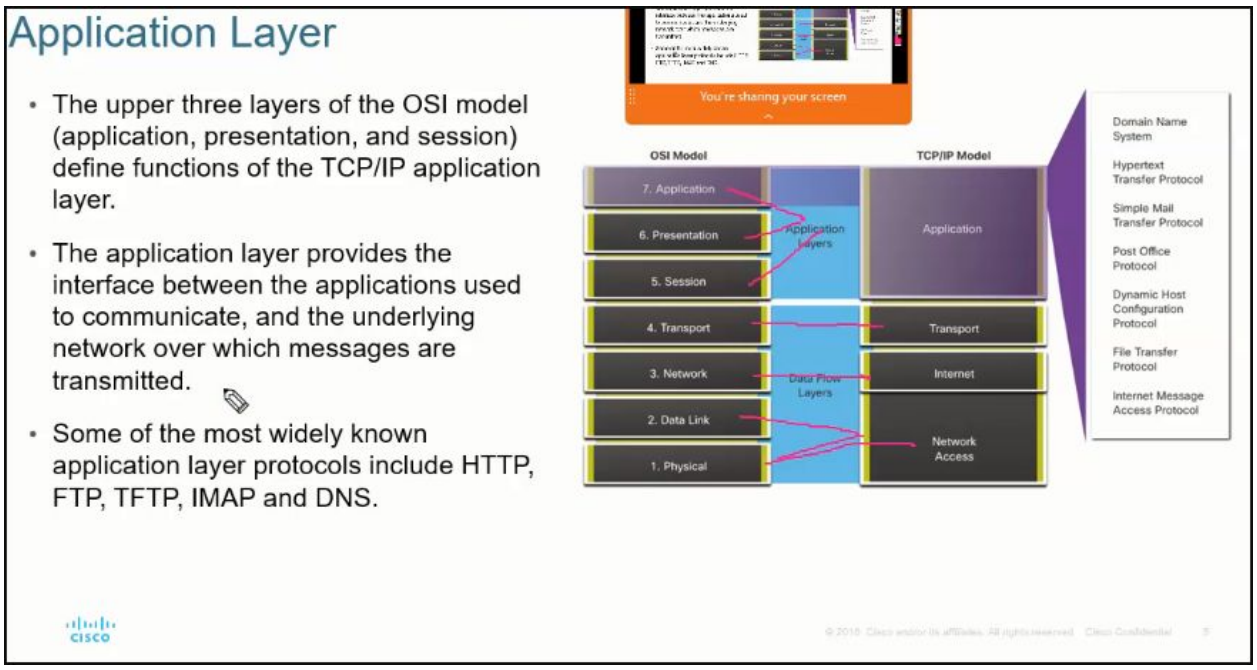
CHAPTER 15

There are many application layer protocols, and new protocols are always being developed. Some of the most widely known application layer protocols include Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP), Internet Message Access Protocol (IMAP), and Domain Name System (DNS) protocol.



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.
- Compressing data in a way that can be decompressed by the destination device.
- Encrypting data for transmission and decrypting data upon receipt.

Session Layer

As the name implies, functions at the 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.

Name System

DNS - Domain Name System (or Service)

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

Host Config

BOOTP - Bootstrap Protocol

- UDP client 68, server 67
- Enables a diskless workstation to discover its own IP address, the IP address of a BOOTP server on the network, and a file to be loaded into memory to boot the machine
- BOOTP is being superseded by DHCP

DHCP - Dynamic Host Configuration Protocol

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

Email

SMTP - Simple Mail Transfer Protocol

- TCP 25
- Enables clients to send email to a mail server
- Enables servers to send email to other servers

POP3 - Post Office Protocol

- TCP 110
- Enables clients to retrieve email from a mail server
- Downloads the email to the local mail application of the client

IMAP - Internet Message Access Protocol

- TCP 143
- Enables clients to access email stored on a mail server
- Maintains email on the server

File Transfer

FTP - File Transfer Protocol

- TCP 20 to 21
- Sets rules that enable a user on one host to access and transfer files to and from another host over a network
- FTP is a reliable, connection-oriented, and acknowledged file delivery protocol

TFTP - Trivial File Transfer Protocol

- UDP client 69
- A simple, connectionless file transfer protocol with best-effort, unacknowledged file delivery
- It uses less overhead than FTP

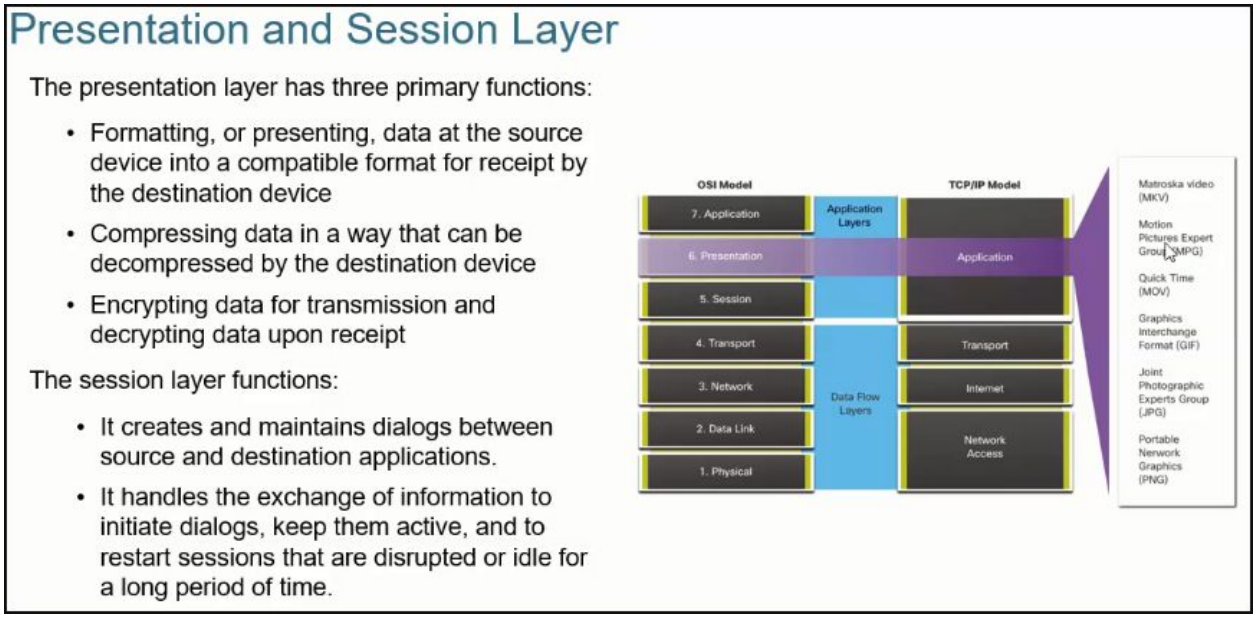
Web

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

HTTPS - HTTP Secure

- TCP, UDP 443
- The browser uses encryption to secure HTTP communications
- Authenticates the website to which you are connecting your browser



Good job!

You have successfully identified the correct answers.

1. The application layer of the OSI model is the layer that is closest to the end user. It provides an interface between application protocols exchanging data between hosts.
2. The presentation layer is concerned with formatting and presenting data in a format that is compatible with the destination device. Examples of presentation layer standards are MKV, GIF, JPG, MOV, and PNG.
3. The upper three OSI layers; application, presentation, and session, define the application layer functions of the TCP/IP model.
4. The application layer of the OSI model provides an interface between applications protocols exchanging data between hosts. Protocols at the application layer include DNS, HTTP, SMTP, FTP, and IMAP.
5. The session layer of the OSI model creates and maintains the dialogs, or sessions, between two communicating hosts.

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.

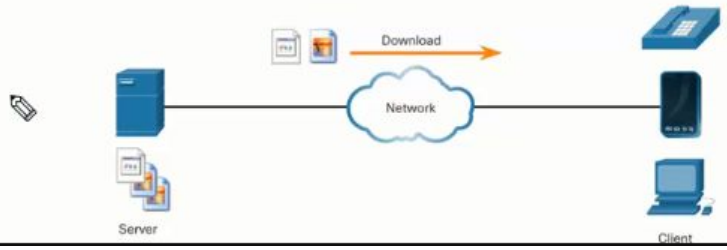
Name System
DNS - Domain Name System (or Service)
- TCP, UDP client 53
- Translates domain names, such as cisco.com, into IP addresses.

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

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.

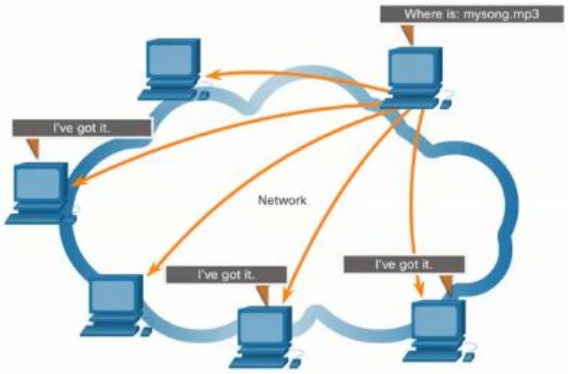


Common P2P Applications

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
- Direct Connect
- eDonkey
- Freenet



In the peer-to-peer (P2P) networking model, the data is accessed from a peer device without the use of a dedicated server.

The P2P network model involves two parts: P2P networks and P2P applications. Both parts have similar features, but in practice work quite differently.

In a 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. 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.

In addition to sharing files, a network such as this one would allow users to enable networked games or share an internet connection.

In a peer-to-peer exchange, both devices are considered equal in the communication process. Peer 1 has files that are shared with Peer 2 and can access the shared printer that is directly connected to Peer 2 to print files.
Some P2P applications are based on the Gnutella protocol, where each user shares whole files with other users. As shown in the figure, 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 Gnutella client applications are available, including µTorrent, BitComet, DC++, Deluge, and emule.

The figure shows a P2P application searching for shared resources. The P2papplication is asking its pers if the have the resource in this case mysong.mp3.

Where is: mysong.mp3I've got it.I've got it.NetworkI've got it.

Good job!

You have successfully identified the correct answers.

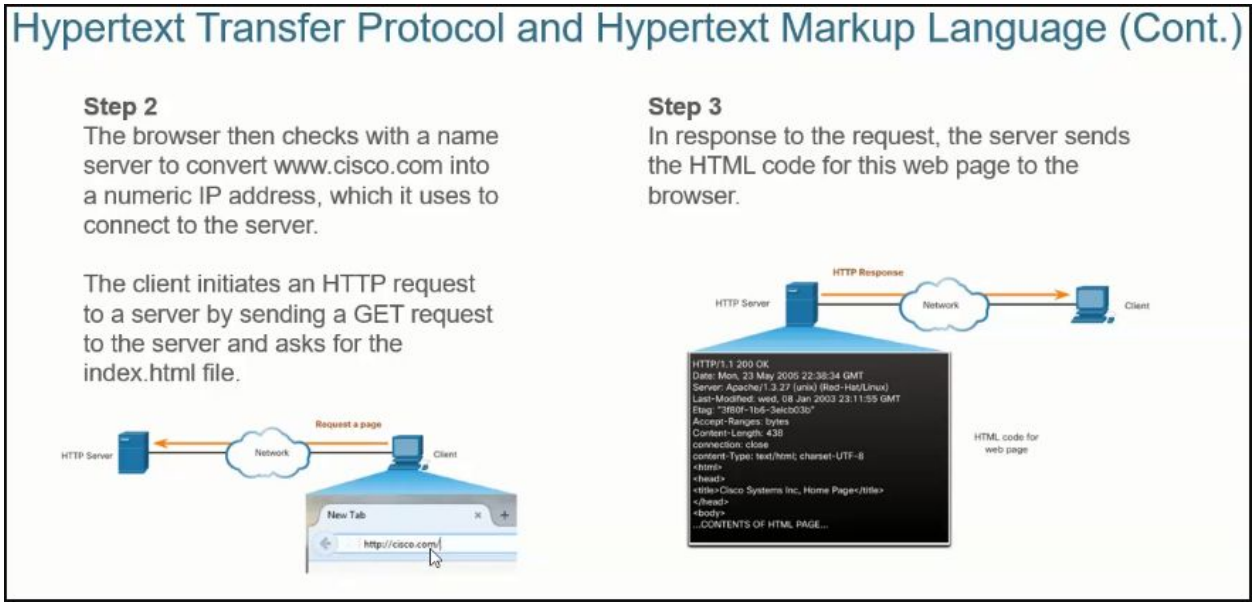
1. The correct answer is False. In the peer-to-peer model, clients can share resources without using a dedicated server.
2. The correct answer is True. A peer-to-peer network does not require a dedicated server because each peer can function as both a client and as a server.
3. BitTorrent clients use a torrent file to locate other clients that are sharing pieces of needed files. In this way, many files can be shared between clients at the same time.
4. Gnutella is a peer-to-peer protocol that allows users to share whole files with other users.

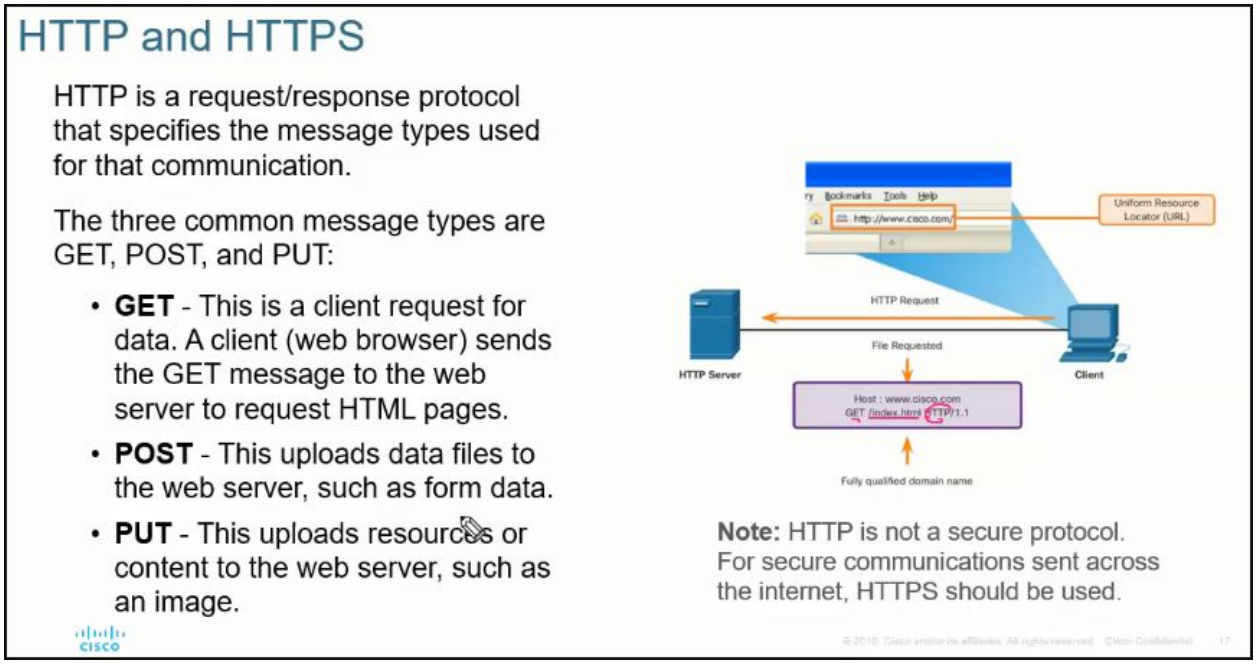
Hypertext Transfer Protocol and Hypertext Markup Language

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)
- index.html (the specific filename requested)

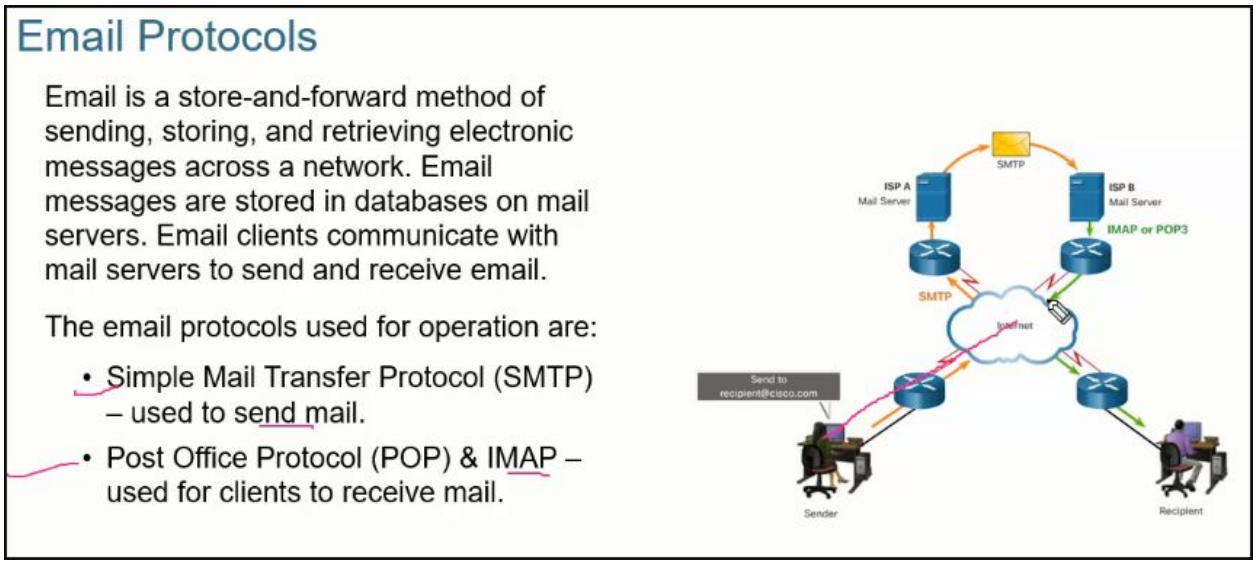




HTTP and HTTPS

HTTP is a request/response protocol. When a client, typically a web browser, sends a request to a web server, HTTP specifies the message types used for that communication. The three common message types are GET (see figure), 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.



SMTP message formats require a message header and a message body. Although the message body can contain any amount of text, the message header must have a properly formatted recipient email address and a sender address.

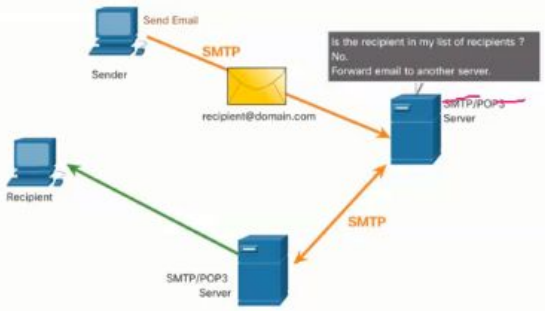
When a client sends email, the client SMTP process connects with a server SMTP process on well-known port 25. After the connection is made, the client attempts to send the email to the server across the connection. When the server receives the message, it either places the message in a local account, 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, when email messages are sent. Therefore, SMTP spools messages to be sent at a later time. Periodically, the server checks the queue for messages and attempts to send them again. If the message is still not delivered after a predetermined expiration time, it is returned to the sender as undeliverable.

1. HTTP uses the POST message to upload data files to a web server. The GET message is used by clients to request data and the PUT message is used to upload content such as images.
2. Web browsers connect to web servers over HTTP. IMAP and SMTP are email protocols. SSL is an encryption protocol used with HTTPS.
3. Email clients connect to SMTP servers over port 25 to send email. POP and IMAP are used by clients to receive email. HTTP is used between web browsers and web servers.
4. IMAP is a protocol for clients to retrieve copies of email messages from an IMAP server. The original messages remain on the server until manually deleted.
5. The correct answer is False. HTTP sends information in plaintext and is not considered secure. If security is desired, HTTP Secure (HTTPS) should be used.

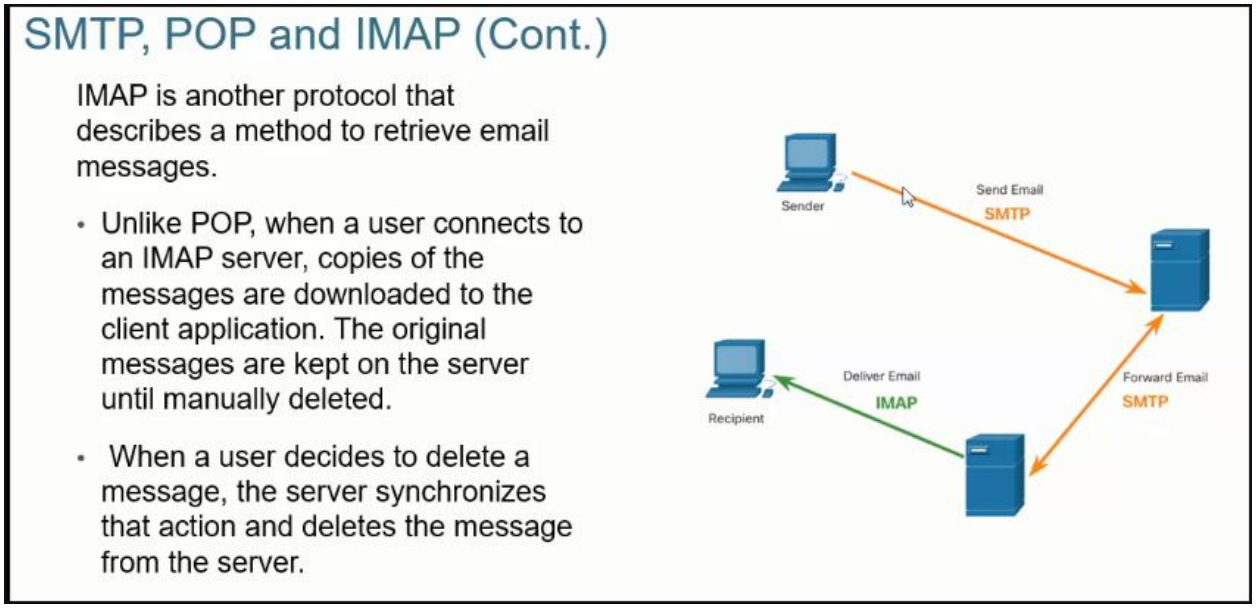
SMTP, POP and IMAP

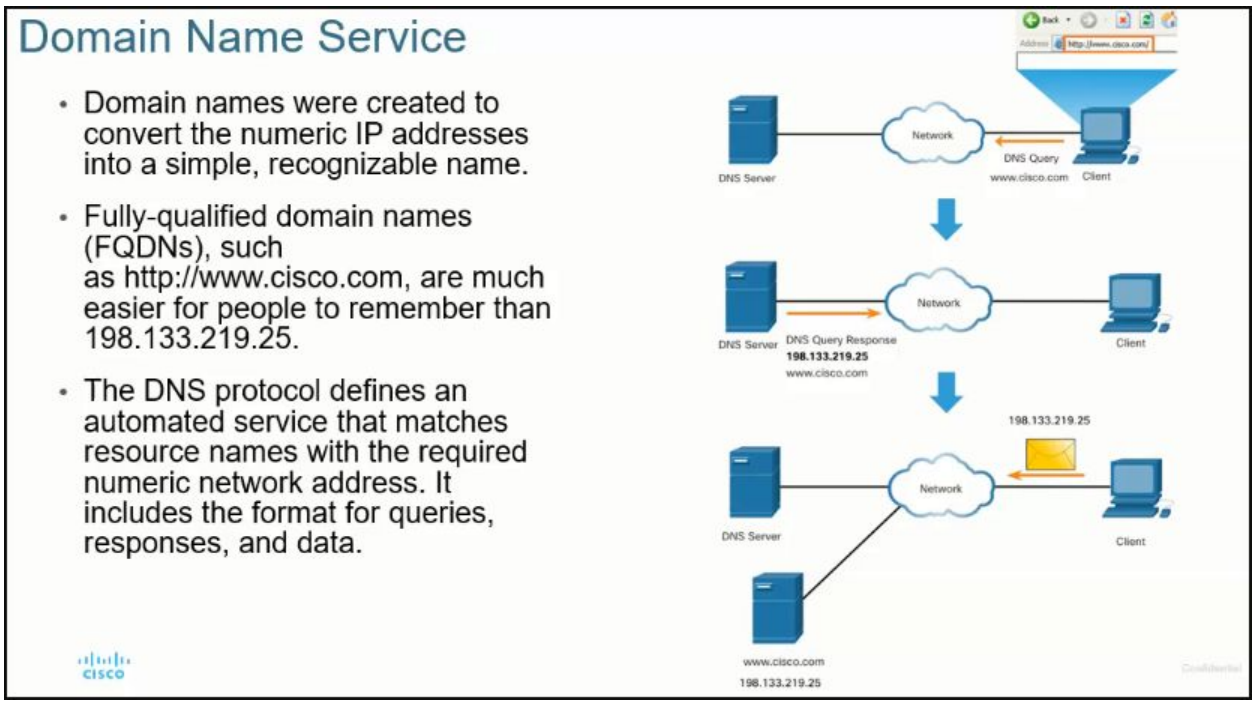
- When a client sends email, the client SMTP process connects with a server SMTP process on well-known port 25.
- After the connection is made, the client attempts to send the email to the server across the connection.
- When the server receives the message, it either places the message in a local account, 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.



Note: SMTP message formats require a message header (recipient email address & sender email address) and a message body.

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





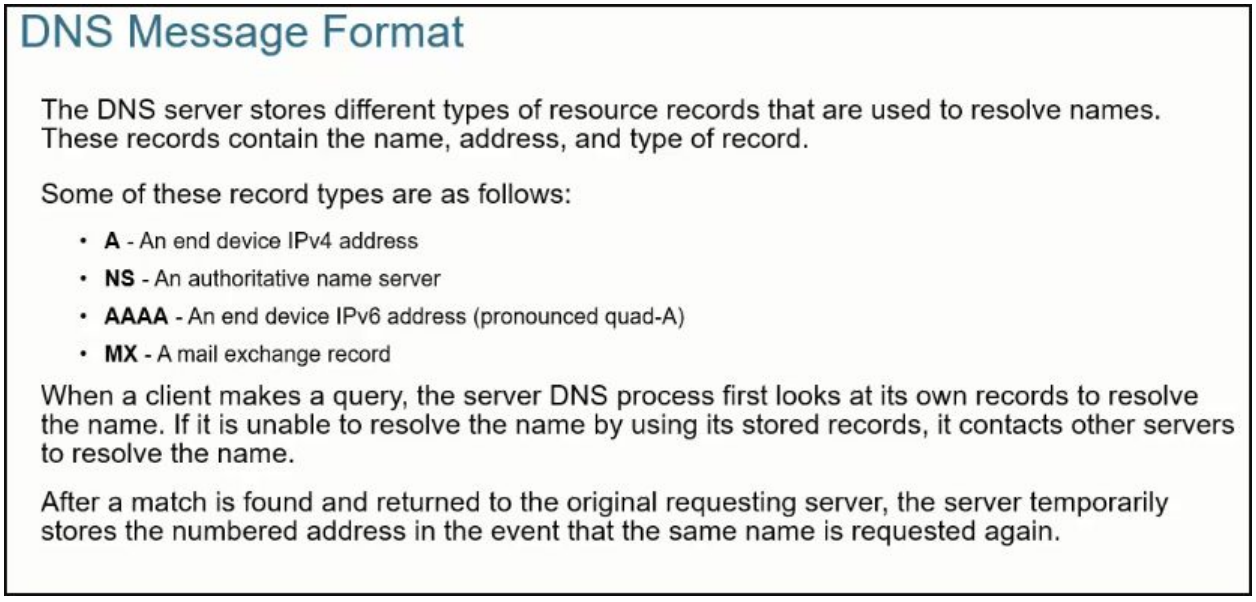
Domain Name Service

There are other application layer-specific protocols that were designed to make it easier to obtain addresses for network devices. These services are essential because it would be very time consuming to remember IP addresses instead of URLs or manually configure all of the devices in a medium to large network. The first topic in this module gave you an overview of these protocols. This topic goes into more detail about the IP addressing services, DNS and DHCP.

In data networks, devices are labeled with numeric IP addresses to send and receive data over networks. Domain names were created to convert the numeric address into a simple, recognizable name.

On the internet, fully-qualified domain names (FQDNs), such as http://www.cisco.com, are much easier for people to remember than 198.133.219.25, which is the actual numeric address for this server. If Cisco decides to change the numeric address of www.cisco.com, it is transparent to the user because the domain name remains the same. The new address is simply linked to the existing domain name and connectivity is maintained.

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 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.



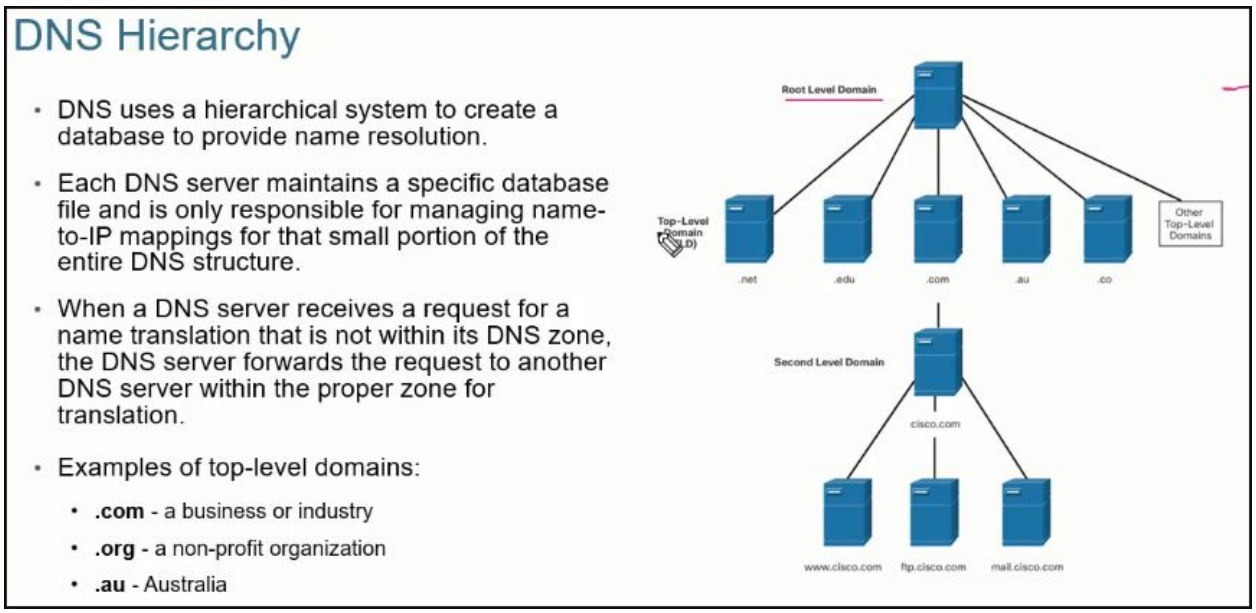
DNS Message Format

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.

The DNS cient service on Windows PCs also stores previously resolved names in memory. The **ipconfig /displaydns** command displays all of the cached DNS entries.



DNS Hierarchy

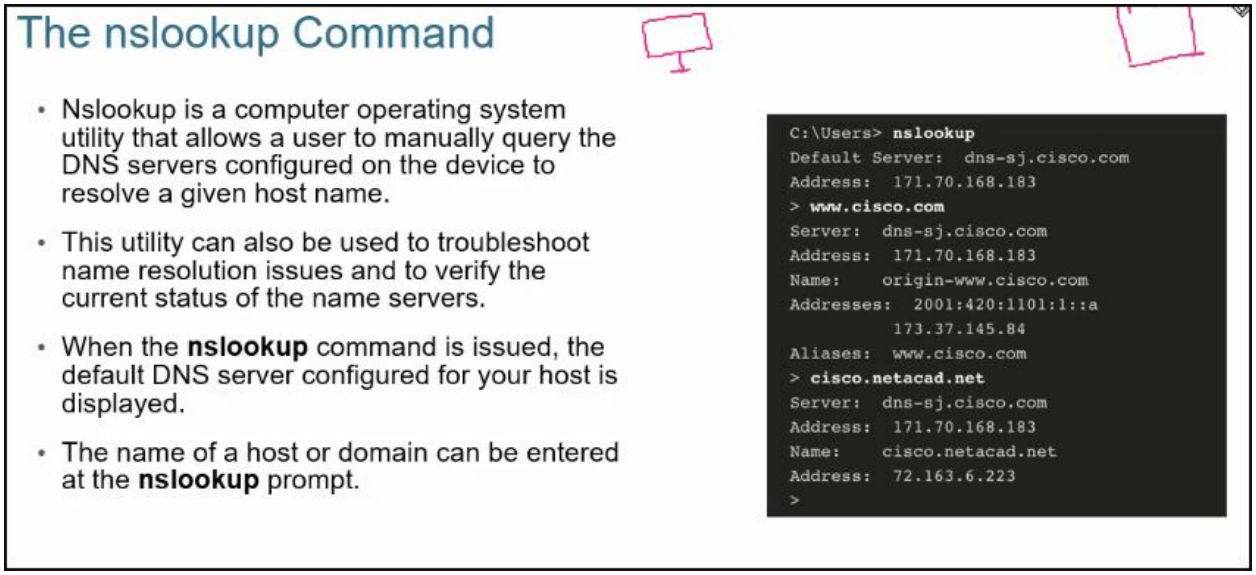
The DNS protocol uses a hierarchical system to create a database to provide name resolution, as shown in the figure. DNS uses domain names to form the hierarchy.

The naming structure is broken down into small, manageable zones. 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. DNS is scalable because hostname resolution is spread across multiple servers.

The different top-level domains represent either the type of organization or the country of origin. Examples of top-level domains are the following:

- **.com** - a business or industry
- **.org** - a non-profit organization
- **.au** - Australia

- **.co** - Colombia



The nslookup Command

When configuring a network device, one or more DNS Server addresses are provided that the DNS client can use for name resolution. Usually the ISP provides the addresses to use for the DNS servers. When a user application requests to connect to a remote device by name, the requesting DNS client queries the name server 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.

In this figure, 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. The Nslookup utility has many options available for extensive testing and verification of the DNS process.

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. This is referred to as dynamic addressing. The alternative to dynamic addressing is static addressing. When using static addressing, the network administrator manually enters IP address information on hosts.

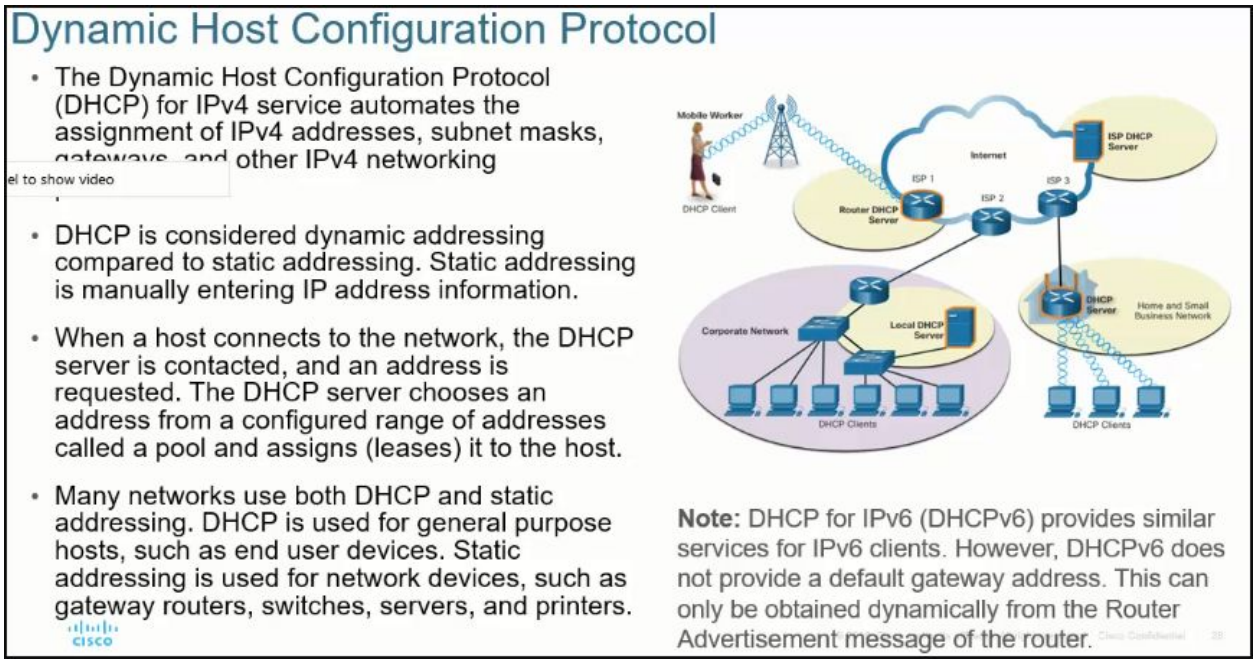
When a host connects to the network, the DHCP server is contacted, and an address is requested. The DHCP server chooses an address from a configured range of addresses called a pool and assigns (leases) it to the host.

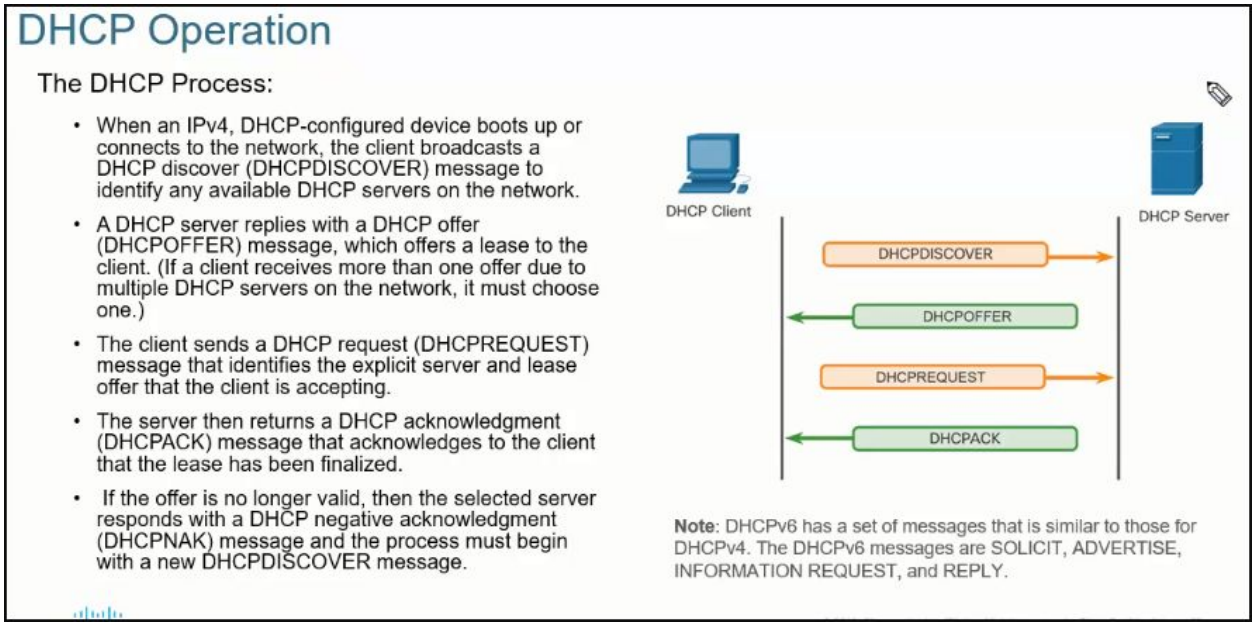
On larger networks, or where the user population changes frequently, DHCP is preferred for address assignment. New users may arrive and need connections; others may have new computers that must be connected. Rather than use static addressing for each connection, it is more efficient to have IPv4 addresses assigned automatically using DHCP.

DHCP can allocate IP addresses for a configurable period of time, called a lease period. The lease period is an important DHCP setting, When the lease period expires or the DHCP server gets a DHCPRELEASE message the address is returned to the DHCP pool for reuse. Users can freely move from location to location and easily re-establish network connections through DHCP.

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.

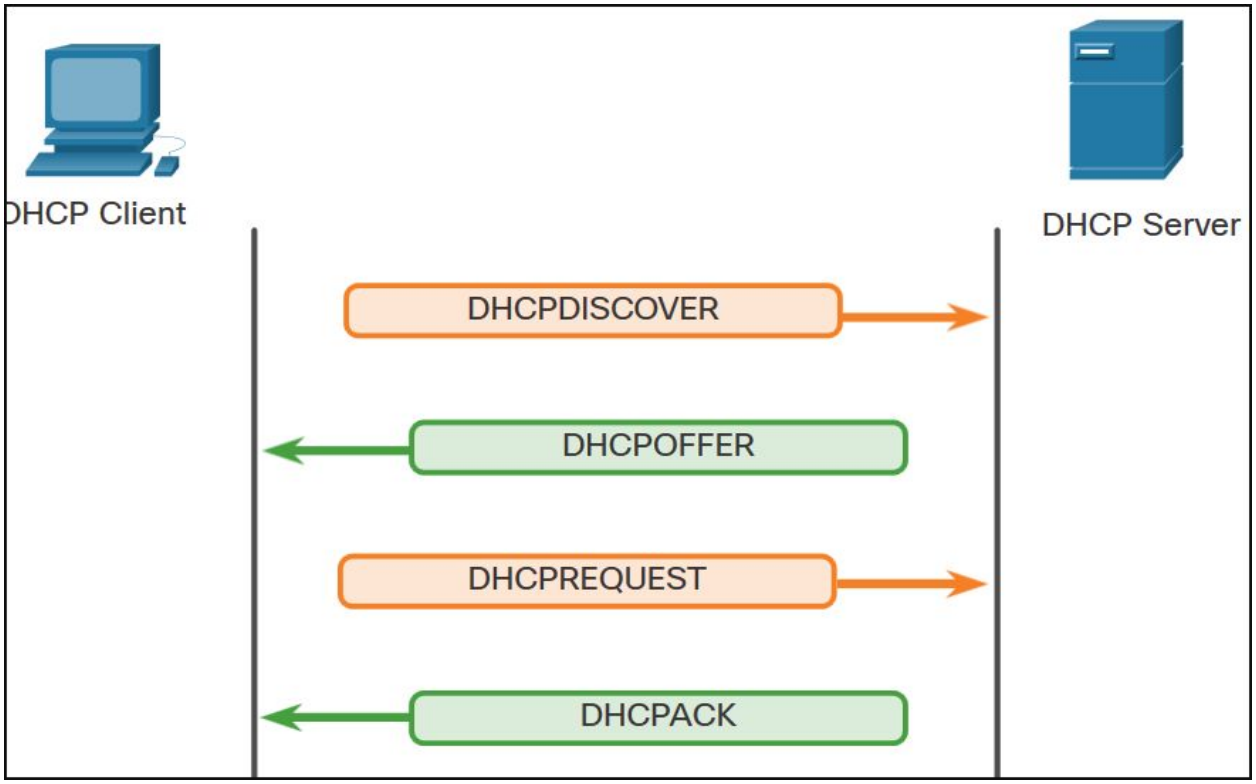
DHCP for IPv6 (DHCPv6) provides similar services for IPv6 clients. One important difference is that DHCPv6 does not provide a default gateway address. This can only be obtained dynamically from the Router Advertisement message of the router.





DHCP Operation

As shown in the figure, 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. A DHCP server replies with a DHCP offer (DHCPOFFER) message, which offers a lease to the client. The offer message contains the IPv4 address and subnet mask to be assigned, the IPv4 address of the DNS server, and the IPv4 address of the default gateway. The lease offer also includes the duration of the lease.



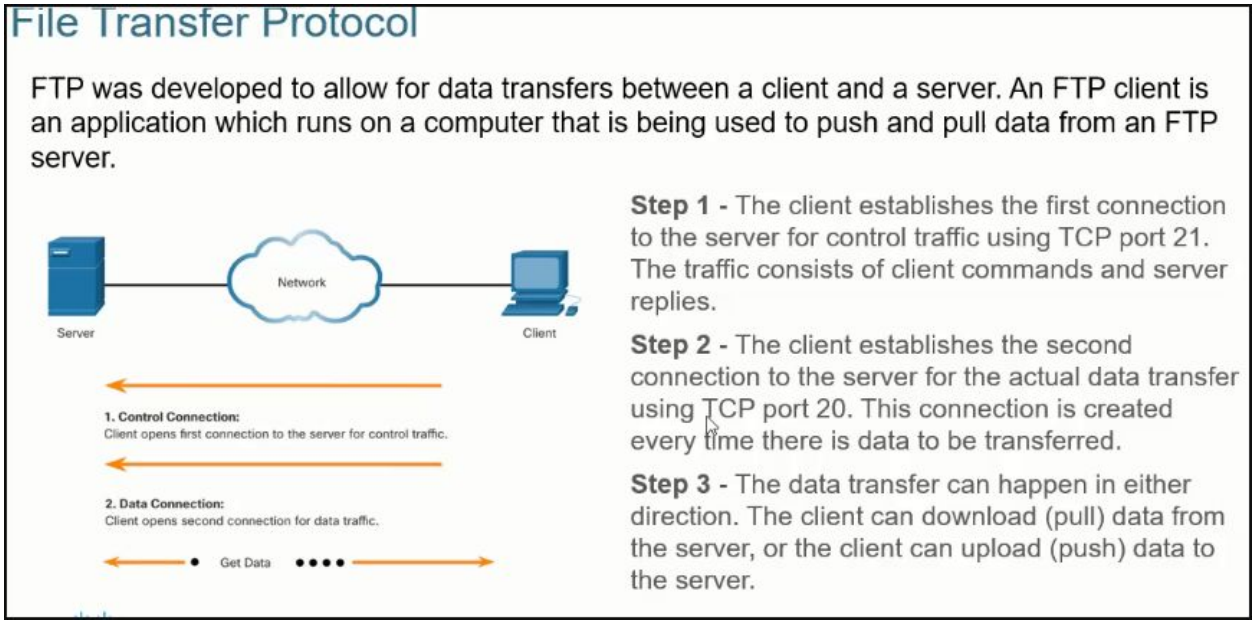
The client may receive multiple DHCPOFFER messages if there is more than one DHCP server on the local network. Therefore, it must choose between them, and sends a DHCP request (DHCPREQUEST) message that identifies the explicit server and lease offer that the client is accepting. A client may also choose to request an address that it had previously been allocated by the server.

Assuming that the IPv4 address requested by the client, or offered by the server, is still available, the server returns a DHCP acknowledgment (DHCPACK) message that acknowledges to the client that the lease has been finalized. If the offer is no longer valid, then the selected server responds with a DHCP negative acknowledgment (DHCPNAK) message. If a DHCPNAK message is returned, then the selection process must begin again with a new DHCPDISCOVER message being transmitted. After the client has the lease, it must be renewed prior to the lease expiration through another DHCPREQUEST message.

The DHCP server ensures that all IP addresses are unique (the same IP address cannot be assigned to two different network devices simultaneously). Most ISPs use DHCP to allocate addresses to their customers.

DHCPv6 has a set of messages that is similar to those for DHCPv4. The DHCPv6 messages are SOLICIT, ADVERTISE, INFORMATION REQUEST, and REPLY.

1. DNS AAAA records are used to resolve names to IPv6 addresses.
2. The correct answer is False. When a DNS server receives a name resolution request for a name not within its zone, the serve will forward the request to another DNS server.
3. By issuing the **nslookup** command, the default DNS server that is configured is displayed.
4. NS records resolve authoritative name servers. DNS A records resolve IPv4 addresses. AAAA records resolve IPv6 addresses, and MX records resolve mail exchange servers.
5. The correct answer is False. There are four DHCP messages exchanged between clients and servers. The client initiates the DHCP process with a DHCP discover message to available DHCP servers.



File Transfer Protocol

As you learned in previous topics, in the client/server model, the client can upload data to a server, and download data from a server, if both devices are using a file transfer protocol (FTP). Like HTTP, email, and addressing protocols, FTP is commonly used application layer protocol. This topic discusses FTP in more detail.

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.

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.

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.

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.

Server Message Block

The Server Message Block (SMB) is a client/server file sharing protocol that describes the structure of shared network resources, such as directories, files, printers, and serial ports. It is a request-response protocol. All SMB messages share a common format. This format uses a fixed-sized header, followed by a variable-sized parameter and data component.

Here are 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 file-sharing and print services have become the mainstay of Microsoft networking. With the introduction of the Windows 2000 software series, Microsoft changed the underlying structure for using SMB. In previous versions of Microsoft products, the SMB services used a non-TCP/IP protocol to implement name resolution. Beginning with Windows 2000, all subsequent Microsoft products use DNS naming, which allows TCP/IP protocols to directly support SMB resource sharing,

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.

The LINUX and UNIX operating systems also provide a method of sharing resources with Microsoft networks by using a version of SMB called SAMBA. The Apple Macintosh operating systems also support resource sharing by using the SMB protocol.

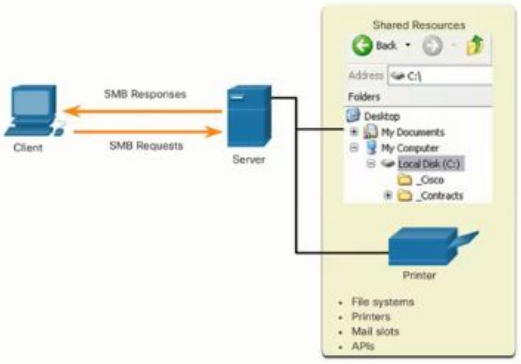
Server Message Block

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

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.



1. FTP requires two connections between the client and the server. One connection is over port 21 for client commands and server replies. The other connection is over port 20 for data transfer.
2. The correct answer is True. Data transfer over FTP can take place in either direction, uploads from client to server, or downloads from server to client.
3. Ports 20 and 21 are used by FTP.
4. The correct answer is False. Resource sharing over SMB is also supported by Apple Macintosh. Linux and Unix operating systems use a version of SMB called SAMBA.

What did I learn in this module?

Application, Presentation, and Session

In the OSI and the TCP/IP models, the application layer is the closest layer to the end user. 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 at the source device into a compatible form for receipt by the destination device, compressing data in a way that can be decompressed by the destination device, and encrypting data for transmission and decrypting data upon receipt. The session layer creates and maintains 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. TCP/IP application layer protocols specify the format and control information necessary for many common internet communication functions. These protocols are used by both the source and destination devices during a session. The protocols implemented on both the source and destination host must be compatible.

Peer-to-Peer

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. The client begins the exchange by requesting data from the server, which responds by sending one or more streams of data to the client. In a P2P network, two or more computers are connected via a network and can share resources without having a dedicated server. Every 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. P2P applications require that each end device provide a user interface and run a background service. Some P2P applications use a hybrid system where resource sharing is decentralized, but the indexes that point to resource locations are stored in a centralized directory. Many P2P applications allow users to share pieces of files with each other at the same time. Clients use a small file called a torrent file to locate other users who have pieces that they need so that they can connect directly to them. This file also contains information about tracker computers that keep track of which users have what pieces of which files.

Web and Email Protocols

When a web address or 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. HTTP is a request/response protocol. When a client, typically a web browser, sends a request to a web server, HTTP specifies the message types used for that communication. The three common message types are GET, POST, and PUT. For secure communication across the internet, HTTPS uses the same client request-server response process as HTTP, but the data stream is encrypted with SSL before being transported across the network. Email supports three separate protocols for operation: SMTP, POP, and IMAP. The application layer process that sends mail uses SMTP. A client retrieves email using POP or IMAP. SMTP message formats require a message header and a message body. While the message body can contain any amount of text, the message header must have a properly formatted recipient email address and a sender address. POP is used by an application to retrieve mail from a mail server. With POP, mail is downloaded from the server to the client and then deleted on the server. With IMAP, unlike POP, when the user connects to an IMAP-capable server, copies of the messages are downloaded to the client application. The original messages are kept on the server until manually deleted.

IP Addressing Services

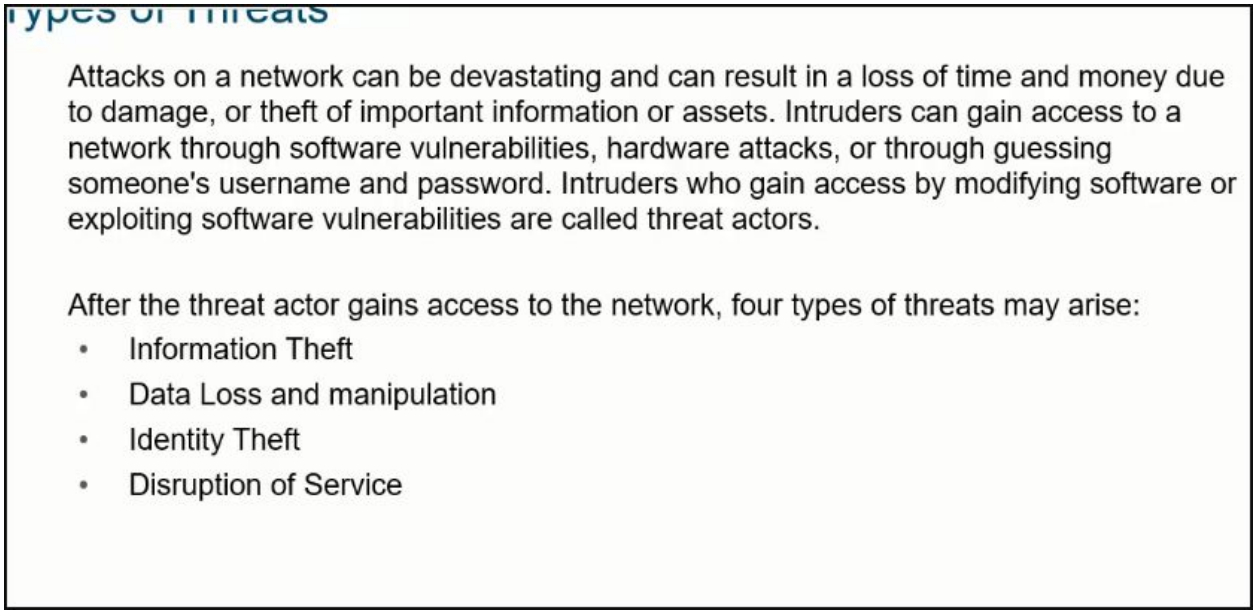
The DNS protocol matches resource names with the required numeric network address. The DNS protocol communications use a message format for all types of client queries and server responses, error messages, and the transfer of resource record information between servers.

DNS uses domain names to form a hierarchy. 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. Computer OSs use Nslookup to allow the user to manually query the name servers to resolve a given host name. DHCP for IPv4 service automates the assignment of IPv4 addresses, subnet masks, gateways, and other IPv4 networking parameters. DHCPv6 provides similar services for IPv6 clients, except that it does not provide a default gateway address. When an IPv4, DHCP-configured device boots up or connects to the network, the client broadcasts a DHCPDISCOVER message to identify any available DHCP servers on the network. A DHCP server replies with a DHCPOFFER message, which offers a lease to the client. DHCPv6 has a set of messages that is similar to those for DHCPv4. The DHCPv6 messages are SOLICIT, ADVERTISE, INFORMATION REQUEST, and REPLY.

File Sharing Services

An FTP client is an application which runs on a computer that is being used to push and pull data from an FTP server. 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. The client can download (pull) data from the server, or the client can upload (push) data to the server. Here are 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. 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 if the resource is local to the client host.

CHAPTER 16



Information theft is breaking into a computer to obtain confidential information. Information can be used or sold for various purposes such as when someone is stealing proprietary information of an organization, like research and development data.

Data loss and manipulation is breaking into a computer to destroy or alter data records. An example of data loss is a threat actor sending a virus that reformats a computer hard drive. An example of data manipulation is breaking into a records system to change information, such as the price of an item.

Identity theft is a form of information theft where personal information is stolen for the purpose of taking over the identity of someone. Using this information, a threat actor can obtain legal documents, apply for credit, and make unauthorized online purchases. Identify theft is a growing problem costing billions of dollars per year.

Disruption of service is preventing legitimate users from accessing services to which they are entitled. Examples include denial of service (DoS) attacks on servers, network devices, or network communications links.

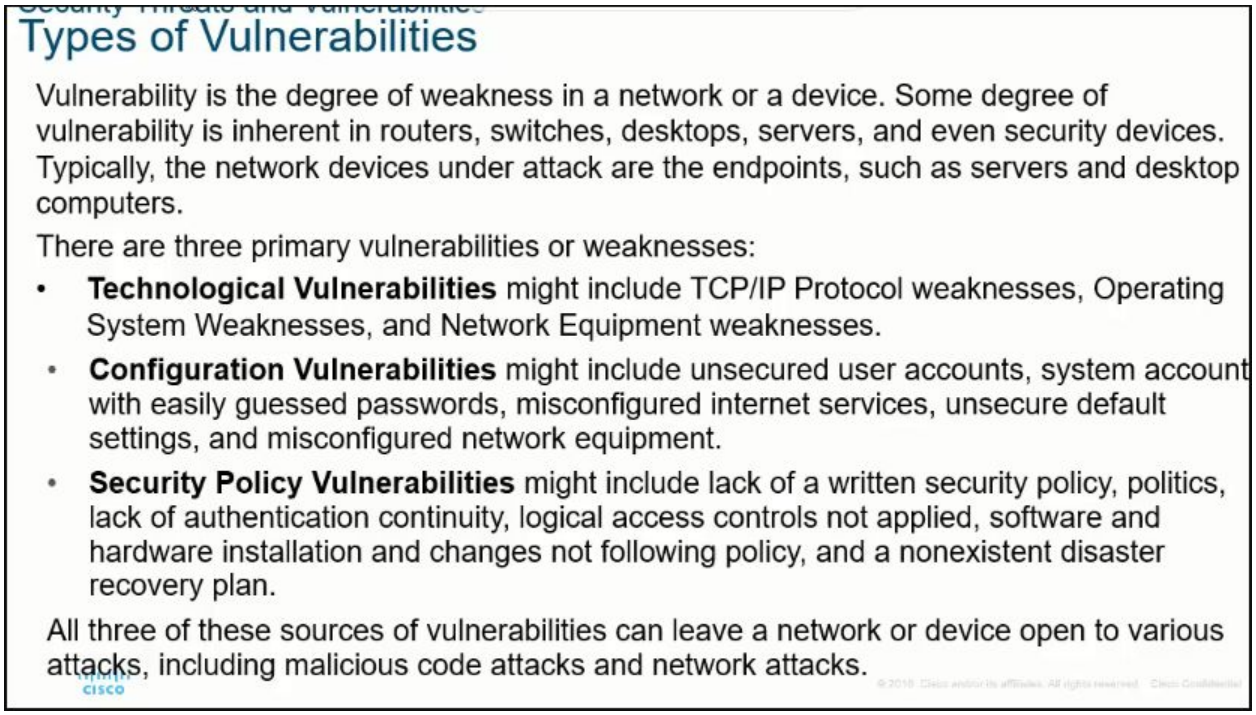
Vulnerability is the degree of weakness in a network or a device. Some degree of vulnerability is inherent in routers, switches, desktops, servers, and even security devices. Typically, the network devices under attack are the endpoints, such as servers and desktop computers.

There are three primary vulnerabilities or weaknesses: technological, configuration, and security policy. All three of these sources of vulnerabilities can leave a network or device open to various attacks, including malicious code attacks and network attacks.

Technological Vulnerabilities

Vulnerability	Description
TCP/IP Protocol Weakness	● Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), and Internet Control Message Protocol (ICMP) are inherently insecure. ● Simple Network Management Protocol (SNMP) and Simple Mail Transfer Protocol (SMTP) are related to the inherently insecure structure upon which TCP was designed.

Operating System Weakness	• Each operating system has security problems what must be addressed. • UNIX, Linux, Mac OS, Mac OS X, Windows Server 2012, Windows 7, Windows 8 • They are documented in the Computer Emergency Response Team (CERT) archives at http://www.cert.org
Network Equipment Weakness	Various types of network equipment, such as routers, firewalls, and switches have security weaknesses that must be recognized and protected against. Their weaknesses include password protection, lack of authentication, routing protocols, and firewall holes.



Configuration Vulnerabilities

Vulnerability	Description
Unsecured user accounts	User account information may be transmitted insecurely across the network, exposing usernames and passwords to threat actors.
System accounts with easily guessed passwords	This common problem is the result of poorly created user passwords.

Misconfigured internet services	Turning on JavaScript in web browsers enables attacks by way of JavaScript controlled by threat actors when accessing untrusted sites. Other potential sources of weaknesses include misconfigured terminal services, FTP, or web servers (e.g., Microsoft Internet Information Services (IIS), and Apache HTTP Server.
Unsecured default settings within products	Many products have default settings that create or enable holes in security.
Misconfigured network equipment	Misconfigurations of the equipment itself can cause significant security problems. For example, misconfigured access lists, routing protocols, or SNMP community strings can create or enable holes in security.

Policy Vulnerabilities

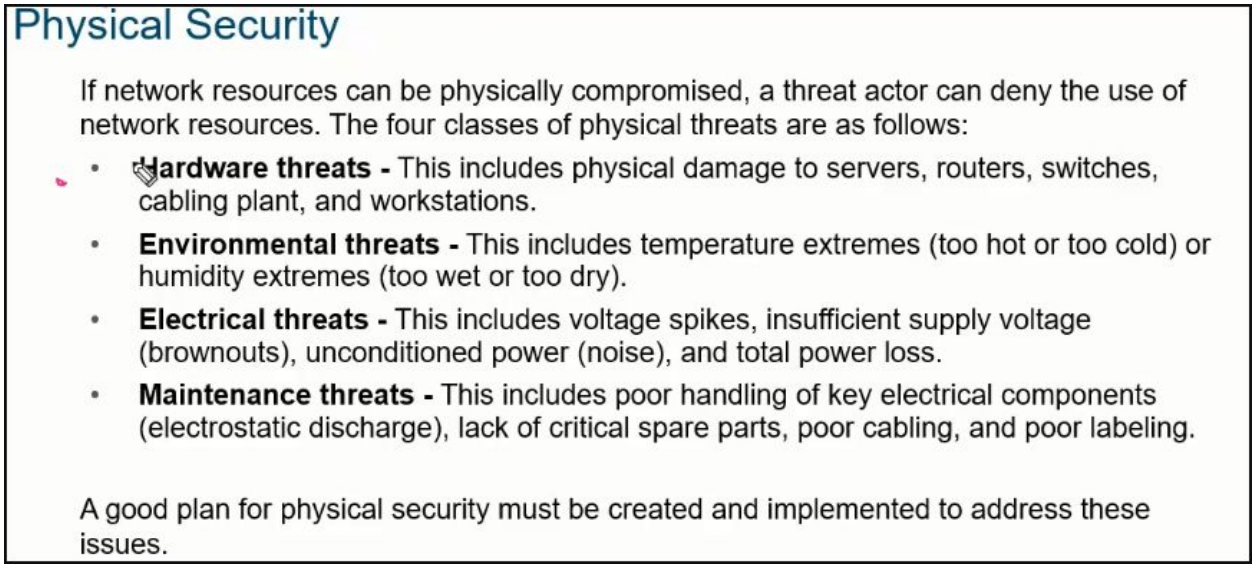
Vulnerability	Description
Lack of written security policy	A security policy cannot be consistently applied or enforced if it is not written down.
Politics	Political battles and turf wars can make it difficult to implement a consistent security policy.
Lack of authentication continuity	Poorly chosen, easily cracked, or default passwords can allow unauthorized access to the network.
Logical access controls not applied	Inadequate monitoring and auditing allow attacks and unauthorized use to continue, wasting company resources. This could result in legal action or termination against IT technicians, IT management, or even company leadership that allows these unsafe conditions to persist.
Software and hardware installation and changes do not follow policy	Unauthorized changes to the network topology or installation of unapproved application create or enable holes in security.
Disaster recovery plan is nonexistent	The lack of a disaster recovery plan allows chaos, panic, and confusion to occur when a natural disaster occurs or a threat actor attacks the enterprise.

Physical Security

An equally important vulnerable area of the network to consider is the physical security of devices. If network resources can be physically compromised, a threat actor can deny the use of network resources.

The four classes of physical threats are as follows:

- **Hardware threats -** This includes physical damage to servers, routers, switches, cabling plant, and workstations.
- **Environmental threats -** This includes temperature extremes (too hot or too cold) or humidity extremes (too wet or too dry).
- **Electrical threats -** This includes voltage spikes, insufficient supply voltage (brownouts), unconditioned power (noise), and total power loss.
- **Maintenance threats -** This includes poor handling of key electrical components (electrostatic discharge), lack of critical spare parts, poor cabling, and poor labeling.



1. Sending a virus that will format the hard drive of a computer is an example of data loss or manipulation threat.
2. Using stolen credit or identity information to make illegal online purchases is an example of identity theft.
3. Disruption of service attacks occur when legitimate users are prevented from accessing data and services.
4. Stealing research data or proprietary information is an example of information theft.
5. Disruption of service attacks occur when legitimate users are prevented from accessing data and services or the network.
6. Altering data records is an example of data loss or manipulation.
7. Stealing data records or proprietary information is an example of information theft.
8. Using identity information to impersonate someone to obtain credit is an example of identity theft.

16.2 Attacks

Types of Malware

The previous topic explained the types of network threats and the vulnerabilities that make threats possible. This topic goes into more detail about how threat actors gain access to network or restrict authorized users from having access.

Malware is short for malicious software. It is code or software specifically designed to damage, disrupt, steal, or inflict “bad” or illegitimate action on data, hosts, or networks. Viruses, worms, and Trojan horses are types of malware.

Viruses

A computer virus is a type of malware that propagates by inserting a copy of itself into, and becoming part of, another program. It spreads from one computer to another, leaving infections as it travels. Viruses can range in severity from causing mildly annoying effects, to damaging

data or software and causing denial of service (DoS) conditions. Almost all viruses are attached to an executable file, which means the virus may exist on a system but will not be active or able to spread until a user runs or opens the malicious host file or program. When the host code is executed, the viral code is executed as well. Normally, the host program keeps functioning after the virus infects it. However, some viruses overwrite other programs with copies of themselves, which destroys the host program altogether. Viruses spread when the software or document they are attached to is transferred from one computer to another using the network, a disk, file sharing, or infected email attachments.

Worms

Computer worms are similar to viruses in that they replicate functional copies of themselves and can cause the same type of damage. In contrast to viruses, which require the spreading of an infected host file, worms are standalone software and do not require a host program or human help to propagate. A worm does not need to attach to a program to infect a host and enter a computer through a vulnerability in the system. Worms take advantage of system features to travel through the network unaided.

Trojan Horses

A Trojan horse is another type of malware named after the wooden horse the Greeks used to infiltrate Troy. It is a harmful piece of software that looks legitimate. Users are typically tricked into loading and executing it on their systems. After it is activated, it can achieve any number of attacks on the host, from irritating the user (with excessive pop-up windows or changing the desktop) to damaging the host (deleting files, stealing data, or activating and spreading other malware, such as viruses). Trojan horses are also known to create back doors to give malicious users access to the system.

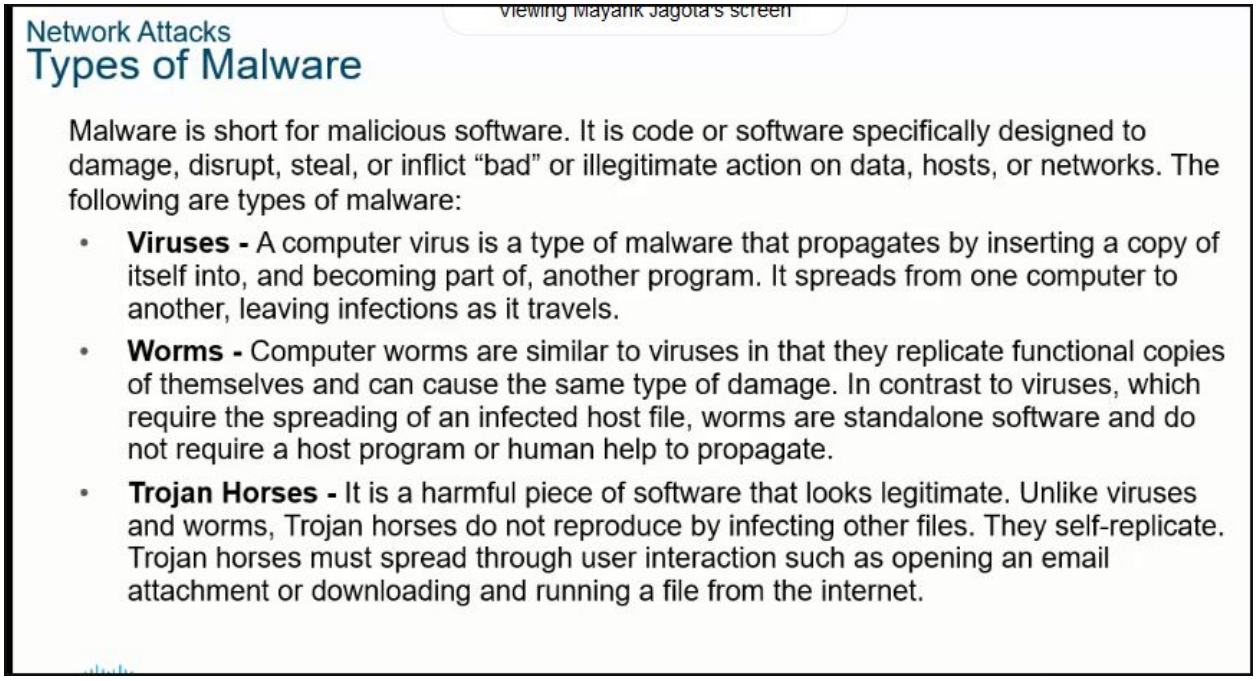
Unlike viruses and worms, Trojan horses do not reproduce by infecting other files. They self-replicate. Trojan horses must spread through user interaction such as opening an email attachment or downloading and running a file from the internet.

Click Play in the figure to view an animated explanation of the three types of malware.

The animation shows a network with two PCs and two routers with the routers are connected to each other sit between the two PCs with each PC connected to one of the routers. The PC on the left has an attacker. As the animation plays a text box opens that reads “The primary vulnerabilities for end-user workstations are virus, worm, and Trojan Horse attacks. As the animation continues to play the attacker at the PC on the left sends a virus attack on the network that travels over the network routers to the PC on the right. A text box opens that reads “A virus is malicious software which executes a specific unwanted, and often harmful, function on a computer”. As the animation continues to play the attacker at the PC on the left sends a worm attack on the network that travels over the network routers to the PC on the right. A text box opens that reads “A worm executes arbitrary code and installs copies of itself in the memory of the infected computer. The main purpose of a worm is to automatically replicate itself and

spread across the network form system to system". As the animation continues to play the attacker at the PC on the left sends a Trojan Horse attack on the network that travels over the network routers to the PC on the right. A text box opens that reads "A Trojan horse is a non-self-replicating type of malware. It often contains malicious code that is designed to look like something else, such as a legitimate application or file. When an infected application or file is downloaded and opened, the Trojan horse can attack the end device from within".

The primary vulnerabilities for end-user workstations are virus, worm, and Trojan Horse attacks. A virus is malicious software which executes a specific unwanted, and often harmful, function on a computer.
A worm executes arbitrary code and installs copies of itself in the memory of the infected computer. The main purpose of a worm is to automatically replicate itself and spread across the network from system to system.
A Trojan horse is a non-self-replicating type of malware. It often contains malicious code that is designed to look like something else, such as a legitimate application or file. When an infected application or file is downloaded and opened, the Trojan horse can attack the end device from within.



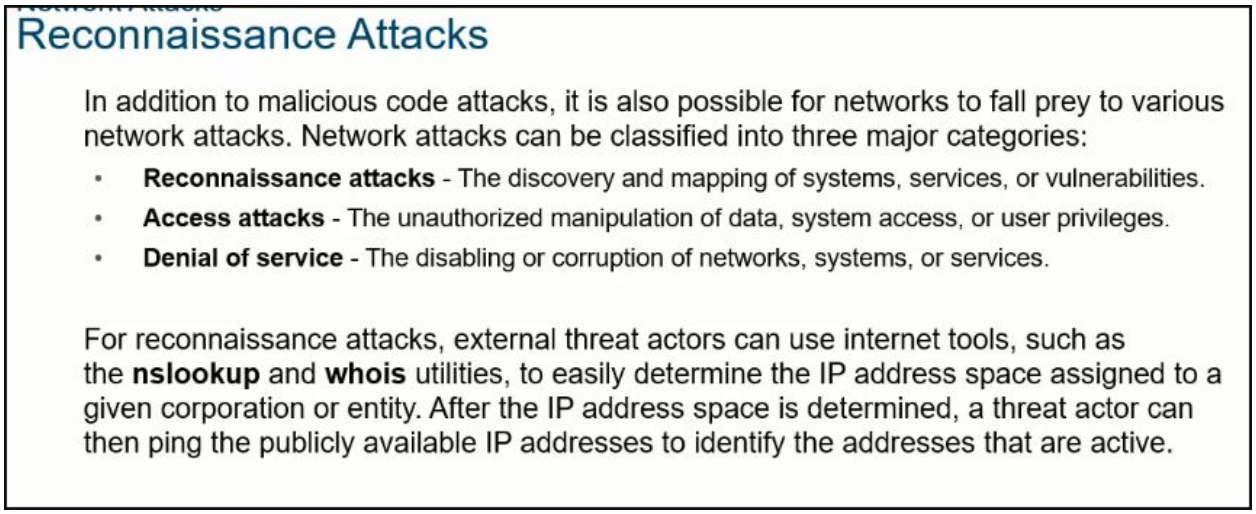
16.2.2

Reconnaissance Attacks

In addition to malicious code attacks, it is also possible for networks to fall prey to various network attacks. Network attacks can be classified into three major categories:

- **Reconnaissance attacks - The discovery and mapping of systems, services, or vulnerabilities.**
- **Access attacks - The unauthorized manipulation of data, system access, or user privileges.**
- **Denial of service - The disabling or corruption of networks, systems, or services.**

For reconnaissance attacks, external threat actors can use internet tools, such as the nslookup and whois utilities, to easily determine the IP address space assigned to a given corporation or entity. After the IP address space is determined, a threat actor can then ping the publicly available IP addresses to identify the addresses that are active. To help automate this step, a threat actor may use a ping sweep tool, such as fping or gping. This systematically pings all network addresses in a given range or subnet. This is similar to going through a section of a telephone book and calling each number to see who answers.



Access Attacks

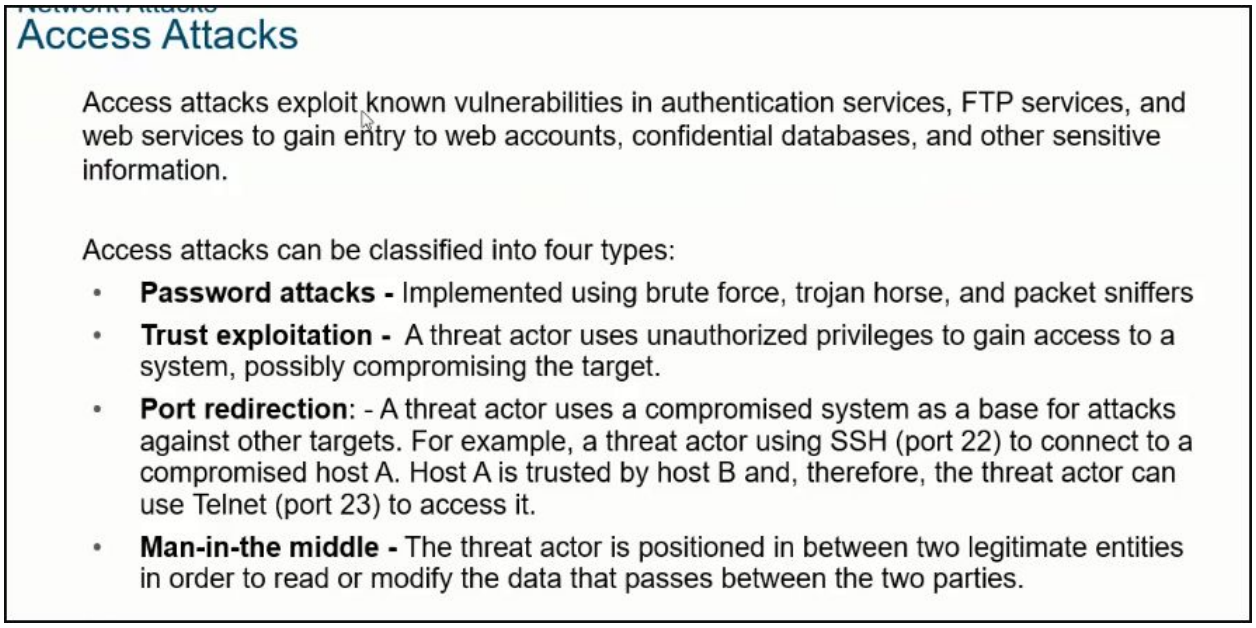
Access attacks exploit known vulnerabilities in authentication services, FTP services, and web services to gain entry to web accounts, confidential databases, and other sensitive information. An access attack allows individuals to gain unauthorized access to information that they have no right to view. Access attacks can be classified into four types: password attacks, trust exploitation, port redirection, and man-in-the middle.

Password Attacks

Threat actors can implement password attacks using several different methods:

- **Brute-force attacks**
- **Trojan horse attacks**

- **Packet sniffers**



Trust Exploitation

In a trust exploitation attack, a threat actor uses unauthorized privileges to gain access to a system, possibly compromising the target. Click Play in the figure to view an example of trust exploitation.

In the animation, System A trusts System B. System B trusts everyone. The threat actor wants to gain access to System A. Therefore, the threat actor compromises System B first and then can use System B to attack System A.

Port Redirection

In a port redirection attack, a threat actor uses a compromised system as a base for attacks against other targets.

Man-in-the-Middle

In a man-in-the-middle attack, the threat actor is positioned in between two legitimate entities in order to read or modify the data that passes between the two parties. The figure displays an example of a man-in-the-middle attack.

Denial of Service Attacks

Denial of service (DoS) attacks are the most publicized form of attack and among the most difficult to eliminate. However, because of their ease of implementation and

potentially significant damage, DoS attacks deserve special attention from security administrators.

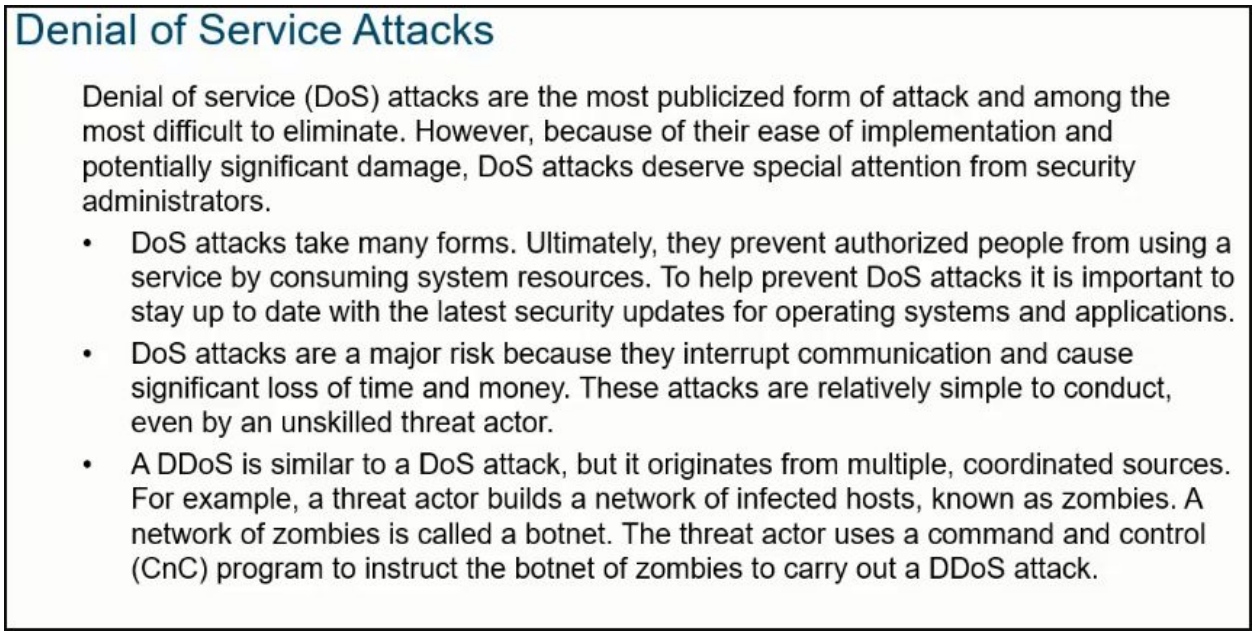
DoS attacks take many forms. Ultimately, they prevent authorized people from using a service by consuming system resources. To help prevent DoS attacks it is important to stay up to date with the latest security updates for operating systems and applications.

DoS Attack

DoS attacks are a major risk because they interrupt communication and cause significant loss of time and money. These attacks are relatively simple to conduct, even by an unskilled threat actor.

DDoS Attack

A DDoS is similar to a DoS attack, but it originates from multiple, coordinated sources. For example, a threat actor builds a network of infected hosts, known as zombies. A network of zombies is called a botnet. The threat actor uses a command and control (CnC) program to instruct the botnet of zombies to carry out a DDoS attack.



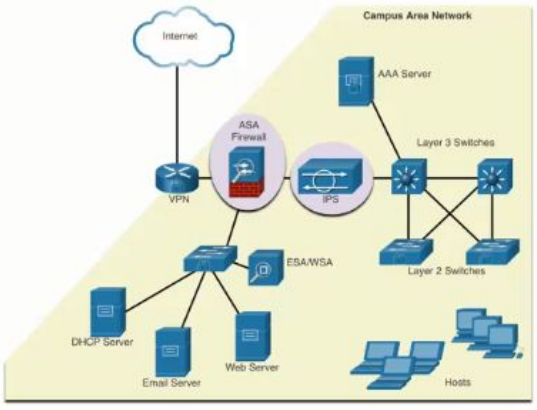
1. A denial of service (DoS) attack, if successful, prevents authorized users from accessing system resources.
2. An access attack, if successful, exploits known vulnerabilities. These attacks can allow a threat actor to gain access to resources they have no rights to access.
3. Malware attacks include viruses, worms, and Trojan horses. These types of attacks can result in crashed systems and deleted or corrupted files.
4. Malware attacks include viruses, worms, and Trojan horses. These types of attacks can allow a threat actor to take control of an infected system.
5. A denial of service (DoS) attack, if successful, prevents authorized users from accessing system resources.
6. In a reconnaissance attack, the threat actor can probe a system to find what ports are open, and what services are running.

The Defense-in-Depth Approach

To mitigate network attacks, you must first secure devices including routers, switches, servers, and hosts. Most organizations employ a defense-in-depth approach (also known as a layered approach) to security. This requires a combination of networking devices and services working in tandem.

Several security devices and services are implemented to protect an organization's users and assets against TCP/IP threats:

- VPN
- ASA Firewall
- IPS
- ESA/WSA
- AAA Server



The Defense-in-Depth Approach

Now that you know more about how threat actors can break into networks, you need to understand what to do to prevent this unauthorized access. This topic details several actions you can take to make your network more secure.

To mitigate network attacks, you must first secure devices including routers, switches, servers, and hosts. Most organizations employ a defense-in-depth approach (also known as a layered approach) to security. This requires a combination of networking devices and services working in tandem.

Consider the network in the figure. There are several security devices and services that have been implemented to protect its users and assets against TCP/IP threats.

All network devices including the router and switches are also hardened as indicated by the combination locks on their respective icons. This indicates that they have been secured to prevent threat actors from gaining access and tampering with the devices.

Keep Backups

Backing up device configurations and data is one of the most effective ways of protecting against data loss. A data backup stores a copy of the information on a computer to removable backup media that can be kept in a safe place. Infrastructure devices should have backups of configuration files and IOS images on an FTP or similar file server. If the computer or a router hardware fails, the data or configuration can be restored using the backup copy.

Backups should be performed on a regular basis as identified in the security policy. Data backups are usually stored offsite to protect the backup media if anything happens to the main facility. Windows hosts have a backup and restore utility. It is important for users to back up their data to another drive, or to a cloud-based storage provider.

The table shows backup considerations and their descriptions.

Consideration	Description
Frequency	• Perform backups on a regular basis as identified in the security policy. • Full backups can be time-consuming, therefore perform monthly or weekly backups with frequent partial backups of changed files.
Validation	• Always validate backups to ensure the integrity of the data and validate the file restoration procedures.

Storage	**● Backups should be transported to an approved offsite storage location on a daily, weekly, or monthly rotation, as required by the security policy.**
Security	**● Backups should be protected using strong passwords. The password is required to restore the data.**

16.3.3

Upgrade, Update, and Patch

Keeping up to date with the latest developments can lead to a more effective defense against network attacks. As new malware is released, enterprises need to keep current with the latest versions of antivirus software.

The most effective way to mitigate a worm attack is to download security updates from the operating system vendor and patch all vulnerable systems. Administering numerous systems involves the creation of a standard software image (operating system and accredited applications that are authorized for use on client systems) that is deployed on new or upgraded systems. However, security requirements change, and already deployed systems may need to have updated security patches installed.

One solution to the management of critical security patches is to make sure all end systems automatically download updates, as shown for Windows 10 in the figure. Security patches are automatically downloaded and installed without user intervention.

Authentication, Authorization, and Accounting

All network devices should be securely configured to provide only authorized individuals with access. Authentication, authorization, and accounting (AAA, or "triple A") network security services provide the primary framework to set up access control on network devices.

AAA is a way to control who is permitted to access a network (authenticate), what actions they perform while accessing the network (authorize), and making a record of what was done while they are there (accounting).

The concept of AAA is similar to the use of a credit card. The credit card identifies who can use it, how much that user can spend, and keeps account of what items the user spent money on

Firewalls

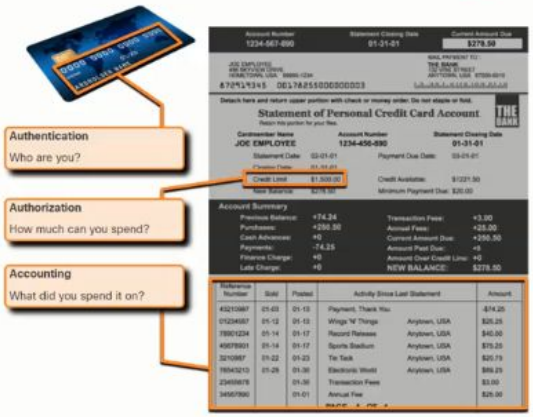
A firewall is one of the most effective security tools available for protecting users from external threats. A firewall protects computers and networks by preventing undesirable traffic from entering internal networks.

Network firewalls reside between two or more networks, control the traffic between them, and help prevent unauthorized access
A firewall could allow outside users controlled access to specific services. For example, servers accessible to outside users are usually located on a special network referred to as the demilitarized zone (DMZ),

Authentication, Authorization, and Accounting

Authentication, authorization, and accounting (AAA, or "triple A") network security services provide the primary framework to set up access control on network devices.

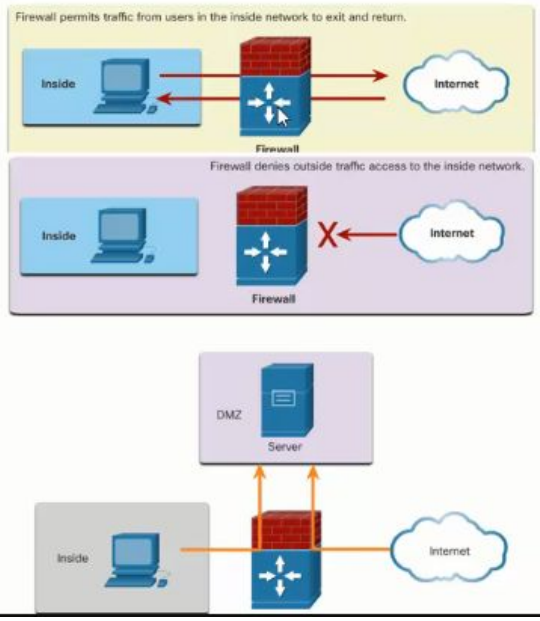
- AAA is a way to control who is permitted to access a network (authenticate), what actions they perform while accessing the network (authorize), and making a record of what was done while they are there (accounting).
- The concept of AAA is similar to the use of a credit card. The credit card identifies who can use it, how much that user can spend, and keeps account of what items the user spent money on.

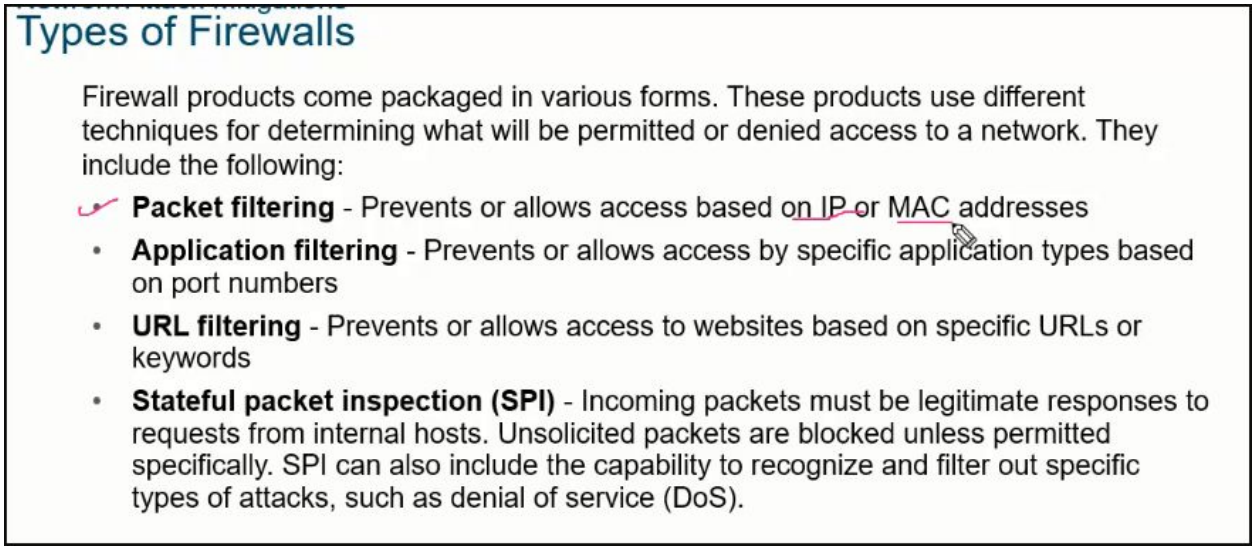


Firewalls

Network firewalls reside between two or more networks, control the traffic between them, and help prevent unauthorized access.

A firewall could allow outside users controlled access to specific services. For example, servers accessible to outside users are usually located on a special network referred to as the demilitarized zone (DMZ). The DMZ enables a network administrator to apply specific policies for hosts connected to that network.





Types of Firewalls

Firewall products come packaged in various forms. These products use different techniques for determining what will be permitted or denied access to a network. They include the following:

- **Packet filtering - Prevents or allows access based on IP or MAC addresses**
- **Application filtering - Prevents or allows access by specific application types based on port numbers**
- **URL filtering - Prevents or allows access to websites based on specific URLs or keywords**
- **Stateful packet inspection (SPI) - Incoming packets must be legitimate responses to requests from internal hosts. Unsolicited packets are blocked unless permitted specifically. SPI can also include the capability to recognize and filter out specific types of attacks, such as denial of service (DoS)**

Endpoint Security

An endpoint, or host, is an individual computer system or device that acts as a network client. Common endpoints are laptops, desktops, servers, smartphones, and tablets. Securing endpoint devices is one of the most challenging jobs of a network administrator because it involves human nature. A company must have well-documented policies in place and employees must be aware of these rules. Employees need to be trained on proper use of the network. Policies often include the use of antivirus software and host intrusion prevention. More comprehensive endpoint security solutions rely on network access control.

Endpoint Security

An endpoint, or host, is an individual computer system or device that acts as a network client. Common endpoints are laptops, desktops, servers, smartphones, and tablets.

Securing endpoint devices is one of the most challenging jobs of a network administrator because it involves human nature. A company must have well-documented policies in place and employees must be aware of these rules.

Employees need to be trained on proper use of the network. Policies often include the use of antivirus software and host intrusion prevention. More comprehensive endpoint security solutions rely on network access control.

1. A firewall is a dedicated device that helps prevent unauthorized access by not allowing external traffic to initiate connections to internal hosts.
2. AAA servers perform authentication, authorization and accounting services on behalf of other devices to manage access to resources.
3. Backup validation is concerned with using strong passwords to protect backups and for restoring data.
4. The DMZ, or demilitarized zone, is used for servers that need to be accessible to external users.
5. Antivirus software running on an endpoint or host is part of a comprehensive endpoint security solution.

Cisco AutoSecure

One area of networks that requires special attention to maintain security is the devices. You probably already have a password for your computer, smart phone, or tablet. Is it as strong as it could be? Are you using other tools to enhance the security of your devices? This topic tells you how.

The security settings are set to the default values when a new operating system is installed on a device. In most cases, this level of security is inadequate. For Cisco routers, the Cisco AutoSecure feature can be used to assist securing the system, as shown in the example.

Router# auto secure
--- AutoSecure Configuration ---
***** AutoSecure configuration enhances the security of**
the router but it will not make router absolutely secure

from all security attacks *

In addition, there are some simple steps that should be taken that apply to most operating systems:

- **Default usernames and passwords should be changed immediately.**
- **Access to system resources should be restricted to only the individuals that are authorized to use those resources.**
- **Any unnecessary services and applications should be turned off and uninstalled when possible.**

Often, devices shipped from the manufacturer have been sitting in a warehouse for a period of time and do not have the most up-to-date patches installed. It is important to update any software and install any security patches prior to implementation.

Introduction to Networks

v7.0

-
    -

1.
2. **Network Security Fundamentals**
3. **Device Security**

Device Security

16.4.1

Cisco AutoSecure

One area of networks that requires special attention to maintain security is the devices. You probably already have a password for your computer, smart phone, or tablet. Is it as strong as it could be? Are you using other tools to enhance the security of your devices? This topic tells you how.

The security settings are set to the default values when a new operating system is installed on a device. In most cases, this level of security is inadequate. For Cisco routers, the Cisco AutoSecure feature can be used to assist securing the system, as shown in the example.

Router# auto secure

--- AutoSecure Configuration ---
***** AutoSecure configuration enhances the security of the router but it will not make router absolutely secure from all security attacks *****

In addition, there are some simple steps that should be taken that apply to most operating systems:

- **Default usernames and passwords should be changed immediately.**
- **Access to system resources should be restricted to only the individuals that are authorized to use those resources.**
- **Any unnecessary services and applications should be turned off and uninstalled when possible.**

Often, devices shipped from the manufacturer have been sitting in a warehouse for a period of time and do not have the most up-to-date patches installed. It is important to update any software and install any security patches prior to implementation.

16.4.2

Passwords

To protect network devices, it is important to use strong passwords. Here are standard guidelines to follow:

- **Use a password length of at least eight characters, preferably 10 or more characters. A longer password is a more secure password.**
- **Make passwords complex. Include a mix of uppercase and lowercase letters, numbers, symbols, and spaces, if allowed.**
- **Avoid passwords based on repetition, common dictionary words, letter or number sequences, usernames, relative or pet names, biographical information, such as birthdates, ID numbers, ancestor names, or other easily identifiable pieces of information.**
- **Deliberately misspell a password. For example, Smith = Smyth = 5mYth or Security = 5ecur1ty.**
- **Change passwords often. If a password is unknowingly compromised, the window of opportunity for the threat actor to use the password is limited.**
- **Do not write passwords down and leave them in obvious places such as on the desk or monitor.**
- **On Cisco routers, leading spaces are ignored for passwords, but spaces after the first character are not. Therefore, one method to create a strong password is to use the space bar and create a phrase made of many words. This is called a passphrase. A passphrase is often easier to remember than a simple password. It is also longer and harder to guess**

Passwords

To protect network devices, it is important to use strong passwords. Here are standard guidelines to follow:

- Use a password length of at least eight characters, preferably 10 or more characters.
- Make passwords complex. Include a mix of uppercase and lowercase letters, numbers, symbols, and spaces, if allowed.
- Avoid passwords based on repetition, common dictionary words, letter or number sequences, usernames, relative or pet names, biographical information, such as birthdates, ID numbers, ancestor names, or other easily identifiable pieces of information.
- Deliberately misspell a password. For example, Smith = Smyth = 5mYth or Security = 5ecur1ty.
- Change passwords often. If a password is unknowingly compromised, the window of opportunity for the threat actor to use the password is limited.
- Do not write passwords down and leave them in obvious places such as on the desk or monitor.

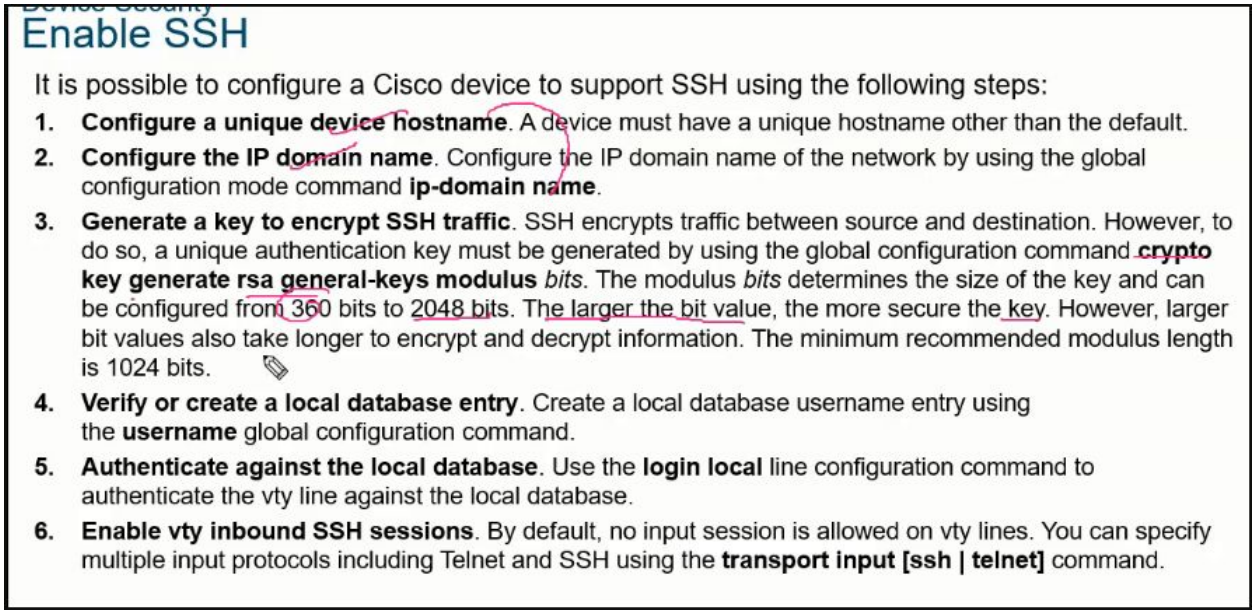
On Cisco routers, leading spaces are ignored for passwords, but spaces after the first character are not. Therefore, one method to create a strong password is to use the space bar and create a phrase made of many words. This is called a passphrase. A passphrase is often easier to remember than a simple password. It is also longer and harder to guess.

Additional Password Security

There are several steps that can be taken to help ensure that passwords remain secret on a Cisco router and switch including these:

- Encrypt all plaintext passwords with the **service password-encryption** command.
- Set a minimum acceptable password length with the **security passwords min-length** command.
- Deter brute-force password guessing attacks with the **login block-for # attempts # within #** command.
- Disable an inactive privileged EXEC mode access after a specified amount of time with the **exec-timeout** command.

```
Router(config)# service password-encryption
Router(config)# security password min-length 8
Router(config)# login block-for 120 attempts 3 within 60
Router(config)# line vty 0 4
Router(config-line)# password cisco
Router(config-line)# exec-timeout 5 30
Router(config-line)# transport input ssh
Router(config-line)# end
Router#
Router# show running-config | section line vty
line vty 0 4
 password 7 03095A0F034F
 exec-timeout 5 30
 login
Router#
```



Additional Password Security

Strong passwords are only useful if they are secret. There are several steps that can be taken to help ensure that passwords remain secret on a Cisco router and switch including these:

- **Encrypting all plaintext passwords**
- **Setting a minimum acceptable password length**
- **Deterring brute-force password guessing attacks**
- **Disabling an inactive privileged EXEC mode access after a specified amount of time.**

As shown in the sample configuration in the figure, the service password-encryption global configuration command prevents unauthorized individuals from viewing plaintext passwords in the configuration file. This command encrypts all plaintext passwords. Notice in the example, that the password "cisco" has been encrypted as "03095A0F034F".

To ensure that all configured passwords are a minimum of a specified length, use the security passwords min-length *length* command in global configuration mode. In the figure, any new password configured would have to have a minimum length of eight characters.

Threat actors may use password cracking software to conduct a brute-force attack on a network device. This attack continuously attempts to guess the valid passwords until one works. Use the login block-for # attempts # within # global configuration command to deter this type of attack. In the figure for example, the login block-for 120 attempts 3

within 60 command will block vty login attempts for 120 seconds if there are three failed login attempts within 60 seconds.

Network administrators can become distracted and accidently leave a privileged EXEC mode session open on a terminal. This could enable an internal threat actor access to change or erase the device configuration.

By default, Cisco routers will logout an EXEC session after 10 minutes of inactivity. However, you can reduce this setting using the exec-timeout *minutes seconds* line configuration command. This command can be applied online console, auxiliary, and vty lines. In the figure, we are telling the Cisco device to automatically disconnect an inactive user on a vty line after the user has been idle for 5 minutes and 30 seconds.

```
Router(config)# service password-encryption
Router(config)# security password min-length 8
Router(config)# login block-for 120 attempts 3 within 60
Router(config)# line vty 0 4
Router(config-line)# password cisco
Router(config-line)# exec-timeout 5 30
Router(config-line)# transport input ssh
Router(config-line)# end
Router#
Router# show running-config | section line vty
line vty 0 4
 password 7 03095A0F034F
 exec-timeout 5 30
 login
 transport input ssh
Router#
```

16.4.4

Enable SSH

Telnet simplifies remote device access, but it is not secure. Data contained within a Telnet packet is transmitted unencrypted. For this reason, it is highly recommended to enable Secure Shell (SSH) on devices for secure remote access.

It is possible to configure a Cisco device to support SSH using the following six steps:

Step 1. Configure a unique device hostname. A device must have a unique hostname other than the default.

Step 2. Configure the IP domain name. Configure the IP domain name of the network by using the global configuration mode command ip domain name *name*.

Step 3. Generate a key to encrypt SSH traffic. SSH encrypts traffic between source and destination. However, to do so, a unique authentication key must be generated by using the global configuration command crypto key generate rsa general-keys modulus *bits*. The modulus *bits* determines the size of the key and can be configured from 360 bits to 2048 bits. The larger the bit value, the more secure the key. However, larger bit values also take longer to encrypt and decrypt information. The minimum recommended modulus length is 1024 bits.

Step 4. Verify or create a local database entry. Create a local database username entry using the username global configuration command. In the example, the parameter secret is used so that the password will be encrypted using MD5.

Step 5. Authenticate against the local database. Use the login local line configuration command to authenticate the vty line against the local database.

Step 6. Enable vty inbound SSH sessions. By default, no input session is allowed on vty lines. You can specify multiple input protocols including Telnet and SSH using the transport input {ssh | telnet} command.

As shown in the example, router R1 is configured in the span.com domain. This information is used along with the bit value specified in the crypto key generate rsa general-keys modulus command to create an encryption key.

Next, a local database entry for a user named Bob is created. Finally, the vty lines are configured to authenticate against the local database and to only accept incoming SSH sessions.

```
Router# configure terminal
Router(config)# hostname R1
R1(config)# ip domain name span.com
R1(config)# crypto key generate rsa general-keys modulus 1024
The name for the keys will be: Rl.span.com % The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
Dec 13 16:19:12.079: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)#
R1(config)# username Bob secret cisco
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# exit
R1(config)#
```

16.4.5

Disable Unused Services

Cisco routers and switches start with a list of active services that may or may not be required in your network. Disable any unused services to preserve system resources, such as CPU cycles and RAM, and prevent threat actors from exploiting these services. The type of services that are on by default will vary depending on the IOS version. For example, IOS-XE typically will have only HTTPS and DHCP ports open. You can verify this with the show ip ports all command, as shown in the example.

```
Router# show ip ports all
Proto Local Address          Foreign Address        State      PID/Program Name
TCB      Local Address          Foreign Address        (state)
tcp   :::443                :::*                   LISTEN     309/[IOS]HTTP CORE
tcp   *:443                 *:*                    LISTEN     309/[IOS]HTTP CORE
udp   *:67                   0.0.0.0:0                         387/[IOS]DHCPD Receive
Router#
```

IOS versions prior to IOS-XE use the show control-plane host open-ports command. We mention this command because you may see it on older devices. The output is similar. However, notice that this older router has an insecure HTTP server and Telnet running. Both of these services should be disabled. As shown in the example, disable HTTP with the no ip http server global configuration command. Disable Telnet by specifying only SSH in the line configuration command, transport input ssh.

```
Router# show control-plane host open-ports
Active internet connections (servers and established)
Prot       Local Address      Foreign Address              Service    State
 tcp              *:23              *:0                Telnet   LISTEN
 tcp              *:80              *:0              HTTP CORE   LISTEN
 udp               *:67              *:0          DHCPD Receive   LISTEN
Router# configure terminal
Router(config)# no ip http server
Router(config)# line vty 0 15
Router(config-line)# transport input ssh
```

What did I learn in this module?

Security Threats and Vulnerabilities

Attacks on a network can be devastating and can result in a loss of time and money due to damage or theft of important information or assets. Intruders who gain access by modifying software or exploiting software vulnerabilities are threat actors. After the threat actor gains access to the network, four types of threats may arise: information theft, data loss and manipulation, identity theft, and disruption of service. There are three primary vulnerabilities or

weaknesses: technological, configuration, and security policy. The four classes of physical threats are: hardware, environmental, electrical, and maintenance.

Network Attacks

Malware is short for malicious software. It is code or software specifically designed to damage, disrupt, steal, or inflict “bad” or illegitimate action on data, hosts, or networks. Viruses, worms, and Trojan horses are types of malware. Network attacks can be classified into three major categories: reconnaissance, access, and denial of service. The four classes of physical threats are: hardware, environmental, electrical, and maintenance. The three types of reconnaissance attacks are: internet queries, ping sweeps, and port scans. The four types of access attacks are: password (brute-force, Trojan horse, packet sniffers), trust exploitation, port redirection, and man-in-the-middle. The two types of disruption of service attacks are: DoS and DDoS.

Network Attack Mitigation

To mitigate network attacks, you must first secure devices including routers, switches, servers, and hosts. Most organizations employ a defense-in-depth approach to security. This requires a combination of networking devices and services working together. Several security devices and services are implemented to protect an organization’s users and assets against TCP/IP threats: VPN, ASA firewall, IPS, ESA/WSA, and AAA server. Infrastructure devices should have backups of configuration files and IOS images on an FTP or similar file server. If the computer or a router hardware fails, the data or configuration can be restored using the backup copy. The most effective way to mitigate a worm attack is to download security updates from the operating system vendor and patch all vulnerable systems. To manage critical security patches, to make sure all end systems automatically download updates. AAA is a way to control who is permitted to access a network (authenticate), what they can do while they are there (authorize), and what actions they perform while accessing the network (accounting). Network firewalls reside between two or more networks, control the traffic between them, and help prevent unauthorized access. Servers accessible to outside users are usually located on a special network referred to as the DMZ. Firewalls use various techniques for determining what is permitted or denied access to a network including: packet filtering, application filtering, URL filtering and SPI. Securing endpoint devices is critical to network security. A company must have well-documented policies in place, which may include the use of antivirus software and host intrusion prevention. More comprehensive endpoint security solutions rely on network access control.

Device Security

The security settings are set to the default values when a new OS is installed on a device. This level of security is inadequate. For Cisco routers, the Cisco AutoSecure feature can be used to assist securing the system. For most OSs default usernames and passwords should be changed immediately, access to system resources should be restricted to only the individuals that are authorized to use those resources, and any unnecessary services and applications should be turned off and uninstalled when possible. To protect network devices, it is important

to use strong passwords. A pass phrase is often easier to remember than a simple password. It is also longer and harder to guess. For routers and switches, encrypt all plaintext passwords, setting a minimum acceptable password length, deter brute-force password guessing attacks, and disable an inactive privileged EXEC mode access after a specified amount of time. Configure appropriate devices to support SSH, and disable unused services.

CHAPTER 17

Cost

The cost of a switch or router is determined by its capacity and features. This includes the number and types of ports available and the backplane speed. Other factors that influence the cost are network management capabilities, embedded security technologies, and optional advanced switching technologies. The expense of cable runs required to connect every device on the network must also be considered. Another key element affecting cost considerations is the amount of redundancy to incorporate into the network.

Speed and Types of Ports/Interfaces

Choosing the number and type of ports on a router or switch is a critical decision. Newer computers have built-in 1 Gbps NICs. Some servers may even have 10 Gbps ports. Although it is more expensive, choosing Layer 2 devices that can accommodate increased speeds allows the network to evolve without replacing central devices.

Expandability

Networking devices are available in fixed and modular physical configurations. Fixed configuration devices have a specific number and type of ports or interfaces and cannot be expanded. Modular devices have expansion slots to add new modules as requirements evolve. Switches are available with additional ports for high-speed uplinks. Routers can be used to connect different types of networks. Care must be taken to select the appropriate modules and interfaces for the specific media.

Operating System Features and Services

Network devices must have operating systems that can support the organizations requirements such as the following:

- Layer 3 switching

- Network Address Translation (NAT)
- Dynamic Host Configuration Protocol (DHCP)
- Security
- Quality of service (QoS)
- Voice over IP (VoIP)

17.1.3

IP Addressing for a Small Network

When implementing a network, create an IP addressing scheme and use it. All hosts and devices within an internetwork must have a unique address.

Devices that will factor into the IP addressing scheme include the following:

- End user devices - The number and type of connection (i.e., wired, wireless, remote access)
- Servers and peripherals devices (e.g., printers and security cameras)
- Intermediary devices including switches and access points

It is recommended that you plan, document, and maintain an IP addressing scheme based on device type. The use of a planned IP addressing scheme makes it easier to identify a type of device and to troubleshoot problems, as for instance, when troubleshooting network traffic issues with a protocol analyzer.

For example, refer to the topology of a small to medium sized organization in the figure.

network topology consisting of three LANs - 192.168.1.0/24, 192.168.2.0/24, and 192.168.3.0/24 - with various end devices, connected to a router connected to the Internet cloud

192.168.1.0/24 192.168.2.0/24
192.168.3.0/24
Internet

The organization requires three user LANs (i.e., 192.168.1.0/24, 192.168.2.0/24, and 192.168.3.0/24). The organization has decided to implement a consistent IP addressing scheme for each 192.168.x.0/24 LAN using the following plan:

Device Type	Assignable IP Address Range	Summarized as …
Default gateway (Router)	192.168.x.**1** - 192.168.x.**2**	192.168.x.**0/30**
Switches (max 2)	192.168.x.**5** - 192.168.x.**6**	192.168.x.**4/30**
Access points (max 6)	192.168.x.**9** - 192.168.x.**14**	192.168.x.**8/29**

Servers (max 6)	192.168.x.**17** - 192.168.x.**22**	192.168.x.**16/29**
Printers (max 6)	192.168.x.**25** - 192.168.x.**30**	192.168.x.**24/29**
IP Phones (max 6)	192.168.x.**33** - 192.168.x.**38**	192.168.x.**32/29**
Wired devices (max 62)	192.168.x.**65** - 192.168.x.**126**	192.168.x.**64/26**
Wireless devices (max 62)	192.168.x.**193** - 192.168.x.**254**	192.168.x.**192/26**

The figure displays an example of the 192.168.2.0/24 network devices with assigned IP addresses using the predefined IP addressing scheme.

The diagram is a small LAN topology with a network address of 192.168.2.0/24. It shows various end devices all connected to a switch, with address .5, connected to a router, at address .1, connected to the Internet cloud. All devices have been assigned an IP address. A printer has an address of .25; server has an address of .17; a PC has an address of .65 connected to an IP phone with an address of .33; and a laptop has an address of .193 connected to an access point with an address of .9.

.193 .9 .5 .33 .65 .25 .17 .1
192.168.2.0/24
Internet

For instance, the default gateway IP address is 192.168.2.1/24, the switch is 192.168.2.5/24, the server is 192.168.2.17/24, etc..

Notice that the assignable IP address ranges were deliberately allocated on subnetnetwork boundaries to simplify summarizing the group type. For instance, assume another switch with IP address 192.168.2.6 is added to the network. To identify all switches in a network policy, the administrator could specify the summarized network address 192.168.x.4/30.

17.1.4

Redundancy in a Small Network

Another important part of network design is reliability. Even small businesses often rely heavily on their network for business operation. A failure of the network can be very costly.

In order to maintain a high degree of reliability, *redundancy* is required in the network design. Redundancy helps to eliminate single points of failure.

There are many ways to accomplish redundancy in a network. Redundancy can be accomplished by installing duplicate equipment, but it can also be accomplished by supplying duplicate network links for critical areas, as shown in the figure.

The diagram illustrates the use of redundant servers, links, switches, and routers in a network. Shown are four layers with an explanation of the redundancy achieved at each. The top layer has three servers and text reads: Redundant servers are available in case of server failure. The next layer shows that each server has two connections leading to two switches and text reads: Redundant links are present to provide alternate paths in case of a link failure. The next layer shows two switches connected to each other with each connected to all three servers above and text reads: Redundant switches are present in case of switch failure. The bottom layer shows two routers connected to each other with each connected to one of the switches and text reads: Redundant routers are available in case of router or route failure.

Redundant servers are available in case of server failure.Redundant links are present to provide alternate paths in case of a link failure.Redundant switches are present in case of switch failure.Redundant routers are available in case of router or route failure.

Small networks typically provide a single exit point toward the internet via one or more default gateways. If the router fails, the entire network loses connectivity to the internet. For this reason, it may be advisable for a small business to pay for a second service provider as backup.

17.1.5

Traffic Management

The goal for a good network design, even for a small network, is to enhance the productivity of the employees and minimize network downtime. The network administrator should consider the various types of traffic and their treatment in the network design.

The routers and switches in a small network should be configured to support real-time traffic, such as voice and video, in an appropriate manner relative to other data traffic. In fact, a good network design will implement quality of service (QoS) to classify traffic carefully according to priority during times of congestion,

17.2.1

Common Applications

The previous topic discussed the components of a small network, as well as some of the design considerations. These considerations are necessary when you are just setting up a network. After you have set it up, your network still needs certain types of applications and protocols in order to work.

The network is only as useful as the applications that are on it. There are two forms of software programs or processes that provide access to the network: network applications and application layer services.

Network Applications

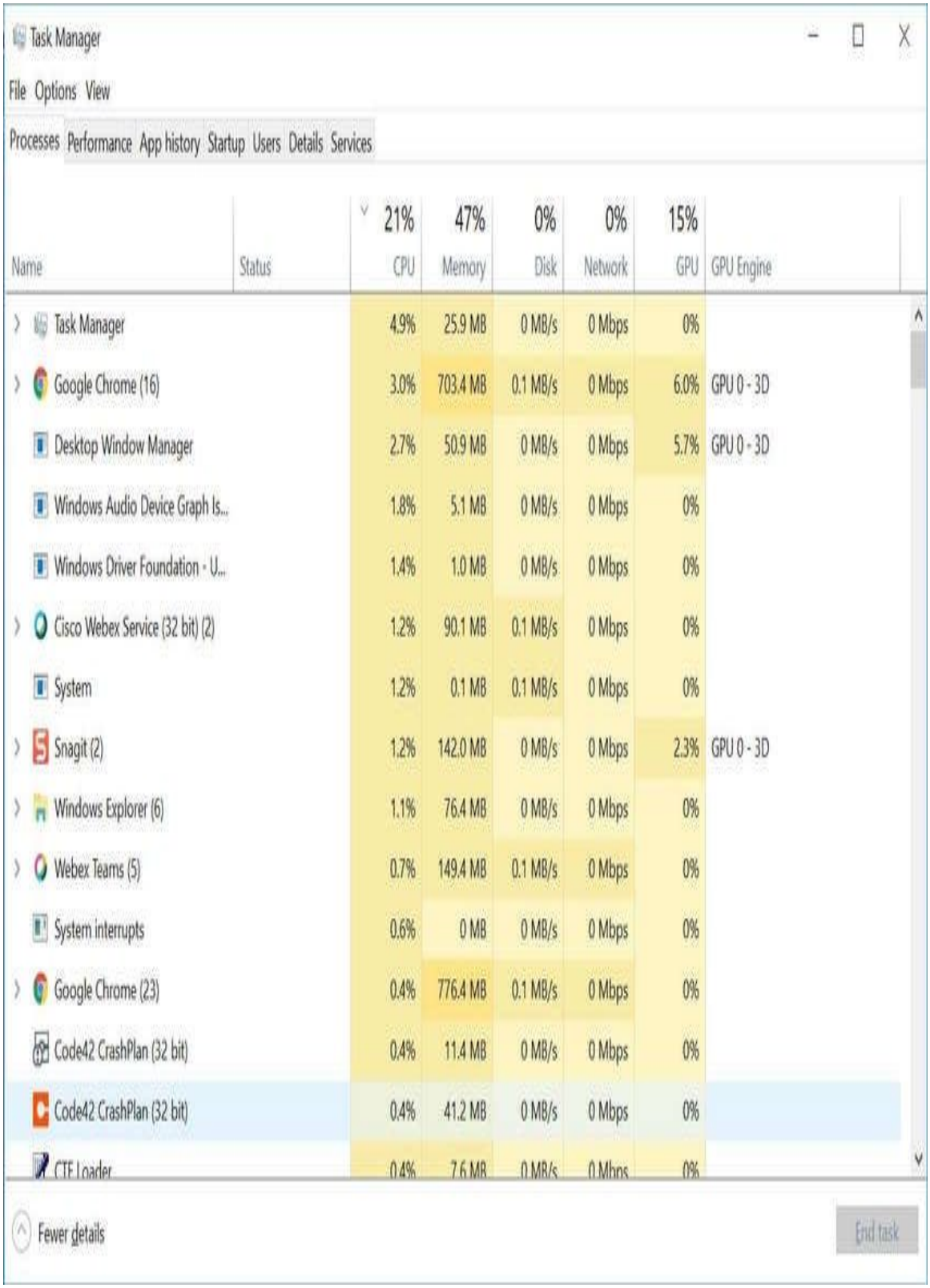
Applications are the software programs used to communicate over the network. Some end-user applications are network-aware, meaning that they implement application layer protocols and are able to communicate directly with the lower layers of the protocol stack. Email clients and web browsers are examples of this type of application.

Application Layer Services

Other programs may need the assistance of application layer services to use network resources like file transfer or network print spooling. Though transparent to an employee, these services are the programs that interface with the network and prepare the data for transfer. Different types of data, whether text, graphics or video, require different network services to ensure that they are properly prepared for processing by the functions occurring at the lower layers of the OSI model.

Each application or network service uses protocols, which define the standards and data formats to be used. Without protocols, the data network would not have a common way to format and direct data. In order to understand the function of various network services, it is necessary to become familiar with the underlying protocols that govern their operation.

Use the Task Manager to view the current applications, processes, and services running on a Windows PC, as shown in the figure.


Task Manager
File Options View
Processes Performance App history Startup Users Details Services
Name Status 21% CPU 47% Memory 0% Disk 0% Network 15% GPU GPU Engine
Task Manager 4.9% 25.9 MB 0 MB/s 0 Mbps 0%
Google Chrome (16) 3.0% 703.4 MB 0.1 MB/s 0 Mbps 6.0% GPU 0 - 3D
Desktop Window Manager 2.7% 50.9 MB 0 MB/s 0 Mbps 5.7% GPU 0 - 3D
Windows Audio Device Graph Is... 1.8% 5.1 MB 0 MB/s 0 Mbps 0%
Windows Driver Foundation - U... 1.4% 1.0 MB 0 MB/s 0 Mbps 0%
Cisco Webex Service (32 bit) (2) 1.2% 90.1 MB 0.1 MB/s 0 Mbps 0%
System 1.2% 0.1 MB 0.1 MB/s 0 Mbps 0%
Snagit (2) 1.2% 142.0 MB 0 MB/s 0 Mbps 2.3% GPU 0 - 3D
Windows Explorer (6) 1.1% 76.4 MB 0 MB/s 0 Mbps 0%
Webex Teams (5) 0.7% 149.4 MB 0.1 MB/s 0 Mbps 0%
System interrupts 0.6% 0 MB 0 MB/s 0 Mbps 0%
Google Chrome (23) 0.4% 776.4 MB 0.1 MB/s 0 Mbps 0%
Code42 CrashPlan (32 bit) 0.4% 11.4 MB 0 MB/s 0 Mbps 0%
Code42 CrashPlan (32 bit) 0.4% 41.2 MB 0 MB/s 0 Mbps 0%
CTF Loader 0.4% 7.6 MB 0 MB/s 0 Mbps 0%
Fewer details
End task

17.2.2

Common Protocols

Most of a technician's work, in either a small or a large network, will in some way be involved with network protocols. Network protocols support the applications and services used by employees in a small network.

Network administrators commonly require access to network devices and servers. The two most common remote access solutions are Telnet and Secure Shell (SSH). SSH service is a secure alternative to Telnet. When connected, administrators can access the SSH server device as though they were logged in locally.

SSH is used to establish a secure remote access connection between an SSH client and other SSH-enabled devices:

- **Network device** - The network device (e.g., router, switch, access point, etc.) must support SSH to provide remote access SSH server services to clients.
- **Server** - The server (e.g., web server, email server, etc.) must support remote access SSH server services to clients.

Network administrators must also support common network servers and their required related network protocols, as shown in the figure.

Web ServerEmail ServerFTP ServerDHCP ServerDNS Server

Click each button for more information about common network servers and their required related network protocols.

Web Server

- Web clients and web servers exchange web traffic using the Hypertext Transfer Protocol (HTTP).
- Hypertext Transfer Protocol Secure (HTTPS) is used for secure web communication.

Note: A server could provide multiple network services. For instance, a server could be an email, FTP, and SSH server.

These network protocols comprise the fundamental toolset of a network professional. Each of these network protocols define:

- Processes on either end of a communication session
- Types of messages
- Syntax of the messages
- Meaning of informational fields
- How messages are sent and the expected response
- Interaction with the next lower layer

Many companies have established a policy of using secure versions (e.g., SSH, SFTP, and HTTPS) of these protocols whenever possible.

17.2.3

Voice and Video Applications

Businesses today are increasingly using IP telephony and streaming media to communicate with customers and business partners. Many organizations are enabling their employees to work remotely. As the figure shows, many of their users still require access to corporate software and files, as well as support for voice and video applications.

The network administrator must ensure the proper equipment is installed in the network and that the network devices are configured to ensure priority delivery.

Click each button for more information about the factors that a small network administrator must consider when supporting real-time applications.

Infrastructure

- The network infrastructure must support the real-time applications.
- Existing devices and cabling must be tested and validated.
- Newer networking products may be required.

VoIP

- VoIP devices convert analog telephone signals into digital IP packets.
- Typically, VOIP is less expensive than an IP telephony solution, but the quality of communications does not meet the same standards.
- Small network voice and video over IP can be solved using Skype and non-enterprise versions of Cisco WebEx.

IP Telephony

- An IP phone performs voice-to-IP conversion with the use of a dedicated server for call control and signaling.
- Many vendors provide small business IP telephony solutions such as the Cisco Business Edition 4000 Series products.

Real-Time Applications

- The network must support quality of service (QoS) mechanisms to minimize latency issues for real-time streaming applications.
- Real-Time Transport Protocol (RTP) and Real-Time Transport Control Protocol (RTCP) are two protocols that support this requirement.

Small Network Growth

If your network is for a small business, presumably, you want that business to grow, and your network to grow along with it. This is called scaling a network, and there are some best practices for doing this.

Growth is a natural process for many small businesses, and their networks must grow accordingly. Ideally, the network administrator has enough lead-time to make intelligent decisions about growing the network in alignment with the growth of the company.

To scale a network, several elements are required:

- **Network documentation** - Physical and logical topology
- **Device inventory** - List of devices that use or comprise the network
- **Budget** - Itemized IT budget, including fiscal year equipment purchasing budget
- **Traffic analysis** - Protocols, applications, and services and their respective traffic requirements should be documented

These elements are used to inform the decision-making that accompanies the scaling of a small network.

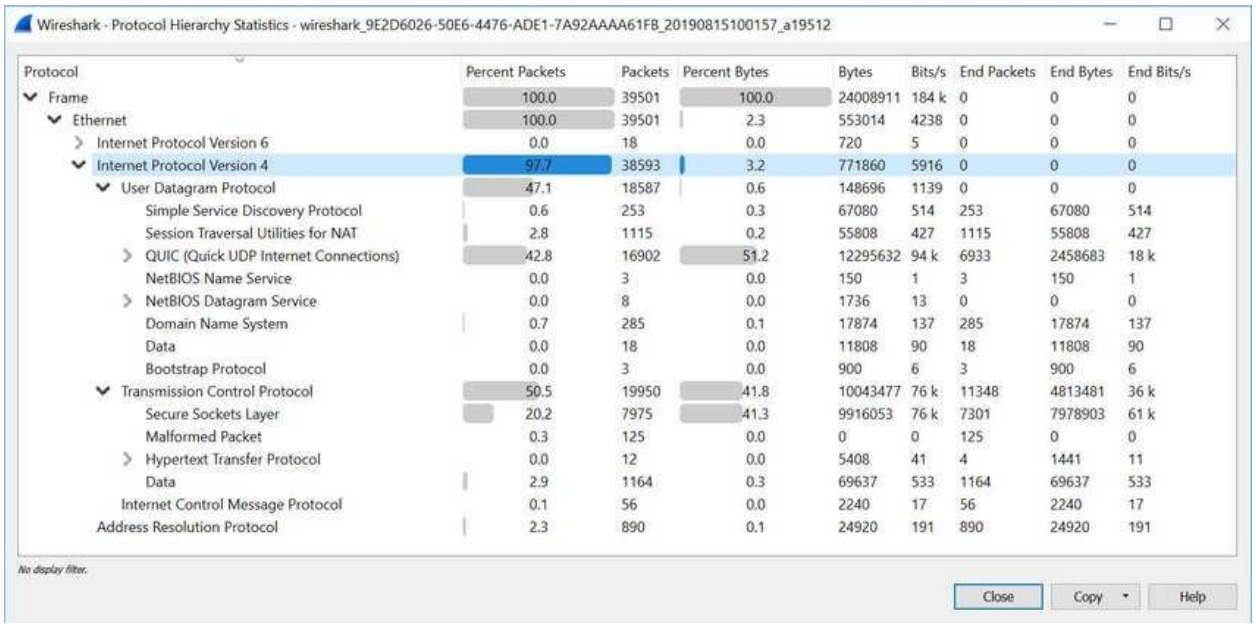
17.3.2

Protocol Analysis

As the network grows, it becomes important to determine how to manage network traffic. It is important to understand the type of traffic that is crossing the network as well as the current traffic flow. There are several network management tools that can be used for this purpose. However, a simple protocol analyzer such as Wireshark can also be used.

For instance, running Wireshark on several key hosts can reveal the types of network traffic flowing through the network. The following figure displays Wireshark protocol hierarchy statistics for a Windows host on a small network.

screen capture of Wireshark protocol hierarchy statistics for traffic captured by a host



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	39501	100.0	24008911	184 k	0	0	0
Ethernet	100.0	39501	2.3	553014	4238	0	0	0
Internet Protocol Version 6	0.0	18	0.0	720	5	0	0	0
Internet Protocol Version 4	97.7	38593	3.2	771860	5916	0	0	0
User Datagram Protocol	47.1	18587	0.6	148696	1139	0	0	0
Simple Service Discovery Protocol	0.6	253	0.3	67080	514	253	67080	514
Session Traversal Utilities for NAT	2.8	1115	0.2	55808	427	1115	55808	427
QUIC (Quick UDP Internet Connections)	42.8	16902	51.2	12295632	94 k	6933	2458683	18 k
NetBIOS Name Service	0.0	3	0.0	150	1	3	150	1
NetBIOS Datagram Service	0.0	8	0.0	1736	13	0	0	0
Domain Name System	0.7	285	0.1	17874	137	285	17874	137
Data	0.0	18	0.0	11808	90	18	11808	90
Bootstrap Protocol	0.0	3	0.0	900	6	3	900	6
Transmission Control Protocol	50.5	19950	41.8	10043477	76 k	11348	4813481	36 k
Secure Sockets Layer	20.2	7975	41.3	9916053	76 k	7301	7978903	61 k
Malformed Packet	0.3	125	0.0	0	0	125	0	0
Hypertext Transfer Protocol	0.0	12	0.0	5408	41	4	1441	11
Data	2.9	1164	0.3	69637	533	1164	69637	533
Internet Control Message Protocol	0.1	56	0.0	2240	17	56	2240	17
Address Resolution Protocol	2.3	890	0.1	24920	191	890	24920	191

The screen capture reveals the host is using IPv6 and IPv4 protocols. The IPv4 specific output also reveals that the host has used DNS, SSL, HTTP, ICMP, and other protocols.

To determine traffic flow patterns, it is important to do the following:

- Capture traffic during peak utilization times to get a good representation of the different traffic types.
- Perform the capture on different network segments and devices as some traffic will be local to a particular segment.

Information gathered by the protocol analyzer is evaluated based on the source and destination of the traffic, as well as the type of traffic being sent. This analysis can be used to make decisions on how to manage the traffic more efficiently. This can be done by reducing unnecessary traffic flows or changing flow patterns altogether by moving a server, for example.

Sometimes, simply relocating a server or service to another network segment improves network performance and accommodates the growing traffic needs. At other times, optimizing the network performance requires major network redesign and intervention.

17.3.3

Employee Network Utilization

In addition to understanding changing traffic trends, a network administrator must be aware of how network use is changing. Many operating systems provide built-in tools to display such information. For example, a Windows host provides tools such as the Task Manager, Event Viewer, and Data Usage tools.

These tools can be used to capture a “snapshot” of information such as the following:

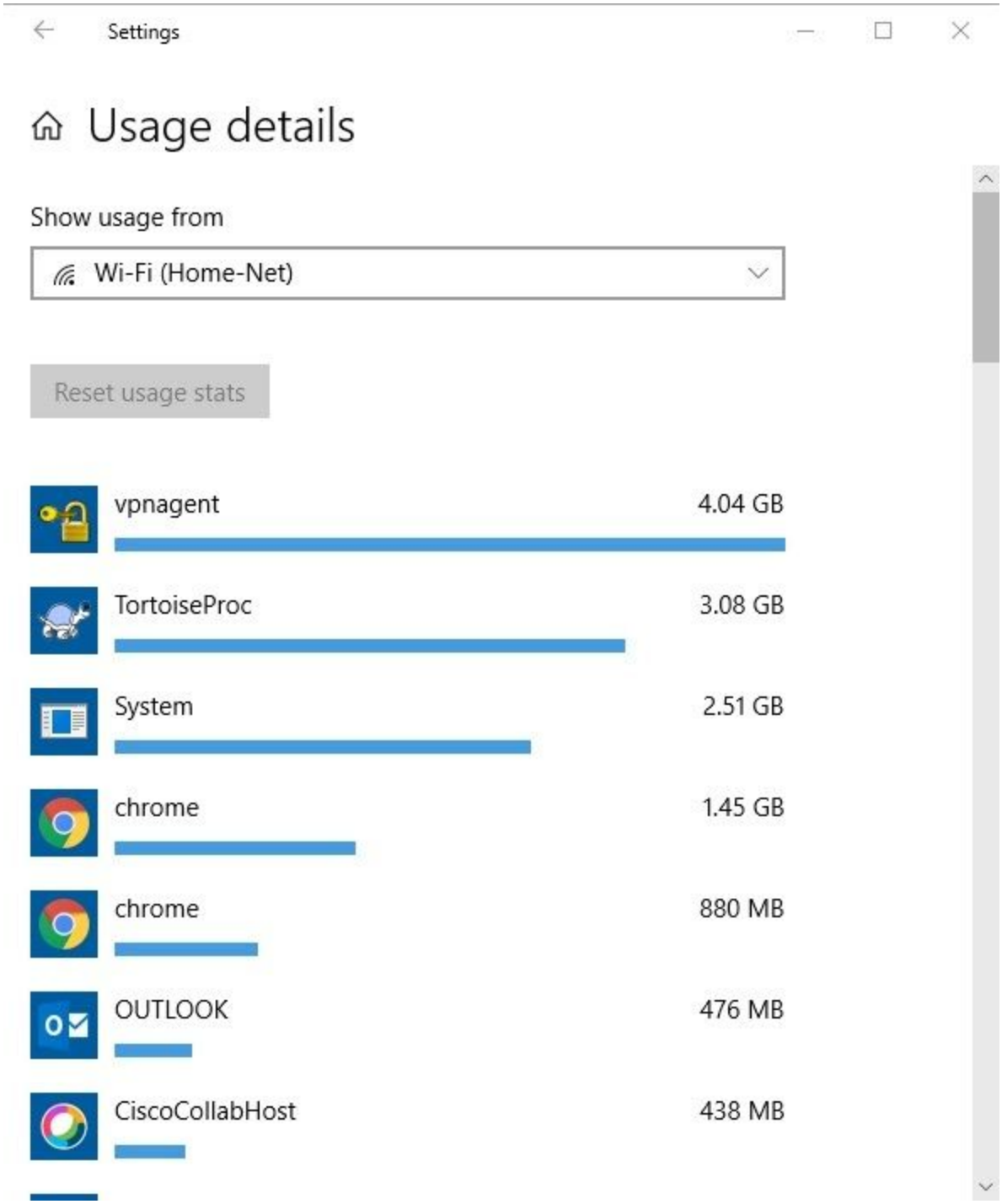
- OS and OS Version
- CPU utilization
- RAM utilization
- Drive utilization
- Non-Network applications
- Network applications

Documenting snapshots for employees in a small network over a period of time is very useful to identify evolving protocol requirements and associated traffic flows. A shift in resource utilization may require the network administrator to adjust network resource allocations accordingly.

The Windows 10 Data Usage tool is especially useful to determine which applications are using network services on a host. The Data Usage tool is accessed using **Settings > Network & Internet > Data usage > network interface** (from the last 30 days).

The example in the figure is displaying the applications running on a remote user Windows 10 host using the local Wi-Fi network connection.

screen capture of the Windows 10 Data Usage Tool showing usage from a local Wi-Fi connection


Settings
Usage details
Show usage from
Wi-Fi (Home-Net)
Reset usage stats
vpnagent
4.04 GB
TortoiseProc
3.08 GB
System
2.51 GB
chrome
1.45 GB
chrome
880 MB
OUTLOOK
476 MB
CiscoCollabHost
438 MB

Small Network Topologies

- The majority of businesses are small most of the business networks are also small.
- A small network design is usually simple.
- Small networks typically have a single WAN connection provided by DSL, cable, or an Ethernet connection.
- Large networks require an IT department to maintain, secure, and troubleshoot network devices and to protect organizational data. Small networks are managed by a local IT technician or by a contracted professional.

Device Selection for a Small Network

Like large networks, small networks require planning and design to meet user requirements. Planning ensures that all requirements, cost factors, and deployment options are given due consideration. One of the first design considerations is the type of intermediary devices to use to support the network.

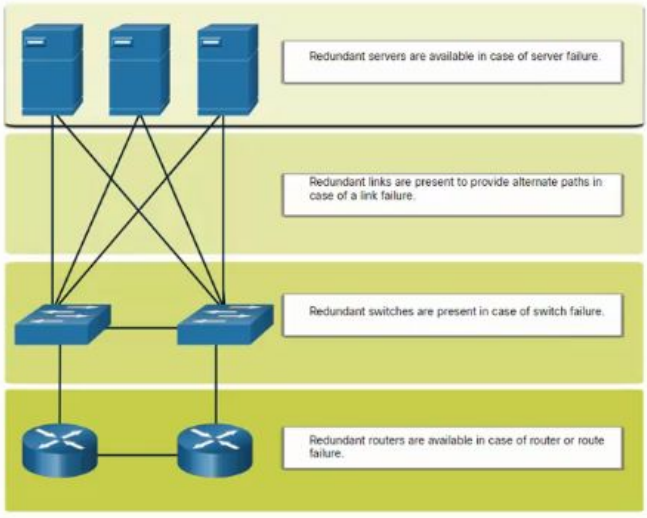
Factors that must be considered when selecting network devices include:

- cost
- speed and types of ports/interfaces
- expandability
- operating system features and services

Redundancy in a Small Network

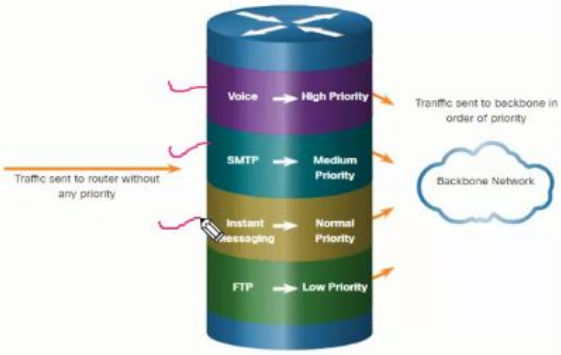
In order to maintain a high degree of reliability, *redundancy* is required in the network design. Redundancy helps to eliminate single points of failure.

Redundancy can be accomplished by installing duplicate equipment. It can also be accomplished by supplying duplicate network links for critical areas.



Traffic Management

- The goal for a good network design is to enhance the productivity of the employees and minimize network downtime.
- The routers and switches in a small network should be configured to support real-time traffic, such as voice and video, in an appropriate manner relative to other data traffic. A good network design will implement quality of service (QoS).
- Priority queuing has four queues. The high-priority queue is always emptied first.

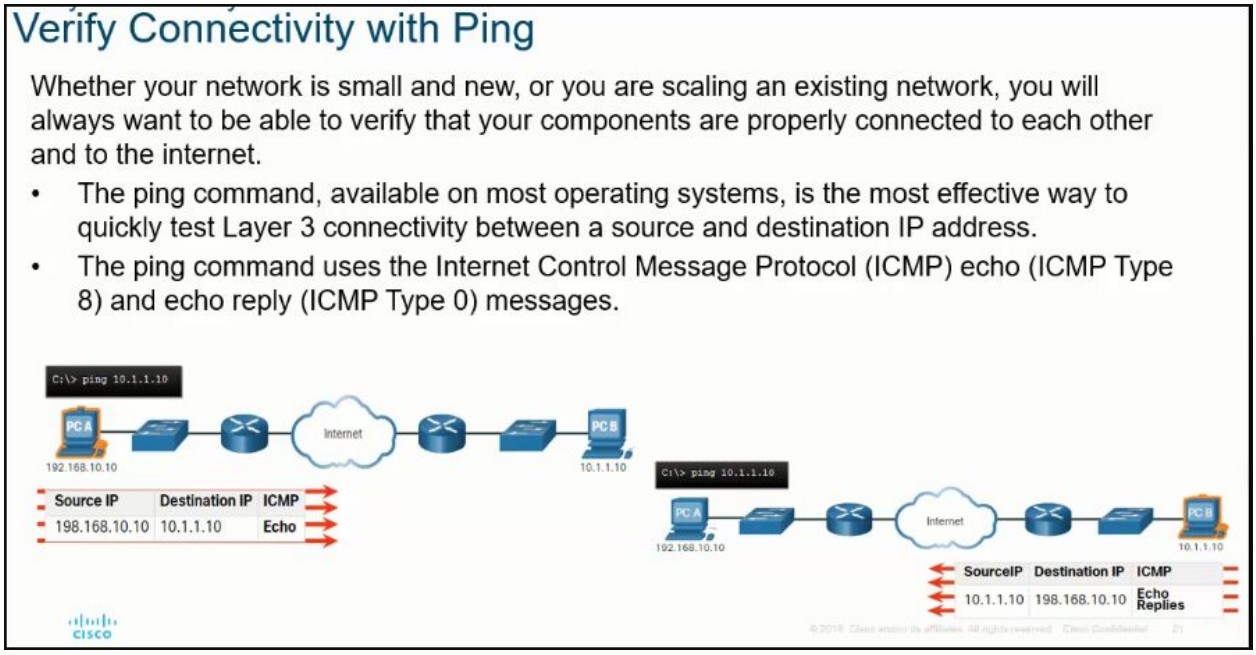


Common Protocols

Network protocols support the applications and services used by employees in a small network.

- Network administrators commonly require access to network devices and servers. The two most common remote access solutions are Telnet and Secure Shell (SSH).
- Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol Secure (HTTP) are used between web clients and web servers.
- Simple Mail Transfer Protocol (SMTP) is used to send email, Post Office Protocol (POP3) or Internet Mail Access Protocol (IMAP) are used by clients to retrieve email.
- File Transfer Protocol (FTP) and Security File Transfer Protocol (SFTP) are used to download and upload files between a client and an FTP server.
- Dynamic Host Configuration Protocol (DHCP) is used by clients to acquire an IP configuration from a DHCP Server.
- The Domain Name Service (DNS) resolves domain names to IP addresses.

Note: A server could provide multiple network services. For instance, a server could be an email, FTP and SSH server.



Verify Connectivity with Ping

Whether your network is small and new, or you are scaling an existing network, you will always want to be able to verify that your components are properly connected to each other and to the internet. This topic discusses some utilities that you can use to ensure that your network is connected.

The ping command is the most effective way to quickly test Layer 3 connectivity between a source and destination IP address. The command also displays various round-trip time statistics.

Specifically, the ping command uses the Internet Control Message Protocol (ICMP) echo request (ICMP Type 8) and echo reply (ICMP Type 0) messages. The ping command is available in most operating systems including Windows, Linux, macOS, and Cisco IOS.

On a Windows 10 host, the ping command sends four consecutive ICMP echo request messages and expects four consecutive ICMP echo replies from the destination.

For example, assume PC A pings PC B. As shown in the figure, the PC A Windows host sends four consecutive ICMP echo request messages. sometimes referred to as an ICMP echo, to PC B (i.e., 10.1.1.10).

The diagram shows host PC A, at address 192.168.10.10, using the ping 10.1.1.10 command from the command prompt to send four ICMP echo messages with a source IP of 198.168.10.10 (should read 192.168.10.10) and a destination IP of 10.1.1.10, which is host PC B on another network.

192.168.10.10 PC A PC B C:\> ping 10.1.1.10
10.1.1.10

Source IP	Destination IP	ICMP
192.168.10.10	10.1.1.10	Echo

Internet

The destination host receives and processes the ICMP echos. As shown in the figure, PC B responds by sending four ICMP echo reply messages to PC A.

The diagram shows host PC B, at address 10.1.1.0, sending four ICMP echo replies with source IP 10.1.1.10 and destination IP 198.168.10.10 (should read 192.168.10.10) in response to a ping from host PC A at address 192.168.10.10.

PC A PC B C:\> ping 10.1.1.10 10.1.1.10
192.168.10.10

SourceIP	Destination IP	ICMP
10.1.1.10	192.168.10.10	Echo Replies

Internet

As shown in the command output, PC A has received echo replies from PC-B verifying the Layer 3 network connection.

C:\Users\PC-A> ping 10.1.1.10
Pinging 10.1.1.10 with 32 bytes of data:
Reply from 10.1.1.10: bytes=32 time=47ms TTL=51
Reply from 10.1.1.10: bytes=32 time=60ms TTL=51
Reply from 10.1.1.10: bytes=32 time=53ms TTL=51
Reply from 10.1.1.10: bytes=32 time=50ms TTL=51
Ping statistics for 10.1.1.10:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 47ms, Maximum = 60ms, Average = 52ms
C:\Users\PC-A>

The output validates Layer 3 connectivity between PC A and PC B.

A Cisco IOS ping command output varies from a Windows host. For instance, the IOS ping sends five ICMP echo messages, as shown in the output.

R1# ping 10.1.1.10
Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.1.1.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
R1#

Notice the !!!!! output characters. The IOS ping command displays an indicator for each ICMP echo reply received. The table lists the most common output characters from the ping command.

IOS Ping Indicators

Element	Description
!	● **Exclamation mark indicates successful receipt of an echo reply message.** ● **It validates a Layer 3 connection between source and destination.**
.	● **A period means that time expired waiting for an echo reply message.** ● **This indicates a connectivity problem occurred somewhere along the path.**
U	● **Uppercase U indicates a router along the path responded with an ICMP Type 3 "destination unreachable" error message.** ● **Possible reasons include the router does not know the direction to the destination network or it could not find the host on the destination network.**

Note: Other possible ping replies include Q, M, ?, or &. However, the meaning of these are out of scope for this module.

17.4.2

Extended Ping

A standard ping uses the IP address of the interface closest to the destination network as the source of the ping. The source IP address of the ping 10.1.1.10 command on R1 would be that of the G0/0/0 interface (i.e., 209.165.200.225), as illustrated in the example.

The diagram shows how a router uses a standard ping to ping a host by sending four consecutive ICMP echo messages sourced from the interface closest to the destination. Router R1 is connected to two networks: on the left is 192.168.10.0/24 on interface G0/0/1 with address .1 and on the right is network 209.165.200.224/30 on interface G0/0/0 with

address .225. The latter network is connected to R2 which is connected to network 10.1.1.0/24 on which host PC B is attached with address .10. R1 is sending PC B four ICMP echo messages with a source IP of 209.165.200.225 and a destination IP of 10.1.1.10.

R2 .10 .1 G0/0/0 .10 209.165.200.224 /30 192.168.10.0 /24 10.1.1.0/24 .225 G0/0/1 PC A PC B R1

Source IP	Destination IP	ICMP
209.165.200.225	10.1.1.10	Echo

The Cisco IOS offers an "extended" mode of the ping command. This mode enables the user to create special type of pings by adjusting parameters related to the command operation.

Extended ping is entered in privileged EXEC mode by typing ping without a destination IP address. You will then be given several prompts to customize the extended ping.

Note: Pressing Enter accepts the indicated default values.

For example, assume you wanted to test connectivity from the R1 LAN (i.e., 192.168.10.0/24) to the 10.1.1.0 LAN. This could be verified from the PC A. However, an extended ping could be configured on R1 to specify a different source address.

As illustrated in the example, the source IP address of the extended ping command on R1 could be configured to use the G0/0/1 interface IP address (i.e., 192.168.10.1).

The diagram shows how a router uses an extended ping command to ping a host by sending four consecutive ICMP echo messages with a specified source IP address. Router R1 is connected to two networks: on the left is 192.168.10.0/24 on interface G0/0/1 with address .1 and on the right is network 209.165.200.224/30 on interface G0/0/0 with address .225. The latter network is connected to R2 which is connected to network 10.1.1.0/24 on which host PC B is attached with address .10. R1 is sending PC B four ICMP echo messages with a source IP of 192.168.10.1 and a destination IP of 10.1.1.10.

R2 .10 .1 G0/0/0 .10 209.165.200.224 /30 192.168.10.0 /24 10.1.1.0/24 .225 G0/0/1 PC A PC B R1

Source IP	Destination IP	ICMP
192.168.10.1	10.1.1.10	Echo

The following command output configures an extended ping on R1 and specifies the source IP address to be that of the G0/0/1 interface (i.e., 192.168.10.1).

R1# ping
Protocol [ip]:
Target IP address: 10.1.1.10
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Ingress ping [n]:
Source address or interface: 192.168.10.1
DSCP Value [0]:
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0x0000ABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.10.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
R1#

Note: The ping ipv6 command is used for IPv6 extended pings.

17.4.3

Verify Connectivity with Traceroute

The ping command is useful to quickly determine if there is a Layer 3 connectivity problem. However, it does not identify where the problem is located along the path.

Traceroute can help locate Layer 3 problem areas in a network. A trace returns a list of hops as a packet is routed through a network. It could be used to identify the point along the path where the problem can be found.

The syntax of the trace command varies between operating systems, as illustrated in the figure.

The diagram shows the difference between the trace command as issued from a Windows host versus a Cisco IOS router. The network topology consists of a host PC A connected to a switch connected to router R1 connected to router R2 connected to router R3 connected to a switch connected to host PC B. PC A, at IP address 192.168.10.10, is

issuing the following command from a Windows command prompt: C:>:tracert 10.1.1.10. R1 is issuing the following command from the Cisco IOS CLI: R#traceroute 10.1.1.10.

Windows and Cisco IOS Trace Commands

PC A PC B 10.1.1.10 192.168.10.10 .1 R3 R2
R1
Trace from Windows host
C:\>:tracert 10.1.1.10
Trace from a Cisco IOS router
R# traceroute 10.1.1.10

The following is a sample output of tracert command on a Windows 10 host.

```
C:\Users\PC-A> tracert 10.1.1.10
Tracing route to 10.1.10 over a maximum of 30 hops:
  1    2 ms    2 ms    2 ms  192.168.10.1
  2    *       *       *     Request timed out.
  3    *       *       *     Request timed out.
  4    *       *       *     Request timed out.
^C
C:\Users\PC-A>
```

Note: Use Ctrl-C to interrupt a tracert in Windows.

The only successful response was from the gateway on R1. Trace requests to the next hop timed out as indicated by the asterisk (*), meaning that the next hop router did not respond. The timed out requests indicate that there is a failure in the internetwork beyond the LAN, or that these routers have been configured to not respond to echo requests used in the trace. In this example there appears to be a problem between R1 and R2.

A Cisco IOS traceroute command output varies from the Windows tracert command. For instance, refer to the following topology.

The diagram shows a network topology with the IP addressing of router interfaces and a traceroute command issued from a Cisco IOS router. The topology consists of the following devices and networks, from left to right. A switch on network 192.168.10.0/24 is connected to router R1 at an interface with an address of .1. R1 is connected to router R2 by network 209.165.200.224/30. The interface on R1 has an address of .225 and the interface on R2 has an address of .226. R2 is connected to router R3 by network 209.165.200.228/30. The interface on R2 has an address of .229 and the interface on R3 has an address of .230. R3 is connected to a switch which is connected to host PC B with address 10.1.1.10. R1 is issuing the following trace command from the CLI: R1# traceroute 10.1.1.10.

PC B 10.1.1.10 192.168.10.0 /24 .1 R3 R1 .225 .226 .229 R2 .230 209.165.200.224 /30 209.165.200.228 /30
R1
Trace from a Cisco IOS router
R1# traceroute 10.1.1.10

The following is a sample output of traceroute command from R1.

```
R1# traceroute 10.1.1.10
Type escape sequence to abort.
Tracing the route to 10.1.1.10
VRF info: (vrf in name/id, vrf out name/id)
  1 209.165.200.226 1 msec 0 msec 1 msec
  2 209.165.200.230 1 msec 0 msec 1 msec
  3 10.1.1.10 1 msec 0 msec
R1#
```

In this example, the trace validated that it could successfully reach PC B.

Timeouts indicate a potential problem. For instance, if the 10.1.1.10 host was not available, the traceroute command would display the following output.

```
R1# traceroute 10.1.1.10
Type escape sequence to abort.
Tracing the route to 10.1.1.10
VRF info: (vrf in name/id, vrf out name/id)
  1 209.165.200.226 1 msec 0 msec 1 msec
  2 209.165.200.230 1 msec 0 msec 1 msec
  3  *  *  *
  4  *  *  *
  5  *
```

Use Ctrl-Shift-6 to interrupt a traceroute in Cisco IOS.

Note: Windows implementation of traceroute (tracert) sends ICMP Echo Requests. Cisco IOS and Linux use UDP with an invalid port number. The final destination will return an ICMP port unreachable message.

17.4.4

Extended Traceroute

Like the extended ping command, there is also an extended traceroute command. It allows the administrator to adjust parameters related to the command operation. This is helpful in locating the problem when troubleshooting routing loops, determining the

exact next-hop router, or determining where packets are getting dropped or denied by a router or firewall.

The Windows tracert command allows the input of several parameters through options in the command line. However, it is not guided like the extended traceroute IOS command. The following output displays the available options for the Windows tracert command.

```
C:\Users\PC-A> tracert /?
Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
               [-R] [-S srcaddr] [-4] [-6] target_name
Options:
   -d                 Do not resolve addresses to hostnames.
   -h maximum_hops    Maximum number of hops to search for target.
   -j host-list       Loose source route along host-list (IPv4-only).
   -w timeout         Wait timeout milliseconds for each reply.
   -R                 Trace round-trip path (IPv6-only).
   -S srcaddr         Source address to use (IPv6-only).
   -4                 Force using IPv4.
   -6                 Force using IPv6.
C:\Users\PC-A>
```

The Cisco IOS extended traceroute option enables the user to create a special type of trace by adjusting parameters related to the command operation. Extended traceroute is entered in privileged EXEC mode by typing traceroute without a destination IP address. IOS will guide you through the command options by presenting a number of prompts related to the setting of all the different parameters.

Note: Pressing Enter accepts the indicated default values.

For example, assume you want to test connectivity to PC B from the R1 LAN. Although this could be verified from PC A, an extended traceroute could be configured on R1 to specify a different source address.

The diagram shows a network topology with the IP addressing of router interfaces and an extended traceroute command issued from a Cisco IOS router. The topology consists of the following devices and networks, from left to right. A switch on network 192.168.10.0/24 is connected to router R1 at an interface with an address of .1. R1 is connected to router R2 by network 209.165.200.224/30. The interface on R1 has an address of .225 and the interface on R2 has an address of .226. R2 is connected to router R3 by network 209.165.200.228/30. The interface on R2 has an address of .229 and the interface on R3 has an address of .230. R3 is connected to a switch which is connected to host PC B with address 10.1.1.10. R1 is issuing the following trace command from the CLI: R1# traceroute.

PC B 192.168.10.0/24 209.165.200.224/30 209.165.200.228/30 10.1.1.10 R1 R3 R2 .1 .225 .226 .229 .230

Extended trace from a Cisco IOS router

```
R1# traceroute
```

As illustrated in the example, the source IP address of the extended traceroute command on R1 could be configured to use the R1 LAN interface IP address (i.e., 192.168.10.1).

```
R1# traceroute
Protocol [ip]:
Target IP address: 10.1.1.10
Ingress traceroute [n]:
Source address: 192.168.10.1
DSCP Value [0]:
Numeric display [n]:
Timeout in seconds [3]:
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Port Number [33434]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Type escape sequence to abort.
Tracing the route to 192.168.10.10
VRF info: (vrf in name/id, vrf out name/id)
  1 209.165.200.226 1 msec 1 msec 1 msec
  2 209.165.200.230 0 msec 1 msec 0 msec
  3  *
    10.1.1.10 2 msec 2 msec
R1#
```

17.4.5

Network Baseline

One of the most effective tools for monitoring and troubleshooting network performance is to establish a network baseline. Creating an effective network performance baseline is accomplished over a period of time. Measuring performance at varying times and loads will assist in creating a better picture of overall network performance.

The output derived from network commands contributes data to the network baseline. One method for starting a baseline is to copy and paste the results from an executed ping, trace, or other relevant commands into a text file. These text files can be time stamped with the date and saved into an archive for later retrieval and comparison.

Among items to consider are error messages and the response times from host to host. If there is a considerable increase in response times, there may be a latency issue to address.

For example, the following ping output was captured and pasted into a text file.

August 19, 2019 at 08:14:43

```
C:\Users\PC-A> ping 10.1.1.10
Pinging 10.1.1.10 with 32 bytes of data:
Reply from 10.1.1.10: bytes=32 time<1ms TTL=64
Reply from 10.1.1.10: bytes=32 time<1ms TTL=64
Reply from 10.1.1.10: bytes=32 time<1ms TTL=64
Reply from 10.1.1.10: bytes=32 time<1ms TTL=64
Ping statistics for 10.1.1.10:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Users\PC-A>
```

Notice the ping round-trip times are less than 1 ms.

A month later, the ping is repeated and captured.

September 19, 2019 at 10:18:21

```
C:\Users\PC-A> ping 10.1.1.10
Pinging 10.1.1.10 with 32 bytes of data:
Reply from 10.1.1.10: bytes=32 time=50ms TTL=64
Reply from 10.1.1.10: bytes=32 time=49ms TTL=64
Reply from 10.1.1.10: bytes=32 time=46ms TTL=64
Reply from 10.1.1.10: bytes=32 time=47ms TTL=64
Ping statistics for 10.1.1.10:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 46ms, Maximum = 50ms, Average = 48ms
C:\Users\PC-A>
```

Notice this time that the ping round-trip times are much longer indicating a potential problem.

Corporate networks should have extensive baselines; more extensive than we can describe in this course. Professional-grade software tools are available for storing and maintaining baseline information. In this course, we cover a few basic techniques and discuss the purpose of baselines.

Cisco's best practices for baseline processes can can be found by searching the internet for "Baseline Process Best Practices".

IP Configuration on a Windows Host

If you have used any of the tools in the previous topic to verify connectivity and found that some part of your network is not working as it should, now is the time to use some commands to troubleshoot your devices. Host and IOS commands can help you determine if the problem is with the IP addressing of your devices, which is a common network problem.

Checking the IP addressing on host devices is a common practice in networking for verifying and troubleshooting end-to-end connectivity. In Windows 10, you can access the IP address details from the **Network and Sharing Center**, as shown in the figure, to quickly view the four important settings: address, mask, router, and DNS.

However, network administrators typically view the IP addressing information on a Windows host by issuing the **ipconfig** command at the command line of a Windows computer, as shown in the sample output.

```
C:\Users\PC-A> ipconfig
Windows IP Configuration
(Output omitted)
Wireless LAN adapter Wi-Fi:
   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::a4aa:2dd1:ae2d:a75e%16
   IPv4 Address. . . . . . . . . . . : 192.168.10.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.10.1
(Output omitted)
```

Use the **ipconfig /all** command to view the MAC address, as well as a number of details regarding the Layer 3 addressing of the device, as shown in the example output.

```
C:\Users\PC-A> ipconfig /all
Windows IP Configuration
   Host Name . . . . . . . . . . . . : PC-A-00H20
   Primary Dns Suffix  . . . . . . . : cisco.com
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : cisco.com
(Output omitted)
Wireless LAN adapter Wi-Fi:
   Connection-specific DNS Suffix  . :
```

```
   Description . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 8265
   Physical Address. . . . . . . . . : F8-94-C2-E4-C5-0A
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::a4aa:2dd1:ae2d:a75e%16(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.10.10(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : August 17, 2019 1:20:17 PM
   Lease Expires . . . . . . . . . . : August 18, 2019 1:20:18 PM
   Default Gateway . . . . . . . . . : 192.168.10.1
   DHCP Server . . . . . . . . . . . : 192.168.10.1
   DHCPv6 IAID . . . . . . . . . . . : 100177090
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-21-F3-76-75-54-E1-AD-DE-DA-9A
   DNS Servers . . . . . . . . . . . : 192.168.10.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

If a host is configured as a DHCP client, the IP address configuration can be renewed using the **ipconfig /release** and **ipconfig /renew** commands, as shown in the sample output.

```
C:\Users\PC-A> ipconfig /release
(Output omitted)
Wireless LAN adapter Wi-Fi:
   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::a4aa:2dd1:ae2d:a75e%16
   Default Gateway . . . . . . . . . :
(Output omitted)
C:\Users\PC-A> ipconfig /renew
(Output omitted)
Wireless LAN adapter Wi-Fi:
   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::a4aa:2dd1:ae2d:a75e%16
   IPv4 Address. . . . . . . . . . . : 192.168.1.124
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
(Output omitted)
C:\Users\PC-A>
```

The DNS Client service on Windows PCs also optimizes the performance of DNS name resolution by storing previously resolved names in memory. The **ipconfig /displaydns** command displays all of the cached DNS entries on a Windows computer system, as shown in the example output.

```
C:\Users\PC-A> ipconfig /displaydns
Windows IP Configuration
(Output omitted)
```

```
    netacad.com
    ----------------------------------------
    Record Name . . . . . : netacad.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 602
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 54.165.95.219
(Output omitted)
```

17.5.2

IP Configuration on a Linux Host

Verifying IP settings using the GUI on a Linux machine will differ depending on the Linux distribution (distro) and desktop interface. The figure shows the **Connection Information** dialog box on the Ubuntu distro running the Gnome desktop.

On the command line, network administrators use the **ifconfig** command to display the status of the currently active interfaces and their IP configuration, as shown in the output.

```
[analyst@secOps ~]$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:b5:d6:cb
          inet addr: 10.0.2.15  Bcast:10.0.2.255  Mask: 255.255.255.0
          inet6 addr: fe80::57c6:ed95:b3c9:2951/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1332239 errors:0 dropped:0 overruns:0 frame:0
          TX packets:105910 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1855455014 (1.8 GB)  TX bytes:13140139 (13.1 MB)
lo: flags=73  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

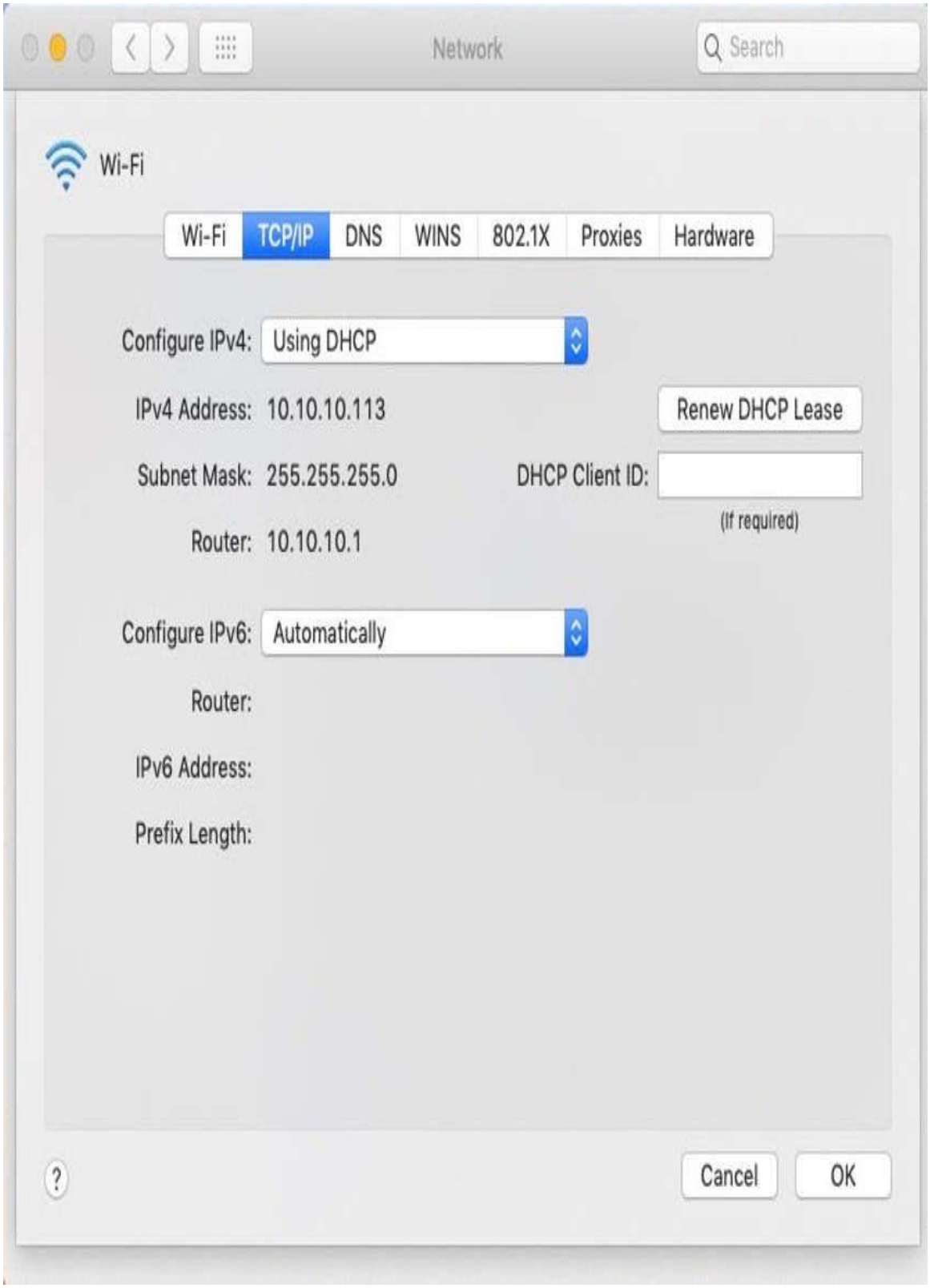
The Linux **ip address** command is used to display addresses and their properties. It can also be used to add or delete IP addresses.

Note: The output displayed may vary depending on the Linux distribution.

17.5.3

IP Configuration on a macOS Host

In the GUI of a Mac host, open **Network Preferences > Advanced** to get the IP addressing information, as shown in the figure.



However, the **ifconfig** command can also be used to verify the interface IP configuration a shown in the output.

```
MacBook-Air:~ Admin$ ifconfig en0
en0: flags=8863 mtu 1500
        ether c4:b3:01:a0:64:98
        inet6 fe80::c0f:1bf4:60b1:3adb%en0 prefixlen 64 secured scopeid 0x5
        inet 10.10.10.113 netmask 0xffffff00 broadcast 10.10.10.255
        nd6 options=201
        media: autoselect
        status: active
MacBook-Air:~ Admin$
```

Other useful macOS commands to verify the host IP settings include **networksetup -listallnetworkservices** and the **networksetup -getinfo <***network service***>,** as shown in the following output.

```
MacBook-Air:~ Admin$ networksetup -listallnetworkservices
An asterisk (*) denotes that a network service is disabled.
iPhone USB
Wi-Fi
Bluetooth PAN
Thunderbolt Bridge
MacBook-Air:~ Admin$
MacBook-Air:~ Admin$ networksetup -getinfo Wi-Fi
DHCP Configuration
IP address: 10.10.10.113
Subnet mask: 255.255.255.0
Router: 10.10.10.1
Client ID:
IPv6: Automatic
IPv6 IP address: none
IPv6 Router: none
Wi-Fi ID: c4:b3:01:a0:64:98
MacBook-Air:~ Admin$
```

17.5.4

The arp Command

The **arp** command is executed from the Windows, Linux, or Mac command prompt. The command lists all devices currently in the ARP cache of the host, which includes the IPv4 address, physical address, and the type of addressing (static/dynamic), for each device.

For instance, refer to the topology in the figure.

five hosts with IP addresses 10.0.0.1/24, 10.0.0.2/24, 10.0.0.3/24, 10.0.0.4/24, and 10.0.0.5/24 are connected to a switch connected to a router with an IP address of 10.0.0.254/24

10.0.0.254/24 10.0.0.1/24 10.0.0.2/24 10.0.0.3/24 10.0.0.4/24 10.0.0.5/24
PC-A

The output of the **arp -a** command on the Windows PC-A host is displayed.

```
C:\Users\PC-A> arp -a
Interface: 192.168.93.175 --- 0xc
  Internet Address      Physical Address      Type
  10.0.0.2              d0-67-e5-b6-56-4b     dynamic
  10.0.0.3              78-48-59-e3-b4-01     dynamic
  10.0.0.4              00-21-b6-00-16-97     dynamic
  10.0.0.254            00-15-99-cd-38-d9     dynamic
```

The **arp -a** command displays the known IP address and MAC address binding. Notice how IP address 10.0.0.5 is not included in the list. This is because the ARP cache only displays information from devices that have been recently accessed.

To ensure that the ARP cache is populated, **ping** a device so that it will have an entry in the ARP table. For instance, if PC-A pinged 10.0.0.5, then the ARP cache would contain an entry for that IP address.

The cache can be cleared by using the **netsh interface ip delete arpcache** command in the event the network administrator wants to repopulate the cache with updated information.

Note: You may need administrator access on the host to be able to use the **netsh interface ip delete arpcache** command.

17.5.5

Common show Commands Revisited

In the same way that commands and utilities are used to verify a host configuration, commands can be used to verify the interfaces of intermediary devices. The Cisco IOS provides commands to verify the operation of router and switch interfaces.

The Cisco IOS CLI **show** commands display relevant information about the configuration and operation of the device. Network technicians use **show** commands extensively for viewing configuration files, checking the status of device interfaces and processes, and verifying the device operational status. The status of nearly every process or function of the router can be displayed using a **show** command.

Commonly used **show** commands and when to use them are listed in the table.

Command	Useful for …
show running-config	To verify the current configuration and settings
show interfaces	To verify the interface status and see if there are any error messages
show ip interface	To verify the Layer 3 information of an interface
show arp	To verify the list of known hosts on the local Ethernet LANs
show ip route	To verify the Layer 3 routing information
show protocols	To verify which protocols are operational
show version	To verify the memory, interfaces, and licences of the device

Click the buttons to see example output from each of these show commands.Note: The output of some commands has been edited to focus on pertinent settings and reduce content.

show running-config

Verifies the current configuration and settings

R1# **show running-config**

(Output omitted)

```
!
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
interface GigabitEthernet0/0/0
 description Link to R2
 ip address 209.165.200.225 255.255.255.252
 negotiation auto
!
interface GigabitEthernet0/0/1
 description Link to LAN
 ip address 192.168.10.1 255.255.255.0
 negotiation auto
```

```
!
router ospf 10
 network 192.168.10.0 0.0.0.255 area 0
 network 209.165.200.224 0.0.0.3 area 0
!
banner motd ^C Authorized access only! ^C
!
line con 0
 password 7 14141B180F0B
 login
line vty 0 4
 password 7 00071A150754
 login
 transport input telnet ssh
!
end
R1#
```

17.5.6

The show cdp neighbors Command

There are several other IOS commands that are useful. The Cisco Discovery Protocol (CDP) is a Cisco proprietary protocol that runs at the data link layer. Because CDP operates at the data link layer, two or more Cisco network devices, such as routers that support different network layer protocols, can learn about each other even if Layer 3 connectivity has not been established.

When a Cisco device boots, CDP starts by default. CDP automatically discovers neighboring Cisco devices running CDP, regardless of which Layer 3 protocol or suites are running. CDP exchanges hardware and software device information with its directly connected CDP neighbors.

CDP provides the following information about each CDP neighbor device:

- **Device identifiers** - The configured host name of a switch, router, or other device
- **Address list** - Up to one network layer address for each protocol supported
- **Port identifier** - The name of the local and remote port in the form of an ASCII character string, such as FastEthernet 0/0
- **Capabilities list** - For example, whether a specific device is a Layer 2 switch or a Layer 3 switch
- **Platform** - The hardware platform of the device--for example, a Cisco 1841 series router.

Refer to the topology and the **show cdp neighbor** command output.

router R3 is connected via interface G0/0/1 to switch S3 at port F0/5 which is connected to switch S4

G0/0/1 F0/5 R3 S3
S4
R3# **show cdp neighbors**
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID Local Intrfce Holdtme Capability Platform Port ID
S3 Gig 0/0/1 122 S I WS-C2960+ Fas 0/5
Total cdp entries displayed : 1
R3#

The output displays that the R3 GigabitEthernet 0/0/1 interface is connected to the FastEthernet 0/5 interface of S3, which is a Cisco Catalyst 2960+ switch. Notice that R3 has not gathered information about S4. This is because CDP can only discover directly connected Cisco devices. S4 is not directly connected to R3 and therefore is not listed in the output.

The **show cdp neighbors detail** command reveals the IP address of a neighboring device, as shown in the output. CDP will reveal the IP address of the neighbor regardless of whether or not you can ping that neighbor. This command is very helpful when two Cisco routers cannot route across their shared data link. The **show cdp neighbors detail** command will help determine if one of the CDP neighbors has an IP configuration error.

As helpful as CDP is, it can also be a security risk because it can provide useful network infrastructure information to threat actors. For example, by default many IOS versions send CDP advertisements out all enabled ports. However, best practices suggest that CDP should be enabled only on interfaces that are connecting to other infrastructure Cisco devices. CDP advertisements should be disabled on user-facing ports.

Because some IOS versions send out CDP advertisements by default, it is important to know how to disable CDP. To disable CDP globally, use the global configuration command **no cdp run**. To disable CDP on an interface, use the interface command **no cdp enable**.

17.5.7

The show ip interface brief Command

One of the most frequently used commands is the **show ip interface brief** command. This command provides a more abbreviated output than the **show ip interface** command. It provides a summary of the key information for all the network interfaces on a router.

For example, the **show ip interface brief** output displays all interfaces on the router, the IP address assigned to each interface, if any, and the operational status of the interface.

R1# **show ip interface brief**

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0/0	209.165.200.225	YES	manual	up	up
GigabitEthernet0/0/1	192.168.10.1	YES	manual	up	up
Serial0/1/0	unassigned	NO	unset	down	down
Serial0/1/1	unassigned	NO	unset	down	down
GigabitEthernet0	unassigned	YES	unset	administratively down	down

R1#

Verify Switch Interfaces

The **show ip interface brief** command can also be used to verify the status of the switch interfaces, as shown in the output.

S1# **show ip interface brief**

Interface	IP-Address	OK?	Method	Status	Protocol
Vlanl	192.168.254.250	YES	manual	up	up
FastEthernet0/l	unassigned	YES	unset	down	down
FastEthernet0/2	unassigned	YES	unset	up	up
FastEthernet0/3	unassigned	YES	unset	up	up

The VLAN1 interface is assigned an IPv4 address of 192.168.254.250, has been enabled, and is operational.

The output also shows that the FastEthernet0/1 interface is down. This indicates that either no device is connected to the interface or the device that is connected has a network interface that is not operational.

In contrast, the output shows that the FastEthernet0/2 and FastEthernet0/3 interfaces are operational. This is indicated by both the status and protocol being shown as up.

17.5.8

Basic Troubleshooting Approaches

In the previous two topics, you learned about some utilities and commands that you can use to help identify problem areas in your network. This is an important part of troubleshooting. There are many ways to troubleshoot a network problem. This topic details a structured troubleshooting process that can help you to become a better network administrator. It also provides a few more commands to help you resolve problems. Network problems can be simple or complex, and can result from a combination of hardware, software, and connectivity issues. Technicians must be able to analyze the problem and determine the cause of the error before they can resolve the network issue. This process is called troubleshooting.

A common and efficient troubleshooting methodology is based on the scientific method.

The table shows the six main steps in the troubleshooting process.

Step	Description
Step 1. Identify the Problem	● This is the first step in the troubleshooting process. ● Although tools can be used in this step, a conversation with the user is often very helpful.
Step 2. Establish a Theory of Probable Causes	● After the problem is identified, try to establish a theory of probable causes. ● This step often yields more than a few probable causes to the problem.
Step 3. Test the Theory to Determine Cause	● Based on the probable causes, test your theories to determine which one is the cause of the problem. ● A technician will often apply a quick procedure to test and see if it solves the problem. ● If a quick procedure does not correct the problem, you might need to research the problem further to establish the exact cause.
Step 4. Establish a Plan of Action and Implement the Solution	After you have determined the exact cause of the problem, establish a plan of action to resolve the problem and implement the solution.
Step 5. Verify Solution and Implement Preventive Measures	● After you have corrected the problem, verify full functionality. ● If applicable, implement preventive measures.
Step 6. Document Findings, Actions, and Outcomes	● In the final step of the troubleshooting process, document your findings, actions, and outcomes. ● This is very important for future reference.

To assess the problem, determine how many devices on the network are experiencing the problem. If there is a problem with one device on the network, start the troubleshooting process at that device. If there is a problem with all devices on the network, start the troubleshooting process at the device where all other devices are connected. You should develop a logical and consistent method for diagnosing network problems by eliminating one problem at a time.

17.6.2

Resolve or Escalate?

In some situations, it may not be possible to resolve the problem immediately. A problem should be escalated when it requires a manager decision, some specific expertise, or network access level unavailable to the troubleshooting technician.

For example, after troubleshooting, the technician concludes a router module should be replaced. This problem should be escalated for manager approval. The manager may have to escalate the problem again as it may require the approval of the financial department before a new module can be purchased.

A company policy should clearly state when and how a technician should escalate a problem.

17.6.3

The debug Command

OS processes, protocols, mechanisms and events generate messages to communicate their status. These messages can provide valuable information when troubleshooting or verifying system operations. The IOS **debug** command allows the administrator to display these messages in real-time for analysis. It is a very important tool for monitoring events on a Cisco IOS device.

All **debug** commands are entered in privileged EXEC mode. The Cisco IOS allows for narrowing the output of **debug** to include only the relevant feature or subfeature. This is important because debugging output is assigned high priority in the CPU process and it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems.

For example, to monitor the status of ICMP messages in a Cisco router, use **debug ip icmp**, as shown in the example.

R1# **debug ip icmp**
ICMP packet debugging is on
R1#
R1# **ping 10.1.1.1**
Type escape sequence to abort.

```
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
R1#
*Aug 20 14:18:59.605: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology
BASE, dscp 0 topoid 0
*Aug 20 14:18:59.606: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology
BASE, dscp 0 topoid 0
*Aug 20 14:18:59.608: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology
BASE, dscp 0 topoid 0
*Aug 20 14:18:59.609: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology
BASE, dscp 0 topoid 0
*Aug 20 14:18:59.611: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology
BASE, dscp 0 topoid 0
R1#
```

To list a brief description of all the debugging command options, use the **debug ?** command in privileged EXEC mode at the command line.

To turn off a specific debugging feature, add the **no** keyword in front of the **debug** command:

Router# **no debug ip icmp**

Alternatively, you can enter the **undebug** form of the command in privileged EXEC mode:

Router# **undebug ip icmp**

To turn off all active debug commands at once, use the **undebug all** command:

Router# **undebug all**

Be cautious using some **debug** command. Commands such as **debug all** and **debug ip packet** generate a substantial amount of output and can use a large portion of system resources. The router could get so busy displaying **debug** messages that it would not have enough processing power to perform its network functions, or even listen to commands to turn off debugging. For this reason, using these command options is not recommended and should be avoided.

17.6.4

The terminal monitor Command

Connections to grant access to the IOS command line interface can be established in the following two ways:

- **Locally** - Local connections (i.e., console connection) require physical access to the router or switch console port using a rollover cable.
- **Remotely** - Remote connections require the use of Telnet or SSH to establish a connection to an IP configured device.

Certain IOS messages are automatically displayed on a console connection but not on a remote connection. For instance, **debug** output is displayed by default on console connections. However, **debug** output is not automatically displayed on remote connections. This is because **debug** messages are log messages which are prevented from being displayed on vty lines.

In the following output for instance, the user established a remote connection using Telnet from R2 to R1. The user then issued the **debug ip icmp** command. However, the command failed to display **debug** output.

R2# **telnet 209.165.200.225**
Trying 209.165.200.225 ... Open
Authorized access only!
User Access Verification
Password:
R1> **enable**
Password:
R1# **debug ip icmp**
ICMP packet debugging is on
R1# **ping 10.1.1.1**
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
R1#
! No debug output displayed>

To display log messages on a terminal (virtual console), use the **terminal monitor** privileged EXEC command. To stop logging messages on a terminal, use the **terminal no monitor** privileged EXEC command.

For instance, notice how the **terminal monitor** command has now been entered and the **ping** command displays the **debug** output.

R1# **terminal monitor**
R1# **ping 10.1.1.1**
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
R1#

*Aug 20 16:03:49.735: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0 topoid 0
**Aug 20 16:03:49.737: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0 topoid 0
**Aug 20 16:03:49.738: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0 topoid 0
**Aug 20 16:03:49.740: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0 topoid 0
**Aug 20 16:03:49.741: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0 topoid 0
R1# **no debug ip icmp**
ICMP packet debugging is off
R1#

Note: The intent of the **debug** command is to capture live output for a short period of time (i.e., a few seconds to a minute or so). Always disable **debug** when not required.

Duplex Operation and Mismatch Issues

Many common network problems can be identified and resolved with little effort. Now that you have the tools and the process for troubleshooting a network, this topic reviews some common networking issues that you are likely to find as a network administrator.

In data communications, *duplex* refers to the direction of data transmission between two devices.

There are two duplex communication modes:

- **Half-duplex** - Communication is restricted to the exchange of data in one direction at a time.
- **Full-duplex** - Communications is permitted to be sent and received simultaneously.

The figure illustrates how each duplex method operates.

The figure is a comparison of half-duplex versus full-duplex communications. The top diagram shows half-duplex communication. Switch S1 is connected to switch S2 with an arrow flowing from S1 to S2 indicating a device can send or receive. The bottom diagram shows-full duplex communication. Switch S1 is connected to switch S2 with arrows pointing in both directions indicating a device can send AND receive simultaneously.

S2 S1 S2
S1
Full-Duplex CommunicationHalf-Duplex CommunicationSend **OR** receiveSend **AND** receive simultaneously

Interconnecting Ethernet interfaces must operate in the same duplex mode for best communication performance and to avoid inefficiency and latency on the link.

The Ethernet autonegotiation feature facilitates configuration, minimizes problems and maximizes link performance between two interconnecting Ethernet links. The connected devices first announce their supported capabilities and then choose the highest performance mode supported by both ends. For example, the switch and router in the figure have successfully autonegotiated full-duplex mode.

S1
R1
I can operate in full-duplex ...I can operate in full-duplex ...F0/5G0/0/1

If one of the two connected devices is operating in full-duplex and the other is operating in half-duplex, a duplex mismatch occurs. While data communication will occur through a link with a duplex mismatch, link performance will be very poor.

Duplex mismatches are typically caused by a misconfigured interface or in rare instances by a failed autonegotiation. Duplex mismatches may be difficult to troubleshoot as the communication between devices still occurs.

17.7.2

IP Addressing Issues on IOS Devices

IP address-related problems will likely keep remote network devices from communicating. Because IP addresses are hierarchical, any IP address assigned to a network device must conform to that range of addresses in that network. Wrongly assigned IP addresses create a variety of issues, including IP address conflicts and routing problems.

Two common causes of incorrect IPv4 assignment are manual assignment mistakes or DHCP-related issues.

Network administrators often have to manually assign IP addresses to devices such as servers and routers. If a mistake is made during the assignment, then communications issues with the device are very likely to occur.

On an IOS device, use the **show ip interface** or **show ip interface brief** commands to verify what IPv4 addresses are assigned to the network interfaces. For example, issuing the **show ip interface brief** command as shown would validate the interface status on R1.

R1# **show ip interface brief**

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0/0	209.165.200.225	YES	manual	up	up
GigabitEthernet0/0/1	192.168.10.1	YES	manual	up	up

```
Serial0/1/0            unassigned      NO  unset  down                  down
Serial0/1/1            unassigned      NO  unset  down                  down
GigabitEthernet0       unassigned      YES unset  administratively down down
R1#
```
17.7.3

IP Addressing Issues on End Devices

In Windows-based machines, when the device cannot contact a DHCP server, Windows will automatically assign an address belonging to the 169.254.0.0/16 range. This feature is called Automatic Private IP Addressing (APIPA) and is designed to facilitate communication within the local network. Think of it as Windows saying, “I will use this address from the 169.254.0.0/16 range because I could not get any other address”.

Often, a computer with an APIPA address will not be able to communicate with other devices in the network because those devices will most likely not belong to the 169.254.0.0/16 network. This situation indicates an automatic IPv4 address assignment problem that should be fixed.

Note: Other operating systems, such Linux and OS X, will not assign an IPv4 address to the network interface if communication with a DHCP server fails.

Most end devices are configured to rely on a DHCP server for automatic IPv4 address assignment. If the device is unable to communicate with the DHCP server, then the server cannot assign an IPv4 address for the specific network and the device will not be able to communicate.

To verify the IP addresses assigned to a Windows-based computer, use the **ipconfig** command, as shown in the output.

```
C:\Users\PC-A> ipconfig
Windows IP Configuration
(Output omitted)
Wireless LAN adapter Wi-Fi:
   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::a4aa:2dd1:ae2d:a75e%16
   IPv4 Address. . . . . . . . . . . : 192.168.10.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.10.1
(Output omitted)
```
17.7.4

Default Gateway Issues

The default gateway for an end device is the closest networking device that can forward traffic to other networks. If a device has an incorrect or nonexistent default gateway address, it will not be able to communicate with devices in remote networks. Because the default gateway is the path to remote networks, its address must belong to the same network as the end device.

The address of the default gateway can be manually set or obtained from a DHCP server. Similar to IPv4 addressing issues, default gateway problems can be related to misconfiguration (in the case of manual assignment) or DHCP problems (if automatic assignment is in use).

To solve misconfigured default gateway issues, ensure that the device has the correct default gateway configured. If the default address was manually set but is incorrect, simply replace it with the proper address. If the default gateway address was automatically set, ensure the device can communicate with the DHCP server. It is also important to verify that the proper IPv4 address and subnet mask were configured on the interface of the router and that the interface is active.

To verify the default gateway on Windows-based computers, use the **ipconfig** command as shown.

```
C:\Users\PC-A> ipconfig
Windows IP Configuration
(Output omitted)
Wireless LAN adapter Wi-Fi:
   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::a4aa:2dd1:ae2d:a75e%16
   IPv4 Address. . . . . . . . . . . : 192.168.10.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.10.1
(Output omitted)
```

On a router, use the **show ip route** command to list the routing table and verify that the default gateway, known as a default route, has been set. This route is used when the destination address of the packet does not match any other routes in its routing table.

For example, the output verifies that R1 has a default gateway (i.e., Gateway of last resort) configured pointing to IP address 209.168.200.226.

```
R1# show ip route | begin Gateway
Gateway of last resort is 209.165.200.226 to network 0.0.0.0
O*E2  0.0.0.0/0 [110/1] via 209.165.200.226, 02:19:50, GigabitEthernet0/0/0
      10.0.0.0/24 is subnetted, 1 subnets
O        10.1.1.0 [110/3] via 209.165.200.226, 02:05:42, GigabitEthernet0/0/0
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, GigabitEthernet0/0/1
L        192.168.10.1/32 is directly connected, GigabitEthernet0/0/1
```

```
     209.165.200.0/24 is variably subnetted, 3 subnets, 2 masks
C        209.165.200.224/30 is directly connected, GigabitEthernet0/0/0
L        209.165.200.225/32 is directly connected, GigabitEthernet0/0/0
O        209.165.200.228/30
         [110/2] via 209.165.200.226, 02:07:19, GigabitEthernet0/0/0
R1#
```

The first highlighted line basically states that the gateway to any (i.e., 0.0.0.0) should be sent to IP address 209.165.200.226. The second highlighted displays how R1 learned about the default gateway. In this case, R1 received the information from another OSPF-enabled router.

17.7.5

Troubleshooting DNS Issues

Domain Name Service (DNS) defines an automated service that matches names, such as www.cisco.com, with the IP address. Although DNS resolution is not crucial to device communication, it is very important to the end user.

It is common for users to mistakenly relate the operation of an internet link to the availability of the DNS. User complaints such as “the network is down” or “the internet is down” are often caused by an unreachable DNS server. While packet routing and all other network services are still operational, DNS failures often lead the user to the wrong conclusion. If a user types in a domain name such as www.cisco.com in a web browser and the DNS server is unreachable, the name will not be translated into an IP address and the website will not display.

DNS server addresses can be manually or automatically assigned. Network administrators are often responsible for manually assigning DNS server addresses on servers and other devices, while DHCP is used to automatically assign DNS server addresses to clients.

Although it is common for companies and organizations to manage their own DNS servers, any reachable DNS server can be used to resolve names. Small office and home office (SOHO) users often rely on the DNS server maintained by their ISP for name resolution. ISP-maintained DNS servers are assigned to SOHO customers via DHCP. Additionally, Google maintains a public DNS server that can be used by anyone and it is very useful for testing. The IPv4 address of Google’s public DNS server is 8.8.8.8 and 2001:4860:4860::8888 for its IPv6 DNS address.

Cisco offers OpenDNS which provides secure DNS service by filtering phishing and some malware sites. You can change your DNS address to 208.67.222.222 and 208.67.220.220 in the Preferred DNS server and Alternate DNS server fields. Advanced features such as web content filtering and security are available to families and businesses.

Use the **ipconfig /all** as shown to verify which DNS server is in use by the Windows computer.

C:\Users\PC-A> **ipconfig /all**

(Output omitted)
Wireless LAN adapter Wi-Fi:
  Connection-specific DNS Suffix . :
  Description . . . . : Intel(R) Dual Band Wireless-AC 8265
  Physical Address. . . . . : F8-94-C2-E4-C5-0A
  DHCP Enabled. . . . . : Yes
  Autoconfiguration Enabled . . . . : Yes
  Link-local IPv6 Address . . . . . : fe80::a4aa:2dd1:ae2d:a75e%16(Preferred)
  IPv4 Address. . . . . : 192.168.10.10(Preferred)
  Subnet Mask . . . . : 255.255.255.0
  Lease Obtained. . . . . : August 17, 2019 1:20:17 PM
  Lease Expires . . . . : August 18, 2019 1:20:18 PM
  Default Gateway . . . . : 192.168.10.1
  DHCP Server . . . . : 192.168.10.1
  DHCPv6 IAID . . . . : 100177090
  DHCPv6 Client DUID. . . . . : 00-01-00-01-21-F3-76-75-54-E1-AD-DE-DA-9A
  DNS Servers . . . . : 208.67.222.222
  NetBIOS over Tcpip. . . . . : Enabled
(Output omitted)

The **nslookup** command is another useful DNS troubleshooting tool for PCs. With **nslookup** a user can manually place DNS queries and analyze the DNS response. The **nslookup** command shows the output for a query for www.cisco.com. Notice you can also simply enter an IP address and **nslookup** will resolve the name.

Note: It is not always possible to type an IP address in **nslookup** and receive the domain name. One of the most common reasons for this is that most websites run on servers that support multiple sites.

C:\Users\PC-A> **nslookup**
Default Server: Home-Net
Address: 192.168.1.1
> **cisco.com**
Server: Home-Net
Address: 192.168.1.1
Non-authoritative answer:
Name: cisco.com
Addresses: 2001:420:1101:1::185
          72.163.4.185
> **8.8.8.8**
Server: Home-Net
Address: 192.168.1.1
Name: dns.google
Address: 8.8.8.8
>

> **208.67.222.222**
Server: Home-Net
Address: 192.168.1.1
Name: resolver1.opendns.com
Address: 208.67.222.222
>

What did I learn in this module?

Devices in a Small Network

Small networks typically have a single WAN connection provided by DSL, cable, or an Ethernet connection. Small networks are managed by a local IT technician or by a contracted professional. Factors to consider when selecting network devices for a small network are cost, speed and types of ports/interfaces, expandability, and OS features and services. When implementing a network, create an IP addressing scheme and use it on end devices, servers and peripherals, and intermediary devices. Redundancy can be accomplished by installing duplicate equipment, but it can also be accomplished by supplying duplicate network links for critical areas. The routers and switches in a small network should be configured to support real-time traffic, such as voice and video, in an appropriate manner relative to other data traffic. In fact, a good network design will implement quality of service (QoS) to classify traffic carefully according to priority.

Small Network Applications and Protocols

There are two forms of software programs or processes that provide access to the network: network applications and application layer services. Some end-user applications implement application layer protocols and are able to communicate directly with the lower layers of the protocol stack. Email clients and web browsers are examples of this type of application. Other programs may need the assistance of application layer services to use network resources like file transfer or network print spooling. These are the programs that interface with the network and prepare the data for transfer. The two most common remote access solutions are Telnet and Secure Shell (SSH). SSH service is a secure alternative to Telnet. Network administrators must also support common network servers and their required related network protocols such as web server, email server, FTP server, DHCP server, and DNS server. Businesses today are increasingly using IP telephony and streaming media to communicate with customers and business partners. These are real-time applications. The network infrastructure must support VoIP, IP telephony, and other real-time applications.

Scale to Larger Networks

To scale a network, several elements are required: network documentation, device inventory, budget, and traffic analysis. Know the type of traffic that is crossing the network as well as the current traffic flow. Capture traffic during peak utilization times to get a good representation of

the different traffic types and perform the capture on different network segments and devices as some traffic will be local to a particular segment. Network administrators must know how network use is changing. Usage details of employee computers can be captured in a ‘snapshot’ with such tools as the Windows Task Manager, Event Viewer, and Data Usage.

Verify Connectivity

The **ping** command is the most effective way to quickly test Layer 3 connectivity between a source and destination IP address. The command also displays various round-trip time statistics. The Cisco IOS offers an "extended" mode of the ping command which lets the user create special types of pings by adjusting parameters related to the command operation. Extended ping is entered in privileged EXEC mode by typing ping without a destination IP address. Traceroute can help locate Layer 3 problem areas in a network. A trace returns a list of hops as a packet is routed through a network. It is used to identify the point along the path where the problem can be found. In Windows, the command is **tracert**. In Cisco IOS the command is **traceroute**. There is also an extended **traceroute** command. It allows the administrator to adjust parameters related to the command operation. The output derived from network commands contributes data to the network baseline. One method for starting a baseline is to copy and paste the results from an executed ping, trace, or other relevant commands into a text file. These text files can be time stamped with the date and saved into an archive for later retrieval and comparison.

Host and IOS Commands

Network administrators view the IP addressing information (address, mask, router, and DNS) on a Windows host by issuing the **ipconfig** command. Other necessary commands are **ipconfig /all**, **ipconfig /release** and **ipconfig /renew**, and **ipconfig /displaydns**. Verifying IP settings by using the GUI on a Linux machine will differ depending on the Linux distribution (distro) and desktop interface. Necessary commands are **ifconfig**, and **ip address**. In the GUI of a Mac host, open Network Preferences > Advanced to get the IP addressing information. Other IP addressing commands for Mac are **ifconfig**, and **networksetup -listallnetworkservices** and **networksetup -getinfo** <*network service*>. The **arp** command is executed from the Windows, Linux, or Mac command prompt. The command lists all devices currently in the ARP cache of the host, which includes the IPv4 address, physical address, and the type of addressing (static/dynamic), for each device. The **arp -a** command displays the known IP address and MAC address binding. Common **show** commands are **show running-config**, **show interfaces**, **show ip address**, **show arp**, **show ip route**, **show protocols**, and **show version**. The **show cdp neighbor** command provides the following information about each CDP neighbor device: identifiers, address list, port identifier, capabilities list, and platform. The **show cdp neighbors detail** command will help determine if one of the CDP neighbors has an IP configuration error. The **show ip interface brief** command output displays all interfaces on the router, the IP address assigned to each interface, if any, and the operational status of the interface.

Troubleshooting Methodologies

Step 1. Identify the problem

Step 2. Establish a theory of probably causes.

Step 3. Test the theory to determine the cause.

Step 4. Establish a plan of action and implement the solution.

Step 5. Verify the solution and implement preventive measures.

Step 6. Document findings, actions, and outcomes.

A problem should be escalated when it requires a the decision of a manager, some specific expertise, or network access level unavailable to the troubleshooting technician. OS processes, protocols, mechanisms and events generate messages to communicate their status. The IOS **debug** command allows the administrator to display these messages in real-time for analysis. To display log messages on a terminal (virtual console), use the **terminal monitor** privileged EXEC command.

Troubleshooting Scenarios

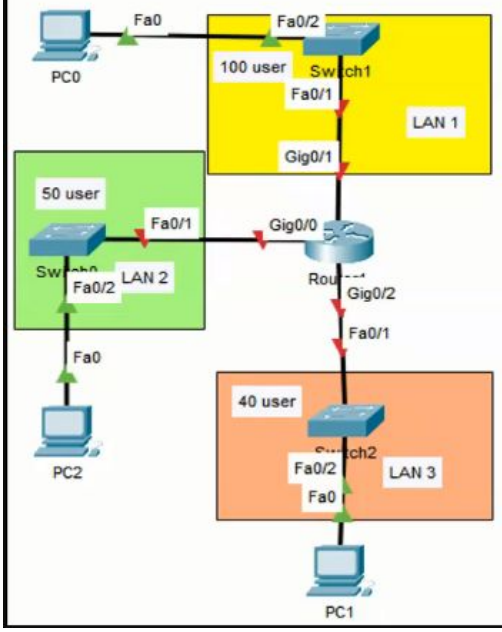
There are two duplex communication modes: half-duplex and full-duplex. If one of the two connected devices is operating in full-duplex and the other is operating in half-duplex, a duplex mismatch occurs. While data communication will occur through a link with a duplex mismatch, link performance will be very poor.

Wrongly assigned IP addresses create a variety of issues, including IP address conflicts and routing problems. Two common causes of incorrect IPv4 assignment are manual assignment mistakes or DHCP-related issues. Most end devices are configured to rely on a DHCP server for automatic IPv4 address assignment. If the device is unable to communicate with the DHCP server, then the server cannot assign an IPv4 address for the specific network and the device will not be able to communicate.

The default gateway for an end device is the closest networking device that can forward traffic to other networks. If a device has an incorrect or nonexistent default gateway address, it will not be able to communicate with devices in remote networks. Because the default gateway is the path to remote networks, its address must belong to the same network as the end device.

DNS failures often lead the user to conclude that the network is down. If a user types in a domain name such as www.cisco.com in a web browser and the DNS server is unreachable, the name will not be translated into an IP address and the website will not display.

PACKET TRACER ACTIVITY 1



MARKS :100

TASK 1 :50 MARKS
TASK 2 : 25 MARKS
TASK 3 : 25 MARKS

TASK 1:
you are a network technicion you need to create a network in which there are

LAN 1 100 USER
LAN 2 50 USER
LAN3 40 USER

NETWORK ADDRESS IS 192.168.10.0 255.255.255.0

TASK 2:
Verify the connectivity between each network

TASK 3:

ENABLE TELNET ON SWITCH 1 AND ACCESS FROM LAN 3 NETWORK