TNE20003 - Internet and Cybersecurity for Engineering Applications

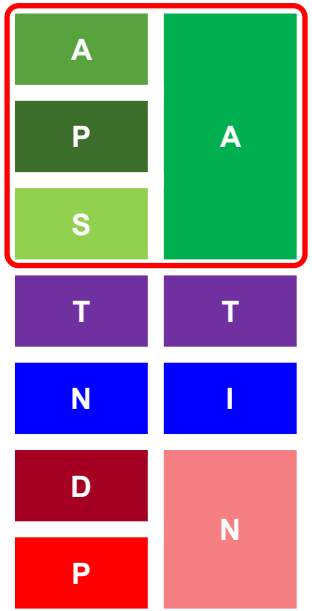
Domain Name Server (DNS)

&

Hypertext Transfer Protocol (HTTP)

Module Objectives

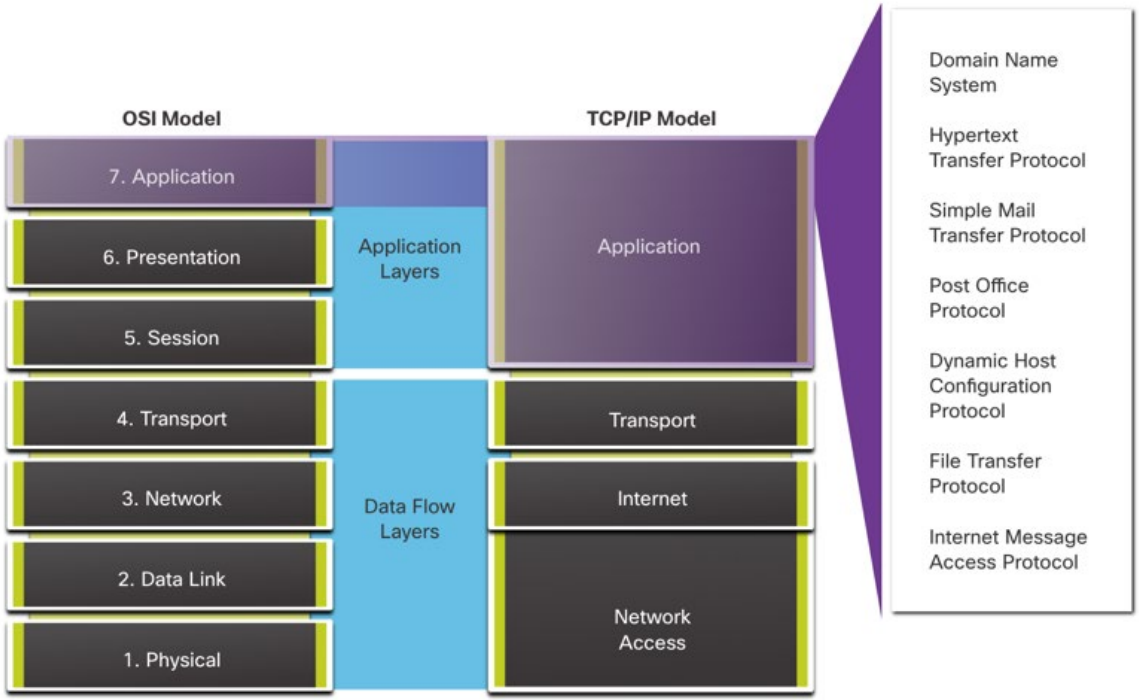
Module Title: Application Layer Services
Module Objective: Explain the function of common application layer services.



Topic Title	Topic Objective
Network Application Services	Describe common network applications.
Domain Name System	Describe DNS.
Web Clients and Servers	Describe HTTP and HTML.
FTP Clients and Servers	Describe FTP.
Virtual Terminals	Describe Telnet and SSH.
Email and Messaging	Describe email protocols.

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.
- Some of the most widely known application layer protocols include HTTP, FTP, TFTP, IMAP and DNS.



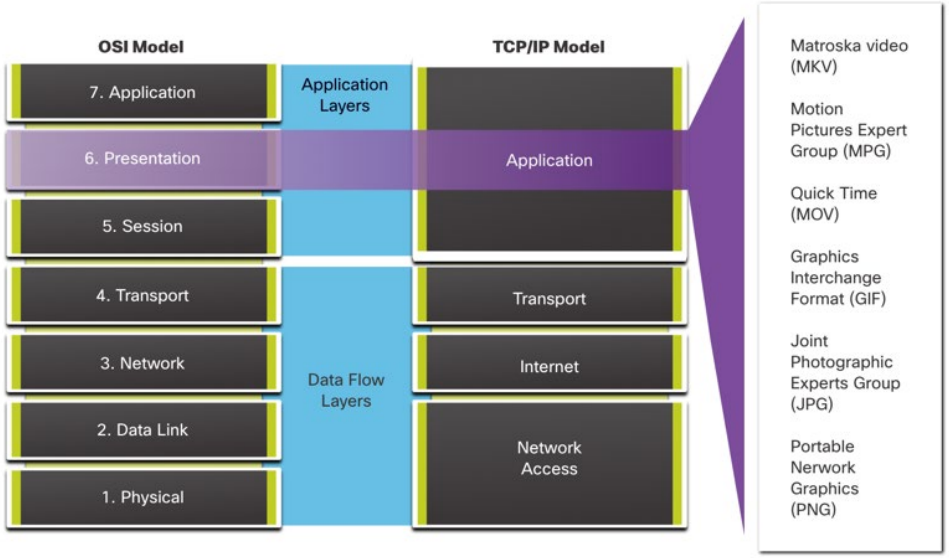
Presentation and Session Layer

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

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.



TCP/IP Application Layer Protocols - *Revisited*...

Well Known Application Layer Protocols and ports.

- Domain Name System (DNS) - TCP/UDP Port 53
- Hypertext Transfer Protocol (HTTP) - TCP Port 80
- Simple Mail Transfer Protocol (SMTP) - TCP Port 25
- Post Office Protocol (POP) - UDP Port 110
- Telnet - TCP Port 23
- Dynamic Host Configuration Protocol - UDP Ports 67 and 68
- File Transfer Protocol (FTP) - TCP Ports 20 & 21
- Secure Shell (SSH) – TCP Port 22

SWINBURNE UNIVERSITY OF TECHNOLOGY

Domain Name System

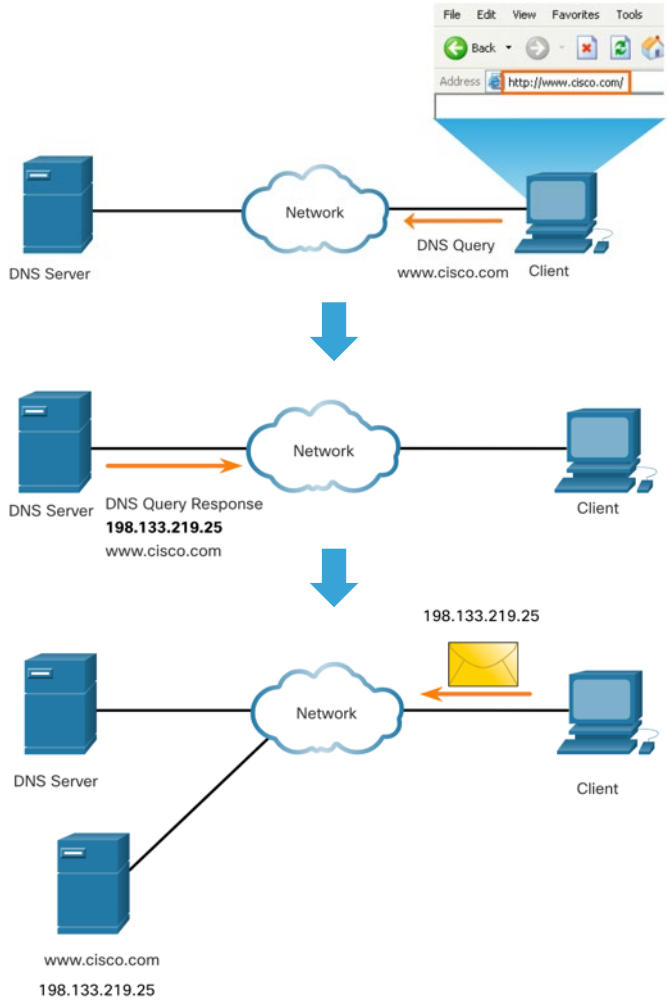
Domain Name Service

Domain names were created to convert the numeric IP addresses into a simple, recognizable name.

Fully-qualified domain names (FQDNs), such as 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 is like a giant lookup table with IP Addresses and FQDNs



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:

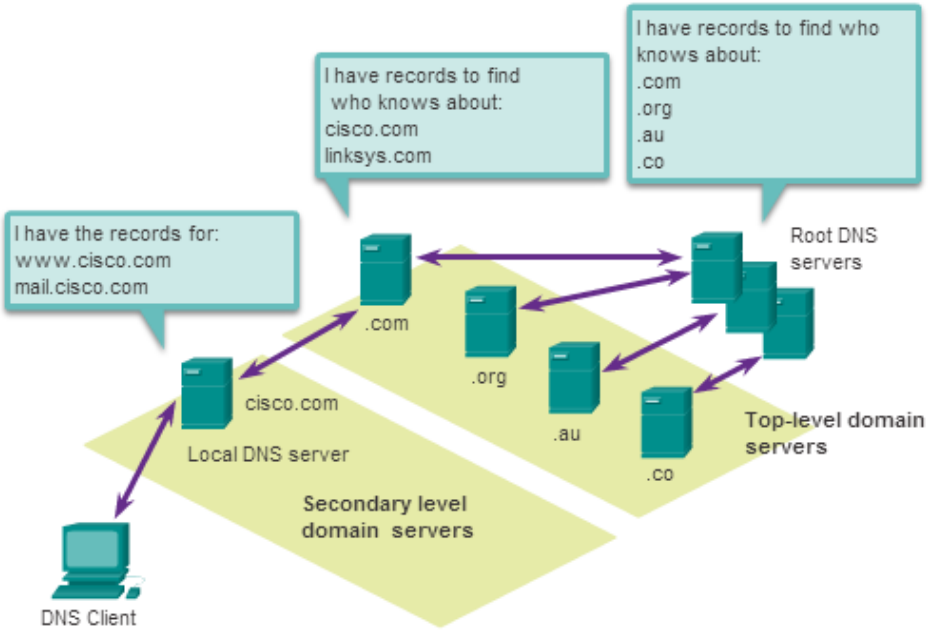
- **A** - An end device IPv4 address
- **NS** - An authoritative name server
- **AAAA** - An end device IPv6 address (pronounced quad-A)
- **MX** - A mail exchange record

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 - ‘cache’.

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

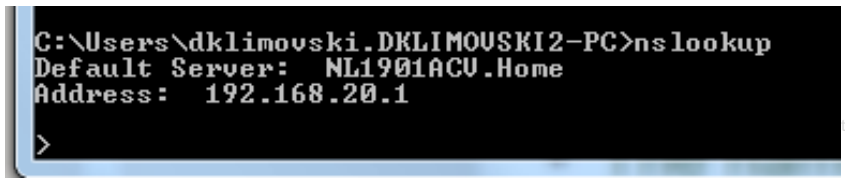


A hierarchy of DNS servers contains the resource records that match names with addresses.

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.

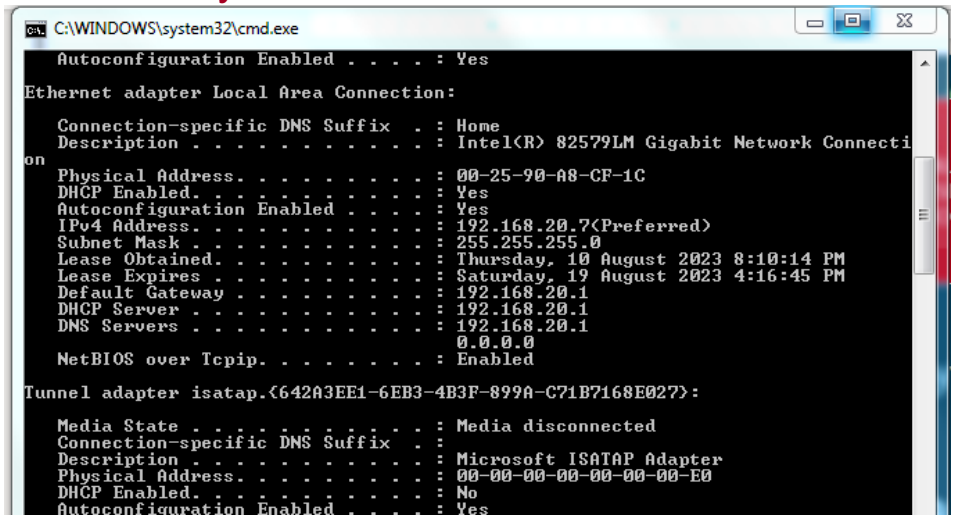
```
C:\Users> nslookup
Default Server:  dns-sj.cisco.com
Address:  171.70.168.183
> www.cisco.com
Server:  dns-sj.cisco.com
Address:  171.70.168.183
Name:    origin-www.cisco.com
Addresses:  2001:420:1101:1::a
          173.37.145.84
Aliases:  www.cisco.com
> cisco.netacad.net
Server:  dns-sj.cisco.com
Address:  171.70.168.183
Name:    cisco.netacad.net
Address:  72.163.6.223
>
```



Example of my DNS server

- Note the DNS server address is in the private address space.

- It's in my LAN behind the ISP connection



Here is the equivalent data looking towards my ISP

Line Rate - Upstream (Kbps):	0
Line Rate - Downstream (Kbps):	0
LAN IPv4 Address:	192.168.20.1
Service connection type:	mobile
Default Gateway:	110.115.34.235
Primary DNS Server:	11.143.174.147

Web Clients and Servers

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

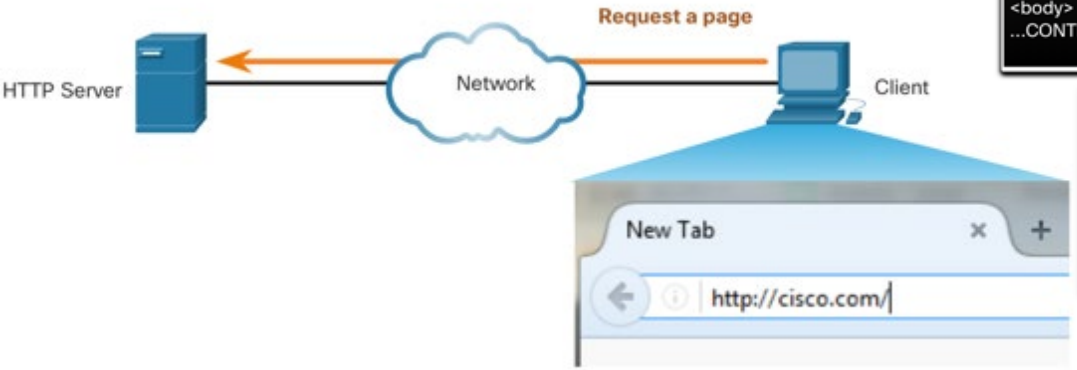
The web browser interprets the three parts of the URL:

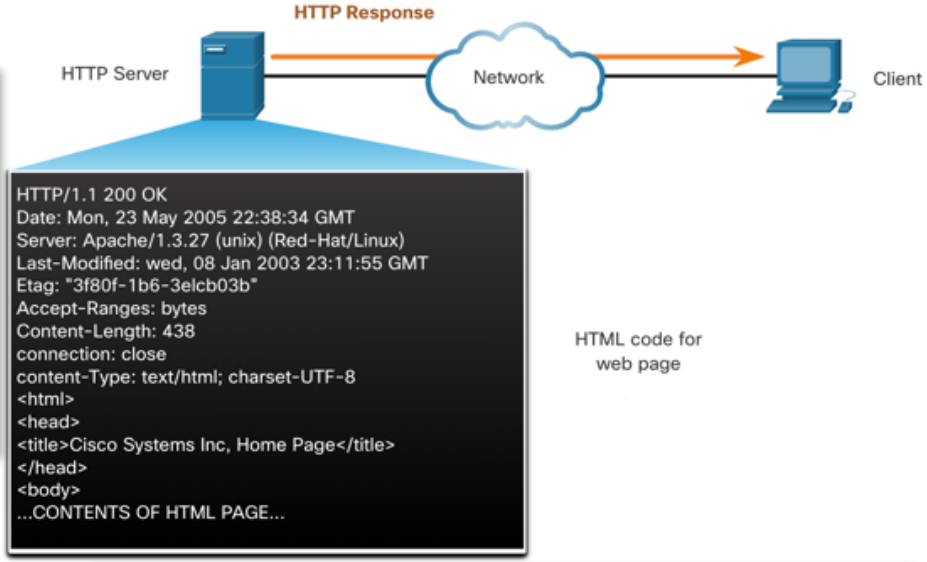
- http *(the protocol or scheme)*
- www.cisco.com *(the server name)*
- index.html *(the specific filename requested)*

Hypertext Transfer Protocol and Hypertext Markup Language (Cont.)

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 by sending a GET request to the server and asks for the index.html file.

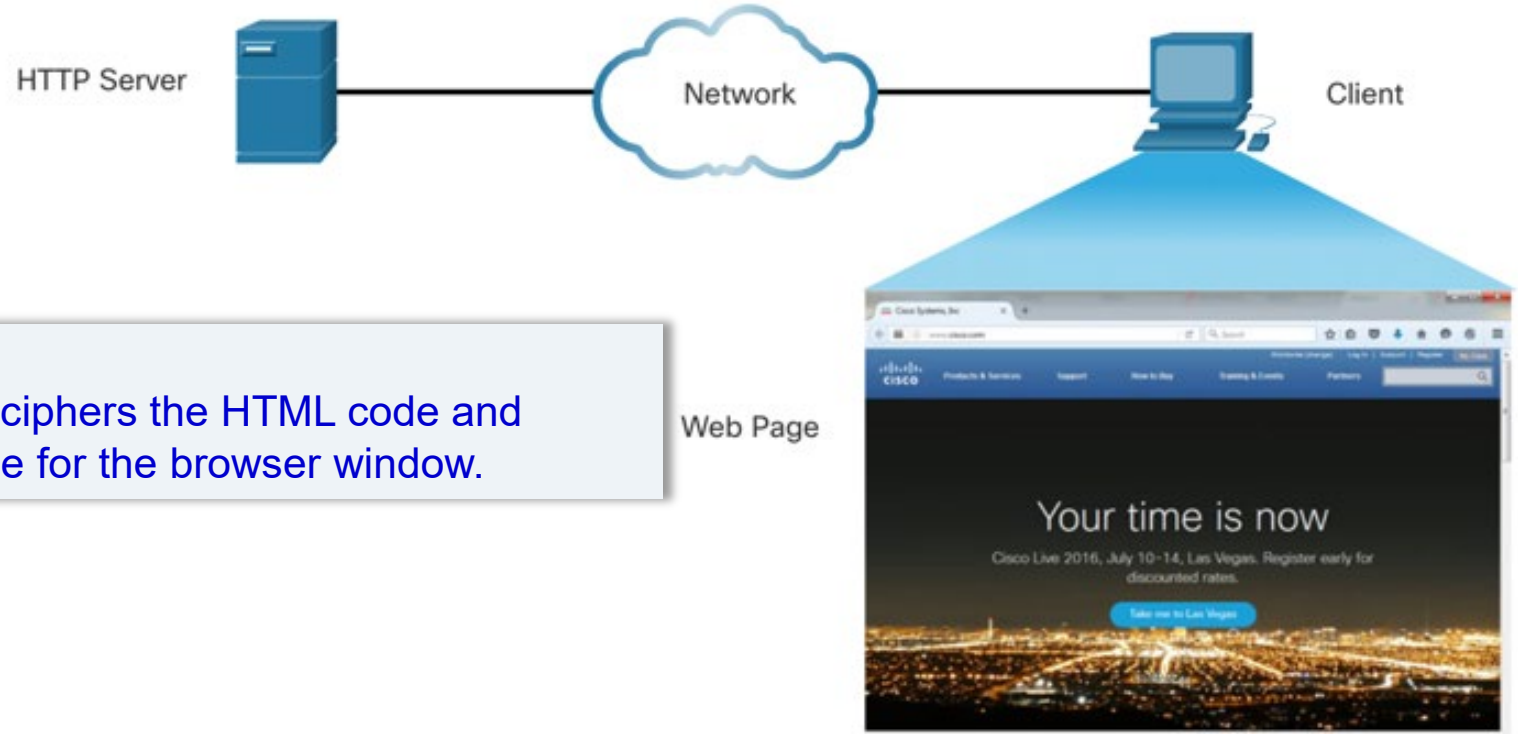




Step 3

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 (Cont.)



Step 4

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

For fun: *open a terminal and type telnet www.facebook.com 80 , spam the keyboard then press ENTER a few times and look at the result…*

HTTP and HTTPS

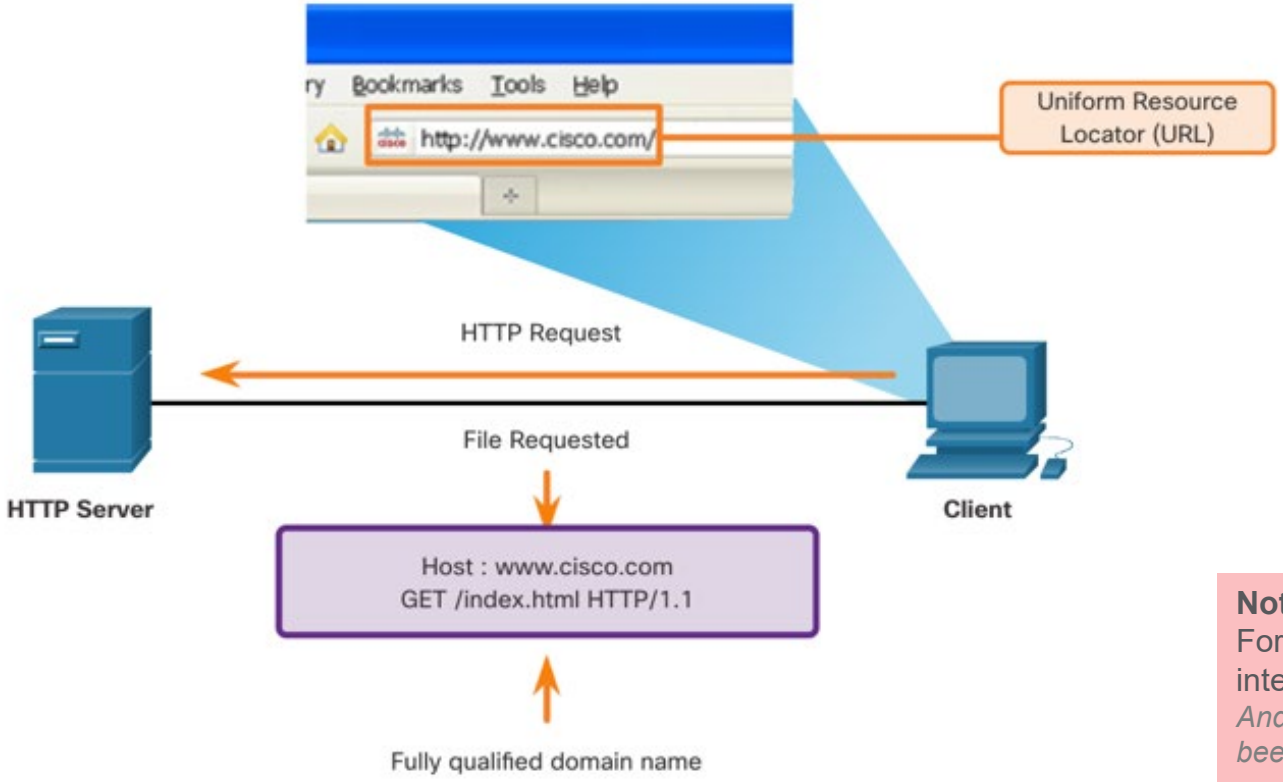
HTTP is a request / response protocol that specifies the message types used for communication between client and server.

The three common message types are GET, POST, and PUT:

- **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.
- HEAD – This asks the server for the size and availability of a resource.
- DELETE - Asks the server to delete a resource.

Note: HTTP is not a secure protocol. For secure web browsing across the internet, HTTPS should be used. *And 99% of all global websites have been HTTPS for a while now…*

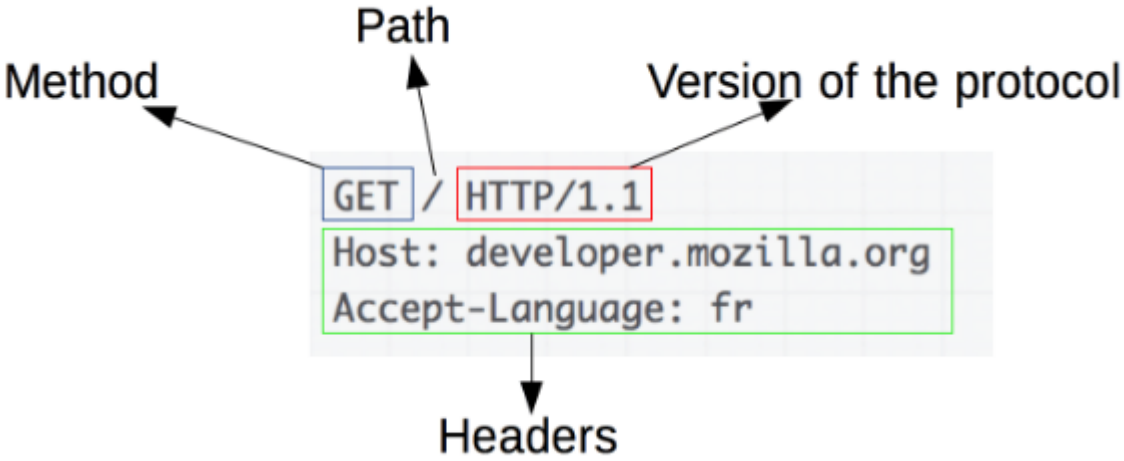
HTTP and HTTPS



Note: HTTP is not a secure protocol. For secure web browsing across the internet, HTTPS should be used. *And 99% of all global websites have been HTTPS for a while now…*

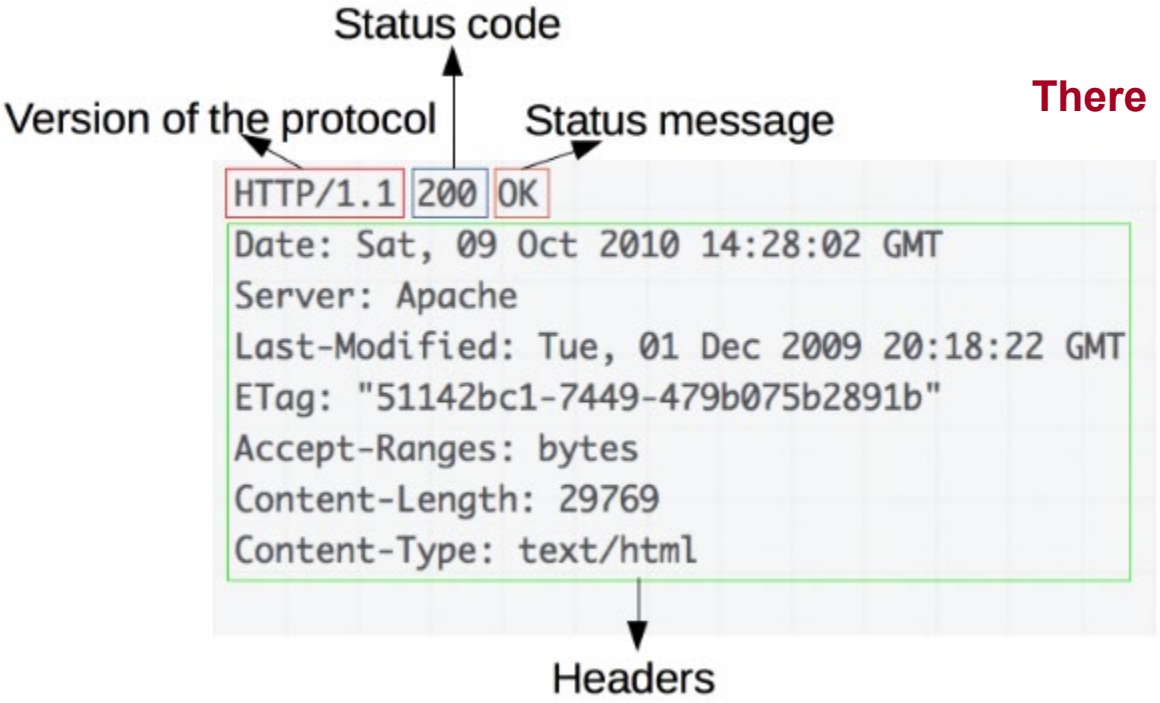
HTTP and HTTPS

An example of a HTTP request



HTTP and HTTPS

An example of a HTTP response



There are 5 categories of status codes

1. Informational responses (`100` – `199`)
2. Successful responses (`200` – `299`)
3. Redirection messages (`300` – `399`)
4. Client error responses (`400` – `499`)
5. Server error responses (`500` – `599`)

HTTP and HTTPS

Some examples of 200 OK status code and their meaning

`200 OK`

The request succeeded. The result meaning of "success" depends on the HTTP method:

- `GET`: The resource has been fetched and transmitted in the message body.
- `HEAD`: The representation headers are included in the response without any message body.
- `PUT` or `POST`: The resource describing the result of the action is transmitted in the message body.

HTTP and HTTPS

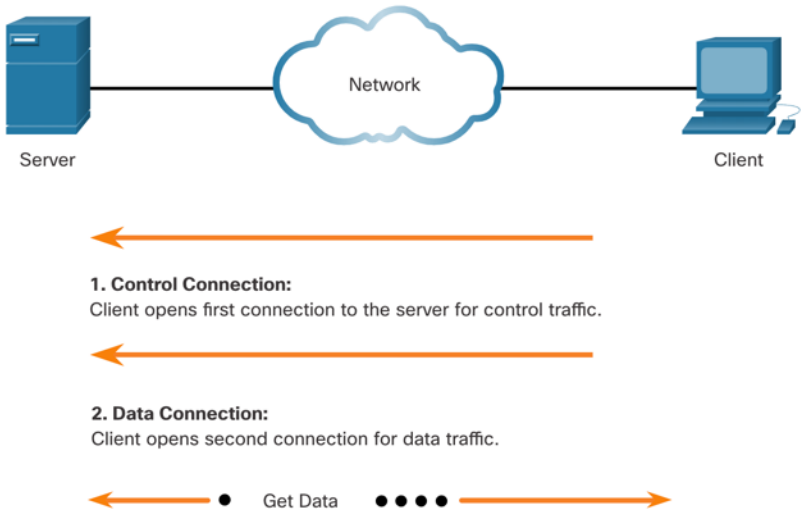
An example of a 400 code

Here I tried to log in to my router and failed authentication and received this message

You can see the code 401 which you have seen in your expreiences

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.



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.

Virtual Terminals

Virtual Terminals

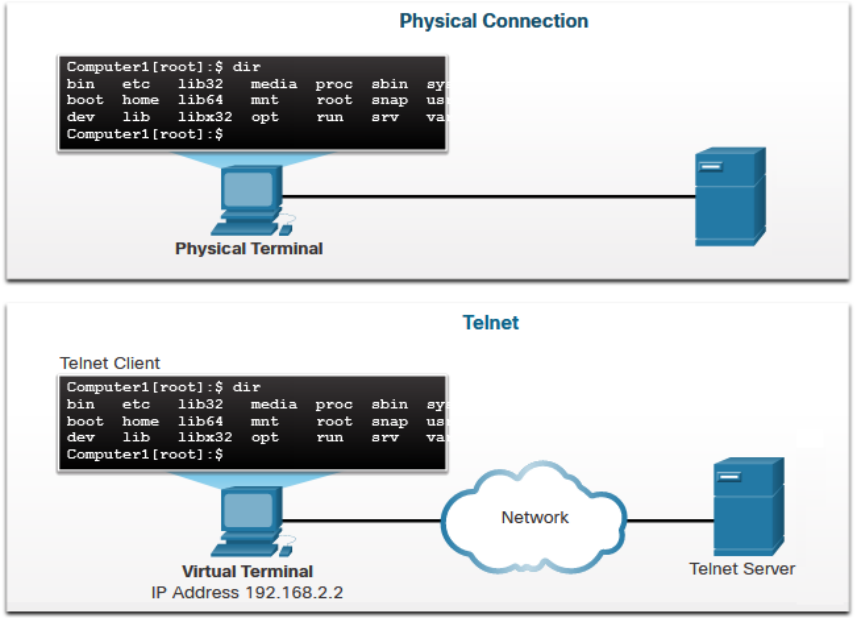
Telnet provides a standard method of emulating text-based terminal devices over the data network.

Telnet servers listen for client requests on TCP port 23.

A connection using Telnet is called a virtual terminal (vty) session, or connection:

- Rather than using a physical device to connect to the server, Telnet uses software to create a virtual device that provides the same features of a terminal session with access to the server's command line interface (CLI).

The client can execute commands as if it were locally (physically) connected to the server.



Virtual Terminals

After a Telnet connection is established, users can perform any authorized function on the server, just as if they were using a command line session on the server itself.

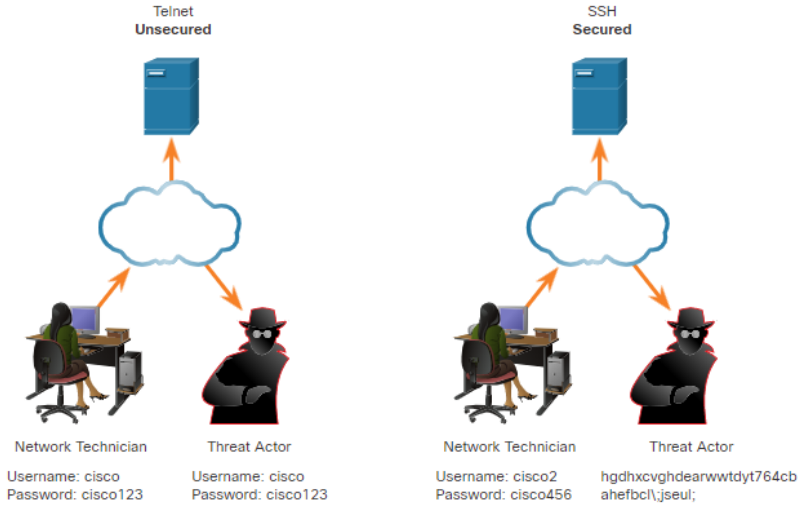
Although the Telnet protocol can require a user to login, it does **NOT** support transporting encrypted data.

- All data exchanged during Telnet sessions is transported as plaintext across the network.

The Secure Shell (SSH) protocol offers an alternate and secure method for server access.

SSH provides the structure for secure remote login and other secure network services.

- SSH provides stronger authentication than Telnet and supports transporting session data using encryption.
- SSH servers listen for client requests on TCP port 22.



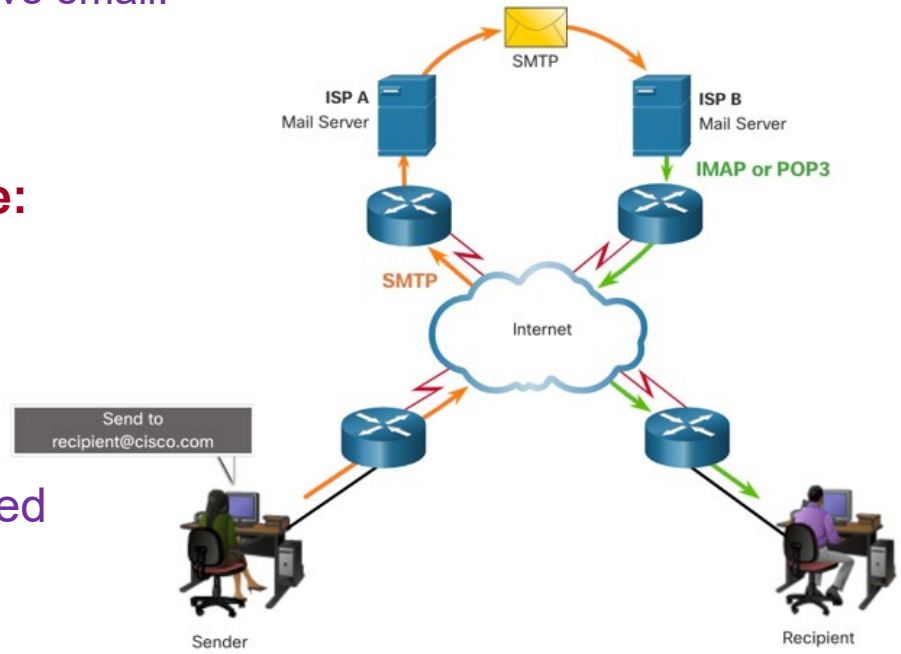
Email and Messaging

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.

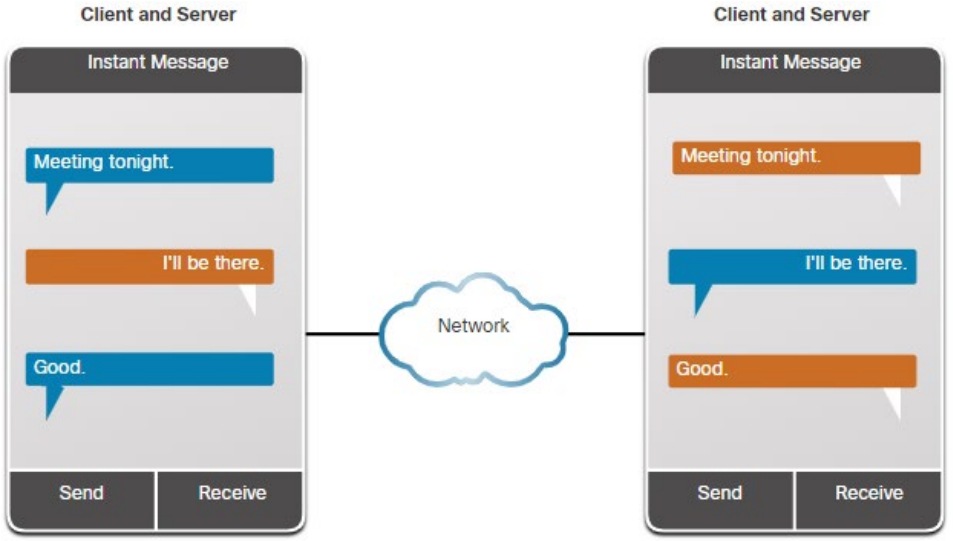
The email protocols used for operation are:

- Simple Mail Transfer Protocol (SMTP) - used to send mail.
- Post Office Protocol (POP) and Internet Message Access Protocol (IMAP) are used for clients to receive mail.



Email and Messaging

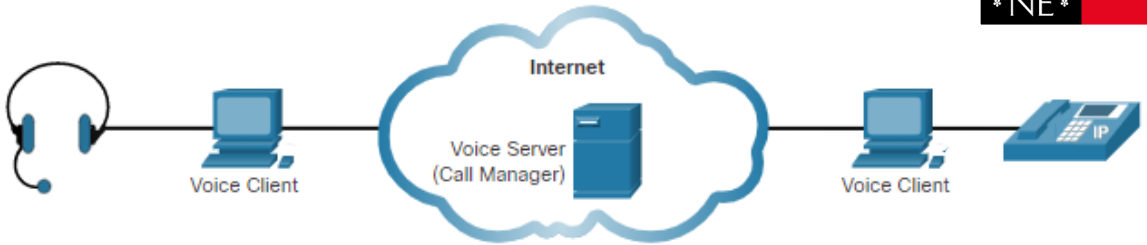
- Enables users to communicate or chat over the internet in real-time
- May also be called instant messages, direct messages, private messages, and chat messages.
- Text messaging software is built into many online applications, smart phone apps, and social media sites.



Text messaging services on a computer are usually accessed through a web-based client that is integrated into a social media or information sharing site.

There are also a number of standalone text message clients such as Cisco Webex Teams, Microsoft Teams, WhatsApp, Facebook Messenger, and many others that support the transfer of documents, video, music, and audio files.

Email and Messaging



An internet telephony client uses peer-to-peer technology similar to that used by instant messaging.

- Protocols and destination ports used by internet telephony applications can vary.

IP telephony makes use of Voice over IP (VoIP) technology, which converts analog voice signals into digital data.

- Voice data is encapsulated into IP packets which carry the phone call through the network.

When the IP phone software has been installed, the user selects a unique name.

- A unique name allows calls to be received from other users.
- Calls are made to other users of the same service by selecting the username from a list.

A call to a regular telephone (landline or cell phone) requires using a gateway to access the Public Switched Telephone Network (PSTN) and depending on the service, there may be charges associated with this type of call.

Application Layer Services Summary

The most common internet services such as internet searches, social media sites, video and audio streaming, on-line shopping sites, email and messaging rely on protocols from the TCP/IP protocol suite to reliably communicate the information between the clients and the servers.

- DNS, SSH, SMTP, POP, IMAP, DHCP, HTTP, & FTP

- Domain Name System (DNS) provides a way for hosts to use this name to request the IP address of a specific server.
  - DNS names are registered and organized on the internet within specific high level groups, or domains. Some of the most common high level domains on the internet are .com, .edu, and .net.
  - When a client has the name of server, such as a web server, but needs to find the IP address, it sends a request to the DNS server on port 53.

- When a web client receives the IP address of a web server, the client browser uses that IP address and port 80 to request web services.
  - This request is sent to the server using the Hypertext Transfer Protocol (HTTP).

Application Layer Services Summary

Requests for secure HTTP are sent to port 443 and they use **https** in the site address.

File Transfer Protocol (FTP) provides an easy method to transfer files from one computer to another.
- Control connection requests are sent to the server using destination TCP port 21.
- The server uses TCP port 20 to transfer the data files.

Telnet provides a standard method of emulating text-based terminal devices over the data network.
- Both the protocol itself and the client software that implements the protocol are commonly referred to as Telnet.
- Telnet servers listen for client requests on TCP port 23.
- Secure Shell (SSH) protocol offers an alternate and secure method for server access

Email servers run server software that enables them to interact with clients and with other email servers over the network.
- Various application protocols used in processing email include SMTP, POP3, and IMAP4.