**NJ3 - CCNA: Introduction to Networks**

**Host Roles**

All computers that are connected to a network and participate directly in network communication are classified as hosts. Hosts can be called end devices. Some hosts are also called clients. However, the term hosts specifically refers to devices on the network that are assigned a number for communication purposes. This number identifies the host within a particular network. This number is called the Internet Protocol (IP) address. An IP address identifies the host and the network to which the host is attached.

Servers are computers with software that allow them to provide information, like email or web pages, to other end devices on the network. Each service requires separate server software. For example, a server requires web server software in order to provide web services to the network. A computer with server software can provide services simultaneously to many different clients.

A cloud with text in the middle

Description automatically generated

A screenshot of a computer program

Description automatically generated

**Peer-to-peer**

Client and server software usually run on separate computers, but it is also possible for one computer to be used for both roles at the same time. In small businesses and homes, many computers function as the servers and clients on the network. This type of network is called a peer-to-peer network.

A black screen with white text

Description automatically generated

**End Devices**

Each end device on a network has an address. When an end device initiates communication, it uses the address of the destination end device to specify where to deliver the message.

An end device is either the source or destination of a message transmitted over the network.

**Intermediary Devices**

Intermediary devices connect the individual end devices to the network. They can connect multiple individual networks to form an internetwork. These intermediary devices provide connectivity and ensure that data flows across the network.

Intermediary devices use the destination end device address, in conjunction with information about the network interconnections, to determine the path that messages should take through the network.

A group of blue cubes with white text

Description automatically generated

A black background with white text

Description automatically generated

**Network Media**

Communication transmits across a network on media. The media provides the channel over which the message travels from source to destination.

Modern networks primarily use three types of media to interconnect devices, as shown in the figure:

* **Metal wires within cables** - Data is encoded into electrical impulses.
* **Glass or plastic fibers within cables (fiber-optic cable)** - Data is encoded into pulses of light.
* **Wireless transmission** - Data is encoded via modulation of specific frequencies of electromagnetic waves.

In addition to these representations, specialized terminology is used to describe how each of these devices and media connect to each other:

* **Network Interface Card (NIC)** - A NIC physically connects the end device to the network.
* **Physical Port** - A connector or outlet on a networking device where the media connects to an end device or another networking device.
* **Interface** - Specialized ports on a networking device that connect to individual networks. Because routers connect networks, the ports on a router are referred to as network interfaces.

**Topology Diagrams**

**Physical Topology Diagrams**

Physical topology diagrams illustrate the physical location of intermediary devices and cable installation

A diagram of a computer network

Description automatically generated

**Logical Topology Diagrams**

Logical topology diagrams illustrate devices, ports, and the addressing scheme of the network, as shown in the figure.

A diagram of a network

Description automatically generated

**LANs and WANs**

Network infrastructures vary greatly in terms of:

* Size of the area covered
* Number of users connected
* Number and types of services available
* Area of responsibility

The two most common types of network infrastructures are Local Area Networks (LANs), and Wide Area Networks (WANs). A LAN is a network infrastructure that provides access to users and end devices in a small geographical area. A LAN is typically used in a department within an enterprise, a home, or a small business network. A WAN is a network infrastructure that provides access to other networks over a wide geographical area, which is typically owned and managed by a larger corporation or a telecommunications service provider.

A diagram of a cloud computing network

Description automatically generated

**LANs**

A LAN is a network infrastructure that spans a small geographical area. LANs have specific characteristics:

* LANs interconnect end devices in a limited area such as a home, school, office building, or campus.
* A LAN is usually administered by a single organization or individual. Administrative control is enforced at the network level and governs the security and access control policies.
* LANs provide high-speed bandwidth to internal end devices and intermediary devices, as shown in the figure.

**WANs**

A WAN is a network infrastructure that spans a wide geographical area. WANs are typically managed by service providers (SPs) or Internet Service Providers (ISPs).

WANs have specific characteristics:

* WANs interconnect LANs over wide geographical areas such as between cities, states, provinces, countries, or continents.
* WANs are usually administered by multiple service providers.
* WANs typically provide slower speed links between LANs.

A diagram of a branch server

Description automatically generated

There are two other terms which are similar to the term internet: intranet and extranet.

Intranet is a term often used to refer to a private connection of LANs and WANs that belongs to an organization. An intranet is designed to be accessible only by the organization's members, employees, or others with authorization.

An organization may use an extranet to provide secure and safe access to individuals who work for a different organization but require access to the organization’s data. Here are some examples of extranets:

* A company that is providing access to outside suppliers and contractors
* A hospital that is providing a booking system to doctors so they can make appointments for their patients
* A local office of education that is providing budget and personnel information to the schools in its district

A diagram of a company

Description automatically generated

**Home and Small Office Internet Connections**

The figure illustrates common connection options for small office and home office users.

A diagram of a communication system

Description automatically generated

* **Cable** - Typically offered by cable television service providers, the internet data signal transmits on the same cable that delivers cable television. It provides a high bandwidth, high availability, and an always-on connection to the internet.
* **DSL** - Digital Subscriber Lines also provide high bandwidth, high availability, and an always-on connection to the internet. DSL runs over a telephone line. In general, small office and home office users connect using Asymmetrical DSL (ADSL), which means that the download speed is faster than the upload speed.
* **Cellular** - Cellular internet access uses a cell phone network to connect. Wherever you can get a cellular signal, you can get cellular internet access. Performance is limited by the capabilities of the phone and the cell tower to which it is connected.
* **Satellite** - The availability of satellite internet access is a benefit in those areas that would otherwise have no internet connectivity at all. Satellite dishes require a clear line of sight to the satellite.
* **Dial-up Telephone** - An inexpensive option that uses any phone line and a modem. The low bandwidth provided by a dial-up modem connection is not sufficient for large data transfer, although it is useful for mobile access while traveling.

**Businesses Internet Connections**

Corporate connection options differ from home user options. Businesses may require higher bandwidth, dedicated bandwidth, and managed services. Connection options that are available differ depending on the type of service providers located nearby.

A diagram of a satellite network

Description automatically generated

* **Dedicated Leased Line** - Leased lines are reserved circuits within the service provider’s network that connect geographically separated offices for private voice and/or data networking. The circuits are rented at a monthly or yearly rate.
* **Metro Ethernet** - This is sometimes known as Ethernet WAN. In this module, we will refer to it as Metro Ethernet. Metro ethernets extend LAN access technology into the WAN. Ethernet is a LAN technology you will learn about in a later module.
* **Business DSL** - Business DSL is available in various formats. A popular choice is Symmetric Digital Subscriber Line (SDSL) which is similar to the consumer version of DSL but provides uploads and downloads at the same high speeds.
* **Satellite** - Satellite service can provide a connection when a wired solution is not available.

**Network Architecture**

The term network architecture, in this context, refers to the technologies that support the infrastructure and the programmed services and rules, or protocols, that move data across the network.

As networks evolve, we have learned that there are four basic characteristics that network architects must address to meet user expectations:

* Fault Tolerance
* Scalability
* Quality of Service (QoS)
* Security

**Fault Tolerance**

A fault tolerant network is one that limits the number of affected devices during a failure. It is built to allow quick recovery when such a failure occurs. These networks depend on multiple paths between the source and destination of a message. If one path fails, the messages are instantly sent over a different link. Having multiple paths to a destination is known as redundancy.

Implementing a packet-switched network is one way that reliable networks provide redundancy. Packet switching splits traffic into packets that are routed over a shared network. A single message, such as an email or a video stream, is broken into multiple message blocks, called packets. Each packet has the necessary addressing information of the source and destination of the message. The routers within the network switch the packets based on the condition of the network at that moment. This means that all the packets in a single message could take very different paths to the same destination.

A diagram of a network

Description automatically generated

**Scalability**

A scalable network expands quickly to support new users and applications. It does this without degrading the performance of services that are being accessed by existing users.

A diagram of a network

Description automatically generated

These networks are scalable because the designers follow accepted standards and protocols. This lets software and hardware vendors focus on improving products and services without having to design a new set of rules for operating within the network.

**Quality of Service**

Quality of Service (QoS) is an increasing requirement of networks today. New applications available to users over networks, such as voice and live video transmissions, create higher expectations for the quality of the delivered services. Have you ever tried to watch a video with constant breaks and pauses? As data, voice, and video content continue to converge onto the same network, QoS becomes a primary mechanism for managing congestion and ensuring reliable delivery of content to all users.

Congestion occurs when the demand for bandwidth exceeds the amount available. Network bandwidth is measured in the number of bits that can be transmitted in a single second, or bits per second (bps). When simultaneous communications are attempted across the network, the demand for network bandwidth can exceed its availability, creating network congestion.

When the volume of traffic is greater than what can be transported across the network, devices will hold the packets in memory until resources become available to transmit them. With a QoS policy in place, the router can manage the flow of data and voice traffic, giving priority to voice communications if the network experiences congestion. The focus of QoS is to prioritize time-sensitive traffic. The type of traffic, not the content of the traffic, is what is important.

A diagram of a computer network

Description automatically generated

**Network Security**

The network infrastructure, services, and the data contained on network-attached devices are crucial personal and business assets. Network administrators must address two types of network security concerns: network infrastructure security and information security.

Securing the network infrastructure includes physically securing devices that provide network connectivity and preventing unauthorized access to the management software that resides on them.

A diagram of a network

Description automatically generated

Network administrators must also protect the information contained within the packets being transmitted over the network, and the information stored on network attached devices. In order to achieve the goals of network security, there are three primary requirements.

* **Confidentiality** - Data confidentiality means that only the intended and authorized recipients can access and read data.
* **Integrity** - Data integrity assures users that the information has not been altered in transmission, from origin to destination.
* **Availability** - Data availability assures users of timely and reliable access to data services for authorized users.

As new technologies and end-user devices come to market, businesses and consumers must continue to adjust to this ever-changing environment. There are several networking trends that affect organizations and consumers:

* Bring Your Own Device (BYOD)
* Online collaboration
* Video communications
* Cloud Computing

**Bring Your Own Device (BYOD)**

BYOD enables end users the freedom to use personal tools to access information and communicate across a business or campus network. With the growth of consumer devices, and the related drop in cost, employees and students may have advanced computing and networking devices for personal use. These include laptops, notebooks, tablets, smart phones, and e-readers. These may be purchased by the company or school, purchased by the individual, or both. BYOD means any device, with any ownership, used anywhere.  
  
**Online Collaboration**

Collaboration is a critical and strategic priority that organizations are using to remain competitive. Collaboration is also a priority in education. Students need to collaborate to assist each other in learning, to develop the team skills used in the workforce, and to work together on team-based projects.

**Video Communications**

Another facet of networking that is critical to the communication and collaboration effort is video. Video is used for communications, collaboration, and entertainment. Video calls are made to and from anyone with an internet connection, regardless of where they are located.

Video conferencing is a powerful tool for communicating with others, both locally and globally. Video is becoming a critical requirement for effective collaboration as organizations extend across geographic and cultural boundaries.

**Cloud Computing**

Cloud computing is one of the ways that we access and store data. Cloud computing allows us to store personal files, even backup an entire drive on servers over the internet. Applications such as word processing and photo editing can be accessed using the cloud.

For businesses, Cloud computing extends the capabilities of IT without requiring investment in new infrastructure, training new personnel, or licensing new software. These services are available on-demand and delivered economically to any device that is anywhere in the world without compromising security or function.

Cloud computing is possible because of data centers. Data centers are facilities used to house computer systems and associated components. A data center can occupy one room of a building, one or more floors, or an entire warehouse-sized building. Data centers are typically very expensive to build and maintain. For this reason, only large organizations use privately built data centers to house their data and provide services to users. Smaller organizations that cannot afford to maintain their own private data center can reduce the overall cost of ownership by leasing server and storage services from a larger data center organization in the cloud.

For security, reliability, and fault tolerance, cloud providers often store data in distributed data centers. Instead of storing all the data of a person or an organization in one data center, it is stored in multiple data centers in different locations.

There are four primary types of clouds: Public clouds, Private clouds, Hybrid clouds, and Community clouds, as shown in the table.

A screenshot of a computer

Description automatically generated

**Powerline Networking**

Powerline networking for home networks uses existing electrical wiring to connect devices, as shown in the figure.

A diagram of a room with a computer and a power outlet

Description automatically generated

Using a standard powerline adapter, devices can connect to the LAN wherever there is an electrical outlet. No data cables need to be installed, and there is little to no additional electricity used. Using the same wiring that delivers electricity, powerline networking sends information by sending data on certain frequencies.

Powerline networking is especially useful when wireless access points cannot reach all the devices in the home. Powerline networking is not a substitute for dedicated cabling in data networks. However, it is an alternative when data network cables or wireless communications are not possible or effective.

**Wireless Broadband**

**Wireless Internet Service Provider**

A Wireless Internet Service Provider (WISP) is an ISP that connects subscribers to a designated access point or hot spot using similar wireless technologies found in home wireless local area networks (WLANs). WISPs are more commonly found in rural environments where DSL or cable services are not available.

Although a separate transmission tower may be installed for the antenna, typically the antenna is attached to an existing elevated structure, such as a water tower or a radio tower. A small dish or antenna is installed on the subscriber’s roof in range of the WISP transmitter. The subscriber’s access unit is connected to the wired network inside the home. From the perspective of the home user, the setup is not much different than DSL or cable service. The main difference is that the connection from the home to the ISP is wireless instead of a physical cable.

**Wireless Broadband Service**

Another wireless solution for the home and small businesses is wireless broadband, as shown in the figure.

A house with a radio tower

Description automatically generated

This solution uses the same cellular technology as a smart phone. An antenna is installed outside the house providing either wireless or wired connectivity for devices in the home. In many areas, home wireless broadband is competing directly with DSL and cable services.

**Security Threats**

There are several common external threats to networks:

* **Viruses, worms, and Trojan horses** - These contain malicious software or code running on a user device.
* **Spyware and adware** - These are types of software which are installed on a user’s device. The software then secretly collects information about the user.
* **Zero-day attacks** - Also called zero-hour attacks, these occur on the first day that a vulnerability becomes known.
* **Threat actor attacks** - A malicious person attacks user devices or network resources.
* **Denial of service attacks** - These attacks slow or crash applications and processes on a network device.
* **Data interception and theft** - This attack captures private information from an organization’s network.
* **Identity theft** - This attack steals the login credentials of a user in order to access private data.

It is equally important to consider internal threats. There have been many studies that show that the most common data breaches happen because of internal users of the network. This can be attributed to lost or stolen devices, accidental misuse by employees, and in the business environment, even malicious employees. With the evolving BYOD strategies, corporate data is much more vulnerable. Therefore, when developing a security policy, it is important to address both external and internal security threats

A diagram of a computer network

Description automatically generated

**Security Solutions**

These are the basic security components for a home or small office network:

* **Antivirus and antispyware** - These applications help to protect end devices from becoming infected with malicious software.
* **Firewall filtering** - Firewall filtering blocks unauthorized access into and out of the network. This may include a host-based firewall system that prevents unauthorized access to the end device, or a basic filtering service on the home router to prevent unauthorized access from the outside world into the network.

In contrast, the network security implementation for a corporate network usually consists of many components built into the network to monitor and filter traffic. Ideally, all components work together, which minimizes maintenance and improves security. Larger networks and corporate networks use antivirus, antispyware, and firewall filtering, but they also have other security requirements:

* **Dedicated firewall systems** - These provide more advanced firewall capabilities that can filter large amounts of traffic with more granularity.
* **Access control lists (ACL)** - These further filter access and traffic forwarding based on IP addresses and applications.
* **Intrusion prevention systems (IPS)** - These identify fast-spreading threats, such as zero-day or zero-hour attacks.
* **Virtual private networks (VPN)** - These provide secure access into an organization for remote workers.

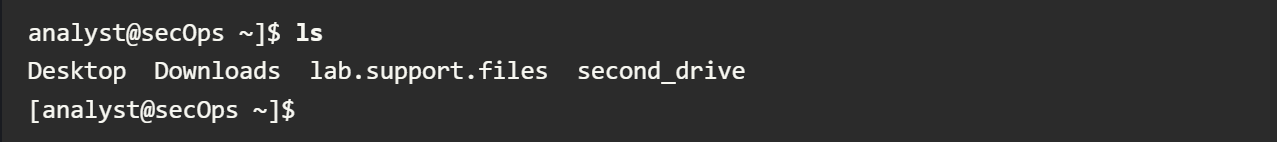
**2. Operating Systems**

All end devices and network devices require an operating system (OS). As shown in the figure, the portion of the OS that interacts directly with computer hardware is known as the kernel. The portion that interfaces with applications and the user is known as the shell. The user can interact with the shell using a command-line interface (CLI) or a graphical user interface (GUI).

A black background with white text

Description automatically generated

When using a CLI, the user interacts directly with the system in a text-based environment by entering commands on the keyboard at a command prompt, as shown in the example. The system executes the command, often providing textual output. The CLI requires very little overhead to operate. However, it does require that the user have knowledge of the underlying command structure that controls the system.



**GUI**

A GUI such as Windows, macOS, Linux KDE, Apple iOS, or Android allows the user to interact with the system using an environment of **graphical icons, menus, and windows.**

However, GUIs may not always be able to provide all the features available with the CLI. GUIs can also fail, crash, or simply not operate as specified. For these reasons, network devices are typically accessed through a CLI. The CLI is less resource intensive and very stable when compared to a GUI.

Network operating systems are similar to a PC operating system. Through a GUI, a PC operating system enables a user to do the following:

* Use a mouse to make selections and run programs
* Enter text and text-based commands
* View output on a monitor

**Access Methods**

A switch will forward traffic by default and does not need to be explicitly configured to operate. For example, two configured hosts connected to the same new switch would be able to communicate.

Regardless of the default behavior of a new switch, all switches should be configured and secured.

A black and white text on a black background

Description automatically generated

Because a **new switch** would not have any initial configurations, it could only be configured through the **console port.**

The AUX port on a Cisco device provided **out-of-band** connections over a telephone line.

**Terminal Emulation Programs**

There are several terminal emulation programs you can use to connect to a networking device either by a serial connection over a console port, or by an SSH/Telnet connection. These programs allow you to enhance your productivity by adjusting window sizes, changing font sizes, and changing color schemes.

**Primary Command Modes for Cisco IOS**

Using the CLI may provide the network administrator with more precise control and flexibility than using the GUI. This topic discusses using CLI to navigate the Cisco IOS.

As a security feature, the Cisco IOS software separates management access into the following two command modes:

* **User EXEC Mode** - This mode has limited capabilities but is useful for basic operations. It allows only a limited number of basic monitoring commands but does not allow the execution of any commands that might change the configuration of the device. The user EXEC mode is identified by the CLI prompt that ends with the > symbol.
* **Privileged EXEC Mode** - To execute configuration commands, a network administrator must access privileged EXEC mode. Higher configuration modes, like global configuration mode, can only be reached from privileged EXEC mode. The privileged EXEC mode can be identified by the prompt ending with the # symbol. **‘enable’** to enter privileged EXEC mode.

The table summarizes the two modes and displays the default CLI prompts of a Cisco switch and router.

A screenshot of a computer error

Description automatically generated

**Configuration Mode and Subconfiguration Modes**

To configure the device, the user must enter global configuration mode, which is commonly called global config mode. **‘configure terminal’**

From global config mode, CLI configuration changes are made that affect the operation of the device as a whole. Global configuration mode is identified by a prompt that ends with (config)# after the device name, such as **Switch(config)#**.

Global configuration mode is accessed before other specific configuration modes. From global config mode, the user can enter different subconfiguration modes. Each of these modes allows the configuration of a particular part or function of the IOS device. Two common subconfiguration modes include:

* **Line Configuration Mode** - Used to configure console, SSH, Telnet, or AUX access.
* **Interface Configuration Mode** - Used to configure a switch port or router network interface.

When the CLI is used, the mode is identified by the command-line prompt that is unique to that mode. By default, every prompt begins with the device name. Following the name, the remainder of the prompt indicates the mode. For example, the default prompt for line configuration mode is **Switch(config-line)#** and the default prompt for interface configuration mode is **Switch(config-if)#**.

**Navigating Between IOS Modes**

Various commands are used to move in and out of command prompts. To move from user EXEC mode to privileged EXEC mode, use the **enable** command. Use the **disable** privileged EXEC mode command to return to user EXEC mode.

**Note:** Privileged EXEC mode is sometimes called *enable mode*.

To move in and out of global configuration mode, use the **configure terminal** privileged EXEC mode command. To return to the privileged EXEC mode, enter the **exit** global config mode command. Or **config t**

There are many different subconfiguration modes. For example, to enter line subconfiguration mode, you use the **line** command followed by the management line type and number you wish to access. Use the **exit** command to exit a subconfiguration mode and return to global configuration mode.

To move from any subconfiguration mode of the global configuration mode to the mode one step above it in the hierarchy of modes, enter the **exit** command.

To move from any subconfiguration mode to the privileged EXEC mode, enter the **end** command or enter the key combination **Ctrl+Z**.



You can also move directly from one subconfiguration mode to another. Notice how after selecting an interface, the command prompt changes from **(config-line)#** to **(config-if)#**.



**2.3.1 Basic IOS Command Structure**

A Cisco IOS device supports many commands. Each IOS command has a specific format, or syntax, and can only be executed in the appropriate mode. The general syntax for a command, shown in the figure, is the command followed by any appropriate keywords and arguments.A diagram of a computer program

Description automatically generated

* **Keyword** - This is a specific parameter defined in the operating system (in the figure, **ip protocols**).
* **Argument** - This is not predefined; it is a value or variable defined by the user (in the figure, **192.168.10.5**).

**2.3.2 IOS Command Syntax Check**

A command might require one or more arguments. To determine the keywords and arguments required for a command, refer to the command syntax. The syntax provides the pattern, or format, that must be used when entering a command.

A screenshot of a computer

Description automatically generated

**2.3.3 IOS Help Features**

The IOS has two forms of help available: context-sensitive help and command syntax check.

Context-sensitive help enables you to quickly find answers to these questions:

* Which commands are available in each command mode?
* Which commands start with specific characters or group of characters?
* Which arguments and keywords are available to particular commands?

To access context-sensitive help, simply enter a question mark, **?**, at the CLI.

**2.3.5 Hot Keys and Shortcuts**

Commands and keywords can be shortened to the minimum number of characters that identify a unique selection. For example, the **configure** command can be shortened to **conf** because **configure** is the only command that begins with **conf**. An even shorter version, **con**, will not work because more than one command begins with **con**. Keywords can also be shortened.

A screenshot of a computer

Description automatically generated

**Note:** While the **Delete** key typically deletes the character to the right of the prompt, the IOS command structure does not recognize the Delete key.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**2.4.1 Device Names**

You have learned a great deal about the Cisco IOS, navigating the IOS, and the command structure. Now, you are ready to configure devices! The first configuration command on any device should be to give it a unique device name or hostname. By default, all devices are assigned a factory default name. For example, a Cisco IOS switch is "Switch."

The problem is if all switches in a network were left with their default names, it would be difficult to identify a specific device. For instance, how would you know that you are connected to the right device when accessing it remotely using SSH? The hostname provides confirmation that you are connected to the correct device.

The default name should be changed to something more descriptive. By choosing names wisely, it is easier to remember, document, and identify network devices. Here are some important naming guidelines for hosts:

* Start with a letter
* Contain no spaces
* End with a letter or digit
* Use only letters, digits, and dashes
* Be less than 64 characters in length

An organization must choose a naming convention that makes it easy and intuitive to identify a specific device. The hostnames used in the device IOS preserve capitalization and lowercase characters. For example, the figure shows that three switches, spanning three different floors, are interconnected together in a network. The naming convention that was used incorporated the location and the purpose of each device. Network documentation should explain how these names were chosen so additional devices can be named accordingly.

A diagram of a diagram of a desk

AI-generated content may be incorrect.

When the naming convention has been identified, the next step is to use the CLI to apply the names to the devices. As shown in the example, from the privileged EXEC mode, access the global configuration mode by entering the **configure terminal** command. Notice the change in the command prompt.

Switch# **configure terminal**

Switch(config)# **hostname Sw-Floor-1**

Sw-Floor-1(config)#

From global configuration mode, enter the command **hostname** followed by the name of the switch and press **Enter**. Notice the change in the command prompt name.

**Note:** To return the switch to the default prompt, use the **no hostname** global config command.

Always make sure the documentation is updated each time a device is added or modified. Identify devices in the documentation by their location, purpose, and address.

**2.4.2 Password Guidelines**

All networking devices should limit administrative access by securing privileged EXEC, user EXEC, and remote Telnet access with passwords. In addition, all passwords should be encrypted and legal notifications provided.

When choosing passwords, use strong passwords that are not easily guessed. There are some key points to consider when choosing passwords:

* Use passwords that are more than eight characters in length.
* Use a combination of upper and lowercase letters, numbers, special characters, and/or numeric sequences.
* Avoid using the same password for all devices.
* Do not use common words because they are easily guessed.

**2.4.3 Configure Passwords**

When you initially connect to a device, you are in user EXEC mode. This mode is secured using the console.

To secure user EXEC mode access, enter line console configuration mode using the **line console 0** global configuration command, as shown in the example. The zero is used to represent the first (and in most cases the only) console interface. Next, specify the user EXEC mode password using the **password** *password* command. Finally, enable user EXEC access using the **login** command.

Sw-Floor-1# **configure terminal**

Sw-Floor-1(config)# **line console 0**

Sw-Floor-1(config-line)# **password cisco**

Sw-Floor-1(config-line)# **login**

Sw-Floor-1(config-line)# **end**

Sw-Floor-1#

Console access will now require a password before allowing access to the user EXEC mode.

To have administrator access to all IOS commands including configuring a device, you must gain privileged EXEC mode access. It is the most important access method because it provides complete access to the device.

To secure privileged EXEC access, use the **enable secret** *password* global config command, as shown in the example.

Sw-Floor-1# **configure terminal**

Sw-Floor-1(config)# **enable secret class**

Sw-Floor-1(config)# **exit**

Sw-Floor-1#

Virtual terminal (VTY) lines enable remote access using Telnet or SSH to the device. Many Cisco switches support up to 16 VTY lines that are numbered 0 to 15.

To secure VTY lines, enter line VTY mode using the **line vty 0 15** global config command. Next, specify the VTY password using the **password** *password* command. Lastly, enable VTY access using the **login** command.

An example of securing the VTY lines on a switch is shown.

Sw-Floor-1# **configure terminal**

Sw-Floor-1(config)# **line vty 0 15**

Sw-Floor-1(config-line)# **password cisco**

Sw-Floor-1(config-line)# **login**

Sw-Floor-1(config-line)# **end**

Sw-Floor-1#

**2.4.4 Encrypt Passwords**

The startup-config and running-config files display most passwords in plaintext. This is a security threat because anyone can discover the passwords if they have access to these files.

To encrypt all plaintext passwords, use the **service password-encryption** global config command as shown in the example.

Sw-Floor-1# **configure terminal**

Sw-Floor-1(config)# **service password-encryption**

Sw-Floor-1(config)#

The command applies weak encryption to all unencrypted passwords. This encryption applies only to passwords in the configuration file, not to passwords as they are sent over the network. The purpose of this command is to keep unauthorized individuals from viewing passwords in the configuration file.

Use the **show running-config** command to verify that passwords are now encrypted.

Sw-Floor-1(config)# **end**

Sw-Floor-1# **show running-config**

!

(Output omitted)

!

line con 0

password 7 094F471A1A0A

login

!

line vty 0 4

password 7 094F471A1A0A

login

line vty 5 15

password 7 094F471A1A0A

login

!

!

End

**2.4.5 Banner Messages**

Although requiring passwords is one way to keep unauthorized personnel out of a network, it is vital to provide a method for declaring that only authorized personnel should attempt to access the device. To do this, add a banner to the device output. Banners can be an important part of the legal process in the event that someone is prosecuted for breaking into a device. Some legal systems do not allow prosecution, or even the monitoring of users, unless a notification is visible.

To create a banner message of the day on a network device, use the **banner motd #** *the message of the day* **#** global config command. The “#” in the command syntax is called the delimiting character. It is entered before and after the message. The delimiting character can be any character as long as it does not occur in the message. For this reason, symbols such as the "#" are often used. After the command is executed, the banner will be displayed on all subsequent attempts to access the device until the banner is removed.

The following example shows the steps to configure the banner on Sw-Floor-1.

Sw-Floor-1# **configure terminal**

Sw-Floor-1(config)# **banner motd #Authorized Access Only#**

**2.5.1 Configuration Files**

You now know how to perform basic configuration on a switch, including passwords and banner messages. This topic will show you how to save your configurations.

There are two system files that store the device configuration:

* **startup-config** - This is the saved configuration file that is stored in NVRAM. It contains all the commands that will be used by the device upon startup or reboot. Flash does not lose its contents when the device is powered off.
* **running-config** - This is stored in Random Access Memory (RAM). It reflects the current configuration. Modifying a running configuration affects the operation of a Cisco device immediately. RAM is volatile memory. It loses all of its content when the device is powered off or restarted.

The **show running-config** privileged EXEC mode command is used to view the running config. As shown in the example, the command will list the complete configuration currently stored in RAM.

Sw-Floor-1# **show running-config**

Building configuration...

Current configuration : 1351 bytes

!

! Last configuration change at 00:01:20 UTC Mon Mar 1 1993

!

version 15.0

no service pad

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

!

hostname Sw-Floor-1

!

(output omitted)

To view the startup configuration file, use the **show startup-config** privileged EXEC command.

If power to the device is lost, or if the device is restarted, all configuration changes will be lost unless they have been saved. To save changes made to the running configuration to the startup configuration file, use the **copy running-config startup-config** privileged EXEC mode command.

**2.5.2 Alter the Running Configuration**

If changes made to the running config do not have the desired effect and the running-config has not yet been saved, you can restore the device to its previous configuration. Remove the changed commands individually, or reload the device using the **reload** privileged EXEC mode command to restore the startup-config.

The downside to using the **reload** command to remove an unsaved running config is the brief amount of time the device will be offline, causing network downtime.

When a reload is initiated, the IOS will detect that the running config has changes that were not saved to the startup configuration. A prompt will appear to ask whether to save the changes. To discard the changes, enter **n** or **no**.

Alternatively, if undesired changes were saved to the startup config, it may be necessary to clear all the configurations. This requires erasing the startup config and restarting the device. The startup config is removed by using the **erase startup-config** privileged EXEC mode command. After the command is issued, the switch will prompt you for confirmation. Press **Enter** to accept.

After removing the startup config from NVRAM, reload the device to remove the current running config file from RAM. On reload, a switch will load the default startup config that originally shipped with the device.