CCNA - V7

CHAPTER 1

Module Title: Networking Today

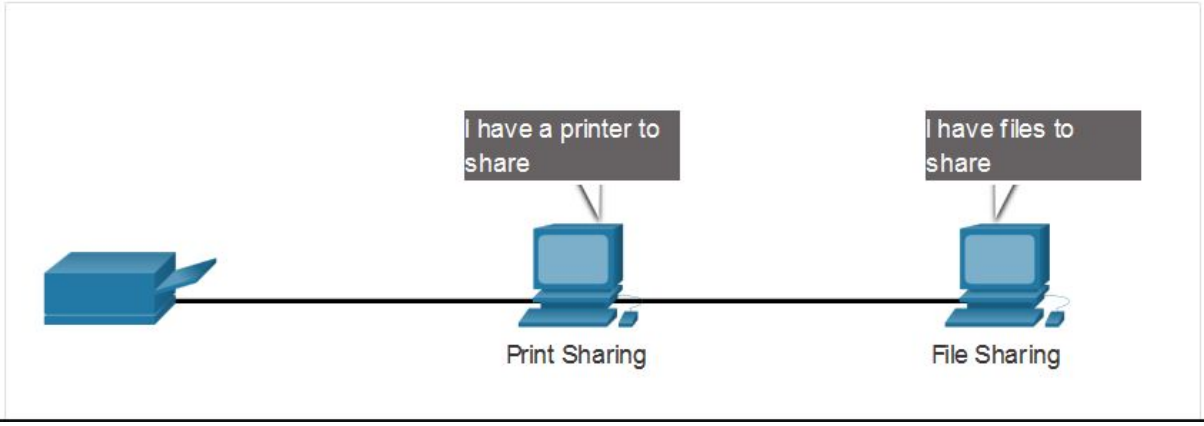
Module Objective: Explain the advances in modern network technologies.

Topic Title	Topic Objective
Networks Affect our Lives	Explain how networks affect our daily lives.
Network Components	Explain how host and network devices are used.
Network Representations and Topologies	Explain network representations and how they are used in network topologies.
Common Types of Networks	Compare the characteristics of common types of networks.
Internet Connections	Explain how LANs and WANs interconnect to the internet.
Reliable Networks	Describe the four basic requirements of a reliable network.
Network Trends	Explain how trends such as BYOD, online collaboration, video, and cloud computing are changing the way we interact.
Network Security	Identify some basic security threats and solution for all networks.
The IT Professional	Explain employment opportunities in the networking field.

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.

In the figure, the print sharing PC has a Universal Serial Bus (USB) connection to the printer and a network connection, using a network interface card (NIC), to the file sharing PC.



The advantages of peer-to-peer networking:

- Easy to set up
- Less complex
- Lower cost because network devices and dedicated servers may not be required
- Can be used for simple tasks such as transferring files and sharing printers

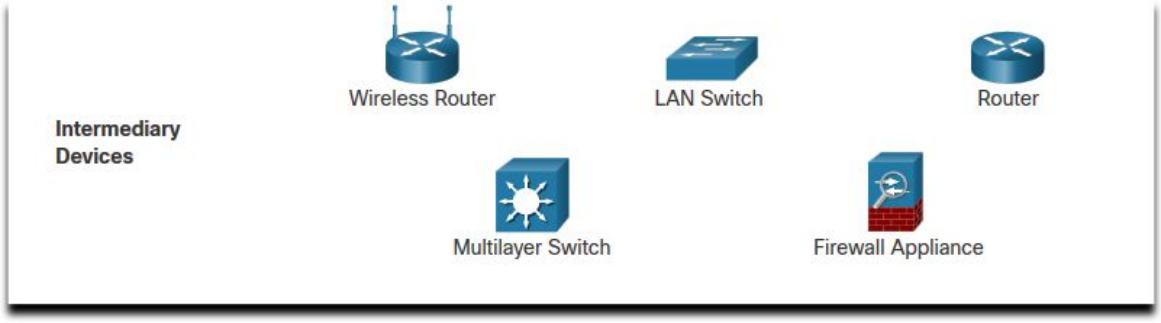
The disadvantages of peer-to-peer networking:

- No centralized administration
- Not as secure
- Not scalable
- All devices may act as both clients and servers which can slow their performance

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. Examples of the more common intermediary devices and a list of functions are shown in the figure.

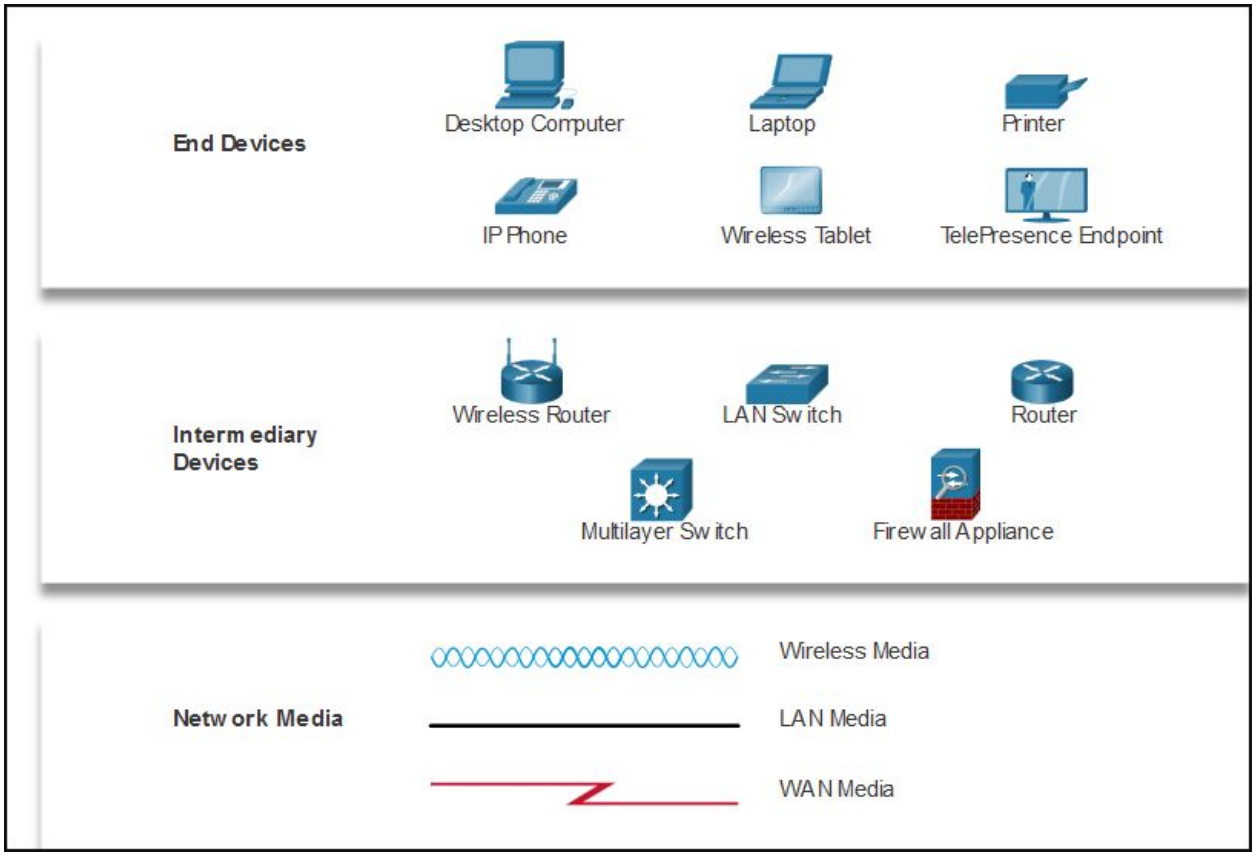


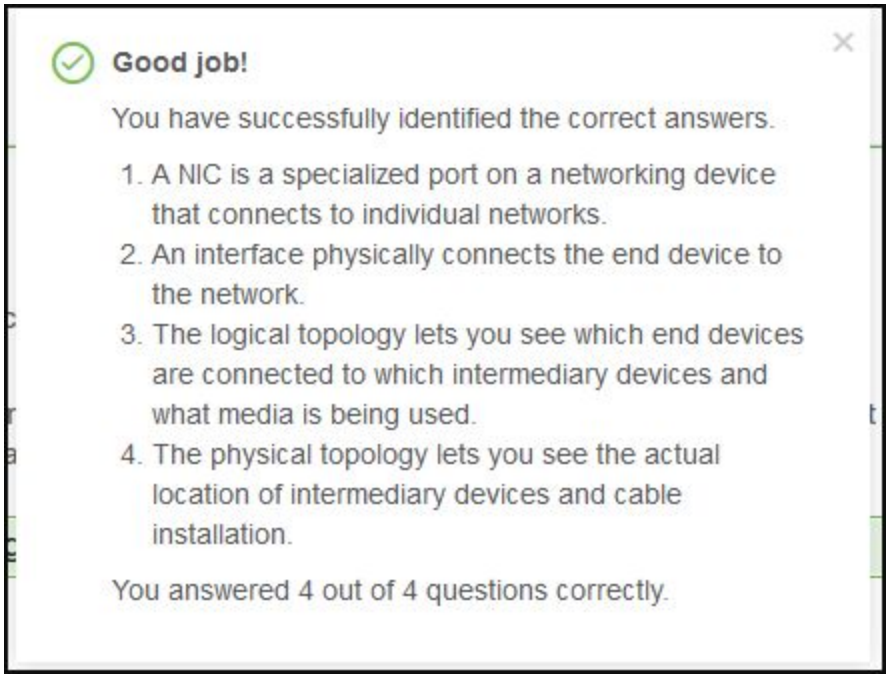
Intermediary network devices perform some or all of these functions:

- Regenerate and retransmit communication signals
- Maintain information about what pathways exist through the network and internetwork
- Notify other devices of errors and communication failures
- Direct data along alternate pathways when there is a link failure
- Classify and direct messages according to priorities
- Permit or deny the flow of data, based on security settings

Note: Not shown is a legacy Ethernet hub. An Ethernet hub is also known as a multiport repeater. Repeaters regenerate and retransmit communication signals. Notice that all intermediary devices perform the function of a repeater.

A diagram provides an easy way to understand how devices connect in a large network. This type of “picture” of a network is known as a topology diagram





Internet Engineering Task Force (IETF),
Internet Corporation for Assigned Names and Numbers (ICANN)
Internet Architecture Board (IAB)

Small Office

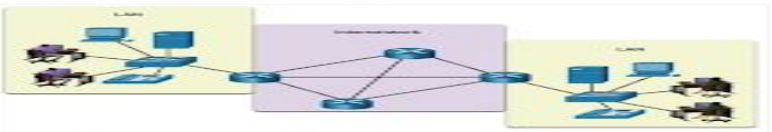
- **Cable** - Typically offered by cable television service providers, the internet data signal transmits on the same cable that delivers cable television. It provides a high bandwidth, high availability, and an always-on connection to the internet.
- **DSL** - Digital Subscriber Lines also provides 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.

Network Components

Host Roles

Peer-to-Peer

End Devices



Intermediary Devices

Network Media

Check Your Understanding – Network Components

Business

- **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.

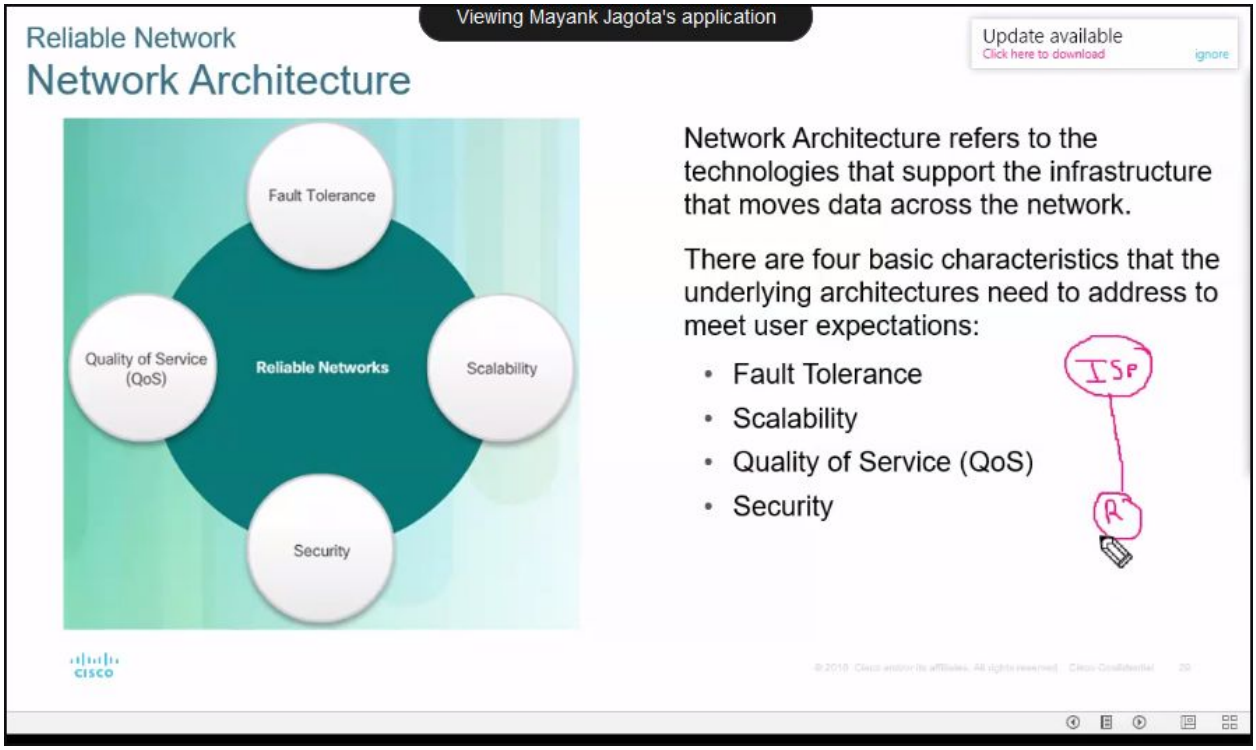
https://contenthub.netacad.com/itn/1.5.5

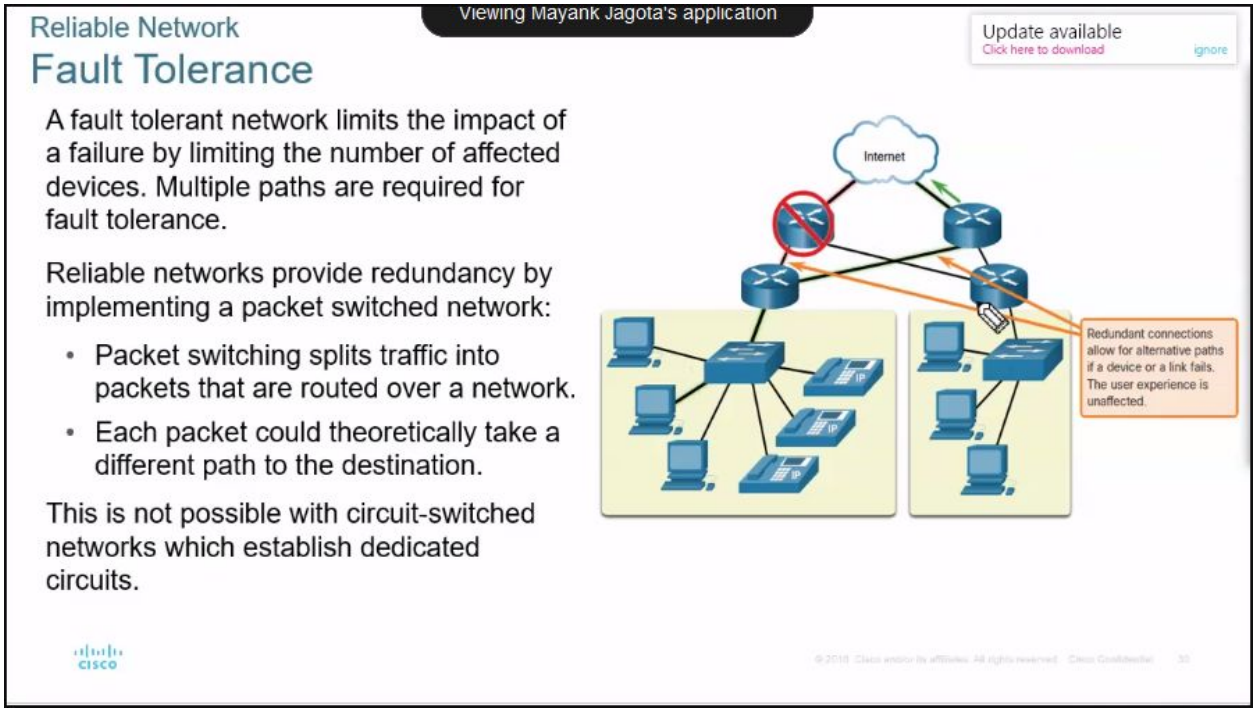
Hubs are at a disadvantage against switches in networking because **hubs** are unable to differentiate between the devices on the network. If one computer is trying to reach another on a **hub**-based network, the computer will send the message to every other computer on the network, consuming bandwidth for each transfer.

A **Hub** operates on the physical layer, whereas **Switch** operates on the data link layer.

hubs have been predominantly replaced by switches, since they are more intelligent devices that have the ability to learn the MAC address of every device connected to it and can send unicast data, instead of broadcasting potentially sensitive information to every device connected to the **hub**.

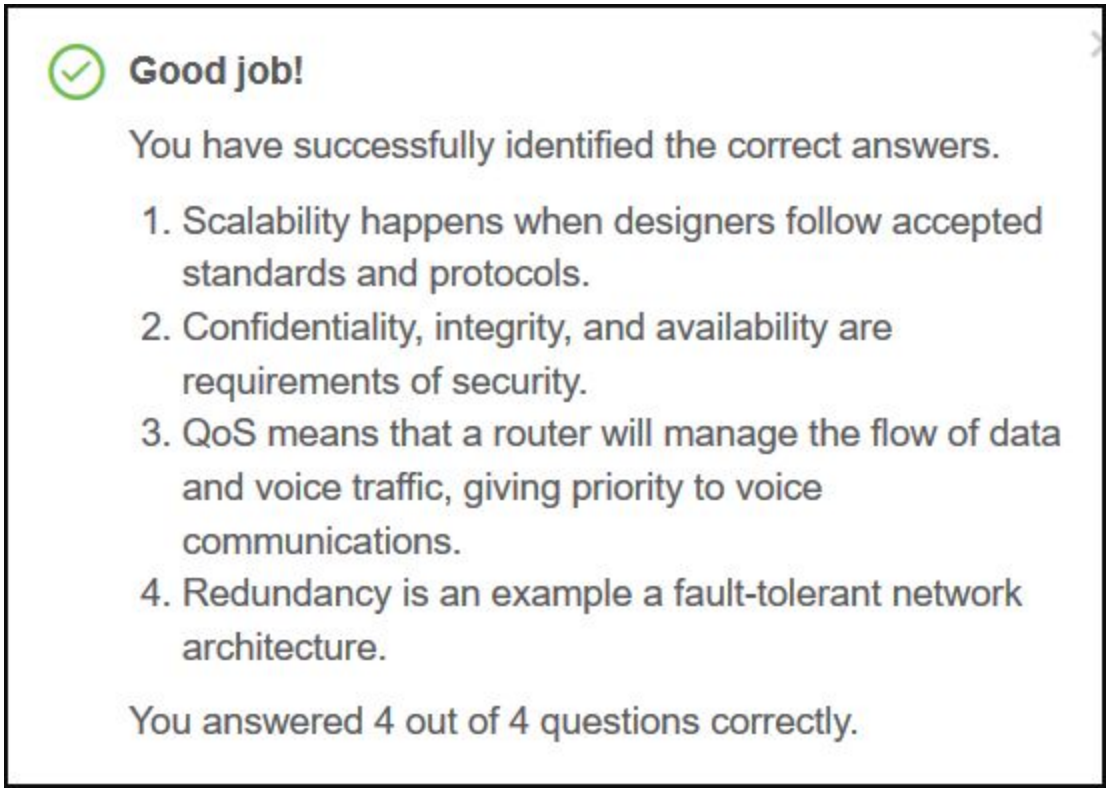
While a network **switch** can connect multiple devices and networks to expand the LAN, a **router** will allow you to share a single IP address among multiple network devices. In simpler terms, the Ethernet **switch** creates networks and the **router** allows for connections between networks





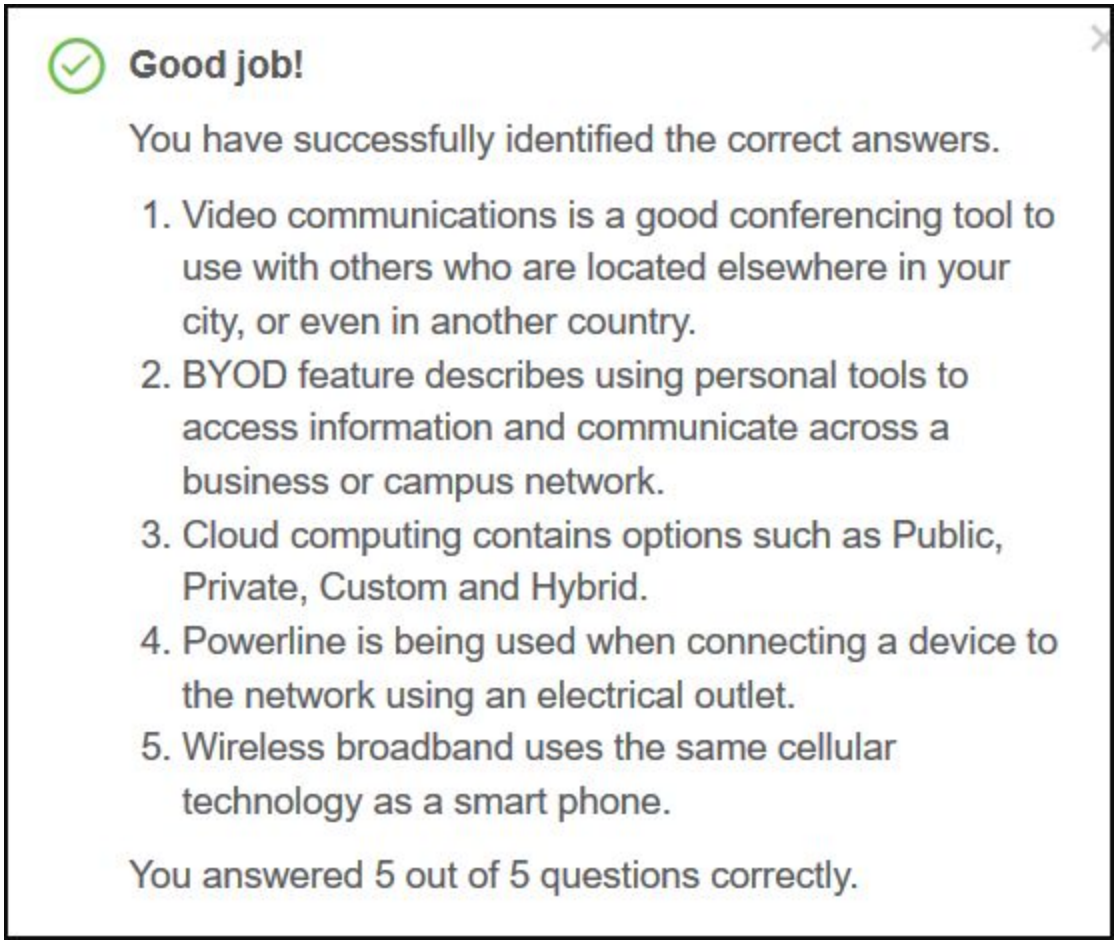
A fault tolerant network is one that limits the number of affected devices during a failure. It is built to allow quick recovery when such a failure occurs. These networks depend on multiple paths between the source and destination of a message. If one path fails, the messages are instantly sent over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

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.



Public clouds
Cloud-based applications and services offered in a public cloud are made available to the general population. Services may be free or are offered on a pay-per-use model, such as paying for online storage. The public cloud uses the internet to provide services.
Private clouds
Cloud-based applications and services offered in a private cloud are intended for a specific organization or entity, such as a government. A private cloud can be set up using the organization's private network, though this can be expensive to build and maintain. A private cloud can also be managed by an outside organization with strict access security.
Hybrid clouds
A hybrid cloud is made up of two or more clouds (example: part private, part public), where each part remains a distinct object, but both are connected using a single architecture. Individuals on a hybrid cloud would be able to have degrees of access to various services based on user access rights.
Community clouds
A community cloud is created for exclusive use by specific entities or organizations. The differences between public clouds and community clouds are the functional needs that have been customized for the community. For example, healthcare organizations must remain compliant with policies and laws (e.g., HIPAA) that require special authentication and confidentiality. Community clouds are used by multiple organizations that have similar needs

and concerns. Community clouds are similar to a public cloud environment, but with set levels of security, privacy, and even regulatory compliance of a private cloud.



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.

You have successfully identified the correct answers.

1. A DoS attack slows down or crashes equipment and programs.
2. A VPN creates a secure connection for remote workers.
3. A firewall blocks unauthorized access to your network.
4. A zero-day or zero-hour attack occurs on the first day that a vulnerability becomes known.
5. A virus, worm, or Trojan horse is malicious code running on user devices.

You answered 5 out of 5 questions correctly.

What did I learn in this module?

Networks Affect our Lives

In today's world, through the use of networks, we are connected like never before. People with ideas can communicate instantly with others to make those ideas a reality. The creation of online communities for the exchange of ideas and information has the potential to increase productivity opportunities across the globe. The creation of the cloud lets us store documents and pictures and access them anywhere, anytime.

Network Components

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. Many computers function as the servers and clients on the network. This type of network is called a peer-to-peer network. An end device is either the source or destination of a message transmitted over the network. Intermediary devices connect the individual end devices to the network and can connect multiple individual networks to form an internetwork. 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. The media provides the channel over which the message travels from source to destination.

Network Representations and Topologies

Diagrams of networks often use symbols to represent the different devices and connections that make up a network. A diagram provides an easy way to understand how devices connect in a large network. This type of "picture" of a network is known as a topology diagram. Physical topology diagrams illustrate the physical location of intermediary devices and cable installation. Logical topology diagrams illustrate devices, ports, and the addressing scheme of the network.

Common Types of Networks

Small home networks connect a few computers to each other and to the internet. The small office/home office (SOHO) network allows computers in a home office or a remote office to connect to a corporate network, or access centralized, shared resources. Medium to large networks, such as those used by corporations and schools, can have many locations with hundreds or thousands of interconnected hosts. The internet is a network of networks that connects hundreds of millions of computers world-wide. 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 spans a small geographical area. A WAN is a network infrastructure that spans a wide geographical area. Intranet refers to a private connection of LANs and WANs that belongs to an organization. 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.

Internet Connections

SOHO internet connections include cable, DSL, Cellular, Satellite, and Dial-up telephone. Business internet connections include Dedicated Leased Line, Metro Ethernet, Business DSL, and Satellite. The choice of connection varies depending on geographical location and service provider availability. Traditional separate networks used different technologies, rules, and standards. Converged networks deliver data, voice, and video between many different types of devices over the same network infrastructure. This network infrastructure uses the same set of rules, agreements, and implementation standards. Packet Tracer is a flexible software program that lets you use network representations and theories to build network models and explore relatively complex LANs and WANs.

Reliable Networks

The term network architecture 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), and Security. A fault tolerant network is one that limits the number of affected devices during a failure. Having multiple paths to a destination is known as redundancy. A scalable network expands quickly to support new users and applications. Networks are scalable because the designers follow accepted standards and protocols. QoS is a primary mechanism for managing congestion and ensuring reliable delivery of content to all users. Network administrators must address two types of network security concerns: network infrastructure security and information security. To achieve the goals of network security, there are three primary requirements: Confidentiality, Integrity, and Availability.

Network Trends

There are several recent networking trends that affect organizations and consumers: Bring Your Own Device (BYOD), online collaboration, video communications, and cloud computing. BYOD means any device, with any ownership, used anywhere. Collaboration tools, like Cisco WebEx give employees, students, teachers, customers, and partners a way to instantly connect, interact, and achieve their objectives. 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. 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. There are four primary types of Clouds: Public Clouds, Private Clouds, Hybrid Clouds, and Custom Clouds. Smart home technology is currently being developed for all rooms within a house. Smart home technology will become more common as home networking and high-speed internet technology expands. Using the same wiring that delivers electricity, powerline networking sends information by sending data on certain frequencies. 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).

Network Security

There are several common external threats to networks:

- Viruses, worms, and Trojan horses
- Spyware and adware
- Zero-day attacks
- Threat Actor attacks
- Denial of service attacks
- Data interception and theft
- Identity theft

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

- Antivirus and antispyware
- Firewall filtering

Larger networks and corporate networks use antivirus, antispyware, and firewall filtering, but they also have other security requirements:

- Dedicated firewall systems
- Access control lists (ACL)
- Intrusion prevention systems (IPS)
- Virtual private networks (VPN)

The IT Professional

The Cisco Certified Network Associate (CCNA) certification demonstrates that you have a knowledge of foundational technologies and ensures you stay relevant with skill sets needed for the adoption of next-generation technologies. Your CCNA certification will prepare you for a variety of jobs in today's market. At www.netacad.com you can click the Careers menu and then select Employment opportunities. You can find employment opportunities where you live by using the Talent Bridge Matching Engine. Search for jobs with Cisco as well as Cisco partners and distributors seeking Cisco Networking Academy students and alumni.

CHAPTER 2

Module Title: Basic Switch and End Device Configuration

Module Objective: Implement initial settings including passwords, IP addressing, and default gateway parameters on a network switch and end devices.

Topic Title	Topic Objective
Cisco IOS Access	Explain how to access a Cisco IOS device for configuration purposes.
IOS Navigation	Explain how to navigate Cisco IOS to configure network devices.
The Command Structure	Describe the command structure of Cisco IOS software.
Basic Device Configuration	Configure a Cisco IOS device using CLI.
Save Configurations	Use IOS commands to save the running configuration.
Ports and Addresses	Explain how devices communicate across network media.
Configure IP Addressing	Configure a host device with an IP address.
Verify Connectivity	Verify connectivity between two end devices.

The family of network operating systems used on many Cisco devices is called the Cisco Internetwork Operating System (IOS). Cisco IOS is used on many Cisco routers and switches regardless of the type or size of the device. Each device router or switch type uses a different version of Cisco IOS. Other Cisco operating systems include IOS XE, IOS XR, and NX-OS.

Note: The operating system on home routers is usually called *firmware*. The most common method for configuring a home router is by using a web browser-based GUI.

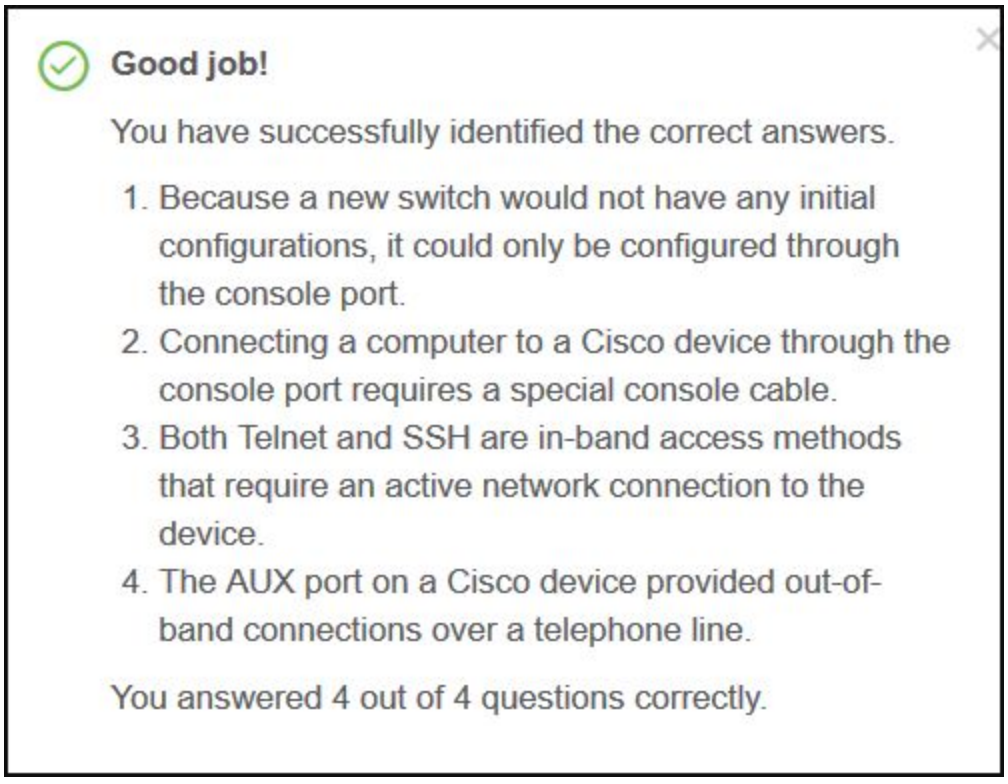
A switch will forward traffic by default and does not need to be explicitly configured to operate. For example, two configured hosts connected to the same new switch would be able to communicate.

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

Method	Description
Console	This is a physical management port that provides out-of-band access to a Cisco device. Out-of-band access refers to access via a dedicated management channel that is used for device maintenance purposes only. The advantage of using a console port is that the device is accessible even if no networking services are configured, such as performing the initial configuration. A computer running terminal emulation software and a special console cable to connect to the device are required for a console connection.

Secure Shell (SSH)	SSH is an in-band and recommended method for remotely establishing a secure CLI connection, through a virtual interface, over a network. Unlike a console connection, SSH connections require active networking services on the device, including an active interface configured with an address. Most versions of Cisco IOS include an SSH server and an SSH client that can be used to establish SSH sessions with other devices.
Telnet	Telnet is an insecure, in-band method of remotely establishing a CLI session, through a virtual interface, over a network. Unlike SSH, Telnet does not provide a secure, encrypted connection and should only be used in a lab environment. User authentication, passwords, and commands are sent over the network in plaintext. The best practice is to use SSH instead of Telnet. Cisco IOS includes both a Telnet server and Telnet client.

Note: Some devices, such as routers, may also support a legacy auxiliary port that was used to establish a CLI session remotely over a telephone connection using a modem. Similar to a console connection, the AUX port is out-of-band and does not require networking services to be configured or available.



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 the 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.

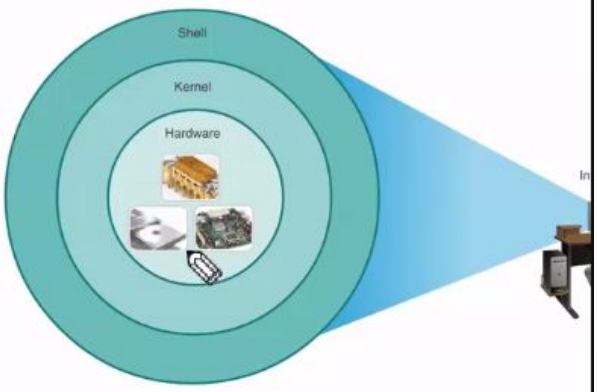
When the CLI is used, the mode is identified by the command-line prompt that is unique to that mode. By default, every prompt begins with the device name. Following the name, the remainder of the prompt indicates the mode. For example, the default prompt for line configuration mode is **Switch(config-line)#**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

Class screenshot : chapter 2

Cisco IOS Access

Operating Systems

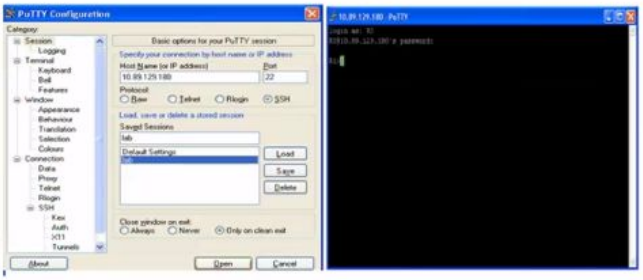
- **Shell** - The user interface that allows users to request specific tasks from the computer. These requests can be made either through the CLI or GUI interfaces.
- **Kernel** - Communicates between the hardware and software of a computer and manages how hardware resources are used to meet software requirements.
- **Hardware** - The physical part of a computer including underlying electronics.



Cisco IOS Access

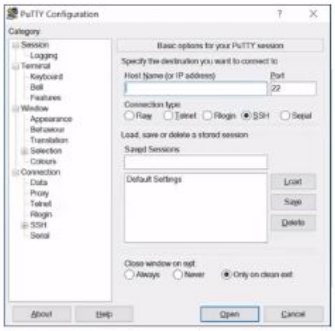
Access Methods

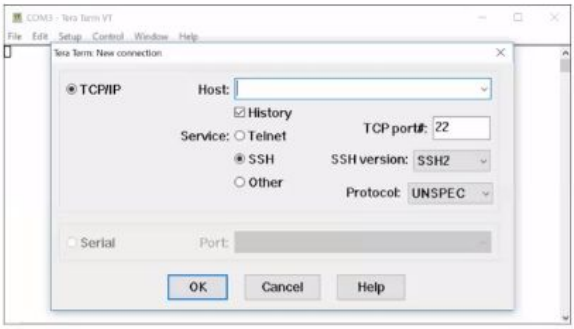
- **Console** – A physical management port used to access a device in order to provide maintenance, such as performing the initial configurations.
- **Secure Shell (SSH)** – Establishes a secure remote CLI connection to a device, through a virtual interface, over a network. (Note: This is the recommended method for remotely connecting to a device.)
- **Telnet** – Establishes an insecure remote CLI connection to a device over the network. (Note: User authentication, passwords and commands are sent over the network in plaintext.)



Terminal Emulation Programs

- Terminal emulation programs are used to connect to a network device by either a console port or by an SSH/Telnet connection.
- There are several terminal emulation programs to chose from such as PuTTY, Tera Term and SecureCRT.





Viewing Mayank Jagota's screen

IOS Navigation

Primary Command Modes

User EXEC Mode:

- Allows access to only a limited number of basic monitoring commands
- Identified by the CLI prompt that ends with the > symbol

```
Router>

Switch>
```

Privileged EXEC Mode:

- Allows access to all commands and features
- Identified by the CLI prompt that ends with the # symbol

```
Router#

Switch#
```

Global Configuration Mode:

- Used to access configuration options on the device

```
Switch(config)#
```

Line Configuration Mode:

- Used to configure console, SSH, Telnet or AUX access

```
Switch(config-line)#
```

Interface Configuration Mode:

- Used to configure a switch port or router interface

```
Switch(config-if)#
```


Navigation Between IOS Modes

- **Privileged EXEC Mode:**
  - To move from user EXEC mode to privilege EXEC mode, use the **enabled** command.

```
Switch> enable
Switch#
```

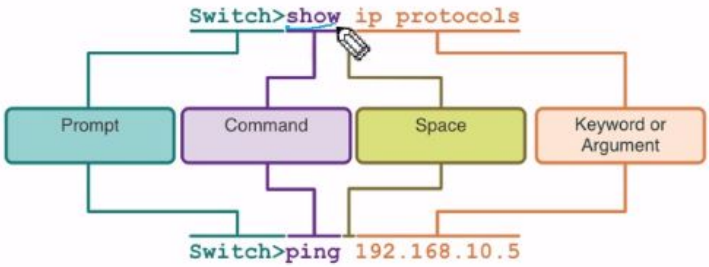
- **Global Configuration Mode:**
  - To move in and out of global configuration mode, use the **configure terminal** command. To return to privilege EXEC mode, use the **exit** command.

```
Switch(config)#
Switch(config)#exit
Switch#
```

- **Line Configuration Mode:**
  - To move in and out of line configuration mode, use the **line** command followed by the management line type. To return to global configuration mode, use the **exit** command.

```
Switch(config)#line console 0
Switch(config-line)#exit
Switch(config)#
```

Basic IOS Command Structure



- **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**).

IOS Command Syntax Check (Cont.)

- The command syntax provides the pattern, or format, that must be used when entering a command.
- The command is **ping** and the user-defined argument is the *ip-address* of the destination device. For example, **ping 10.10.10.5**.

```
ping ip-address
```

- The command is **traceroute** and the user-defined argument is the *ip-address* of the destination device. For example, **traceroute 192.168.254.254**.

```
traceroute ip-address
```

- If a command is complex with multiple arguments, you may see it represented like this:

```
Switch(config-if)# switchport port-security aging { static | time time | type {absolute | inactivity}}
```

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?

```
Router#ping ?
  WORD  Ping destination address or hostname
  ip    IP echo
  ipv6  IPv6 echo
```

- Command syntax check verifies that a valid command was entered by the user.
  - If the interpreter cannot understand the command being entered, it will provide feedback describing what is wrong with the command.

```
Switch#interface fastEthernet 0/1
                ^
% Invalid input detected at '^' marker.
```

Hot Keys and Shortcuts

- The IOS CLI provides hot keys and shortcuts that make configuring, monitoring, and troubleshooting easier.
- 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**.

```
Router#con
% Ambiguous command: "con"
Router#con?
configure  connect
```

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
```

- The table below is a brief list of keystrokes to enhance command line editing.

Keystroke	Description
Tab	Completes a partial command name entry.
Backspace	Erases the character to the left of the cursor.
Left Arrow or **Ctrl+B**	Moves the cursor one character to the left.
Right Arrow or **Ctrl+F**	Moves the cursor one character to the right.
Up Arrow or **Ctrl+P**	Recalls the commands in the history buffer, beginning with the most recent commands.

Hot Keys and Shortcuts (Cont.)

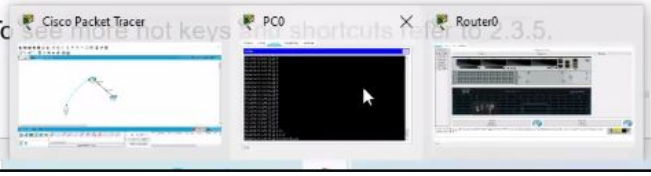
- When a command output produces more text than can be displayed in a terminal window, the IOS will display a **"--More--"** prompt. The table below describes the keystrokes that can be used when this prompt is displayed.

Keystroke	Description
Enter Key	Displays the next line.
Space Bar	Displays the next screen.
Any other key	Ends the display string, returning to privileged EXEC mode.

- The table below lists commands that can be used to exit out of an operation.

Keystroke	Description
Ctrl-C	When in any configuration mode, ends the configuration mode and returns to privileged EXEC mode.
Ctrl-Z	When in any configuration mode, ends the configuration mode and returns to privileged EXEC mode.
Ctrl-Shift-6	All-purpose break sequence used to abort DNS lookups, traceroutes, pings, etc.

Note: To see more hot keys or shortcuts refer to 2.3.5.



```
IT_DEPT_R1(config)#
IT_DEPT_R1(config)#
IT_DEPT_R1(config)#
IT_DEPT_R1(config)#
IT_DEPT_R1(config)#
IT_DEPT_R1(config)#
IT_DEPT_R1(config)#
IT_DEPT_R1(config)#
IT_DEPT_R1(config)#do show history
  ex
  exit
  interface
  exit
  hostname IT_DEPT_R1
  line aux 0
  password cisco
  login
  exit
  do show history
IT_DEPT_R1(config)#
```

```
Press RETURN to get started.



User Access Verification

Password:
Password:
Password:

IT_DEPT_R1>enabl
IT_DEPT_R1>enable
IT_DEPT_R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
IT_DEPT_R1(config)#ena
IT_DEPT_R1(config)#enable pass
IT_DEPT_R1(config)#enable password cisco
```

Ctrl+F6 to exit CLI focus

Configure Passwords

Securing user EXEC mode access:

- First enter line console configuration mode using the **line console 0** command in global configuration mode.
- Next, specify the user EXEC mode password using the **password** *password* command.
- Finally, enable user EXEC access using the **login** command.

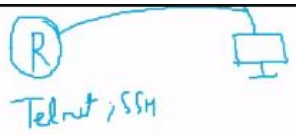
```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# line console 0
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# login
Sw-Floor-1(config-line)# end
Sw-Floor-1#
```

Securing privileged EXEC mode access:

- First enter global configuration mode.
- Next, use the **enable secret** *password* command.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# enable secret class
Sw-Floor-1(config)# exit
Sw-Floor-1#
```

Configure Passwords (Cont.)

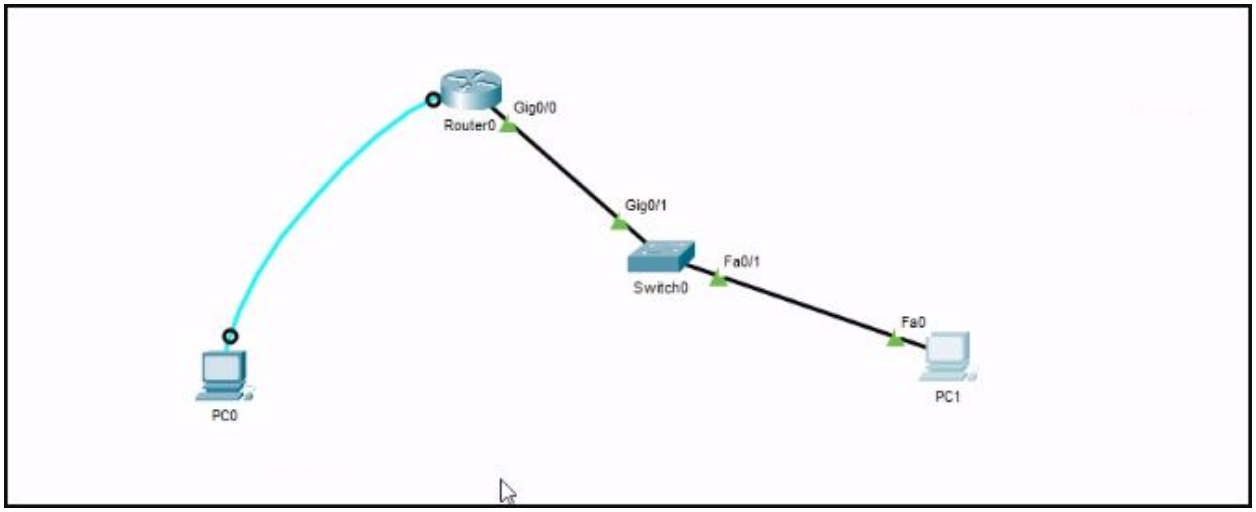


Securing VTY line access:

- First enter line VTY configuration mode using the **line vty 0 15** command in global configuration mode.
- Next, specify the VTY password using the **password** *password* command.
- Finally, enable VTY access using the **login** command.

```
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#
```

- Note: 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.



Banner Messages

- A banner message is important to warn unauthorized personnel from attempting to access the device.
- To create a banner message of the day on a network device, use the **banner motd #** *the message of the day* **#** global config command.

Note: The "#" in the command syntax is called the delimiting character. It is entered before and after the message.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# banner motd #Authorized Access Only!#
```

The banner will be displayed on attempts to access the device.

```
Press RETURN to get started.


Authorized Access Only!
User Access Verification
Password:
```

Switch(config)# **line console 0**
Switch(config-line)# **exit**
Switch(config)#

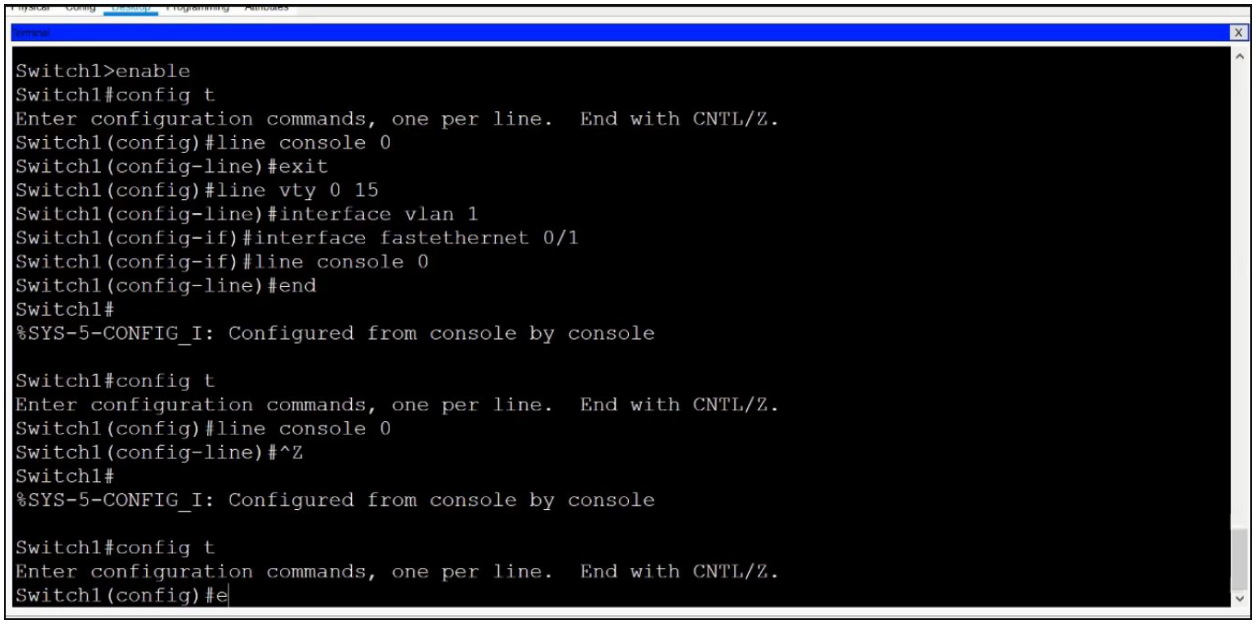
To move from any subconfiguration mode of the global configuration mode to the mode one step above it in the hierarchy of modes, enter the **exit** command.

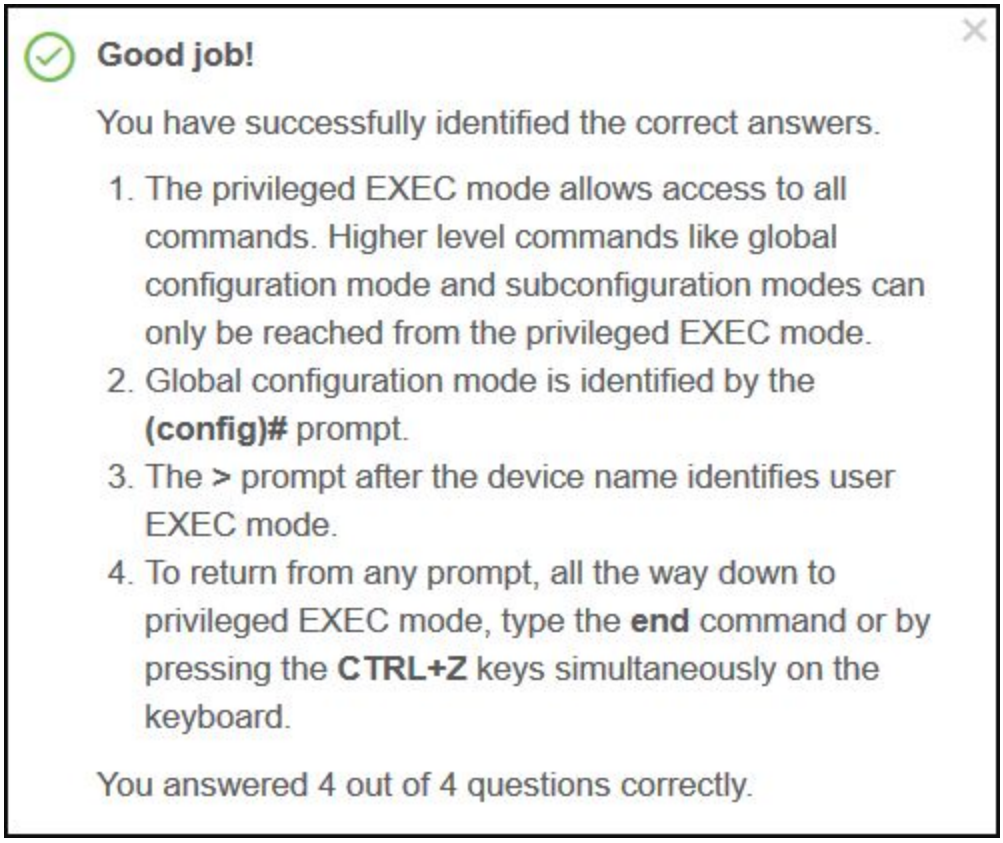
To move from any subconfiguration mode to the privileged EXEC mode, enter the **end** command or enter the key combination **Ctrl+Z**.

Switch(config-line)# **end**
Switch#

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)#**.

Switch(config-line)# **interface FastEthernet 0/1**
Switch(config-if)#





Keystroke	Description
Tab	Completes a partial command name entry.
Backspace	Erases the character to the left of the cursor.
Ctrl+D	Erases the character at the cursor.
Ctrl+K	Erases all characters from the cursor to the end of the command line.
Esc D	Erases all characters from the cursor to the end of the word.
Ctrl+U or **Ctrl+X**	Erases all characters from the cursor back to the beginning of the command line.
Ctrl+W	Erases the word to the left of the cursor.
Ctrl+A	Moves the cursor to the beginning of the line.
Left Arrow or **Ctrl+B**	Moves the cursor one character to the left.
Esc B	Moves the cursor back one word to the left.
Esc F	Moves the cursor forward one word to the right.
Right Arrow or **Ctrl+F**	Moves the cursor one character to the right.
Ctrl+E	Moves the cursor to the end of command line.
Up Arrow or **Ctrl+P**	Recalls the previous command in the history buffer, beginning with the most recent command.
Down Arrow or **Ctrl+N**	Goes to the next line in the the history buffer.

Ctrl+R or **Ctrl+I** or **Ctrl+L** Redisplays the system prompt and command line after a console message is received.

Ctrl-C
When in any configuration mode, ends the configuration mode and returns to privileged EXEC mode. When in setup mode, aborts back to the command prompt.
Ctrl-Z
When in any configuration mode, ends the configuration mode and returns to privileged EXEC mode.
Ctrl-Shift-6
All-purpose break sequence used to abort DNS lookups, traceroutes, pings, etc.

Till 2.3

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.

pASSWORD

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 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.

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#

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
```

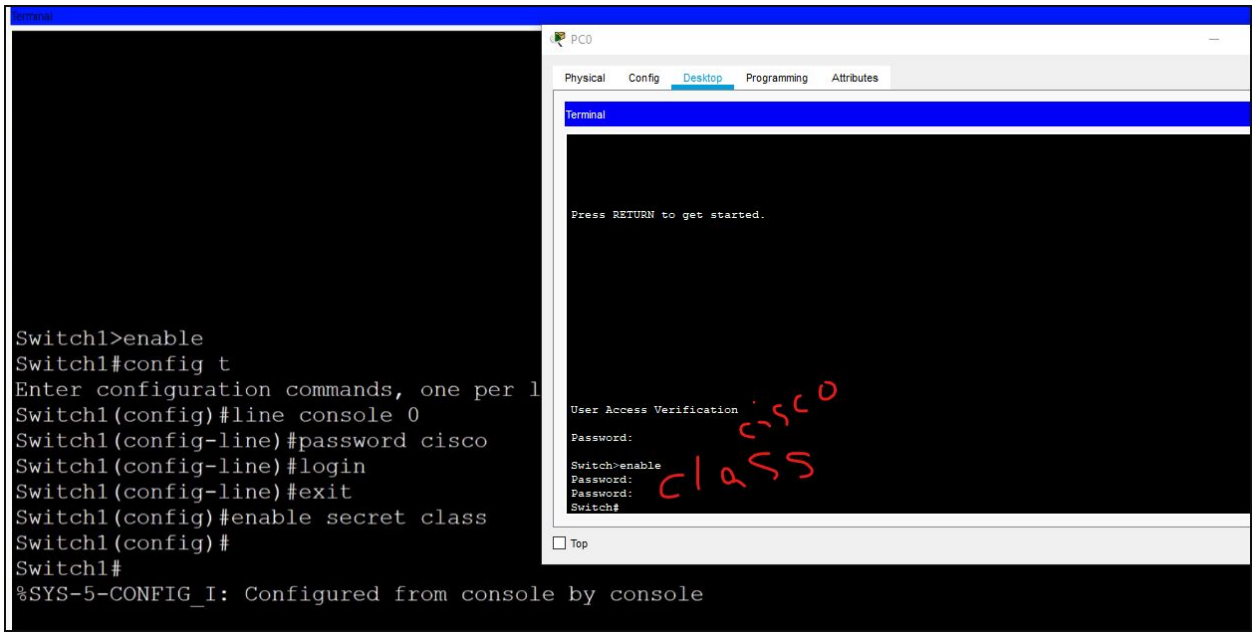
Banner Messages

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#
```



Enter global configuration mode.

Switch#conf t
You must enter the exact and full command.
Switch#configure terminal

Name the switch “Sw-Floor-1”.

Switch(config)#hostname Sw-Floor-1

Secure user EXEC mode access by entering **line console 0**, assign the password **cisco**, enable login, and return to the global configuration mode using **exit.**

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)#exit

Secure privileged EXEC mode access using the password **class.**

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

Secure the VTY lines 0 through 15, assign the password **cisco**, enable login, and return to the global configuration mode using **exit.**

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)#exit

Encrypt all plaintext passwords.

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

Create a banner message using the "**#**" symbol as the delimiter. The banner should display exactly: **Warning! Authorized access only!**

Sw-Floor-1(config)#banner motd #Warning!Authorized access only!#
You must enter the exact and full command.
Sw-Floor-1(config)#banner motd # Warning! Authorized access only! #
You must enter the exact and full command.
Sw-Floor-1(config)#banner motd #Warning! Authorized access only!#
You successfully completed the basic requirements to access and secure a device.

1. The global configuration command to set the host name on a Cisco device is hostname. So, in this example the full command is Switch(config)# **hostname Sw-Floor-2**.
2. Securing access to the EXEC mode on a Cisco switch is accomplished with the enable secret command followed by the password. In this example the command is Switch(config)# **enable secret class.**
3. User EXEC mode access through the console port is enabled with the login command entered in line mode. For example: Switch(config-line)# **login**.
4. The **service password-encryption** command entered in global configuration mode will encrypt all plaintext passwords.
5. The command to set a banner stating "Keep out" that will be displayed when connection to a Cisco switch is Switch(config)# **banner motd $ Keep out $**

You answered 5 out of 5 questions correctly.

Configuration Files

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.

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.

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.

```
User Access Verification

Password:

Switch>enable
Password:
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#copy running-config startup-config
```

```
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S1#dir ?
  flash:  Directory or file name
  nvram:  Directory or file name
  <cr>
S1#dir nvram:
Directory of nvram:/

  238  -rw-        1205          <no date>  startup-config

1205 bytes total (237588 bytes free)

S1#
```

Configuration Files

RAM NVRAM

- 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.
  - To save changes made to the running configuration to the startup configuration file, use the **copy running-config startup-config** privileged EXEC mode command.

```
Router#show startup-config
Using 624 bytes
!
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
```

```
Router#show running-config
Building configuration...

Current configuration : 624 bytes
!
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
```



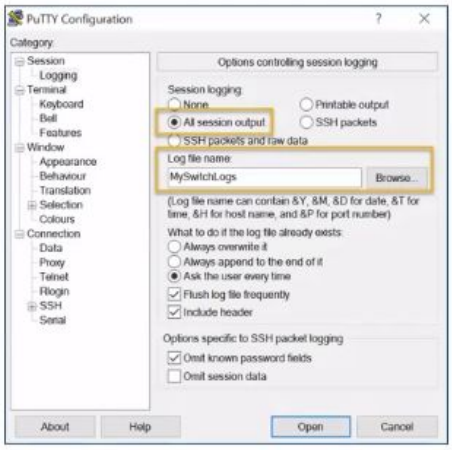
```
IT_DEPT_R1#
IT_DEPT_R1#
IT_DEPT_R1#
IT_DEPT_R1#
IT_DEPT_R1#
IT_DEPT_R1#
IT_DEPT_R1#
IT_DEPT_R1#
IT_DEPT_R1#
IT_DEPT_R1#
IT_DEPT_R1#
IT_DEPT_R1#
IT_DEPT_R1#
IT_DEPT_R1#
IT_DEPT_R1#
IT_DEPT_R1#
IT_DEPT_R1#
IT_DEPT_R1#
IT_DEPT_R1#
IT_DEPT_R1#cop
IT_DEPT_R1#copy run
IT_DEPT_R1#copy running-config sta
IT_DEPT_R1#copy running-config startup-config
```

RAM NVRAM

Capture Configuration to a Text File

Configuration files can also be saved and archived to a text document.

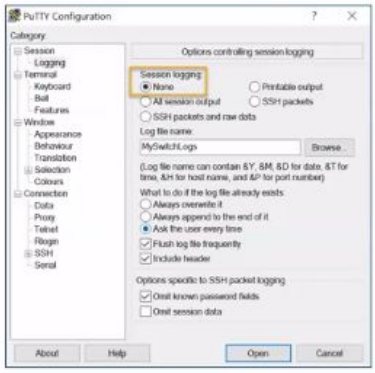
- **Step 1.** Open terminal emulation software, such as PuTTY or Tera Term, that is already connected to a switch.
- **Step 2.** Enable logging in to the terminal software and assign a name and file location to save the log file. The figure displays that **All session output** will be captured to the file specified (i.e., MySwitchLogs).



Capture Configuration to a Text File (Cont.)

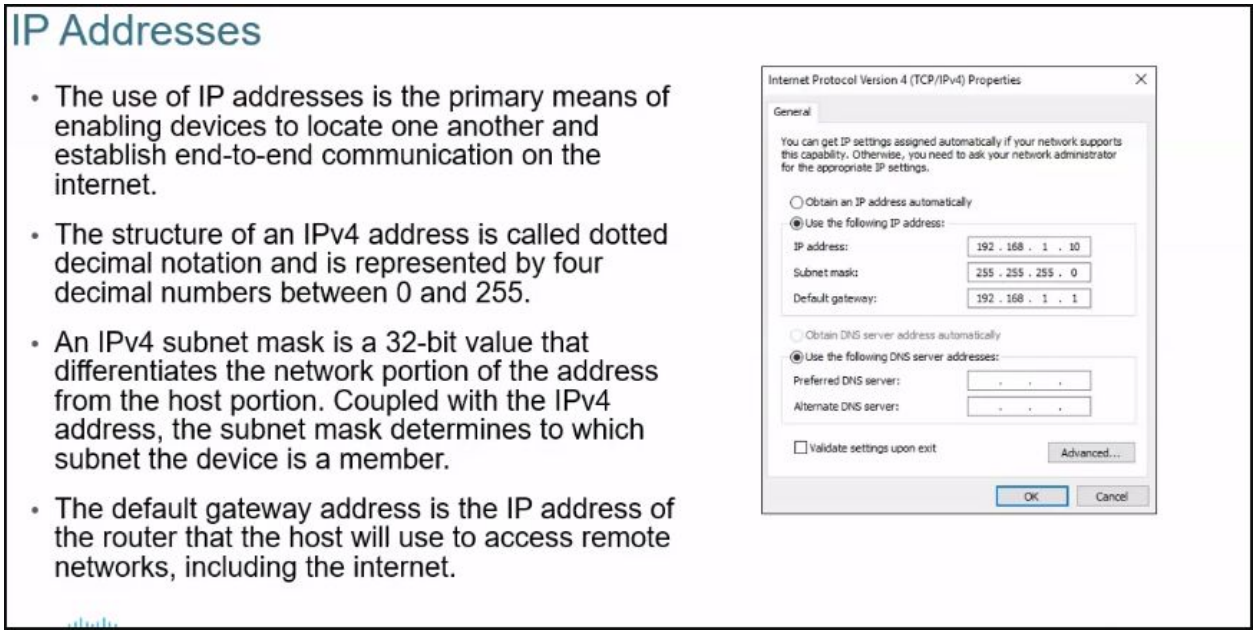
- **Step 3.** Execute the **show running-config** or **show startup-config** command at the privileged EXEC prompt. Text displayed in the terminal window will be placed into the chosen file.
- **Step 4.** Disable logging in the terminal software. The figure shows how to disable logging by choosing the **None** session logging option

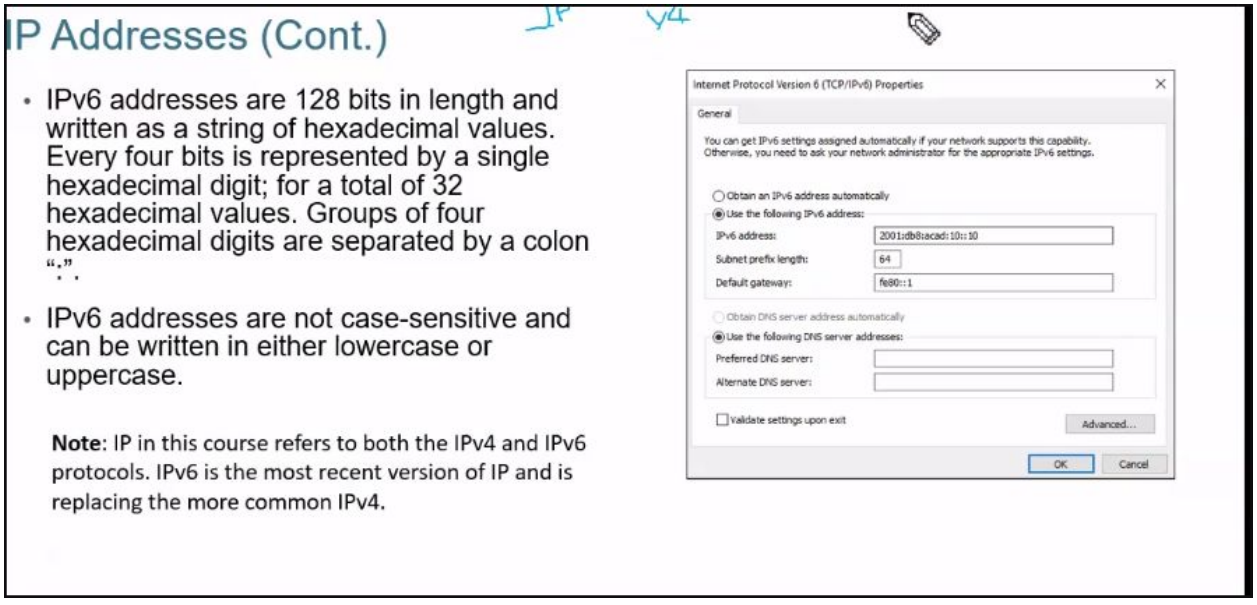
```
Switch# show running-config
Building configuration...
```



Note: The text file created can be used as a record of how the device is currently implemented. The file could require editing before being used to restore a saved configuration to a device.

IP Addresses



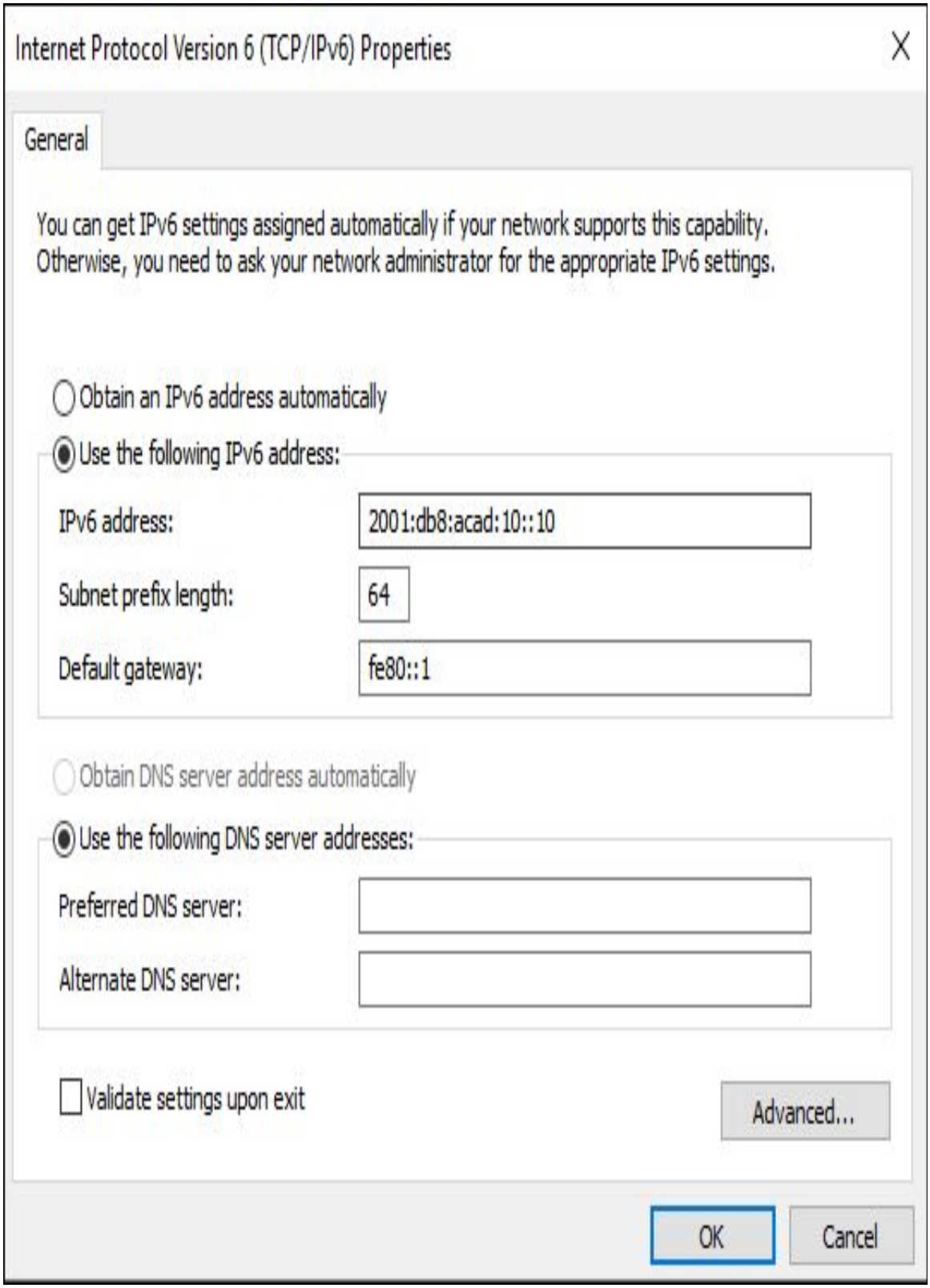


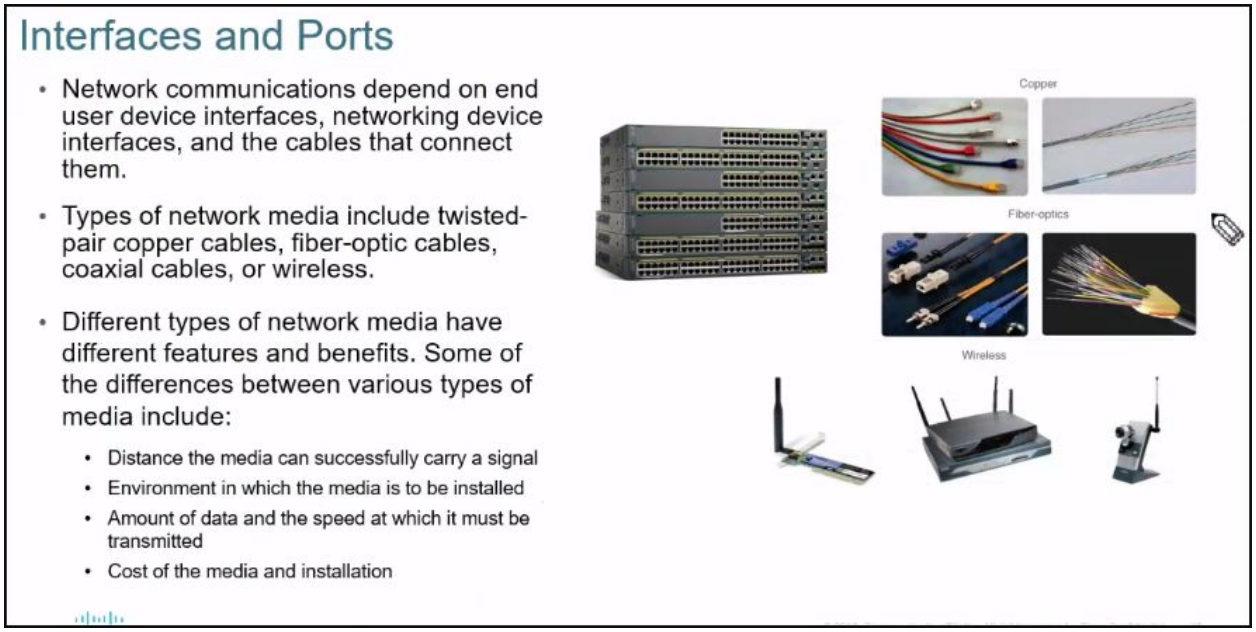
The structure of an IPv4 address is called dotted decimal notation and is represented by four decimal numbers between 0 and 255. IPv4 addresses are assigned to individual devices connected to a network.

With the IPv4 address, a subnet mask is also necessary. An IPv4 subnet mask is a 32-bit value that differentiates the network portion of the address from the host portion. Coupled with the IPv4 address, the subnet mask determines to which subnet the device is a member.

The example in the figure displays the IPv4 address (192.168.1.10), subnet mask (255.255.255.0), and default gateway (192.168.1.1) assigned to a host. The default gateway address is the IP address of the router that the host will use to access remote networks, including the internet.

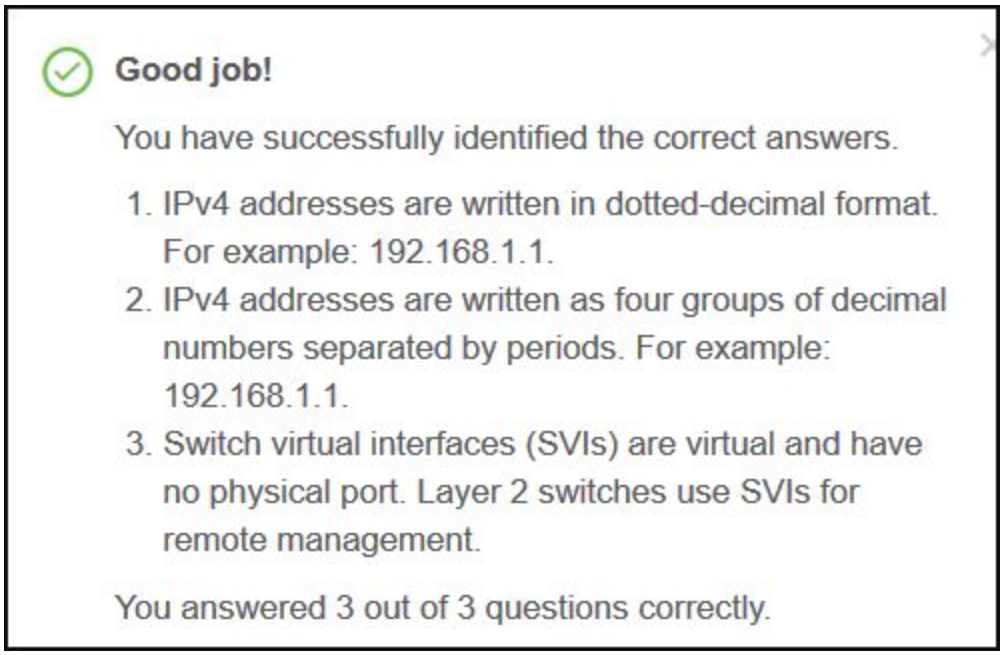
IPv6 addresses are 128 bits in length and written as a string of hexadecimal values. Every four bits is represented by a single hexadecimal digit; for a total of 32 hexadecimal values. Groups of four hexadecimal digits are separated by a colon (:) . IPv6 addresses are not case-sensitive and can be written in either lowercase or uppercase.


Internet Protocol Version 6 (TCP/IPv6) Properties
X
General
You can get IPv6 settings assigned automatically if your network supports this capability.
Otherwise, you need to ask your network administrator for the appropriate IPv6 settings.
Obtain an IPv6 address automatically
Use the following IPv6 address:
IPv6 address:
2001:db8:acad:10::10
Subnet prefix length:
64
Default gateway:
fe80::1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel



Cisco IOS Layer 2 switches have physical ports for devices to connect. These ports do not support Layer 3 IP addresses. Therefore, switches have one or more switch virtual interfaces (SVIs). These are virtual interfaces because there is no physical hardware on the device associated with it. An SVI is created in software.

The virtual interface lets you remotely manage a switch over a network using IPv4 and IPv6. Each switch comes with one SVI appearing in the default configuration "out-of-the-box." The default SVI is interface VLAN1.



Till 2.6

Manual IP Address Configuration for End Devices

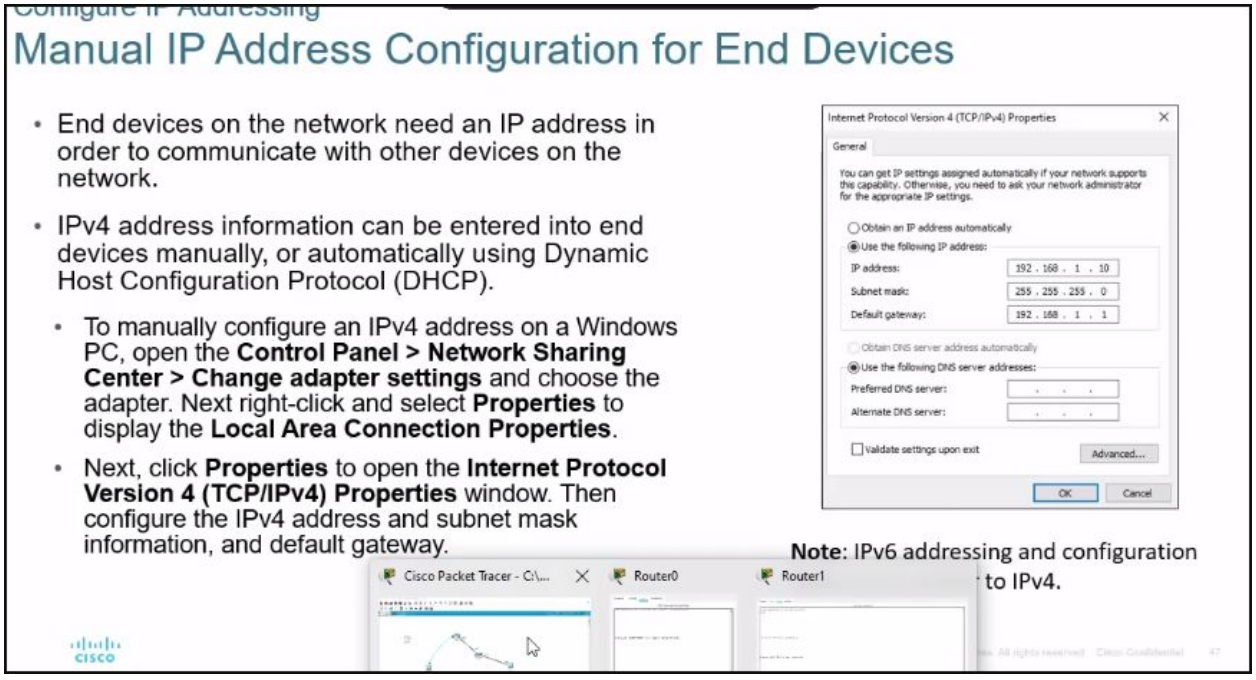
Much like you need your friends' telephone numbers to text or call them, end devices in your network need an IP address so that they can communicate with other devices on your network. In this topic, you will implement basic connectivity by configuring IP addressing on switches and PCs.

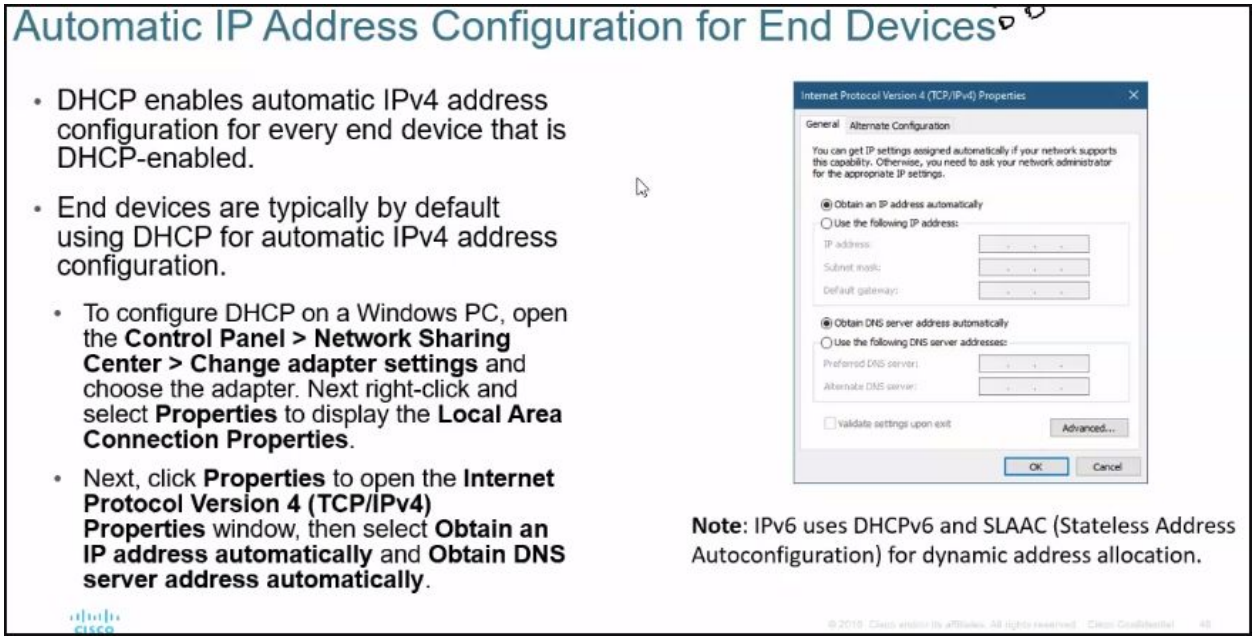
IPv4 address information can be entered into end devices manually, or automatically using Dynamic Host Configuration Protocol (DHCP).

To manually configure an IPv4 address on a Windows host, open the **Control Panel > Network Sharing Center > Change adapter settings** and choose the adapter. Next right-click and select **Properties** to display the **Local Area Connection Properties**, as shown in the figure.

Highlight Internet Protocol Version 4 (TCP/IPv4) and click **Properties** to open the **Internet Protocol Version 4 (TCP/IPv4) Properties** window, shown in the figure. Configure the IPv4 address and subnet mask information, and default gateway.

Note: IPv6 addressing and configuration options are similar to IPv4.





End devices typically default to using DHCP for automatic IPv4 address configuration. DHCP is a technology that is used in almost every network. The best way to understand why DHCP is so popular is by considering all the extra work that would have to take place without it.

Switch Virtual Interface Configuration

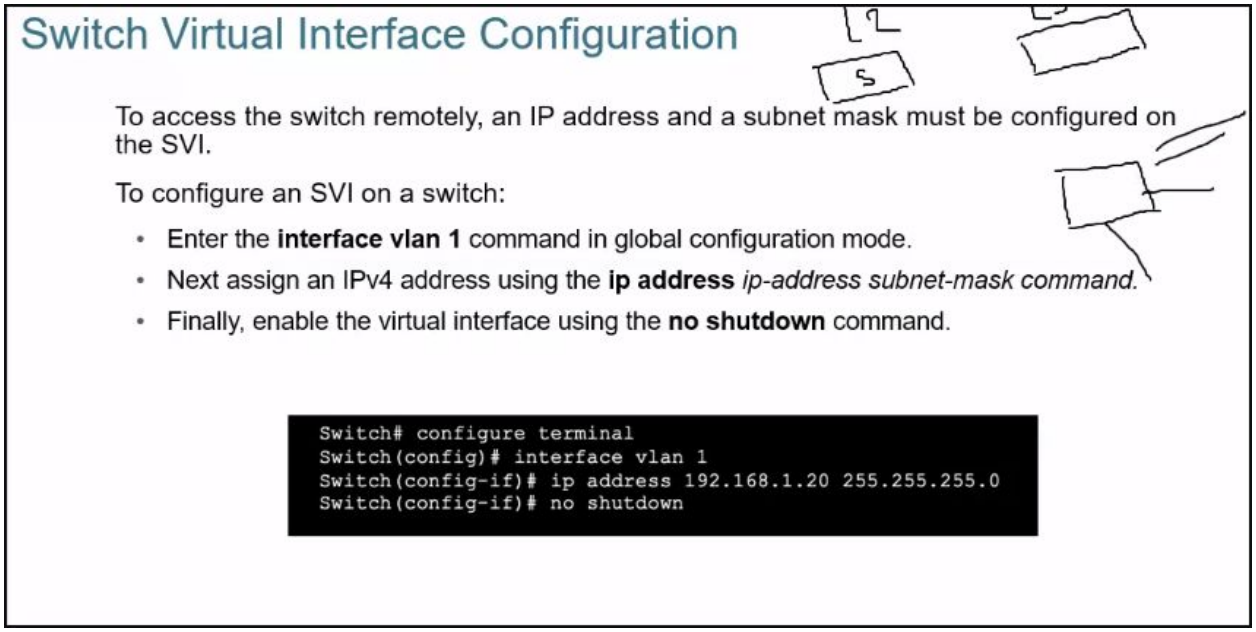
To access the switch remotely, an IP address and a subnet mask must be configured on the SVI. To configure an SVI on a switch, use the **interface vlan 1** global configuration command. Vlan 1 is not an actual physical interface but a virtual one. Next assign an IPv4 address using the **ip address** *ip-address subnet-mask* interface configuration command. Finally, enable the virtual interface using the **no shutdown** interface configuration command.

After these commands are configured, the switch has all the IPv4 elements ready for communication over the network.

Note: Similar to a Windows hosts, switches configured with an IPv4 address will typically also need to have a default gateway assigned. This can be done using the **ip default-gateway** *ip-address* global configuration command. The *ip-address* parameter would be the IPv4 address of the local router on the network, as shown in the example. However, in this module you will only be configuring a network with switches and hosts. Routers will be introduced later.

Sw-Floor-1# **configure terminal**
Sw-Floor-1(config)# **interface vlan 1**
Sw-Floor-1(config-if)# **ip address 192.168.1.20 255.255.255.0**
Sw-Floor-1(config-if)# **no shutdown**
Sw-Floor-1(config-if)# **exit**

Sw-Floor-1(config)# **ip default-gateway 192.168.1.1**



Till 2.7

What did I learn in this module?

All end devices and network devices require an operating system (OS). The user can interact with the shell using a command-line interface (CLI) to use a keyboard to run CLI-based network programs, use a keyboard to enter text and text-based commands, and view output on a monitor.

As a security feature, the Cisco IOS software separates management access into the following two command modes: User EXEC Mode and Privileged EXEC Mode.

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 and Interface Configuration 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.

Each IOS command has a specific format or syntax and can only be executed in the appropriate mode. The general syntax for a command is the command followed by any appropriate keywords and arguments. The IOS has two forms of help available: context-sensitive help and command syntax check.

The first configuration command on any device should be to give it a unique device name or hostname. Network devices should always have passwords configured to limit administrative access. Cisco IOS can be configured to use hierarchical mode passwords to allow different access privileges to a network device. Configure and encrypt all passwords. Provide a method for declaring that only authorized personnel should attempt to access the device by adding a banner to the device output.

There are two system files that store the device configuration: startup-config and running-config. Running configuration files can be altered if they have not been saved. Configuration files can also be saved and archived to a text document.

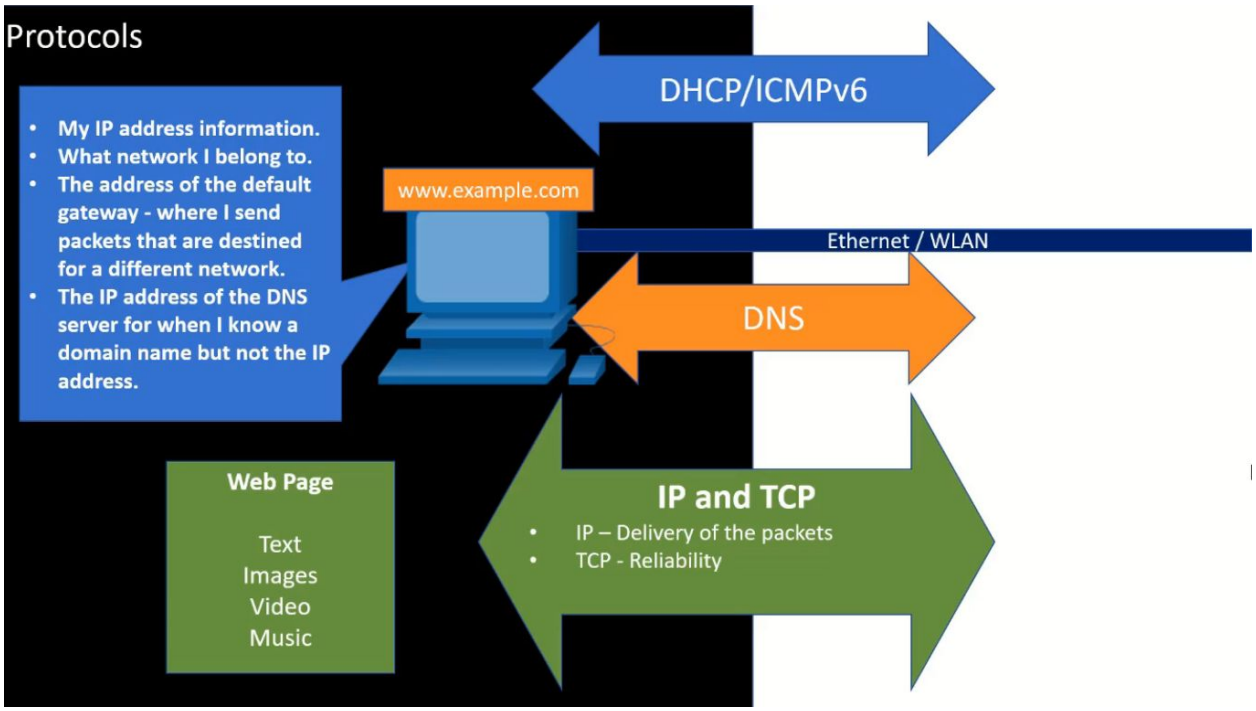
IP addresses enable devices to locate one another and establish end-to-end communication on the internet. Each end device on a network must be configured with an IP address. The structure of an IPv4 address is called dotted decimal notation and is represented by four decimal numbers between 0 and 255.

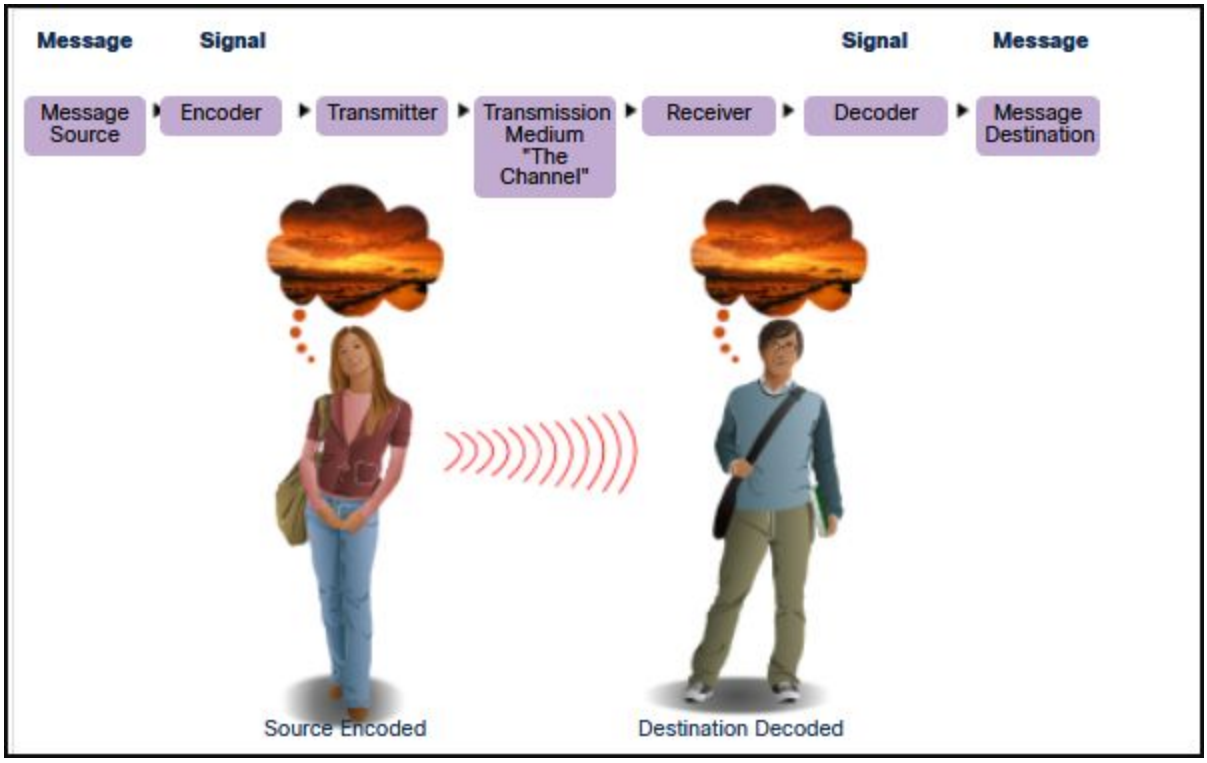
IPv4 address information can be entered into end devices manually, or automatically using Dynamic Host Configuration Protocol (DHCP). In a network, DHCP enables automatic IPv4 address configuration for every end device that is DHCP-enabled. To access the switch remotely, an IP address and a subnet mask must be configured on the SVI. To configure an SVI on a switch, use the **interface vlan 1 global configuration** command. Vlan 1 is not an actual physical interface but a virtual one.

In the same way that you use commands and utilities to verify a PC host's network configuration, you also use commands to verify the interfaces and address settings of intermediary devices like switches and routers. The **show ip interface brief** command verifies the condition of the switch interfaces. The **ping** command can be used to test connectivity to another device on the network or a website on the internet.

CHAPTER 3

Topic Title	Topic Objective
The Rules	Describe the types of rules that are necessary to successfully communicate.
Protocols	Explain why protocols are necessary in network communication.
Protocol Suites	Explain the purpose of adhering to a protocol suite.
Standards Organizations	Explain the role of standards organizations in establishing protocols for network interoperability.
Reference Models	Explain how the TCP/IP model and the OSI model are used to facilitate standardization in the communication process.
Data Encapsulation	Explain how data encapsulation allows data to be transported across the network.
Data Access	Explain how local hosts access local resources on a network.





Message Formatting and Encapsulation

When a message is sent from source to destination, it must use a specific format or structure. Message formats depend on the type of message and the channel that is used to deliver the message.

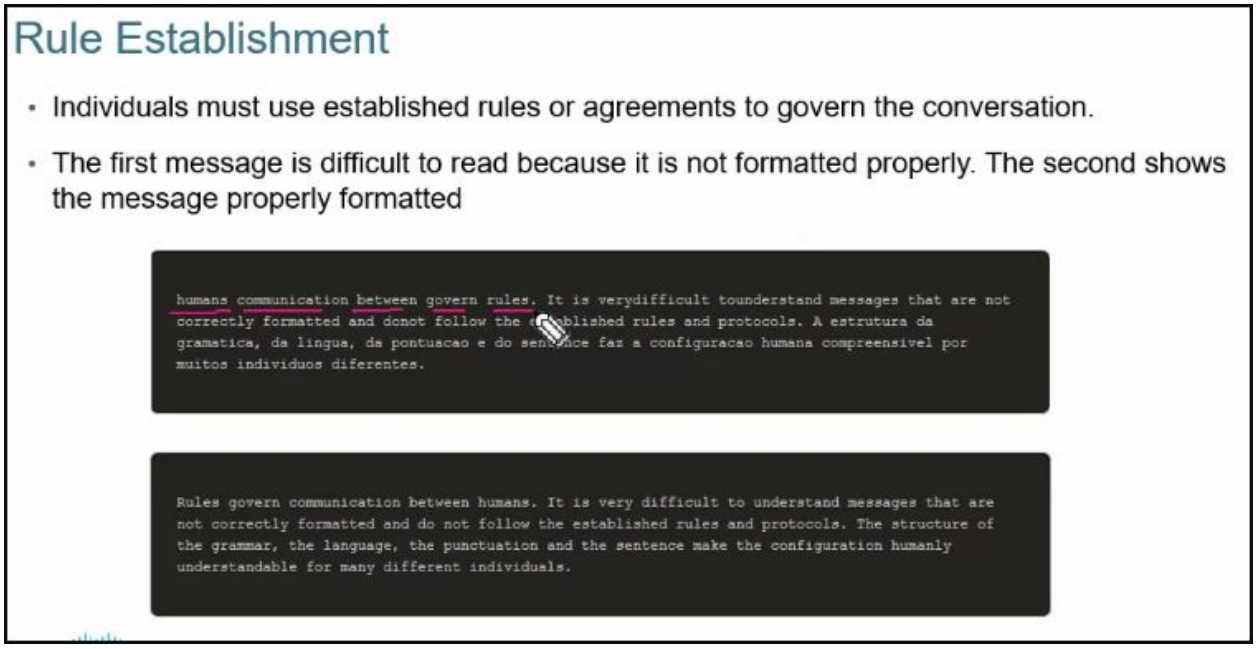
Message Encoding

One of the first steps to sending a message is encoding. Encoding is the process of converting information into another acceptable form, for transmission. Decoding reverses this process to interpret the information.

Message Timing

Message timing is also very important in network communications. Message timing includes the following:

- **Flow Control -** This is the process of managing the rate of data transmission. Flow control defines how much information can be sent and the speed at which it can be delivered. For example, if one person speaks too quickly, it may be difficult for the receiver to hear and understand the message. In network communication, there are network protocols used by the source and destination devices to negotiate and manage the flow of information.
- **Response Timeout -** If a person asks a question and does not hear a response within an acceptable amount of time, the person assumes that no answer is coming and reacts accordingly. The person may repeat the question or instead, may go on with the conversation. Hosts on the network use network protocols that specify how long to wait for responses and what action to take if a response timeout occurs.
- **Access method -** This determines when someone can send a message. Click Play in the figure to see an animation of two people talking at the same time, then a "collision of information" occurs, and it is necessary for the two to back off and start again. Likewise, when a device wants to transmit on a wireless LAN, it is necessary for the WLAN network interface card (NIC) to determine whether the wireless medium is available.



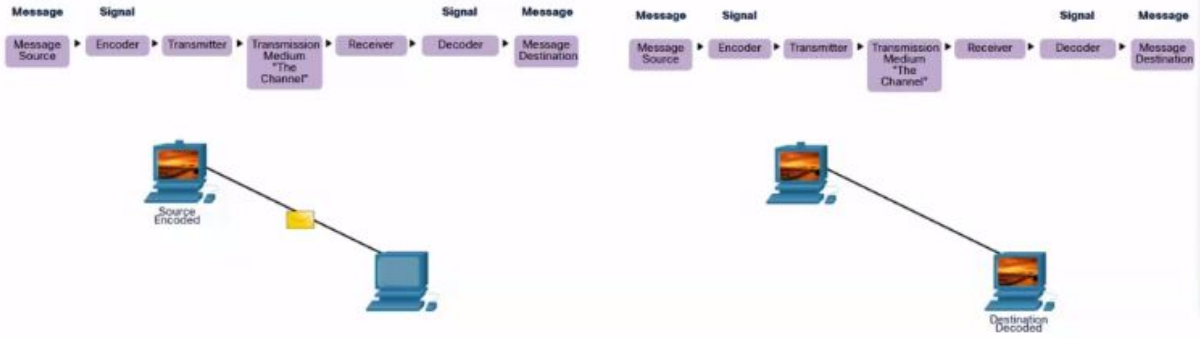
Network Protocol Requirements

Common computer protocols must be in agreement and include the following requirements:

- Message encoding
- Message formatting and encapsulation
- Message size
- Message timing
- Message delivery options

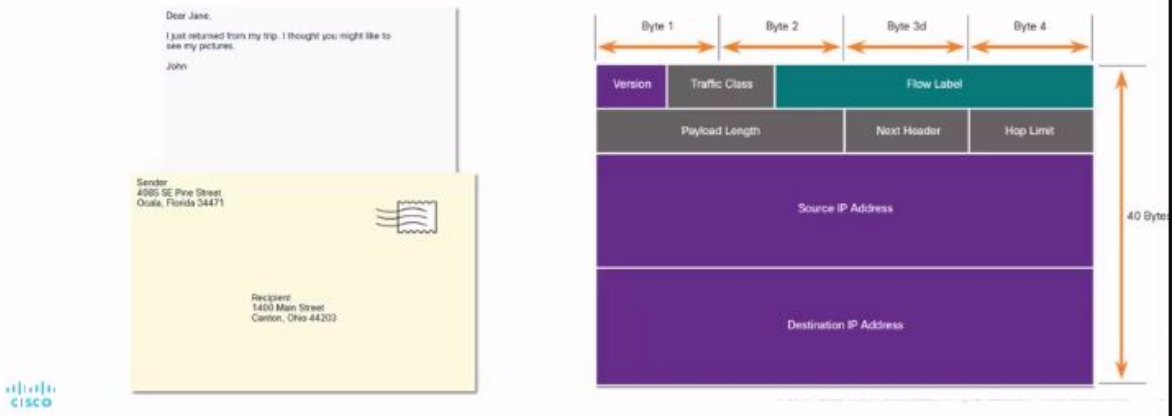
Message Encoding

- Encoding is the process of converting information into another acceptable form for transmission.
- Decoding reverses this process to interpret the information.



Message Formatting and Encapsulation

- When a message is sent, it must use a specific format or structure.
- Message formats depend on the type of message and the channel that is used to deliver the message.



Message Timing

Message timing includes the following:

Flow Control – Manages the rate of data transmission and defines how much information can be sent and the speed at which it can be delivered.

Response Timeout – Manages how long a device waits when it does not hear a reply from the destination.

Access method - Determines when someone can send a message.

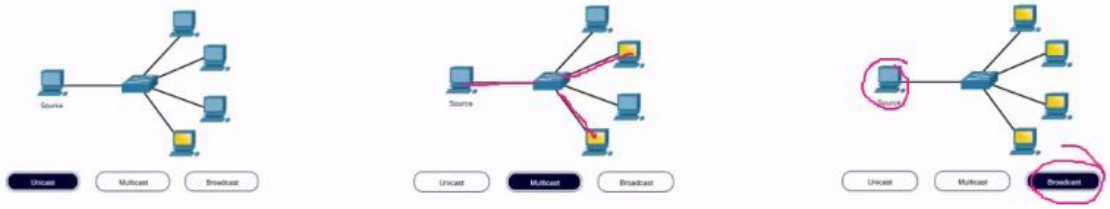
- There may be various rules governing issues like “collisions”. This is when more than one device sends traffic at the same time and the messages become corrupt.
- Some protocols are proactive and attempt to prevent collisions; other protocols are reactive and establish a recovery method after the collision occurs.

Message Delivery Options

Message delivery may one of the following methods:

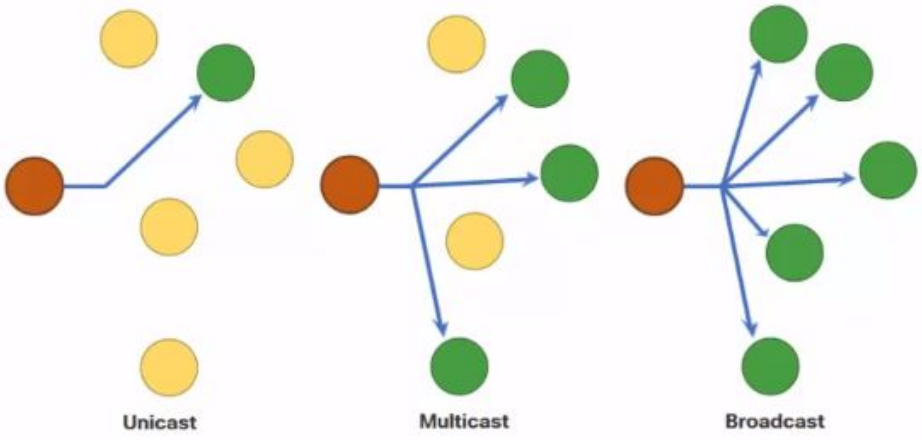
- **Unicast –** one to one communication
- **Multicast –** one to many, typically not all
- **Broadcast** – one to all

Note: Broadcasts are used in IPv4 networks, but are not an option for IPv6. Later we will also see "Anycast" as an additional delivery option for IPv6.



A Note About the Node Icon

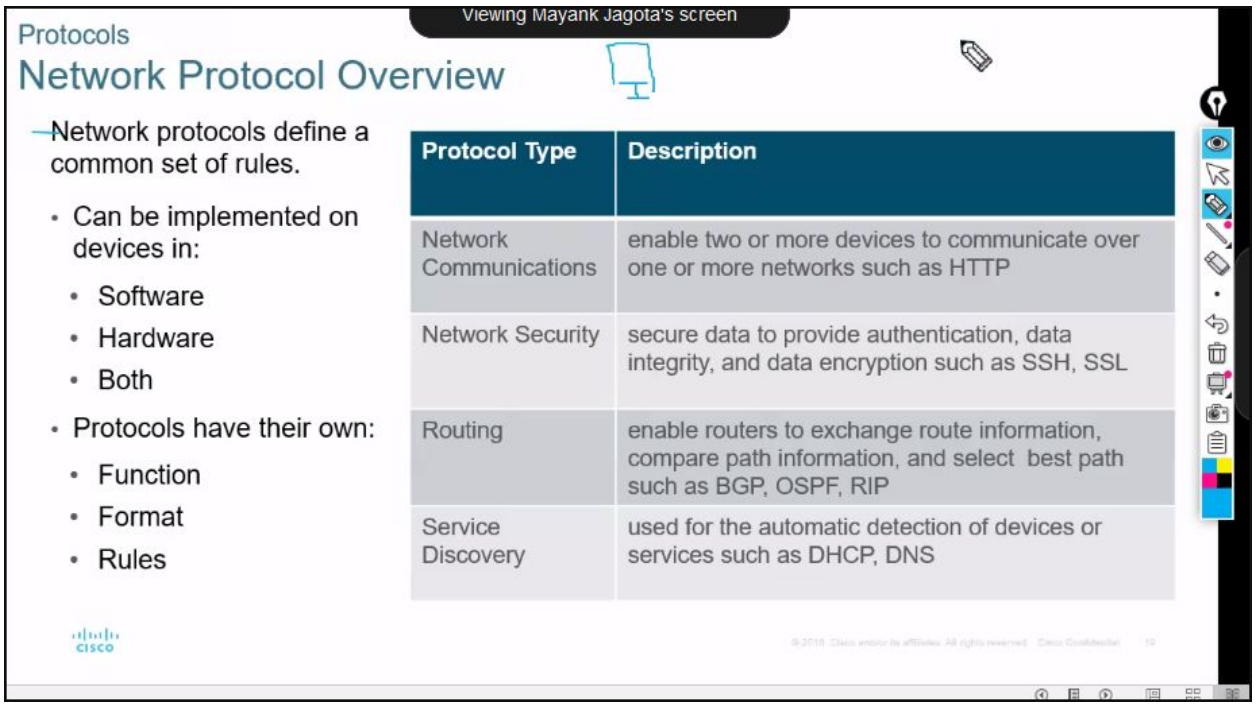
- Documents may use the node icon , typically a circle, to represent all devices.
- The figure illustrates the use of the node icon for delivery options.



You have successfully identified the correct answers.

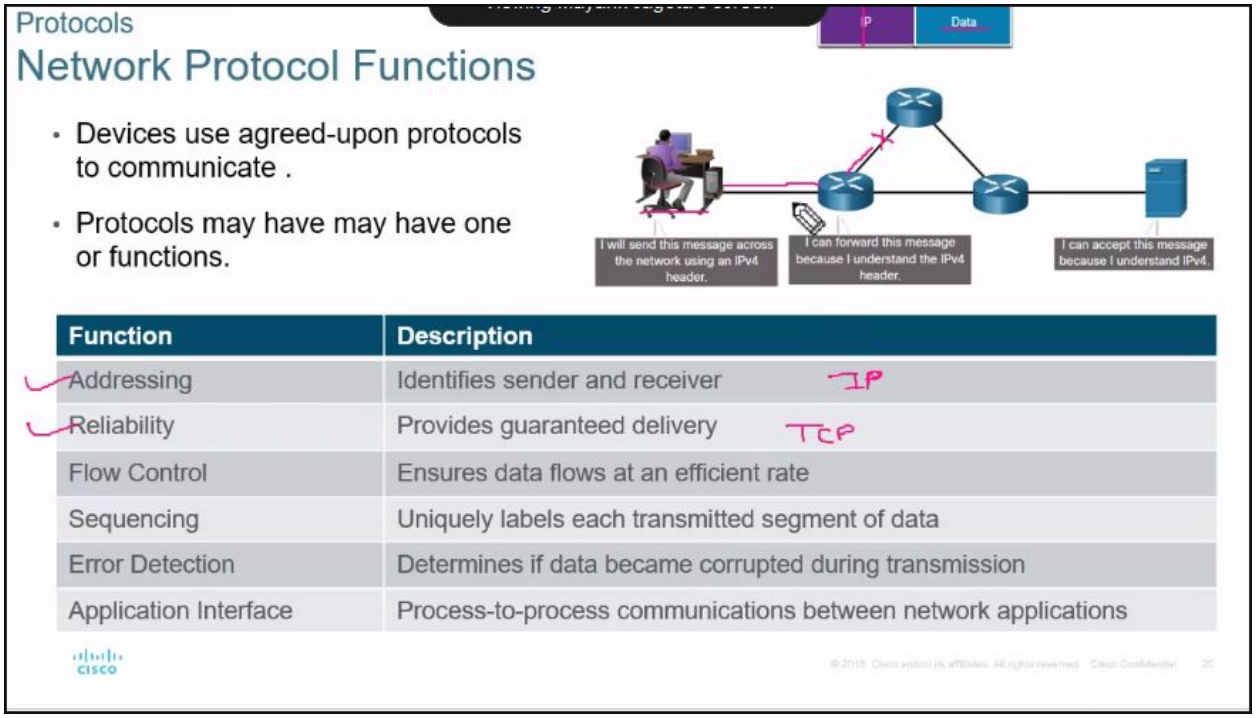
1. One of the first steps to sending a message is encoding. During the encoding process, information is converted from its original form into an acceptable form for transmission.
2. Messages sent over a computer network must be in the correct format for them to be delivered and processed. Part of the formatting process is properly identifying the source of the message and its destination.
3. Flow control is the managing of the rate of transmission. Response timeout is how long to wait for responses. Access methods determine when someone can send a message. These are the three components of message timing.
4. Multicast messages are addressed for transmission to one or more end devices on a network. Broadcast messages are addressed for transmission to all devices on the network. Unicast messages are addressed for transmission to one device on the network.

You answered 4 out of 4 questions correctly.



The table lists the various types of protocols that are needed to enable communications across one or more networks.

Protocol Type	Description
Network Communications Protocols	Protocols enable two or more devices to communicate over one or more networks. The Ethernet family of technologies involves a variety of protocols such as IP, Transmission Control Protocol (TCP), HyperText Transfer Protocol (HTTP), and many more.
Network Security Protocols	Protocols secure data to provide authentication, data integrity, and data encryption. Examples of secure protocols include Secure Shell (SSH), Secure Sockets Layer (SSL), and Transport Layer Security (TLS).
Routing Protocols	Protocols enable routers to exchange route information, compare path information, and then to select the best path to the destination network. Examples of routing protocols include Open Shortest Path First (OSPF) and Border Gateway Protocol (BGP).
Service Discovery Protocols	Protocols are used for the automatic detection of devices or services. Examples of service discovery protocols include Dynamic Host Configuration Protocol (DHCP) which discovers services for IP address allocation, and Domain Name System (DNS) which is used to perform name-to-IP address translation.



Function	Description
Addressing	This identifies the sender and the intended receiver of the message using a defined addressing scheme. Examples of protocols that provide addressing include Ethernet, IPv4, and IPv6.
Reliability	This function provides guaranteed delivery mechanisms in case messages are lost or corrupted in transit. TCP provides guaranteed delivery.
Flow control	This function ensures that data flows at an efficient rate between two communicating devices. TCP provides flow control services.
Sequencing	This function uniquely labels each transmitted segment of data. The receiving device uses the sequencing information to reassemble the information correctly. This is useful if the data segments are lost, delayed or received out-of-order. TCP provides sequencing services.
Error Detection	This function is used to determine if data became corrupted during transmission. Various protocols that provide error detection include Ethernet, IPv4, IPv6, and TCP.

Application Interface	This function contains information used for process-to-process communications between network applications. For example, when accessing a web page, HTTP or HTTPS protocols are used to communicate between the client and server web processes.

- **Hypertext Transfer Protocol (HTTP) -** This protocol governs the way a web server and a web client interact. HTTP defines the content and formatting of the requests and responses that are exchanged between the client and server. Both the client and the web server software implement HTTP as part of the application. HTTP relies on other protocols to govern how the messages are transported between the client and server.
- **Transmission Control Protocol (TCP)** - This protocol manages the individual conversations. TCP is responsible for guaranteeing the reliable delivery of the information and managing flow control between the end devices.
- **Internet Protocol (IP) -** This protocol is responsible for delivering messages from the sender to the receiver. IP is used by routers to forward the messages across multiple networks.
- **Ethernet** - This protocol is responsible for the delivery of messages from one NIC to another NIC on the same Ethernet local area network (LAN).

Good job!

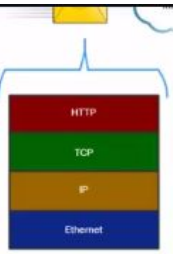
You have successfully identified the correct answers.

1. BGP and OSPF are routing protocols. They enable routers to exchange route information to reach remote networks.
2. Service discovery protocols, such as DNS and DHCP enable automatic detection of service. DHCP is used to discover services for automatic IP address allocation and DNS for name-to-IP address resolution services.
3. Sequencing uniquely identifies or labels each transmitted segment with a sequence number that is used by the receiver to reassemble the segments in the proper order.
4. Transmission Control Protocol (TCP) manages the conversation between end devices and guarantees the reliable delivery of information.

You answered 4 out of 4 questions correctly.

Protocol Interaction

- Networks require the use of several protocols.
- Each protocol has its own function and format.



Protocol	Function
Hypertext Transfer Protocol (HTTP)	▪ Governs the way a web server and a web client interact ▪ Defines content and format
Transmission Control Protocol (TCP)	▪ Manages the individual conversations ▪ Provides guaranteed delivery ▪ Manages flow control
Internet Protocol (IP)	Delivers messages globally from the sender to the receiver
Ethernet	Delivers messages from one NIC to another NIC on the same Ethernet Local Area Network (LAN)

Protocol Suites

Network Protocol Suites

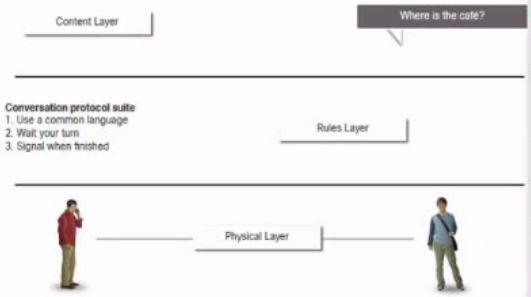
Protocols must be able to work with other protocols.

Protocol suite:

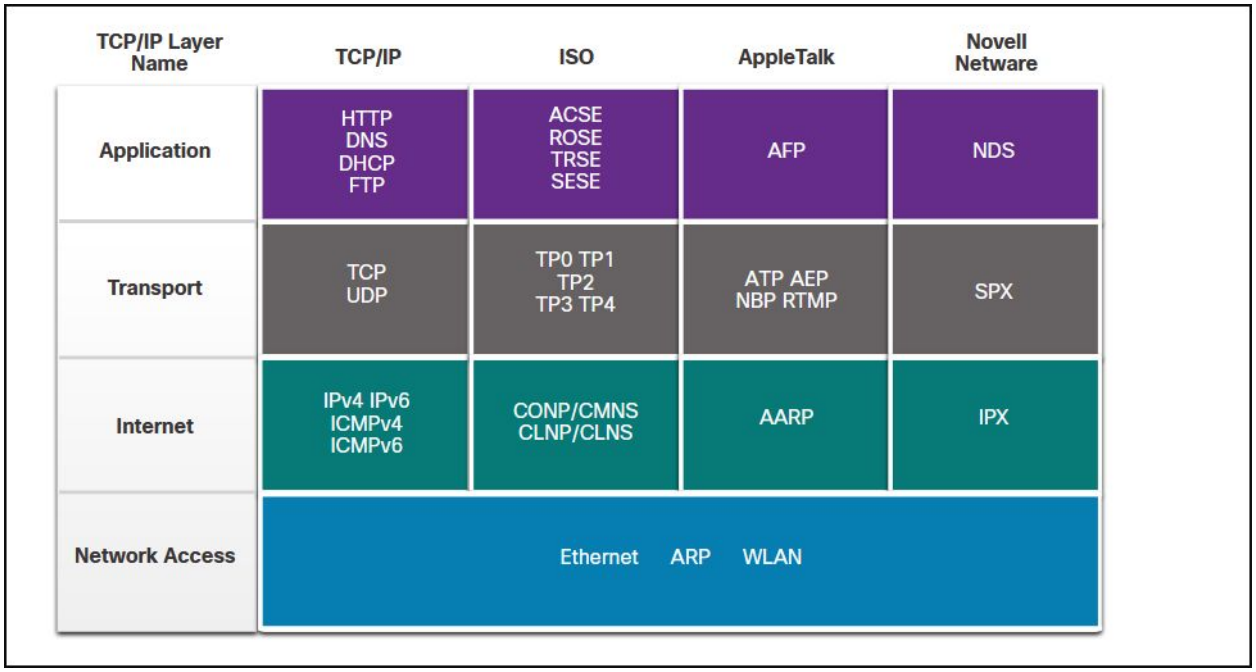
- A group of inter-related protocols necessary to perform a communication function
- Sets of rules that work together to help solve a problem

The protocols are viewed in terms of layers:

- Higher Layers
- Lower Layers- concerned with moving data and provide services to upper layers



Protocol suites are sets of rules that work together to help solve a problem.

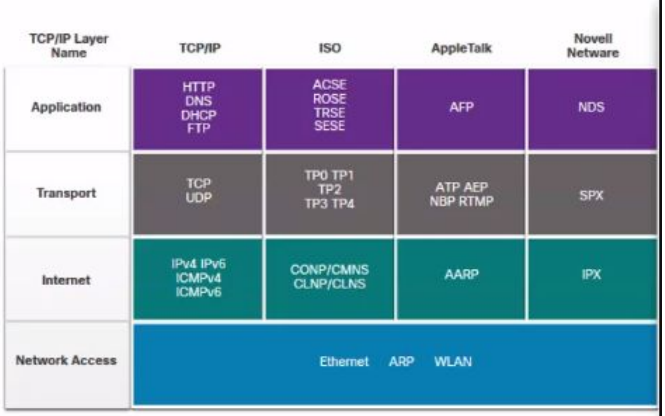


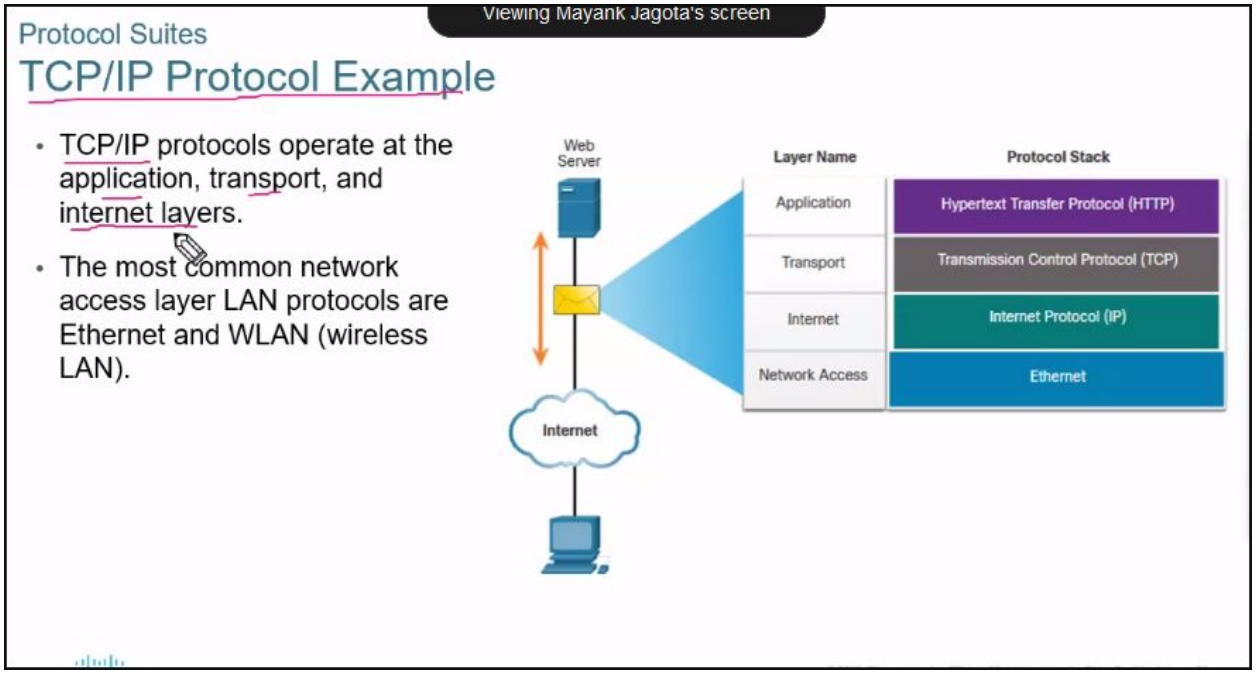
Internet Protocol Suite or TCP/IP - This is the most common and relevant protocol suite used today. The TCP/IP protocol suite is an open standard protocol suite maintained by the Internet Engineering Task Force (IETF).
Open Systems Interconnection (OSI) protocols - This is a family of protocols developed jointly in 1977 by the International Organization for Standardization (ISO) and the International Telecommunications Union (ITU). The OSI protocol also included a seven-layer model called the OSI reference model. The OSI reference model categorizes the functions of its protocols. Today OSI is mainly known for its layered model. The OSI protocols have largely been replaced by TCP/IP.
AppleTalk - A short-lived proprietary protocol suite released by Apple Inc. in 1985 for Apple devices. In 1995, Apple adopted TCP/IP to replace AppleTalk.
Novell NetWare - A short-lived proprietary protocol suite and network operating system developed by Novell Inc. in 1983 using the IPX network protocol. In 1995, Novell adopted TCP/IP to replace IPX.

Evolution of Protocol Suites

There are several protocol suites.

- **Internet Protocol Suite or TCP/IP-** The most common protocol suite and maintained by the Internet Engineering Task Force (IETF)
- **Open Systems Interconnection (OSI) protocols-** Developed by the International Organization for Standardization (ISO) and the International Telecommunications Union (ITU)
- **AppleTalk-** Proprietary suite release by Apple Inc.
- **Novell NetWare-** Proprietary suite developed by Novell Inc.



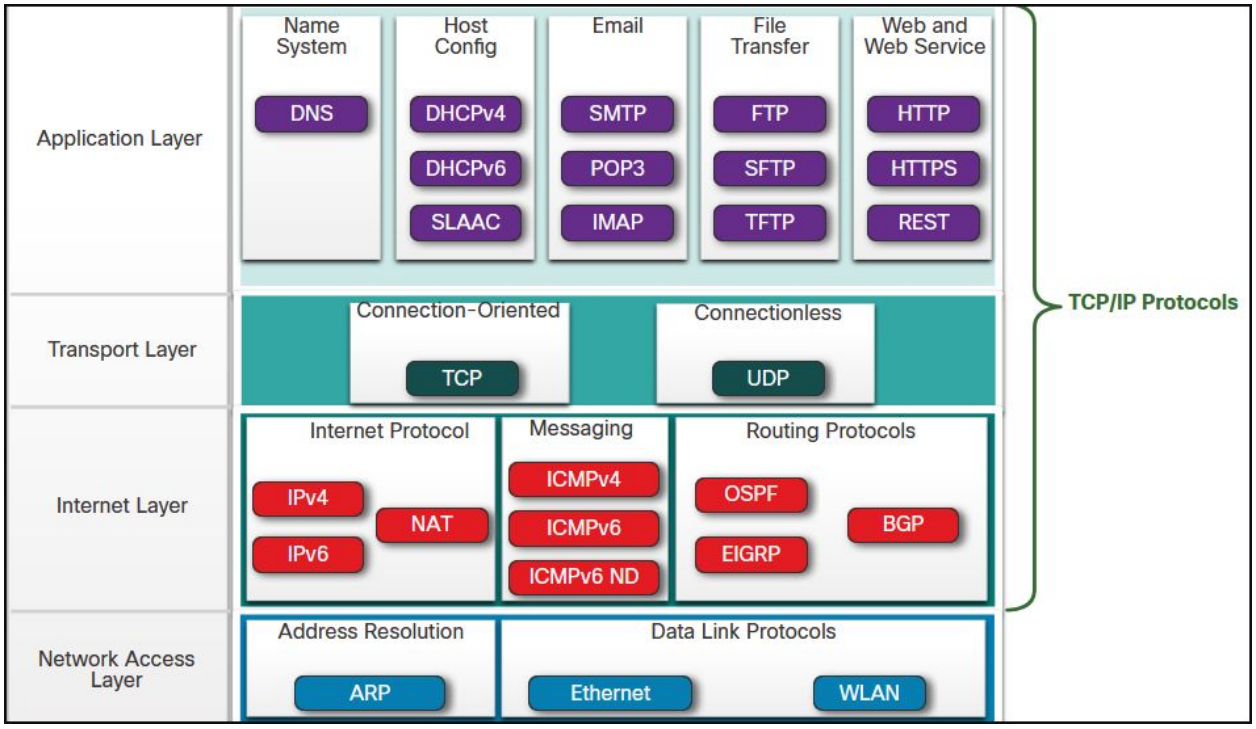


TCP/IP Protocol Example

TCP/IP protocols are available for the application, transport, and internet layers. There are no TCP/IP protocols in the network access layer. The most common network access layer LAN protocols are Ethernet and WLAN (wireless LAN) protocols. Network access layer protocols are responsible for delivering the IP packet over the physical medium.

The figure shows an example of the three TCP/IP protocols used to send packets between the web browser of a host and the web server. HTTP, TCP, and IP are the TCP/IP protocols used. At the network access layer, Ethernet is used in the example. However, this could also be a wireless standard such as WLAN or cellular service.

The figure shows the TCP/IP protocols used to send packets between the web browser of a host and a web server. A network topology shows a host connected to the Internet cloud with a connection to a Web server. An envelope representing a packet is shown flowing between the Internet and the server. Radiating from the packet is information on the protocols used at each layer. From top to bottom: application layer and hypertext transfer protocol (HTTP); transport layer and transmission control protocol (TCP); internet layer and internet protocol (IP); and network access layer and Ethernet.



TCP/IP is the protocol suite used by the internet and the networks of today. TCP/IP has two important aspects for vendors and manufacturers:

- **Open standard protocol suite** - This means it is freely available to the public and can be used by any vendor on their hardware or in their software.
- **Standards-based protocol suite** - This means it has been endorsed by the networking industry and approved by a standards organization. This ensures that products from different manufacturers can interoperate successfully.

Application Layer

Name System

- **DNS** - Domain Name System. Translates domain names such as cisco.com, into IP addresses.

Host Config

- **DHCPv4** - Dynamic Host Configuration Protocol for IPv4. A DHCPv4 server dynamically assigns IPv4 addressing information to DHCPv4 clients at start-up and allows the addresses to be re-used when no longer needed.
- **DHCPv6** - Dynamic Host Configuration Protocol for IPv6. DHCPv6 is similar to DHCPv4. A DHCPv6 server dynamically assigns IPv6 addressing information to DHCPv6 clients at start-up.
- **SLAAC** - Stateless Address Autoconfiguration. A method that allows a device to obtain its IPv6 addressing information without using a DHCPv6 server.

Email

- **SMTP** - Simple Mail Transfer Protocol. Enables clients to send email to a mail server and enables servers to send email to other servers.
- **POP3** - Post Office Protocol version 3. Enables clients to retrieve email from a mail server and download the email to the client's local mail application.
- **IMAP** - Internet Message Access Protocol. Enables clients to access email stored on a mail server as well as maintaining email on the server.

File Transfer

- **FTP** - File Transfer Protocol. Sets the 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.
- **SFTP** - SSH File Transfer Protocol. As an extension to Secure Shell (SSH) protocol, SFTP can be used to establish a secure file transfer session in which the file transfer is encrypted. SSH is a method for secure remote login that is typically used for accessing the command line of a device.
- **TFTP** - Trivial File Transfer Protocol. A simple, connectionless file transfer protocol with best-effort, unacknowledged file delivery. It uses less overhead than FTP.

Web and Web Service

- **HTTP** - Hypertext Transfer Protocol. A set of rules for exchanging text, graphic images, sound, video, and other multimedia files on the World Wide Web.
- **HTTPS** - HTTP Secure. A secure form of HTTP that encrypts the data that is exchanged over the World Wide Web.
- **REST** - Representational State Transfer. A web service that uses application programming interfaces (APIs) and HTTP requests to create web applications.

Transport layer

Connection-Oriented

- **TCP** - Transmission Control Protocol. Enables reliable communication between processes running on separate hosts and provides reliable, acknowledged transmissions that confirm successful delivery.

Connectionless

- **UDP** - User Datagram Protocol. Enables a process running on one host to send packets to a process running on another host. However, UDP does not confirm successful datagram transmission.

Internet Layer

Internet Protocol

- **IPv4** - Internet Protocol version 4. Receives message segments from the transport layer, packages messages into packets, and addresses packets for end-to-end delivery over a network. IPv4 uses a 32-bit address.
- **IPv6** - IP version 6. Similar to IPv4 but uses a 128-bit address.
- **NAT** - Network Address Translation. Translates IPv4 addresses from a private network into globally unique public IPv4 addresses.

Messaging

- **ICMPv4** - Internet Control Message Protocol for IPv4. Provides feedback from a destination host to a source host about errors in packet delivery.
- **ICMPv6** - ICMP for IPv6. Similar functionality to ICMPv4 but is used for IPv6 packets.
- **ICMPv6 ND** - ICMPv6 Neighbor Discovery. Includes four protocol messages that are used for address resolution and duplicate address detection.

Routing Protocols

- **OSPF** - Open Shortest Path First. Link-state routing protocol that uses a hierarchical design based on areas. OSPF is an open standard interior routing protocol.
- **EIGRP** - EIGRP - Enhanced Interior Gateway Routing Protocol. An open standard routing protocol developed by Cisco that uses a composite metric based on bandwidth, delay, load and reliability.
- **BGP** - Border Gateway Protocol. An open standard exterior gateway routing protocol used between Internet Service Providers (ISPs). BGP is also commonly used between ISPs and their large private clients to exchange routing information.

Network Access Layer

Address Resolution

- **ARP** - Address Resolution Protocol. Provides dynamic address mapping between an IPv4 address and a hardware address.
  Note: You may see other documentation state that ARP operates at the Internet Layer (OSI Layer 3). However, in this course we state that ARP operates at the Network Access layer (OSI Layer 2) because it's primary purpose is the discover the MAC address of the destination. A MAC address is a Layer 2 address.

Data Link Protocols

- **Ethernet** - Defines the rules for wiring and signaling standards of the network access layer.

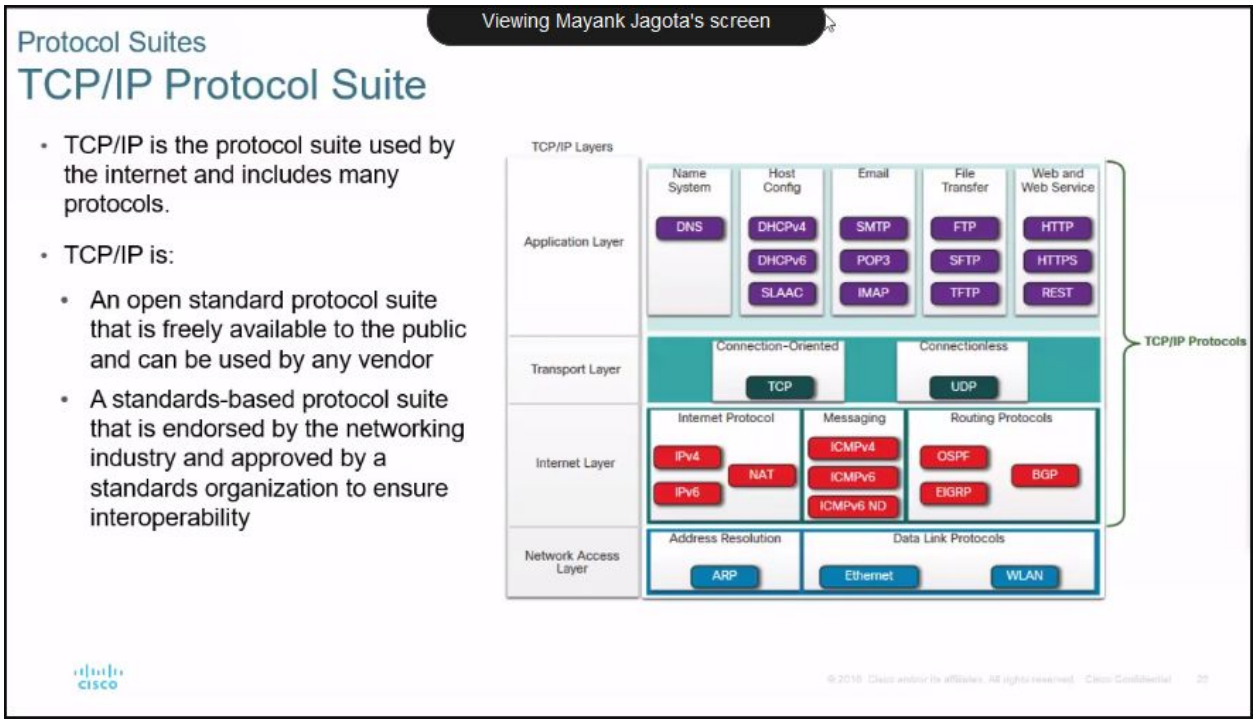
- **WLAN** - Wireless Local Area Network. Defines the rules for wireless signaling across the 2.4 GHz and 5 GHz radio frequencies.

Good job!

You have successfully identified the correct answers.

1. TCP and UDP are both transport layer protocols.
2. DHCP and DNS are both application layer protocols.
3. Ethernet is a network access layer protocol.
4. ICMPv4 and ICMPv6 provide feedback when errors occur.
5. Data is de-encapsulated so the next layer to receive the data would be the internet layer.
6. IP (Internet Protocol), ICMP (Messaging), and Routing Protocols are services provided at the Internet Layer.

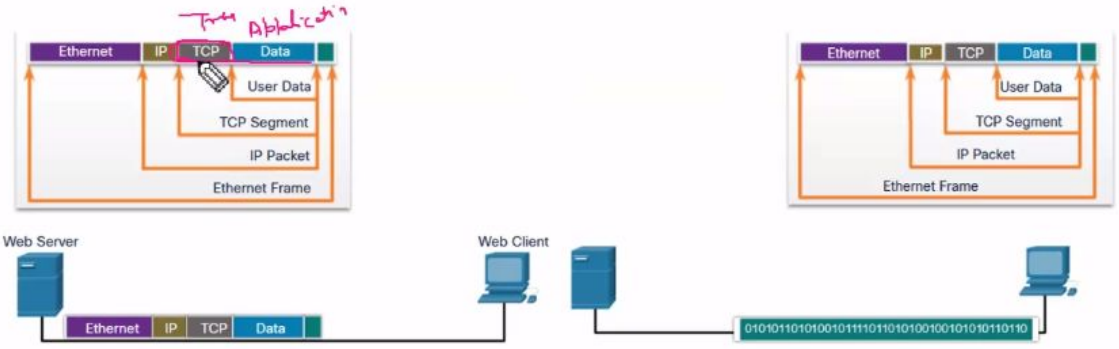
You answered 6 out of 6 questions correctly.



Protocol Suites

TCP/IP Communication Process

- A web server encapsulating and sending a web page to a client.
- A client de-encapsulating the web page for the web browser



Standards Organizations

Open Standards

IEEE

iana
Internet Assigned Numbers Authority

IETF

ICANN
The Internet Corporation for Assigned Names and Numbers

ITU

TIA

Open standards encourage:

- interoperability
- competition
- innovation

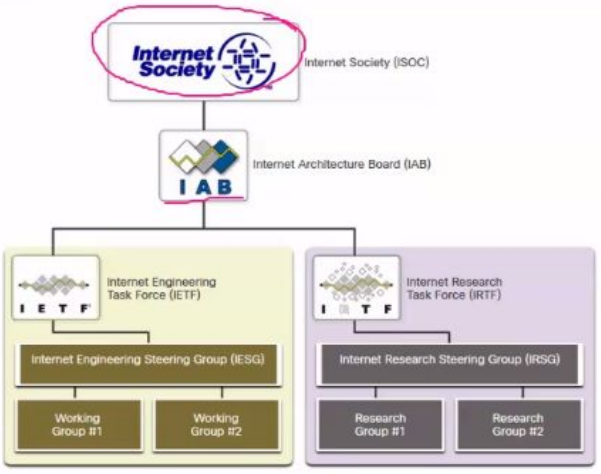
Standards organizations are:

- vendor-neutral
- non-profit organizations
- established to develop and promote the concept of open standards.

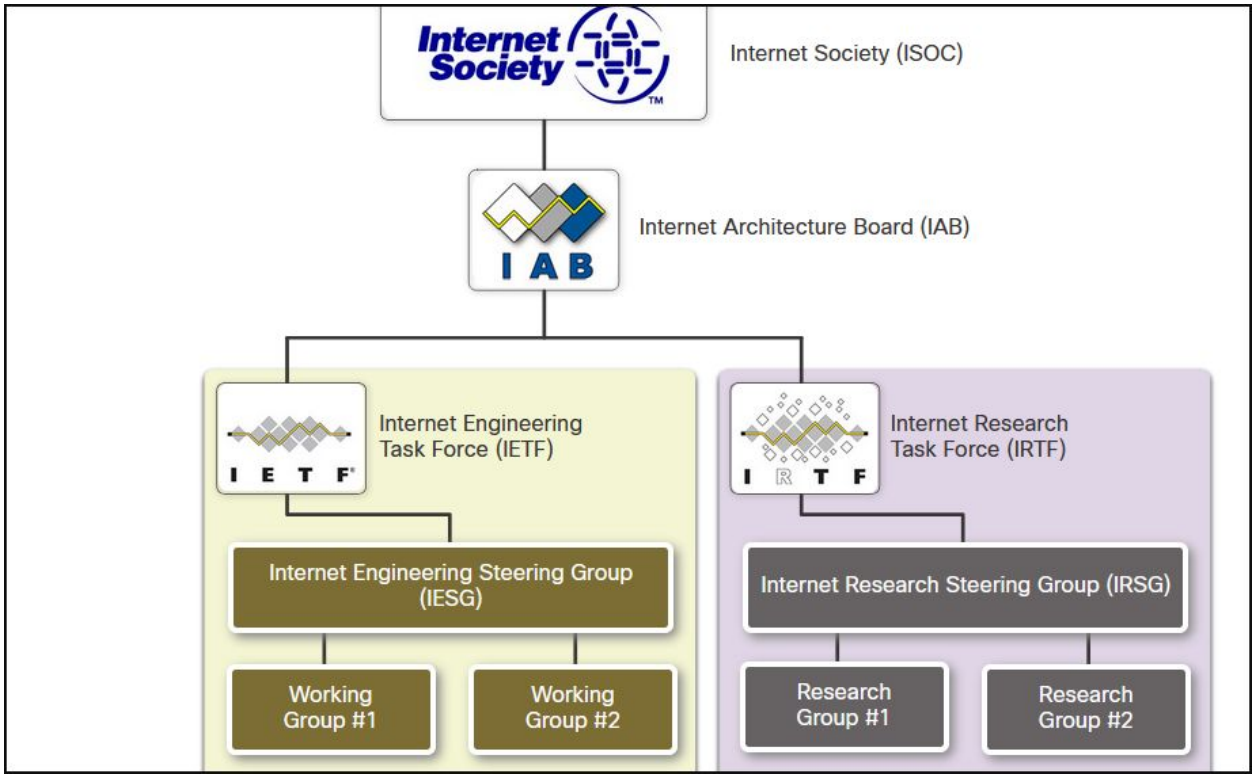
Viewing Mayank Jagota's screen

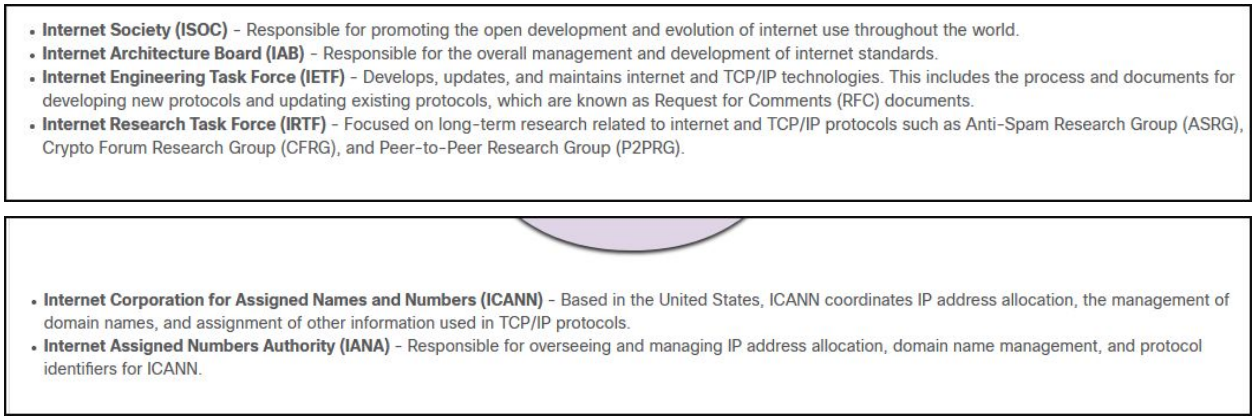
Standards Organizations

Internet Standards



- **Internet Society (ISOC)** - Promotes the open development and evolution of internet
- **Internet Architecture Board (IAB)** - Responsible for management and development of internet standards
- **Internet Engineering Task Force (IETF)** - Develops, updates, and maintains internet and TCP/IP technologies
- **Internet Research Task Force (IRTF)** - Focused on long-term research related to internet and TCP/IP protocols





Electronic and Communications Standards

Other standards organizations have responsibilities for promoting and creating the electronic and communication standards used to deliver the IP packets as electronic signals over a wired or wireless medium.

These standard organizations include the following:

- **Institute of Electrical and Electronics Engineers** (**IEEE**, pronounced “I-triple-E”) - Organization of electrical engineering and electronics dedicated to advancing technological innovation and creating standards in a wide area of industries including power and energy, healthcare, telecommunications, and networking. Important IEEE networking standards include 802.3 Ethernet and 802.11 WLAN standard. Search the internet for other IEEE network standards.
- **Electronic Industries Alliance (EIA)** - Organization is best known for its standards relating to electrical wiring, connectors, and the 19-inch racks used to mount networking equipment.
- **Telecommunications Industry Association (TIA)** - Organization responsible for developing communication standards in a variety of areas including radio equipment, cellular towers, Voice over IP (VoIP) devices, satellite communications, and more.
- **International Telecommunications Union-Telecommunication Standardization Sector (ITU-T)** - One of the largest and oldest communication standards organizations. The ITU-T defines standards for video compression, Internet Protocol Television (IPTV), and broadband communications, such as a digital subscriber line (DSL).

Good job!

You have successfully identified the correct answers.

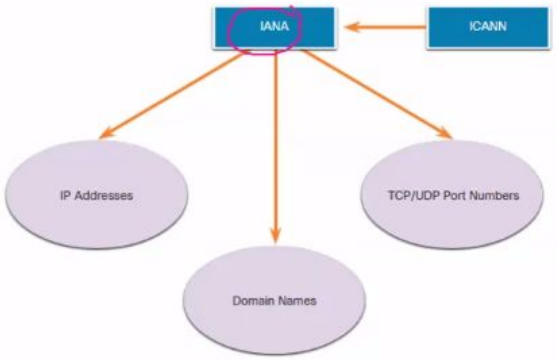
1. The correct answer is True. Most standards organizations are vendor-neutral, non-profit organizations that develop and promote open standards.
2. The IETF develops and maintains the specifications for new protocols and updates to existing protocols through published documents called Request for Comments (RFCs).
3. IANA is responsible for overseeing and managing IP address allocation, domain name management, and protocol identifiers for ICANN.
4. The Electronics Industries Alliance (EIA) develops standards related to electrical wiring, connectors, and network equipment racks.

You answered 4 out of 4 questions correctly.

Viewing Mayank Jagota's screen

Standards Organizations

Internet Standards (Cont.)



Standards organizations involved with the development and support of TCP/IP

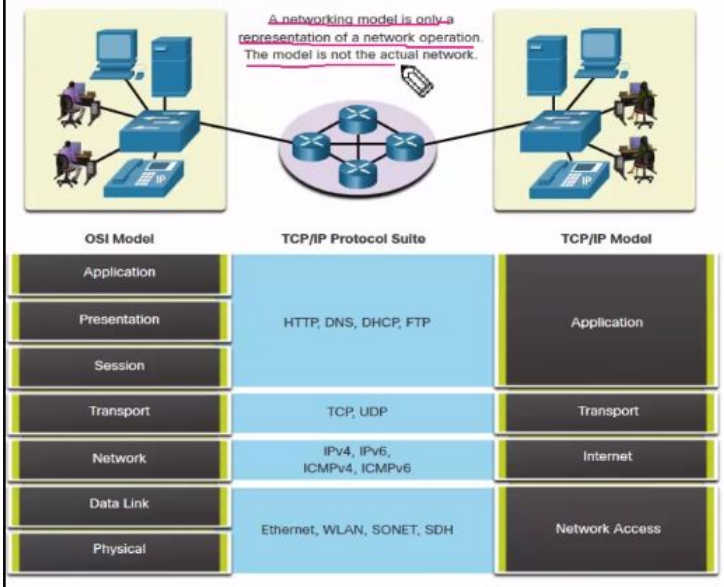
- **Internet Corporation for Assigned Names and Numbers (ICANN)** - Coordinates IP address allocation, the management of domain names, and assignment of other information
- **Internet Assigned Numbers Authority (IANA)** - Oversees and manages IP address allocation, domain name management, and protocol identifiers for ICANN

Electronic and Communications Standards

- **Institute of Electrical and Electronics Engineers** (**IEEE**, pronounced "I-triple-E") - dedicated to creating standards in power and energy, healthcare, telecommunications, and networking
- **Electronic Industries Alliance (EIA)** - develops standards relating to electrical wiring, connectors, and the 19-inch racks used to mount networking equipment
- **Telecommunications Industry Association (TIA)** - develops communication standards in radio equipment, cellular towers, Voice over IP (VoIP) devices, satellite communications, and more
- **International Telecommunications Union-Telecommunication Standardization Sector (ITU-T)** - defines standards for video compression, Internet Protocol Television (IPTV), and broadband communications, such as a digital subscriber line (DSL)

Reference Models

The Benefits of Using a Layered Model

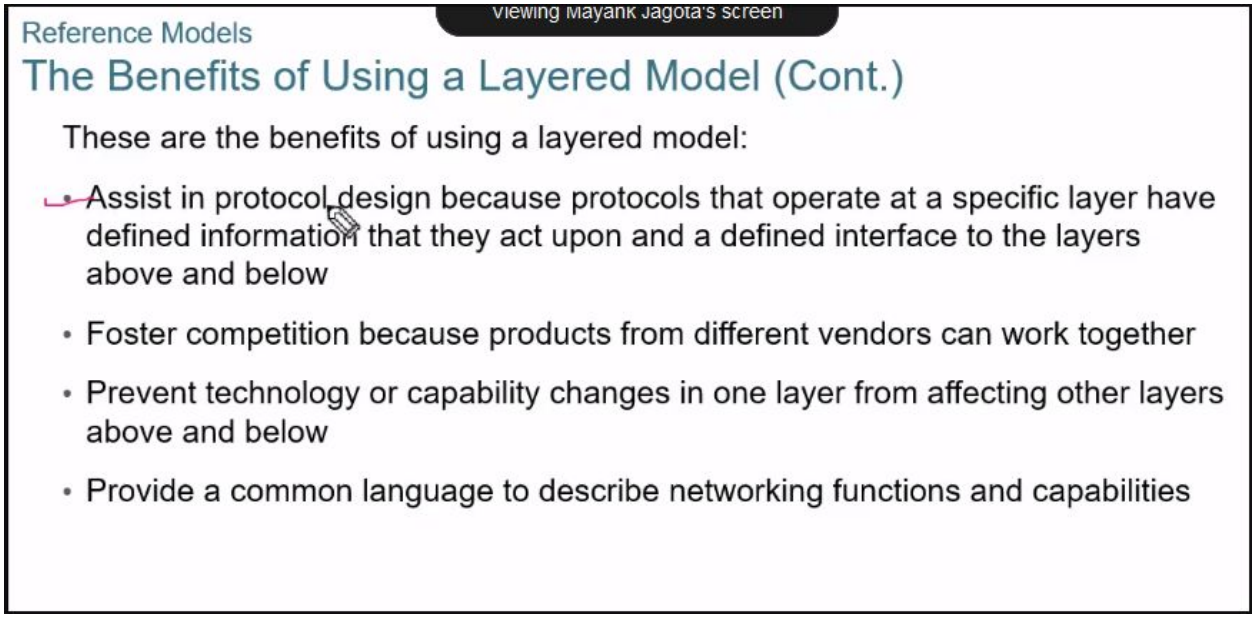


Complex concepts such as how a network operates can be difficult to explain and understand. For this reason, a layered model is used.

Two layered models describe network operations:

- Open System Interconnection (OSI) Reference Model
- TCP/IP Reference Model

OSI Model Layer	Description
7 - Application	The application layer contains protocols used for process-to-process communications.
6 - Presentation	The presentation layer provides for common representation of the data transferred between application layer services.
5 - Session	The session layer provides services to the presentation layer to organize its dialogue and to manage data exchange.
4 - Transport	The transport layer defines services to segment, transfer, and reassemble the data for individual communications between the end devices.
3 - Network	The network layer provides services to exchange the individual pieces of data over the network between identified end devices.
2 - Data Link	The data link layer protocols describe methods for exchanging data frames between devices over a common media
1 - Physical	The physical layer protocols describe the mechanical, electrical, functional, and procedural means to activate, maintain, and de-activate physical connections for a bit transmission to and from a network device.



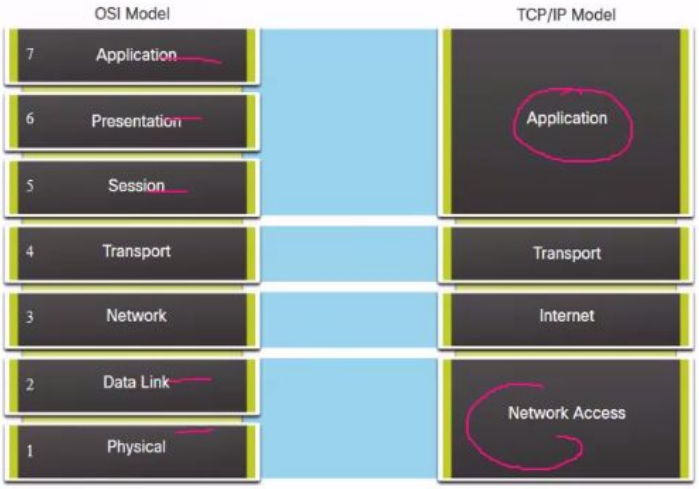
As data moves through the network, it is broken down into smaller pieces and identified so that the pieces can be put back together when they arrive at the destination. Each piece is assigned a specific name and is associated with a specific layer of the TCP/IP and OSI models. The assigned name is called a protocol data unit (PDU).

Reference Models

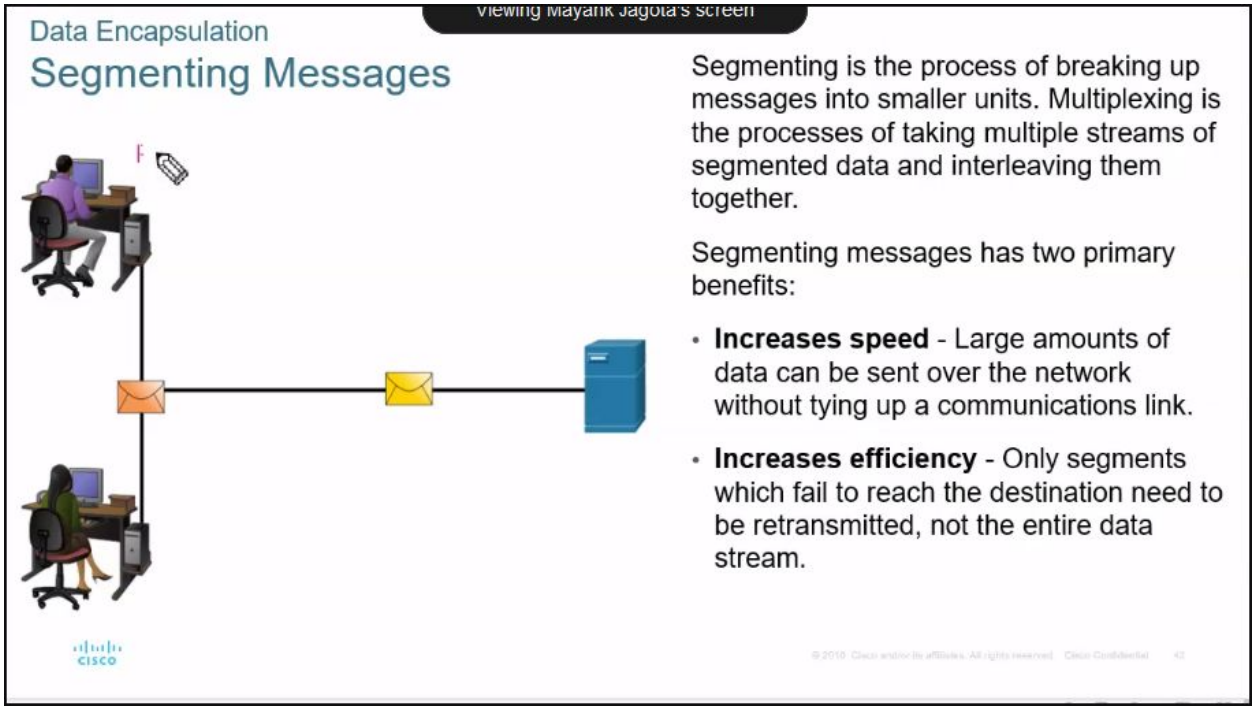
The OSI Reference Model

OSI Model Layer	Description
7 - Application	Contains protocols used for process-to-process communications.
6 - Presentation	Provides for common representation of the data transferred between application layer services.
5 - Session	Provides services to the presentation layer and to manage data exchange.
4 - Transport	Defines services to segment, transfer, and reassemble the data for individual communications.
3 - Network	Provides services to exchange the individual pieces of data over the network.
2 - Data Link	Describes methods for exchanging data frames over a common media.
1 - Physical	Describes the means to activate, maintain, and de-activate physical connections.

OSI and TCP/IP Model Comparison



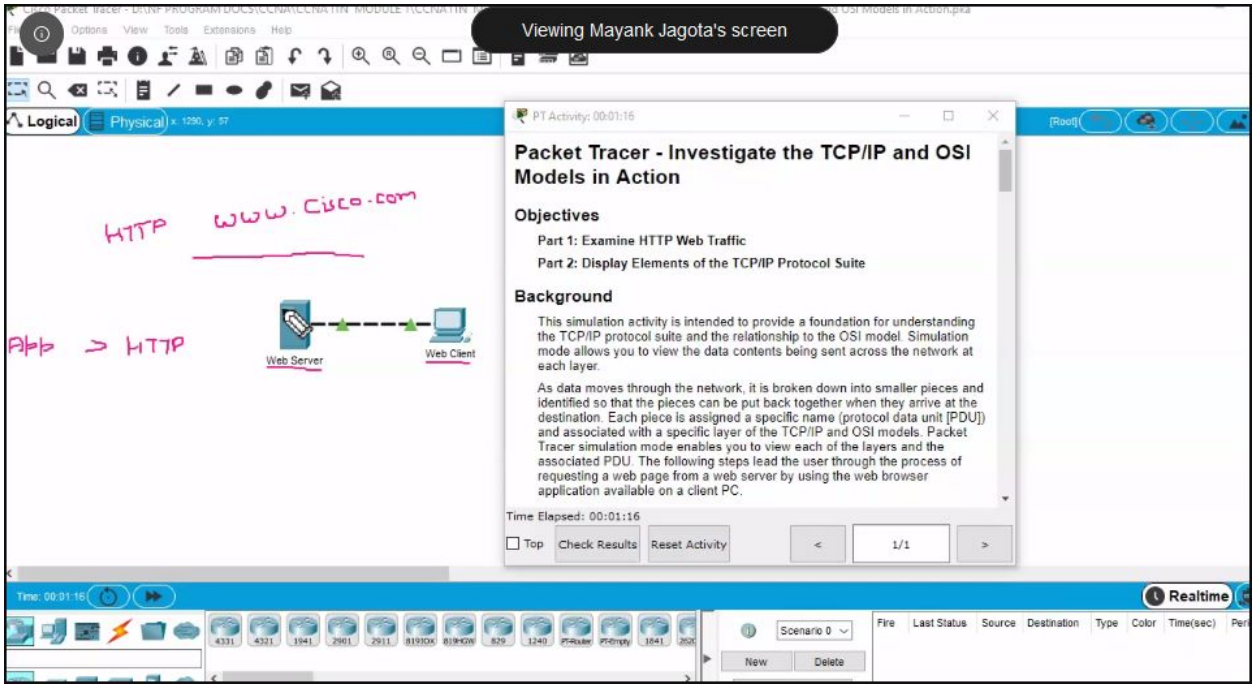
- The OSI model divides the network access layer and the application layer of the TCP/IP model into multiple layers.
- The TCP/IP protocol suite does not specify which protocols to use when transmitting over a physical medium.
- OSI Layers 1 and 2 discuss the necessary procedures to access the media and the physical means to send data over a network.

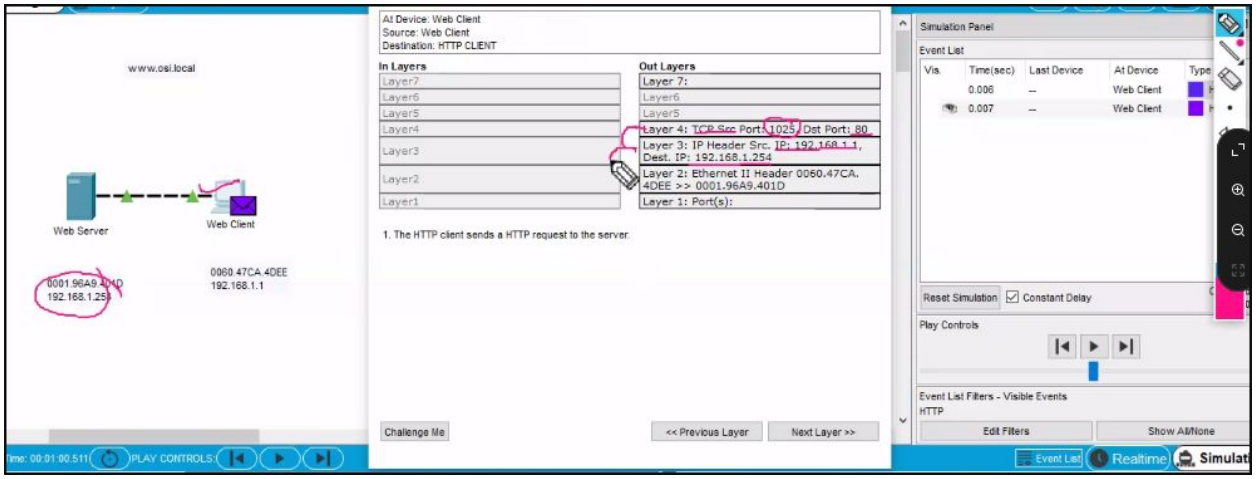


segmenting messages having two primary benefits:

- **Increases speed** - Because a large data stream is segmented into packets, large amounts of data can be sent over the network without tying up a communications link. This allows many different conversations to be interleaved on the network called multiplexing.
- **Increases efficiency** -If a single segment is fails to reach its destination due to a failure in the network or network congestion, only that segment needs to be retransmitted instead of resending the entire data stream.

TCP is responsible for sequencing the individual segment





As application data is passed down the protocol stack on its way to be transmitted across the network media, various protocol information is added at each level. This is known as the encapsulation process.

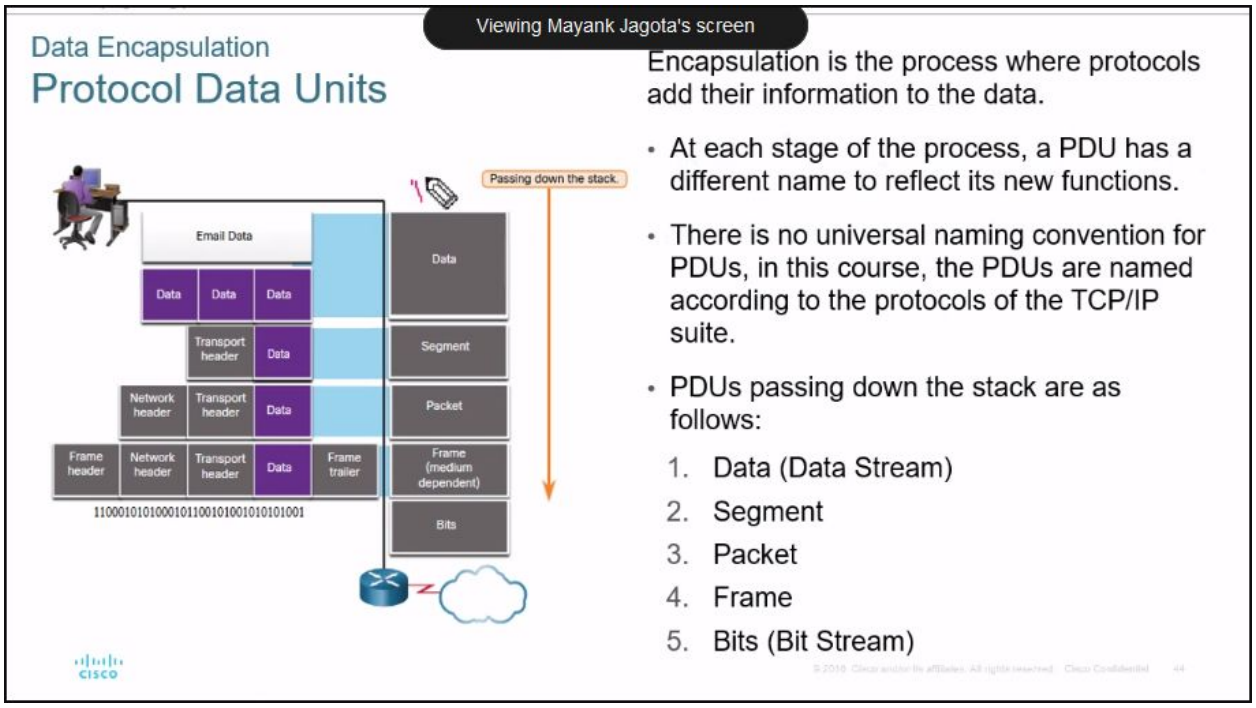
Although the UDP PDU is called datagram, IP packets are sometimes also referred to as IP datagrams.

The form that a piece of data takes at any layer is called a protocol data unit (PDU). During encapsulation, each succeeding layer encapsulates the PDU that it receives from the layer above in accordance with the protocol being used. At each stage of the process, a PDU has a different name to reflect its new functions. Although there is no universal naming convention for PDUs, in this course, the PDUs are named according to the protocols of the TCP/IP suite. The PDUs for each form of data are shown in the figure.

- Data - The general term for the PDU used at the application layer
- Segment - Transport layer PDU
- Packet - Network layer PDU
- Frame - Data Link layer PDU
- Bits - Physical layer PDU used when physically transmitting data over the medium

If the Transport header is TCP, then it is a segment. If the Transport header is UDP then it is a datagram.

De-encapsulation is the process used by a receiving device to remove one or more of the protocol headers. The data is de-encapsulated as it moves up the stack toward the end-user application.

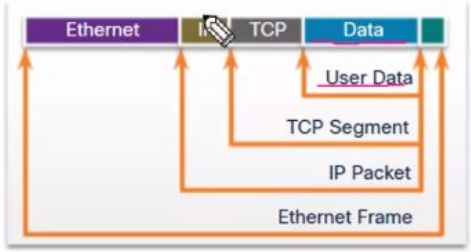


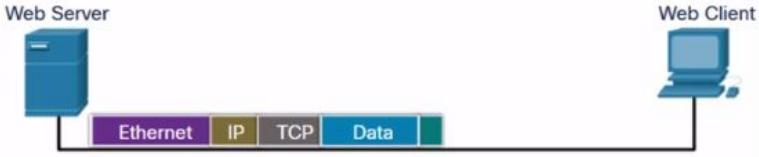
Viewing Mayank Jagota's screen

Data Encapsulation

Encapsulation Example

- Encapsulation is a top down process.
- The level above does its process and then passes it down to the next level of the model. This process is repeated by each layer until it is sent out as a bit stream.





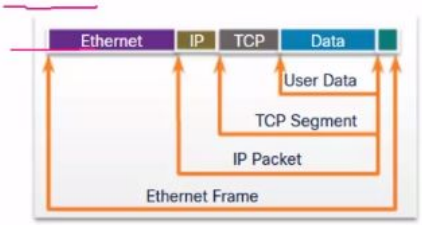
Viewing Mayank Jagota's screen

Data Encapsulation

De-encapsulation Example

- Data is de-encapsulated as it moves up the stack.
- When a layer completes its process, that layer strips off its header and passes it up to the next level to be processed. This is repeated at each layer until it is a data stream that the application can process.

1. Received as Bits (Bit Stream)
2. Frame
3. Packet
4. Segment
5. Data (Data Stream)

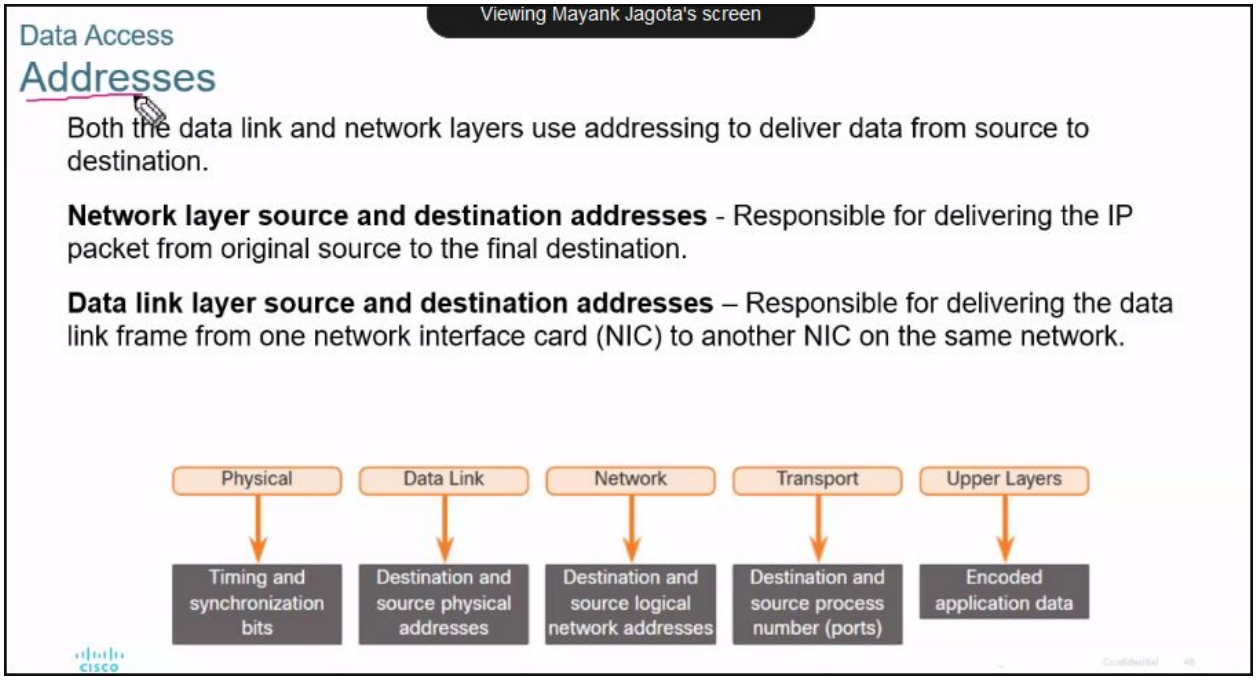


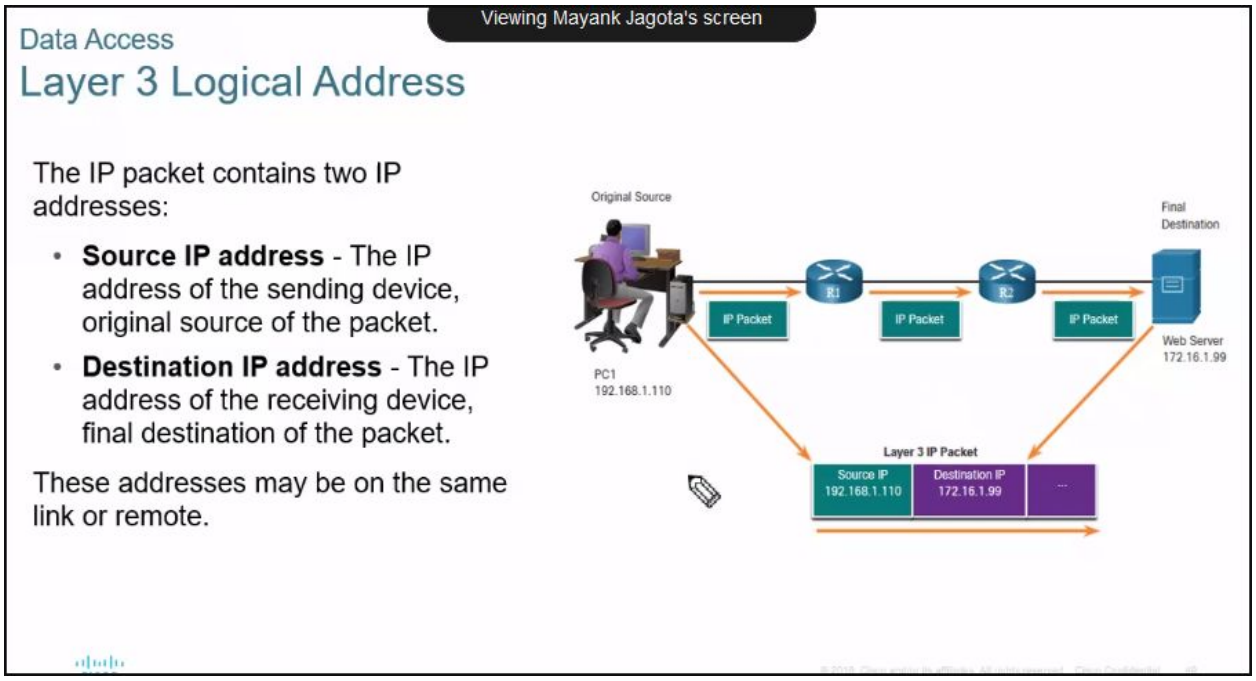
Good job!

You have successfully identified the correct answers.

1. Segmentation is the process of dividing a large data stream into smaller pieces which are then transmitted to the receiver.
2. The transport layer PDU is known as a segment.
3. The data link layer encapsulates data into a frame.
4. As data moves down the protocol stack, protocol data is added to the original data. This process is known as encapsulation.

You answered 4 out of 4 questions correctly.





The network and data link layers are responsible for delivering the data from the source device to the destination device.

- **Network layer source and destination addresses** - Responsible for delivering the IP packet from the original source to the final destination, which may be on the same network or a remote network.
- **Data link layer source and destination addresses** - Responsible for delivering the data link frame from one network interface card (NIC) to another NIC on the same network.

The IP packet contains two IP addresses:

- **Source IP address** - The IP address of the sending device, which is the original source of the packet.
- **Destination IP address** - The IP address of the receiving device, which is the final destination of the packet.

The IP addresses indicate the original source IP address and final destination IP address. This is true whether the source and destination are on the same IP network or different IP networks.

An IP address contains two parts:

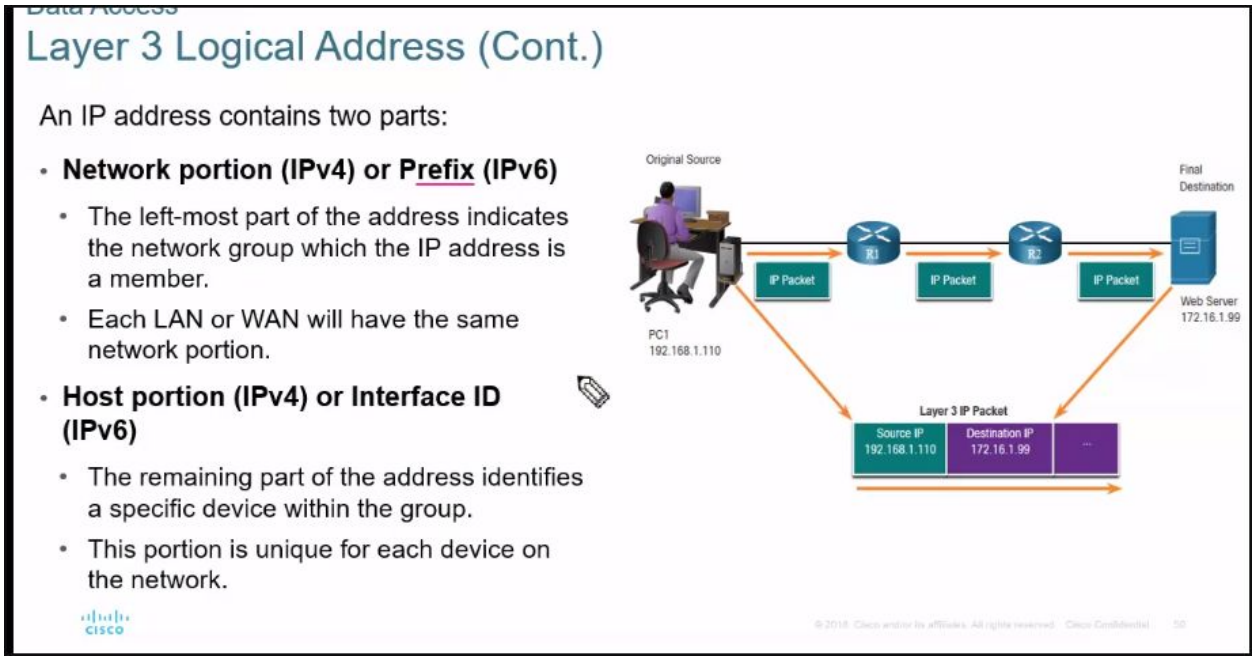
- **Network portion (IPv4) or Prefix (IPv6)** - The left-most part of the address that indicates the network in which the IP address is a member. All devices on the same network will have the same network portion of the address.
- **Host portion (IPv4) or Interface ID (IPv6)** - The remaining part of the address that identifies a specific device on the network. This portion is unique for each device or interface on the network.

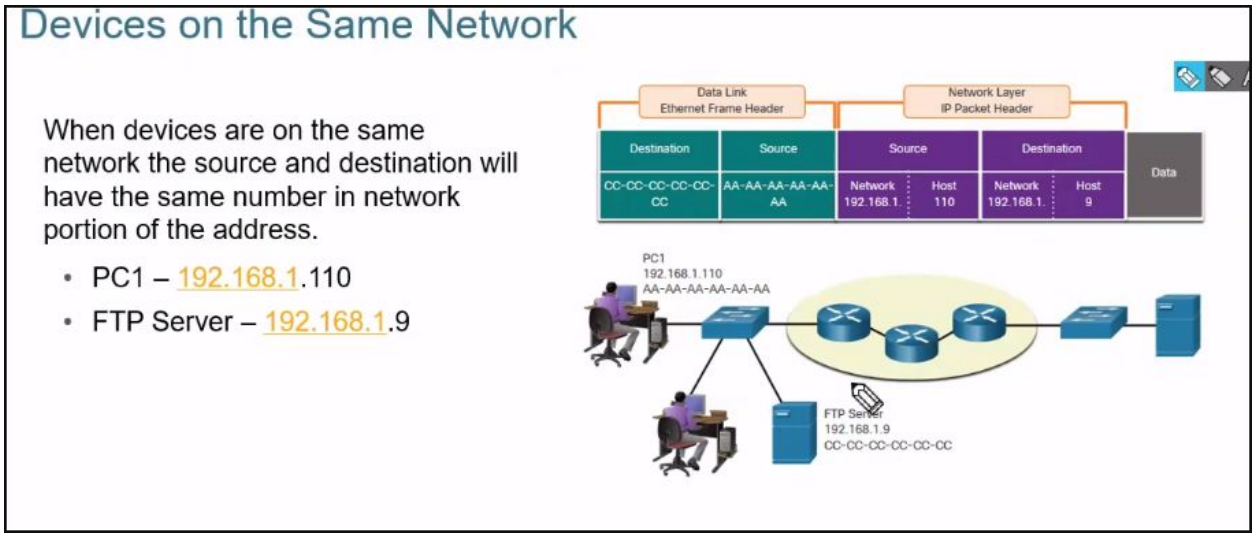
Note: The subnet mask (IPv4) or prefix-length (IPv6) is used to identify the network portion of an IP address from the host portion.

When the sender and receiver of the IP packet are on the same network, the data link frame is sent directly to the receiving device. On an Ethernet network, the data link addresses are known as Ethernet Media Access Control (MAC) addresses

MAC addresses are physically embedded on the Ethernet NIC.

- **Source MAC address** - This is the data link address, or the Ethernet MAC address, of the device that sends the data link frame with the encapsulated IP packet. The MAC address of the Ethernet NIC of PC1 is AA-AA-AA-AA-AA-AA, written in hexadecimal notation.
- **Destination MAC address** - When the receiving device is on the same network as the sending device, this is the data link address of the receiving device. In this example, the destination MAC address is the MAC address of the FTP server:
  CC-CC-CC-CC-CC-CC, written in hexadecimal notation.





the Ethernet data link frame cannot be sent directly to the destination host because the host is not directly reachable in the network of the sender. The Ethernet frame must be sent to another device known as the router or default gateway.

When the receiving device, the destination IP address, is on a different network from the sending device, the sending device uses the Ethernet MAC address of the default gateway or router.

The purpose of the data link address is to deliver the data link frame from one network interface to another network interface on the same network.

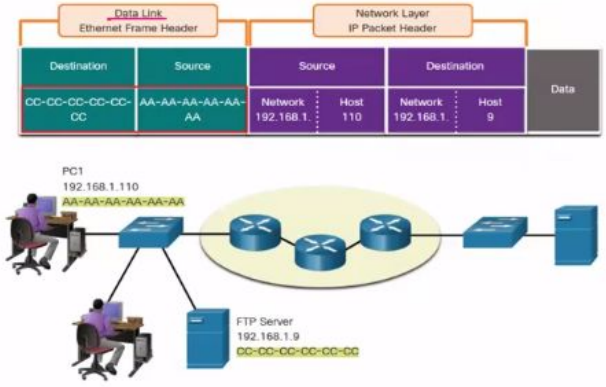
Before an IP packet can be sent over a wired or wireless network, it must be encapsulated in a data link frame, so it can be transmitted over the physical medium.

Role of the Data Link Layer Addresses: Same IP Network

When devices are on the same Ethernet network the data link frame will use the actual MAC address of the destination NIC.

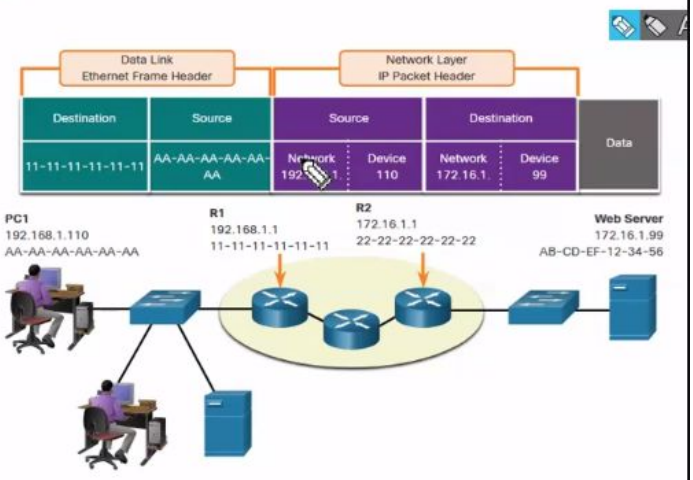
MAC addresses are physically embedded into the Ethernet NIC and are local addressing.

- The Source MAC address will be that of the originator on the link.
- The Destination MAC address will always be on the same link as the source, even if the ultimate destination is remote.



Devices on a Remote Network

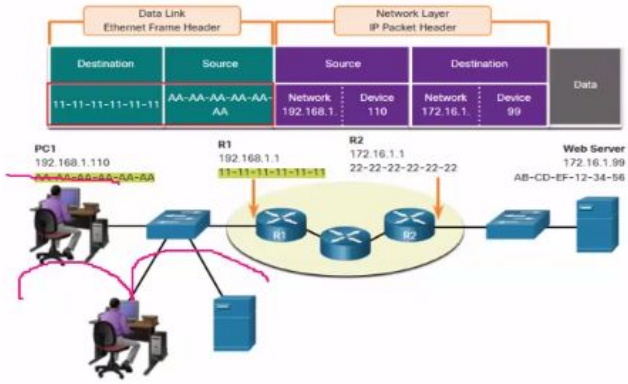
- What happens when the actual (ultimate) destination is not on the same LAN and is remote?
- What happens when PC1 tries to reach the Web Server?
- Does this impact the network and data link layers?



Role of the Data Link Layer Addresses: Different IP Networks (Cont.)

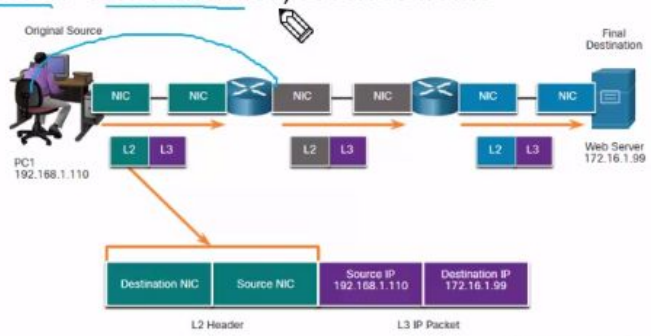
- The data link addressing is local addressing so it will have a source and destination for each link.
- The MAC addressing for the first segment is :
  - Source – AA-AA-AA-AA-AA-AA (PC1) Sends the frame.
  - Destination – 11-11-11-11-11-11 (R1-Default Gateway MAC) Receives the frame.

Note: While the L2 local addressing will change from link to link or hop to hop, the L3 addressing remains the same.



Data Link Addresses

- Since data link addressing is local addressing, it will have a source and destination for each segment or hop of the journey to the destination.
- The MAC addressing for the first segment is:
  - Source – (PC1 NIC) sends frame
  - Destination – (First Router- DGW interface) receives frame



What did I learn in this module?

The Rules

- Protocols must have a sender and a receiver.
- Common computer protocols include these requirements: message encoding, formatting and encapsulation, size, timing, and delivery options.

Protocols

- To send a message across the network requires the use of several protocols.
- Each network protocol has its own function, format, and rules for communications.

Protocol Suites

- A protocol suite is a group of inter-related protocols.
- TCP/IP protocol suite are the protocols used today.

Standards Organizations

- Open standards encourage interoperability, competition, and innovation.

You have successfully identified the correct answers.

1. The correct answer is True. When two devices are on different IP networks, frames cannot be sent directly to the receiver since it is on a different logical network. The frames must first be forwarded to a default gateway (router).
2. The correct answer is False. It is the left-most portion of an IP address that identifies the network. The right-most portion is used to identify the specific device or interface.
3. It is the subnet mask used in IPv4 that is used to determine the network portion of an IPv4 address.
4. MAC addresses are physical addresses and 48 bits or 12 hex digits in length. IPv4 addresses and IPv6 addresses are logical. IPv4 addresses are 32 bits and IPv6 addresses are 128 bits.
5. The data link frame addressing consists of a destination and source MAC address in that order.
6. The correct answer is False. Data link addresses change within the data link frame when the receiving device is not on the same network.

You answered 6 out of 6 questions correctly.