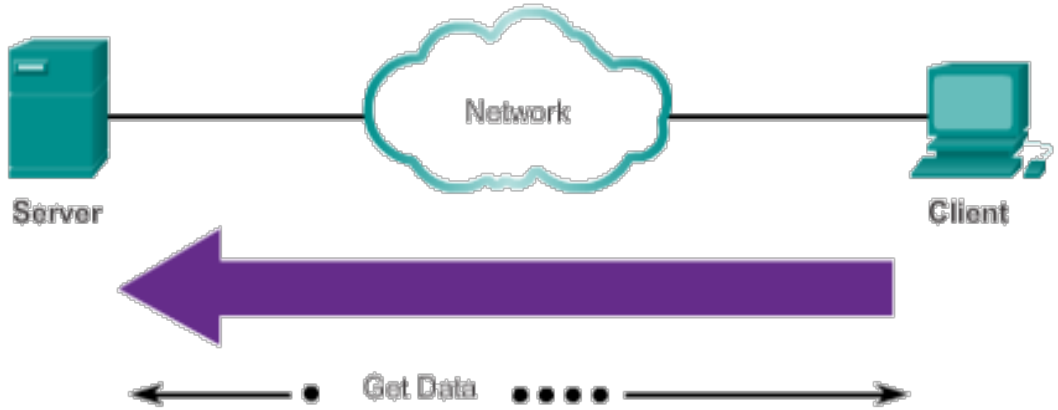
- FTP was developed to allow for data transfers between a client and a server.
- An **FTP client** is an application which runs on a computer that is being used to push and pull data from an **FTP server** running a **FTP daemon**.



- **Step 1 -** The client establishes the first connection to the server for control traffic using TCP port **21**. The traffic consists of client commands and server replies.
- **Step 2 -** 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.
- **Step 3 -** 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.

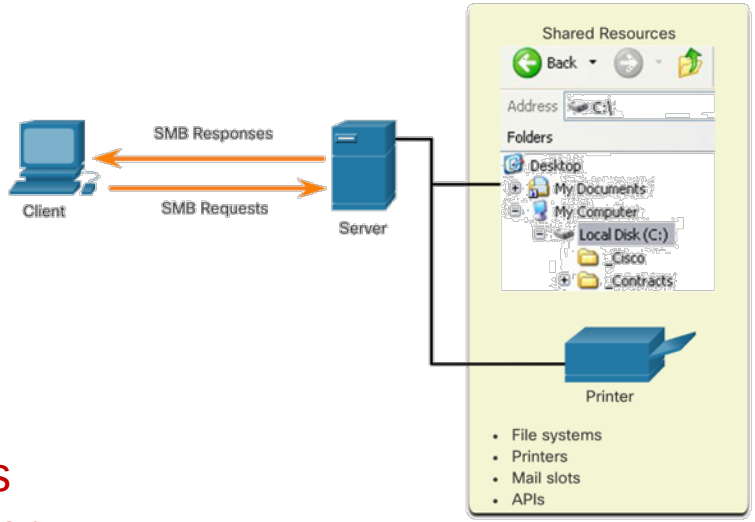
Trivial File Transfer Protocol (TFTP)

- Used for connectionless active file transfer.
- Usually anonymous.
- Allow data transfers between a client and a server.
- Uses port UDP 69.



Server Message Block

- The Server Message Block (SMB) is a client/server, request-response file sharing protocol. Servers can make their own resources available to clients on the network.
- 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 uses the FTP protocol for communication.
- 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.



15.6 Module Practice and Quiz

What did I learn in this module?

- 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, compressing data, and encrypting data for transmission and decrypting data upon receipt. The session layer creates and maintains dialogs between source and destination applications.
- 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.
- In a P2P network, two or more computers are connected via a network and can share resources without having a dedicated server.
- The three common HTTP message types are GET, POST, and PUT.

What did I learn in this module?

- Email supports three separate protocols for operation: SMTP, POP, and IMAP.
- DNS protocol matches resource names with the required numeric network address.
- DHCP for IPv4 service automates the assignment of IPv4 addresses, subnet masks, gateways, and other IPv4 networking parameters. The DHCPv6 messages are SOLICIT, ADVERTISE, INFORMATION REQUEST, and REPLY.
- An FTP client is an application which runs on a computer that is being used to push and pull data from an FTP server.
- 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.

New Terms and Commands

- Application Layer
- Presentation Layer
- Session Layer
- Client-server model
- Peer-to-peer
- Uniform Resource Locator (URL)
- Uniform Resource Identifiers (URI)
- HTTP/HTTPS
- GET
- POST
- PUT
- SMTP
- POP
- IMAP
- Domain Name Service (DNS)
- Fully-Qualified Domain Names (FQDNs)
- nslookup
- Dynamic Host Configuration Protocol (DHCP)
- DHCPDISCOVER
- DHCPOFFER
- DHCPREQUEST
- DHCPACK
- File Transfer Protocol (FTP)
- Server Message Block (SMB)


CISCO


Elk Technologies
https://elktech.org
Scott Stephenson