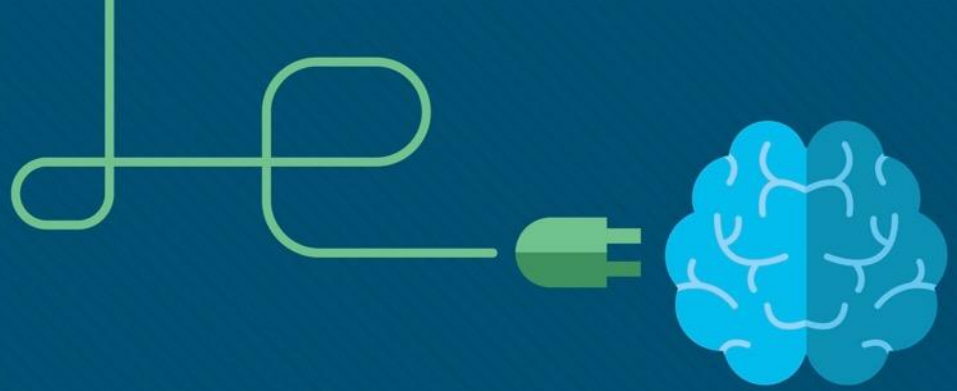


Module 15: Application Layer

Introduction to Networks v7.0
(ITN)

Module Objectives

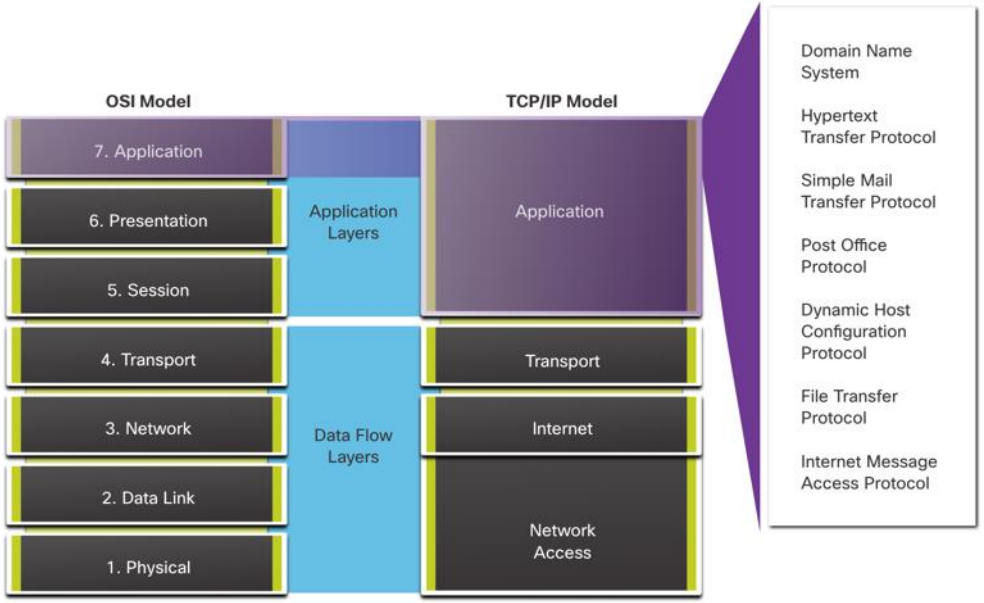
- **Module Title**: Application Layer
- **Module Objective**: Explain the operation of application layer protocols in providing support to end-user applications.

Topic Title	Topic Objective
Application, Presentation, and Session	Explain how the functions of the application layer, presentation layer, and session layer work together to provide network services to end user applications.
Peer-to-Peer	Explain how end user applications operate in a peer-to-peer network.
Web and Email Protocols	Explain how web and email protocols operate.
IP Addressing Services	Explain how DNS and DHCP operate.
File Sharing Services	Explain how file transfer protocols operate.

15.1 Application, Presentation, and Session

Application Layer

- The upper three layers of the OSI model (application, presentation, and session) define functions of the TCP/IP application layer.
- The application layer provides the interface between the applications used to communicate, and the underlying network over which messages are transmitted.
- Some of the most widely known application layer protocols include HTTP, FTP, TFTP, IMAP and DNS.



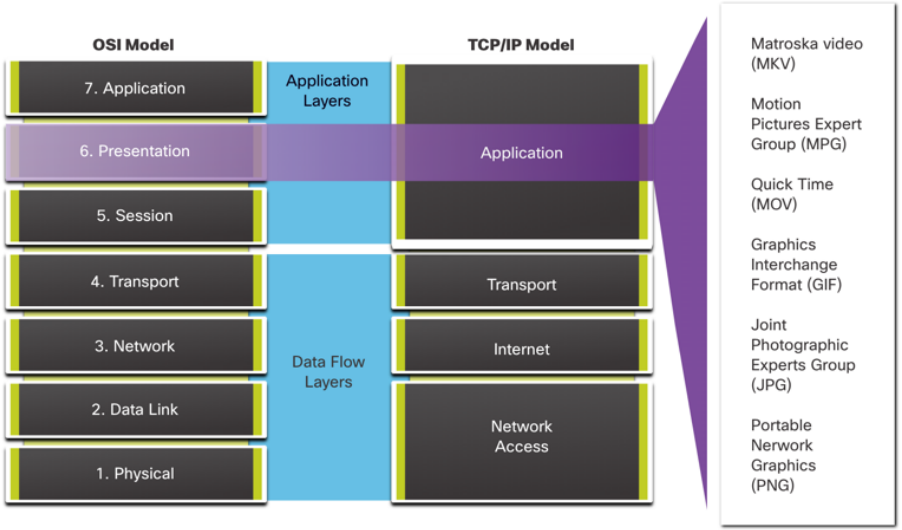
Presentation and Session Layer

The presentation layer has three primary functions:

- Formatting, or presenting, data at the source device into a compatible format for receipt by the destination device
- Compressing data in a way that can be decompressed by the destination device
- Encrypting data for transmission and decrypting data upon receipt

The session layer functions:

- It creates and maintains dialogs between source and destination applications.
- It handles the exchange of information to initiate dialogs, keep them active, and to restart sessions that are disrupted or idle for a long period of time.



TCP/IP Application Layer Protocols

- 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.

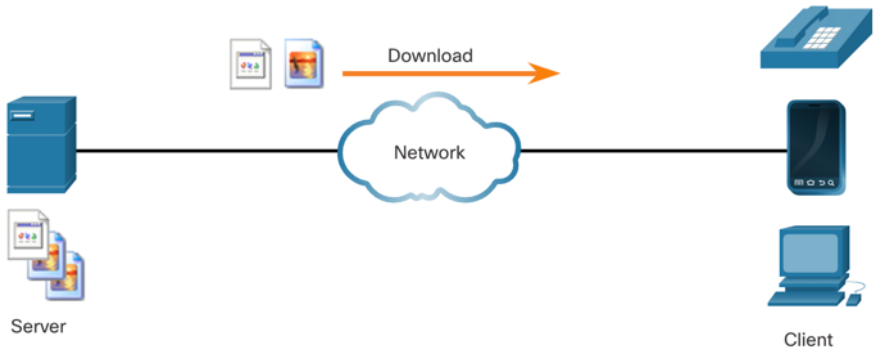
Host Config
DHCP - Dynamic Host Configuration Protocol
- UDP client 68, server 67
- Dynamically assigns IP addresses to be re-used when no longer needed

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

15.2 Peer-to-Peer

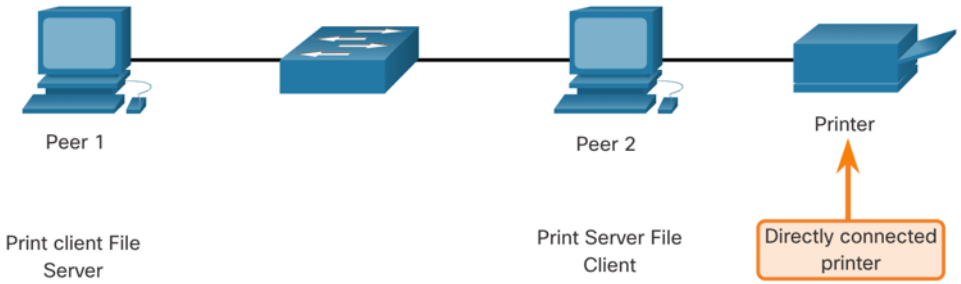
Client-Server Model

- 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.



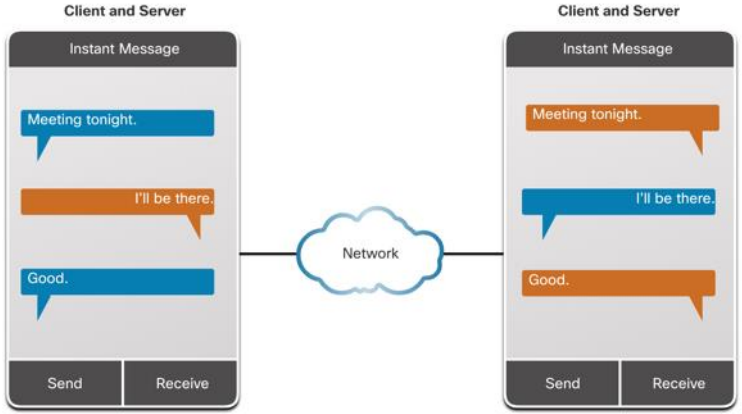
Peer-to-Peer Networks

- In a peer-to-peer (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.



Peer-to-Peer Applications

- A P2P application allows a device to act as both a client and a server within the same communication.
- Some P2P applications use a hybrid system where each peer accesses an index server to get the location of a resource stored on another peer.

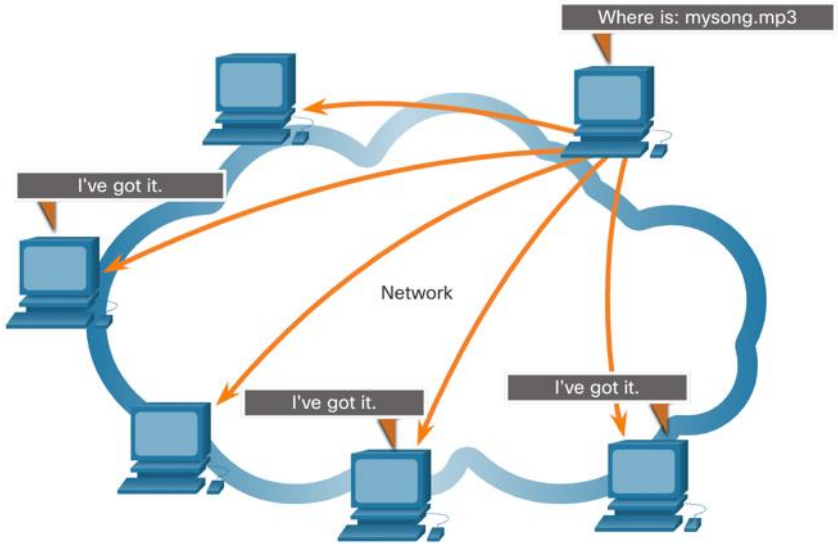


Common P2P Applications

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



15.3 Web and Email Protocols

Hypertext Transfer Protocol and Hypertext Markup Language

When a web address or Uniform Resource Locator (URL) is typed into a web browser, the web browser establishes a connection to the web service. 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:

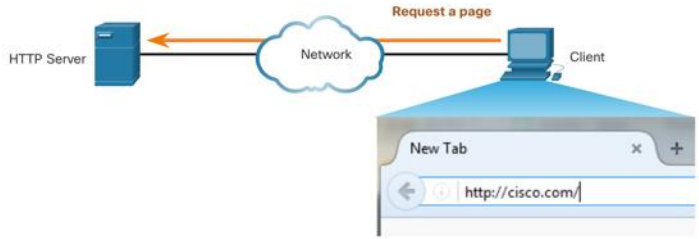
- http (the protocol or scheme)
- www.cisco.com (the server name)
- index.html (the specific filename requested)

Hypertext Transfer Protocol and Hypertext Markup Language (Cont.)

Step 2

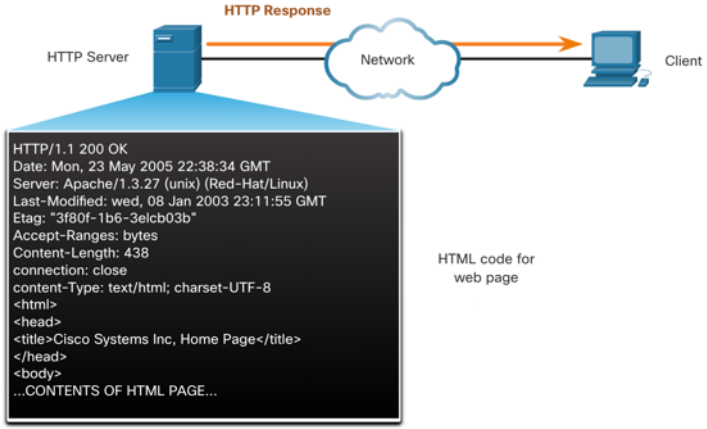
The browser then checks with a name server to convert www.cisco.com into a numeric IP address, which it uses to connect to the server.

The client initiates an HTTP request to a server by sending a GET request to the server and asks for the index.html file.



Step 3

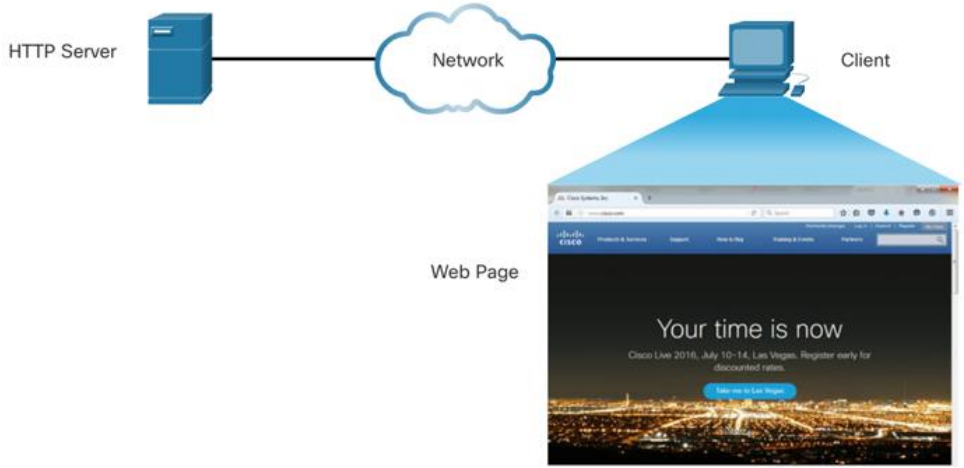
In response to the request, the server sends the HTML code for this web page to the browser.



Hypertext Transfer Protocol and Hypertext Markup Language (Cont.)

Step 4

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

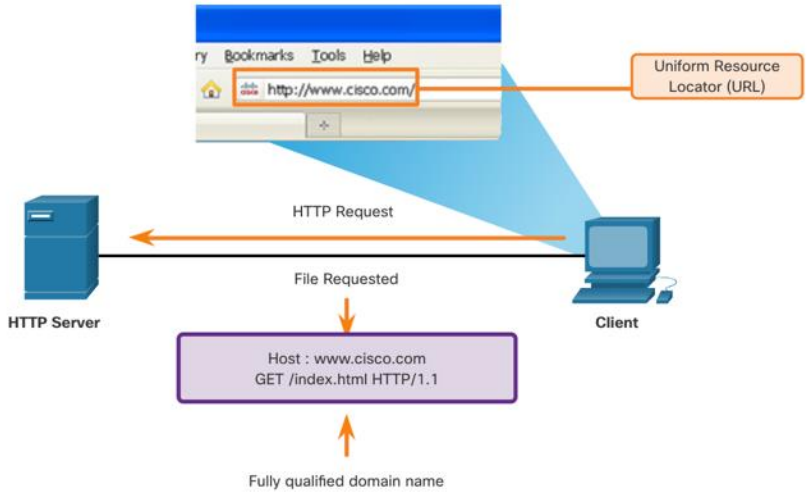


HTTP and HTTPS

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

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

- **GET** - This is a client request for data. A client (web browser) sends the GET message to the web server to request HTML pages.
- **POST** - This uploads data files to the web server, such as form data.
- **PUT** - This uploads resources or content to the web server, such as an image.



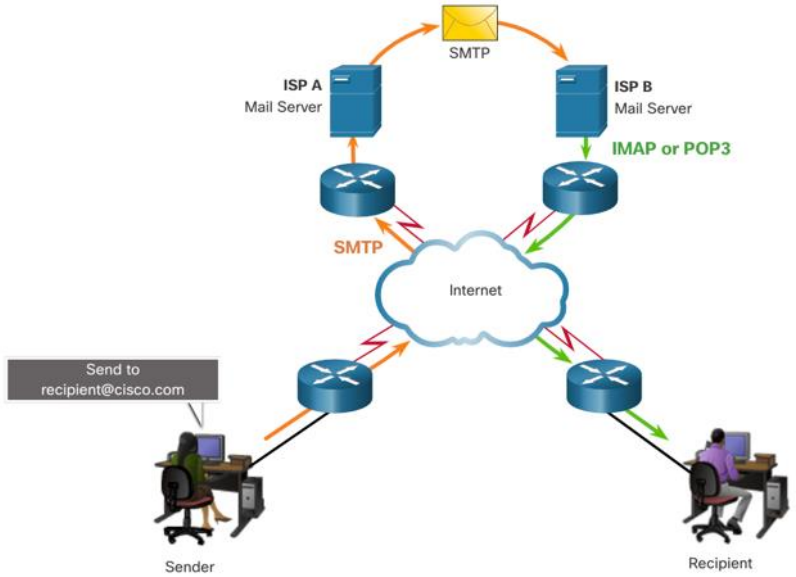
Note: HTTP is not a secure protocol. For secure communications sent across the internet, HTTPS should be used.

Email Protocols

Email is a store-and-forward method of sending, storing, and retrieving electronic messages across a network. Email messages are stored in databases on mail servers. Email clients communicate with mail servers to send and receive email.

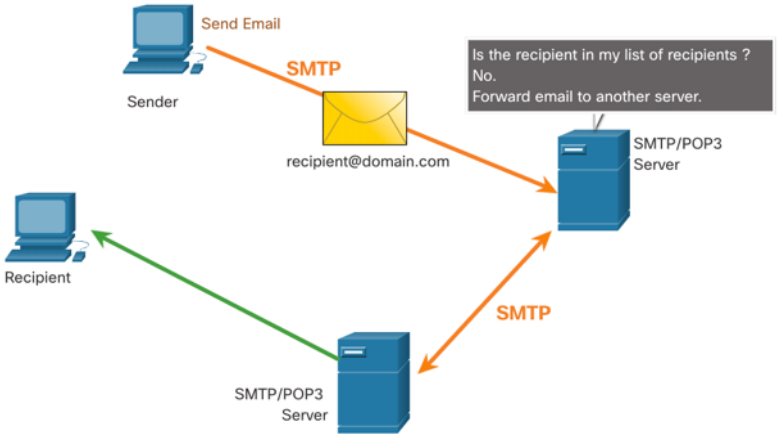
The email protocols used for operation are:

- Simple Mail Transfer Protocol (SMTP) – used to send mail.
- Post Office Protocol (POP) & IMAP – used for clients to receive mail.



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.

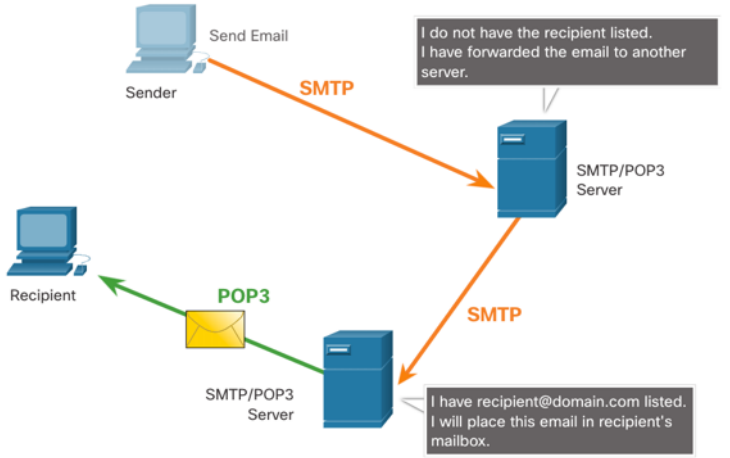


Note: SMTP message formats require a message header (recipient email address & sender email address) and a message body.

SMTP, POP and IMAP (Cont.)

POP is used by an application to retrieve mail from a mail server. When mail is downloaded from the server to the client using POP the messages are then deleted on the server.

- The server starts the POP service by passively listening on TCP port 110 for client connection requests.
- When a client wants to make use of the service, it sends a request to establish a TCP connection with the server.
- When the connection is established, the POP server sends a greeting.
- The client and POP server then exchange commands and responses until the connection is closed or aborted.

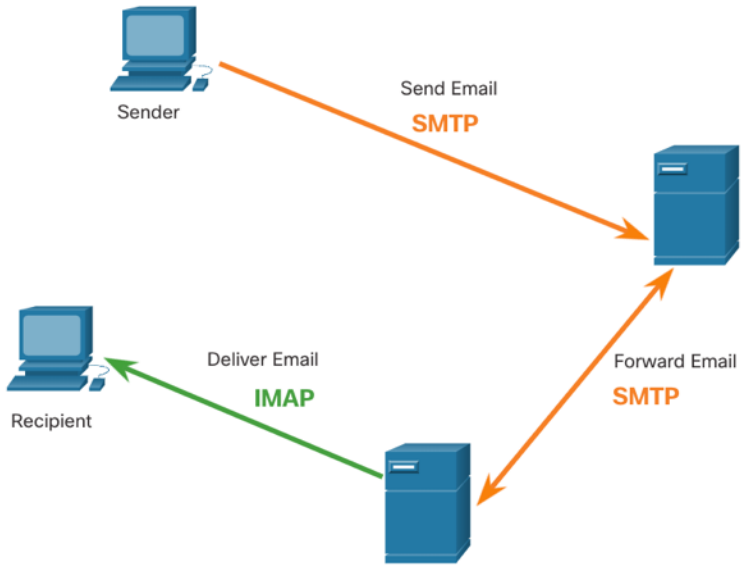


Note: Since POP does not store messages, it is not recommended for small businesses that need a centralized backup solution.

SMTP, POP and IMAP (Cont.)

IMAP is another protocol that describes a method to retrieve email messages.

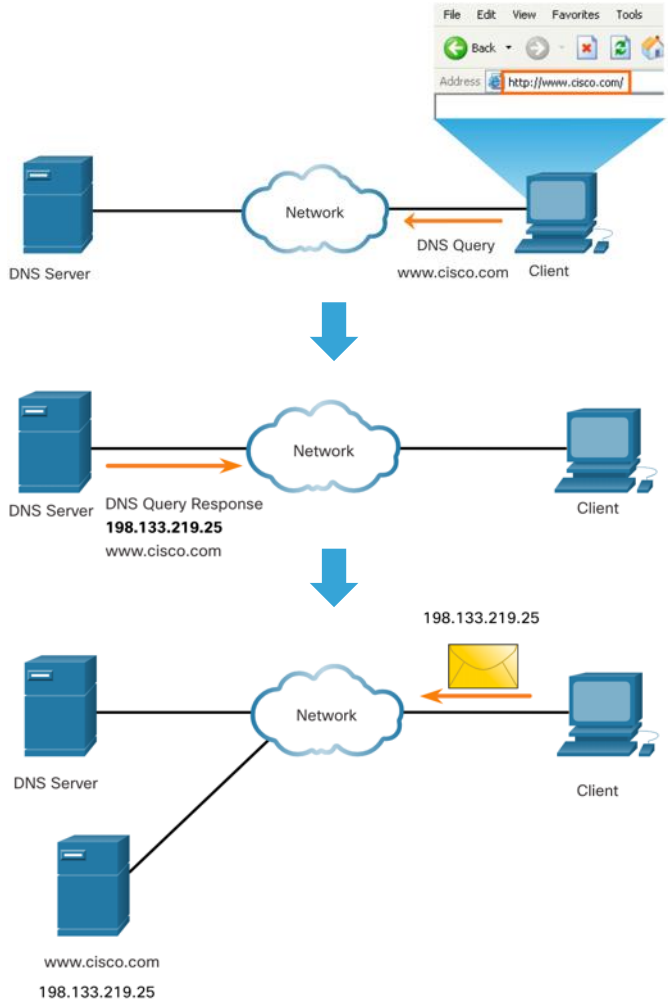
- Unlike POP, when a user connects to an IMAP server, copies of the messages are downloaded to the client application. The original messages are kept on the server until manually deleted.
- When a user decides to delete a message, the server synchronizes that action and deletes the message from the server.



15.4 IP Addressing Services

Domain Name Service

- Domain names were created to convert the numeric IP addresses into a simple, recognizable name.
- Fully-qualified domain names (FQDNs), such as http://www.cisco.com, are much easier for people to remember than 198.133.219.25.
- The DNS protocol defines an automated service that matches resource names with the required numeric network address. It includes the format for queries, responses, and data.



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.

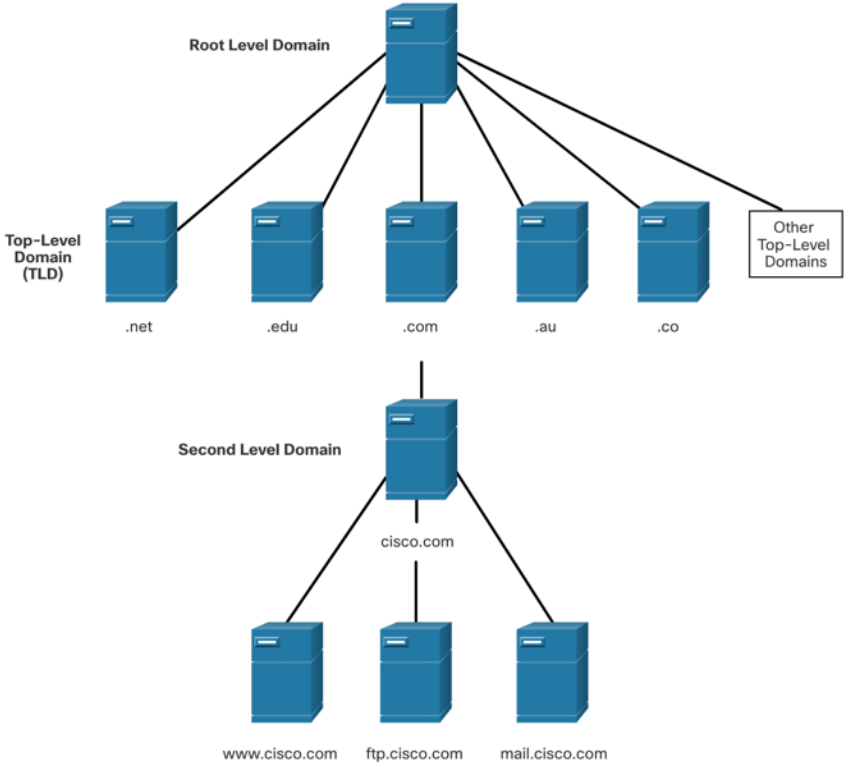
DNS Message Format (Cont.)

DNS uses the same message format between servers, consisting of a question, answer, authority, and additional information for all types of client queries and server responses, error messages, and transfer of resource record information.

DNS message section	Description
Question	The question for the name server
Answer	Resource Records answering the question
Authority	Resource Records pointing toward an authority
Additional	Resource Records holding additional information

DNS Hierarchy

- DNS uses a hierarchical system to create a database to provide name resolution.
- Each DNS server maintains a specific database file and is only responsible for managing name-to-IP mappings for that small portion of the entire DNS structure.
- When a DNS server receives a request for a name translation that is not within its DNS zone, the DNS server forwards the request to another DNS server within the proper zone for translation.
- Examples of top-level domains:
  - **.com** - a business or industry
  - **.org** - a non-profit organization
  - **.au** - Australia



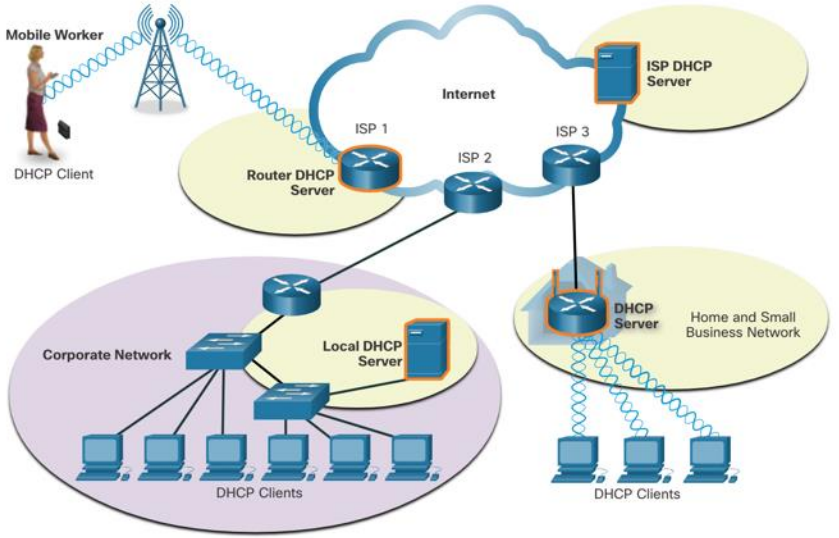
The nslookup Command

- Nslookup is a computer operating system utility that allows a user to manually query the DNS servers configured on the device to resolve a given host name.
- This utility can also be used to troubleshoot name resolution issues and to verify the current status of the name servers.
- When the **nslookup** command is issued, the default DNS server configured for your host is displayed.
- The name of a host or domain can be entered at the **nslookup** prompt.

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

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.
- DHCP is considered dynamic addressing compared to static addressing. Static addressing is manually entering IP address information.
- 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.
- 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.

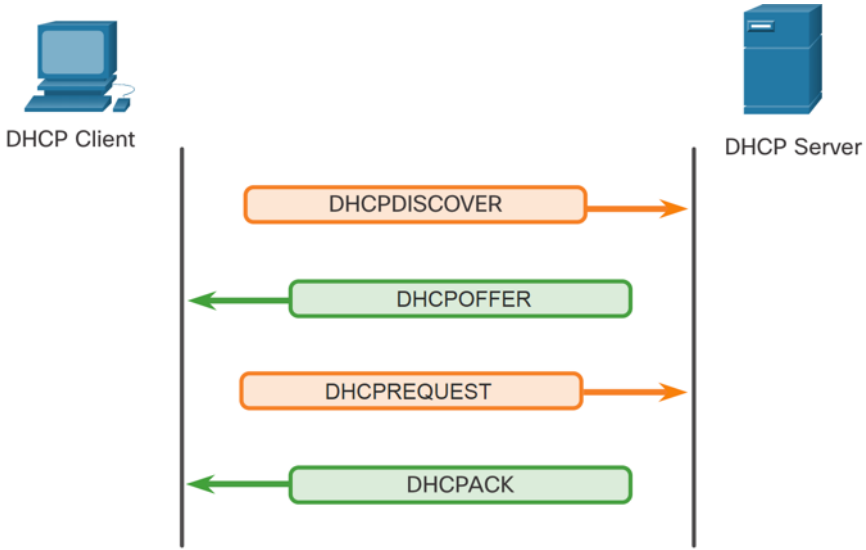


Note: DHCP for IPv6 (DHCPv6) provides similar services for IPv6 clients. However, DHCPv6 does not provide a default gateway address. This can only be obtained dynamically from the Router Advertisement message of the router.

DHCP Operation

The DHCP Process:

- 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. (If a client receives more than one offer due to multiple DHCP servers on the network, it must choose one.)
- The client sends a DHCP request (DHCPREQUEST) message that identifies the explicit server and lease offer that the client is accepting.
- The server then 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 and the process must begin with a new DHCPDISCOVER message.

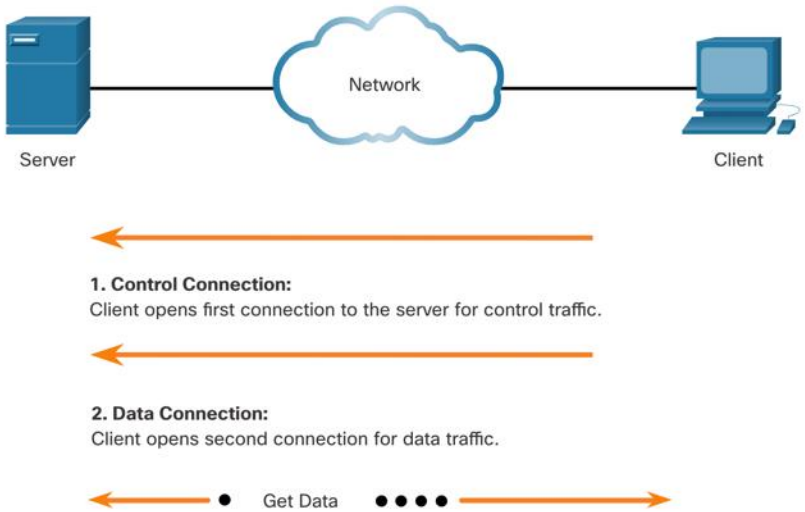


Note: DHCPv6 has a set of messages that is similar to those for DHCPv4. The DHCPv6 messages are SOLICIT, ADVERTISE, INFORMATION REQUEST, and REPLY.

15.5 File Sharing Services

File Transfer Protocol

FTP was developed to allow for data transfers between a client and a server. An FTP client is an application which runs on a computer that is being used to push and pull data from an FTP server.



Step 1 - The client establishes the first connection to the server for control traffic using TCP port 21. The traffic consists of client commands and server replies.

Step 2 - The client establishes the second connection to the server for the actual data transfer using TCP port 20. This connection is created every time there is data to be transferred.

Step 3 - The data transfer can happen in either direction. The client can download (pull) data from the server, or the client can upload (push) data to the server.

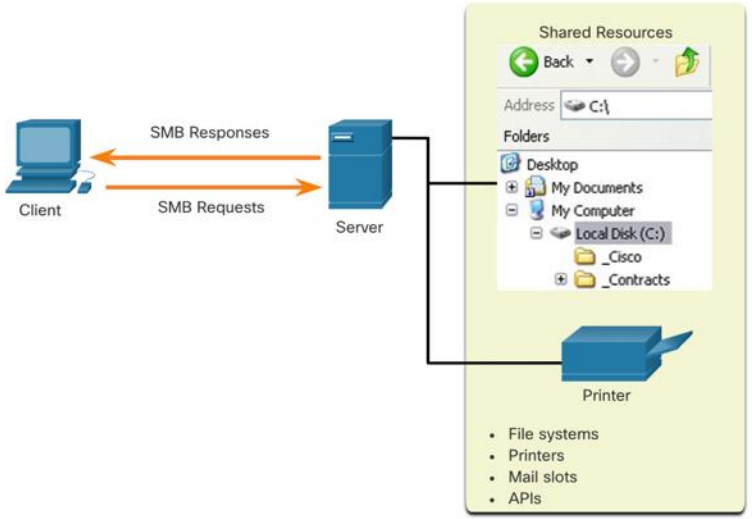
Server Message Block

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

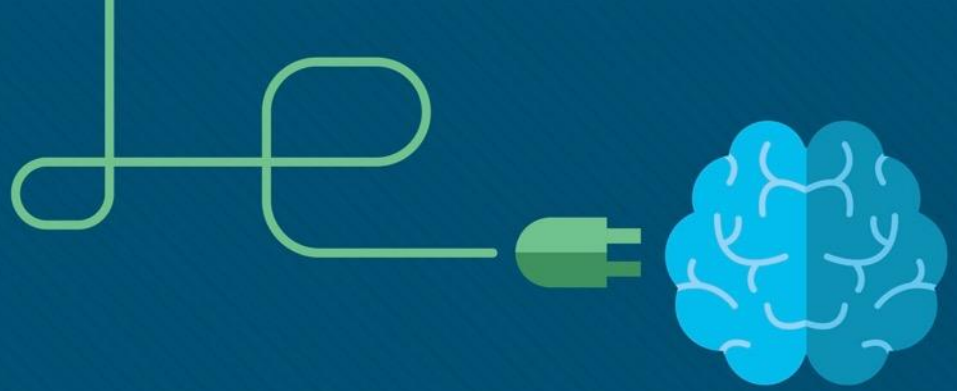
Unlike the file sharing supported by FTP, clients establish a long-term connection to servers. After the connection is established, the user of the client can access the resources on the server as though the resource is local to the client host.



15.6 Module Practice and Quiz

What did I learn in this module?

- 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, compressing data, and encrypting data for transmission and decrypting data upon receipt. The session layer creates and maintains dialogs between source and destination applications.
- 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.
- In a P2P network, two or more computers are connected via a network and can share resources without having a dedicated server.
- The three common HTTP message types are GET, POST, and PUT.
- Email supports three separate protocols for operation: SMTP, POP, and IMAP.
- DNS protocol matches resource names with the required numeric network address.
- DHCP for IPv4 service automates the assignment of IPv4 addresses, subnet masks, gateways, and other IPv4 networking parameters. The DHCPv6 messages are SOLICIT, ADVERTISE, INFORMATION REQUEST, and REPLY.
- An FTP client is an application which runs on a computer that is being used to push and pull data from an FTP server.
- 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.



Module 16: Network Security Fundamentals

Introduction to Networks v7.0
(ITN)

Module Objectives

Module Title: Network Security Fundamentals

Module Objective: Configure switches and routers with device hardening features to enhance security.

Topic Title	Topic Objective
Security Threats and Vulnerabilities	Explain why basic security measure are necessary on network devices.
Network Attacks	Identify security vulnerabilities.
Network Attack Mitigation	Identify general mitigation techniques.
Device Security	Configure network devices with device hardening features to mitigate security threats.

16.1 Security Threats and Vulnerabilities

Types of Threats

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 can gain access to a network through software vulnerabilities, hardware attacks, or through guessing someone's username and password. Intruders who gain access by modifying software or exploiting software vulnerabilities are called 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
- Disruption of Service

Types of Vulnerabilities

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 Vulnerabilities might include TCP/IP Protocol weaknesses, Operating System Weaknesses, and Network Equipment weaknesses.
- Configuration Vulnerabilities might include unsecured user accounts, system accounts with easily guessed passwords, misconfigured internet services, unsecure default settings, and misconfigured network equipment.
- Security Policy Vulnerabilities might include lack of a written security policy, politics, lack of authentication continuity, logical access controls not applied, software and hardware installation and changes not following policy, and a nonexistent disaster recovery plan.

All three of these sources of vulnerabilities can leave a network or device open to various attacks, including malicious code attacks and network attacks.

Physical Security

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.

A good plan for physical security must be created and implemented to address these issues.

16.2 Network Attacks

Types of Malware

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. The following 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.
- **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.
- **Trojan Horses -** It is a harmful piece of software that looks legitimate. 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.

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.

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.

Access attacks can be classified into four types:

- **Password attacks -** Implemented using brute force, trojan horse, and packet sniffers
- **Trust exploitation -** A threat actor uses unauthorized privileges to gain access to a system, possibly compromising the target.
- **Port redirection**: - A threat actor uses a compromised system as a base for attacks against other targets. For example, a threat actor using SSH (port 22) to connect to a compromised host A. Host A is trusted by host B and, therefore, the threat actor can use Telnet (port 23) to access it.
- **Man-in-the middle -** The threat actor is positioned in between two legitimate entities in order to read or modify the data that passes between the two parties.

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 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.
- 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.

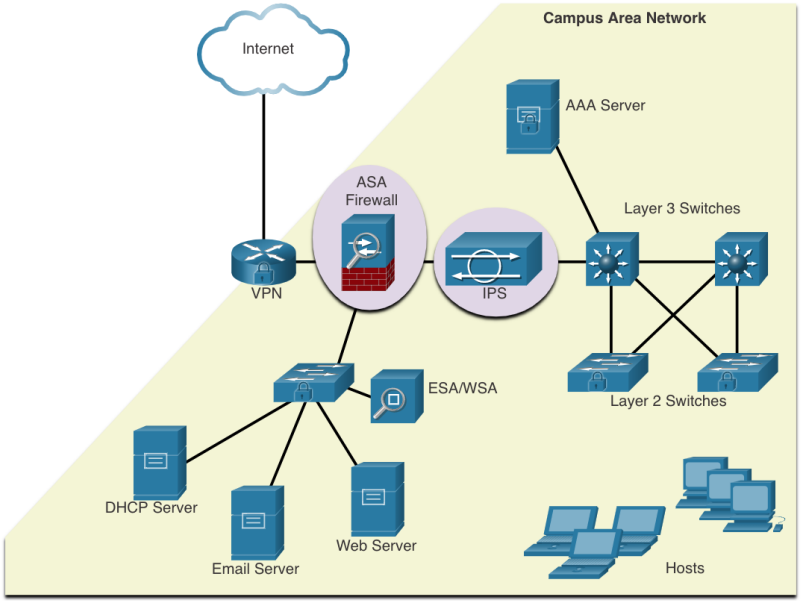
16.3 Network Attack Mitigations

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 (Adaptive Security Appliance) Firewall
- IPS (Intrusion Prevention System)
- ESA/WSA (Email Security Appliance/
- Web Security Appliance)
- AAA Server (Authentication, Authorization, and Accounting)



Keep Backups

Backing up device configurations and data is one of the most effective ways of protecting against data loss. 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.

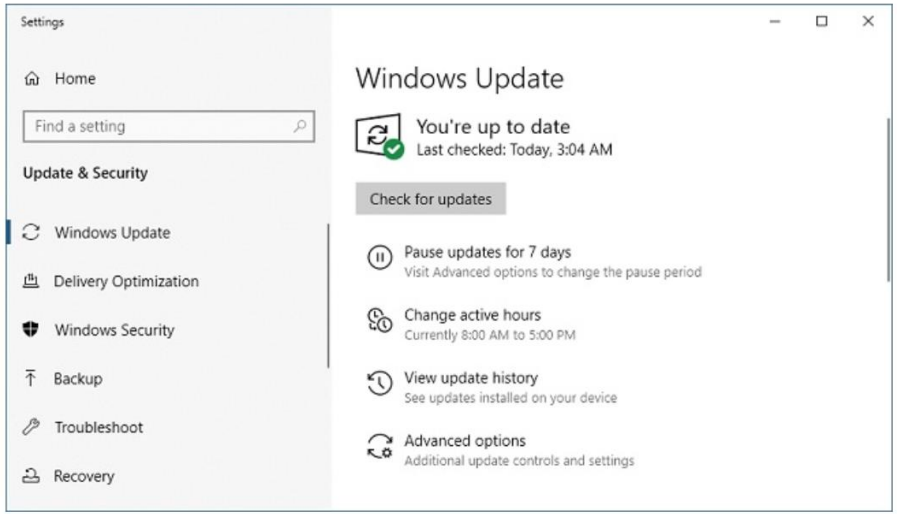
The table shows backup considerations and their descriptions.

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.
Storage	•Always validate backups to ensure the integrity of the data and validate the file restoration procedures.
Security	•Backups should be transported to an approved offsite storage location on a daily, weekly, or monthly rotation, as required by the security policy.
Validation	•Backups should be protected using strong passwords. The password is required to restore the data.

Upgrade, Update, and Patch

As new malware is released, enterprises need to keep current with the latest versions of antivirus software.

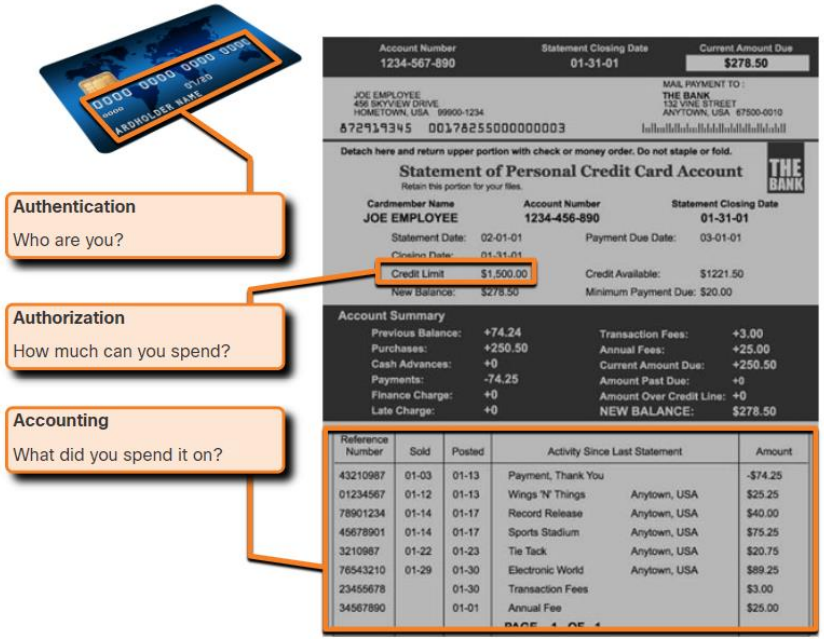
- The most effective way to mitigate a worm attack is to download security updates from the operating system vendor and patch all vulnerable systems.
- One solution to the management of critical security patches is to make sure all end systems automatically download updates.



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.

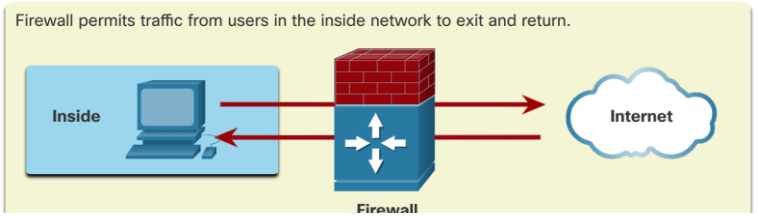
- AAA is a way to control who is permitted to access a network (authenticate), what actions they perform while accessing the network (authorize), and making a record of what was done while they are there (accounting).
- The concept of AAA is similar to the use of a credit card. The credit card identifies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

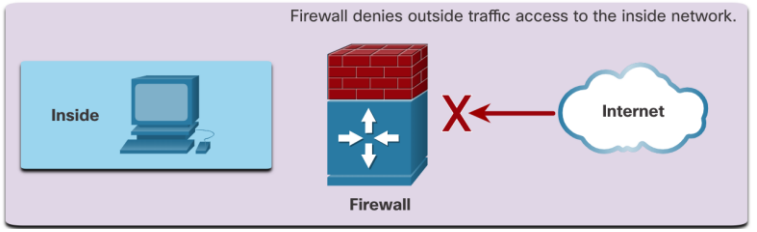


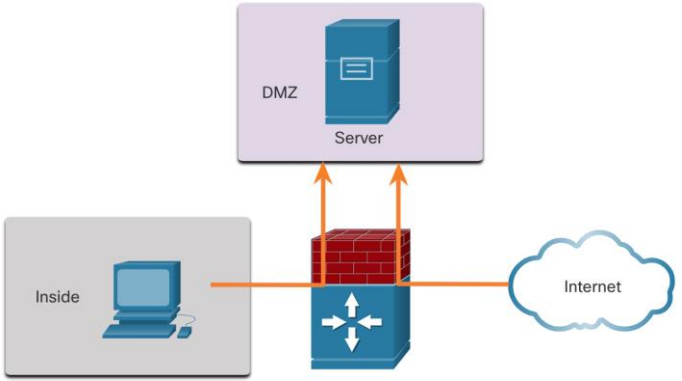
Firewalls

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.

16.4 Device Security

Cisco AutoSecure

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.

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.

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#
```

Enable SSH

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

1. **Configure a unique device hostname**. A device must have a unique hostname other than the default.
2. **Configure the IP domain name**. Configure the IP domain name of the network by using the global configuration mode command **ip-domain name**.
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.
4. **Verify or create a local database entry**. Create a local database username entry using the **username** global configuration command.
5. **Authenticate against the local database**. Use the **login local** line configuration command to authenticate the vty line against the local database.
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.

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.
- IOS versions prior to IOS-XE use the **show control-plane host open-ports** command.

16.5 Module Practice and Quiz

Packet Tracer – Secure Network Devices

In this activity you will configure a router and a switch based on a list of requirements.

Lab – Secure Network Devices

In this lab, you will complete the following objectives:

- Configure Basic Device Settings
- Configure Basic Security Measures on the Router
- Configure Basic Security Measures on the Switch

What Did I Learn In This Module?

- 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.
- 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.
- 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.

What Did I Learn In This Module? (Cont.)

- 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.
- 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.

What Did I Learn In This Module? (Cont.)

- 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 passphrase 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.


CISCO