Chapter 10: Application Layer

Curriculum Title

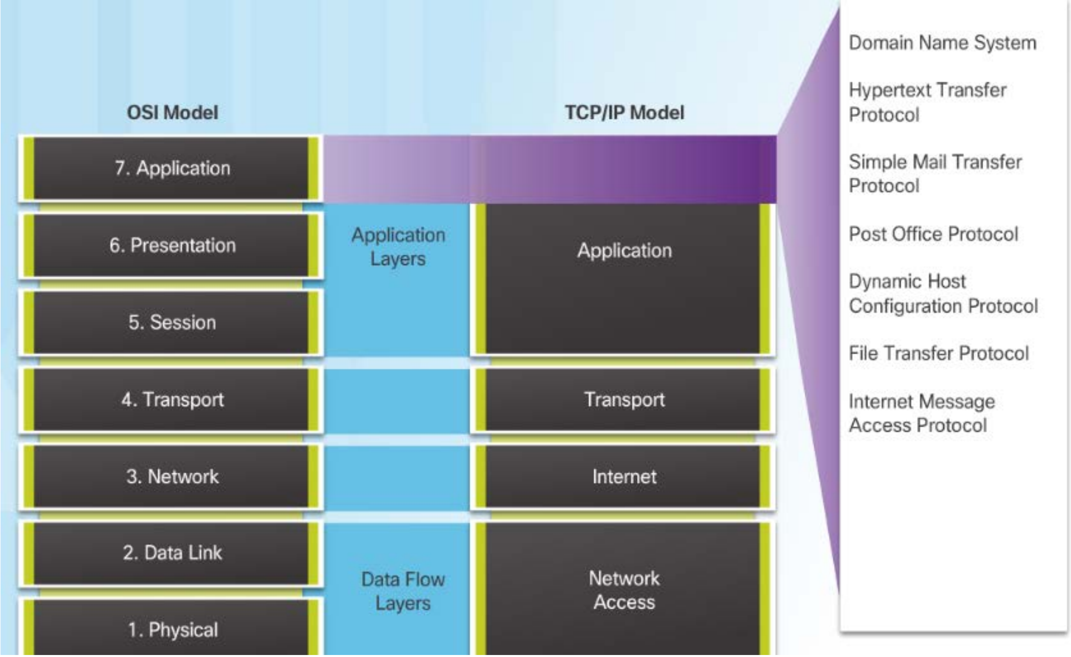
Introduction to Networks v6.0

Chapter 10 - Sections & Objectives

- 10.1 Application Layer Protocols
  - Explain the operation of the application layer in providing support to end-user applications.
    - 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 Protocols and Services
  - Explain how well-known TCP/IP application layer protocols operate.
    - Explain how web and email protocols operate.
    - Explain how DNS and DHCP operate.
    - Explain how file transfer protocols operate.

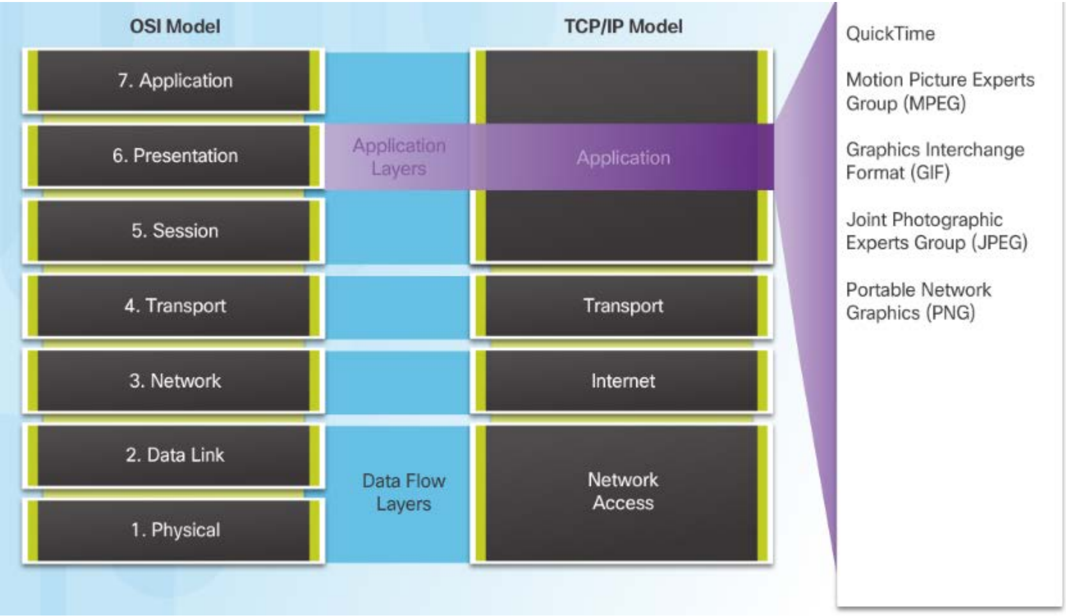
10.1 Application Layer Protocols

Application Layer



- Application Layer:
  - Closest to the end user.
  - Used to exchange data between programs running on the source and destination hosts.

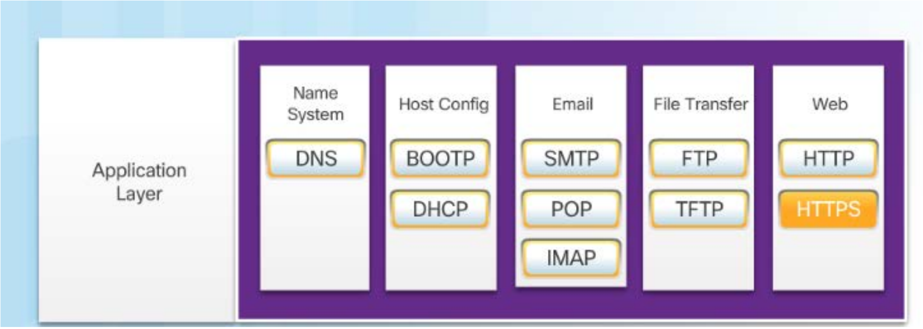
Presentation and Session Layer



- Presentation Layer function:
  - Formatting data at the source device into a compatible form for the receiving device.
  - Compressing data.
  - Encrypting data.
- Session Layer Function
  - Create and maintain dialogs between source and destination applications.

Application, Presentation, and Session

TCP/IP Application Layer Protocols



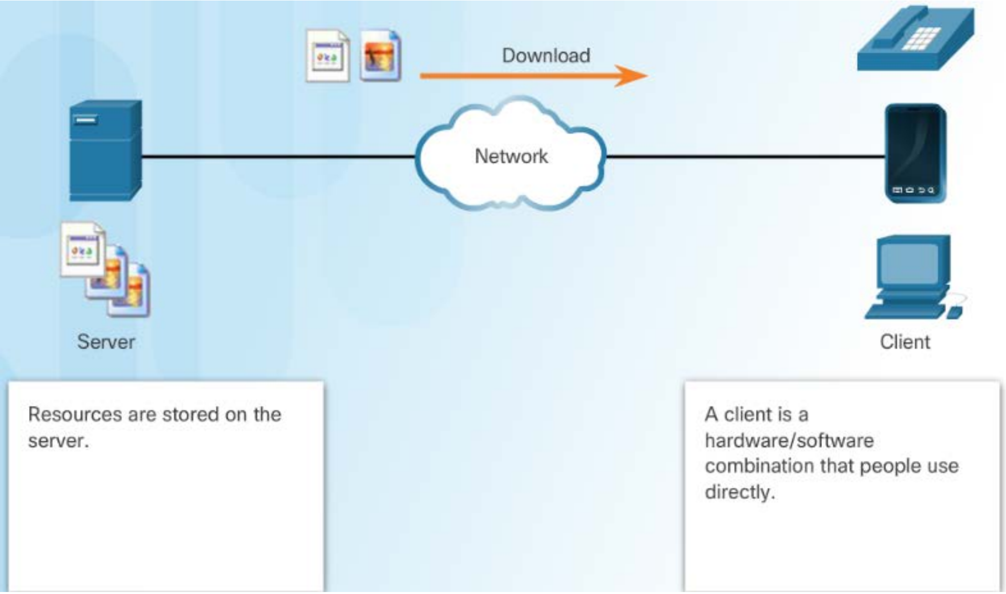
Application Layer	Name System	Host Config	Email	File Transfer	Web
	DNS	BOOTP	SMTP	FTP	HTTP
		DHCP	POP	TFTP	HTTPS
			IMAP		

- Domain Name Server (DNS) TCP,UDP 53 - Translates domain names, such as cisco.com, into IP addresses.
- (BOOTP) – Bootstrap Protocol - BOOTP is being superseded by DHCP.
- Dynamic Host Configuration Protocol (DHCP) UDP client 68, server 67 – Dynamically assigns IP addresses to client stations at start-up.
- Simple Mail Transport Protocol (SMTP) TCP 25 - Enables clients to send email to a mail server.
- Post Office Protocol (POP) TCP 110 - Enables clients to retrieve email from a mail server.
- Internet Message Access Protocol (IMAP) TCP 143 - Enables clients to retrieve email from a mail server, maintains email on server.
- File Transfer Protocol (FTP) TCP 20 and 21 - Reliable, connection-oriented, and acknowledged file delivery protocol.
- Trivial File Transfer Protocol (TFTP) UDP 69 – simple connectionless file transfer protocol.
- Hypertext Transfer Protocol (HTTP) TCP 80, 8080 - Set of rules for exchanging text, graphic images, etc. on the World Wide Web.
- Hypertext Transfer Protocol Secure (HTTPS) TCP, UDP 443 – Uses encryption and authentication to secure communication.

How Application Protocols Interact with End-User Applications

Client-Server Model

- Client and server processes are considered to be in the application layer.
- Application layer protocols describe the format of the requests and responses between clients and servers.
- Example of a client-server network is using an ISP’s email service to send, receive and store email.



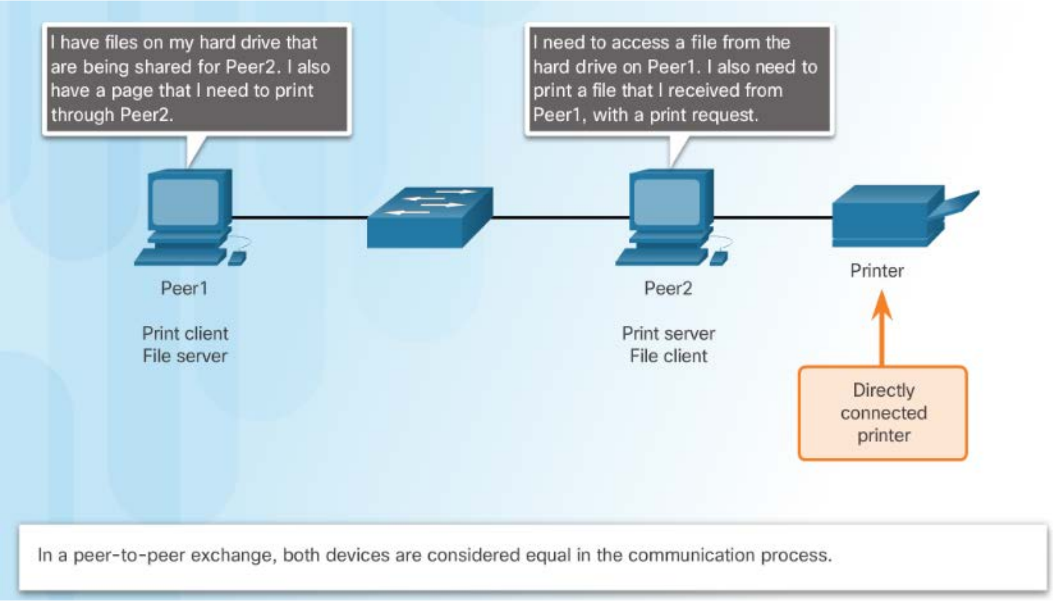
Resources are stored on the server.

A client is a hardware/software combination that people use directly.

How Application Protocols Interact with End-User Applications

Peer-to-Peer Networks

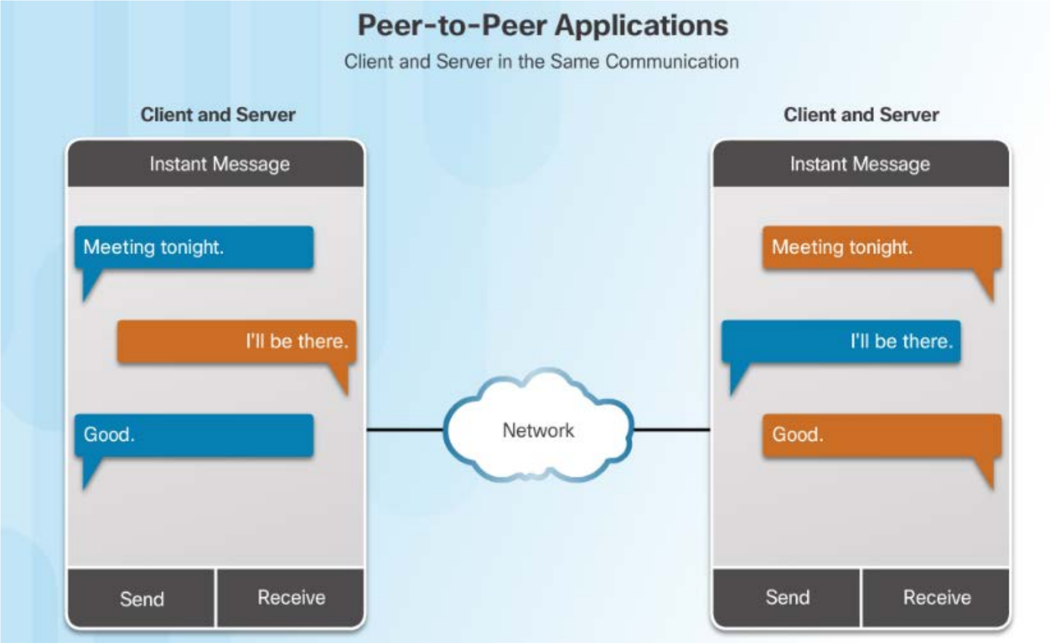
- Data is accessed from a peer device without the use of a dedicated server.
- Each device (known as a peer) can function as both a server and a client.


I have files on my hard drive that are being shared for Peer2. I also have a page that I need to print through Peer2.
I need to access a file from the hard drive on Peer1. I also need to print a file that I received from Peer1, with a print request.
Peer1
Print client
File server
Peer2
Print server
File client
Printer
Directly connected printer

In a peer-to-peer exchange, both devices are considered equal in the communication process.

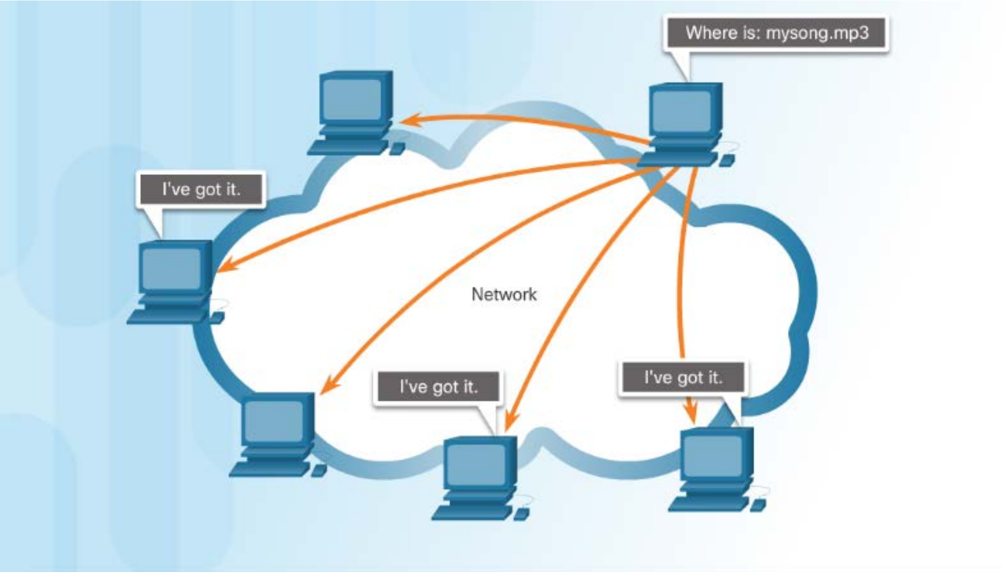
Peer-to-Peer Applications

- A P2P application allows a device to act as both a client and a server within the same communication.
- P2P applications require that each end device provide a user interface and run a background service.



How Application Protocols Interact with End-User Applications

Common P2P Applications

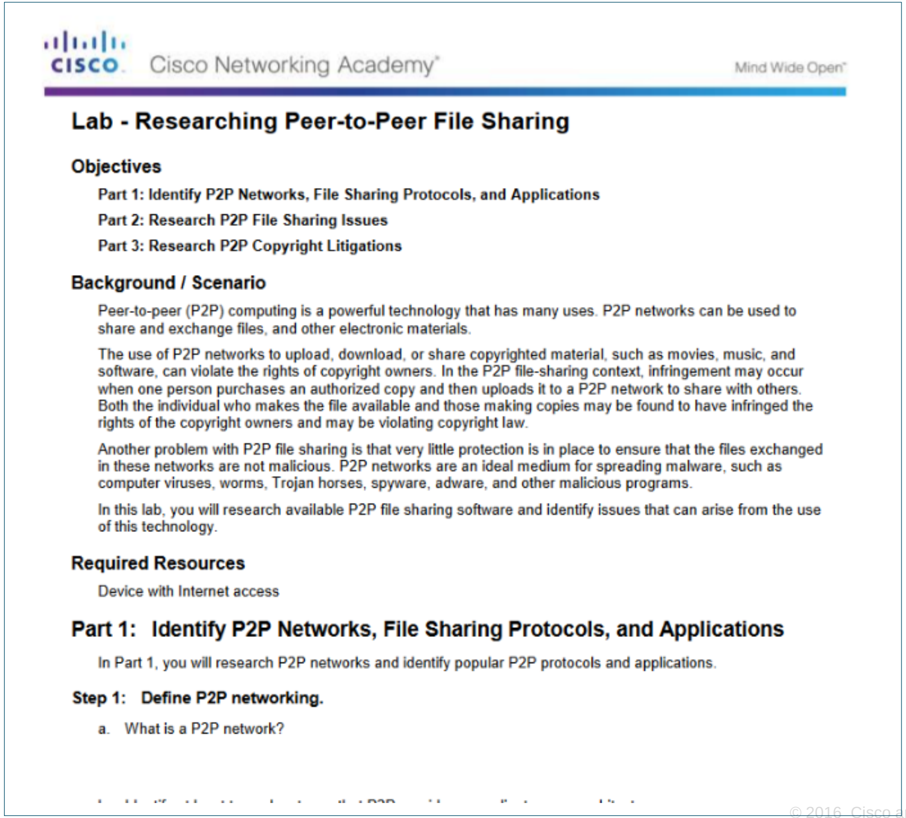


Gnutella allows P2P applications to search for shared resources on peers.

- Common P2P networks include:
  - G2
  - Bitcoin
  - BitTorrent
  - eDonkey
- Some P2P applications are based on the Gnutella protocol, where each user shares whole files with other users.
- Many P2P applications allow users to share pieces of many files with each other at the same time –this is BitTorrent technology.

How Application Protocols Interact with End-User Applications

Researching Peer-to-Peer File Sharing



Cisco Networking Academy®

Mind Wide Open™

Lab - Researching Peer-to-Peer File Sharing

Objectives

Part 1: Identify P2P Networks, File Sharing Protocols, and Applications

Part 2: Research P2P File Sharing Issues

Part 3: Research P2P Copyright Litigations

Background / Scenario

Peer-to-peer (P2P) computing is a powerful technology that has many uses. P2P networks can be used to share and exchange files, and other electronic materials.

The use of P2P networks to upload, download, or share copyrighted material, such as movies, music, and software, can violate the rights of copyright owners. In the P2P file-sharing context, infringement may occur when one person purchases an authorized copy and then uploads it to a P2P network to share with others. Both the individual who makes the file available and those making copies may be found to have infringed the rights of the copyright owners and may be violating copyright law.

Another problem with P2P file sharing is that very little protection is in place to ensure that the files exchanged in these networks are not malicious. P2P networks are an ideal medium for spreading malware, such as computer viruses, worms, Trojan horses, spyware, adware, and other malicious programs.

In this lab, you will research available P2P file sharing software and identify issues that can arise from the use of this technology.

Required Resources

Device with Internet access

Part 1: Identify P2P Networks, File Sharing Protocols, and Applications

In Part 1, you will research P2P networks and identify popular P2P protocols and applications.

Step 1: Define P2P networking.

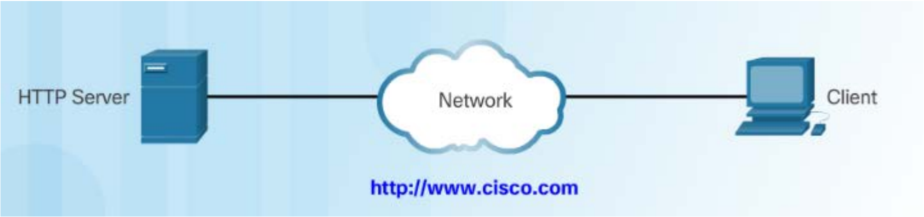
a. What is a P2P network?

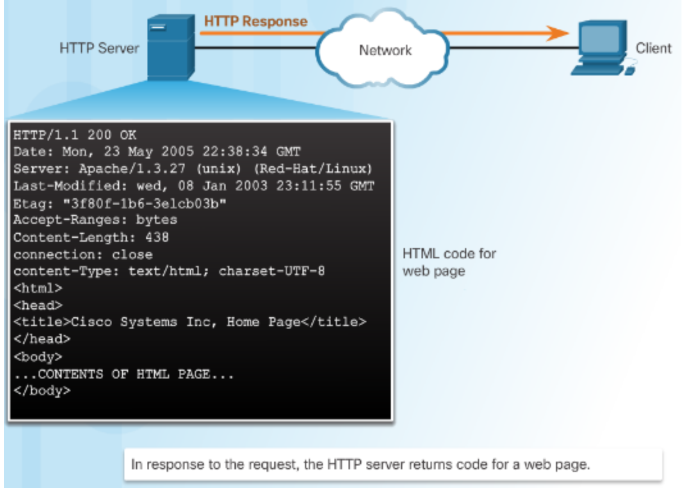
10.2 Well-Known Application Layer Protocols and Services

Web and Email Protocols

Hypertext Transfer Protocol and Hypertext Markup Language

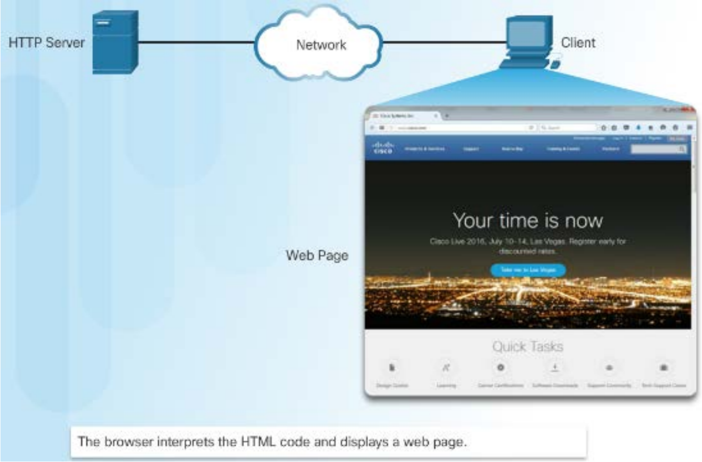
- When a web address or uniform resource locator (URL) is typed into a web browser, the web browser establishes a connection to the web service running on the server, using the HTTP protocol.





```
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...
</body>
```

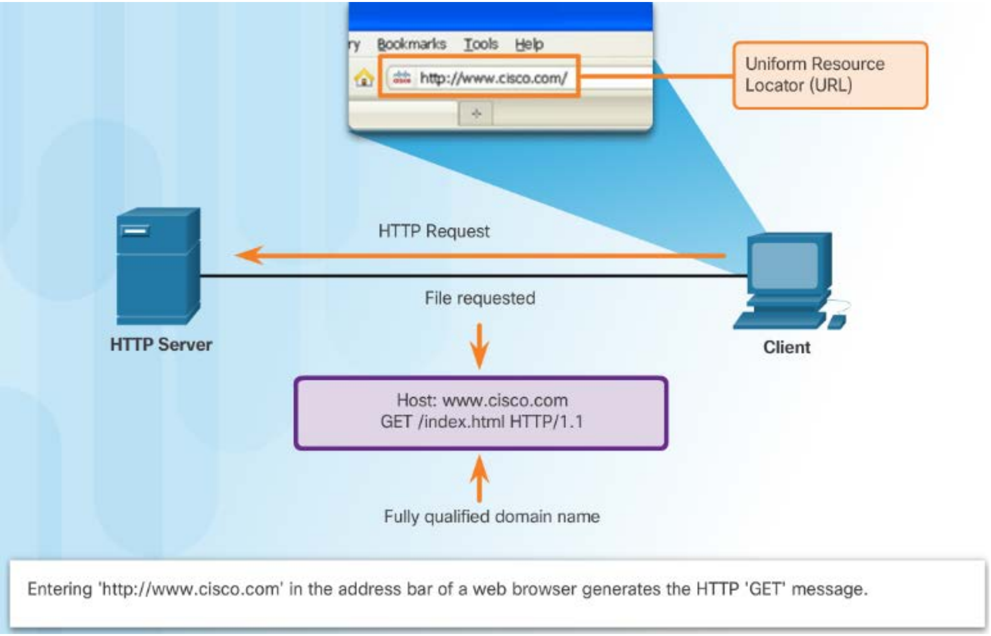
In response to the request, the HTTP server returns code for a web page.



The browser interprets the HTML code and displays a web page.

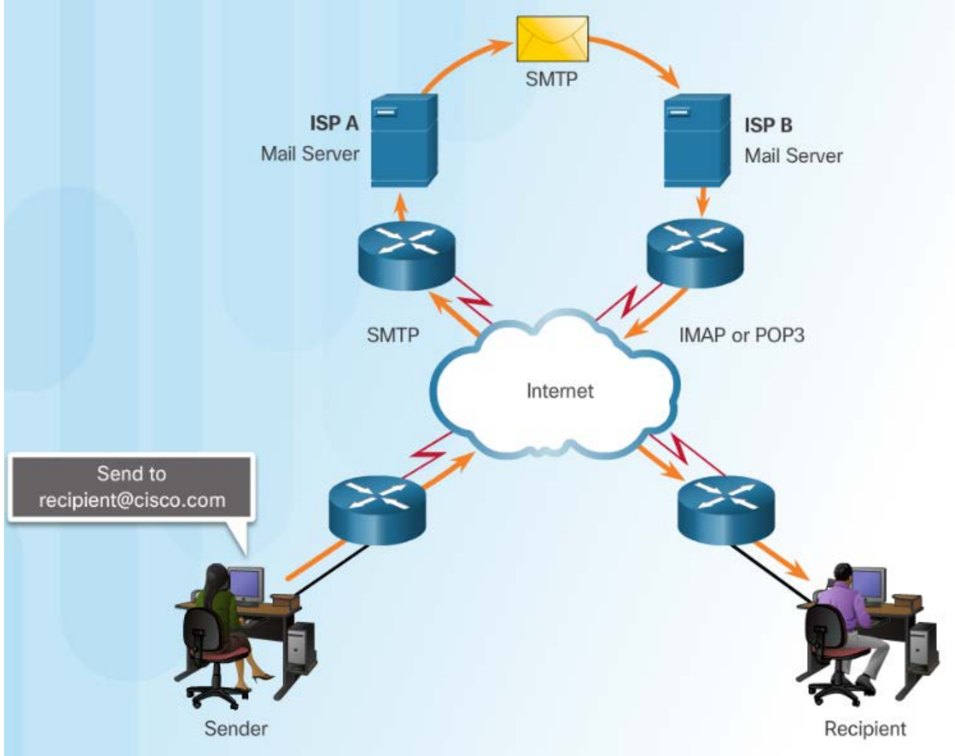
HTTP and HTTPS

- HTTP is a request/response protocol.
- Three common HTTP message types are:
  - GET - A client request for data.
  - POST - Uploads data files to the web server.
  - PUT - Uploads resources or content to the web server.
- HTTP Secure (HTTPS) protocol uses encryption and authentication to secure data.



Entering 'http://www.cisco.com' in the address bar of a web browser generates the HTTP 'GET' message.

Email Protocols

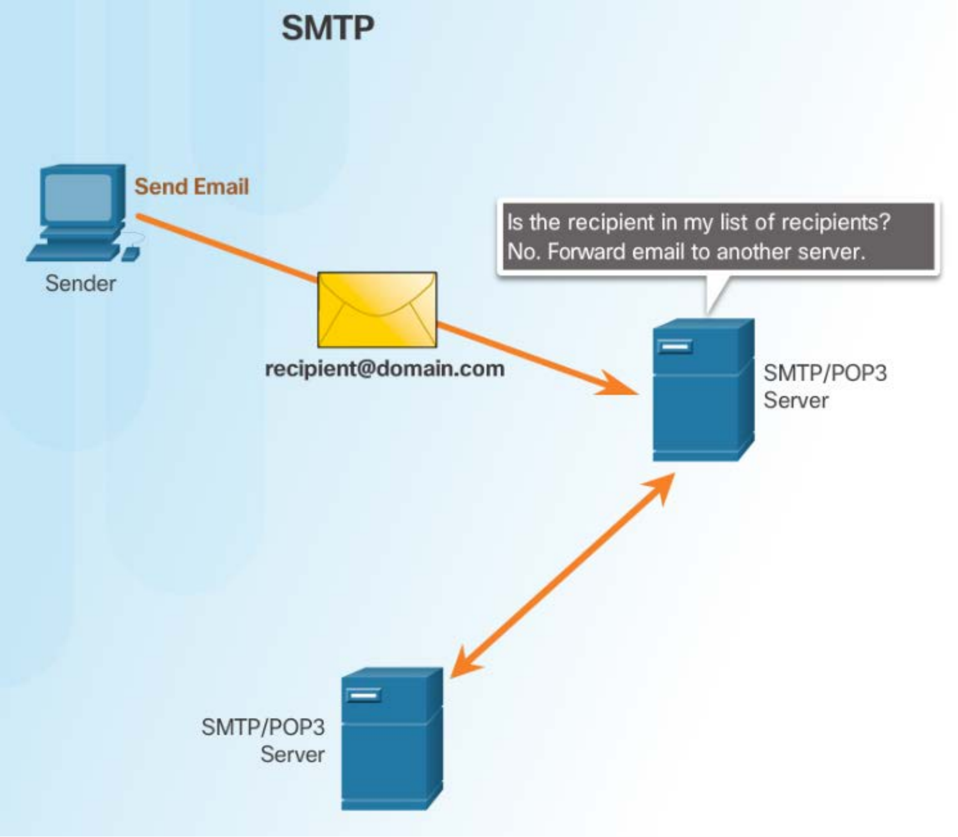


- Email clients communicate with mail servers to send and receive email.
- Mail servers communicate with other mail servers to transport messages from one domain to another.
- Three protocols for email:
  - Simple Mail Transfer Protocol (SMTP) to send email.
  - Post Office Protocol (POP) to retrieve email.
  - Internet Message Access Protocol (IMAP) to retrieve email.

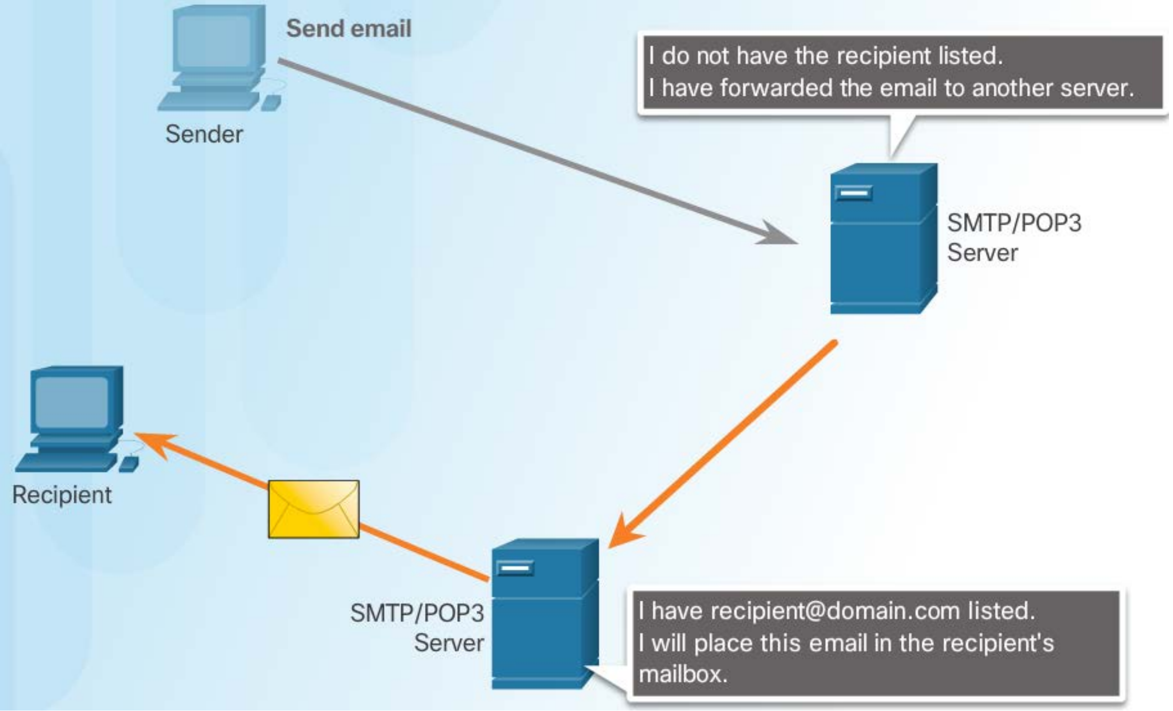
Web and Email Protocols

SMTP Operation

- SMTP is used to send email

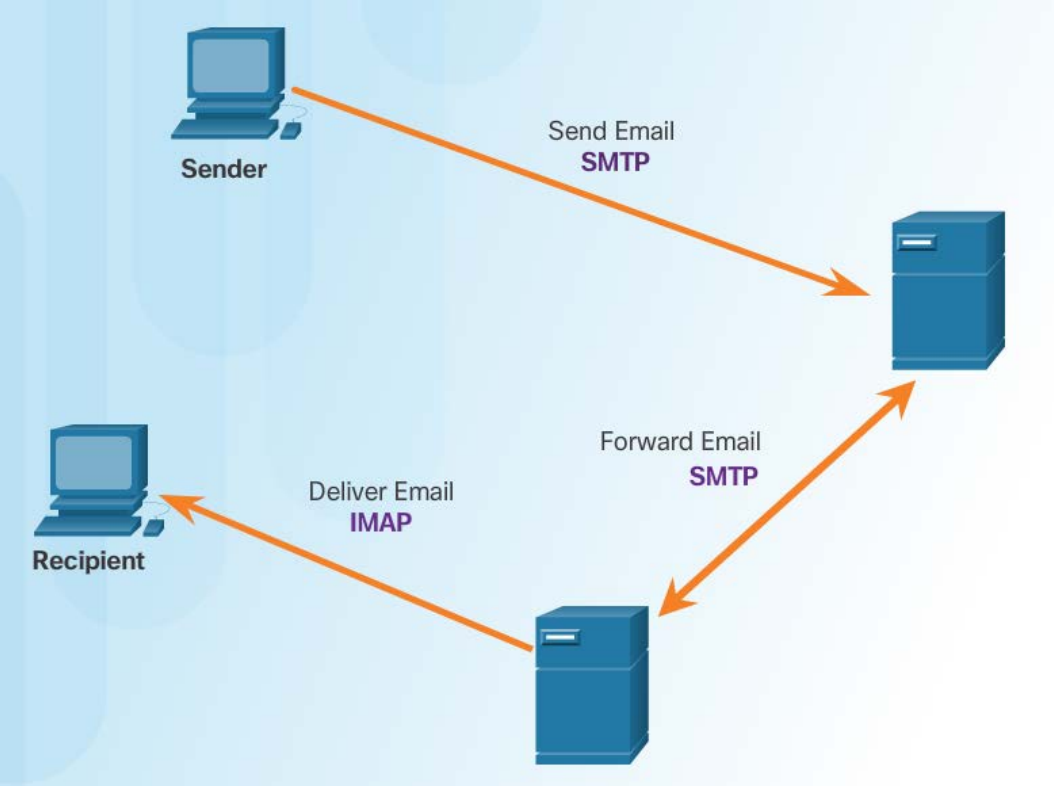

SMTP
Send Email
Sender
recipient@domain.com
Is the recipient in my list of recipients? No. Forward email to another server.
SMTP/POP3 Server
SMTP/POP3 Server

POP Operation


Send email
Sender
I do not have the recipient listed.
I have forwarded the email to another server.
SMTP/POP3 Server
Recipient
SMTP/POP3 Server
I have recipient@domain.com listed.
I will place this email in the recipient's mailbox.

- POP is used to retrieve email from a mail server.
- Email is downloaded from the server to the client and then deleted on the server.

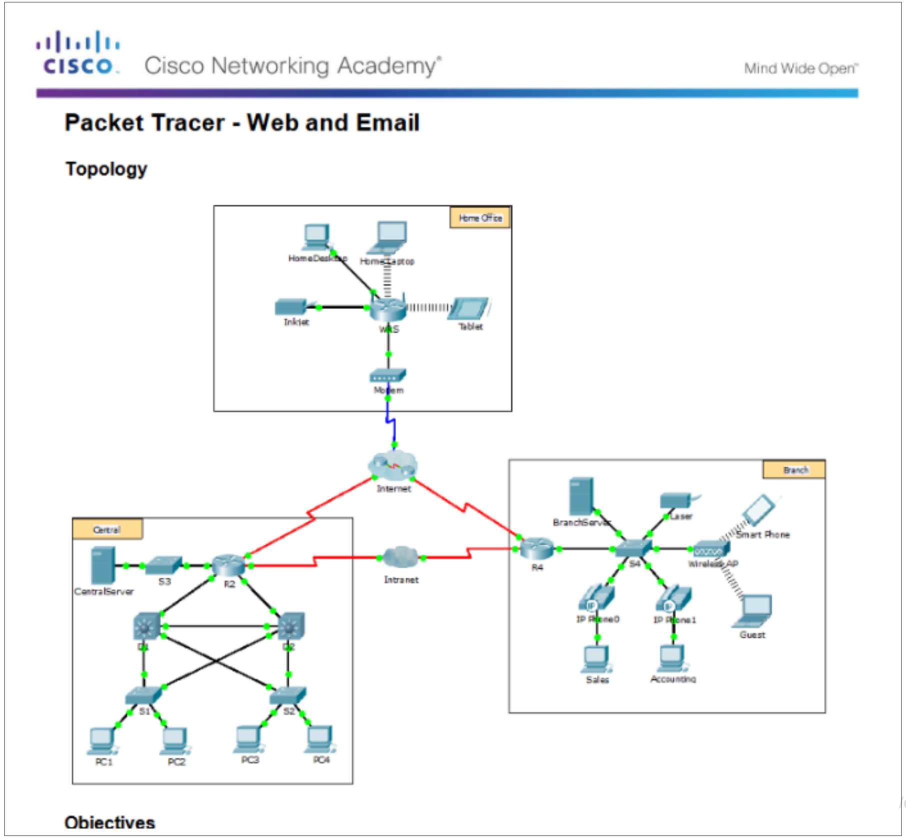
IMAP Operation



- IMAP is used to retrieve mail from a mail server.
- Copies of messages are downloaded from the server to the client and the original messages are stored on the server.

Web and Email Protocols

Packet Tracer – Web and Email



Cisco Networking Academy®

Mind Wide Open™

Packet Tracer - Web and Email

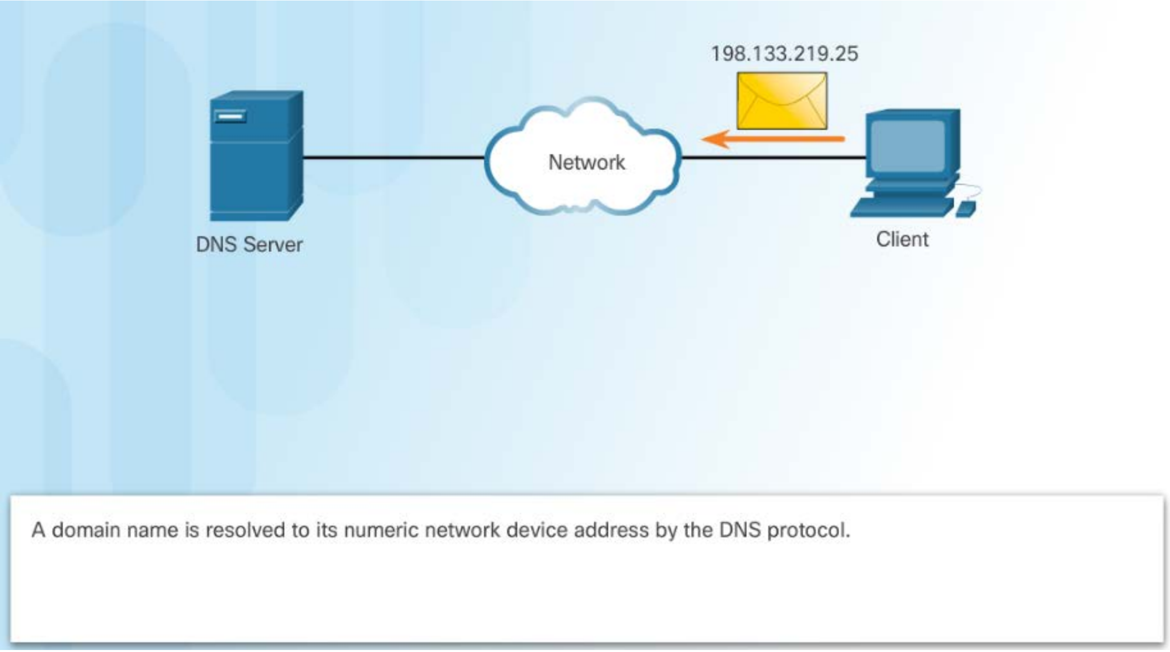
Topology

Objectives

IP Addressing Services

Domain Name Service

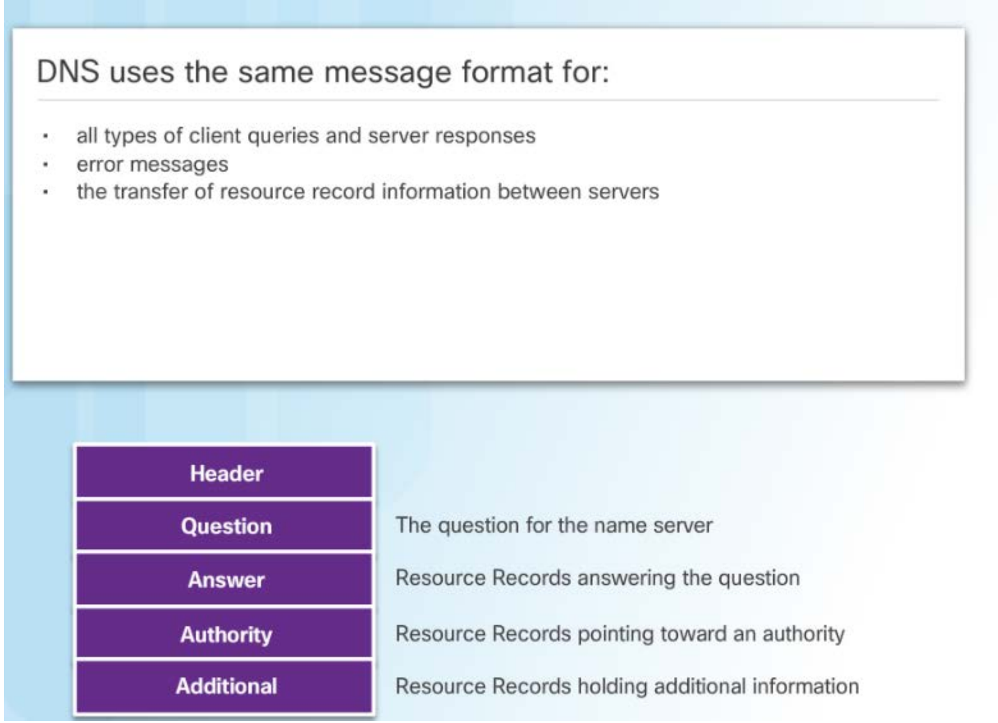
- Domain names convert the numeric address into a simple, recognizable name.
- The DNS protocol defines an automated service that matches resource names with the required numeric network address.



A domain name is resolved to its numeric network device address by the DNS protocol.

IP Addressing Services

DNS Message Format



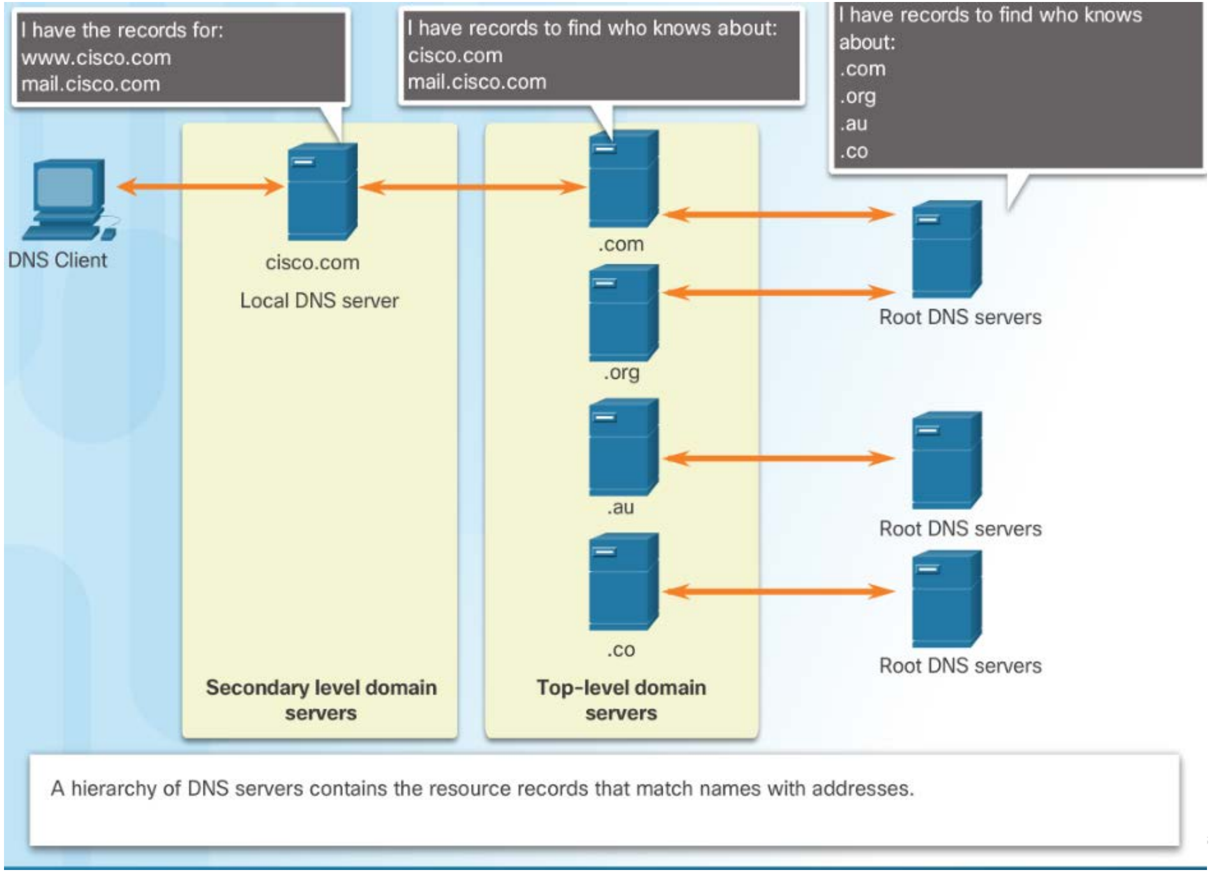
DNS uses the same message format for:

- 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

- When a client makes a query, the server’s DNS process first looks at its own records to resolve the name.
- If unable to resolve, it contacts other servers to resolve the name.
- The server temporarily stores the numbered address in the event that the same name is requested again.
- The **ipconfig /displaydns** command displays all of the cached DNS entries on a Windows PC.

DNS Hierarchy



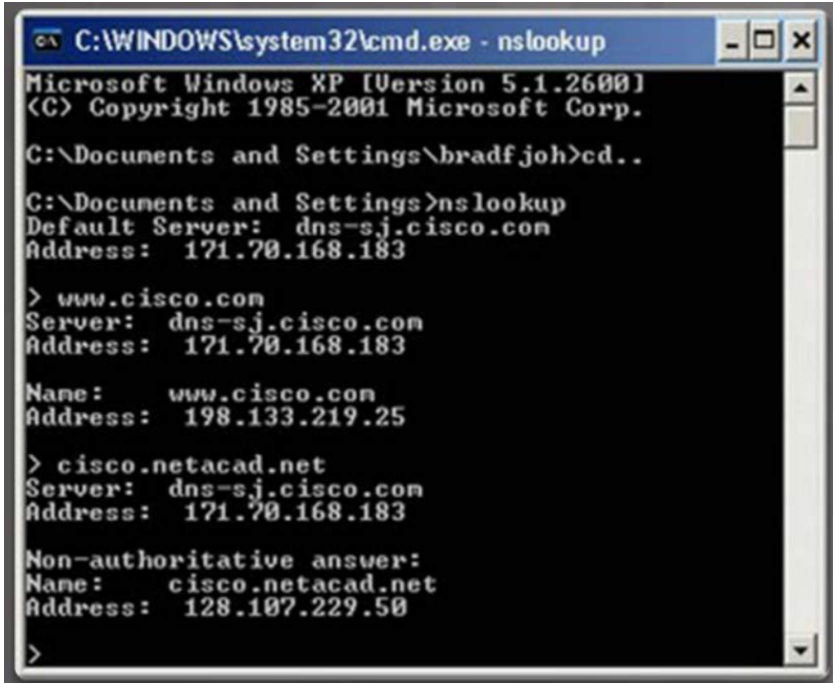
I have the records for:
www.cisco.com
mail.cisco.com

I have records to find who knows about:
cisco.com
mail.cisco.com

I have records to find who knows about:
.com
.org
.au
.co

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

The nslookup Command

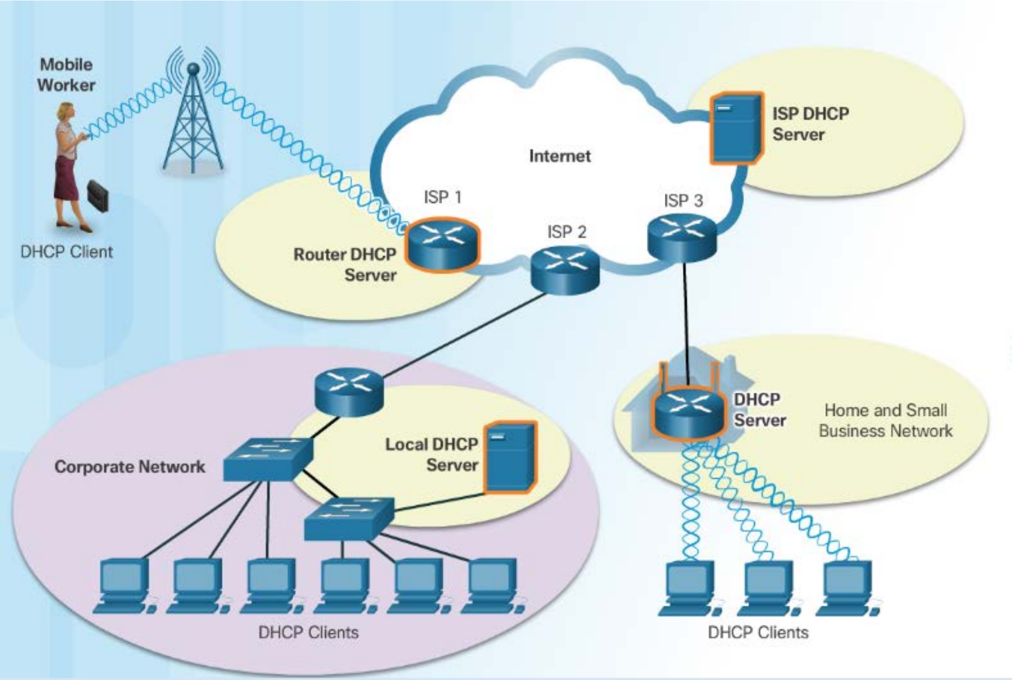


```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

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

>
```

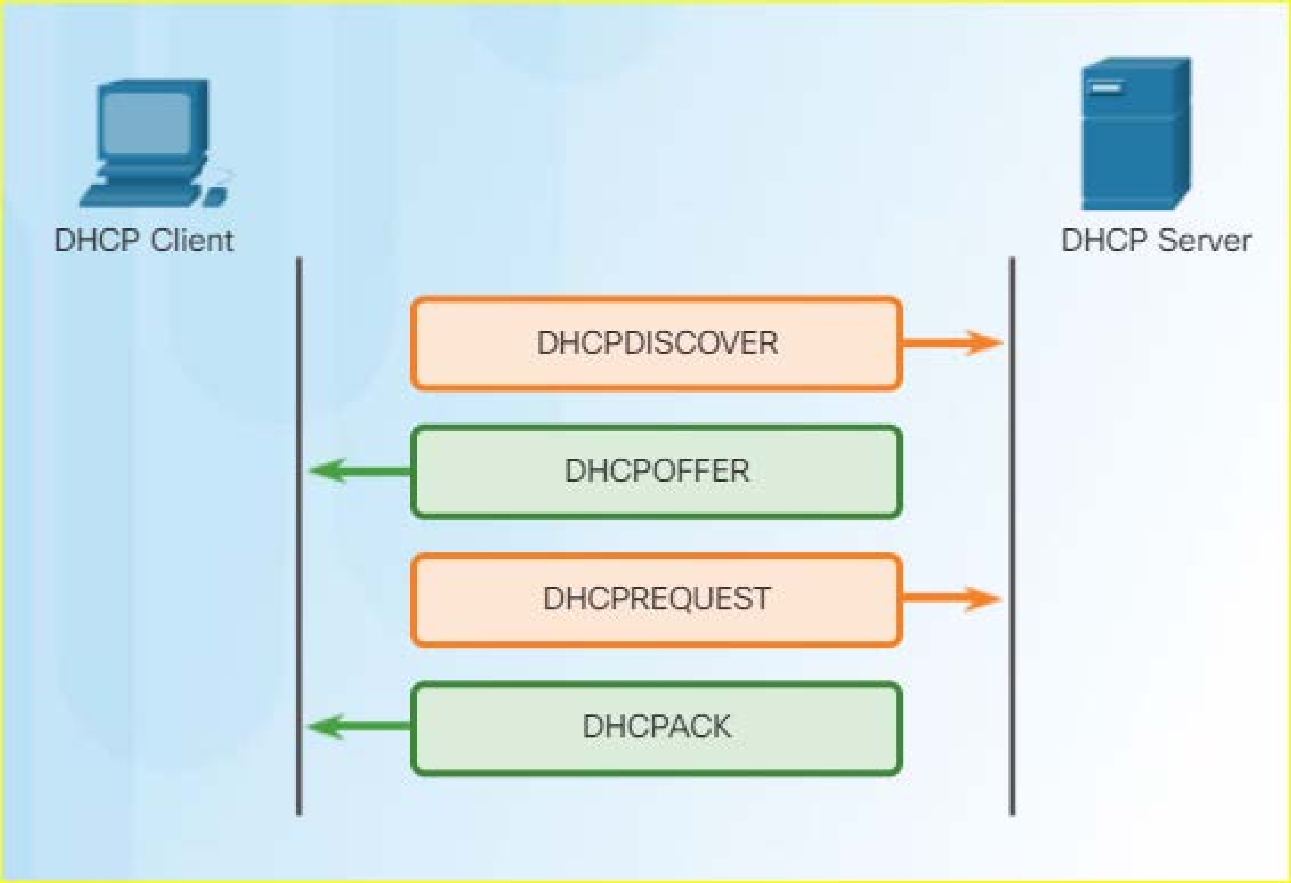
- **Nslookup** - a utility that allows a user to manually query the name servers to resolve a given host.
  - Can also be used to troubleshoot name resolution issues and to verify the current status of the name servers.

Dynamic Host Configuration Protocol

- The Dynamic Host Configuration Protocol (DHCP) for IPv4 automates the assignment of IPv4 addresses, subnet masks, gateways, and other parameters.
- DHCP-distributed addresses are leased for a set period of time, then returned to pool for reuse.
- DHCP is usually employed for end user devices. Static addressing is used for network devices, such as gateways, switches, servers, and printers.
- DHCPv6 (DHCP for IPv6) provides similar services for IPv6 clients.

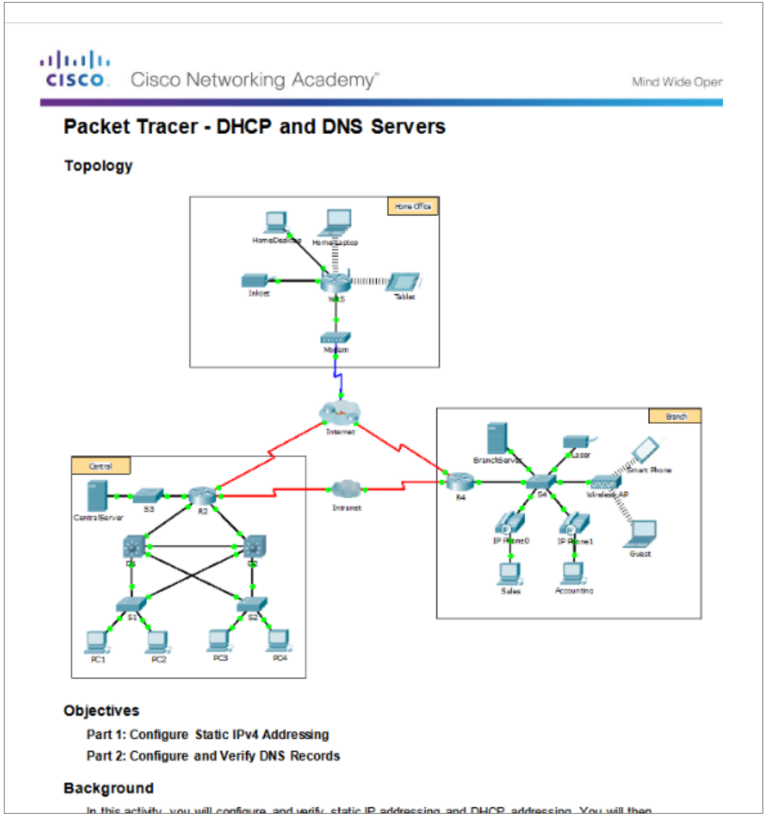


DHCP Operation



IP Addressing Services

Packet Tracer – DHCP and DNS Servers



Cisco Networking Academy®

Mind Wide Oper

Packet Tracer - DHCP and DNS Servers

Topology

Objectives

Part 1: Configure Static IPv4 Addressing

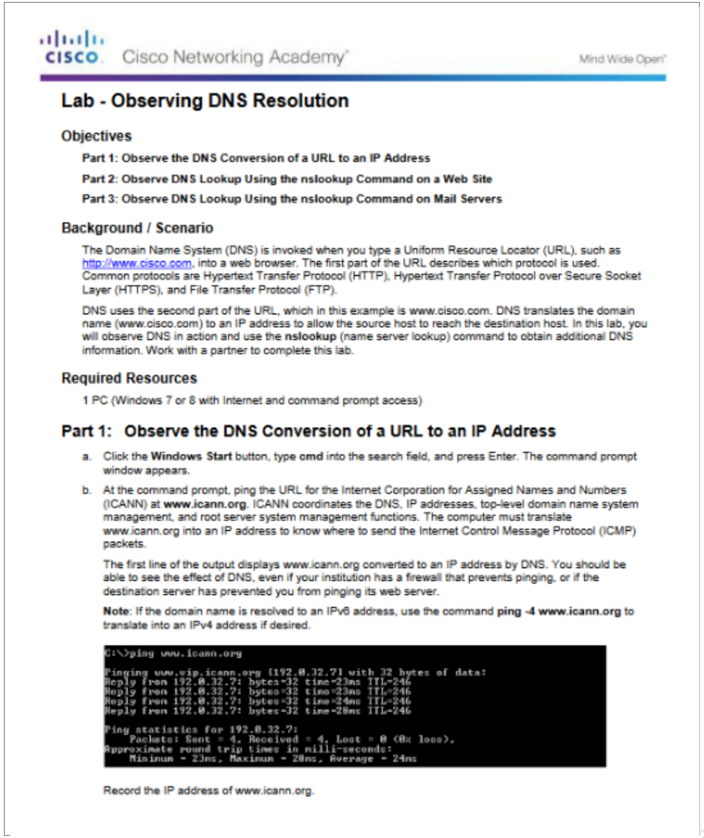
Part 2: Configure and Verify DNS Records

Background

In this activity, you will configure and verify static IP addressing and DHCP addressing. You will then

IP Addressing Services

Lab – Observing DNS Resolution



Cisco Networking Academy® Mind Wide Open™

Lab - Observing DNS Resolution

Objectives

Part 1: Observe the DNS Conversion of a URL to an IP Address

Part 2: Observe DNS Lookup Using the nslookup Command on a Web Site

Part 3: Observe DNS Lookup Using the nslookup Command on Mail Servers

Background / Scenario

The Domain Name System (DNS) is invoked when you type a Uniform Resource Locator (URL), such as http://www.cisco.com, into a web browser. The first part of the URL describes which protocol is used. Common protocols are Hypertext Transfer Protocol (HTTP), Hypertext Transfer Protocol over Secure Socket Layer (HTTPS), and File Transfer Protocol (FTP).

DNS uses the second part of the URL, which in this example is www.cisco.com. DNS translates the domain name (www.cisco.com) to an IP address to allow the source host to reach the destination host. In this lab, you will observe DNS in action and use the **nslookup** (name server lookup) command to obtain additional DNS information. Work with a partner to complete this lab.

Required Resources

1 PC (Windows 7 or 8 with Internet and command prompt access)

Part 1: Observe the DNS Conversion of a URL to an IP Address

a. Click the **Windows Start** button, type **cmd** into the search field, and press Enter. The command prompt window appears.

b. At the command prompt, ping the URL for the Internet Corporation for Assigned Names and Numbers (ICANN) at **www.icann.org**. ICANN coordinates the DNS, IP addresses, top-level domain name system management, and root server system management functions. The computer must translate www.icann.org into an IP address to know where to send the Internet Control Message Protocol (ICMP) packets.

The first line of the output displays www.icann.org converted to an IP address by DNS. You should be able to see the effect of DNS, even if your institution has a firewall that prevents pinging, or if the destination server has prevented you from pinging its web server.

Note: If the domain name is resolved to an IPv6 address, use the command **ping -4 www.icann.org** to translate into an IPv4 address if desired.

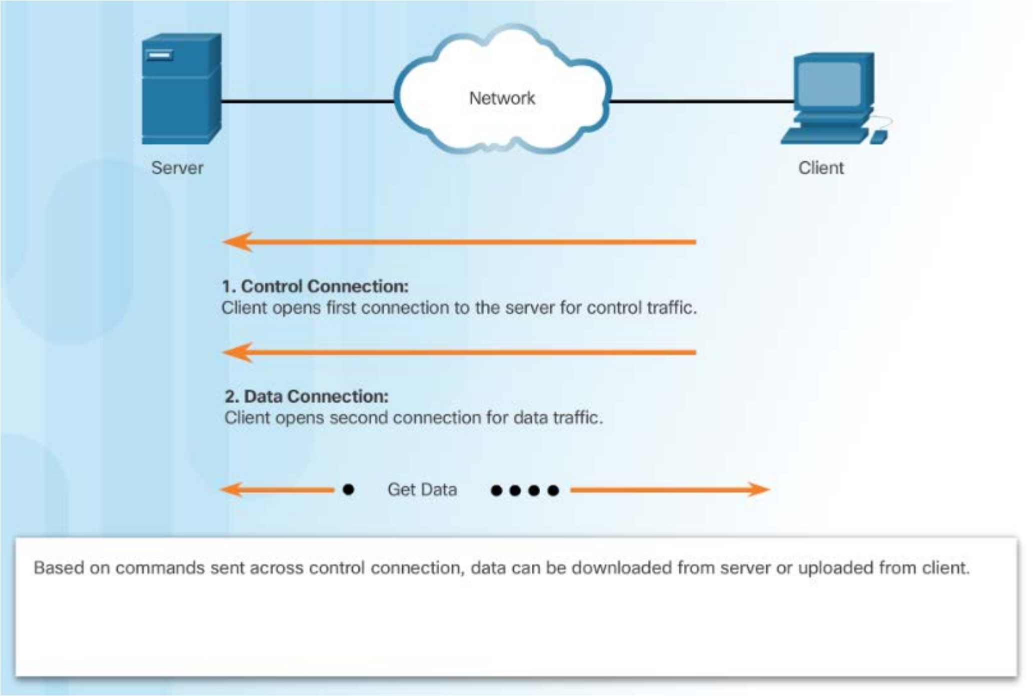
```
C:\>ping www.icann.org

Pinging www.vip.icann.org [192.0.32.7] with 32 bytes of data:
Reply from 192.0.32.7: bytes=32 time=23ms TTL=246
Reply from 192.0.32.7: bytes=32 time=23ms TTL=246
Reply from 192.0.32.7: bytes=32 time=24ms TTL=246
Reply from 192.0.32.7: bytes=32 time=28ms TTL=246

Ping statistics for 192.0.32.7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 23ms, Maximum = 28ms, Average = 24ms
```

Record the IP address of www.icann.org.

File Sharing Services

File Transfer Protocol

- FTP requires two connections between the client and the server, one for commands and replies, the other for the actual file transfer:
  - The client establishes the first connection to the server for control traffic using TCP port 21.
  - The client establishes the second connection to the server for the actual data transfer using TCP port 20.



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

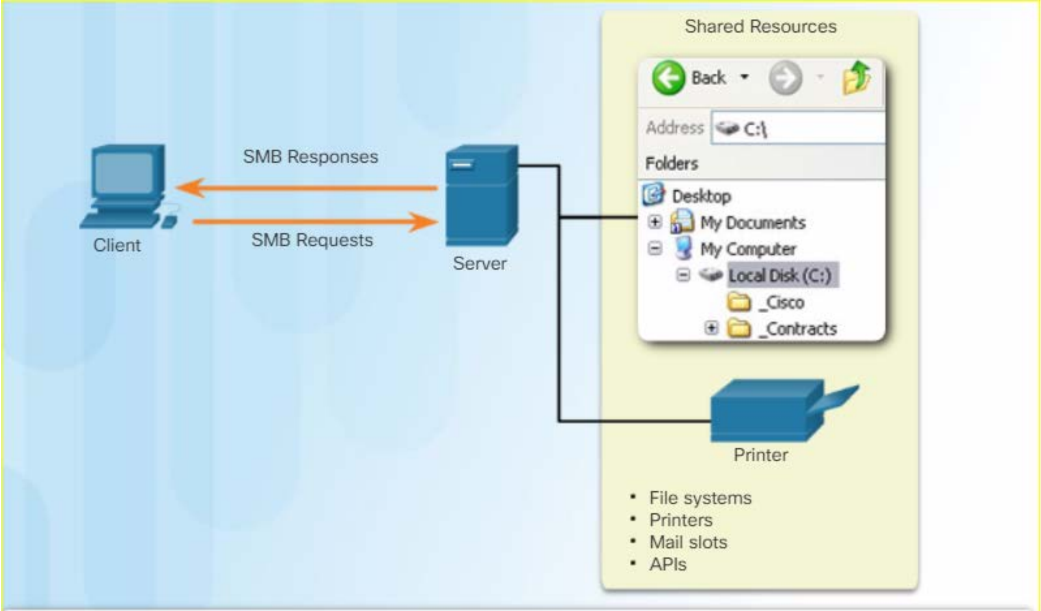
2. Data Connection:
Client opens second connection for data traffic.

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

File Sharing Services

Server Message Block

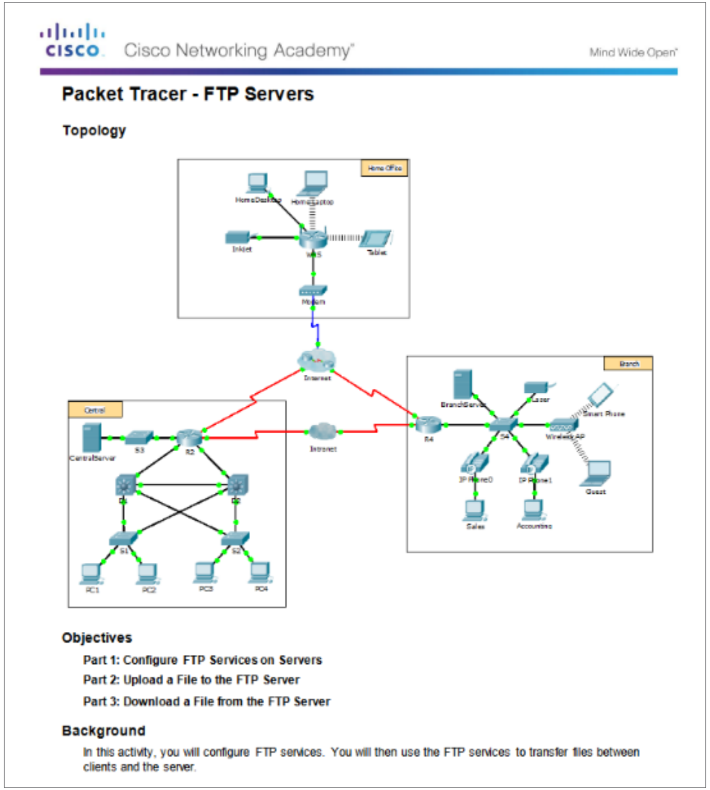
- The Server Message Block (SMB) is a client/server file sharing protocol:
  - SMB file-sharing and print services have become the mainstay of Microsoft networking.
  - Clients establish a long-term connection to servers and can access the resources on the server as if the resource is local to the client host.



SMB is a client-server, request-response protocol. Servers can make their resources available to clients on the network.

File Sharing Services

Packet Tracer - FTP



Cisco Networking Academy®

Mind Wide Open®

Packet Tracer - FTP Servers

Topology

Objectives

Part 1: Configure FTP Services on Servers

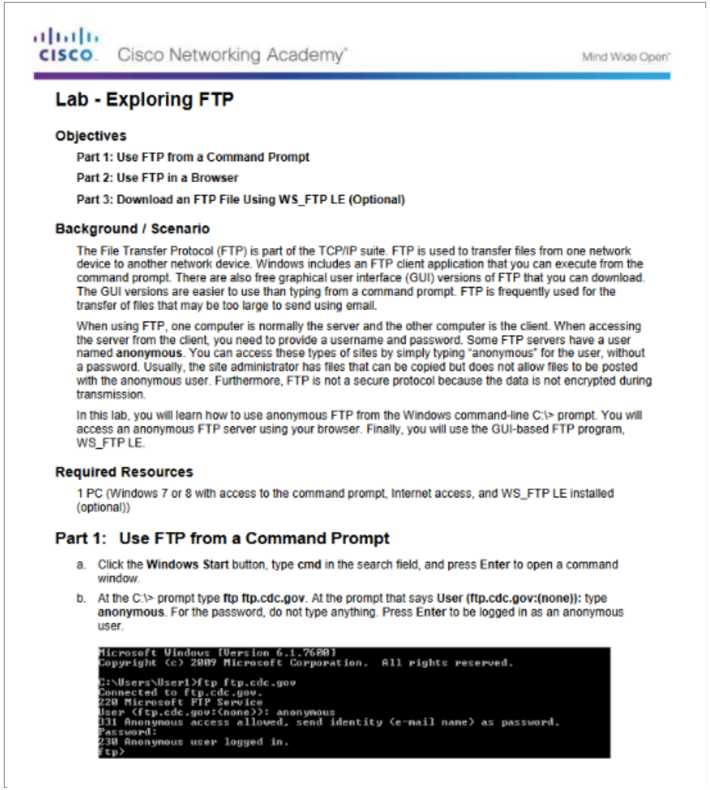
Part 2: Upload a File to the FTP Server

Part 3: Download a File from the FTP Server

Background

In this activity, you will configure FTP services. You will then use the FTP services to transfer files between clients and the server.

Lab – Exploring FTP



Cisco Networking Academy®

Mind Wide Open™

Lab - Exploring FTP

Objectives

Part 1: Use FTP from a Command Prompt

Part 2: Use FTP in a Browser

Part 3: Download an FTP File Using WS_FTP LE (Optional)

Background / Scenario

The File Transfer Protocol (FTP) is part of the TCP/IP suite. FTP is used to transfer files from one network device to another network device. Windows includes an FTP client application that you can execute from the command prompt. There are also free graphical user interface (GUI) versions of FTP that you can download. The GUI versions are easier to use than typing from a command prompt. FTP is frequently used for the transfer of files that may be too large to send using email.

When using FTP, one computer is normally the server and the other computer is the client. When accessing the server from the client, you need to provide a username and password. Some FTP servers have a user named **anonymous**. You can access these types of sites by simply typing "anonymous" for the user, without a password. Usually, the site administrator has files that can be copied but does not allow files to be posted with the anonymous user. Furthermore, FTP is not a secure protocol because the data is not encrypted during transmission.

In this lab, you will learn how to use anonymous FTP from the Windows command-line C:\> prompt. You will access an anonymous FTP server using your browser. Finally, you will use the GUI-based FTP program, WS_FTP LE.

Required Resources

1 PC (Windows 7 or 8 with access to the command prompt, Internet access, and WS_FTP LE installed (optional))

Part 1: Use FTP from a Command Prompt

a. Click the **Windows Start** button, type **cmd** in the search field, and press **Enter** to open a command window.

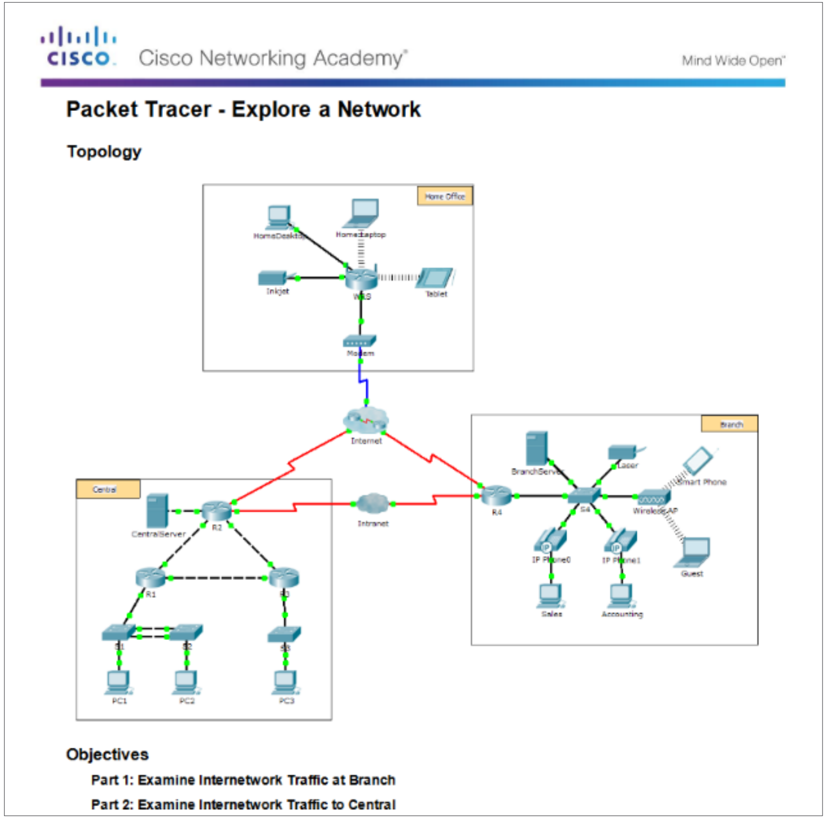
b. At the C:\> prompt type **ftp ftp.cdc.gov**. At the prompt that says **User (ftp.cdc.gov:(none)):** type **anonymous**. For the password, do not type anything. Press **Enter** to be logged in as an anonymous user.

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\User1>ftp ftp.cdc.gov
Connected to ftp.cdc.gov.
220 Microsoft FTP Service
User (ftp.cdc.gov:(none)): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 Anonymous user logged in.
ftp>
```

10.3 Summary

Conclusion

Packet Tracer - Explore a Network



Cisco Networking Academy®

Mind Wide Open™

Packet Tracer - Explore a Network

Topology

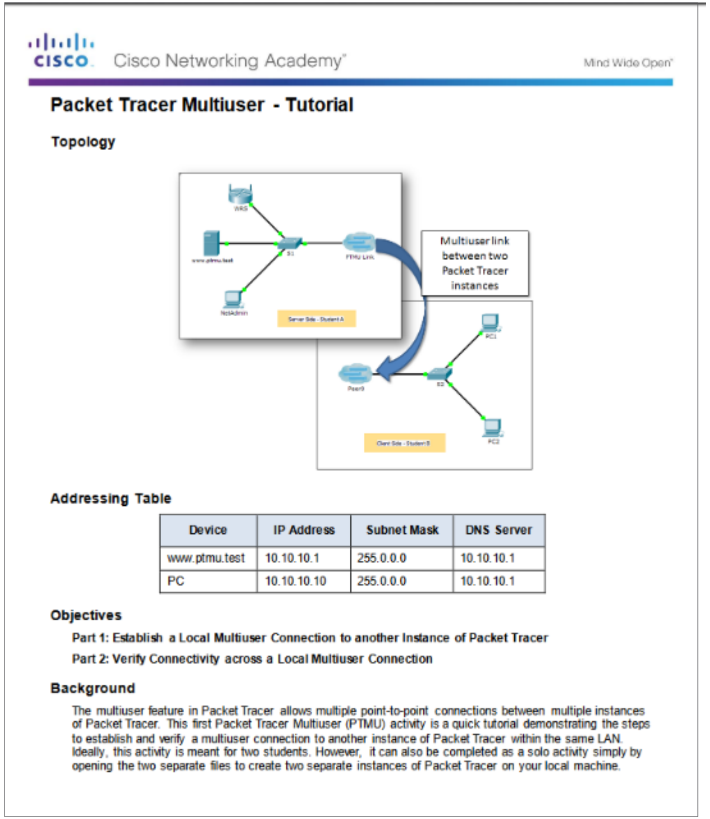
Objectives

Part 1: Examine Internetwork Traffic at Branch

Part 2: Examine Internetwork Traffic to Central

Conclusion

Packet Tracer - Multiuser - Tutorial



Cisco Networking Academy®

Mind Wide Open®

Packet Tracer Multiuser - Tutorial

Topology

Addressing Table

Device	IP Address	Subnet Mask	DNS Server
www.ptmu.test	10.10.10.1	255.0.0.0	10.10.10.1
PC	10.10.10.10	255.0.0.0	10.10.10.1

Objectives

Part 1: Establish a Local Multiuser Connection to another Instance of Packet Tracer

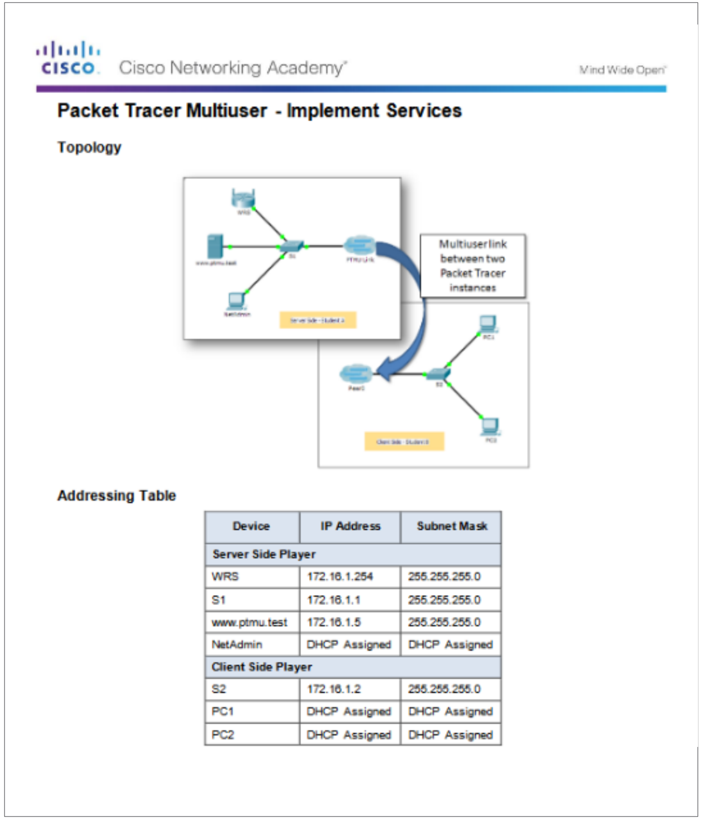
Part 2: Verify Connectivity across a Local Multiuser Connection

Background

The multiuser feature in Packet Tracer allows multiple point-to-point connections between multiple instances of Packet Tracer. This first Packet Tracer Multiuser (PTMU) activity is a quick tutorial demonstrating the steps to establish and verify a multiuser connection to another instance of Packet Tracer within the same LAN. Ideally, this activity is meant for two students. However, it can also be completed as a solo activity simply by opening the two separate files to create two separate instances of Packet Tracer on your local machine.

Conclusion

Packet Tracer Multiuser - Implement Services



Cisco Networking Academy®

Mind Wide Open®

Packet Tracer Multiuser - Implement Services

Topology

Addressing Table

Device	IP Address	Subnet Mask
Server Side Player		
WRS	172.16.1.254	255.255.255.0
S1	172.16.1.1	255.255.255.0
www.ptmu.test	172.16.1.5	255.255.255.0
NetAdmin	DHCP Assigned	DHCP Assigned
Client Side Player		
S2	172.16.1.2	255.255.255.0
PC1	DHCP Assigned	DHCP Assigned
PC2	DHCP Assigned	DHCP Assigned

Conclusion

Chapter 10: Application Layer

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

Chapter 10

New Terms and Commands

- Bootstrap Protocol (BOOTP)
- Simple Mail Transfer Protocol (SMTP)
- Post Office Protocol (POP)
- Internet Message Access Protocol (IMAP)
- File Transfer Protocol (FTP)
- Trivial File Transfer Protocol (TFTP)
- client-server
- Server Message Block (SMB)