CCNA Exploration Network Fundamentals

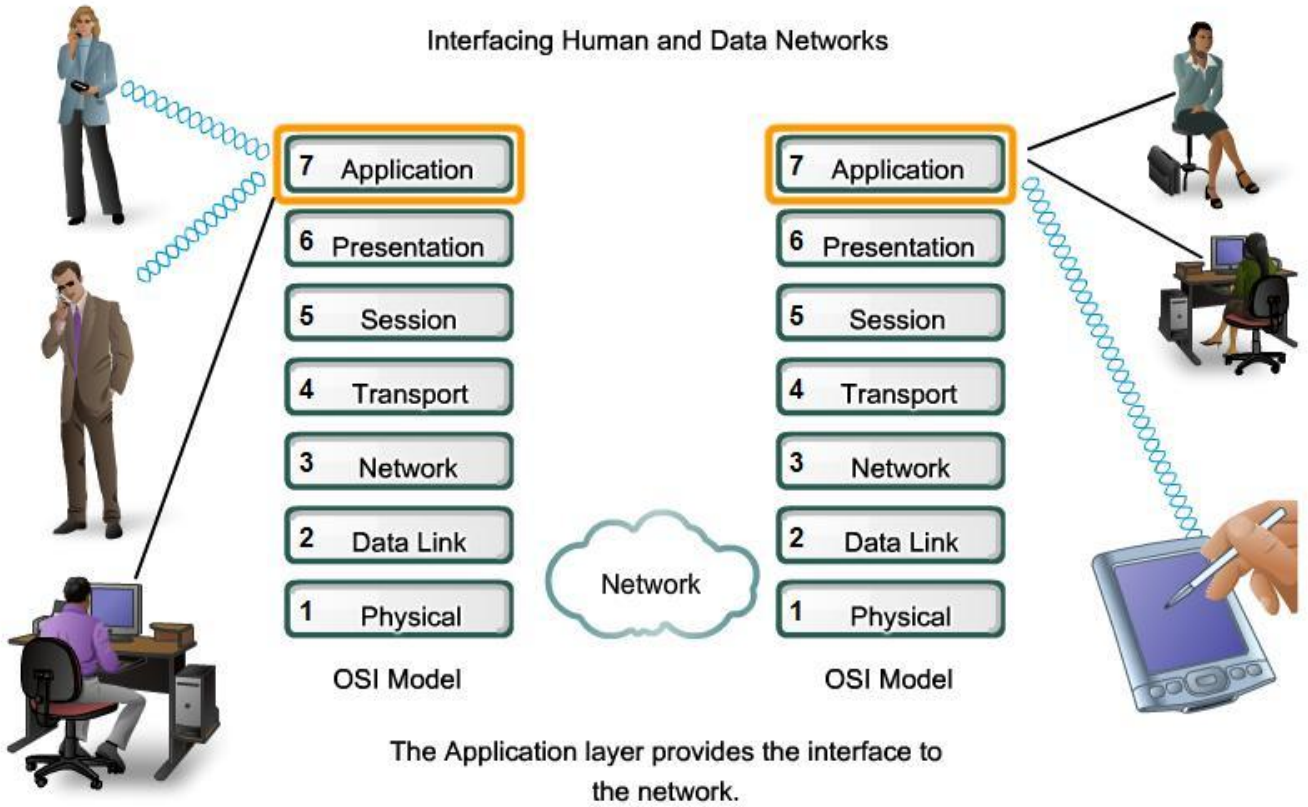
Chapter 03

Application Functionality and Protocols

Updated: 27/04/2008

3.1 Applications: The Interface Between Human and Networks

- Applications provide the means for generating and receiving data that can be transported on the network

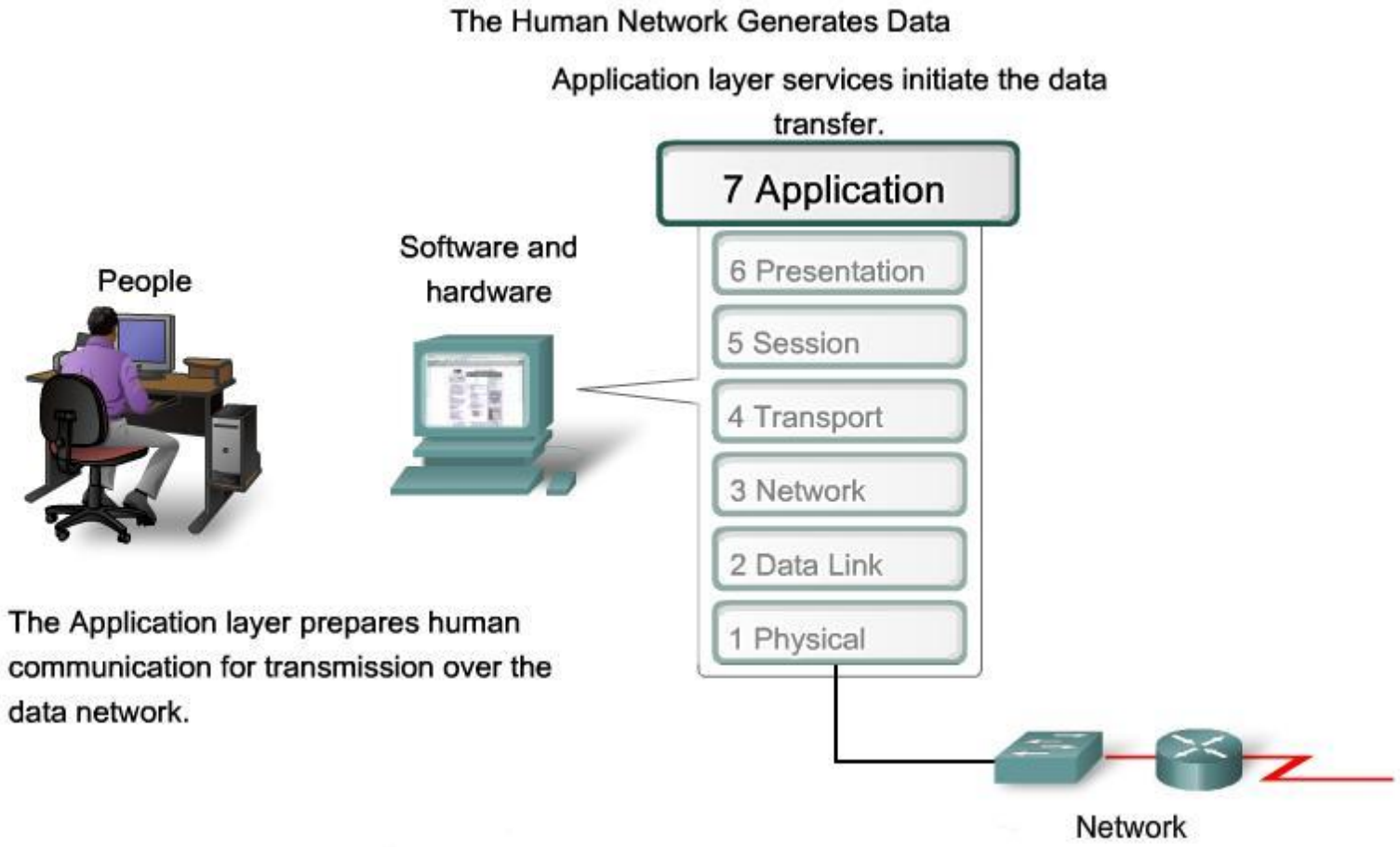


3.1.1 OSI and TCP/IP Model

- The Open Systems Interconnection reference model is a layered, abstract representation created as a guideline for network protocol design.
- The OSI model divides the networking process into seven logical layers, each of which has unique functionality and to which are assigned specific services and protocols.
- The Application layer, Layer seven, is the top layer of both the OSI and TCP/IP models.
- It is the layer that provides the interface between the applications we use to communicate and the underlying network over which our messages are transmitted.
- Application layer protocols are used to exchange data between programs running on the source and destination hosts.
- There are many Application layer protocols and new protocols are always being developed.

3.1.1 OSI and TCP/IP Model

- Applications, services and protocols convert communication to data that can be transferred across the data network



3.1.1 OSI and TCP/IP Model

- The Presentation layer has three primary functions:
  - Coding and conversion of Application layer data to ensure that data from the source device can be interpreted by the appropriate application on the destination device.
  - Compression of the data in a manner that can be decompressed by the destination device.
  - Encryption of the data for transmission and the decryption of data upon receipt by the destination.
- Some well-known standards for video include QuickTime and Motion Picture Experts Group (MPEG). QuickTime is an Apple Computer specification for video and audio, and MPEG is a standard for video compression and coding.
- Among the well-known graphic image formats are Graphics Interchange Format (GIF), Joint Photographic Experts Group (JPEG), and Tagged Image File Format (TIFF). GIF and JPEG are compression and coding standards for graphic images, and TIFF is a standard coding format for graphic images.

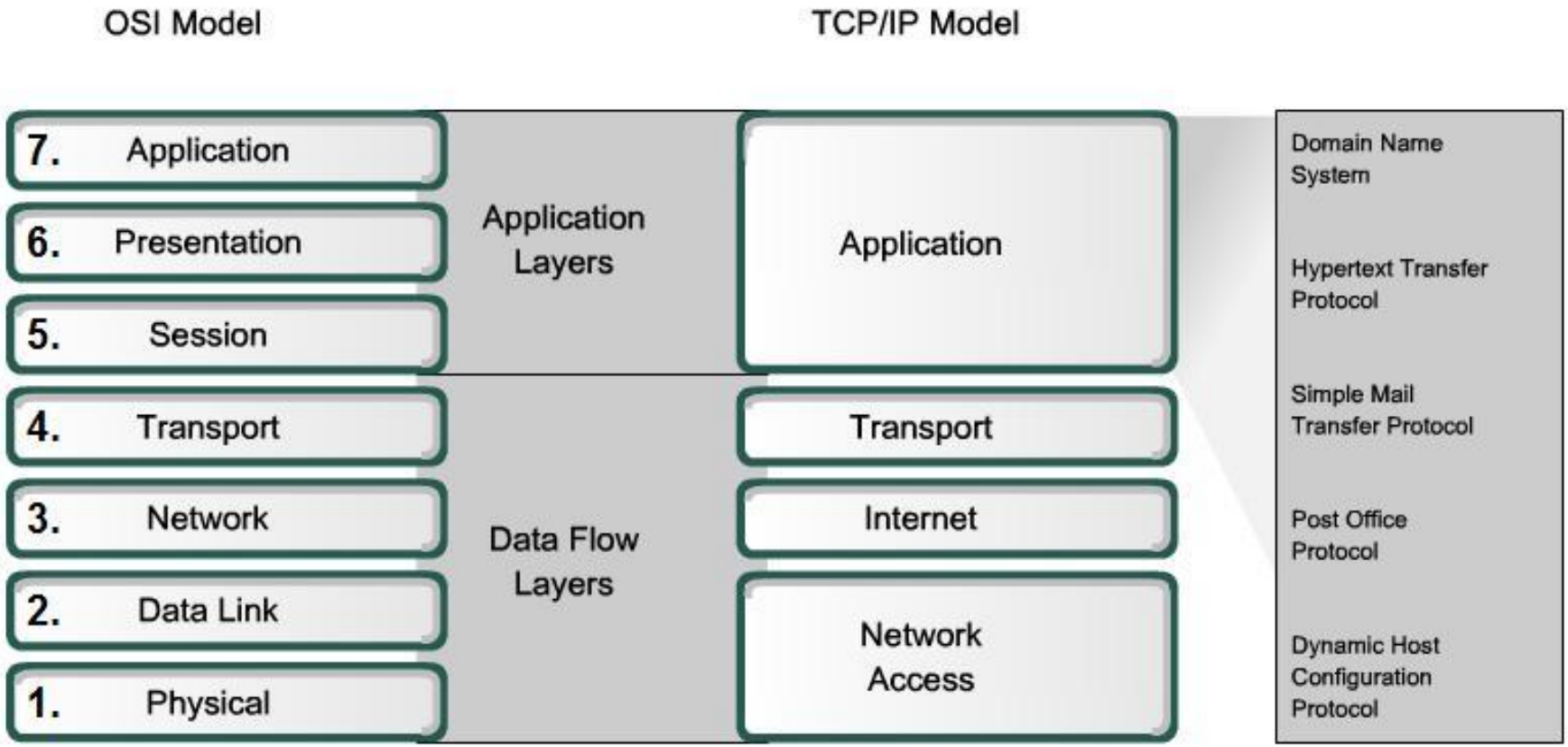
3.1.1 OSI and TCP/IP Model

- Session layer
  - Session layer create and maintain 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 for a long period of time.

- Most applications, like web browsers or e-mail clients, incorporate functionality of the OSI layers 5, 6 and 7.

3.1.1 OSI and TCP/IP Model

- The separate roles applications, services and protocols play in transporting data through networks



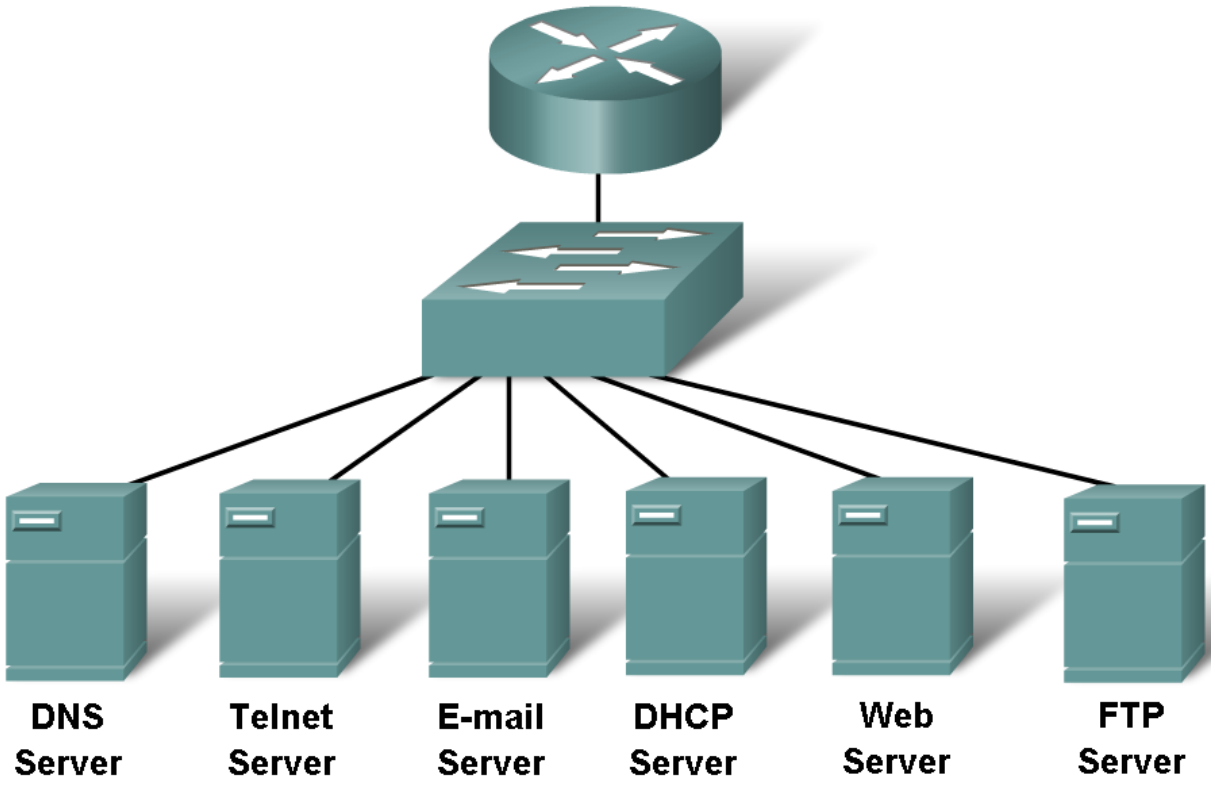
3.1.1 OSI and TCP/IP Model

- The most widely-known TCP/IP Application layer protocols are those that provide for the exchange of user information. These protocols specify the format and control information necessary for many of the common Internet communication functions. Among these TCP/IP protocols are:
  - Domain Name Service Protocol (DNS) is used to resolve Internet names to IP addresses.
  - Hypertext Transfer Protocol (HTTP) is used to transfer files that make up the Web pages of the World Wide Web.
  - Simple Mail Transfer Protocol (SMTP) is used for the transfer of mail messages and attachments.
  - Telnet, a terminal emulation protocol, is used to provide remote access to servers and networking devices.
  - File Transfer Protocol (FTP) is used for interactive file transfer between systems.

- The protocols in the TCP/IP suite are generally defined by Requests for Comments (RFCs). The Internet Engineering Task Force maintains the RFCs as the standards for the TCP/IP suite.

3.1.1 OSI and TCP/IP Model

- Role protocols play in networking.



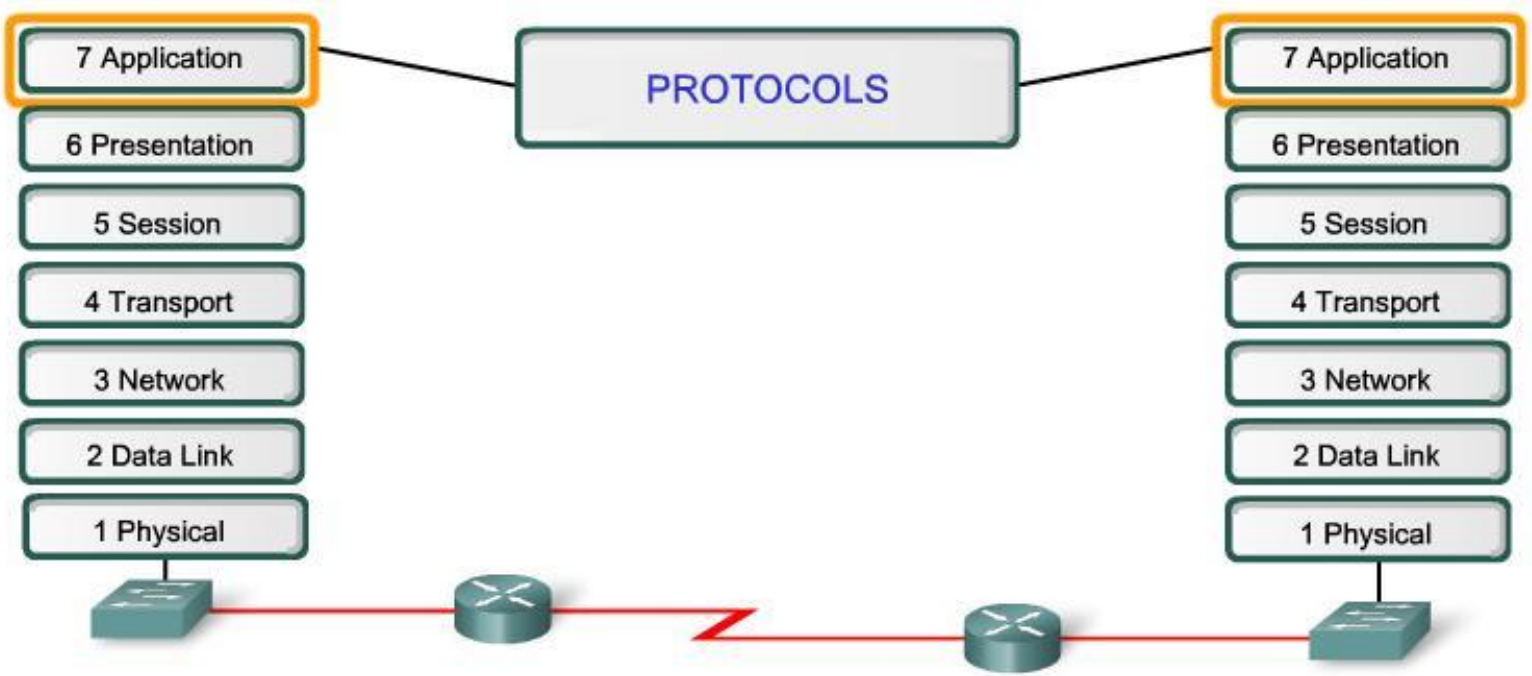
3.1.2 Application Layer Software

- Processes are individual software programs running concurrently. Processes can be: Applications, Services, System operations. One program can be running several times, each in its own process.
- Within the Application layer, there are two forms of software programs or processes that provide access to the network:
  - Network Aware Applications: Applications that implement the application layer protocols and are able to communicate directly with the lower layers of the protocol stack. E-mail clients and web browsers are examples of these types of applications.
  - Application layer Services: provide assistance to other programs to use network resources, like file transfer or network print spooling.

3.1.3 User Applications, Services and Application Layer Protocols

- Application layer uses protocols that are implemented within applications and services.
- While applications provide people with a way to create messages and application layer services establish an interface to the network, protocols provide the rules and formats that govern how data is treated.
- In the OSI model, applications that interact directly with people are considered to be at the top of the stack, as are the people themselves.
- Like all layers within the OSI model, the Application layer relies on the functions of the lower layers in order to complete the communication process.
- Within the Application layer, protocols specify what messages are exchanged between the source and destination hosts, the syntax of the control commands, the type and format of the data being transmitted, and the appropriate methods for error notification and recovery.

3.1.4 Application Layer Protocol Functions



Application layer protocols provide the rules for communication between applications.

Protocols:

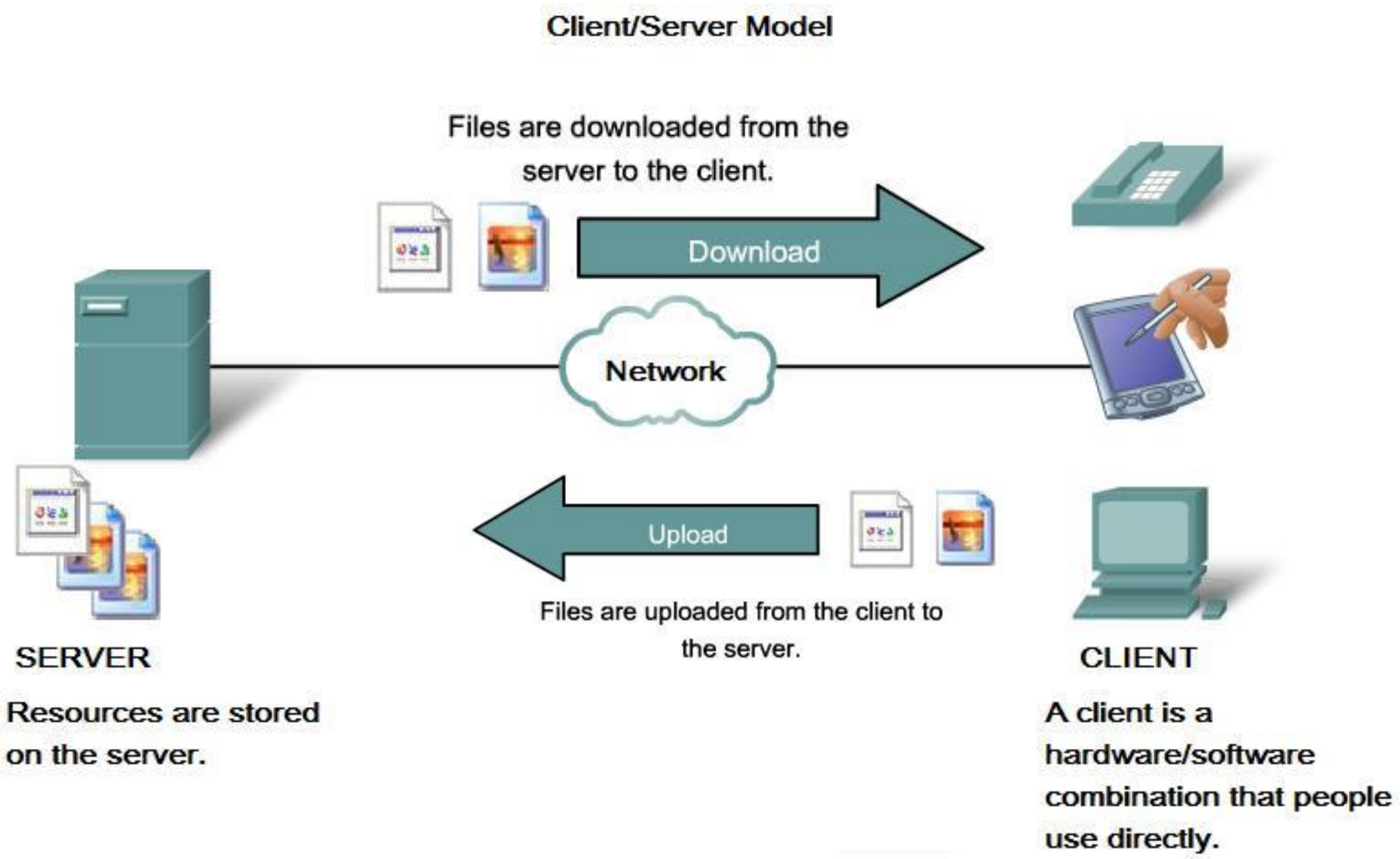
Define processes on either end of the communication
Define the types of messages
Define the syntax of messages
Define the meaning of any informational fields
Define how messages are sent and the expected response
Define interaction with the next lower layer

3.2 Making Provisions for Applications and Services

3.2.1 The Client-Server Model

- 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.
- Client and server processes are considered to be in the Application layer.
- The client begins the exchange by requesting data from the server, which 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.
- In addition to the actual data transfer, this exchange may also require control information, such as user authentication and the identification of a data file to be transferred.

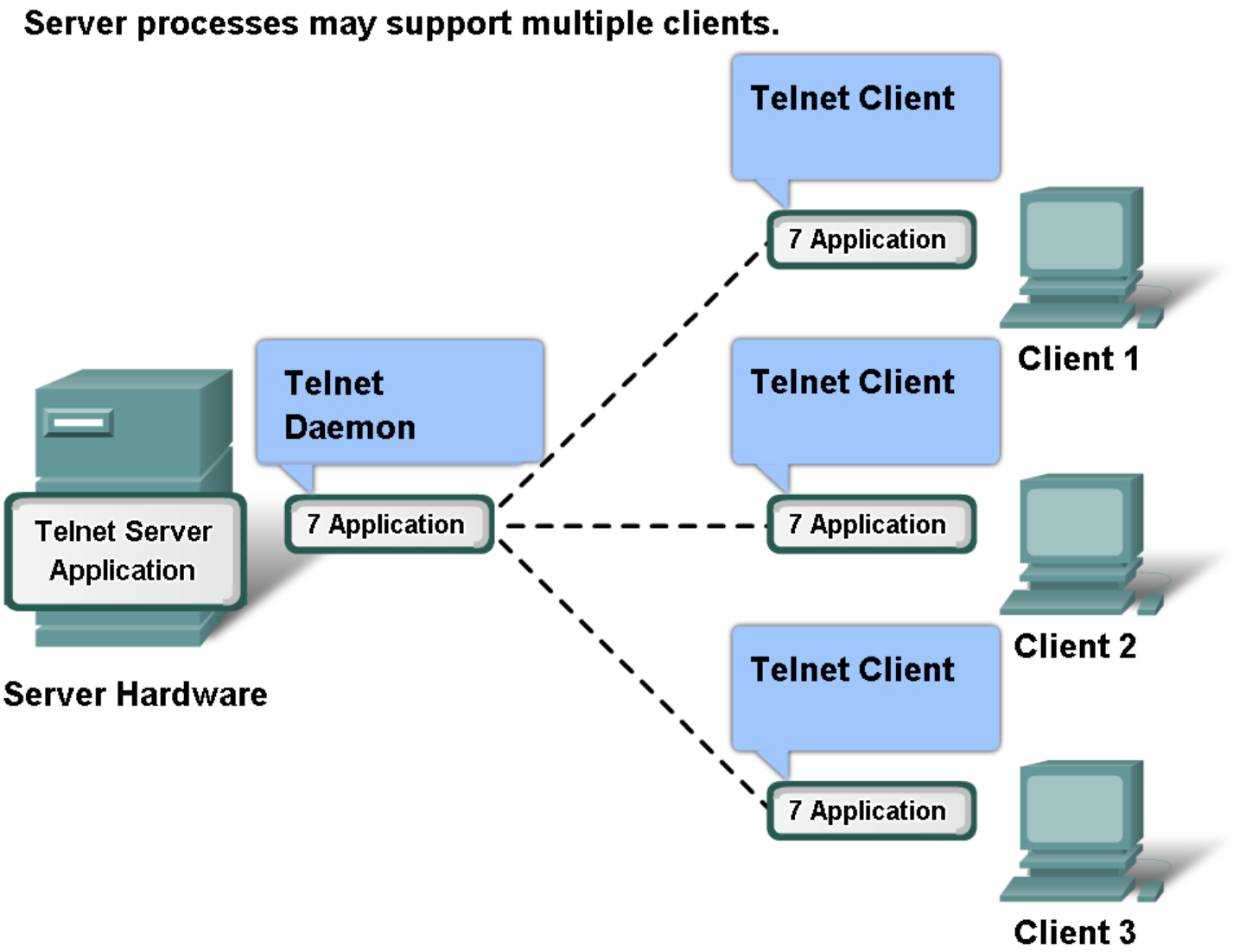
3.2.1 The Client-Server Model



3.2.2 Servers

- Servers are depositories of information. Processes control the delivery of files to clients.
- In a general networking context, any device that responds to requests from client applications is functioning as a server. A server is usually a computer that contains information to be shared with many client systems. For example, web pages, documents, databases, pictures, video, and audio files can all be stored on a server and delivered to requesting clients.
- In other cases, such as a network printer, the print server delivers the client print requests to the specified printer.
- In a client/server network, the server runs a service, or process in the background.

3.2.3 Application Layer Services and Protocols

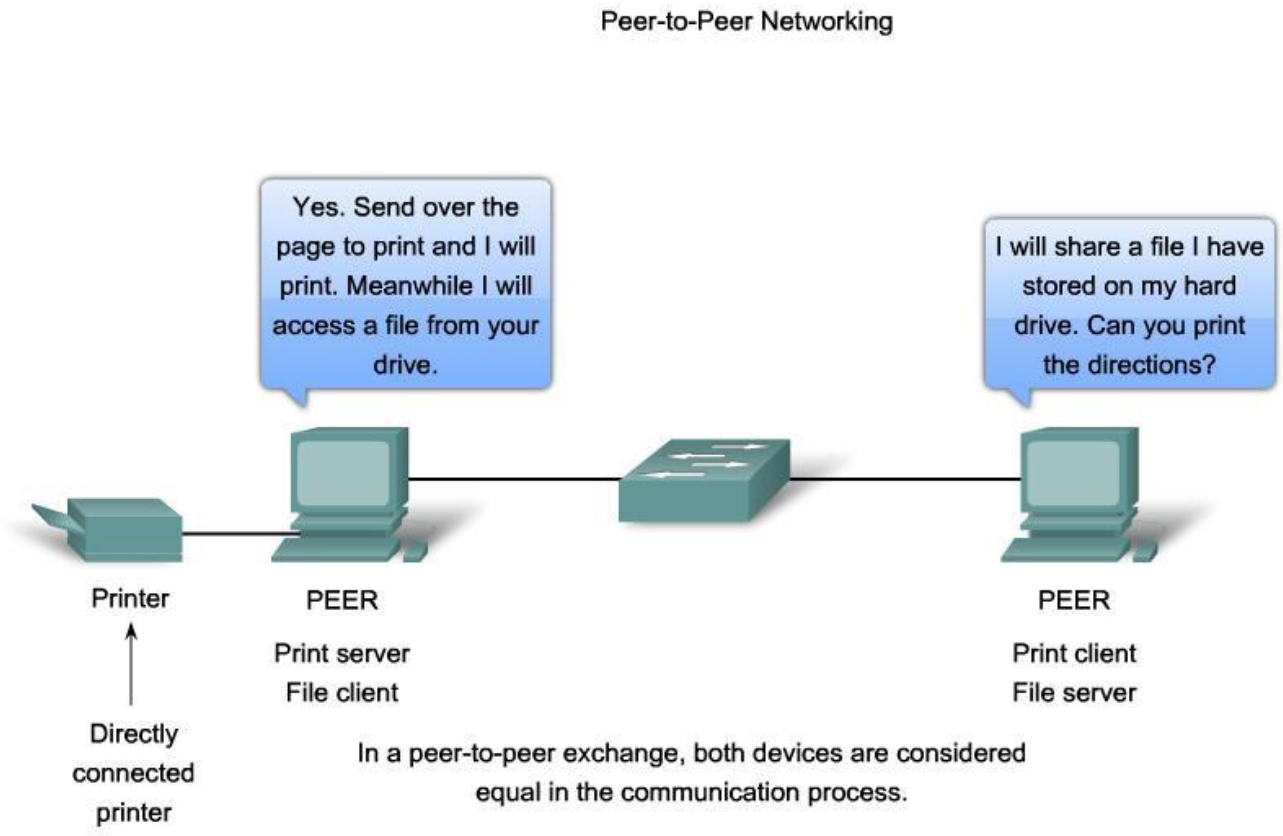


3.2.4 Peer-to-Peer Networking & Applications (P2P)

- Peer-to-peer model involves two distinct forms:
  - peer-to-peer network design and
  - peer-to-peer applications (P2P).
- Both forms have similar features but in practice work very differently.
- In a peer-to-peer network, two or more computers are connected via a network and can share resources (such as printers and files) without having a dedicated server.
- Every connected end device (known as a peer) can function as either a server or 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.

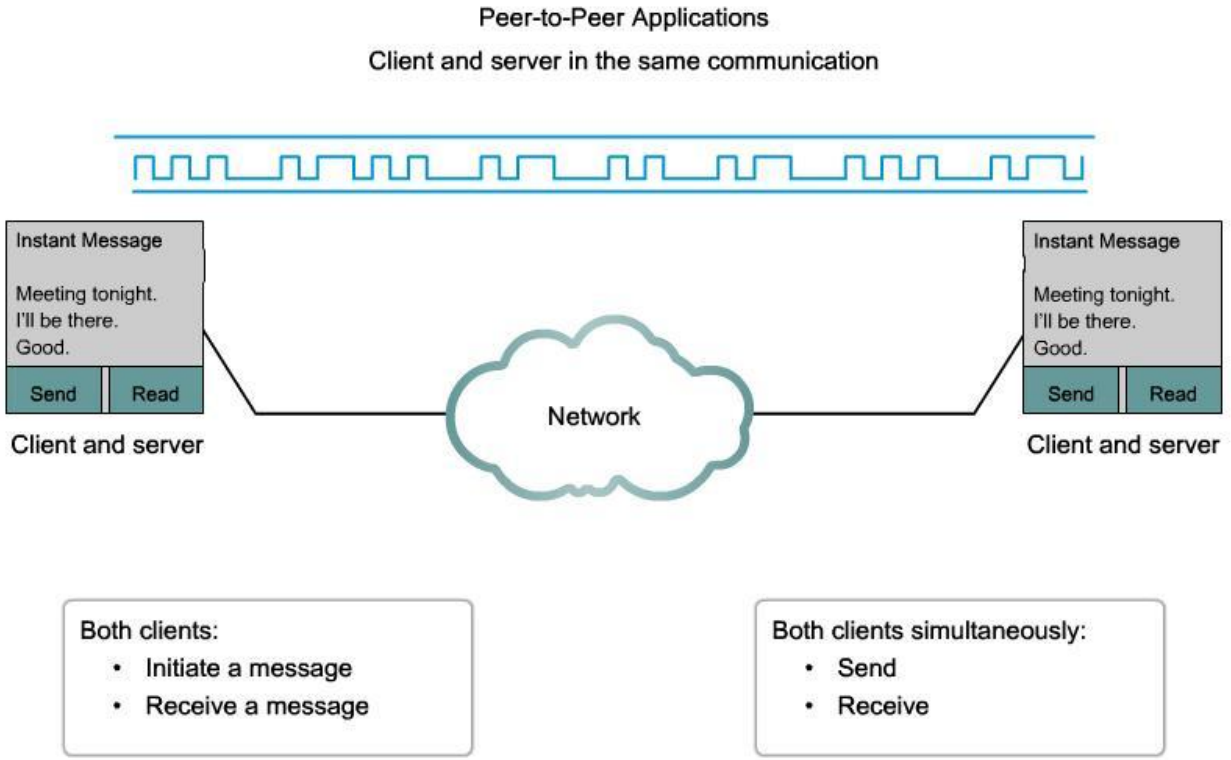
3.2.4 Peer-to-Peer Networking & Applications (P2P)

- Because peer-to-peer networks usually do not use centralized user accounts, permissions, or monitors, it is difficult to enforce security and access policies in networks containing more than just a few computers. User accounts and access rights must be set individually on each peer device.



3.2.4 Peer-to-Peer Networking & Applications (P2P)

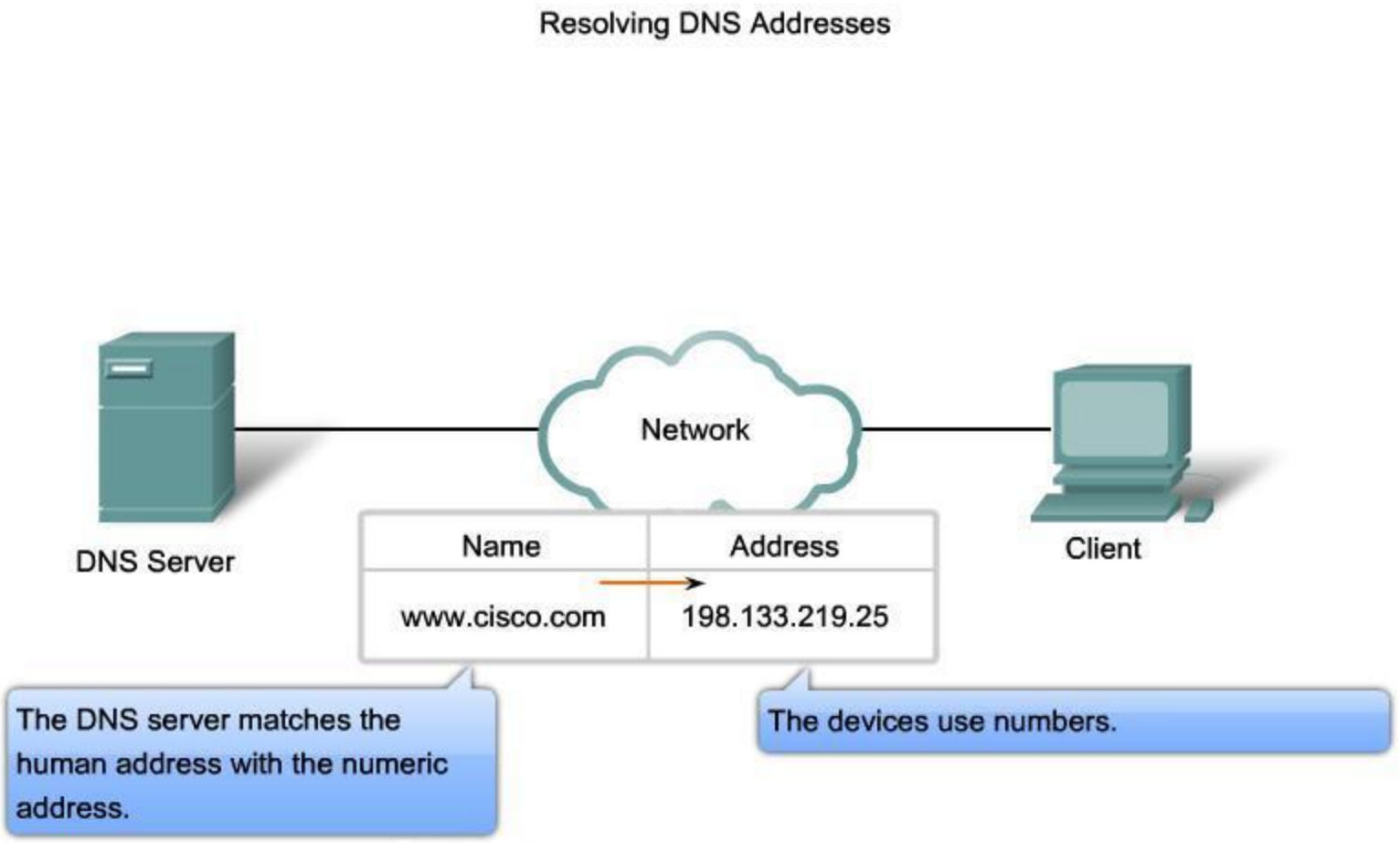
- A peer-to-peer application (P2P), unlike a peer-to-peer network, allows a device to act as both a client and a server within the same communication.
- In this model, every client is a server and every server a client. Both can initiate a communication and are considered equal in the communication process. However, peer-to-peer applications require that each end device provide a user interface and run a background service. After that the devices can communicate directly.



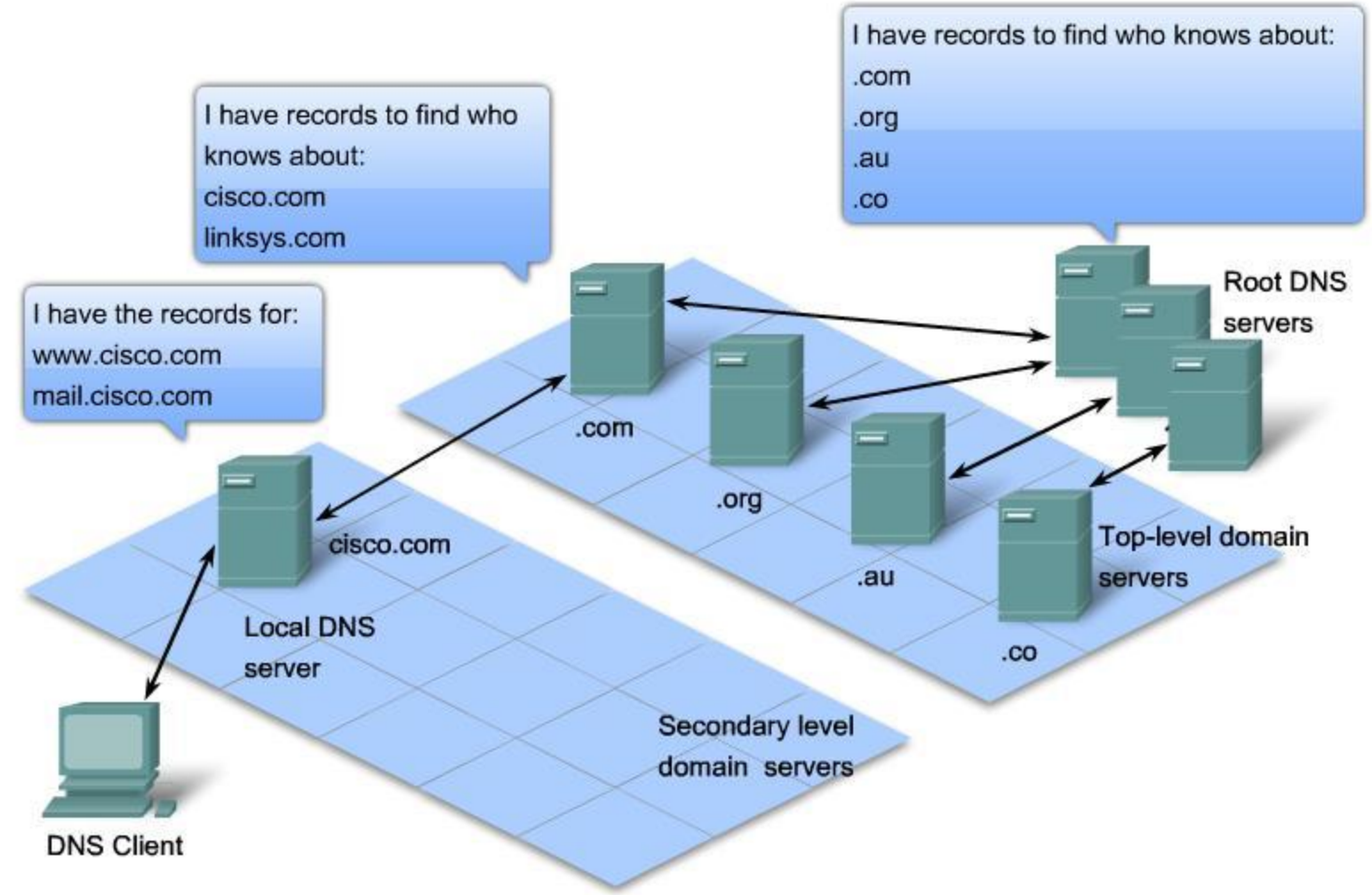
3.3 Application Layer Protocols & Services Examples

- The Transport layer uses an addressing scheme called a port number.
- Port numbers identify applications and Application layer services that are the source and destination of data.
- Server programs generally use predefined port numbers that are commonly known by clients.TCP and UDP port numbers normally associated with these services. Some of these services are:
  - 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 Port 67
  - File Transfer Protocol (FTP) - TCP Ports 20 and 21

3.3.1 DNS Services and Protocols



3.3.1 DNS Services and Protocols



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

3.3.1 DNS Services and Protocols

- In data networks, devices are labeled with numeric IP addresses, so that they can participate in sending and receiving messages over the network.
- Domain names were created to convert the numeric address into a simple, recognizable name (e.g. 198.133.219.25 - www.cisco.com) .
- Any new address will simply be linked to the existing domain name and connectivity is maintained.
- As networks began to grow and the number of devices increased, the manual system to maintain mapping between domain names and their IP addresses became unworkable.
- The Domain Name System (DNS) was created for domain name to address resolution for these networks. DNS uses a distributed set of servers to resolve the names associated with these numbered addresses.
- 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 formats. DNS protocol communications use a single format called a message. This message format is used for all types of client queries and server responses, error messages, and the transfer of resource record information between servers.

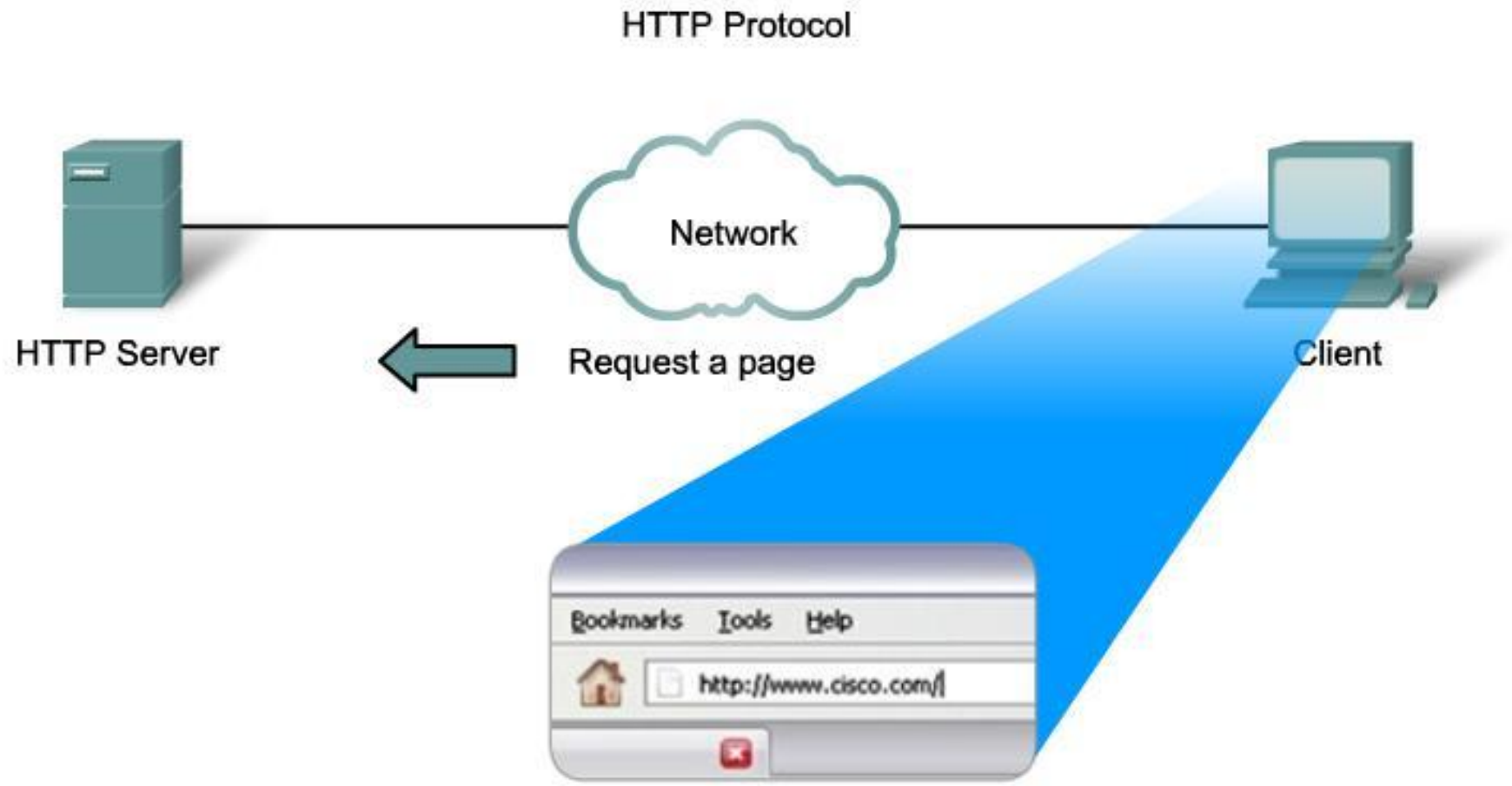
3.3.1 DNS Services and Protocols

- When configuring a network device, we generally provide one or more DNS Server addresses that the DNS client can use for name resolution.
- Usually the Internet service provider provides the addresses to use for the DNS servers.
- When a user's application requests to connect to a remote device by name, the requesting DNS client queries one of these name servers to resolve the name to a numeric address.
- Computer operating systems also have a utility called “nslookup” that allows the user to manually query the name servers 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.
- A DNS server provides the name resolution using the name daemon, which is often called named, (pronounced name-dee)

3.3.1 DNS Services and Protocols

- The DNS server stores different types of resource records used to resolve names. These records contain the name, address, and type of record. Some of these record types are:
  - A - an end device address
  - NS - an authoritative name server
  - CNAME - the canonical name (or Fully Qualified Domain Name) for an alias; used when multiple services have the single network address but each service has its own entry in DNS
  - MX - mail exchange record; maps a domain name to a list of mail exchange servers for that domain
- When a client makes a query, the server's "named" process first looks at its own records to see if it can resolve the name. If it is unable to resolve the name using its stored records, it contacts other servers in order to resolve the name.
- The request may be passed along to a number of servers, which can take extra time and consume bandwidth. Once a match is found and returned to the original requesting server, the server temporarily stores the numbered address that matches the name in cache.
- The ipconfig /displaydns command displays all of the cached DNS entries on a Windows XP or 2000 computer system.

3.3.2 WWW Service and HTTP



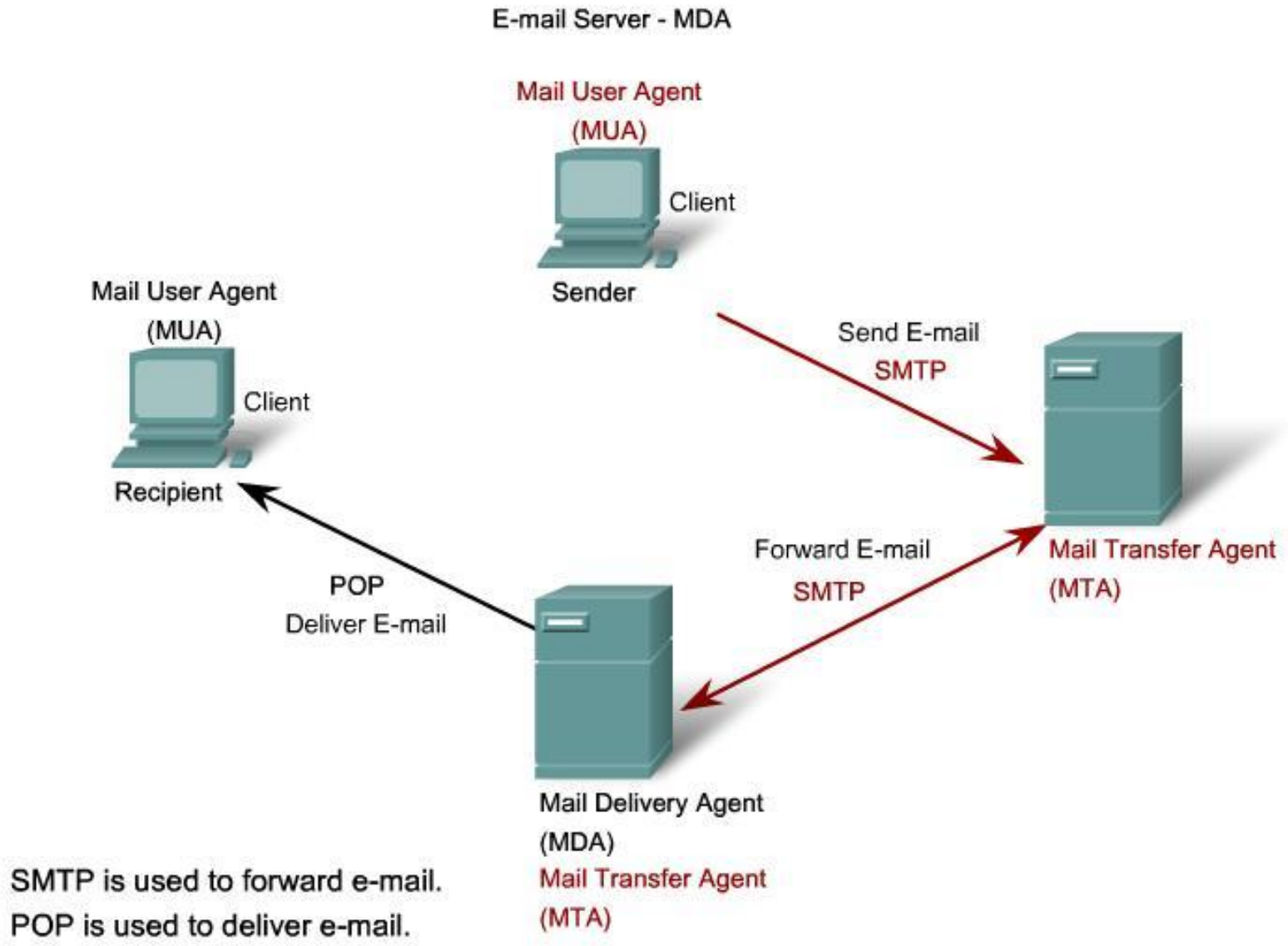
3.3.2 WWW Service and HTTP

- When a web address (or 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. URLs (or Uniform Resource Locator) and URIs (Uniform Resource Identifier) are the names most people associate with web addresses.
- For example, URL: http://www.cisco.com/web-server.htm.
- First, the browser interprets the three parts of the URL:
  1. http (the protocol or scheme)
  2. www.cisco.com (the server name)
  3. web-server.htm (the specific file name requested).
- The browser then checks with a name server to convert www.cisco.com into a numeric address, which it uses to connect to the server.
- Using the HTTP protocol requirements, the browser sends a GET request to the server and asks for the file web-server.htm. The server in turn sends the HTML code for this web page to the browser.
- Finally, the browser deciphers the HTML code and formats the page for the browser window.

3.3.2 WWW Service and HTTP

- HTTP specifies a request/response protocol.
- The three common message types are GET, POST, and PUT.
- GET is a client request for data.
- POST and PUT are used to send messages that upload data to the web server.
- When the user enters data into a form embedded in a web page, POST includes the data in the message sent to the server.
- PUT uploads resources or content to the web server.
- HTTP is not a secure protocol. The POST messages upload information to the server in plain text that can be intercepted and read. Similarly, the server responses, typically HTML pages, are also unencrypted.
- For secure communication across the Internet, the HTTP Secure (HTTPS) protocol is used for accessing or posting web server information. HTTPS can use authentication and encryption to secure data as it travels between the client and server.

3.2.3 E-mail Services and SMTP/POP Protocols



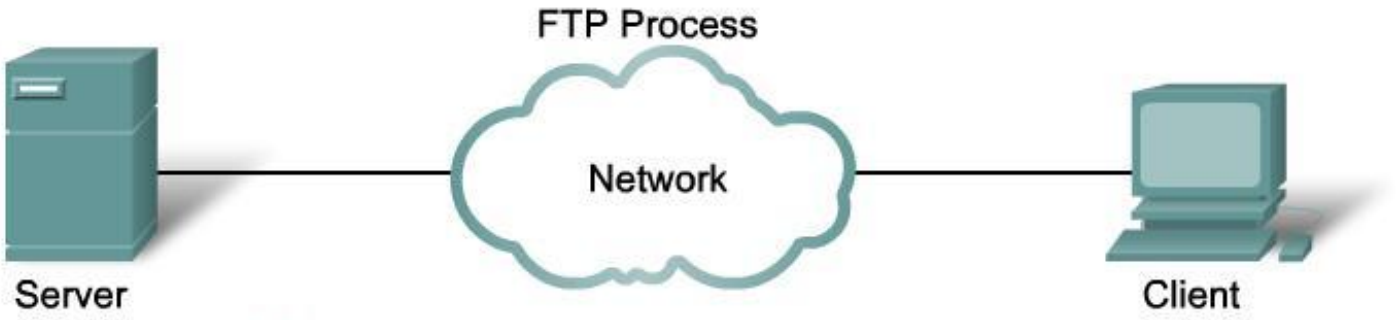
3.2.3 E-mail Services and SMTP/POP Protocols

- e-mail requires several applications and services. Examples: Application layer protocols are Post Office Protocol (POP) and Simple Mail Transfer Protocol (SMTP).
- When people compose e-mail messages, they typically use an application called a Mail User Agent (MUA), or e-mail client. The MUA allows messages to be sent and places received messages into the client's mailbox, both of which are distinct processes.
- In order to receive e-mail messages from an e-mail server, the e-mail client can use POP. Sending e-mail from either a client or a server uses message formats and command strings defined by the SMTP protocol. Usually an e-mail client provides the functionality of both protocols within one application.
- The e-mail server operates two separate processes:
  - Mail Transfer Agent (MTA)
  - Mail Delivery Agent (MDA)

3.2.3 E-mail Services and SMTP/POP Protocols

- The Mail Transfer Agent (MTA) process is used to forward e-mail.
- The MTA receives messages from the MUA or from another MTA on another e-mail server.
- Based on the message header, it determines how a message has to be forwarded to reach its destination.
- If the mail is addressed to a user whose mailbox is on the local server, the mail is passed to the MDA. If the mail is for a user not on the local server, the MTA routes the e-mail to the MTA on the
- The MDA receives all the inbound mail from the MTA and places it into the appropriate users' mailboxes.
- The MDA can also resolve final delivery issues, such as virus scanning, spam filtering, and return-receipt handling.
- Most e-mail communications use the MUA, MTA, and MDA applications.

3.2.4 FTP



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

Data Connection:
Client opens second connection for data traffic.

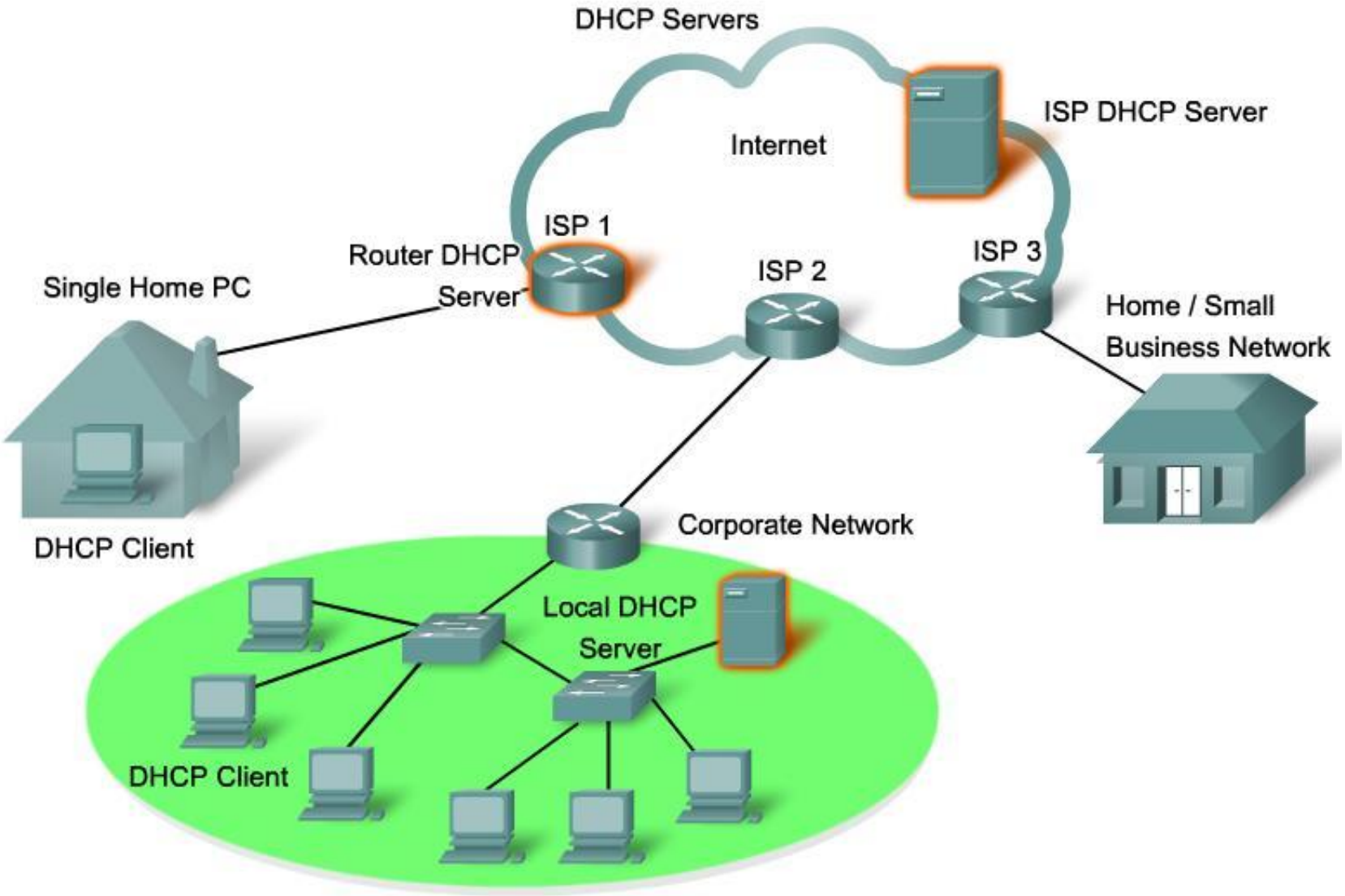
Get Data

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

3.2.4 FTP

- An FTP client is an application that runs on a computer that is used to push and pull files from a server running the FTP daemon (FTPd).
- 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 on TCP port 21. This connection is used for control traffic, consisting of client commands and server replies.
- The client establishes the second connection to the server over TCP port 20. This connection is for the actual file transfer and is created every time there is a file transferred.
- The file transfer can happen in either direction. The client can download (pull) a file from the server or, the client can upload (push) a file to the server.

3.3.5 DHCP

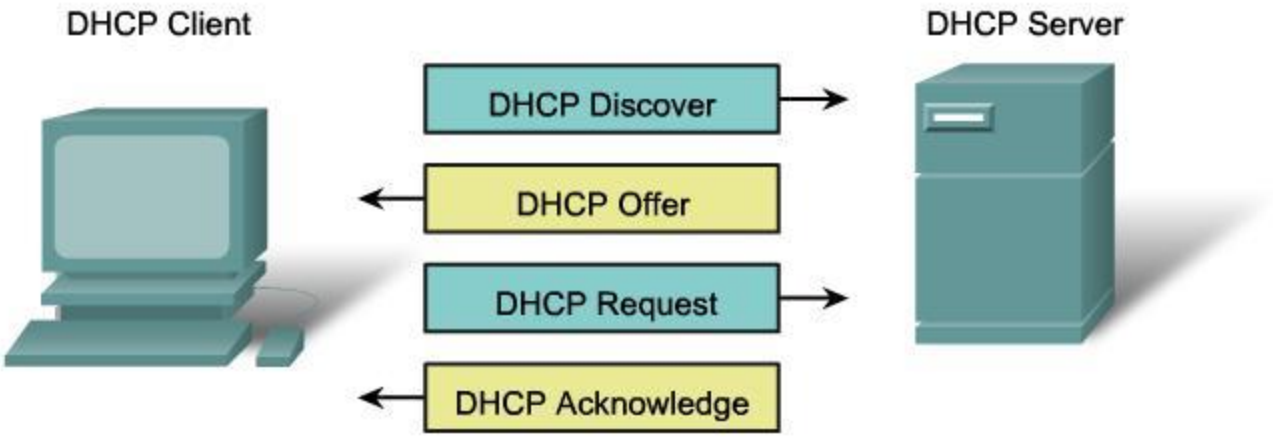

DHCP Servers
Internet
ISP DHCP Server
ISP 1
Router DHCP
Server
ISP 2
ISP 3
Single Home PC
Home / Small
Business Network
DHCP Client
Corporate Network
Local DHCP
Server
DHCP Client

3.3.5 DHCP

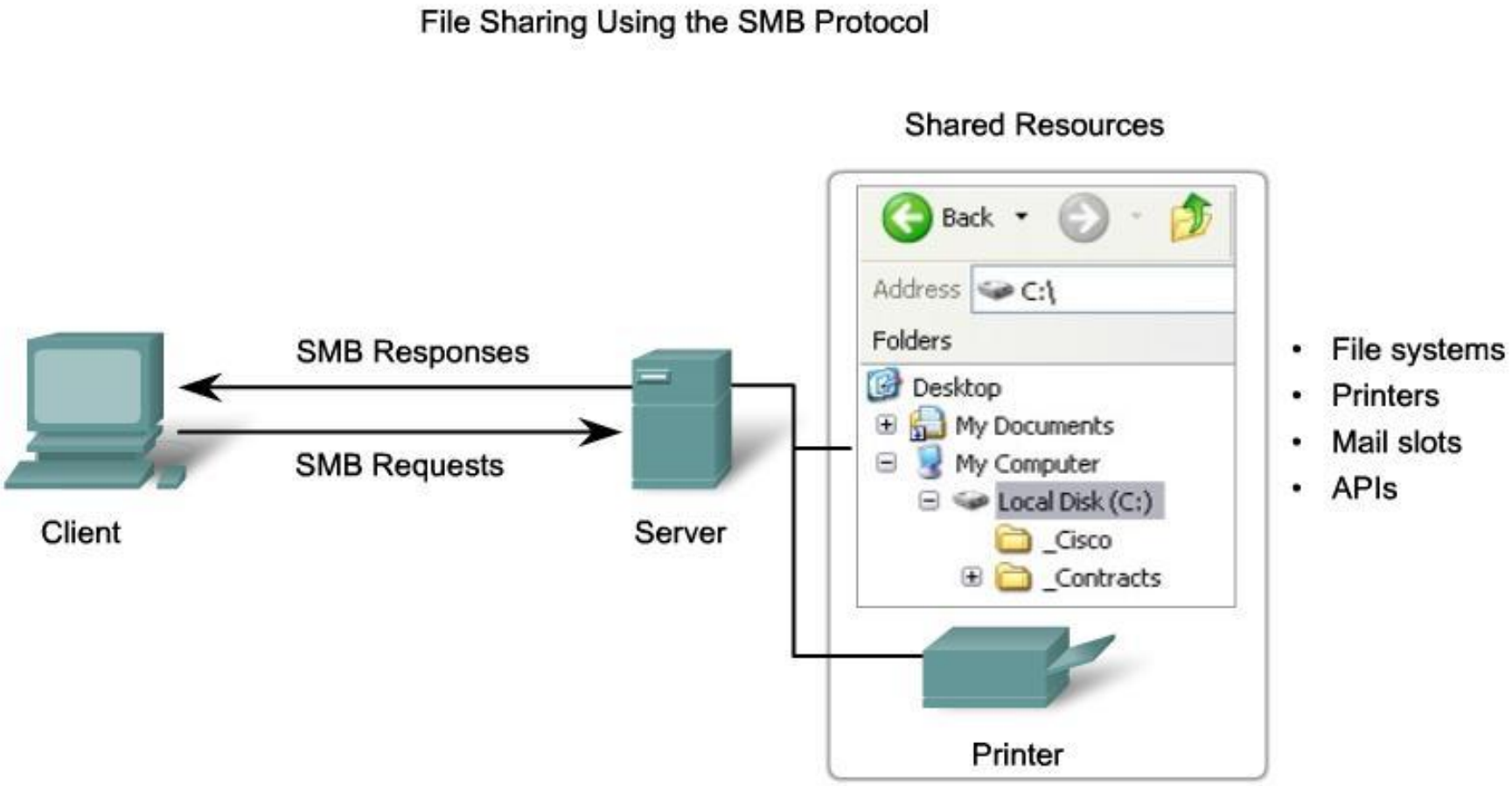
- The Dynamic Host Configuration Protocol (DHCP) service enables devices on a network to obtain IP addresses and other information from a DHCP server. This service automates the assignment of IP addresses, subnet masks, gateway and other IP networking parameters.
- DHCP allows a host to obtain an IP address dynamically when it connects to the network. The DHCP server is contacted and an address requested. The DHCP server chooses an address from a configured range of addresses called a pool and assigns ("leases") it to the host for a set period.
- On larger local networks, or where the user population changes frequently, DHCP is preferred.
- Various types of devices can be DHCP servers when running DHCP service software.
- The DHCP server in most medium to large networks is usually a local dedicated PC-based server.
- With home networks the DHCP server is usually located at the ISP and a host on the home network receives its IP configuration directly from the ISP.

3.3.5 DHCP

- DHCP can pose a security risk because any device connected to the network can receive an address. This risk makes physical security an important factor when determining whether to use dynamic or manual addressing.
- Dynamic and static addressing both have their places in network designs. Many networks use both DHCP and static addressing. DHCP is used for general purpose hosts such as end user devices, and fixed addresses are used for network devices such as gateways, switches, servers and printers.



3.3.6 File Sharing Services and SMB Protocol



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

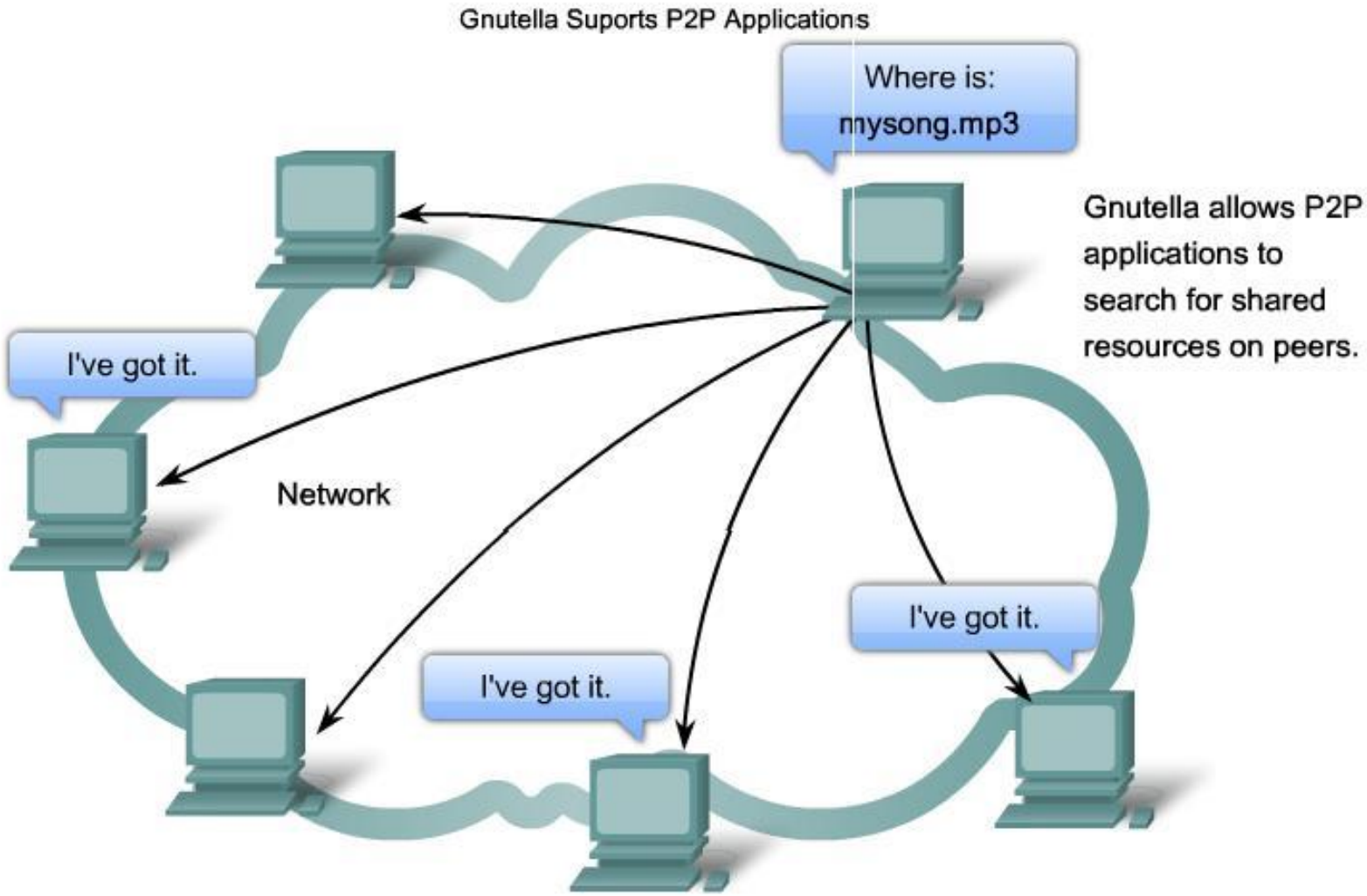
3.3.6 File Sharing Services and SMB Protocol

- The Server Message Block (SMB) is a client/server file sharing protocol. IBM developed Server Message Block (SMB) in the late 1980s to describe the structure of shared network resources, such as directories, files, printers, and serial ports.
- It is a request-response protocol. Unlike the file sharing supported by FTP, clients establish a long term connection to servers. Once 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.
- Beginning with Windows 2000, all subsequent Microsoft products use DNS naming. This allows TCP/IP protocols to directly support SMB resource sharing, as shown in the figure.
- The LINUX and UNIX operating systems also provide a method of sharing resources with Microsoft networks using a version of SMB called SAMBA.
- The Apple Macintosh operating systems also support resource sharing using the SMB

3.3.6 File Sharing Services and SMB Protocol

- The SMB protocol describes file system access and how clients can make requests for files.
- It also describes the SMB protocol inter-process communication.
- All SMB messages share a common format. This format uses a fixed-sized header followed by a variable-sized parameter and data component.
- SMB messages can:
  - Start, authenticate, and terminate sessions
  - Control file and printer access
  - Allow an application to send or receive messages to or from another device

3.2.7 P2P Services and Gnutella Protocol



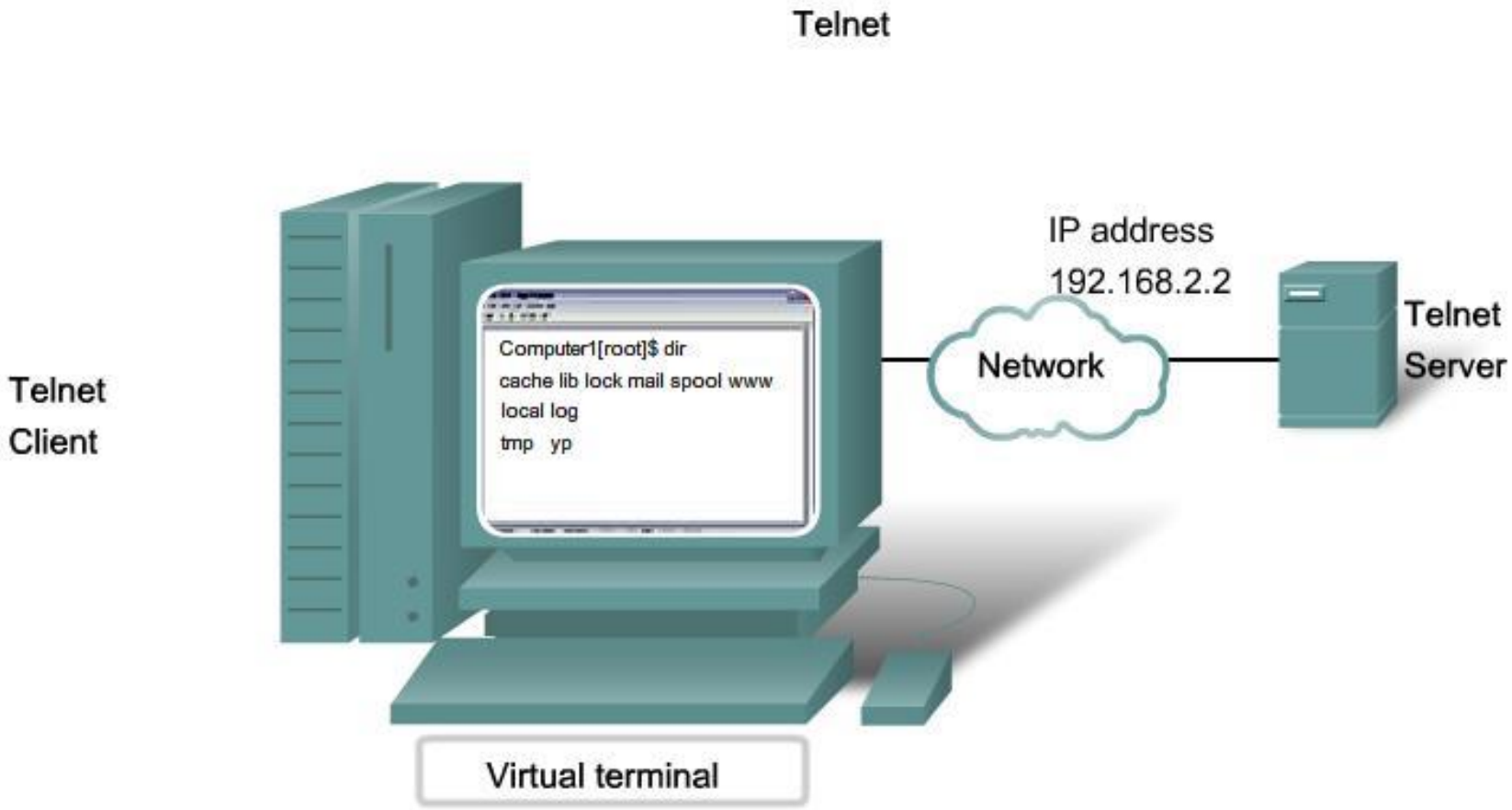
3.2.7 P2P Services and Gnutella Protocol

- With P2P applications based on the Gnutella protocol, people can make files on their hard disks available to others for downloading.
- Gnutella-compatible client software allows users to connect to Gnutella services over the Internet and to locate and access resources shared by other Gnutella peers.
- Many P2P applications do not use a central database to record all the files available on the peers.
- Instead, the devices on the network each tell the other what files are available when queried and use the Gnutella protocol and services to support locating resources.
- .

3.2.7 P2P Services and Gnutella Protocol

- When a user is connected to a Gnutella service, the client applications will search for other Gnutella nodes to connect to.
- These nodes handle queries for resource locations and replies to those requests.
- They also govern control messages, which help the service discover other nodes.
- The actual file transfers usually rely on HTTP services.
- The Gnutella protocol defines five different packet types:
  - ping - for device discovery
  - pong - as a reply to a ping
  - query - for file location
  - query hit - as a reply to a query
  - push - as a download request

3.3.8 Telnet



Telnet provides a way to use a computer, connected via the network, to access a network device as if the keyboard and monitor were directly connected to the device.

3.3.8 Telnet

- Once networks were available, people needed a way to remotely access the computer systems in the same manner that they did with the directly attached terminals.
- Telnet was developed to meet that need.
- A connection using Telnet is called a Virtual Terminal (VTY) session, or connection.
- To support Telnet client connections, the server runs a service called the Telnet daemon.
- Most operating systems include an Application layer Telnet client. On a Microsoft Windows PC, Telnet can be run from the command prompt. Other common terminal applications that run as Telnet clients are HyperTerminal, Minicom, and TeraTerm.
- Once 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. If authorized, they can start and stop processes, configure the device, and even shut down the system.

3.3.8 Telnet

- Telnet is a client/server protocol.
- It provides the syntax and order of the commands used to initiate the Telnet session, as well as control commands that can be issued during a session.
- Each Telnet command consists of at least two bytes. The first byte is a special character called the Interpret as Command (IAC) character.
- Sample Telnet protocol commands include:
  - Are You There (AYT) - Lets the user request that something appear on the terminal screen to indicate that the VTY session is active.
  - Erase Line (EL) - Deletes all text from the current line.
  - Interrupt Process (IP) - Suspends, interrupts, aborts, or terminates the process to which the Virtual Terminal is connected.
- While the Telnet protocol supports user authentication, it does not support the transport of encrypted data. This means that the data can be intercepted and easily understood.
- If security is a concern, 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. It also provides stronger authentication than Telnet and supports the transport of session data using encryption. As a best practice, network professionals should always use SSH in place of Telnet, whenever possible.