Chapter 3: Network Protocols and Services

Information Security

Dr. Ayman Aljarbouh

3.6 Network Services

Module Objectives

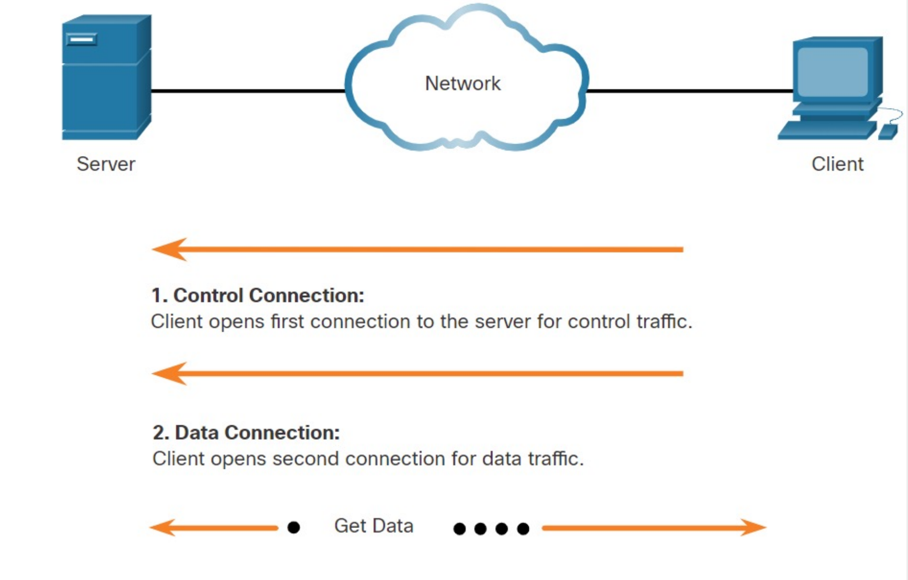
Module Title: Network Services

Module Objective: Explain how network services enable network functionality

Topic Title	Topic Objective
File Transfer and Sharing Services	Explain how file transfer services enable network functionality.
Email	Explain how email services enable network functionality.
HTTP	Explain how HTTP services enable network functionality.

FTP and TFTP

- FTP allows data transfers between a client and a server.
- An FTP client runs on a computer and is used to push and pull data from an FTP server.
- FTP connections between the client and server:
  - **Control Connection**: The client opens the first connection to the server for control traffic.
  - **Data Connection**: The client opens the second connection to the server for data traffic.
- Trivial File Transfer Protocol (TFTP) is a simplified file transfer protocol that uses well-known UDP port number 69.



1. Control Connection:
Client opens first connection to the server for control traffic.

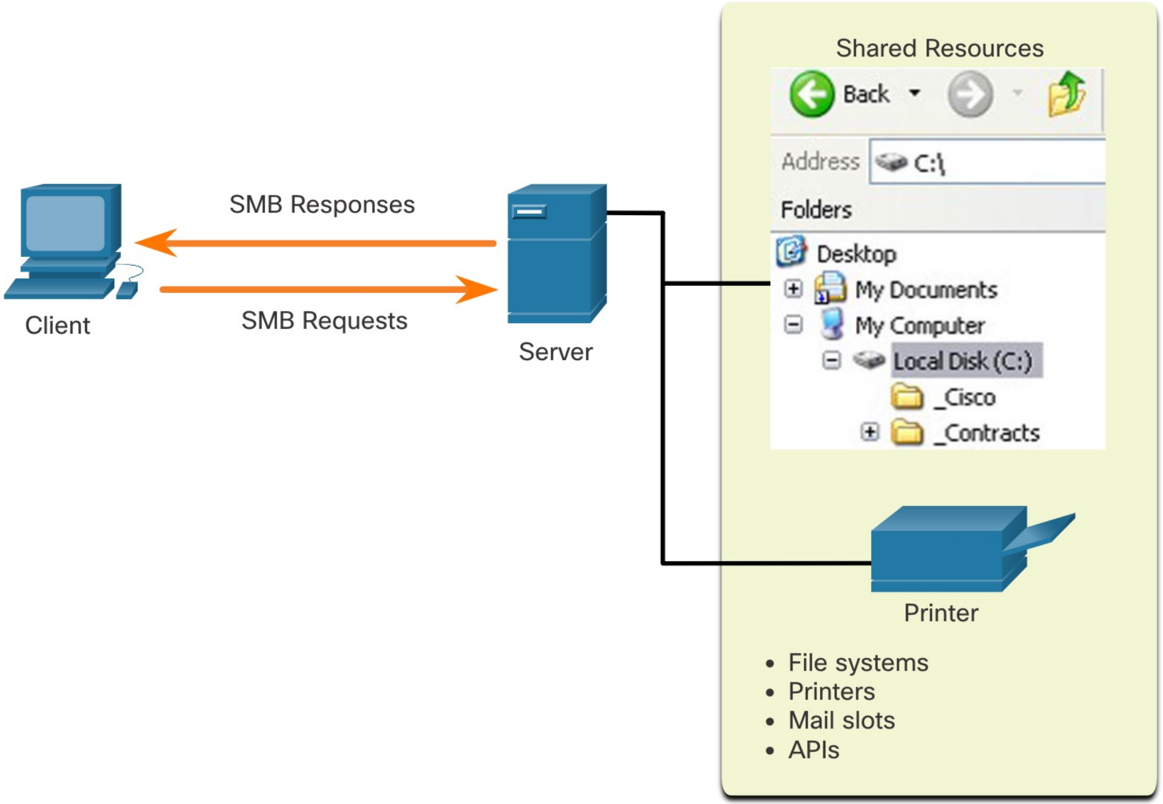
2. Data Connection:
Client opens second connection for data traffic.

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

File Transfer and Sharing Services

SMB

- The Server Message Block (SMB) is a client/server file sharing protocol that describes the structure of shared network resources.
- SMB is a client/server, request-response protocol.
- Servers can make their own resources available to clients on the network.

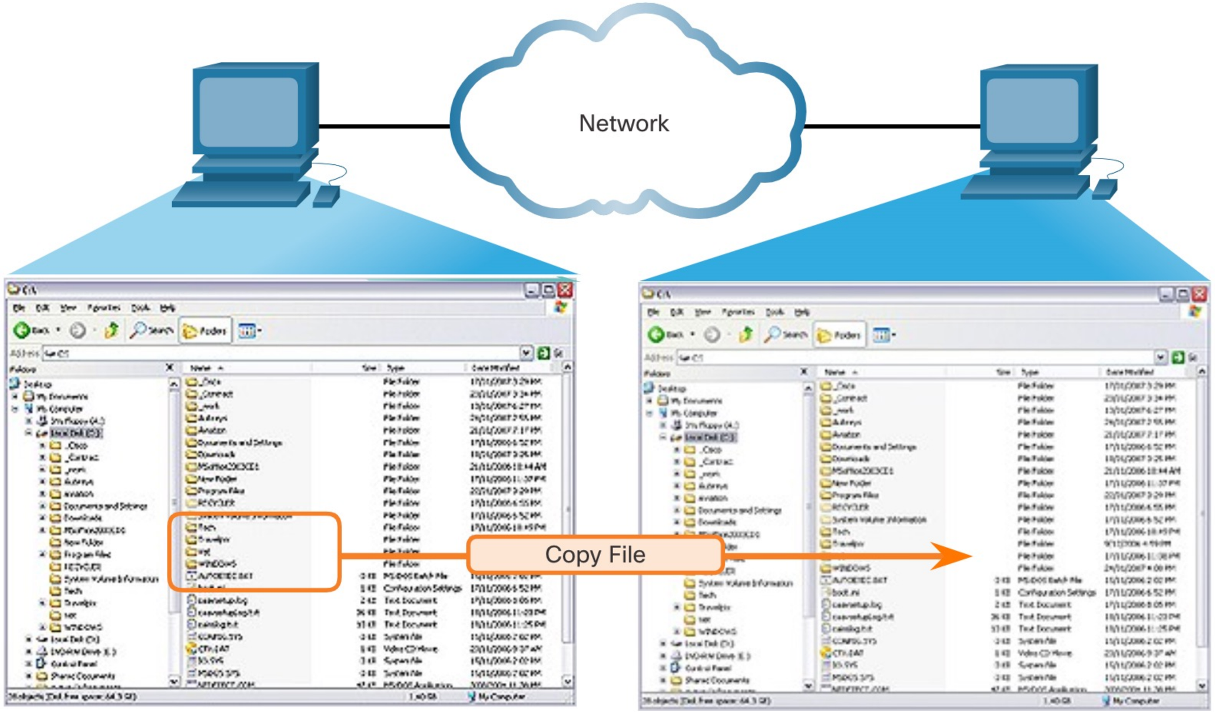


- File systems
- Printers
- Mail slots
- APIs

File Transfer and Sharing Services

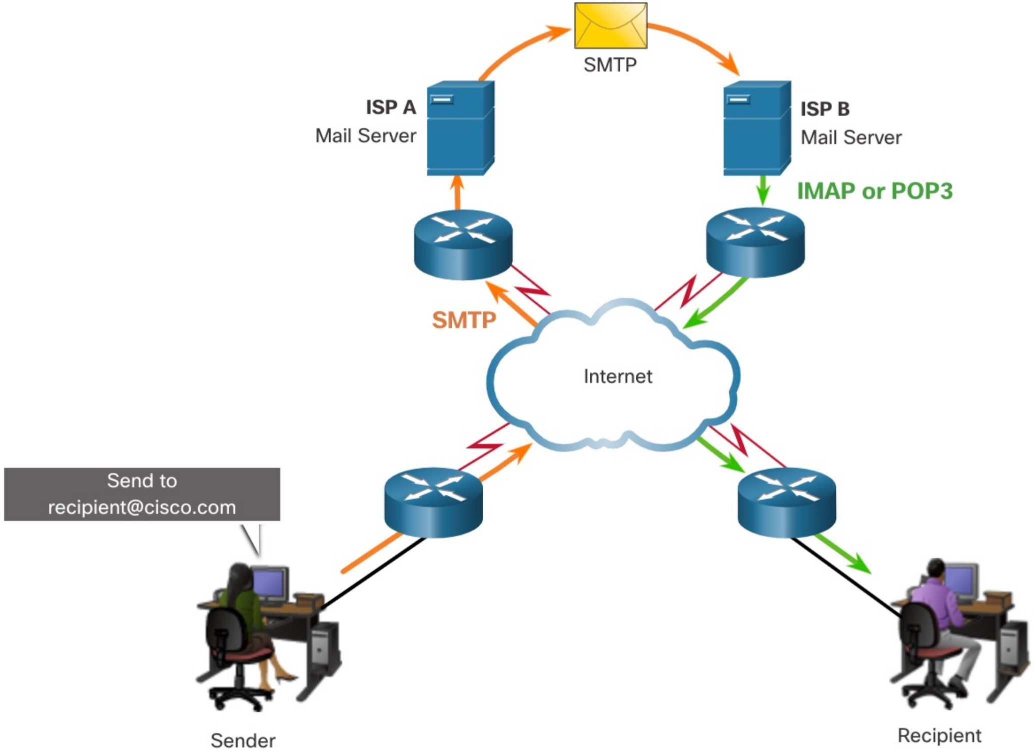
SMB (Contd.)

- SMB messages can start, authenticate, and terminate sessions, control file and printer access, and 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.
- A file may be copied from PC to PC with Windows Explorer using the SMB protocol.



Email protocols

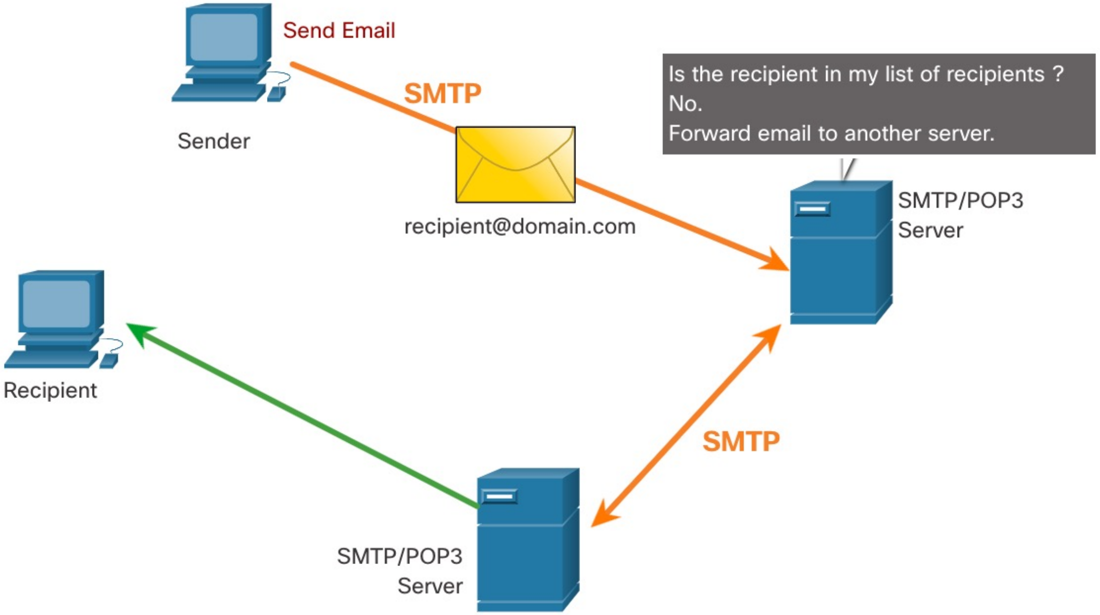
- Email supports three separate protocols for operation:
  - Simple Mail Transfer Protocol (SMTP)
  - Post Office Protocol version 3 (POP3)
  - IMAP
- The application layer process that sends mail uses SMTP. A client retrieves email using one of the two application layer protocols: POP3 or IMAP.



Email

SMTP

- SMTP
  - Simple Mail Transfer Protocol (SMTP) – 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.

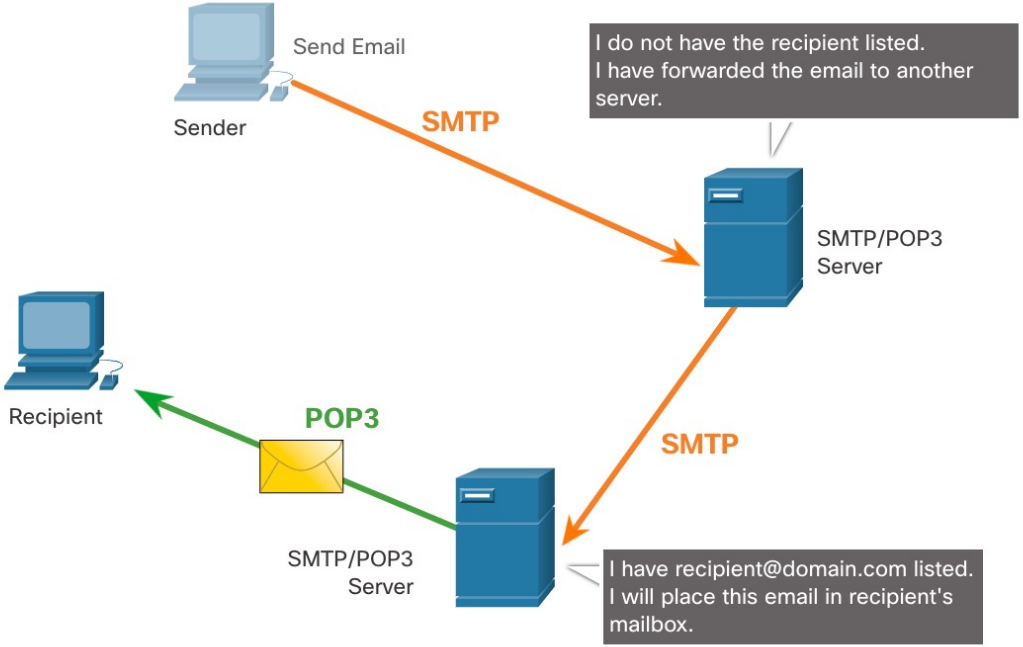


Is the recipient in my list of recipients ?
No.
Forward email to another server.

Email

POP3

- POP3 is used by an application to retrieve a mail from a mail server
- With POP3, mail is downloaded from the server to the client and then deleted on the server.
- With POP3, email messages are downloaded to the client and removed from the server, so there is no centralized location where email messages are kept.

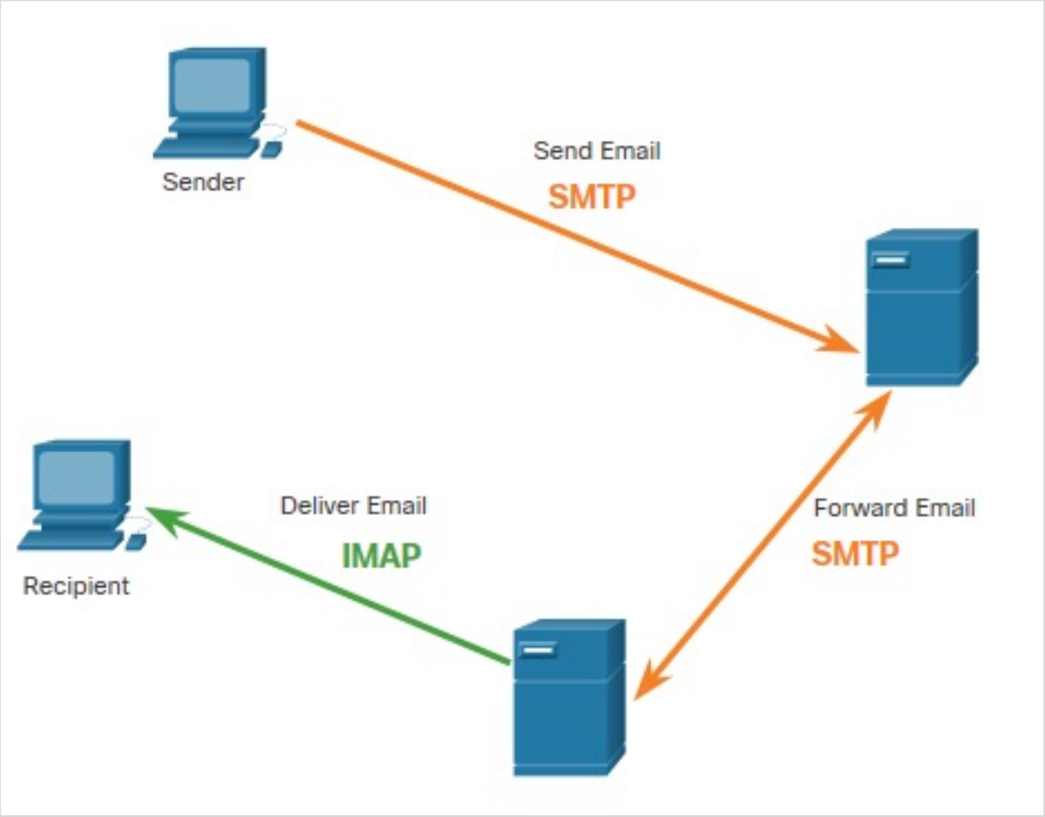


I do not have the recipient listed. I have forwarded the email to another server.

I have recipient@domain.com listed. I will place this email in recipient's mailbox.

IMAP

- IMAP is the protocol that describes a method to retrieve email messages.
- When a user connects to an IMAP-capable server, copies of the messages are downloaded to the client application.
- When a user decides to delete a message, the server synchronizes that action and deletes the message from the server.



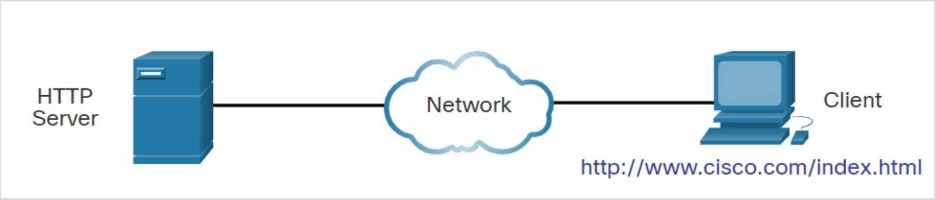
HTTP Overview

- Hypertext Transfer Protocol (HTTP) :
  - Port 80
  - Governs the way a web server and client interact.
  - Has specific server responses.
- Steps:
  1. Client initiates HTTP request to server.
  2. HTTP returns code for a webpage.
  3. Browser interprets HTML code and displays on webpage.
  4. The browser deciphers the HTML code and formats the page for the browser window.

HTTP

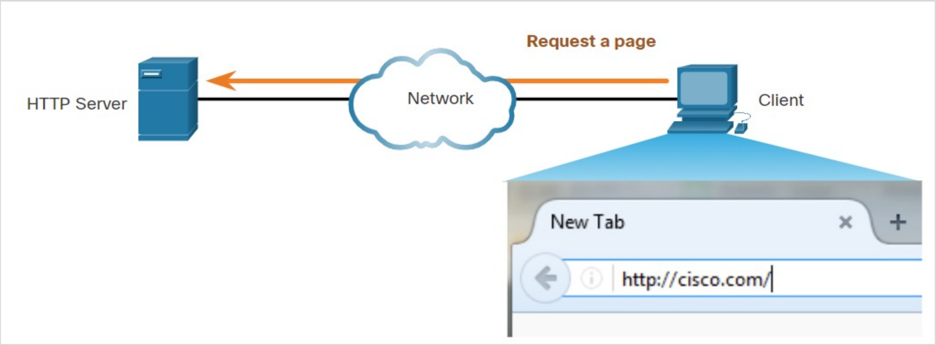
HTTP Overview

- Hypertext Transfer Protocol (HTTP) :
  - Port 80
  - Governs the way a web server and client interact.
  - Has specific server responses.
- Steps:
  1. Client initiates HTTP request to server.
  2. HTTP returns code for a webpage.
  3. Browser interprets HTML code and displays on webpage.
  4. The browser deciphers the HTML code and formats the page for the browser window.



HTTP Overview

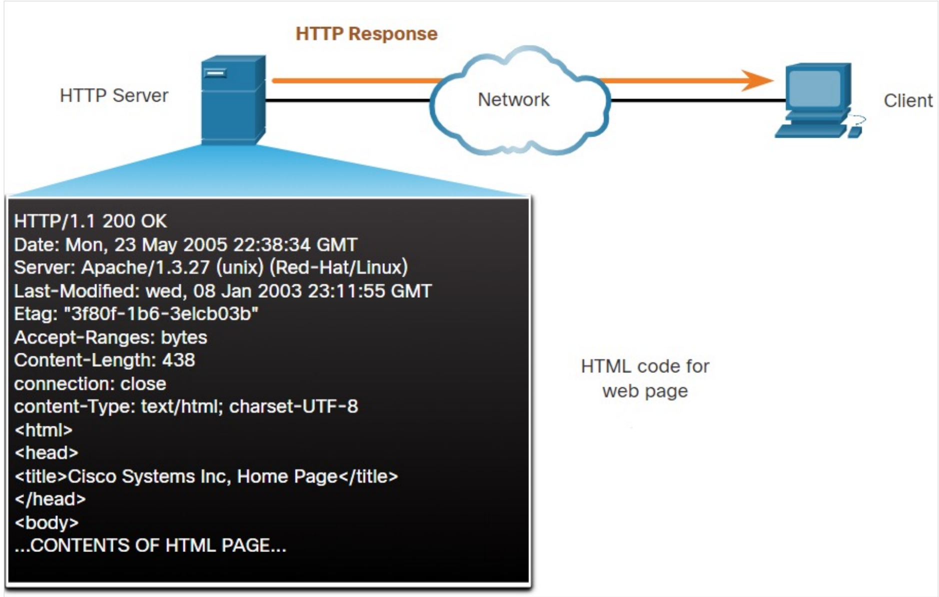
- Hypertext Transfer Protocol (HTTP) :
  - Port 80
  - Governs the way a web server and client interact.
  - Has specific server responses.
- Steps:
  1. Client initiates HTTP request to server.
  2. HTTP returns code for a webpage.
  3. Browser interprets HTML code and displays on webpage.
  4. The browser deciphers the HTML code and formats the page for the browser window.



HTTP

HTTP Overview

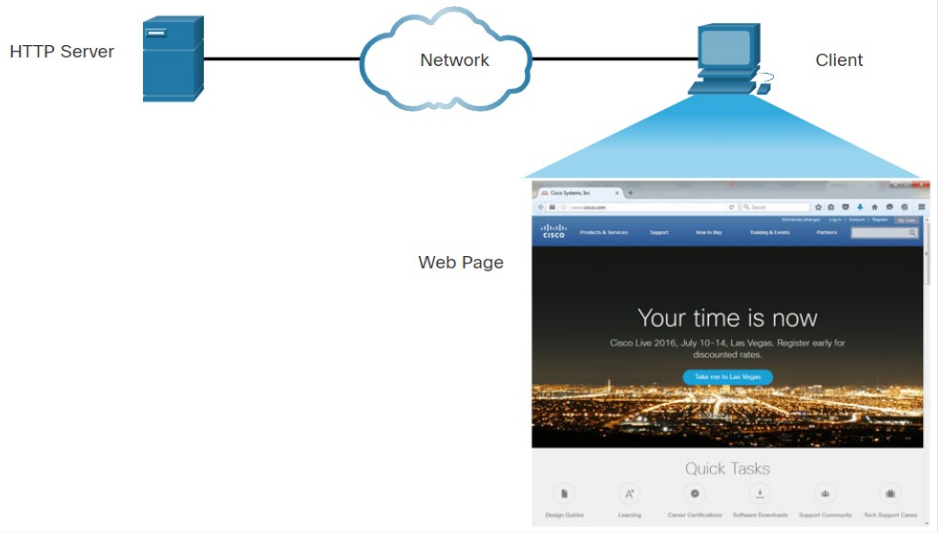
- Hypertext Transfer Protocol (HTTP) :
  - Port 80
  - Governs the way a web server and client interact.
  - Has specific server responses.
- Steps:
  1. Client initiates HTTP request to server.
  2. HTTP returns code for a webpage.
  3. Browser interprets HTML code and displays on webpage.
  4. The browser deciphers the HTML code and formats the page for the browser window.



```
HTTP/1.1 200 OK
Date: Mon, 23 May 2005 22:38:34 GMT
Server: Apache/1.3.27 (unix) (Red-Hat/Linux)
Last-Modified: wed, 08 Jan 2003 23:11:55 GMT
Etag: "3f80f-1b6-3elcb03b"
Accept-Ranges: bytes
Content-Length: 438
connection: close
content-Type: text/html; charset-UTF-8
<html>
<head>
<title>Cisco Systems Inc, Home Page</title>
</head>
<body>
...CONTENTS OF HTML PAGE...
```

HTTP Overview

- Hypertext Transfer Protocol (HTTP) :
  - Port 80
  - Governs the way a web server and client interact.
  - Has specific server responses.
- Steps:
  1. Client initiates HTTP request to server.
  2. HTTP returns code for a webpage.
  3. Browser interprets HTML code and displays on webpage.
  4. The browser deciphers the HTML code and formats the page for the browser window.



Your time is now

Cisco Live 2016, July 10-14, Las Vegas. Register early for discounted rates.

Quick Tasks

HTTP Status Codes

- The HTTP Status codes are numeric, with the first number in the code indicating the type of message.
- The five status code groups are **1xx** - Informational, **2xx** - Success, **3xx** - Redirection , **4xx** - Client Error and **5xx** - Server Error
- The below table explains some common status codes:

Code	Status	Meaning
1xx - Informational		
100	Continue	The client should continue with the request. The Server has verified that the request can be fulfilled.
2xx - Success		
200	OK	The request completed successfully.
202	Accepted	The request has been accepted for processing, but processing is not completed.

HTTP

HTTP Status Codes (Contd.)

Code	Status	Meaning
4xx – Client Error		
403	Forbidden	The request is understood by the server, but the resource will not be fulfilled. This is possibly because the requester is not authorized to view the resource.
404	Not Found	The server could not find the requested resource. This can be caused by an out-of-date or incorrect URL.

Network Protocols and Services

New Terms and Commands

- FTP
- TFTP
- TCP
- UDP
- SMB
- SMTP
- POP
- IMAP

Network Protocols and Services

Lab 15 - Exploring Nmap

- Port scanning is usually part of a reconnaissance attack.
- There are a variety of port scanning methods that can be used.
- We will explore how to use the Nmap utility. Nmap is a powerful network utility that is used for network discovery and security auditing.

Lab 16 - Using Wireshark to Examine HTTP and HTTPS Traffic

- In this lab, you will complete the following objectives:
  - Capture and view HTTP traffic
  - Capture and view HTTPS traffic