

Host Roles

If you want to be a part of a global online community, your computer, tablet, or smart phone must first be connected to a network. That network must be connected to the internet. This topic discusses the parts of a network. See if you recognize these components in your own home or school network!

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

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

As mentioned before, clients are a type of host. Clients have software for requesting and displaying the information obtained from the server, as shown in the figure.

This figure depicts a client PC and a server connected through a cloud symbolizing the Internet

ClientInternetServer

An example of client software is a web browser, like Chrome or FireFox. A single computer can also run multiple types of client software. For example, a user can check email and view a web page while instant messaging and listening to an audio stream. The table lists three common types of server software.

TypeDescriptionEmailThe email server runs email server software. Clients use mail client software, such as Microsoft Outlook, to access email on the server. WebThe web server runs web server software. Clients use browser software, such as Windows Internet Explorer, to access web pages on the server.FileThe file server stores corporate and user files in a central location. The client devices access these files with client software such as the Windows File Explorer.	
Type	Description
Email	The email server runs email server software. Clients use mail client software, such as Microsoft Outlook, to access email on the server.
Web	The web server runs web server software. Clients use browser software, such as Windows Internet Explorer, to access web pages on the server.
File	The file server stores corporate and user files in a central location. The client devices access these files with client software such as the Windows File Explorer.

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 figure shows a small network with three devices. A printer is on the left, connected to a print sharing PC in the middle, which is also connected to a file sharing PC on the right. Under the topology is a list of the advantages and disadvantage of peer-to-peer networking. The advantages of peer-to-peer networking are: easy

to set up, less complex, lower cost because network devices and dedicated servers may not be required, and can be used for simple tasks such as transferring files and sharing printers. The disadvantages of peer-to-peer networking are: no centralized administration, not as secure, not scalable, all devices may act as both clients and servers which can slow their performance.

I have a printer to shareI have files to sharePrint SharingFile Sharing

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

1.2.3

End Devices

The network devices that people are most familiar with are end devices. To distinguish one end device from another, each end device on a network has an address. When an end device initiates communication, it uses the address of the destination end device to specify where to deliver the message.

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

Click Play in the figure to see an animation of data flowing through a network.

The figure shows a physical network topology with a block of LAN, a block of InternetWork, and a block of another LAN. From left to right, a LAN has two users an IP phone, a PC, and a server connected to a switch. A physical link connects the LAN switch to an edge router that boards the LAN block and the Internetwork block. The Internetwork block consists of four routers connected in a full mesh topology. An edge router boards the Internetwork block and a second LAN block. The second LAN block consists of two users, an IP phone, a PC, and a server. When the animation is started a message originates from one of the users in the first LAN and travels from the user, to the switch and to the edge router that boards the Internetwork. At the Internetwork the message is routed through to the other edger router that boards with the second LAN. The message is forwarded into the second LAN, through the switch and to the destination end user. Text under the graphic reads Data originates with an end device, flows through the network, and arrives at the end device.

Internetwork
LAN
LAN

Messages can take
alternate routes.

Data originates with an end device, flows through the network, and arrives at an end device.

1.2.4

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.

The picture shows symbols of five common intermediary devices and describes some of their functions. At the top is a wireless router, LAN switch, and router. Below is a multilayer switch and firewall appliance. 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.

Intermediary DevicesWireless RouterLAN SwitchRouterMultilayer SwitchFirewall Appliance
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.

1.2.5

Network Media

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

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

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

There are three images of common network media followed by criteria to use when choosing network media. The top image shows twisted pair wires and connectors used with copper media. The middle image is a multi-strand fiber optic cable and fiber optic connectors. The bottom image shows wireless devices including a router and a camera. Different types of network media have different features and benefits. Not all types of network media have the same characteristics, nor are they appropriate for the same purposes. The four main criteria for choosing network media are these: What is the maximum distance that the media can successfully carry a signal? What is the environment in which the media will be installed? What is the amount of data and at what speed must it be transmitted? What is the cost of the media and installation?

1.3.1

Network Representations

Network architects and administrators must be able to show what their networks will look like. They need to be able to easily see which components connect to other components, where they will be located, and how they will be connected. Diagrams of networks often use symbols, like those shown in the figure, to represent the different devices and connections that make up a network.

Image shows symbols used in network diagrams. At the top are the following end devices: desktop computer, laptop, printer, IP phone, wireless tablet, and TelePresence endpoint. In the middle are the following intermediary devices: wireless router, LAN switch, router, multilayer switch, and firewall appliance. At the bottom are the following network media: blue waves depicting wireless media, a solid black line depicting LAN media, and a red lighting bolt depicting WAN media.

End DevicesDesktop ComputerLaptopPrinterIP PhoneWireless TabletTelePresence Endpoint**Intermediary Devices**Wireless RouterLAN SwitchRouterMultilayer SwitchFirewall Appliance**Network Media**Wireless MediaLAN MediaWAN Media

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. The ability to recognize the logical representations of the physical networking components is critical to being able to visualize the organization and operation of a network.

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

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

Note: The terms port and interface are often used interchangeably.

1.3.2

Topology Diagrams

Topology diagrams are mandatory documentation for anyone working with a network. They provide a visual map of how the network is connected. There are two types of topology diagrams: physical and logical.

Physical Topology Diagrams

Physical topology diagrams illustrate the physical location of intermediary devices and cable installation, as shown in the figure. You can see that the rooms in which these devices are located are labeled in this physical topology.

The physical network topology shows six rooms, each highlighted in a light yellow box, with various networking devices and cabling. On the left side is the server room labeled room 2158. It contains a router labeled R1 mounted on rack 1 shelf 1 with six cable connections. A cable at the top connects to a cloud labeled Internet. A cable to the left connects to a switch labeled S1 mounted on rack 1 shelf 2. S1 is connected to three servers: a web server mounted on rack 2 shelf 1, an email server mounted on rack 2 shelf 2, and a file server mounted on rack 2 shelf 3. A cable connected to the bottom of R1 connects to a switch labeled S2 mounted on rack 1 shelf 3. S2 has two connections leading to a printer and a PC in the IT office labeled room 2159. R1 has three cables to the right connected to three switches located in room 2124. The top switch is labeled S3 and mounted on rack 1 shelf 1. The middle switch is labeled S4 and mounted on rack 1 shelf 2. The bottom switch is labeled S5 and mounted on rack 1 shelf 3. S3 has a cable on the left connected to a laptop in a room labeled class 1 room 2125. S4 has a cable on the left connected to a laptop in a room labeled class 2 room 2126. S5 has a cable on the left connected to a laptop in a room labeled class 3 room 2127.

R1S1S2S3S4S5
InternetEmail Server
Rack 2
Shelf 2Web Server
Rack 2
Shelf 1File Server
Rack 2
Shelf 3Rack 1
Shelf 2Rack 1
Shelf 1Rack 1
Shelf 2Rack 1
Shelf 1Rack 1
Shelf 3Rack 1
Shelf 3**Server Room: Rm: 2158IT Office: Rm: 2159Class 1: Rm: 2125Class 2: Rm: 2126Class 3: Rm: 2127Rm: 2124**

Logical Topology Diagrams

Logical topology diagrams illustrate devices, ports, and the addressing scheme of the network, as shown in the figure. You can see which end devices are connected to which intermediary devices and what media is being used.

The logical network topology shows devices, port labels, and the network addressing scheme. In the middle of the picture is a router labeled R1. A port labeled G0/0 connects to a cloud at the top labeled Internet. A port labeled G0/1 connects at the left to a switch labeled S1 at port G0/1. S1 is connected to three servers. S1 and the servers are highlighted in a light yellow circle with the network 192.168.10.0 written at the top. Port F0/1 on S1 connects to a web server. Port F0/2 on S1 connects to an email server. Port F0/3 on S1 connects to a file server. Port F0/1 on R1 connects at the bottom to a switch labeled S2. S2 connects to a printer and a PC, all of which are highlighted in a light yellow circle with the network 192.168.11.0 written on the bottom. At the left of R1 are three additional connections, each connecting to a switch at port G0/1 which is then connected to a laptop at port F0/1. Each switch and laptop are highlighted in yellow and the network address shown. Port G0/0 of R1 connects at the top to a switch labeled S3 on network 192.168.100.0. Port G1/1 of R1 connects in the middle to a switch labeled S4 on network 192.169.101.0. Port G1/2 on R1 connects at the bottom to a switch labeled S5 on network 192.168.102.0.

R1Fa0/1Fa0/2Fa0/3G0/1G0/1G0/0G1/0G0/1G0/1G1/1G0/1Fa0/1Fa0/1Fa0/1G1/2G0/1G0/2S1S2S3S4S5Fa0/2Fa0/1
InternetEmail ServerWeb ServerFile Server**Network**
192.168.10.0Network 192.168.11.0Network 192.168.100.0Network 192.168.101.0Network 192.168.102.0

The topologies shown in the physical and logical diagrams are appropriate for your level of understanding at this point in the course. Search the internet for “network topology diagrams” to see some more complex examples. If you add the word “Cisco” to your search phrase, you will find many topologies using icons that are similar to what you have seen in these figures.

Networks of Many Sizes

Now that you are familiar with the components that make up networks and their representations in physical and logical topologies, you are ready to learn about the many different types of networks.

Networks come in all sizes. They range from simple networks consisting of two computers, to networks connecting millions of devices.

Simple home networks let you share resources, such as printers, documents, pictures, and music, among a few local end devices.

Small office and home office (SOHO) networks allow people to work from home, or a remote office. Many self-employed workers use these types of networks to advertise and sell products, order supplies, and communicate with customers.

Businesses and large organizations use networks to provide consolidation, storage, and access to information on network servers. Networks provide email, instant messaging, and collaboration among employees. Many organizations use their network’s connection to the internet to provide products and services to customers.

The internet is the largest network in existence. In fact, the term internet means a “network of networks”. It is a collection of interconnected private and public networks.

In small businesses and homes, many computers function as both the servers and clients on the network. This type of network is called a peer-to-peer network.

Click each button for more information.

- Small Home Networks
- Small Office and Home Office Networks
- Medium to Large Networks
- World Wide Networks

Small Home Networks

Small home networks connect a few computers to each other and to the internet.

LANs and WANs

Network infrastructures vary greatly in terms of:

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

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

The network topology shows three LANs connected via a WAN link in the center. A legend shows that LANs are highlighted in yellow and WANs in light purple. The WAN is located in the center of the diagram. It contains a cloud symbol labeled cloud with red WAN connections to three routers. Each router is located partly in the WAN and partly in a LAN. At the bottom left is the Central LAN. It contains a server, two multilayer switches, two LAN switches, and four PCs. At the bottom right is the Branch LAN. It contains a switch, a server, a printer, two IP phones each connected to a PC, and a wireless access point with wireless connections to a laptop and a smartphone. At the top right is the home office LAN. It contains a wireless router with a wired connection to a printer and wireless conections to a laptop and a monitor.

LANs

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

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

The diagram is an illustration of a LAN. At the center of the diagram is a switch. There are four Ethernet connections on the switch. At the top left is a connection to a PC. Below that is a connection to the computer at the desk of a worker. Below that is another connection to the computer at the desk of a worker. At the bottom left is a connection to an IP phone. To the right of the switch is a connection to a server. Text under the figure reads: a network serving a home, small building, or a small campus is considered a LAN.

A network serving a home, small building, or a small campus is considered a LAN.

WANs

The figure shows a WAN which interconnects two LANs. A WAN is a network infrastructure that spans a wide geographical area. WANs are typically managed by service providers (SPs) or Internet Service Providers (ISPs).

WANs have specific characteristics:

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

The figure shows two branch LANs connected via a WAN link. Both LANs are highlighted in a light yellow box and consist of a central switch connected to three PCs, an IP phone, a server, and a router. The two routers are connected via a red WAN link. On the left is the branch 1 LAN and on the right is the branch 2 LAN.

Branch 1 LANBranch 2 LAN

1.4.3

The Internet

The internet is a worldwide collection of interconnected networks (internetworks, or internet for short). The figure shows one way to view the internet as a collection of interconnected LANs and WANs.

Five multilayer switches with redundant links are shown inside a large cloud. Around the edge of the cloud are seven routers connected to various LANs. There is a hospital LAN, a school LAN, a business LAN, a government LAN, and three home LANs. Text at the bottom reads LANs use WAN services to interconnect.

Home LANHospital LANGovernment LANBusiness LANSchool LAN
LANs use WAN services to interconnect.

Some of the LAN examples are connected to each other through a WAN connection. WANs are then connected to each other. The red WAN connection lines represent all the varieties of ways we connect networks. WANs can connect through copper wires, fiber-optic cables, and wireless transmissions (not shown).

The internet is not owned by any individual or group. Ensuring effective communication across this diverse infrastructure requires the application of consistent and commonly recognized technologies and standards as well as the cooperation of many network administration agencies. There are organizations that were developed to help maintain the structure and standardization of internet protocols and processes. These organizations include the Internet Engineering Task Force (IETF), Internet Corporation for Assigned Names and Numbers (ICANN), and the Internet Architecture Board (IAB), plus many others.

1.4.4

Intranets and Extranets

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

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

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

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

The figure illustrates the levels of access that different groups have to a company intranet, a company extranet, and the internet.

1.5.1

Internet Access Technologies

So, now you have a basic understanding of what makes up a network and the different types of networks. But, how do you actually connect users and organizations to the internet? As you may have guessed, there are many different ways to do this.

Home users, remote workers, and small offices typically require a connection to an ISP to access the internet. Connection options vary greatly between ISPs and geographical locations. However, popular choices include broadband cable, broadband digital subscriber line (DSL), wireless WANs, and mobile services.

Organizations usually need access to other corporate sites as well as the internet. Fast connections are required to support business services including IP phones, video conferencing, and data center storage. SPs offer business-class interconnections. Popular business-class services include business DSL, leased lines, and Metro Ethernet.

1.5.2

Home and Small Office Internet Connections

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

The figure shows common connection options for small office and home office users. From left to right, a box on the left-most shows three end user scenarios, at the top is a house and a home user inside the house, in the middle is a standing user labeled Teleworker, and at the bottom is an office building labeled Small Office. There is another box on the right which shows a large office building labeled Internet Service Provider. Four different connection method are shown between the end user box and the ISP box. At the top is a straight line labeled DSL. Below DSL is another straight line labeled Cable. Below Cable is a blue air wave line labeled Cellular. Below Cellular is a satellite that links both boxes with dish receivers/transmitters. At the bottom is another straight line label Dial-Up Telephone. On the rightmost is a cloud depicting Internet. A lightening bolt line shows the connection between the ISP and Internet.

Home UserTeleworkerSmall OfficeDSL CableCellularInternetSatelliteDial-Up TelephoneInternet Service Provider

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

The choice of connection varies depending on geographical location and service provider availability.

Businesses Internet Connections

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

The figure illustrates common connection options for businesses.

common connection options for businesses

OrganizationInternet Service ProviderSatelliteBusiness DSLMetro EthernetDedicated Leased LinesInternet

- **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 ethernet extends 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.

The choice of connection varies depending on geographical location and service provider availability.

The Converging Network

Traditional Separate Networks

Consider a school built thirty years ago. Back then, some classrooms were cabled for the data network, telephone network, and video network for televisions. These separate networks could not communicate with each other. Each network used different technologies to carry the communication signal. Each network had its own set of rules and standards to ensure successful communication. Multiple services ran on multiple networks.

separate computer, telephone, and broadcast networks

DevicesMediumMessageRule Agreement StandardRule Agreement StandardRule Agreement
StandardMediumMessageDevicesMediumMessageDevicesComputer NetworksTelephone NetworksBroadcast Networks

Converged Networks

Today, the separate data, telephone, and video networks converge. Unlike dedicated networks, converged networks are capable of delivering 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. Converged data networks carry multiple services on one network.

Converged data network carrying multiple services on one network.

Network Architecture

Have you ever been busy working online, only to have “the internet go down”? As you know by now, the internet did not go down, you just lost your connection to it. It is very frustrating. With so many people in the world relying on network access to work and learn, it is imperative that networks are reliable. In this context, reliability means more than your connection to the internet. This topic focuses on the four aspects of network reliability.

The role of the network has changed from a data-only network to a system that enables the connections of people, devices, and information in a media-rich, converged network environment. For networks to function efficiently and grow in this type of environment, the network must be built upon a standard network architecture.

Networks also support a wide range of applications and services. They must operate over many different types of cables and devices, which make up the physical infrastructure. The term network architecture, in this context, refers to the technologies that support the infrastructure and the programmed services and rules, or protocols, that move data across the network.

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

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

1.6.2

Fault Tolerance

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

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

The network topology consists of four routers with redundant links. At the top of the diagram is the Internet cloud with two connections at the bottom, each leading to a router. Below these routers is a connection to another router. Each bottom router connects back to both routers that connect to the Internet. The router on the bottom left is connected to a switch with three desktops and three IP phones. The router on the bottom right is connected to a switch with three desktops. The top left router has a red circle with a diagonal line. The top right router has a green arrow leading to the Internet. A text box reads: redundant connections allow for alternative paths if a device fails; the user experience is unaffected.

Internet Redundant connections allow for alternative paths if a device or a link fails. The user experience is unaffected.

1.6.3

Scalability

A scalable network expands quickly to support new users and applications. It does this without degrading the performance of services that are being accessed by existing users. The figure shows how a new network is easily added to an existing network. These networks are scalable because the designers follow accepted standards and protocols. This lets software and hardware vendors focus on improving products and services without having to design a new set of rules for operating within the network.

The network topology consists of four routers with redundant links including two connections to the Internet cloud. There are three LANs, one of which has been recently added. A text box reads: additional users and whole networks can be connected to the internet without degrading performance for existing users.

Internet Additional users and whole networks can be connected to the internet without degrading performance for existing users.

1.6.4

Quality of Service

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

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

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

network topology with PCs and IP phones connected to a switch which is connected to a router that is managing quality of service by prioritizing traffic

Quality of Service, managed by the router, ensures that priorities are matched with the type of communication and its importance to the organization. Web pages can usually receive a lower priority. A Voice over IP (VoIP) Call will need priority to maintain a smooth, uninterrupted user experience. Internet

1.6.5

Network Security

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

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

network topology with PCs and IP phones connected to a switch which is connected to a router that can protect the network with software and hardware security and by preventing physical access to network devices.

Administrators can protect the network with software and hardware security and by preventing physical access to network devices. Internet Security measures protect the network from unauthorized access. Login: ? Password: ?

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

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

1.7.1

Recent Trends

You know a lot about networks now, what they are made of, how they connect us, and what is needed to keep them reliable. But networks, like everything else, continue to change. There are a few trends in networking that you, as a NetAcad student, should know about.

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

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

1.7.2

Bring Your Own Device (BYOD)

The concept of any device, for any content, in any manner, is a major global trend that requires significant changes to the way we use devices and safely connect them to networks. This is called Bring Your Own Device (BYOD).

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

BYOD means any device, with any ownership, used anywhere.



1.7.3

Online Collaboration

Individuals want to connect to the network, not only for access to data applications, but also to collaborate with one another. Collaboration is defined as “the act of working with another or others on a joint project.” Collaboration tools, like Cisco WebEx, shown in the figure, give employees, students, teachers, customers, and partners a way to instantly connect, interact, and achieve their objectives.



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

Cisco Webex Teams is a multifunctional collaboration tool that lets you send instant messages to one or more people, post images, and post videos and links. Each team 'space' maintains a history of everything that is posted there.

1.7.4

Video Communications

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

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

1.7.5

Video - Cisco Webex for Huddles

Click Play in the figure to view how Cisco Webex is incorporated into everyday life and business.

Play Video

1.7.6

Cloud Computing

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

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

Cloud computing is possible because of data centers. Data centers are facilities used to house computer systems and associated components. A data center can occupy one room of a building, one or more floors, or an entire warehouse-sized building. Data centers are typically very expensive to build and maintain. For this reason, only large organizations use privately built data centers to house their data and provide services to users. Smaller

organizations that cannot afford to maintain their own private data center can reduce the overall cost of ownership by leasing server and storage services from a larger data center organization in the cloud.

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

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

Cloud Types

Table caption	
Cloud Type	Description
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.

1.7.7

Technology Trends in the Home

Networking trends are not only affecting the way we communicate at work and at school, but also changing many aspects of the home. The newest home trends include ‘smart home technology’.

Smart home technology integrates into every-day appliances, which can then connect with other devices to make the appliances more ‘smart’ or automated. For example, you could prepare food and place it in the oven for cooking prior to leaving the house for the day. You program your smart oven for the food you want it to cook. It would also be connected to your ‘calendar of events’ so that it could determine what time you should be available to eat and adjust start times and length of cooking accordingly. It could even adjust cooking times and temperatures based on changes in schedule. Additionally, a smart phone or tablet connection lets you connect to the oven directly, to make any desired adjustments. When the food is ready, the oven sends an alert message to you (or someone you specify) that the food is done and warming.

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.

A depiction of smart home technology showing a cloud with arrows pointing to a house, a car, and a smartphone. Text at the bottom reads: The smart phone is updated from the cloud with the status of the smart home devices and the smart car; the user can then use the smart phone to interact with the smart home and smart car.

Cloud

The smart phone is updated from the cloud with the status of the smart home devices and the smart car. The user can then use the smart phone to interact with the smart home and smart car.

Powerline Networking

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

An open floorplan of a home using powerline networking for a home network. There are three PLEK400 4-port powerline adapters plugged into three different electrical outlets all connected together via wired connections. Each adapter has at least one powerline connection to a networked device including desktops and TVs.

PLEK400
4-Port Powerline
AdapterWireless-N
Router**PLE400PLSK400**
4-Port Powerline
AdapterPowerline ConnectionWired Connection

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

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

Wireless Broadband

In many areas where cable and DSL are not available, wireless may be used to connect to the internet.

Wireless Internet Service Provider

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

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

Wireless Broadband Service

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

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

Security Threats

You have, no doubt, heard or read news stories about a company network being breached, giving threat actors access to the personal information of thousands of customers. For this reason, network security is always going to be a top priority of administrators.

Network security is an integral part of computer networking, regardless of whether the network is in a home with a single connection to the internet or is a corporation with thousands of users. Network security must consider the

environment, as well as the tools and requirements of the network. It must be able to secure data while still allowing for the quality of service that users expect of the network.

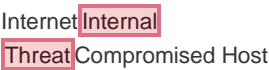
Securing a network involves protocols, technologies, devices, tools, and techniques in order to protect data and mitigate threats. Threat vectors may be external or internal. Many external network security threats today originate from the internet.

There are several common external threats to networks:

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

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

two arrows leading to a compromised host; one coming from the Internet cloud going through a firewall, the other coming from an internal threat on the inside network



1.8.2

Security Solutions

No single solution can protect the network from the variety of threats that exist. For this reason, security should be implemented in multiple layers, using more than one security solution. If one security component fails to identify and protect the network, others may succeed.

A home network security implementation is usually rather basic. Typically, you implement it on the end devices, as well as at the point of connection to the internet, and can even rely on contracted services from the ISP.

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

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

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

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

Network security requirements must consider the environment, as well as the various applications, and computing requirements. Both home and business environments must be able to secure their data while still allowing for the quality of service that users expect of each technology. Additionally, the security solution implemented must be adaptable to the growing and changing trends of the network.

The study of network security threats and mitigation techniques starts with a clear understanding of the underlying switching and routing infrastructure used to organize network services.

CCNA

As a NetAcad student, you may already have a career in IT, or are still educating yourself to prepare for your career. In either case, it is good to know about the skills needed to match the types of jobs that are available in IT.

The role and skills required of network engineers are evolving and are more vital than ever. 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.

A consolidated and updated CCNA for networking engineers is three courses and one exam which covers the fundamental topics for all network technologies. The new CCNA focuses on IP foundation and security topics along with wireless, virtualization, automation, and network programmability.

There are new DevNet certifications at the associate, specialist and professional levels, to validate your software development skills.

There are specialist certification options to validate your skills in line with your job role and interests. This includes the Cisco Enterprise Advanced Infrastructure Specialist certification.

You can start where you want. There are no prerequisites to start earning your associate, specialist, professional, or expert level certification. Continuing education credits for recertification and ongoing development are now available for CCNA.

Networking Jobs

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 new program, the Talent Bridge Matching Engine. Search for jobs with Cisco, as well as Cisco partners and distributors seeking Cisco Networking Academy students and alumni.

You can also search for IT jobs using online search engines such as Indeed, Glassdoor, and Monster. Use search terms such as IT, network administrator, network architects, and computer systems administrator. You can also search using the term Cisco CCNA.

Operating Systems

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

There are three concentric circles that appear to radiate from the monitor of a computer labeled user interface. They show the relationship between the different portions of an operating system. The inner circle labeled hardware shows examples of computer hardware, the middle circle is labeled kernel, and the outer circle is labeled shell. Text at the bottom reads: 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.

ShellKernelHardwareUser Interface

- **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.

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

```
analyst@secOps ~]$ ls
```

```
Desktop Downloads lab.support.files second_drive
```

```
[analyst@secOps ~]$
```

2.1.2

GUI

A GUI such as Windows, macOS, Linux KDE, Apple iOS, or Android allows the user to interact with the system using an environment of graphical icons, menus, and windows. The GUI example in the figure is more user-friendly and requires less knowledge of the underlying command structure that controls the system. For this reason, most users rely on GUI environments.



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

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.

2.1.3

Purpose of an OS

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

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

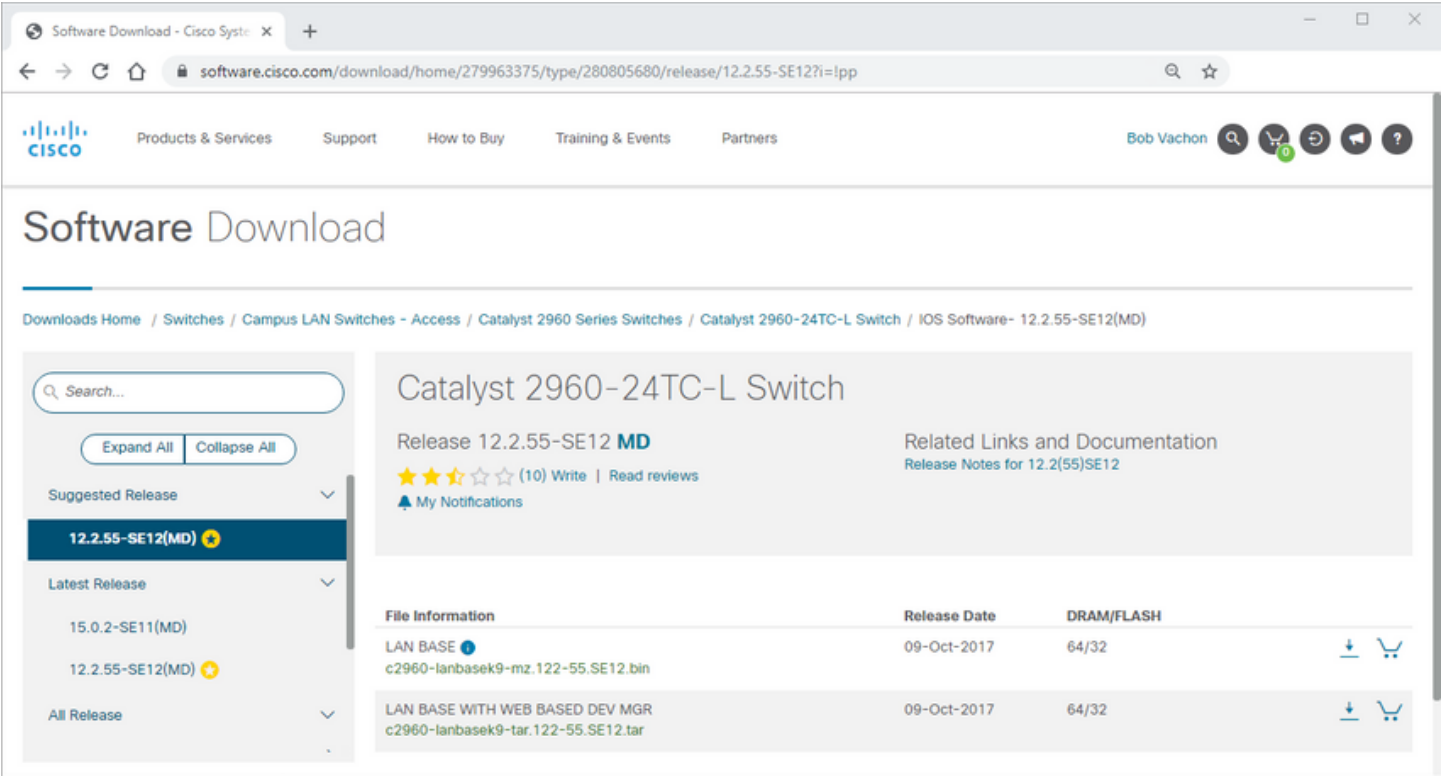
A CLI-based network operating system (e.g., the Cisco IOS on a switch or router) enables a network technician to do the following:

- Use a keyboard to run CLI-based network programs
- Use a keyboard to enter text and text-based commands
- View output on a monitor

Cisco networking devices run particular versions of the Cisco IOS. The IOS version is dependent on the type of device being used and the required features. While all devices come with a default IOS and feature set, it is possible to upgrade the IOS version or feature set to obtain additional capabilities.

The figure displays a list of IOS software releases for a Cisco Catalyst 2960 Switch.

Cisco Software Download Example



2.1.4

Access Methods

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

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

Table caption	
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

Table caption	
Method	Description
	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.

2.1.5

Terminal Emulation Programs

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

2.2.1

Primary Command Modes

In the previous topic, you learned that all network devices require an OS and that they can be configured using the CLI or a GUI. Using the CLI may provide the network administrator with more precise control and flexibility than using the GUI. This topic discusses using CLI to navigate the Cisco IOS.

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

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

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

Table caption		
Command Mode	Description	Default Prompt
User Exec Mode	<ul style="list-style-type: none">Mode allows access to only a limited number of basic monitoring commands.It is often referred to as “view-only” mode.	Switch> Router>
Privileged EXEC Mode	<ul style="list-style-type: none">Mode allows access to all commands and features.The user can use any monitoring commands and execute configuration and management commands.	Switch# Router#

2.2.2

Configuration Mode and Subconfiguration Modes

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

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

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

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

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

2.2.3

Video - IOS CLI Primary Command Modes

Click Play in the figure to view a video demonstration of navigating between IOS modes.

Play Video

2.2.4

Navigate Between IOS Modes

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

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

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

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

```
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)#
```

2.3.1

Basic IOS Command Structure

This topic covers the basic structure of commands for the Cisco IOS. A network administrator must know the basic IOS command structure to be able to use the CLI for device configuration.

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

The diagram shows the general syntax for a switch command (which is prompt, command, space, and keyword or argument) and provides two examples. In the first example, the prompt is Switch>, the command is show, a space follows, and the keywords are ip protocols. In the second example, the prompt is Switch>, the command is ping, a space follows, and the argument is 192 dot 168 dot 10 dot 5.

```
Switch>show ip protocolsSwitch>ping 192.168.10.5
```

Prompt	Command	Space	Keyword(s) or Argument(s)
--------	---------	-------	---------------------------

- **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**).

After entering each complete command, including any keywords and arguments, press the **Enter** key to submit the command to the command interpreter.

2.3.2

IOS Command Syntax Check

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

As identified in the table, boldface text indicates commands and keywords that are entered as shown. Italic text indicates an argument for which the user provides the value.

Table caption	
Convention	Description
boldface	Boldface text indicates commands and keywords that you enter literally as shown.
<i>italics</i>	Italic text indicates arguments for which you supply values.
[x]	Square brackets indicate an optional element (keyword or argument).
{x}	Braces indicate a required element (keyword or argument).

Table caption	
Convention	Description
[x {y z }]	Braces and vertical lines within square brackets indicate a required choice within an optional element. Spaces are used to delineate parts of the command.

For instance, the syntax for using the **description** command is **description** *string*. The argument is a *string* value provided by the user. The **description** command is typically used to identify the purpose of an interface. For example, entering the command, **description Connects to the main headquarter office switch**, describes where the other device is at the end of the connection.

The following examples demonstrate conventions used to document and use IOS commands:

- **ping** *ip-address* - The command is **ping** and the user-defined argument is the *ip-address* of the destination device. For example, **ping 10.10.10.5**.
- **traceroute** *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**.

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}}
```

The command will typically be followed with a detailed description of the command and each argument.

The Cisco IOS Command Reference is the ultimate source of information for a particular IOS command.

2.3.3

IOS Help Features

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

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

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

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

Command syntax check verifies that a valid command was entered by the user. When a command is entered, the command line interpreter evaluates the command from left to right. If the interpreter understands the command, the requested action is executed, and the CLI returns to the appropriate prompt. However, if the interpreter cannot understand the command being entered, it will provide feedback describing what is wrong with the command.

2.3.4

Video - Context Sensitive Help and Command Syntax Check

Click Play in the figure to view a video demonstration of context-sensitive help and command syntax check.

Play Video

2.3.5

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**. An even shorter version, **con**, will not work because more than one command begins with **con**. Keywords can also be shortened.

The table lists keystrokes to enhance command line editing.

Table caption	
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 Arrowor 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 Arrowor Ctrl+F	Moves the cursor one character to the right.
Ctrl+E	Moves the cursor to the end of command line.
Up Arrowor Ctrl+P	Recalls the previous command in the history buffer, beginning with the most recent command.
Down Arrowor 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.

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

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

Table caption	
Keystroke	Description
Enter Key	Displays the next line.
Space Bar	Displays the next screen.
Any other key *	Ends the display string, returning to previous prompt. * Except "y", which answers "yes" to the --More-- prompt, and acts like the Space bar

This table lists commands used to exit out of an operation.

Table caption	
Keystroke	Description
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.

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

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

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

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

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

The diagram shows three interconnected switches spanning three floors. The top switch is named Sw-Floor-3, the middle switch is named Sw-Floor-2, and the bottom switch is name Sw-Floor-1. A user sitting at a host PC is connected to the Sw-Floor-1 switch. Text at bottom reads: when network devices are named, they are easy to identify for configuration purposes.

Sw-Floor-3Sw-Floor-2Sw-Floor-1
When network devices are named, they are easy to identify for configuration purposes.

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

```
Switch# configure terminal
```

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

```
Sw-Floor-1(config)#
```

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

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

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

2.4.2

Password Guidelines

The use of weak or easily guessed passwords continues to be the biggest security concern of organizations. Network devices, including home wireless routers, 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.

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

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

- Use passwords that are more than eight characters in length.

- Use a combination of upper and lowercase letters, numbers, special characters, and/or numeric sequences.
- Avoid using the same password for all devices.
- Do not use common words because they are easily guessed.

Use an internet search to find a password generator. Many will allow you to set the length, character set, and other parameters.

Note: Most of the labs in this course use simple passwords such as **cisco** or **class**. These passwords are considered weak and easily guessable and should be avoided in production environments. We only use these passwords for convenience in a classroom setting, or to illustrate configuration examples.

2.4.3

Configure Passwords

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

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

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

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

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

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

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

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

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

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

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# line vty 0 15
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# login
Sw-Floor-1(config-line)# end
```

```
Sw-Floor-1#
```

2.4.4

Encrypt Passwords

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

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

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# service password-encryption
Sw-Floor-1(config)#
```

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

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

```
Sw-Floor-1(config)# end
Sw-Floor-1# show running-config
!
(Output omitted)
!
line con 0
password 7 094F471A1A0A
login
!
line vty 0 4
password 7 094F471A1A0A
login
line vty 5 15
password 7 094F471A1A0A
login
!
!
end
```

2.4.5

Banner Messages

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

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

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

```
Sw-Floor-1# configure terminal
```

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

2.4.6

Video - Secure Administrative Access to a Switch

Click Play in the figure to view a video demonstration of how to secure administrative access to a switch.

Play Video

2.4.7

Syntax Checker - Basic Device Configuration

Secure management access to a switch.

- Assign a device name.
- Secure user EXEC mode access.
- Secure privileged EXEC mode access.
- Secure VTY access.
- Encrypt all plaintext passwords.
- Display a login banner.

```
Enter global configuration mode.

Switch#
```

2.5.1

Configuration Files

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

There are two system files that store the device configuration:

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

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

```
Sw-Floor-1# show running-config
```

```
Building configuration...
```

```
Current configuration : 1351 bytes
```

```
!
```

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

```
!
```

```
version 15.0
```

```
no service pad
```

```
service timestamps debug datetime msec
```

```
service timestamps log datetime msec
```

```
service password-encryption
```

```
!
```

```
hostname Sw-Floor-1
```

```
!
```

```
(output omitted)
```

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

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

2.5.2

Alter the Running Configuration

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

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

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

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

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

2.5.3

Video - Alter the Running Configuration

Click Play in the figure to view a video demonstration on how to save switch configuration files.

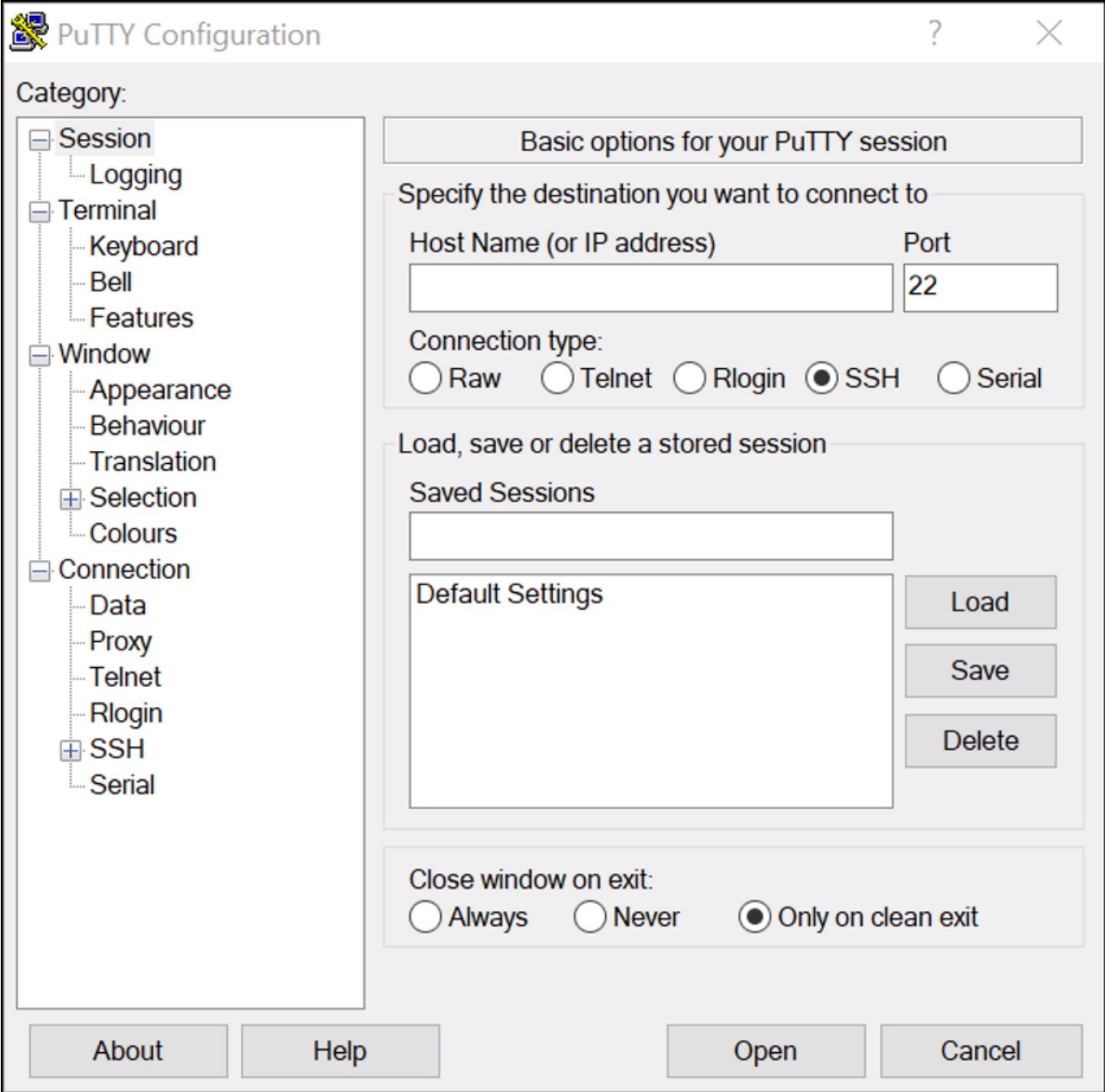
Play Video

Capture Configuration to a Text File

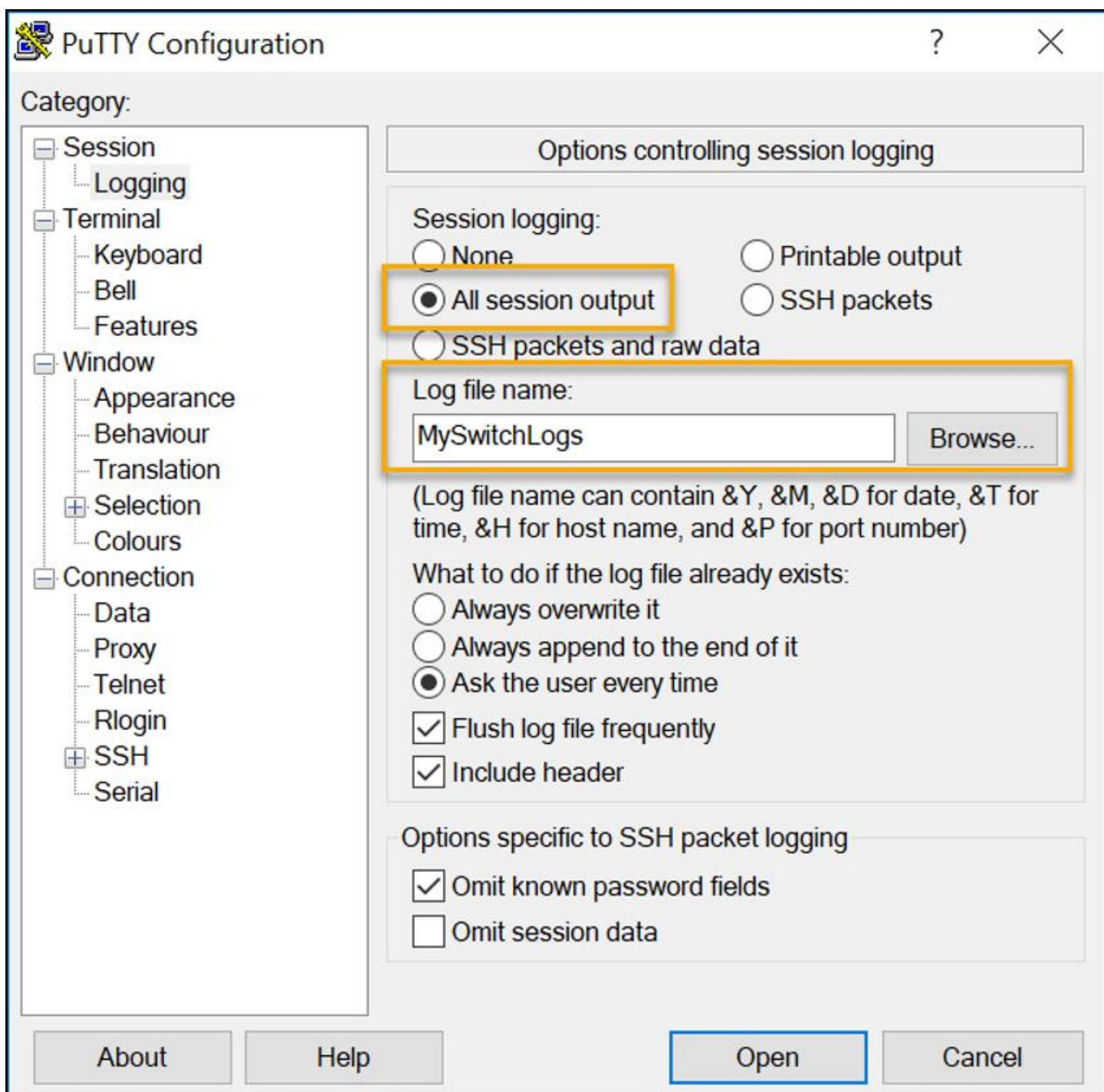
Configuration files can also be saved and archived to a text document. This sequence of steps ensures that a working copy of the configuration file is available for editing or reuse later.

For example, assume that a switch has been configured, and the running config has been saved on the device.

Step 1. Open terminal emulation software, such as PuTTY or Tera Term, that is already connected to a switch.



Step 2. Enable logging in 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).



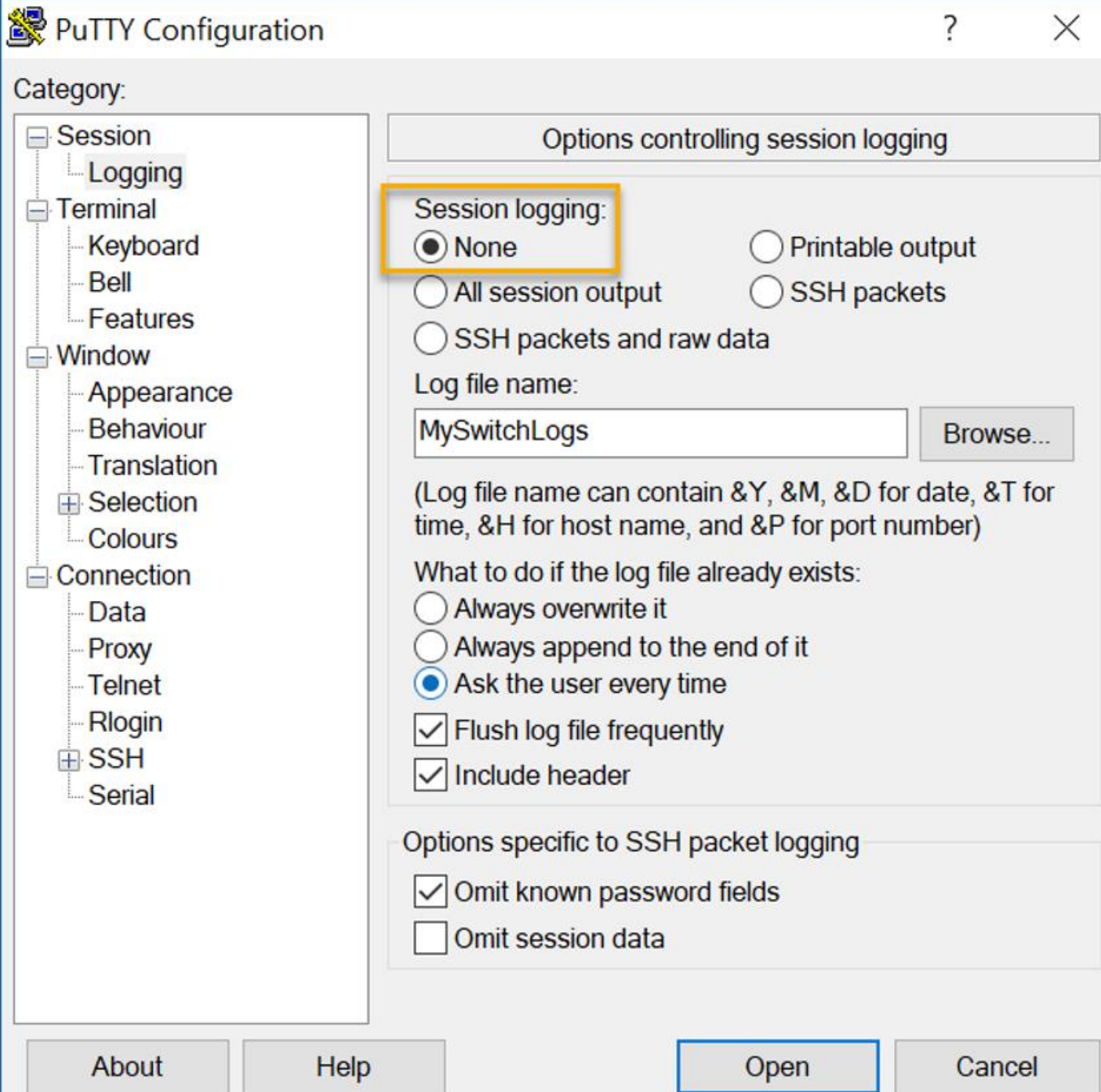
Step 3. Execute the **show running-config** or **show startup-config** command at the privileged EXEC prompt. Text displayed in the terminal window will be placed into the chosen file.

```
Sw-Floor-1# show running-config
```

```
Building configuration...
```

```
(output omitted)
```

Step 4. Disable logging in the terminal software. The figure shows how to disable logging by choosing the **None** session logging option.



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.

To restore a configuration file to a device:

Step 1. Enter global configuration mode on the device.

Step 2. Copy and paste the text file into the terminal window connected to the switch.

The text in the file will be applied as commands in the CLI and become the running configuration on the device. This is a convenient method of manually configuring a device.

2.6.1

IP Addresses

Congratulations, you have performed a basic device configuration! Of course, the fun is not over yet. If you want your end devices to communicate with each other, you must ensure that each of them has an appropriate IP address and is correctly connected. You will learn about IP addresses, device ports and the media used to connect devices in this topic.

The use of IP addresses is the primary means of enabling 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. Examples of end devices include these:

- Computers (work stations, laptops, file servers, web servers)
- Network printers
- VoIP phones
- Security cameras
- Smart phones
- Mobile handheld devices (such as wireless barcode scanners)

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.

Note: IP in this course refers to both the IPv4 and IPv6 protocols. IPv6 is the most recent version of IP and is replacing the more common IPv4.

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.

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address: 192 . 168 . 1 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 1 . 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

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

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

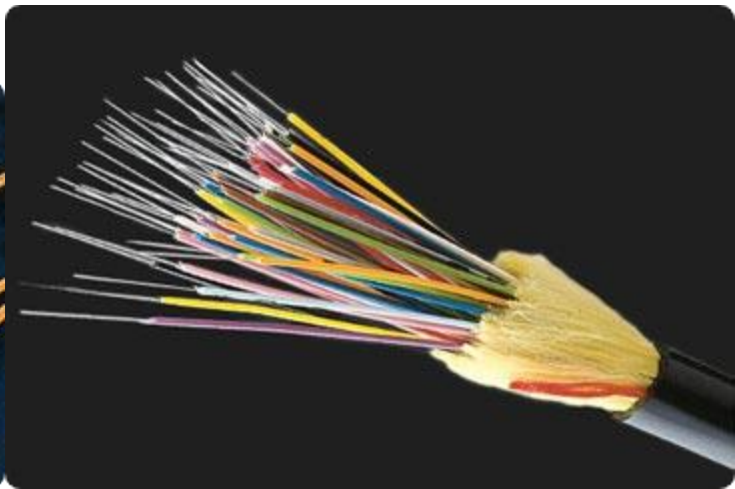
Cancel

2.6.2

Interfaces and Ports

Network communications depend on end user device interfaces, networking device interfaces, and the cables that connect them. Each physical interface has specifications, or standards, that define it. A cable connecting to the interface must be designed to match the physical standards of the interface. Types of network media include twisted-pair copper cables, fiber-optic cables, coaxial cables, or wireless, as shown in the figure.

A stack of six black network switches or routers, each with multiple ports and status lights. Below the stack, there are several network cables: a bundle of colorful Ethernet cables (red, blue, green, yellow) and a bundle of fiber-optic cables with multiple colored strands.



CopperWirelessFiber-optics

Different types of network media have different features and benefits. Not all network media have the same characteristics. Not all media are appropriate for the same purpose. These are some of the differences between various types of media:

- Distance the media can successfully carry a signal
- Environment in which the media is to be installed
- Amount of data and the speed at which it must be transmitted
- Cost of the media and installation

Not only does each link on the internet require a specific network media type, but each link also requires a particular network technology. For example, Ethernet is the most common local-area network (LAN) technology used today. Ethernet ports are found on end-user devices, switch devices, and other networking devices that can physically connect to the network using a cable.

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.

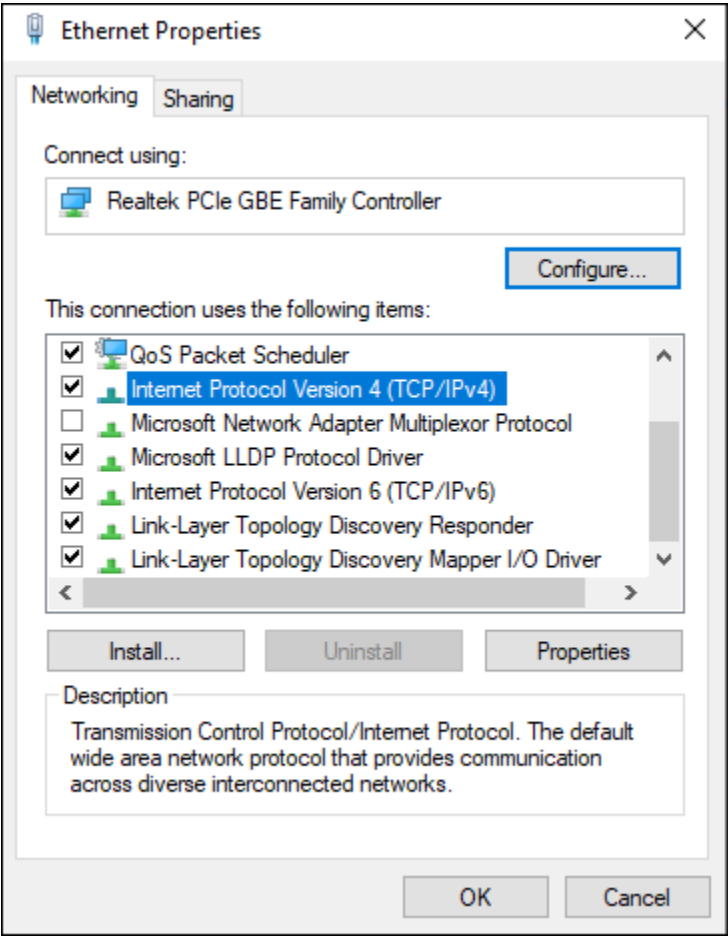
Note: A Layer 2 switch does not need an IP address. The IP address assigned to the SVI is used to remotely access the switch. An IP address is not necessary for the switch to perform its operations.

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.

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address:

192 . 168 . 1 . 10

Subnet mask:

255 . 255 . 255 . 0

Default gateway:

192 . 168 . 1 . 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

Note: The DNS server addresses are the IPv4 and IPv6 addresses of the Domain Name System (DNS) servers, which are used to translate IP addresses to domain names, such as www.cisco.com.

2.7.2

Automatic IP Address Configuration for End Devices

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.

In a network, DHCP enables automatic IPv4 address configuration for every end device that is DHCP-enabled. Imagine the amount of time it would take if every time you connected to the network, you had to manually enter the IPv4 address, the subnet mask, the default gateway, and the DNS server. Multiply that by every user and every device in an organization and you see the problem. Manual configuration also increases the chance of misconfiguration by duplicating another device's IPv4 address.

As shown in the figure, to configure DHCP on a Windows PC, you only need to select **Obtain an IP address automatically** and **Obtain DNS server address automatically**. Your PC will search out a DHCP server and be assigned the address settings necessary to communicate on the network.

Note: IPv6 uses DHCPv6 and SLAAC (Stateless Address Autoconfiguration) for dynamic address allocation.



2.7.3

Syntax Checker - Verify Windows PC IP Configuration

It is possible to display the IP configuration settings on a Windows PC by using the **ipconfig** command at the command prompt. The output will show the IPv4 address, subnet mask, and gateway information received from the DHCP server.

Enter the command to display the IP configuration on a Windows PC.

Enter the command to display the IP configuration on a Windows PC.

```
C:\> ipconfig /all
```

2.7.4

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
```

2.7.5

Syntax Checker - Configure a Switch Virtual Interface

Enter interface configuration mode for VLAN 1.

```
Switch(config)#
```

3.1.1

Video - Devices in a Bubble

Click Play in the figure to view a video explaining how a network device operates within a network.

Play Video

3.1.2

Communications Fundamentals

Networks vary in size, shape, and function. They can be as complex as devices connected across the internet, or as simple as two computers directly connected to one another with a single cable, and anything in-between. However, simply having a wired or wireless physical connection between end devices is not enough to enable communication. For communication to occur, devices must know “how” to communicate.

People exchange ideas using many different communication methods. However, all communication methods have the following three elements in common:

- **Message source (sender)** - Message sources are people, or electronic devices, that need to send a message to other individuals or devices.
- **Message Destination (receiver)** - The destination receives the message and interprets it.
- **Channel** - This consists of the media that provides the pathway over which the message travels from source to destination.

3.1.3

Communication Protocols

Sending a message, whether by face-to-face communication or over a network, is governed by rules called protocols. These protocols are specific to the type of communication method being used. In our day-to-day personal communication, the rules we use to communicate over one medium, like a telephone call, are not necessarily the same as the rules for using another medium, such as sending a letter.

The process of sending a letter is similar to communication that occurs in computer networks.

Click each button for an analogy and a network example of the communication process.

Analogy
Network

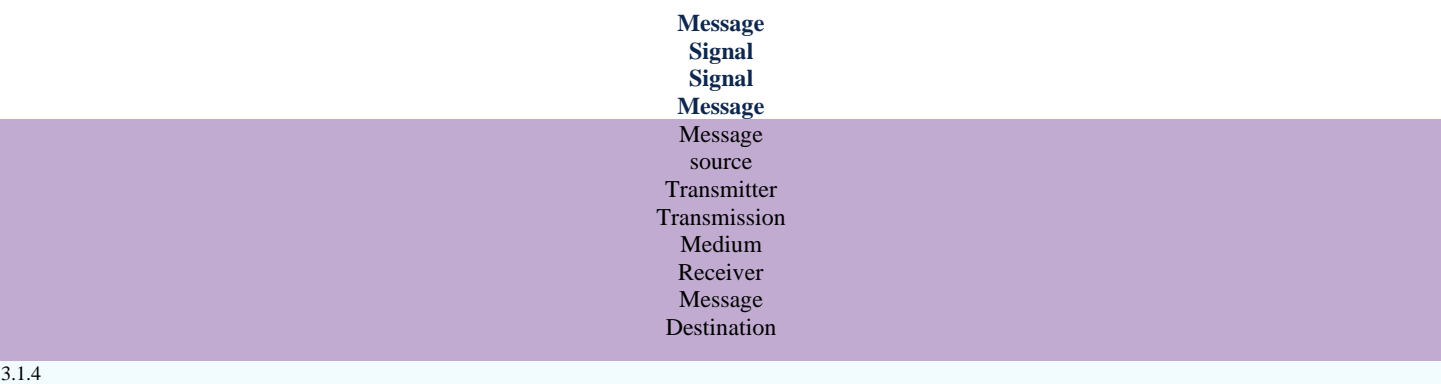
Analogy

Click Play in the figure to view an animation of two people communicating face-to-face.

Prior to communicating, they must agree on how to communicate. If the communication is using voice, they must first agree on the language. Next, when they have a message to share, they must be able to format that message in a way that is understandable.

If someone uses the English language, but poor sentence structure, the message can easily be misunderstood. Each of these tasks describe protocols that are used to accomplish communication.

The figure is an animated representation of communication between a female and a male. Up top are words with right arrows between them: message, message source signal transmitter transmission medium signal receiver, and message, message destination. The animation shows a lightbulb appearing above the female traveling to the male and a lightbulb appear above his head.



3.1.4

Rule Establishment

Before communicating with one another, individuals must use established rules or agreements to govern the conversation. Consider this message for example:

humans communication between govern rules. It is verydifficult tounderstand messages

that are not correctly formatted and donot follow the established rules and protocols.

A estrutura da gramatica, da lingua, da pontuacao e do sentence faz a configuracao

humana compreensivel por muitos individuos diferentes.

Notice how it is difficult to read the message because it is not formatted properly. It should be written using rules (i.e., protocols) that are necessary for effective communication. The example shows the message which is now properly formatted for language and grammar.

Rules govern communication between humans. It is very difficult to understand messages

that are not correctly formatted and do not follow the established rules and protocols.

The structure of the grammar, the language, the punctuation and the sentence make the

configuration humanly understandable for many different individuals.

Protocols must account for the following requirements to successfully deliver a message that is understood by the receiver:

- An identified sender and receiver
- Common language and grammar
- Speed and timing of delivery
- Confirmation or acknowledgment requirements

3.1.5

Network Protocol Requirements

The protocols that are used in network communications share many of these fundamental traits. In addition to identifying the source and destination, computer and network protocols define the details of how a message is transmitted across a network. Common computer protocols include the following requirements:

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

3.1.6

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.

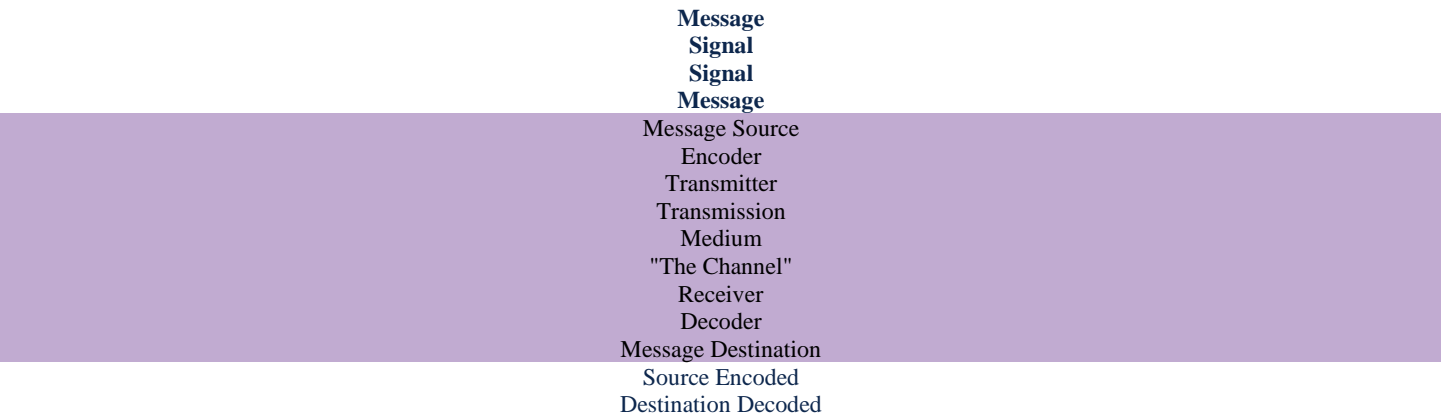
Click each button for an analogy and a network example of message encoding.

Analogy
Network

Analogy

Imagine a person calls a friend to discuss the details of a beautiful sunset. Click Play in the figure to view an animation of message encoding.

To communicate the message, she converts her thoughts into an agreed upon language. She then speaks the words using the sounds and inflections of spoken language that convey the message. Her friend listens to the description and decodes the sounds to understand the message he received.



3.1.7

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.

Click each button for an analogy and a network example of message formatting and encapsulation.

Analogy
Network

Analogy

A common example of requiring the correct format in human communications is when sending a letter. Click Play in the figure to view an animation of formatting and encapsulating a letter.

An envelope has the address of the sender and receiver, each located at the proper place on the envelope. If the destination address and formatting are not correct, the letter is not delivered.

The process of placing one message format (the letter) inside another message format (the envelope) is called encapsulation. De-encapsulation occurs when the process is reversed by the recipient and the letter is removed from the envelope.

The animation shows an envelope with a stamp, a sender of 4085 SE Pine Street, Ocala, Florida 34471 and a recipient at 1400 Main Street, Canton, Ohio 44203. The envelope opens and shows a letter: dear Jane, I just returned from my trip. I thought you might like to see my pictures. John. A breakout table appears with the following headings: Recipient (destination) location address, sender (source) location address, salutation (start of message indicator), recipient (destination) identifier, content of letter (encapsulated data) sender (source) identifier, end of frame (end of message indicator). The next row has envelope addressing under the first 2 sections, then encapsulated letter under the next 4 sections. The 1400 Main Street Canton, Ohio 44203 goes in a new row under the recipient (destination) and envelope addressing sections. The 4085 SE Pine Street Ocala, Florida 34471 goes under the sender (source) and envelope addressing sections. The dear goes under the salutation (start of message indicator) and encapsulated letter sections. The Jane goes under the recipient (destination) identifier and encapsulated letter sections. The words I just returned from my trip. I thought you might like to see my pictures. Goes under the content of letter (encapsulated data) and encapsulated letter sections. The word John goes under the sender (source) identifier and encapsulated letter sections. The stamp on the letter goes under the end of frame (end of message indicator) section.

Recipient (destination) Location address	
Sender (source) Location address	
Salutation (start of message indicator)	
Recipient (destination) identifier	
Content of Letter (encapsulated data)	
Sender (source) identifier	
End of Frame (End of message indicator)	
Envelope Addressing	
Encapsulated Letter	
Sender	
4085 SE Pine Street	
Ocala, Florida 34471	
Recipient	
1400 Main Street	
Canton, Ohio 44203	
4085 SE Pine Street	
Ocala, Florida 34471	
4085 SE Pine Street	
Ocala, Florida 34471	
1400 Main Street	
Canton, Ohio 44203	
1400 Main Street	
Canton, Ohio 44203	
Dear Jane,	
I just returned from my trip. I thought you might like to see my pictures.	
John	
Dear	
Jane	
I just returned from my trip. I thought you might like to see my pictures.	
John	
Dear	
Jane	
I just returned from my trip. I thought you might like to see my pictures.	
John	

3.1.8

Message Size

Another rule of communication is message size.

Click each button for an analogy and a network example of message size.

Analogy
Network

Analogy

Click Play in the figure to view an animation of message size in face-to-face communications.

When people communicate with each other, the messages that they send are usually broken into smaller parts or sentences. These sentences are limited in size to what the receiving person can process at one time, as shown in the figure. It also makes it easier for the receiver to read and comprehend.

3.1.9

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.

The animation shows a woman and a man speaking at the same time. The woman says What time is the movie? and the man says When are we meeting for dinner?. Because they spoke simultaneously, neither understood the other and they both say Sorry? I did not understand you.

3.1.10

Message Delivery Options

A message can be delivered in different ways.

Click each button for an analogy and a network example of message delivery options.

Analogy
Network

Analogy

Sometimes, a person wants to communicate information to a single individual. At other times, the person may need to send information to a group of people at the same time, or even to all people in the same area.

Click the unicast, multicast, and broadcast buttons in the figure for an example of each.

Unicast
Multicast
Broadcast
Source

3.1.11

A Note About the Node Icon

Networking documents and topologies often represent networking and end devices using a node icon. Nodes are typically represented as a circle. The figure shows a comparison of the three different delivery options using node icons instead of computer icons.

The figure uses circles representing network nodes to illustrate the three different message delivery options. There are three topologies shown from left to right. The topology on the left depicts a unicast message and consists of one red node, one green node, and four yellow nodes. It has an arrow from the red node leading to the green node. The middle topology depicts a multicast message and consists of one red node, three green nodes, and two yellow nodes. It has an arrow from the red node leading to each of the green nodes. The topology on the right depicts a broadcast. It has one red node and five green nodes. It has an arrow from the red node leading to each of the green nodes.

3.2.1

Network Protocol Overview

You know that for end devices to be able to communicate over a network, each device must abide by the same set of rules. These rules are called protocols and they have many functions in a network. This topic gives you a overview of network protocols.

Network protocols define a common format and set of rules for exchanging messages between devices. Protocols are implemented by end devices and intermediary devices in software, hardware, or both. Each network protocol has its own function, format, and rules for communications.

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

Table caption	
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 security 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.

3.2.2

Network Protocol Functions

Network communication protocols are responsible for a variety of functions necessary for network communications between end devices. For example, in the figure how does the computer send a message, across several network devices, to the server?

The figure shows how the protocol IPv4 can be used to send a message from a computer across a network to a server. In the center of the figure are three routers connected together in a triangle. The router on the left is connected to a computer. The router on the right is connected to a server. A message below the computer reads: I will send this message across the network using an IPv4 header. A message below the attached router reads: I can forward this message because I understand the IPv4 header. A message below the server reads: I can accept this message because I understand IPv4.

I will send this message across the network using an IPv4 header.I can forward this message because I understand the IPv4 header.I can accept this message because I understand IPv4.

Computers and network devices use agreed-upon protocols to communicate. The table lists the functions of these protocols.

Table caption	
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 sequence 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.

3.2.3

Protocol Interaction

A message sent over a computer network typically requires the use of several protocols, each one with its own functions and format. The figure shows some common network protocols that are used when a device sends a request to a web server for its web page.

A small network diagram shows, from left to right, a laptop connected to the Internet cloud which is connected to a server. An envelope is crossing the connection between the laptop and the cloud. Below the envelope are a list of

protocols used when a device sends a request to a web server for a web page. Text at the bottom of the figure describes these protocols and reads: Hypertext Transfer Protocol (H T T P) - This protocol governs the way a web server and a web client interact. H T T P 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 H T T P as part of the application. H T T P relies on other protocols to govern how the messages are transported between the client and server. Transmission Control Protocol (T C P) - This protocol manages the individual conversations. T C P is responsible for guaranteeing the reliable delivery of the information and managing flow control between the end devices. Internet Protocol (I P) - This protocol is responsible for delivering messages from the sender to the receiver. I P 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).

Internet
The protocols in the figure are described as follows:

- **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).

3.3.1

Network Protocol Suites

In many cases, protocols must be able to work with other protocols so that your online experience gives you everything you need for network communications. Protocol suites are designed to work with each other seamlessly.

A protocol suite is a group of inter-related protocols necessary to perform a communication function.

One of the best ways to visualize how the protocols within a suite interact is to view the interaction as a stack. A protocol stack shows how the individual protocols within a suite are implemented. The protocols are viewed in terms of layers, with each higher-level service depending on the functionality defined by the protocols shown in the lower levels. The lower layers of the stack are concerned with moving data over the network and providing services to the upper layers, which are focused on the content of the message being sent.

As illustrated in the figure, we can use layers to describe the activity occurring in face-to-face communication. At the bottom is the physical layer where we have two people with voices saying words out loud. In the middle is the rules layer that stipulates the requirements of communication including that a common language must be chosen. At the top is the content layer and this is where the content of the communication is actually spoken.

The figure shows three different layers used to describe what occurs during face-to-face communications. The bottom layer, labeled physical layer, shows two people exchanging a message. The middle layer, labeled rules layer, lists the conversation protocol suite to be used including: use a common language; wait your turn; and signal when finished. The top layer is labeled content layer and includes the message: Where is the cafe? Text at the bottom reads: Protocol suites are sets of rules that work together to help solve a problem.

Where is the café? Content LayerRules LayerPhysical LayerConversation protocol suite

1. Use a common language
2. Wait your turn
3. Signal when finished

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

3.3.2

Evolution of Protocol Suites

A protocol suite is a set of protocols that work together to provide comprehensive network communication services. Since the 1970s there have been several different protocol suites, some developed by a standards organization and others developed by various vendors.

During the evolution of network communications and the internet there were several competing protocol suites, as shown in the figure.

The figure is a table with text underneath. The table consists of four rows and five columns. The first column header is TCP/IP layer name and reads top to bottom: Application, Transport, Internet, and Network Access. The second column header is TCP/IP. Application protocols are HTTP, DNS, DHCP, and FTP. Transport protocols are TCP and UDP. Internet protocols are IPv4, IPv6, ICMPv4, and ICMPv6. The network access protocols are Ethernet, ARP, and WLAN. The third column header is ISO. Application protocols are ACSE, ROSE, TRSE, and SESE. Transport protocols are TP0, TP1, TP2, TP3, and TP4. Internet protocols are CONP/CMNS and CLNP/CLNS. Network access protocols are Ethernet, ARP, and WLAN. The fourth column header is AppleTalk. Application protocol is AFP. Transport protocols are ATP, AEP, NBP, and RTMP. Internet protocols are AARP. Network access protocols are Ethernet, ARP, and WLAN. The fifth column header is Novell Netware. Application protocol is NDS. Transport protocol is SPX. Internet protocols is IPX. Network Access protocols are Etherent, ARP, and WLAN. Text below the table reads: 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.

TCP/IPISOAppleTalkNovell
Netware

TCP/IP Layer NameApplicationTransportInternetNetwork Access

- **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.

3.3.3

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.

Server	Protocol Stack	Layer Name	Application	Transport	Internet	Network Access	Internet	Web
3.3.4								

TCP/IP Protocol Suite

Today, the TCP/IP protocol suite includes many protocols and continues to evolve to support new services. Some of the more popular ones are shown in the figure.

The figure shows the TCP/IP layers and associated protocols. At the application layer: DNS is a name system protocol; DHCPv4, DHCPv6, and SLAAC are host config protocols; SMTP, POP3, and IMAP are email protocols; FTP, SFTP, and TFTP are file transfer protocols; and HTTP, HTTPS, and REST are web and web service protocols. At the transport layer: TCP is a connection-oriented protocol and UDP is a connectionless protocol. At the internet layer: IPv4, IPv6, and NAT are Internet protocols; ICMPv4, ICMPv6, and ICMPv6 ND are messaging protocols; and OSPF, EIGRP, and BGP are routing protocols. At the network access layer: ARP is an address resolution protocol; and Ethernet and WLAN are data link protocols. Text at the bottom reads: 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.

TCP/IP Layers	Application Layer	Name	System	Host	Config	Email	File	Transfer	Web and	Web Service	Transport Layer	Connection-Oriented	Connectionless	Internet Layer	Internet Protocol	Messaging	Routing	Protocols	Network Access		
Layer	Address	Resolution	Data	Link	Protocols	TCP/IP															
Protocols	DNS	DHCPv4	DHCPv6	SLAAC	SMTP	POP3	IMAP	FTP	SFTP	TFTP	HTTP	HTTPS	REST	TCP	UDP	IPv4	IPv6	NAT	ICMPv4	ICMPv6	ICMPv6
	ND	OSPF	EIGRP	BGP	ARP	Ethernet	WLAN														

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.

Click each button for a brief description of protocols at each layer.

- Application Layer
- Transport layer
- Internet Layer
- Network Access Layer

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.

3.3.5

TCP/IP Communication Process

The animations in the figures demonstrate the complete communication process using an example of a web server transmitting data to a client.

Click the Play in the figure to view an animation of a web server encapsulating and sending a web page to a client.

The animation shows a small network with a Web Server and a Web Client. There is a graphic that shows the components that make up a message. An Ethernet Frame, and IP Packet, a TCP segment, and the user data. The animation begins with the web server preparing the Hypertext Markup Language (HTML) page as data to be sent. The application protocol HTTP header is added (prepended) to the front of the HTML data. The header contains various information, including the HTTP version the server is using and a status code indicating it has information for the web client. The HTTP application layer protocol delivers the HTML-formatted web page data to the TCP transport layer. The transport layer protocol prepends additional information to the HTTP data to manage the exchange of information between the web server and web client. The IP information is prepended to the TCP information. IP assigns the appropriate source and destination IP addresses. This information is known as an IP packet. The Ethernet protocol prepends and adds to the end (appends) information to the IP packet to create a data link frame. The frame is then converted into a string of binary bits that are sent along the network path to the web client.



Click the Play in the next figure to view an animation of the client receiving, and de-encapsulating the web page for display in the web browser.

The animation shows a small network with a Server and a Client. The client receives a string of binary bits from the server. The client takes the binary string of bits and converts it into an Ethernet frame. The Frame contains the Ethernet header, the IP packet, the TCP segment, and the data. Each protocol header is processed and then removed in the opposite order it was added. The Ethernet information is processed and removed, followed by the IP protocol information, the TCP information, and finally the HTTP information. The HTML web page information is then passed on to the web browser software of the client.

3.4.1

Open Standards

When buying new tires for a car, there are many manufacturers you might choose. Each of them will have at least one type of tire that fits your car. That is because the automotive industry uses standards when they make cars. It is the same with protocols. Because there are many different manufacturers of network components, they must all use the same standards. In networking, standards are developed by international standards organizations.

Open standards encourage interoperability, competition, and innovation. They also guarantee that the product of no single company can monopolize the market or have an unfair advantage over its competition.

A good example of this is when purchasing a wireless router for the home. There are many different choices available from a variety of vendors, all of which incorporate standard protocols such as IPv4, IPv6, DHCP, SLAAC, Ethernet, and 802.11 Wireless LAN. These open standards also allow a client running the Apple OS X operating system to download a web page from a web server running the Linux operating system. This is because both operating systems implement the open standard protocols, such as those in the TCP/IP protocol suite.

Standards organizations are usually vendor-neutral, non-profit organizations established to develop and promote the concept of open standards. These organizations are important in maintaining an open internet with freely accessible specifications and protocols that can be implemented by any vendor.

A standards organization may draft a set of rules entirely on its own or, in other cases, may select a proprietary protocol as the basis for the standard. If a proprietary protocol is used, it usually involves the vendor who created the protocol.

The figure shows the logo for each standards organization.

logos for standards organizations including IEEE, IETF, IANA, ICANN, ITU, and TIA



3.4.2

Internet Standards

Various organizations have different responsibilities for promoting and creating standards for the internet and TCP/IP protocol.

The figure displays standards organizations involved with the development and support of the internet.

The figure shows standards organizations involved with the development and support of the internet. At the top of the figure is the Internet Society (ISOC) logo. A line underneath connects to the Internet Architecture Board (IAB) logo. Underneath and to the left is the Internet Engineering Task Force (IETF) and to the right is the Internet Research Task Force (IRTF). Below the IETF is the Internet Engineering Steering Group (IESG) and below that are working group #1 and working group #2. Below the IRTF is the Internet Research Steering Group (IRSG) and below that are research group #1 and research group #2. Text at the bottom reads: Internet Society (ISOC) - Responsible for promoting the open development and evolution of internet use throughout the world. Internet Architecture Board (IAB) - Responsible for the overall management and development of internet standards. Internet Engineering Task Force (IETF) - Develops, updates, and maintains internet and TCP/IP technologies. This includes the process and documents for developing new protocols and updating existing protocols, which are known as Request for Comments (RFC) documents. Internet Research Task Force (IRTF) - Focused on long-term research related to internet and TCP/IP protocols such as Anti-Spam Research Group (ASRG), Crypto Forum Research Group (CFRG), and Peer-to-Peer Research Group (P2PRG).



Internet Society (ISOC) Internet Architecture Board (IAB) Internet Engineering Task Force (IETF) Internet Engineering Steering Group (IESG) Internet Research Task Force (IRTF) Internet Research Steering Group (IRSG) Working Group #1 Working Group #2 Research

- **Internet Society (ISOC)** - Responsible for promoting the open development and evolution of internet use throughout the world.
- **Internet Architecture Board (IAB)** - Responsible for the overall management and development of internet standards.
- **Internet Engineering Task Force (IETF)** - Develops, updates, and maintains internet and TCP/IP technologies. This includes the process and documents for developing new protocols and updating existing protocols, which are known as Request for Comments (RFC) documents.
- **Internet Research Task Force (IRTF)** - Focused on long-term research related to internet and TCP/IP protocols such as Anti-Spam Research Group (ASRG), Crypto Forum Research Group (CFRG), and Peer-to-Peer Research Group (P2PRG).

The next figure displays standards organizations involved with the development and support of TCP/IP and include IANA and ICANN.

The figure shows the standards organizations involved with the development and support of TCP/IP. Image shows ICANN on the right with an arrow pointing to IANA. Below IANA are three arrows leading to IP addresses, domain names, and TCP/UDP port numbers. Text at the bottom reads: Internet Corporation for Assigned Names and Numbers (ICANN) - Based in the United States, ICANN coordinates IP address allocation, the management of domain names, and assignment of other information used in TCP/IP protocols. Internet Assigned Numbers Authority (IANA) - Responsible for overseeing and managing IP address allocation, domain name management, and protocol identifiers for ICANN.

Domain NamesTCP/UDP Port NumbersIP Addresses

- **Internet Corporation for Assigned Names and Numbers (ICANN)** - Based in the United States, ICANN coordinates IP address allocation, the management of domain names, and assignment of other information used in TCP/IP protocols.
- **Internet Assigned Numbers Authority (IANA)** - Responsible for overseeing and managing IP address allocation, domain name management, and protocol identifiers for ICANN.

3.4.3

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).

3.5.1

The Benefits of Using a Layered Model

You cannot actually watch real packets travel across a real network, the way you can watch the components of a car being put together on an assembly line. so, it helps to have a way of thinking about a network so that you can imagine what is happening. A model is useful in these situations.

Complex concepts such as how a network operates can be difficult to explain and understand. For this reason, a layered model is used to modularize the operations of a network into manageable layers.

These are the benefits of using a layered model to describe network protocols and operations:

- Assisting in protocol design because protocols that operate at a specific layer have defined information that they act upon and a defined interface to the layers above and below
- Fostering competition because products from different vendors can work together
- Preventing technology or capability changes in one layer from affecting other layers above and below
- Providing a common language to describe networking functions and capabilities

As shown in the figure, there are two layered models that are used to describe network operations:

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

At the top of the image are two LANs connected via a WAN with the text: A networking model is only a representation of a network operation. The model is not the actual network. Underneath are the OSI and TCP/IP model layers and protocols. The seven layers of the OSI model from top to bottom and their associated protocols are: application, presentation, session (protocols at the top three layers are HTTP, DNS, DHCP, and FTP), transport (TCP and UDP), network (IPv4, IPv6, ICMPv4, and ICMPv6), data link, and physical (protocols at the bottom two layers are Ethernet, WLAN, SONET, and SDH). The four layers of the TCP/IP model from top to bottom and their associated protocols are: application (HTTP, DNS, DHCP, and FTP), transport (TCP and UDP), Internet (IPv4, IPv6, ICMPv4, and ICMPv6), and network access (Ethernet, WLAN, SONET, and SDH).



HTTP, DNS, DHCP, FTPTCP, UDPIIPv4, IPv6, ICMPv4, ICMPv6Ethernet, WLAN, SONET, SDHTCP/IP Protocol SuiteA networking model is only a representation of a network operation. The model is not the actual network.

TCP/IP Model

OSI Model

3.5.2

The OSI Reference Model

The OSI reference model provides an extensive list of functions and services that can occur at each layer. This type of model provides consistency within all types of network protocols and services by describing what must be done at a particular layer, but not prescribing how it should be accomplished.

It also describes the interaction of each layer with the layers directly above and below. The TCP/IP protocols discussed in this course are structured around both the OSI and TCP/IP models. The table shows details about each layer of the OSI model. The functionality of each layer and the relationship between layers will become more evident throughout this course as the protocols are discussed in more detail.

OSI Model LayerDescription7 - ApplicationThe application layer contains protocols used for process-to-process communications.6 - PresentationThe presentation layer provides for common representation of the data transferred between application layer services.5 - SessionThe session layer provides services to the presentation layer to organize dialogue and to manage data exchange.4 - TransportThe transport layer defines services to segment, transfer, and reassemble the data for individual communications between the end devices.3 - NetworkThe network layer provides services to exchange the individual pieces of data over the network between identified end devices.2 - Data LinkThe data link layer protocols describe methods for exchanging data frames between devices over a common media1 - PhysicalThe 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.	
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 communication 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.

OSI Model LayerDescription7 - ApplicationThe application layer contains protocols used for process-to-process communications.6 - PresentationThe presentation layer provides for common representation of the data transferred between application layer services.5 - SessionThe session layer provides services to the presentation layer to organize dialogue and to manage data exchange.4 - TransportThe transport layer defines services to segment, transfer, and reassemble the data for individual communications between the end devices.3 - NetworkThe network layer provides services to exchange the individual pieces of data over the network between identified end devices.2 - Data LinkThe data link layer protocols describe methods for exchanging data frames between devices over a common media1 - PhysicalThe 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.

OSI Model Layer	Description
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.

Note: Whereas the TCP/IP model layers are referred to only by name, the seven OSI model layers are more often referred to by number rather than by name. For instance, the physical layer is referred to as Layer 1 of the OSI model, data link layer is Layer2, and so on.

3.5.3

The TCP/IP Protocol Model

The TCP/IP protocol model for internetwork communications was created in the early 1970s and is sometimes referred to as the internet model. This type of model closely matches the structure of a particular protocol suite. The TCP/IP model is a protocol model because it describes the functions that occur at each layer of protocols within the TCP/IP suite. TCP/IP is also used as a reference model. The table shows details about each layer of the TCP/IP model.

TCP/IP Model LayerDescription4 - ApplicationRepresents data to the user, plus encoding and dialog control.3 - TransportSupports communication between various devices across diverse networks.2 - InternetDetermines the best path through the network.1 - Network AccessControls the hardware devices and media that make up the network.	
TCP/IP Model Layer	Description
4 - Application	Represents data to the user, plus encoding and dialog control.
3 - Transport	Supports communication between various devices across diverse networks.
2 - Internet	Determines the best path through the network.
1 - Network Access	Controls the hardware devices and media that make up the network.

The definitions of the standard and the TCP/IP protocols are discussed in a public forum and defined in a publicly available set of IETF RFCs. An RFC is authored by networking engineers and sent to other IETF members for comments.

3.5.4

OSI and TCP/IP Model Comparison

The protocols that make up the TCP/IP protocol suite can also be described in terms of the OSI reference model. In the OSI model, the network access layer and the application layer of the TCP/IP model are further divided to describe discrete functions that must occur at these layers.

At the network access layer, the TCP/IP protocol suite does not specify which protocols to use when transmitting over a physical medium; it only describes the handoff from the internet layer to the physical network protocols. OSI Layers 1 and 2 discuss the necessary procedures to access the media and the physical means to send data over a network.

The figure shows the O S I model on the left and the t c p / i p model on the right. The o s i model is labeled from top down with the numbers 7 down to 1 and the following words at each layer: application, presentation, session, transport, network, data link, and physical. The top three layers of the o s i model are across the application layer of the t c p / i p model. The transport layers of each model are across from each other. The network o s i model layer is across from the internet layer on the right. Layers 1 and 2 of the o s i model are across from the network access layer of the t c p / i p model.

The key similarities are in the transport and network layers; however, the two models differ in how they relate to the layers above and below each layer:

- OSI Layer 3, the network layer, maps directly to the TCP/IP internet layer. This layer is used to describe protocols that address and route messages through an internetwork.
- OSI Layer 4, the transport layer, maps directly to the TCP/IP transport layer. This layer describes general services and functions that provide ordered and reliable delivery of data between source and destination hosts.
- The TCP/IP application layer includes several protocols that provide specific functionality to a variety of end user applications. The OSI model Layers 5, 6, and 7 are used as references for application software developers and vendors to produce applications that operate on networks.
- Both the TCP/IP and OSI models are commonly used when referring to protocols at various layers. Because the OSI model separates the data link layer from the physical layer, it is commonly used when referring to these lower layers.

3.5.5

3.6.1

Segmenting Messages

Knowing the OSI reference model and the TCP/IP protocol model will come in handy when you learn about how data is encapsulated as it moves across a network. It is not as simple as a physical letter being sent through the mail system.

In theory, a single communication, such as a video or an email message with many large attachments, could be sent across a network from a source to a destination as one massive, uninterrupted stream of bits. However, this would create problems for other devices needing to use the same communication channels or links. These large streams of data would result in significant delays. Further, if any link in the interconnected network infrastructure failed during the transmission, the complete message would be lost and would have to be retransmitted in full.

A better approach is to divide the data into smaller, more manageable pieces to send over the network. Segmentation is the process of dividing a stream of data into smaller units for transmissions over the network. Segmentation is necessary because data networks use the TCP/IP protocol suite send data in individual IP packets. Each packet is sent separately, similar to sending a long letter as a series of individual postcards. Packets containing segments for the same destination can be sent over different paths.

This leads to 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 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.

Click each button in the figure to view the animations of segmentation and multiplexing.

The animation shows a small LAN with two hosts and a server. When the Segmentation button is pressed a large message from the first host is broken up into smaller messages that are sent across the network to the server. Then the Multiplexing button is pressed messages from both hosts are sent onto the network one after the other to the server.

Segmentation
Multiplexing

3.6.2

Sequencing

The challenge to using segmentation and multiplexing to transmit messages across a network is the level of complexity that is added to the process. Imagine if you had to send a 100-page letter, but each envelope could only hold one page. Therefore, 100 envelopes would be required and each envelope would need to be addressed individually. It is possible that the 100-page letter in 100 different envelopes arrives out-of-order. Consequently, the information in the envelope would need to include a sequence number to ensure that the receiver could reassemble the pages in the proper order.

In network communications, each segment of the message must go through a similar process to ensure that it gets to the correct destination and can be reassembled into the content of the original message, as shown in the figure. TCP is responsible for sequencing the individual segments.

The figure shows two computers sending messages on a network to a server. Each message has been divided up into multiple pieces shown as yellow and orange envelopes, some are interleaved and numbered. Text reads: Multiple pieces are labeled for easy direction and re-assembly. Labeling provides for ordering and assembling the pieces when they arrive.

321321



Labeling provides for ordering and assembling the pieces when they arrive. Multiple pieces are labeled for easy direction and re-assembly.

3.6.3

Protocol Data Units

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.

Note: 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.

The figure shows the protocol data units (PDUs) at various layers of the OSI model. At the top of the image is a person sitting at a computer workstation sending email data. That data is passed down the stack and encapsulated into a new PDU at each layer. At the top, the email data is divided into smaller chunks of data. Below that, a transport header is added in front of the chunk of data and it becomes a segment. Below that, a network header is added in front of the transport header and it becomes a packet. Below that, a frame header is added in front of the network header and a frame trailer is added behind the data and it becomes a frame (medium dependent). The frame is shown as a stream of bits prior to being received by a router which is connected to the cloud. Text at the bottom reads: 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. Note: If the Transport header is TCP, then it is a segment. If the Transport header is UDP then it is a datagram.

11000101010001011001010010101001
Email Data

Passing down the stack.

- 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

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

3.6.4

Encapsulation Example

When messages are being sent on a network, the encapsulation process works from top to bottom. At each layer, the upper layer information is considered data within the encapsulated protocol. For example, the TCP segment is considered data within the IP packet.

You saw this animation previously in this module. This time, click Play and focus on the encapsulation process as a web server sends a web page to a web client.

The animation shows a small network with a Web Server and a Web Client. There's a graphic that shows the components that make up a message. An Ethernet Frame, and IP Packet, a TCP segment, and the user data. The animation begins with the web server preparing the Hypertext Markup Language (HTML) page as data to be sent.

The application protocol HTTP header is added (prepended) to the front of the HTML data. The header contains various information, including the HTTP version the server is using and a status code indicating it has information for the web client. The HTTP application layer protocol delivers the HTML-formatted web page data to the TCP transport layer. The transport layer protocol prepends additional information to the HTTP data to manage the exchange of information between the web server and web client. The IP information is prepended to the TCP information. IP assigns the appropriate source and destination IP addresses. This information is known as an IP packet. The Ethernet protocol prepends and adds to the end (appends) information to the IP packet to create a data link frame. The frame is then converted into a string of binary bits that are sent along the network path to the web client.

Web Server
Web Client

User Data
TCP Segment
IP Packet
Ethernet Frame



3.6.5

De-encapsulation Example

This process is reversed at the receiving host and is known as de-encapsulation. 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.

You saw this animation previously in this module. This time, click Play and focus on the de-encapsulation process.

3.7.1

Addresses

As you just learned, it is necessary to segment messages in a network. But those segmented messages will not go anywhere if they are not addressed properly. This topic gives an overview of network addresses. You will also get the chance to use the Wireshark tool, which will help you to ‘view’ network traffic.

The network and data link layers are responsible for delivering the data from the source device to the destination device. As shown in the figure, protocols at both layers contain a source and destination address, but their addresses have different purposes:

- **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 figure shows the addressing and labeling used at various layers of the OSI model for delivering data. Starting from left to right, it shows: the physical layer provides timing and synchronization bits; the data link layer provides destination and source physical addresses; the network layer provides destination and source logical network addresses; the transport layer provides destination and source process number (ports); and the upper layers provide encoded application data.

Physical	Data Link	Network	Transport	Upper Layers	Timing and synchronization bits	Destination and source physical addresses	Destination and source logical network addresses	Destination and source process number (ports)	Encoded application data
----------	-----------	---------	-----------	--------------	---------------------------------	---	--	---	--------------------------

3.7.2

Layer 3 Logical Address

An IP address is the network layer, or Layer 3, logical address used to deliver the IP packet from the original source to the final destination, as shown in the figure.

The figure shows a layer 3 IP packet moving from the original source to the final destination. The original source is PC1, shown on the left, with IP address 192.168.1.110. The final destination is a web server, shown on the far right, with IP address 172.16.1.99. An IP packet is shown leaving PC1 heading to router R1. The IP packet is then shown leaving router R1 and heading to router R2. The IP packet is then shown leaving R2 and heading towards the web server. Below the network topology is a diagram of a layer 3 IP packet header showing 192.168.1.110 as the source and 172.16.1.99 as the destination.



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.

3.7.3

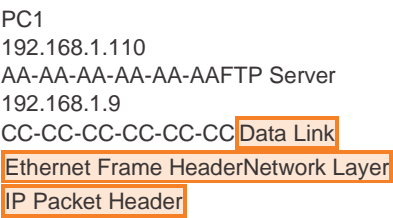
Devices on the Same Network

In this example we have a client computer, PC1, communicating with an FTP server on the same IP network.

- **Source IPv4 address** - The IPv4 address of the sending device, the client computer PC1: 192.168.1.110.
- **Destination IPv4 address** - The IPv4 address of the receiving device, FTP server: 192.168.1.9.

Notice in the figure that the network portion of the source IPv4 address and the network portion of the destination IPv4 address are the same and therefore; the source and destination are on the same network.

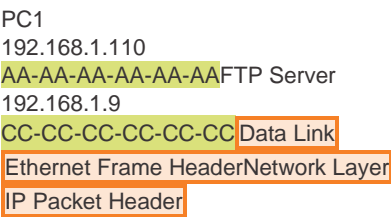
The figure shows the data link Ethernet frame header and network layer IP packet header for information flowing from a source to a destination on the same network. At the bottom is a network topology. Starting at the left, it consists of PC1 with IP address 192.168.1.110 and MAC address AA-AA-AA-AA-AA-AA, an FTP server with IP address 192.168.1.9 and MAC address CC-CC-CC-CC-CC-CC, and another PC, all connected to the same switch. In the middle of the topology is a string of three routers to which the switch is connected. At the right is another switch connected to a server. Above the topology is the message broken down into its various components. It begins on the left with the data link Ethernet frame header showing a destination of CC-CC-CC-CC-CC-CC and a source of AA-AA-AA-AA-AA-AA. Next is the network layer IP packet header showing a source of 192.168.1 (network) 110 (host) and a destination of 192.168.1 (network) 9 (host). Lastly is the data.



Role of the Data Link Layer Addresses: Same IP Network

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, as highlighted in the figure.

The figure shows the data link Ethernet frame header and network layer IP packet header for information flowing from a source to a destination on the same network, highlighting the role of the MAC address. At the bottom is a network topology. Starting at the left, it consists of PC1 with IP address 192.168.1.110 and MAC address AA-AA-AA-AA-AA-AA (shown highlighted), an FTP server with IP address 192.168.1.9 and MAC address CC-CC-CC-CC-CC-CC (shown highlighted), and another PC, all connected to the same switch. In the middle of the topology is a string of three routers to which the switch is connected. At the right is another switch connected to a server. Above the topology is the message broken down into its various components. It begins on the left with the data link Ethernet frame header showing a destination of CC-CC-CC-CC-CC-CC and a source of AA-AA-AA-AA-AA-AA. Next is the network layer IP packet header showing a source of 192.168.1 (network) 110 (host) and a destination of 192.168.1 (network) 9 (host). Lastly is the data.



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 frame with the encapsulated IP packet can now be transmitted from PC1 directly to the FTP server.

Devices on a Remote Network

But what are the roles of the network layer address and the data link layer address when a device is communicating with a device on a remote network? In this example we have a client computer, PC1, communicating with a server, named Web Server, on a different IP network.

Role of the Network Layer Addresses

When the sender of the packet is on a different network from the receiver, the source and destination IP addresses will represent hosts on different networks. This will be indicated by the network portion of the IP address of the destination host.

- **Source IPv4 address** - The IPv4 address of the sending device, the client computer PC1: 192.168.1.110.
- **Destination IPv4 address** - The IPv4 address of the receiving device, the server, Web Server: 172.16.1.99.

Notice in the figure that the network portion of the source IPv4 address and destination IPv4 address are on different networks.

The figure shows the data link Ethernet frame header and network layer IP packet header for information flowing from a source on one network to a destination on a different network. At the bottom is a network topology. Starting at the left, it consists of PC1 with IP 192.168.1.110 and MAC AA-AA-AA-AA-AA-AA, a server, and another PC, all connected to the same switch. In the middle of the topology is a string of three routers to which the switch is

connected. The router on the left is labeled R1 with IP 192.168.1.1 and MAC 11-11-11-11-11-11. The middle router is unlabeled. The router on the right is labeled R2 with IP 172.16.1.1 and MAC 22-22-22-22-22-22. At the right is another switch connected to a Web server with IP 172.16.1.99 and MAC AB-CD-EF-12-34-56. Above the topology is the message broken down into its various components. It begins on the left with the data link Ethernet frame header showing a destination of 11-11-11-11-11-11 and a source of AA-AA-AA-AA-AA-AA. Next is the network layer IP packet header showing a source of 192.168.1 (network) 110 (device) and a destination of 172.16.1 (network) 99 (device). Lastly is the data.

Data Link
Ethernet Frame HeaderNetwork Layer
IP Packet Header

PC1
192.168.1.110
AA-AA-AA-AA-AA-AAR1
192.168.1.1
11-11-11-11-11-11R2
172.16.1.1
22-22-22-22-22-22Web Server
172.16.1.99
AB-CD-EF-12-34-56
3.7.7


Role of the Data Link Layer Addresses: Different IP Networks

When the sender and receiver of the IP packet are on different networks, 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. In our example, the default gateway is R1. R1 has an Ethernet data link address that is on the same network as PC1. This allows PC1 to reach the router directly.

- **Source MAC address** - The Ethernet MAC address of the sending device, PC1. The MAC address of the Ethernet interface of PC1 is AA-AA-AA-AA-AA-AA.
- **Destination MAC address** - 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. In this example, the destination MAC address is the MAC address of the R1 Ethernet interface, 11-11-11-11-11-11. This is the interface that is attached to the same network as PC1, as shown in the figure.

The figure shows the data link Ethernet frame header and network layer IP packet header for information flowing from a source on one network to a destination on a different network, highlighting the role of the MAC address. At the bottom is a network topology. Starting at the left, it consists of PC1 with IP 192.168.1.110 and MAC AA-AA-AA-AA-AA-AA(shown highlighted), a server, and another PC, all connected to the same switch. In the middle of the topology is a string of three routers to which the switch is connected. The router on the left is labeled R1 with IP 192.168.1.1 and MAC 11-11-11-11-11-11 (shown highlighted). The middle router is unlabeled. The router on the right is labeled R2 with IP 172.16.1.1 and MAC 22-22-22-22-22-22. At the right is another switch connected to a Web server with IP 172.16.1.99 and MAC AB-CD-EF-12-34-56. Above the topology is the message broken down into its various components. It begins on the left with the data link Ethernet frame header showing a destination of 11-11-11-11-11-11 and a source of AA-AA-AA-AA-AA-AA. Next is the network layer IP packet header showing a source of 192.168.1 (network) 110 (device) and a destination of 172.16.1 (network) 99 (device). Lastly is the data.

R1R2



Data Link
Ethernet Frame HeaderNetwork Layer
IP Packet Header

PC1
192.168.1.110
AA-AA-AA-AA-AA-AAR1
192.168.1.1
11-11-11-11-11-11R2
172.16.1.1
22-22-22-22-22-22Web Server
172.16.1.99
AB-CD-EF-12-34-56

The Ethernet frame with the encapsulated IP packet can now be transmitted to R1. R1 forwards the packet to the destination, Web Server. This may mean that R1 forwards the packet to another router or directly to Web Server if the destination is on a network connected to R1.

It is important that the IP address of the default gateway be configured on each host on the local network. All packets to a destination on remote networks are sent to the default gateway. Ethernet MAC addresses and the default gateway are discussed in more detail in other modules.

3.7.8

Data Link Addresses

The data link Layer 2 physical address has a different role. 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.

Click each button to view an illustration of how the data link layer addresses change at every hop from source to destination

- Host to Router
- Router to Router
- Router to Server

Host to Router

The figure shows the L2 header in the first hop as information flows from a host on one network to a server on a different network. A network topology shows the original source PC1 at 192.168.1.10 connected to a router, connected to another router, connected to the final destination Web server at 172.16.1.99. Below the topology is an L3 IP packet with source IP 192.168.1.110 and destination IP 172.16.1.99. In front of the packet is the L2 header with destination NIC and source NIC. These L2 header addresses match the NIC of the original source (PC1) and the interface of the next hop router.



Original Source	Final Destination
PC1	
192.168.1.110	Web Server
172.16.1.99	

L2 HeaderL3 IP Packet

As the IP packet travels from host-to-router, router-to-router, and finally router-to-host, at each point along the way the IP packet is encapsulated in a new data link frame. Each data link frame contains the source data link address of the NIC card sending the frame, and the destination data link address of the NIC card receiving the frame.

The Layer 2, data link protocol is only used to deliver the packet from NIC-to-NIC on the same network. The router removes the Layer 2 information as it is received on one NIC and adds new data link information before forwarding out the exit NIC on its way towards the final destination.

The IP packet is encapsulated in a data link frame that contains the following data link information:

- **Source data link address** - The physical address of the NIC that is sending the data link frame.
- **Destination data link address** - The physical address of the NIC that is receiving the data link frame. This address is either the next hop router or the address of the final destination device.

4.1.1

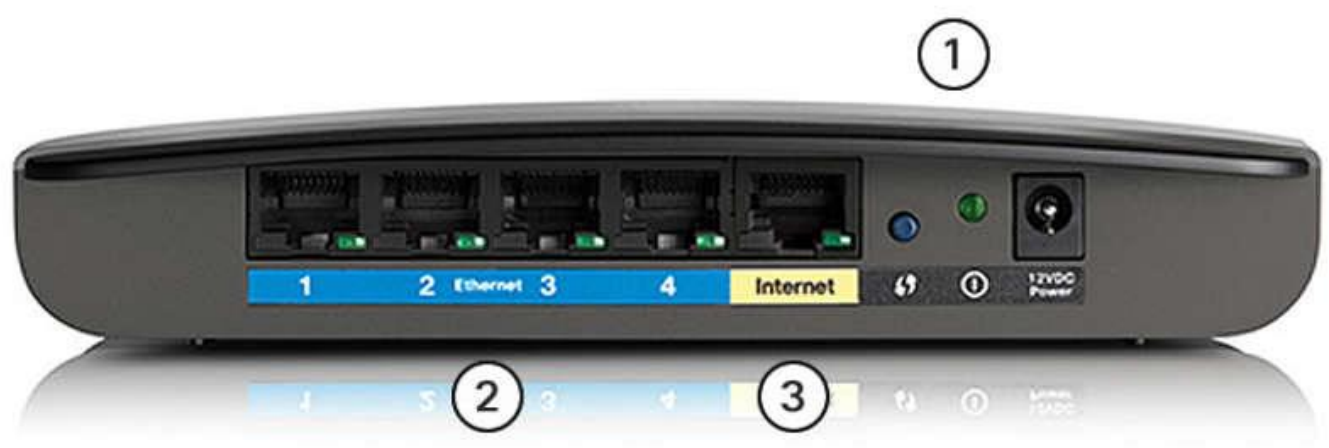
The Physical Connection

Whether connecting to a local printer in the home or a website in another country, before any network communications can occur, a physical connection to a local network must be established. A physical connection can be a wired connection using a cable or a wireless connection using radio waves.

The type of physical connection used depends upon the setup of the network. For example, in many corporate offices, employees have desktop or laptop computers that are physically connected, via cable, to a shared switch. This type of setup is a wired network. Data is transmitted through a physical cable.

In addition to wired connections, many businesses also offer wireless connections for laptops, tablets, and smartphones. With wireless devices, data is transmitted using radio waves. Wireless connectivity is common as individuals and businesses alike discover its advantages. Devices on a wireless network must be connected to a wireless access point (AP) or wireless router like the one shown in the figure.

Wireless Router



These are the components of an access point:

- 1. The wireless antennas (These are embedded inside the router version shown in the figure above.)
- 2. Several Ethernet switchports
- 3. An internet port

Similar to a corporate office, most homes offer both wired and wireless connectivity to the network. The figures show a home router and a laptop connecting to the local area network (LAN).

Wired Connection to Wireless Router



Network Interface Cards

Network interface cards (NICs) connect a device to the network. Ethernet NICs are used for a wired connection, as shown in the figure, whereas wireless local area network (WLAN) NICs are used for wireless. An end-user device may include one or both types of NICs. A network printer, for example, may only have an Ethernet NIC, and

therefore, must connect to the network using an Ethernet cable. Other devices, such as tablets and smartphones, might only contain a WLAN NIC and must use a wireless connection.

Wired Connection Using an Ethernet NIC



Not all physical connections are equal, in terms of the performance level, when connecting to a network.

4.1.2

The Physical Layer

The OSI physical layer provides the means to transport the bits that make up a data link layer frame across the network media. This layer accepts a complete frame from the data link layer and encodes it as a series of signals that are transmitted to the local media. The encoded bits that comprise a frame are received by either an end device or an intermediate device.

Click Play in the figure to see an example of the encapsulation process. The last part of this process shows the bits being sent over the physical medium. The physical layer encodes the frames and creates the electrical, optical, or radio wave signals that represent the bits in each frame. These signals are then sent over the media, one at a time.

The destination node physical layer retrieves these individual signals from the media, restores them to their bit representations, and passes the bits up to the data link layer as a complete frame.

4.2.1

Physical Layer Standards

In the previous topic, you gained a high level overview of the physical layer and its place in a network. This topic dives a bit deeper into the specifics of the physical layer. This includes the components and the media used to build a network, as well as the standards that are required so that everything works together.

The protocols and operations of the upper OSI layers are performed using software designed by software engineers and computer scientists. The services and protocols in the TCP/IP suite are defined by the Internet Engineering Task Force (IETF).

The physical layer consists of electronic circuitry, media, and connectors developed by engineers. Therefore, it is appropriate that the standards governing this hardware are defined by the relevant electrical and communications engineering organizations.

There are many different international and national organizations, regulatory government organizations, and private companies involved in establishing and maintaining physical layer standards. For instance, the physical layer hardware, media, encoding, and signaling standards are defined and governed by these standards organizations:

- International Organization for Standardization (ISO)
- Telecommunications Industry Association/Electronic Industries Association (TIA/EIA)
- International Telecommunication Union (ITU)
- American National Standards Institute (ANSI)
- Institute of Electrical and Electronics Engineers (IEEE)
- National telecommunications regulatory authorities including the Federal Communication Commission (FCC) in the USA and the European Telecommunications Standards Institute (ETSI)

In addition to these, there are often regional cabling standards groups such as CSA (Canadian Standards Association), CENELEC (European Committee for Electrotechnical Standardization), and JSA/JIS (Japanese Standards Association), which develop local specifications.

The physical layer standards are implemented in hardware and are governed by many organizations including:

- ISO
- ANSI/TIA
- ITU-T
- ANSI
- IEEE

The TCP/IP standards are implemented in software and governed by the IETF.

ApplicationPresentationSessionTransportNetworkData LinkPhysical

4.2.2

Physical Components

The physical layer standards address three functional areas:

- Physical Components
- Encoding
- Signaling

Physical Components

The physical components are the electronic hardware devices, media, and other connectors that transmit the signals that represent the bits. Hardware components such as NICs, interfaces and connectors, cable materials, and cable designs are all specified in standards associated with the physical layer. The various ports and interfaces on a Cisco 1941 router are also examples of physical components with specific connectors and pinouts resulting from standards.

4.2.3

Encoding

Encoding or line encoding is a method of converting a stream of data bits into a predefined "code". Codes are groupings of bits used to provide a predictable pattern that can be recognized by both the sender and the receiver. In other words, encoding is the method or pattern used to represent digital information. This is similar to how Morse code encodes a message using a series of dots and dashes.

For example, Manchester encoding represents a 0 bit by a high to low voltage transition, and a 1 bit is represented as a low to high voltage transition. An example of Manchester encoding is illustrated in the figure. The transition occurs at the middle of each bit period. This type of encoding is used in 10 Mbps Ethernet. Faster data rates require more complex encoding. Manchester encoding is used in older Ethernet standards such as 10BASE-T. Ethernet 100BASE-TX uses 4B/5B encoding and 1000BASE-T uses 8B/10B encoding.

The image is a line graph of voltage over time depicting Manchester encoding of a stream of seven bits. There are horizontal lines spaced evenly apart that represent bit periods. There is also a vertical line drawn halfway up the y axis used as a reference point. As the stream of bits (signal) is sent, there are drops and rises in voltage levels in the middle of each bit period. If the bit is a binary zero, then the voltage drops in the middle. If the bit is a binary one, then the voltage rises in the middle. The bits transmitted are 0100110.

11100000100110
VoltageTime
The transition occurs at the middle of each bit period.

4.2.4

Signaling

The physical layer must generate the electrical, optical, or wireless signals that represent the "1" and "0" on the media. The way that bits are represented is called the signaling method. The physical layer standards must define what type of signal represents a "1" and what type of signal represents a "0". This can be as simple as a change in the level of an electrical signal or optical pulse. For example, a long pulse might represent a 1 whereas a short pulse might represent a 0.

This is similar to the signaling method used in Morse code, which may use a series of on-off tones, lights, or clicks to send text over telephone wires or between ships at sea.

The figures display signaling

Click each button for illustrations of signaling for copper cable, fiber-optic cable, and wireless media.

Copper Cable
Fiber Optic Cable
Wireless Media

Electrical Signals Over Copper Cable

graph of voltage over time showing square waves with varying levels of peaks and troughs

VoltageTime

4.2.5

Bandwidth

Different physical media support the transfer of bits at different rates. Data transfer is usually discussed in terms of bandwidth. Bandwidth is the capacity at which a medium can carry data. Digital bandwidth measures the amount of data that can flow from one place to another in a given amount of time. Bandwidth is typically measured in kilobits per second (kbps), megabits per second (Mbps), or gigabits per second (Gbps). Bandwidth is sometimes thought of as the speed that bits travel, however this is not accurate. For example, in both 10Mbps and 100Mbps Ethernet, the bits are sent at the speed of electricity. The difference is the number of bits that are transmitted per second.

A combination of factors determines the practical bandwidth of a network:

- The properties of the physical media
- The technologies chosen for signaling and detecting network signals

Physical media properties, current technologies, and the laws of physics all play a role in determining the available bandwidth.

The table shows the commonly used units of measure for bandwidth.

Table caption		
Unit of Bandwidth	Abbreviation	Equivalence
Bits per second	bps	1 bps = fundamental unit of bandwidth
Kilobits per second	Kbps	1 Kbps = 1,000 bps = 10 ³ bps
Megabits per second	Mbps	1 Mbps = 1,000,000 bps = 10 ⁶ bps
Gigabits per second	Gbps	1 Gbps = 1,000,000,000 bps = 10 ⁹ bps
Terabits per second	Tbps	1 Tbps = 1,000,000,000,000 bps = 10 ¹² bps

4.2.6

Bandwidth Terminology

Terms used to measure the quality of bandwidth include:

- Latency
- Throughput
- Goodput

Latency

Latency refers to the amount of time, including delays, for data to travel from one given point to another.

In an internetwork, or a network with multiple segments, throughput cannot be faster than the slowest link in the path from source to destination. Even if all, or most, of the segments have high bandwidth, it will only take one segment in the path with low throughput to create a bottleneck in the throughput of the entire network.

Throughput

Throughput is the measure of the transfer of bits across the media over a given period of time.

Due to a number of factors, throughput usually does not match the specified bandwidth in physical layer implementations. Throughput is usually lower than the bandwidth. There are many factors that influence throughput:

- The amount of traffic
- The type of traffic
- The latency created by the number of network devices encountered between source and destination

There are many online speed tests that can reveal the throughput of an internet connection. The figure provides sample results from a speed test.

Goodput

There is a third measurement to assess the transfer of usable data; it is known as goodput. Goodput is the measure of usable data transferred over a given period of time. Goodput is throughput minus traffic overhead for establishing sessions, acknowledgments, encapsulation, and retransmitted bits. Goodput is always lower than throughput, which is generally lower than the bandwidth.

4.3.1

Characteristics of Copper Cabling

Copper cabling is the most common type of cabling used in networks today. In fact, copper cabling is not just one type of cable. There are three different types of copper cabling that are each used in specific situations.

Networks use copper media because it is inexpensive, easy to install, and has low resistance to electrical current. However, copper media is limited by distance and signal interference.

Data is transmitted on copper cables as electrical pulses. A detector in the network interface of a destination device must receive a signal that can be successfully decoded to match the signal sent. However, the farther the signal travels, the more it deteriorates. This is referred to as signal attenuation. For this reason, all copper media must follow strict distance limitations as specified by the guiding standards.

The timing and voltage values of the electrical pulses are also susceptible to interference from two sources:

- **Electromagnetic interference (EMI) or radio frequency interference (RFI)** - EMI and RFI signals can distort and corrupt the data signals being carried by copper media. Potential sources of EMI and RFI include radio waves and electromagnetic devices, such as fluorescent lights or electric motors.
- **Crosstalk** - Crosstalk is a disturbance caused by the electric or magnetic fields of a signal on one wire to the signal in an adjacent wire. In telephone circuits, crosstalk can result in hearing part of another voice conversation from an adjacent circuit. Specifically, when an electrical current flows through a wire, it creates a small, circular magnetic field around the wire, which can be picked up by an adjacent wire.

The figure shows how data transmission can be affected by interference.

The diagram is four graphs, each with voltage over time. The first graph shows square waves of a pure digital signal and its binary equivalent, 1011001001101. The second graph is of an interference signal with varying degrees of voltage. The third graph shows the digital signal with the interference. The fourth graph shows how the computer reads the changed signal as the binary equivalent of 1011001011101 with the 5th bit from the right changed from a 0 to a 1.

1011001001101101100100110110110010111011234

Pure Digital Signal	Voltage	Time	Interference Signal	Voltage	Time	Digital Signal with Interference	Voltage	Time	What the Computer Reads
									Changed Signal

1. A pure digital signal is transmitted.
2. On the medium, there is an interference signal.
3. The digital signal is corrupted by the interference signal.
4. The receiving computer reads a changed signal. Notice that a 0 bit is now interpreted as a 1 bit.

To counter the negative effects of EMI and RFI, some types of copper cables are wrapped in metallic shielding and require proper grounding connections.

To counter the negative effects of crosstalk, some types of copper cables have opposing circuit wire pairs twisted together, which effectively cancels the crosstalk.

The susceptibility of copper cables to electronic noise can also be limited using these recommendations:

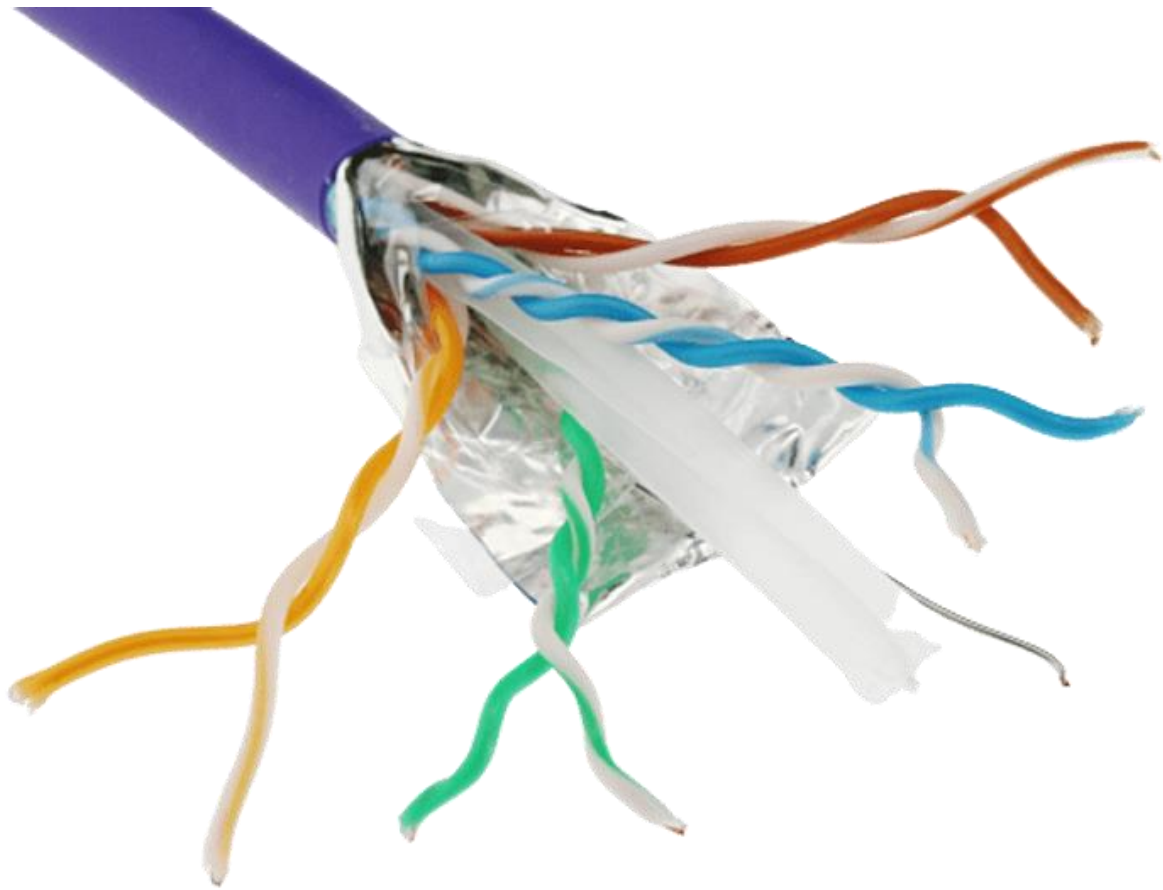
- Selecting the cable type or category most suited to a given networking environment
- Designing a cable infrastructure to avoid known and potential sources of interference in the building structure
- Using cabling techniques that include the proper handling and termination of the cables

4.3.2

Types of Copper Cabling

There are three main types of copper media used in networking.

The figure is composed of pictures showing the three types of copper cabling, each with a portion of the outer cable jacket stripped to expose the cable construction. The first picture shows unshielded twisted-pair (UTP) cable with four color pairs of twisted wires - blue, orange, green, and brown. The second picture is shielded twisted-pair (STP) cable showing four pairs of twisted wires - blue, green, brown, and orange - with a foil shield surrounding all four pairs. The last picture shows a center copper conductor surrounded by plastic insulation surrounded by a braided shield.



Unshielded Twisted-Pair (UTP) CableShielded Twisted-Pair (STP) CableCoaxial Cable

4.3.3

Unshielded twisted-pair (UTP)

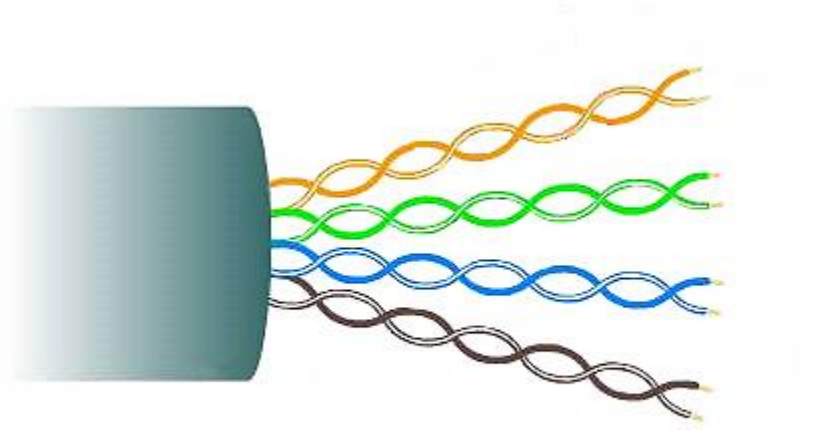
Unshielded twisted-pair (UTP) cabling is the most common networking media. UTP cabling, terminated with RJ-45 connectors, is used for interconnecting network hosts with intermediary networking devices, such as switches and routers.

In LANs, UTP cable consists of four pairs of color-coded wires that have been twisted together and then encased in a flexible plastic sheath that protects from minor physical damage. The twisting of wires helps protect against signal interference from other wires.

As seen in the figure, the color codes identify the individual pairs and wires and aid in cable termination.

UTP cable showing the outer cable jacket (labeled 1), the twisted wire pairs (labeled 2), and the orange, green, blue, and brown insulation (labeled 3)

123



The numbers in the figure identify some key characteristics of unshielded twisted-pair cable:

- 1. The outer jacket protects the copper wires from physical damage.
- 2. Twisted-pairs protect the signal from interference.
- 3. Color-coded plastic insulation electrically isolates wires from each other and identifies each pair.

4.3.4

Shielded twisted-pair (STP)

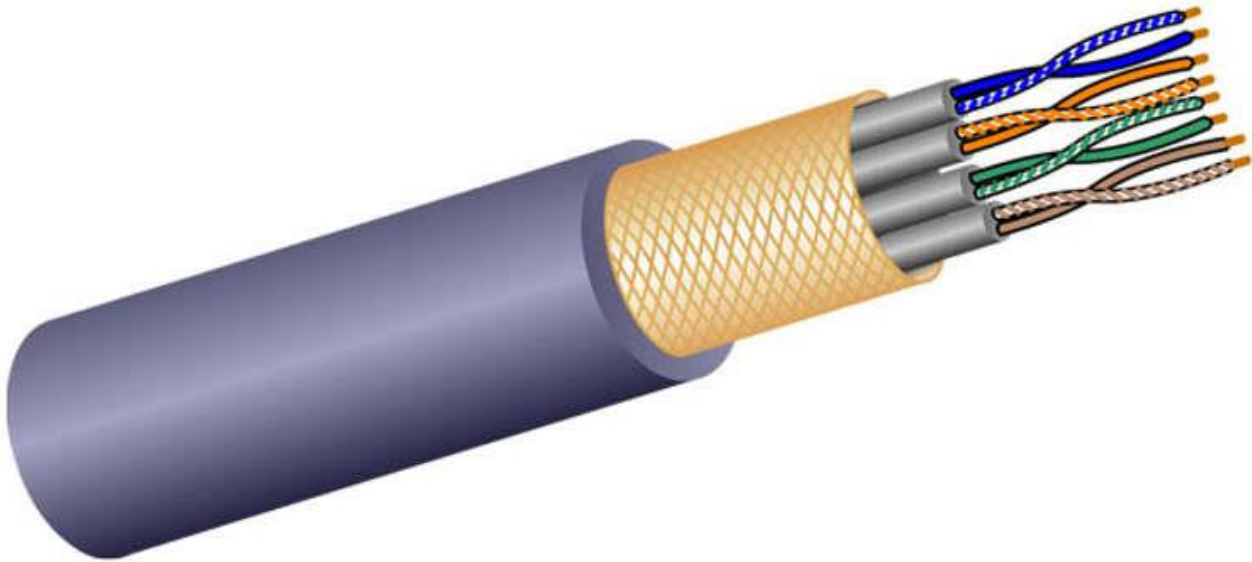
Shielded twisted-pair (STP) provides better noise protection than UTP cabling. However, compared to UTP cable, STP cable is significantly more expensive and difficult to install. Like UTP cable, STP uses an RJ-45 connector.

STP cables combine the techniques of shielding to counter EMI and RFI, and wire twisting to counter crosstalk. To gain the full benefit of the shielding, STP cables are terminated with special shielded STP data connectors. If the cable is improperly grounded, the shield may act as an antenna and pick up unwanted signals.

The STP cable shown uses four pairs of wires, each wrapped in a foil shield, which are then wrapped in an overall metallic braid or foil.

STP cable showing the outer cable jacket (labeled 1), a braided shield around all the wire pairs (labeled 2), foil shields around the individual wire pairs (labeled 3), and the twisted colored wire pairs (labeled 4)

1234



The numbers in the figure identify some key features of shielded twisted-pair cable:

- 1. Outer jacket
- 2. Braided or foil shield
- 3. Foil shields
- 4. Twisted pairs

4.3.5

Coaxial cable

Coaxial cable, or coax for short, gets its name from the fact that there are two conductors that share the same axis. As shown in the figure, coaxial cable consists of the following:

- A copper conductor is used to transmit the electronic signals.
- A layer of flexible plastic insulation surrounds a copper conductor.
- The insulating material is surrounded in a woven copper braid, or metallic foil, that acts as the second wire in the circuit and as a shield for the inner conductor. This second layer, or shield, also reduces the amount of outside electromagnetic interference.
- The entire cable is covered with a cable jacket to prevent minor physical damage.

There are different types of connectors used with coax cable. The Bayonet Neill–Concelman (BNC), N type, and F type connectors are shown in the figure.

Although UTP cable has essentially replaced coaxial cable in modern Ethernet installations, the coaxial cable design is used in the following situations:

- **Wireless installations** - Coaxial cables attach antennas to wireless devices. The coaxial cable carries radio frequency (RF) energy between the antennas and the radio equipment.
- **Cable internet installations** - Cable service providers provide internet connectivity to their customers by replacing portions of the coaxial cable and supporting amplification elements with fiber-optic cable. However, the wiring inside the customer's premises is still coax cable.

three figures showing the construction of a coaxial cable, a cross-section of a coaxial cable, and three types of coaxial cable connectors

1243



Coaxial ConnectorsF typeN typeBNC

The numbers in the figure identify some key features of coaxial cable:

1. Outer jacket
2. Braided copper shielding
3. Plastic insulation
4. Copper conductor

4.4.1

Properties of UTP Cabling

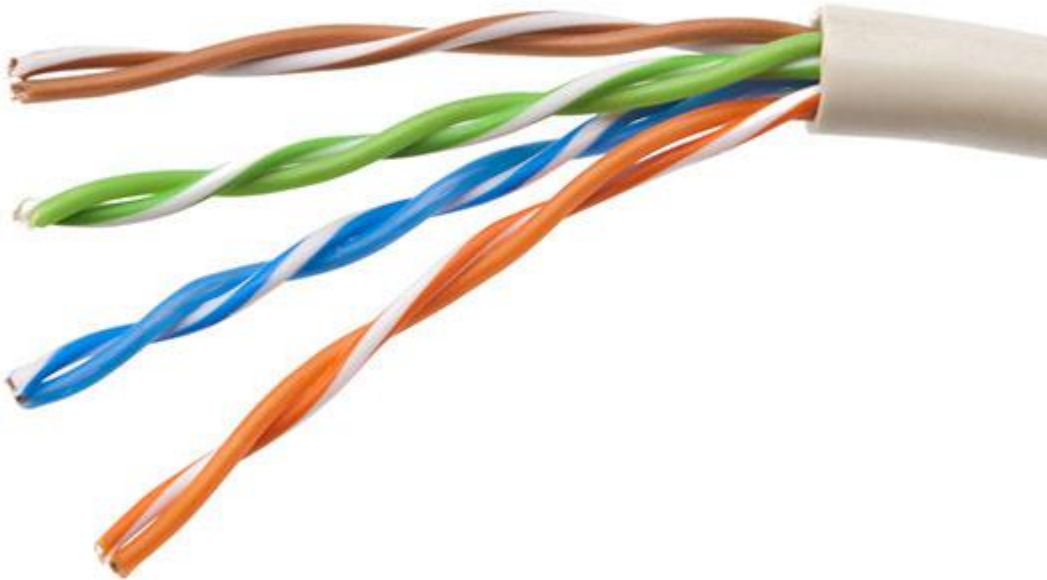
In the previous topic, you learned a bit about unshielded twisted-pair (UTP) copper cabling. Because UTP cabling is the standard for use in LANs, this topic goes into detail about its advantages and limitations, and what can be done to avoid problems.

When used as a networking medium, UTP cabling consists of four pairs of color-coded copper wires that have been twisted together and then encased in a flexible plastic sheath. Its small size can be advantageous during installation.

UTP cable does not use shielding to counter the effects of EMI and RFI. Instead, cable designers have discovered other ways that they can limit the negative effect of crosstalk:

- **Cancellation** - Designers now pair wires in a circuit. When two wires in an electrical circuit are placed close together, their magnetic fields are the exact opposite of each other. Therefore, the two magnetic fields cancel each other and also cancel out any outside EMI and RFI signals.
- **Varying the number of twists per wire pair** - To further enhance the cancellation effect of paired circuit wires, designers vary the number of twists of each wire pair in a cable. UTP cable must follow precise specifications governing how many twists or braids are permitted per meter (3.28 feet) of cable. Notice in the figure that the orange/orange white pair is twisted less than the blue/blue white pair. Each colored pair is twisted a different number of times.

UTP cable relies solely on the cancellation effect produced by the twisted wire pairs to limit signal degradation and effectively provide self-shielding for wire pairs within the network media.



4.4.2

UTP Cabling Standards and Connectors

UTP cabling conforms to the standards established jointly by the TIA/EIA. Specifically, TIA/EIA-568 stipulates the commercial cabling standards for LAN installations and is the standard most commonly used in LAN cabling environments. Some of the elements defined are as follows:

- Cable types
- Cable lengths
- Connectors
- Cable termination
- Methods of testing cable

The electrical characteristics of copper cabling are defined by the Institute of Electrical and Electronics Engineers (IEEE). IEEE rates UTP cabling according to its performance. Cables are placed into categories based on their ability to carry higher bandwidth rates. For example, Category 5 cable is used commonly in 100BASE-TX Fast Ethernet installations. Other categories include Enhanced Category 5 cable, Category 6, and Category 6a.

Cables in higher categories are designed and constructed to support higher data rates. As new gigabit speed Ethernet technologies are being developed and adopted, Category 5e is now the minimally acceptable cable type, with Category 6 being the recommended type for new building installations.

The figure shows three categories of UTP cable:

- Category 3 was originally used for voice communication over voice lines, but later used for data transmission.
- Category 5 and 5e is used for data transmission. Category 5 supports 100Mbps and Category 5e supports 1000 Mbps
- Category 6 has an added separator between each wire pair to support higher speeds. Category 6 supports up to 10 Gbps.
- Category 7 also supports 10 Gbps.
- Category 8 supports 40 Gbps.

Some manufacturers are making cables exceeding the TIA/EIA Category 6a specifications and refer to these as Category 7.

The figure shows the difference in construction between categories of UTP cable. At the top is category 3 with four wires. In the middle is category 5 and 5e with four twisted wire pairs. At the bottom is category 6 with four twisted wire pairs, each with a plastic separator.

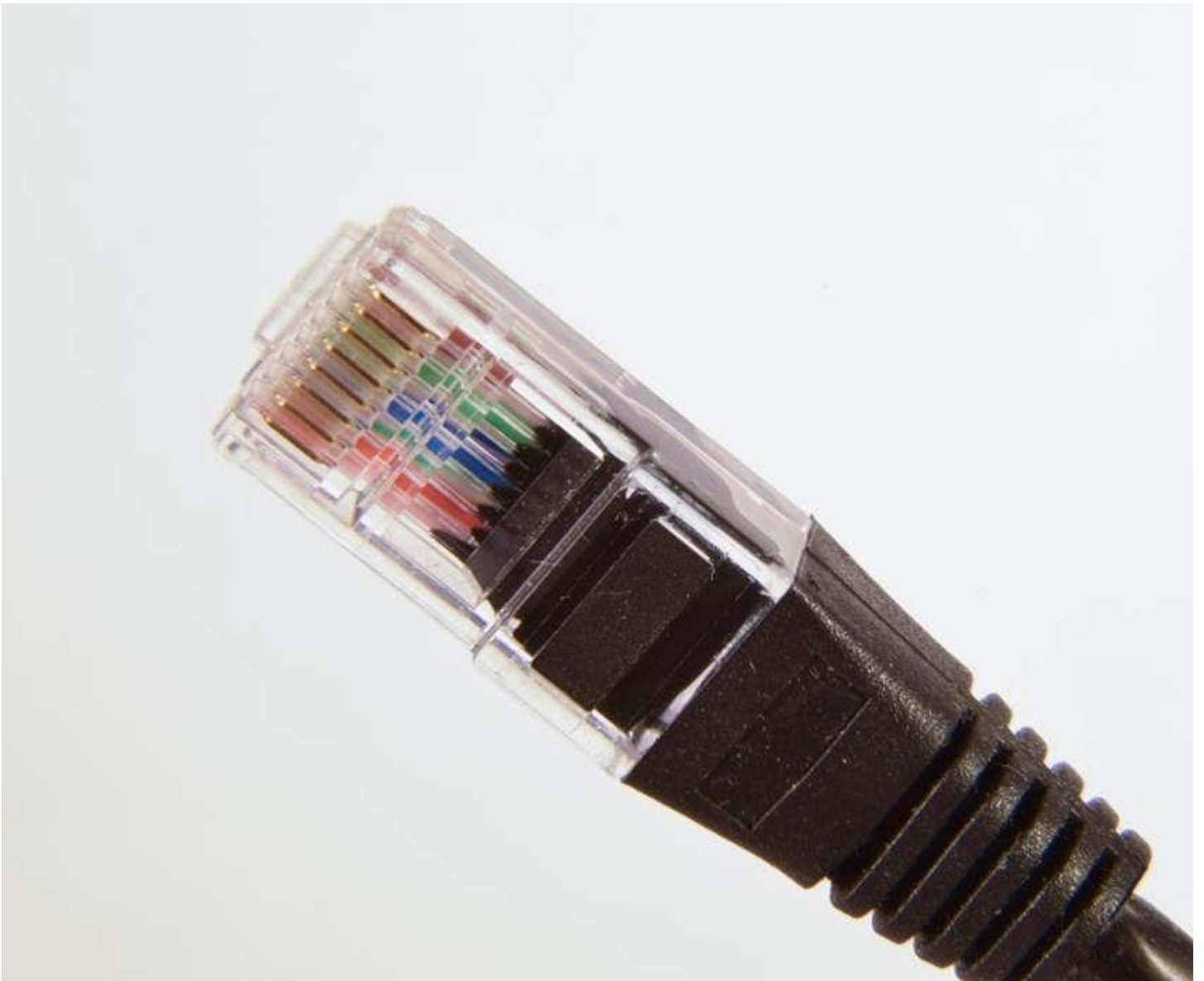
Category 3 Cable (UTP)Category 5 and 5e Cable (UTP)Category 6 Cable (STP)

UTP cable is usually terminated with an RJ-45 connector. The TIA/EIA-568 standard describes the wire color codes to pin assignments (pinouts) for Ethernet cables.

As shown in the figure, the RJ-45 connector is the male component, crimped at the end of the cable.

an RJ45 connector and a cable terminated with an RJ45 connector

RJ-45 UTP Plugs



The socket, shown in the figure, is the female component of a network device, wall, cubicle partition outlet, or patch panel. When terminated improperly, each cable is a potential source of physical layer performance degradation.

front and side view of an RJ45 UTP socket, including the color code for wire termination

RJ-45 UTP Sockets



This figure shows an example of a badly terminated UTP cable. This bad connector has wires that are exposed, untwisted, and not entirely covered by the sheath.

poorly terminated UTP cable showing untwisted wires extending outside of the RJ45 connector

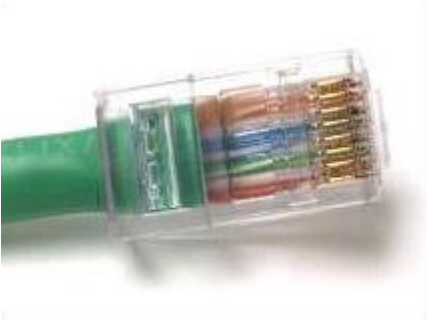
Poorly Terminated UTP Cable



The next figure shows a properly terminated UTP cable. It is a good connector with wires that are untwisted only to the extent necessary to attach the connector.

properly termination UTP cable showing the cable jacket extending into the RJ45 connector enough to be crimped securely with all eight wires reaching the end of the connector

Properly Terminated UTP Cable



Note: Improper cable termination can impact transmission performance.

4.4.3

Straight-through and Crossover UTP Cables

Different situations may require UTP cables to be wired according to different wiring conventions. This means that the individual wires in the cable have to be connected in different orders to different sets of pins in the RJ-45 connectors.

The following are the main cable types that are obtained by using specific wiring conventions:

- **Ethernet Straight-through** - The most common type of networking cable. It is commonly used to interconnect a host to a switch and a switch to a router.
- **Ethernet Crossover** - A cable used to interconnect similar devices. For example, to connect a switch to a switch, a host to a host, or a router to a router. However, crossover cables are now considered legacy as NICs use medium-dependent interface crossover (auto-MDIX) to automatically detect the cable type and make the internal connection.

Note: Another type of cable is a rollover cable, which is Cisco proprietary. It is used to connect a workstation to a router or switch console port.

Using a crossover or straight-through cable incorrectly between devices may not damage the devices, but connectivity and communication between the devices will not take place. This is a common error and checking that the device connections are correct should be the first troubleshooting action if connectivity is not achieved.

The figure identifies the individual wire pairs for the T568A and T568B standards.

The figure shows diagrams of the T568A and T568B wiring standards. Each shows the correct pinout for the individual wire pairs. Each color wire pair is numbered and consists of a solid color wire and a white striped wire. Pair 1 is blue, pair 2 is orange, pair 3 is green, and pair 4 is brown. Each standard alternates between white striped and solid wires. For the T568A standard, the blue pair are terminated at pins 4 and 5, the orange pair are terminated at pins 3 and 6, the green pair is terminated at pins 1 and 2, and the brown pair is terminated at pins 7 and 8. For the T568B standard, the blue pair is terminated at pins 4 and 5, the orange pair is terminated at pins 1 and 2, the green pair is termination at pins 3 and 6, and the brown pair is terminated at pins 7 and 8.

T568A and T568B Standards

1234567812345678

Pair 2Pair 2Pair 4Pair 1Pair 3T568AT568BPair 3Pair 4Pair 1

The table shows the UTP cable type, related standards, and typical application of these cables.

Cable Types and Standards

Cable Type	Standard	Application
Ethernet Straight-through	Both ends T568A or both ends T568B	Connects a network host to a network device such as a switch or hub
Ethernet Crossover	One end T568A, other end T568B	Connects two network hosts Connects two network intermediary devices (switch to switch or router to router)
Rollover	Cisco proprietary	Connects a workstation serial port to a router console port, using an adapter

4.4.4

Activity - Cable Pinouts

For this activity, correctly order the wire colors to a TIA/EIA cable pinout. Select a wire case color by clicking it. Then click a wire to apply that casing to it.

Select the pin case, then the cable pin to apply the casing.

T568A Pinout

CheckShow MeReset

Select the pin case, then the cable pin to apply the casing.

T568B Pinout

CheckShow MeReset

4.5.1

Properties of Fiber-Optic Cabling

As you have learned, fiber-optic cabling is the other type of cabling used in networks. Because it is expensive, it is not as commonly used at the various types of copper cabling. But fiber-optic cabling has certain properties that make it the best option in certain situations, which you will discover in this topic.

Optical fiber cable transmits data over longer distances and at higher bandwidths than any other networking media. Unlike copper wires, fiber-optic cable can transmit signals with less attenuation and is completely immune to EMI and RFI. Optical fiber is commonly used to interconnect network devices.

Optical fiber is a flexible, but extremely thin, transparent strand of very pure glass, not much bigger than a human hair. Bits are encoded on the fiber as light impulses. The fiber-optic cable acts as a waveguide, or “light pipe,” to transmit light between the two ends with minimal loss of signal.

As an analogy, consider an empty paper towel roll with the inside coated like a mirror. It is a thousand meters in length, and a small laser pointer is used to send Morse code signals at the speed of light. Essentially that is how a fiber-optic cable operates, except that it is smaller in diameter and uses sophisticated light technologies.



4.5.2

Types of Fiber Media

Fiber-optic cables are broadly classified into two types:

- Single-mode fiber (SMF)
- Multimode fiber (MMF)

Click each button for an illustration and explanation of each type.
Single-Mode Fiber

Multimode Fiber

Single-Mode Fiber

SMF consists of a very small core and uses expensive laser technology to send a single ray of light, as shown in the figure. SMF is popular in long-distance situations spanning hundreds of kilometers, such as those required in long haul telephony and cable TV applications.

A cross-section of a single-mode fiber optic cable consisting of a center glass core of 9 microns in diameter, surrounded by a glass cladding of 125 microns in diameter, surrounded by a polymeric coating. An x-ray vision sideview shows that this type of cable construction produces a single straight path for the light.

Glass Core diameter = 9 micrometer (µm)Glass Cladding 125 microns diameterPolymeric Coating Produces single straight path for light

One of the highlighted differences between MMF and SMF is the amount of dispersion. Dispersion refers to the spreading out of a light pulse over time. Increased dispersion means increased loss of signal strength. MMF has a greater dispersion than SMF. That is why MMF can only travel up to 500 meters before signal loss.

4.5.3

Fiber-Optic Cabling Usage

Fiber-optic cabling is now being used in four types of industry:

- **Enterprise Networks** - Used for backbone cabling applications and interconnecting infrastructure devices
- **Fiber-to-the-Home (FTTH)** - Used to provide always-on broadband services to homes and small businesses
- **Long-Haul Networks** - Used by service providers to connect countries and cities
- **Submarine Cable Networks** - Used to provide reliable high-speed, high-capacity solutions capable of surviving in harsh undersea environments at up to transoceanic distances. Search the internet for “submarine cables telegeography map” to view various maps online.

Our focus in this course is the use of fiber within the enterprise.

4.5.4

Fiber-Optic Connectors

An optical-fiber connector terminates the end of an optical fiber. A variety of optical-fiber connectors are available. The main differences among the types of connectors are dimensions and methods of coupling. Businesses decide on the types of connectors that will be used, based on their equipment.

Note: Some switches and routers have ports that support fiber-optic connectors through a small form-factor pluggable (SFP) transceiver. Search the internet for various types of SFPs.

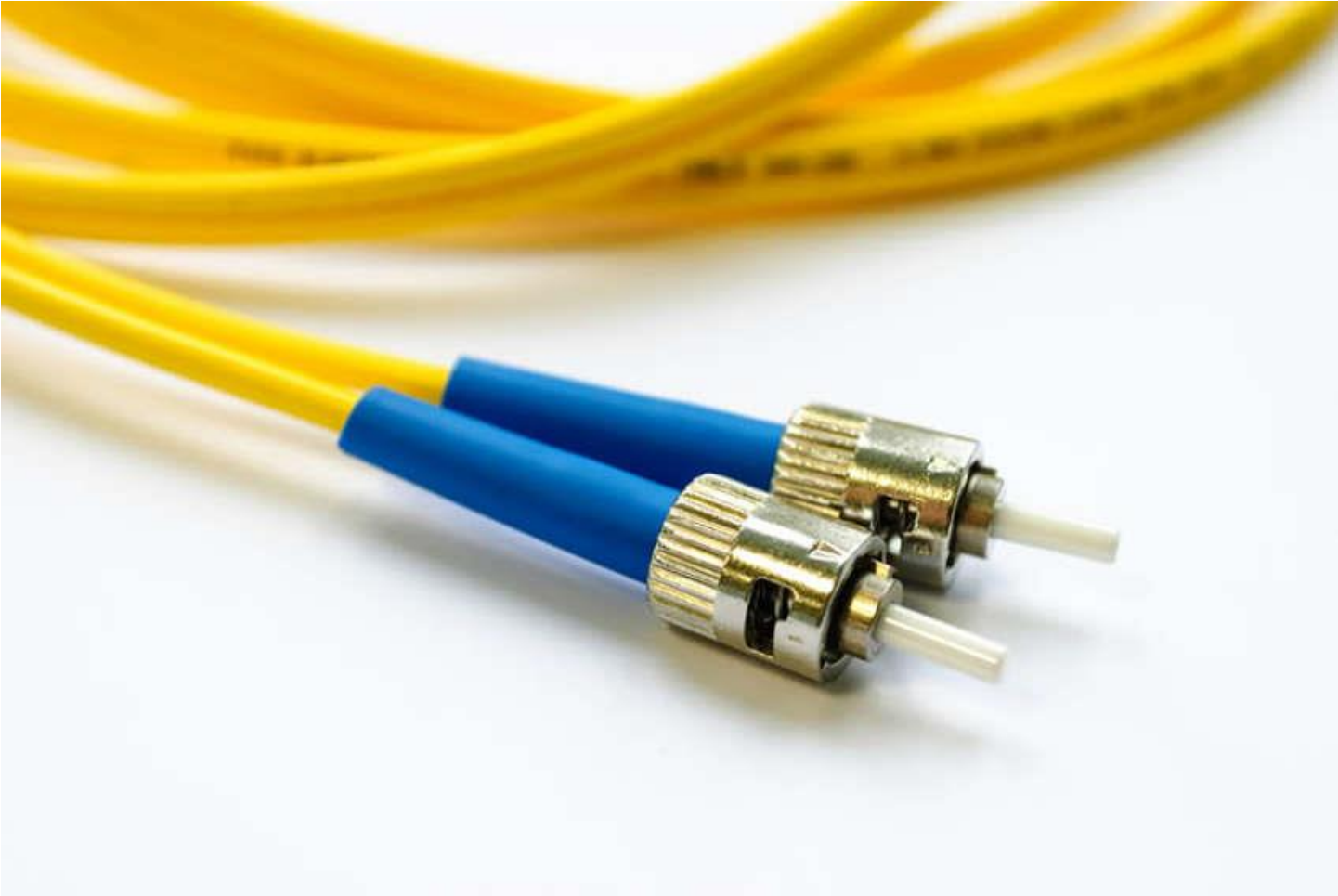
Click each fiber-optic connector type for an image and more information.
Straight-Tip (ST) Connectors

Subscriber Connector (SC) Connectors

Lucent Connector (LC) Simplex Connectors

Duplex Multimode LC Connectors

ST connectors were one of the first connector types used. The connector locks securely with a 'twist-on/twist-off' bayonet-style mechanism.



Until recently, light could only travel in one direction over optical fiber. Two fibers were required to support the full duplex operation. Therefore, fiber-optic patch cables bundle together two optical fiber cables and terminate them with a pair of standard, single-fiber connectors. Some fiber connectors accept both the transmitting and receiving fibers in a single connector known as a duplex connector, as shown in the Duplex Multimode LC Connector in the figure. BX standards such as 100BASE-BX use different wavelengths for sending and receiving over a single fiber.

4.5.5

Fiber Patch Cords

Fiber patch cords are required for interconnecting infrastructure devices. The use of color distinguishes between single-mode and multimode patch cords. A yellow jacket is for single-mode fiber cables and orange (or aqua) for multimode fiber cables.

Click each fiber patch cord for an image.
SC-SC Multimode Patch Cord

LC-LC Single-Mode Patch Cord

ST-LC Multimode Patch Cord

SC-ST Single-Mode Patch Cord



Note: Fiber cables should be protected with a small plastic cap when not in use.

4.5.6

Fiber versus Copper

There are many advantages to using fiber-optic cable compared to copper cables. The table highlights some of these differences.

At present, in most enterprise environments, optical fiber is primarily used as backbone cabling for high-traffic, point-to-point connections between data distribution facilities. It is also used for the interconnection of buildings in multi-building campuses. Because fiber-optic cables do not conduct electricity and have a low signal loss, they are well suited for these uses.

UTP and Fiber-Optic Cabling Comparison

Table caption		
Implementation Issues	UTP Cabling	Fiber-Optic Cabling
Bandwidth supported	10 Mb/s - 10 Gb/s	10 Mb/s - 100 Gb/s
Distance	Relatively short (1 - 100 meters)	Relatively long (1 - 100,000 meters)

Table caption		
Implementation Issues	UTP Cabling	Fiber-Optic Cabling
Immunity to EMI and RFI	Low	High (Completely immune)
Immunity to electrical hazards	Low	High (Completely immune)
Media and connector costs	Lowest	Highest
Installation skills required	Lowest	Highest
Safety precautions	Lowest	Highest

4.6.1

Properties of Wireless Media

You may be taking this course using a tablet or a smart phone. This is only possible due to wireless media, which is the third way to connect to the physical layer of a network.

Wireless media carry electromagnetic signals that represent the binary digits of data communications using radio or microwave frequencies.

Wireless media provide the greatest mobility options of all media, and the number of wireless-enabled devices continues to increase. Wireless is now the primary way users connect to home and enterprise networks.

These are some of the limitations of wireless:

- **Coverage area** - Wireless data communication technologies work well in open environments. However, certain construction materials used in buildings and structures, and the local terrain, will limit the effective coverage.
- **Interference** - Wireless is susceptible to interference and can be disrupted by such common devices as household cordless phones, some types of fluorescent lights, microwave ovens, and other wireless communications.
- **Security** - Wireless communication coverage requires no access to a physical strand of media. Therefore, devices and users, not authorized for access to the network, can gain access to the transmission. Network security is a major component of wireless network administration.
- **Shared medium** - WLANs operate in half-duplex, which means only one device can send or receive at a time. The wireless medium is shared amongst all wireless users. Many users accessing the WLAN simultaneously results in reduced bandwidth for each user.

Although wireless is increasing in popularity for desktop connectivity, copper and fiber are the most popular physical layer media for deployment of intermediary network devices, such as routers and switches.

4.6.2

Types of Wireless Media

The IEEE and telecommunications industry standards for wireless data communications cover both the data link and physical layers. In each of these standards, physical layer specifications are applied to areas that include the following:

- Data to radio signal encoding
- Frequency and power of transmission
- Signal reception and decoding requirements
- Antenna design and construction

These are the wireless standards:

- **Wi-Fi (IEEE 802.11)** - Wireless LAN (WLAN) technology, commonly referred to as Wi-Fi. WLAN uses a contention-based protocol known as carrier sense multiple access/collision avoidance (CSMA/CA). The wireless NIC must first listen before transmitting to determine if the radio channel is clear. If another wireless device is transmitting, then the NIC must wait until the channel is clear. Wi-Fi is a trademark of the Wi-Fi Alliance. Wi-Fi is used with certified WLAN devices based on the IEEE 802.11 standards.
- **Bluetooth (IEEE 802.15)** - This is a wireless personal area network (WPAN) standard, commonly known as “Bluetooth.” It uses a device pairing process to communicate over distances from 1 to 100 meters.
- **WiMAX (IEEE 802.16)** - Commonly known as Worldwide Interoperability for Microwave Access (WiMAX), this wireless standard uses a point-to-multipoint topology to provide wireless broadband access.
- **Zigbee (IEEE 802.15.4)** - Zigbee is a specification used for low-data rate, low-power communications. It is intended for applications that require short-range, low data-rates and long battery life. Zigbee is typically used for industrial and Internet of Things (IoT) environments such as wireless light switches and medical device data collection.

Note: Other wireless technologies such as cellular and satellite communications can also provide data network connectivity. However, these wireless technologies are out of scope for this module.

4.6.3

Wireless LAN

A common wireless data implementation is enabling devices to connect wirelessly via a LAN. In general, a WLAN requires the following network devices:

- **Wireless Access Point (AP)** - These concentrate the wireless signals from users and connect to the existing copper-based network infrastructure, such as Ethernet. Home and small business wireless routers integrate the functions of a router, switch, and access point into one device, as shown in the figure.
- **Wireless NIC adapters** - These provide wireless communication capability to network hosts.

As the technology has developed, a number of WLAN Ethernet-based standards have emerged. When purchasing wireless devices, ensure compatibility and interoperability.

The benefits of wireless data communications technologies are evident, especially the savings on costly premises wiring and the convenience of host mobility. Network administrators must develop and apply stringent security policies and processes to protect WLANs from unauthorized access and damage.

Cisco Meraki MX64W



5.1.1

Binary and IPv4 Addresses

IPv4 addresses begin as binary, a series of only 1s and 0s. These are difficult to manage, so network administrators must convert them to decimal. This topic shows you a few ways to do this.

Binary is a numbering system that consists of the digits 0 and 1 called bits. In contrast, the decimal numbering system consists of 10 digits consisting of the digits 0 – 9.

Binary is important for us to understand because hosts, servers, and network devices use binary addressing. Specifically, they use binary IPv4 addresses, as shown in the figure, to identify each other.

There is a central router with two LANs directly connected and one WAN connected to a cloud. Each LAN has a switch and a PC. The WAN has one PC. Each device has an IPv4 address that is in dotted binary notation instead of dotted decimal notation.

PC1PC211000000.10101000.00001010.0000101011000000.10101000.00001011.0000101011000000.10101000.00001010.0000000111000000.10101000.00001011.00000001G0/0/0G0/0/111010001.10100101.11001000.11100001PC1R1PC2
LAN A Network Address
11000000.10101000.00001010.00000000 /24LAN B Network Address
11000000.10101000.00001011.00000000 /24

Each address consists of a string of 32 bits, divided into four sections called octets. Each octet contains 8 bits (or 1 byte) separated with a dot. For example, PC1 in the figure is assigned IPv4 address 11000000.10101000.00001010.00001010. Its default gateway address would be that of R1 Gigabit Ethernet interface 11000000.10101000.00001010.00000001.

Binary works well with hosts and network devices. However, it is very challenging for humans to work with.

For ease of use by people, IPv4 addresses are commonly expressed in dotted decimal notation. PC1 is assigned the IPv4 address 192.168.10.10, and its default gateway address is 192.168.10.1, as shown in the figure.

This diagram is the same as the first, a central router with two LANs and a WAN connected to a cloud. This has the same devices as the first diagram; however, instead of having the IPv4 addressing in binary, it is in dotted decimal notation.

PC1PC2192.168.10.10192.168.11.10192.168.10.1192.168.11.1G0/0/0G0/0/1209.165.200.225PC1R1PC2
LAN A Network Address
192.168.10.0 /24LAN B Network Address
192.168.11.0 /24

For a solid understanding of network addressing, it is necessary to know binary addressing and gain practical skills converting between binary and dotted decimal IPv4 addresses. This section will cover how to convert between base two (binary) and base 10 (decimal) numbering systems.

5.1.2

Video - Converting Between Binary and Decimal Numbering Systems

Click Play in the figure for a video demonstrating how to convert between binary and decimal numbering systems.

Play Video

5.1.3

Binary Positional Notation

Learning to convert binary to decimal requires an understanding of positional notation. Positional notation means that a digit represents different values depending on the “position” the digit occupies in the sequence of numbers. You already know the most common numbering system, the decimal (base 10) notation system.

The decimal positional notation system operates as described in the table.

Radix10101010Position in Number3210Calculate(103)(102)(101)(100)Position value1000100101				
Radix	10	10	10	10
Position in Number	3	2	1	0
Calculate	(10 ³)	(10 ²)	(10 ¹)	(10 ⁰)
Position value	1000	100	10	1

The following bullets describe each row of the table.

- Row 1, Radix is the number base. Decimal notation is based on 10, therefore the radix is 10.
- Row 2, Position in number considers the position of the decimal number starting with, from right to left, 0 (1st position), 1 (2nd position), 2 (3rd position), 3 (4th position). These numbers also represent the exponential value use to calculate the positional value in the 4th row.
- Row 3 calculates the positional value by taking the radix and raising it by the exponential value of its position in row 2.
Note: n⁰ is = 1.
- Row 4 positional value represents units of thousands, hundreds, tens, and ones.

To use the positional system, match a given number to its positional value. The example in the table illustrates how positional notation is used with the decimal number 1234.

ThousandsHundredsTensOnesPositional Value1000100101Decimal Number (1234)1234Calculate1 x 10002 x 1003 x 104 x 1Add them up...1000+ 200+ 30+ 4Result1,234				
	Thousands	Hundreds	Tens	Ones
Positional Value	1000	100	10	1
Decimal Number (1234)	1	2	3	4
Calculate	1 x 1000	2 x 100	3 x 10	4 x 1
Add them up...	1000	+ 200	+ 30	+ 4
Result	1,234			

In contrast, the binary positional notation operates as described in the table.

Radix22222222Position in Number76543210Calculate(27)(26)(25)(24)(23)(22)(21)(20)Position value1286432168421								
Radix	2	2	2	2	2	2	2	2
Position in Number	7	6	5	4	3	2	1	0
Calculate	(2 ⁷)	(2 ⁶)	(2 ⁵)	(2 ⁴)	(2 ³)	(2 ²)	(2 ¹)	(2 ⁰)
Position value	128	64	32	16	8	4	2	1

The following bullets describe each row of the table.

- Row 1, Radix is the number base. Binary notation is based on 2, therefore the radix is 2.
- Row 2, Position in number considers the position of the binary number starting with, from right to left, 0 (1st position), 1 (2nd position), 2 (3rd position), 3 (4th position). These numbers also represent the exponential value use to calculate the positional value in the 4th row.
- Row 3 calculates the positional value by taking the radix and raising it by the exponential value of its position in row 2.
Note: n⁰ is = 1.
- Row 4 positional value represents units of ones, twos, fours, eights, etc.

The example in the table illustrates how a binary number 11000000 corresponds to the number 192. If the binary number had been 10101000, then the corresponding decimal number would be 168.

Positional Value1286432168421Binary Number (11000000)11000000Calculate1 x 1281 x 640 x 320 x 160 x 80 x 40 x 20 x 1Add Them Up..128+ 64+ 0+ 0+ 0+ 0+ 0+ 0Result192								
Positional Value	128	64	32	16	8	4	2	1
Binary Number (11000000)	1	1	0	0	0	0	0	0
Calculate	1 x 128	1 x 64	0 x 32	0 x 16	0 x 8	0 x 4	0 x 2	0 x 1
Add Them Up..	128	+ 64	+ 0	+ 0	+ 0	+ 0	+ 0	+ 0
Result	192							

5.1.4

Check Your Understanding - Binary Number System

Check your understanding of binary number systems by choosing the correct answer to the following questions.

1. Which is the binary equivalent to the 192.168.11.10 IP address?

11000000.11000000.00001011.00001010
11000000.10101000.00001011.00001010
11000000.10101000.00001010.00001011
11000000.10101000.00001011.00010010
2. Which of the following is the binary equivalent to the 172.16.31.30 IP address?

11000000.00010000.00011111.00011110

10101000.00010000.00011111.00011110
10101100.00010000.00011110.00011110
10101100.00010000.00011111.00011110

CheckShow MeReset

5.1.5

Convert Binary to Decimal

To convert a binary IPv4 address to its dotted decimal equivalent, divide the IPv4 address into four 8-bit octets. Next apply the binary positional value to the first octet binary number and calculate accordingly.

For example, consider that 11000000.10101000.00001011.00001010 is the binary IPv4 address of a host. To convert the binary address to decimal, start with the first octet, as shown in the table. Enter the 8-bit binary number under the positional value of row 1 and then calculate to produce the decimal number 192. This number goes into the first octet of the dotted decimal notation.

Positional Value1286432168421Binary Number (11000000)11000000Calculate1286432168421Add Them Up...128+ 64+ 0+ 0+ 0+ 0+ 0+ 0+ 0Result192								
Positional Value	128	64	32	16	8	4	2	1
Binary Number (11000000)	1	1	0	0	0	0	0	0
Calculate	128	64	32	16	8	4	2	1
Add Them Up...	128	+ 64	+ 0	+ 0	+ 0	+ 0	+ 0	+ 0
Result	192							

Next convert the second octet of 10101000 as shown in the table. The resulting decimal value is 168, and it goes into the second octet.

Positional Value1286432168421Binary Number (11000000)10101000Calculate1286432168421Add Them Up...128+ 0+ 32+ 0+ 8+ 0+ 0+ 0+ 0Result168								
Positional Value	128	64	32	16	8	4	2	1
Binary Number (10101000)	1	0	1	0	1	0	0	0
Calculate	128	64	32	16	8	4	2	1
Add Them Up...	128	+ 0	+ 32	+ 0	+ 8	+ 0	+ 0	+ 0
Result	168							

Convert the third octet of 00001011 as shown in the table.

Positional Value1286432168421Binary Number (11000000)00001011Calculate1286432168421Add Them Up...0+ 0+ 0+ 0+ 8+ 0+ 2+ 1Result11								
Positional Value	128	64	32	16	8	4	2	1
Binary Number (00001011)	0	0	0	0	1	0	1	1
Calculate	128	64	32	16	8	4	2	1
Add Them Up...	0	+ 0	+ 0	+ 0	+ 8	+ 0	+ 2	+ 1
Result	11							

Convert the fourth octet of 00001010 as shown in the table. This completes the IP address and produces **192.168.11.10**.

Positional Value1286432168421Binary Number (11000000)00001010Calculate1286432168421Add Them Up...0+ 0+ 0+ 0+ 8+ 0+ 2+ 0Result10								
Positional Value	128	64	32	16	8	4	2	1
Binary Number (00001010)	0	0	0	0	1	0	1	0
Calculate	128	64	32	16	8	4	2	1
Add Them Up...	0	+ 0	+ 0	+ 0	+ 8	+ 0	+ 2	+ 0
Result	10							

5.1.6

Activity - Binary to Decimal Conversions

Instructions

This activity allows you to practice 8-bit binary to decimal conversion as much as necessary. We recommend that you work with this tool until you are able to do the conversion without error. Convert the binary number shown in the octet to its decimal value.

Enter decimal answer below.

Decimal Value								
Base	2	2	2	2	2	2	2	2
Exponent	7	6	5	4	3	2	1	0
Position	128	64	32	16	8	4	2	1
Bit	0	0	0	1	0	0	0	0

Binary Number

CheckNew NumberShow MeReset

5.1.7

Decimal to Binary Conversion

It is also necessary to understand how to convert a dotted decimal IPv4 address to binary. A useful tool is the binary positional value table.

Click each position starting at 128 and work your way from left to right to the 1 position.

128
64
32
16
8
4
2
1

Is the decimal number of the octet (n) equal to or greater than the most-significant bit (**128**)?

- If no, then enter binary **0** in the **128** positional value.
- If yes, then add a binary **1** in the **128** positional value and subtract **128** from the decimal number.

The graphic shows a table that has 8 columns for one Byte or 8 bits. The top row shows the values from left to right; 128, 64, 32, 16, 8, 4, 2, 1. To the left of this top line are the words Positional Value. The bottom row is blank, but field under 128 is highlighted when selecting the 128 tab. Above the table is a flow chart that has

only one proposition $n \geq 128$. No is to the left and Yes is to the right. There is a line going from the proposition in the center, one line to the left and one line to the right. The line moves across the top and then once it clears the chart, the line points straight down. On the No side or the left is a box with Add zero in it and a new line points to the highlighted field. On the right or Yes side the box has Add one. The line then continues and points to the highlighted field under 128. Under the Add one box is another line that points down to another box that has $n - 128$. Where the original number will subtract 128 from it and then consider the next column with 64.

1286432168421
Non ≥ 128 Yes Positional Value Add 0 Add 1 $n - 128$

5.1.8

Decimal to Binary Conversion Example

To help understand the process, consider the IP address **192.168.10.11**.

The first octet number **192** is converted to binary using the previously explained positional notation process.

It is possible to bypass the process of subtraction with easier or smaller decimal numbers. For instance, notice that it is fairly easy to calculate the third octet converted to a binary number without actually going through the subtraction process ($8 + 2 = 10$). The binary value of the third octet is **00001010**.

The fourth octet is 11 ($8 + 2 + 1$). The binary value of the fourth octet is **00001011**.

Converting between binary and decimal may seem challenging at first, but with practice it should become easier over time.

Click each step to see the conversion of the IP address of **192.168.10.11** into binary.

- Step 1
- Step 2
- Step 3
- Step 4
- Step 5
- Step 6
- Step 7
- Step 8
- Step 9
- Step 10
- Step 11

Is the first octet number **192** equal to or greater than the high-order bit **128**?

- Yes it is, therefore add a **1** to the high-order positional value to represent **128**.
- Subtract **128** from **192** to produce a remainder of **64**.

When selecting the Step 1 button, the graphic states Example: 192.168.10.11 with 192 in a different color. To the Right of that is a diamond that states: $192 \geq 128$. There is a Yes on the right side of the diamond. A table is shown below that contains 8 columns for one Byte or 8 bits. The top row shows the values from left to right: 128, 64, 32, 16, 8, 4, 2, and 1 with the words Positional Value to the left. The bottom row field under 128 is highlighted. Above the table, from the flow chart diamond with Yes is to the right is line that moves across the top and then once it clears the chart, the line points straight down to a box that has Add one. The line then continues under the chart and points to the highlighted field under 128. Under the Add one box is another line that points down to another box that has $192 - 128 = 64$. There is also a 1 under the 128 in the highlighted field; the other columns are still blank on this line.

11286432168421
Example: **192.168.10.11** Yes Positional Value $192 \geq 128$ $192 - 128 = 64$ Add 1

5.1.9

Activity - Decimal to Binary Conversions

Instructions

This activity allows you to practice decimal conversions to 8-bit binary values. We recommend that you work with this tool until you are able to do the conversion without error. Convert the decimal number shown in the Decimal Value row to its binary bits.

Decimal Value	253							
Base	2	2	2	2	2	2	2	2
Exponent	7	6	5	4	3	2	1	0
Position	128	64	32	16	8	4	2	1
Bit								

CheckNew NumberShow MeReset

5.1.10

Activity - Binary Game

This is a fun way to learn binary numbers for networking.

Game Link: <https://learningnetwork.cisco.com/docs/DOC-1803>

You will need to log in to cisco.com to use this link. It will be necessary to create an account if you do not already have one.

There are also a variety of free mobile binary games. Search for "binary game" in your app store.

5.1.11

IPv4 Addresses

As mentioned in the beginning of this topic, routers and computers only understand binary, while humans work in decimal. It is important for you to gain a thorough understanding of these two numbering systems and how they are used in networking.

Click each button to contrast the dotted decimal address and the 32-bit address.

Dotted Decimal Address

Octets

32-bit Address

192.168.10.10 is an IP address that is assigned to a computer.

The graphic shows the numbers 192.168.10.10 with the binary in an orange box around the dotted decimal numbers 192.168.10.10. 11000000 is under 192 in the first octet, 10101000 under 168 in the second octet, 00001010 under 10 in the third octet, and 00001010 under the last 10 in the fourth octet.

110000001010100000001010000010101921681010...110000001010100000001010000010101921681010...

5.2.1

Hexadecimal and IPv6 Addresses

Now you know how to convert binary to decimal and decimal to binary. You need that skill to understand IPv4 addressing in your network. But you are just as likely to be using IPv6 addresses in your network. To understand IPv6 addresses, you must be able to convert hexadecimal to decimal and vice versa.

1. Convert the decimal number to 8-bit binary strings.
2. Divide the binary strings in groups of four starting from the rightmost position.
3. Convert each four binary numbers into their equivalent hexadecimal digit.

The example provides the steps for converting **168** to hexadecimal.

For example, **168** converted into hex using the three-step process.

1. **168** in binary is **10101000**.
2. **10101000** in two groups of four binary digits is **1010** and **1000**.
3. **1010**is hex **A** and **1000** is hex **8**.

Answer: **168** is **A8** in hexadecimal.

5.2.4

Hexadecimal to Decimal Conversion

Converting hexadecimal numbers to decimal values is also straightforward. Follow the steps listed:

1. Convert the hexadecimal number to 4-bit binary strings.
2. Create 8-bit binary grouping starting from the rightmost position.
3. Convert each 8-bit binary grouping into their equivalent decimal digit.

This example provides the steps for converting **D2** to decimal.

1. **D2** in 4-bit binary strings is **1101** and **0010**.
2. **1101** and **0010** is **11010010** in an 8-bit grouping.
3. **11010010** in binary is equivalent to **210** in decimal.

Answer: **D2** in hexadecimal is **210** in decimal.

6.1.1

The Data Link Layer

The data link layer of the OSI model (Layer 2), as shown in the figure, prepares network data for the physical network. The data link layer is responsible for network interface card (NIC) to network interface card communications. The data link layer does the following:

- Enables upper layers to access the media. The upper layer protocol is completely unaware of the type of media that is used to forward the data.
- Accepts data, usually Layer 3 packets (i.e., IPv4 or IPv6), and encapsulates them into Layer 2 frames.
- Controls how data is placed and received on the media.
- Exchanges frames between endpoints over the network media.
- Receives encapsulated data, usually Layer 3 packets, and directs them to the proper upper-layer protocol.
- Performs error detection and rejects any corrupt frame.

The image shows the seven layers of the OSI model in order from the top down, Layer 7, Application, Layer 6 Presentation, Layer 5 Session, Layer 4 Transport, Layer 3 Network, Layer 2 Data Link, Layer 1 Physical. The data link layer is highlighted and next to the data link layer is text stating The data link layer prepares network data for the physical network. An arrow representing traffic flow from a user sitting above the application layer is drawn over the OSI model down to a router and ending at a network cloud.

7654321

NetworkThe data link layer prepares network data for the physical network

In computer networks, a node is a device that can receive, create, store, or forward data along a communications path. A node can be either an end device such as a laptop or mobile phone, or an intermediary device such as an Ethernet switch.

Without the data link layer, network layer protocols such as IP, would have to make provisions for connecting to every type of media that could exist along a delivery path. Additionally, every time a new network technology or medium was developed IP, would have to adapt.

The figure displays an example of how the data link layer adds Layer 2 Ethernet destination and source NIC information to a Layer 3 packet. It would then convert this information to a format supported by the physical layer (i.e., Layer 1).

The image shows a user at a desktop computer with an IP address of 192.168.1.110 sending traffic from its NIC to the NIC of a Web Server with the IP address of 192.168.1.5. A box with the label L2, representing the Layer 2 header and a box with label L3 representing the Layer 3 header are shown by the user. An arrow from the L2 box points to a larger rectangular box with the text destination NIC and Source NIC to represent the destination Layer 2 address and the destination Layer 3 address. To the right of the L2 header is a rectangular box called L3 IP Packet which has text indicating the source IP address of 192.168.1.110 and the destination IP address of 192.168.1.5.

L2 HeaderL3 IP Packet

PC1
192.168.1.110Web Server
192.168.1.5
L3 = Layer 3

L2 = Layer 2

6.1.2

IEEE 802 LAN/MAN Data Link Sublayers

IEEE 802 LAN/MAN standards are specific to Ethernet LANs, wireless LANs (WLAN), wireless personal area networks (WPAN) and other types of local and metropolitan area networks. The IEEE 802 LAN/MAN data link layer consists of the following two sublayers:

- **Logical Link Control (LLC)** - This IEEE 802.2 sublayer communicates between the networking software at the upper layers and the device hardware at the lower layers. It places information in the frame that identifies which network layer protocol is being used for the frame. This information allows multiple Layer 3 protocols, such as IPv4 and IPv6, to use the same network interface and media.
- **Media Access Control (MAC)** – Implements this sublayer (IEEE 802.3, 802.11, or 802.15) in hardware. It is responsible for data encapsulation and media access control. It provides data link layer addressing and it is integrated with various physical layer technologies.

The figure shows the two sublayers (LLC and MAC) of the data link layer.

The image is of a table with three rows for Network, Data Link, and Physical layers. The top row of the table has Network and Network Layer Protocol. The second row has Data link and is further split into two rows, one for LLC Sublayer and one for MAC Sublayer. The LLC Sublayer has a column stating LLC Sublayer - IEEE 802.2. The MAC Sublayer has three columns stating Ethernet IEEE 802.3, WLAN 802.11, and WPAN IEEE 802.15. Under the Ethernet 802.3 column, between the MAC sublayer and the Physical layer it states Various Ethernet standards for Fast Ethernet, Gigabit Ethernet, etc. Under the WLAN IEEE 802.11 column, between the MAC sublayer and the Physical layer it states Various WLAN standards for different types of wireless communications. Under the WPAN column between the MAC sublayer and the Physical layer it states Various WPAN standards for Bluetooth, RFID, etc.

The LLC sublayer takes the network protocol data, which is typically an IPv4 or IPv6 packet, and adds Layer 2 control information to help deliver the packet to the destination node.

The MAC sublayer controls the NIC and other hardware that is responsible for sending and receiving data on the wired or wireless LAN/MAN medium.

The MAC sublayer provides data encapsulation:

- **Frame delimiting** - The framing process provides important delimiters to identify fields within a frame. These delimiting bits provide synchronization between the transmitting and receiving nodes.
- **Addressing** - Provides source and destination addressing for transporting the Layer 2 frame between devices on the same shared medium.
- **Error detection** - Includes a trailer used to detect transmission errors.

The MAC sublayer also provides media access control, allowing multiple devices to communicate over a shared (half-duplex) medium. Full-duplex communications do not require access control.

6.1.3

Providing Access to Media

Each network environment that packets encounter as they travel from a local host to a remote host can have different characteristics. For example, an Ethernet LAN usually consists of many hosts contending for access on the network medium. The MAC sublayer resolves this. With serial links the access method may only consist of a direct connection between only two devices, usually two routers. Therefore, they do not require the techniques employed by the IEEE 802 MAC sublayer.

Router interfaces encapsulate the packet into the appropriate frame. A suitable media access control method is used to access each link. In any given exchange of network layer packets, there may be numerous data link layers and media transitions.

At each hop along the path, a router performs the following Layer 2 functions:

1. Accepts a frame from a medium
2. De-encapsulates the frame
3. Re-encapsulates the packet into a new frame
4. Forwards the new frame appropriate to the medium of that segment of the physical network

Press play to view the animation. The router in the figure has an Ethernet interface to connect to the LAN and a serial interface to connect to the WAN. As the router processes frames, it will use data link layer services to receive the frame from one medium, de-encapsulate it to the Layer 3 PDU, re-encapsulate the PDU into a new frame, and place the frame on the medium of the next link of the network.

This animation illustrates how a Layer 2 frame is encapsulated and de-encapsulated as it travels in a network. A user sends an Ethernet frame to the default gateway router. When the router receives the frame, it decapsulates the Ethernet frame to read its content. It then processes the Layer 3 packet and makes a routing decision to choose a serial interface as the exit interface to the next hop IP address. The router then re-encapsulate the packet into a new Layer 2 frame and sends it to the next router across the serial link.

Serial Connection	
The data link layer is responsible for controlling the transfer of frames across the media.	
Ethernet Connection	

6.1.4

Data Link Layer Standards

Data link layer protocols are generally not defined by Request for Comments (RFCs), unlike the protocols of the upper layers of the TCP/IP suite. The Internet Engineering Task Force (IETF) maintains the functional protocols and services for the TCP/IP protocol suite in the upper layers, but they do not define the functions and operation of the TCP/IP network access layer.

Engineering organizations that define open standards and protocols that apply to the network access layer (i.e., the OSI physical and data link layers) include the following:

- Institute of Electrical and Electronics Engineers (IEEE)
- International Telecommunication Union (ITU)
- International Organization for Standardization (ISO)
- American National Standards Institute (ANSI)

The logos for these organizations are shown in the figure.

Engineering Organization Logos



6.1.5

6.2.1

Physical and Logical Topologies

As you learned in the previous topic, the data link layer prepares network data for the physical network. It must know the logical topology of a network in order to be able to determine what is needed to transfer frames from one device to another. This topic explains the ways in which the data link layer works with different logical network topologies.

The topology of a network is the arrangement, or the relationship, of the network devices and the interconnections between them.

There are two types of topologies used when describing LAN and WAN networks:

- **Physical topology** – Identifies the physical connections and how end devices and intermediary devices (i.e, routers, switches, and wireless access points) are interconnected. The topology may also include specific device location such as room number and location on the equipment rack. Physical topologies are usually point-to-point or star.
- **Logical topology** - Refers to the way a network transfers frames from one node to the next. This topology identifies virtual connections using device interfaces and Layer 3 IP addressing schemes.

The data link layer "sees" the logical topology of a network when controlling data access to the media. It is the logical topology that influences the type of network framing and media access control used.

The figure displays a sample **physical** topology for a small sample network.

The physical network topology shows six rooms, each highlighted in a light yellow box, with various networking devices and cabling. On the left side is the server room labeled room 2158. It contains a router labeled R1 mounted on rack 1 shelf 1 with six cable connections. A cable at the top connects to a cloud labeled Internet. A cable to the left connects to a switch labeled S1 mounted on rack 1 shelf 2. S1 is connected to three servers: a web server mounted on rack 2 shelf 1, an email server mounted on rack 2 shelf 2, and a file server mounted on rack 2 shelf 3. A cable connected to the bottom of R1 connects to a switch labeled S2 mounted on rack 1 shelf 3. S2 has two connections leading to a printer and a PC in the IT office labeled room 2159. R1 has three cables to the right connected to three switches located in room 2124. The top switch is labeled S3 and mounted on rack 1 shelf 1. The

middle switch is labeled S4 and mounted on rack 1 shelf 2. The bottom switch is labeled S5 and mounted on rack 1 shelf 3. S3 has a cable on the left connected to a laptop in a room labeled class 1 room 2125. S4 has a cable on the left connected to a laptop in a room labeled class 2 room 2126. S5 has a cable on the left connected to a laptop in a room labeled class 3 room 2127.

Physical Topology

R1S1S2S3S4S5

InternetEmail Server
Rack 2
Shelf 2Web Server
Rack 2
Shelf 1File Server
Rack 2
Shelf 3Rack 1
Shelf 2Rack 1
Shelf 1Rack 1
Shelf 2Rack 1
Shelf 1Rack 1
Shelf 3Rack 1
Shelf 3**Server Room: Rm: 2158IT Office: Rm: 2159Class 1: Rm: 2125Class 2: Rm: 2126Class 3: Rm: 2127Rm: 2124**

The next figure displays a sample **logical** topology for the same network.

The logical network topology shows devices, port labels, and the network addressing scheme. In the middle of the picture is a router labeled R1. A port labeled G0/0/0 connects to a cloud at the top labeled Internet. A port labeled G0/2/0 connects at the left to a switch labeled S1 at port G0/1. S1 is connected to three servers. S1 and the servers are highlighted in a light yellow circle with the network 192.168.10.0/24 written at the top. Port F0/1 on S1 connects to a web server. Port F0/2 on S1 connects to an email server. Port F0/3 on S1 connects to a file server. Port G0/0/1 on R1 connects at the bottom to a switch labeled S2. S2 connects to a printer and a PC, all of which are highlighted in a light yellow circle with the network 192.168.11.0/24 written on the bottom. At the right of R1 are three additional connections, each connecting to a switch at port G0/1 which is then connected to a laptop at port F0/1. Each switch and laptop are highlighted in yellow and the network address shown. Port G0/0/1 of R1 connects at the top to a switch labeled S3 on network 192.168.100.0. Port G0/1/0 of R1 connects in the middle to a switch labeled S4 on network 192.169.101.0. Port G0/1/1 on R1 connects at the bottom to a switch labeled S5 on network 192.168.102.0. R1 connects to the Internet on interface G0/0/0.

Logical Topology

R1F0/1F0/2F0/3G0/0/0G0/1G0/0/1G0/1G0/1/0G0/1/1G0/1S1S2S3S4S5G0/2/0G0/2/1G0/1G0/1

InternetEmail ServerWeb ServerFile Server**Network**
192.168.10.0/24Network
192.168.11.0/24Network 192.168.100.0/24Network 192.168.101.0/24Network 192.168.102.0/24

6.2.2

WAN Topologies

The figures illustrate how WANs are commonly interconnected using three common physical WAN topologies.

Click each button for more information.
Point-to-Point

Hub and Spoke

Mesh

This is the simplest and most common WAN topology. It consists of a permanent link between two endpoints.

The image shows two routers with a single line, representing a link, connecting them.

A hybrid is a variation or combination of any topologies. For example, a partial mesh is a hybrid topology in which some, but not all, end devices are interconnected.

6.2.3

Point-to-Point WAN Topology

Physical point-to-point topologies directly connect two nodes, as shown in the figure. In this arrangement, two nodes do not have to share the media with other hosts. Additionally, when using a serial communications protocol such as Point-to-Point Protocol (PPP), a node does not have to make any determination about whether an incoming frame is

destined for it or another node. Therefore, the logical data link protocols can be very simple, as all frames on the media can only travel to or from the two nodes. The node places the frames on the media at one end and those frames are taken from the media by the node at the other end of the point-to-point circuit.

The image shows a point-to-point network example consisting of two routers, labeled Node 1 and Node 2, each connected to a network cloud over WAN links.

Node 1Node 2Network

Point-to-point topologies are limited to two nodes.

Note: A point-to-point connection over Ethernet requires the device to determine if the incoming frame is destined for this node.

A source and destination node may be indirectly connected to each other over some geographical distance using multiple intermediary devices. However, the use of physical devices in the network does not affect the logical topology, as illustrated in the figure. In the figure, adding intermediary physical connections may not change the logical topology. The logical point-to-point connection is the same.

The image shows a point-to-point network example consisting of two routers, labeled Source Node and Destination Node, each connected to a network cloud over WAN links. The two routers are shown sending frames to the network cloud.

Source
NodeFrameFrameFrameFrameDestination
Node

6.2.4

LAN Topologies

In multiaccess LANs, end devices (i.e., nodes) are interconnected using star or extended star topologies, as shown in the figure. In this type of topology, end devices are connected to a central intermediary device, in this case, an Ethernet switch. An **extended star** extends this topology by interconnecting multiple Ethernet switches. The star and extended topologies are easy to install, very scalable (easy to add and remove end devices), and easy to troubleshoot. Early star topologies interconnected end devices using Ethernet hubs.

At times there may be only two devices connected on the Ethernet LAN. An example is two interconnected routers. This would be an example of Ethernet used on a point-to-point topology.

Legacy LAN Topologies

Early Ethernet and legacy Token Ring LAN technologies included two other types of topologies:

- Bus** - All end systems are chained to each other and terminated in some form on each end. Infrastructure devices such as switches are not required to interconnect the end devices. Legacy Ethernet networks were often bus topologies using coax cables because it was inexpensive and easy to set up.
- Ring** - End systems are connected to their respective neighbor forming a ring. The ring does not need to be terminated, unlike in the bus topology. Legacy Fiber Distributed Data Interface (FDDI) and Token Ring networks used ring topologies.

The figures illustrate how end devices are interconnected on LANs. It is common for a straight line in networking graphics to represent an Ethernet LAN including a simple star and an extended star.

comparison of four physical topologies: star, extended star, bus, and ring

Physical Topologies

Star TopologyExtended Star TopologyBus TopologyRing Topology

6.2.5

Half and Full Duplex Communication

Understanding duplex communication is important when discussing LAN topologies because it refers to the direction of data transmission between two devices. There are two common modes of duplex.

Half-duplex communication

Both devices can transmit and receive on the media but cannot do so simultaneously. WLANs and legacy bus topologies with Ethernet hubs use the half-duplex mode. Half-duplex allows only one device to send or receive at a time on the shared medium. Click play in the figure to see the animation showing half-duplex communication.

half duplex communication between a server and a hub



Full-duplex communication

Both devices can simultaneously transmit and receive on the shared media. The data link layer assumes that the media is available for transmission for both nodes at any time. Ethernet switches operate in full-duplex mode by default, but they can operate in half-duplex if connecting to a device such as an Ethernet hub. Click play in the figure to see the animation showing full-duplex communication.

full duplex communication between a server and a hub



In summary, half-duplex communications restrict the exchange of data to one direction at a time. Full-duplex allows the sending and receiving of data to happen simultaneously.

It is important that two interconnected interfaces, such as a host NIC and an interface on an Ethernet switch, operate using the same duplex mode. Otherwise, there will be a duplex mismatch creating inefficiency and latency on the link.

6.2.6

Access Control Methods

Ethernet LANs and WLANs are examples of multiaccess networks. A multiaccess network is a network that can have two or more end devices attempting to access the network simultaneously.

Some multiaccess networks require rules to govern how devices share the physical media. There are two basic access control methods for shared media:

- Contention-based access
- Controlled access

Contention-based access

In contention-based multiaccess networks, all nodes are operating in half-duplex, competing for the use of the medium. However, only one device can send at a time. Therefore, there is a process if more than one device transmits at the same time. Examples of contention-based access methods include the following:

- Carrier sense multiple access with collision detection (CSMA/CD) used on legacy bus-topology Ethernet LANs
- Carrier sense multiple access with collision avoidance (CSMA/CA) used on Wireless LANs

The image shows three PCs connected to an Ethernet hub. Two of the PCs are sending frames simultaneously.



Controlled access

In a controlled-based multiaccess network, each node has its own time to use the medium. These deterministic types of legacy networks are inefficient because a device must wait its turn to access the medium. Examples of multiaccess networks that use controlled access include the following:

- Legacy Token Ring
- Legacy ARCNET

The image shows four PCs connected to a token ring network.

Token Ring Network

Each node must wait for its turn to access the network medium.

Note: Today, Ethernet networks operate in full-duplex and do not require an access method.

6.2.7

Contention-Based Access - CSMA/CD

Examples of contention-based access networks include the following:

- Wireless LAN (uses CSMA/CA)
- Legacy bus-topology Ethernet LAN (uses CSMA/CD)
- Legacy Ethernet LAN using a hub (uses CSMA/CD)

These networks operate in half-duplex mode, meaning only one device can send or receive at a time. This requires a process to govern when a device can send and what happens when multiple devices send at the same time.

If two devices transmit at the same time, a collision will occur. For legacy Ethernet LANs, both devices will detect the collision on the network. This is the collision detection (CD) portion of CSMA/CD. The NIC compares data transmitted with data received, or by recognizing that the signal amplitude is higher than normal on the media. The data sent by both devices will be corrupted and will need to be resent.

Click each button for an image and description of the CSMA/CD process in legacy Ethernet LANs that use a hub.
PC1 Sends a Frame

The Hub Receives the Frame

The Hub Sends the Frame

PC1 has an Ethernet frame to send to PC3. The PC1 NIC needs to determine if any device is transmitting on the medium. If it does not detect a carrier signal (in other words, it is not receiving transmissions from another device), it will assume the network is available to send.

The PC1 NIC sends the Ethernet Frame when the medium is available, as shown in the figure.

The image shows three PCs (PC1, PC2, and PC3) connected to an Ethernet hub. PC1 is sending a frame. A text box above PC1 reads The medium is available so I will send the Ethernet frame to PC3.

Frame The medium is available so I will send the Ethernet frame to PC3.

6.2.8

Contention-Based Access - CSMA/CA

Another form of CSMA used by IEEE 802.11 WLANs is carrier sense multiple access/collision avoidance (CSMA/CA).

CMSA/CA uses a method similar to CSMA/CD to detect if the media is clear. CMSA/CA uses additional techniques. In wireless environments it may not be possible for a device to detect a collision. CMSA/CA does not detect collisions but attempts to avoid them by waiting before transmitting. Each device that transmits includes the time duration that it needs for the transmission. All other wireless devices receive this information and know how long the medium will be unavailable.

In the figure, if host A is receiving a wireless frame from the access point, hosts B, and C will also see the frame and how long the medium will be unavailable.

The image shows a wireless network consisting of an access point and three laptops, laptop A, B, and C. Laptop A has a text box that reads Im receiving this wireless frame. Laptop B has text box that reads I see in the wireless frame that the is channel is unavailable for a specific amount of time so I cannot send. Laptop C has a text box that reads I see in the wireless frame that the channel is going to be unavailable for a specific amount of time so I cannot send.

I'm receiving this wireless frame. I see in the wireless frame that the channel is going to be unavailable for a specific amount of time so I cannot send. I see in the wireless frame that the channel is unavailable for a specific amount of time so I cannot send.

After a wireless device sends an 802.11 frame, the receiver returns an acknowledgment so that the sender knows the frame arrived.

Whether it is an Ethernet LAN using hubs, or a WLAN, contention-based systems do not scale well under heavy media use.

Note: Ethernet LANs using switches do not use a contention-based system because the switch and the host NIC operate in full-duplex mode.

6.3.1

The Frame

This topic discusses in detail what happens to the data link frame as it moves through a network. The information appended to a frame is determined by the protocol being used.

The data link layer prepares the encapsulated data (usually an IPv4 or IPv6 packet) for transport across the local media by encapsulating it with a header and a trailer to create a frame.

The data link protocol is responsible for NIC-to-NIC communications within the same network. Although there are many different data link layer protocols that describe data link layer frames, each frame type has three basic parts:

- Header
- Data
- Trailer

Unlike other encapsulation protocols, the data link layer appends information in the form of a trailer at the end of the frame.

All data link layer protocols encapsulate the data within the data field of the frame. However, the structure of the frame and the fields contained in the header and trailer vary according to the protocol.

There is no one frame structure that meets the needs of all data transportation across all types of media. Depending on the environment, the amount of control information needed in the frame varies to match the access control requirements of the media and logical topology. For example, a WLAN frame must include procedures for collision avoidance and therefore requires additional control information when compared to an Ethernet frame.

As shown in the figure, in a fragile environment, more controls are needed to ensure delivery. The header and trailer fields are larger as more control information is needed.

Two routers communicating over a wireless WAN through a satellite connection

FrameFrame

Greater effort is needed to ensure delivery. This means higher overhead and slower transmission rates.

6.3.2

Frame Fields

Framing breaks the stream into decipherable groupings, with control information inserted in the header and trailer as values in different fields. This format gives the physical signals a structure that are by recognized by nodes and decoded into packets at the destination.

The generic frame fields are shown in the figure. Not all protocols include all these fields. The standards for a specific data link protocol define the actual frame format.

The image shows a data packet encapsulated by a data link header and a data link trailer. The data link header is broken down to for fields: Frame start, addressing, type, and control. The data link trailer is broken down to two fields: Error detection and frame stop.

Frame fields include the following:

- **Frame start and stop indicator flags** - Used to identify the beginning and end limits of the frame.
- **Addressing** - Indicates the source and destination nodes on the media.
- **Type** - Identifies the Layer 3 protocol in the data field.
- **Control** - Identifies special flow control services such as quality of service (QoS). QoS gives forwarding priority to certain types of messages. For example, voice over IP (VoIP) frames normally receive priority because they are sensitive to delay.
- **Data** - Contains the frame payload (i.e., packet header, segment header, and the data).
- **Error Detection** - Included after the data to form the trailer.

Data link layer protocols add a trailer to the end of each frame. In a process called error detection, the trailer determines if the frame arrived without error. It places a logical or mathematical summary of the bits that comprise the frame in the trailer. The data link layer adds error detection because the signals on the media could be subject to interference, distortion, or loss that would substantially change the bit values that those signals represent.

A transmitting node creates a logical summary of the contents of the frame, known as the cyclic redundancy check (CRC) value. This value is placed in the frame check sequence (FCS) field to represent the contents of the frame. In the Ethernet trailer, the FCS provides a method for the receiving node to determine whether the frame experienced transmission errors.

6.3.3

Layer 2 Addresses

The data link layer provides the addressing used in transporting a frame across a shared local media. Device addresses at this layer are referred to as physical addresses. Data link layer addressing is contained within the frame header and specifies the frame destination node on the local network. It is typically at the beginning of the frame, so the NIC can quickly determine if it matches its own Layer 2 address before accepting the rest of the frame. The frame header may also contain the source address of the frame.

Unlike Layer 3 logical addresses, which are hierarchical, physical addresses do not indicate on what network the device is located. Rather, the physical address is unique to the specific device. A device will still function with the same Layer 2 physical address even if the device moves to another network or subnet. Therefore, Layer 2 addresses are only used to connect devices within the same shared media, on the same IP network.

The figures illustrate the function of the Layer 2 and Layer 3 addresses. As the IP packet travels from host-to-router, router-to-router, and finally router-to-host, at each point along the way the IP packet is encapsulated in a new data link frame. Each data link frame contains the source data link address of the NIC sending the frame, and the destination data link address of the NIC receiving the frame.

Click each button for more information.

- Host-to-Router
- Router-to-Router
- Router-to-Host

The source host encapsulates the Layer 3 IP packet in a Layer 2 frame. In the frame header, the host adds its Layer 2 address as the source and the Layer 2 address for R1 as the destination.

The image shows a network consisting of a source PC, router R1, router R2, and a final destination web server. A text box representing the NIC of each device interface is shown. PC1 has IP address 192.168.1.100. The server has IP address 172.16.1.99. PC1 is sending an L2 frame with a Destination NIC address of R1 and a source NIC address of its own NIC. The frame is encapsulating a L3 IP packet with a Source IP address of 192.168.1.110 and a destination IP address of 172.16.1.99.

R1R2



Original SourceFinal DestinationPC1 192.168.1.110Web Server 172.16.1.99L2 = Layer 2L3 = Layer 3L2 HeaderL3 IP Packet

The data link layer address is only used for local delivery. Addresses at this layer have no meaning beyond the local network. Compare this to Layer 3, where addresses in the packet header are carried from the source host to the destination host, regardless of the number of network hops along the route.

If the data must pass onto another network segment, an intermediary device, such as a router, is necessary. The router must accept the frame based on the physical address and de-encapsulate the frame in order to examine the hierarchical address, which is the IP address. Using the IP address, the router can determine the network location of the destination device and the best path to reach it. When it knows where to forward the packet, the router then creates a new frame for the packet, and the new frame is sent on to the next network segment toward its final destination.

6.3.4

LAN and WAN Frames

Ethernet protocols are used by wired LANs. Wireless communications fall under WLAN (IEEE 802.11) protocols. These protocols were designed for multiaccess networks.

WANs traditionally used other types of protocols for various types of point-to-point, hub-spoke, and full-mesh topologies. Some of the common WAN protocols over the years have included:

- Point-to-Point Protocol (PPP)
- High-Level Data Link Control (HDLC)
- Frame Relay
- Asynchronous Transfer Mode (ATM)
- X.25

These Layer 2 protocols are now being replaced in the WAN by Ethernet.

In a TCP/IP network, all OSI Layer 2 protocols work with IP at OSI Layer 3. However, the Layer 2 protocol used depends on the logical topology and the physical media.

Each protocol performs media access control for specified Layer 2 logical topologies. This means that a number of different network devices can act as nodes that operate at the data link layer when implementing these protocols. These devices include the NICs on computers as well as the interfaces on routers and Layer 2 switches.

The Layer 2 protocol that is used for a particular network topology is determined by the technology used to implement that topology. The technology used is determined by the size of the network, in terms of the number of hosts and the geographic scope, and the services to be provided over the network.

A LAN typically uses a high bandwidth technology capable of supporting large numbers of hosts. The relatively small geographic area of a LAN (a single building or a multi-building campus) and its high density of users make this technology cost-effective.

However, using a high bandwidth technology is usually not cost-effective for WANs that cover large geographic areas (cities or multiple cities, for example). The cost of the long-distance physical links and the technology used to carry the signals over those distances typically results in lower bandwidth capacity.

The difference in bandwidth normally results in the use of different protocols for LANs and WANs.

Data link layer protocols include:

- Ethernet
- 802.11 Wireless
- Point-to-Point Protocol (PPP)
- High-Level Data Link Control (HDLC)
- Frame Relay

Click Play to see an animation of examples of Layer 2 protocols.

a depiction of a network consisting of interconnected LANs and WANs

Ethernet Encapsulation

This module starts with a discussion of Ethernet technology including an explanation of MAC sublayer and the Ethernet frame fields.

Ethernet is one of two LAN technologies used today, with the other being wireless LANs (WLANs). Ethernet uses wired communications, including twisted pair, fiber-optic links, and coaxial cables.

Ethernet operates in the data link layer and the physical layer. It is a family of networking technologies defined in the IEEE 802.2 and 802.3 standards. Ethernet supports data bandwidths of the following:

- 10 Mbps
- 100 Mbps
- 1000 Mbps (1 Gbps)
- 10,000 Mbps (10 Gbps)
- 40,000 Mbps (40 Gbps)
- 100,000 Mbps (100 Gbps)

As shown in the figure, Ethernet standards define both the Layer 2 protocols and the Layer 1 technologies.

Ethernet and the OSI Model

802.2802.3Ethernet

Ethernet is defined by data link layer and physical layer protocols.

Data Link Sublayers

IEEE 802 LAN/MAN protocols, including Ethernet, use the following two separate sublayers of the data link layer to operate. They are the Logical Link Control (LLC) and the Media Access Control (MAC), as shown in the figure.

Recall that LLC and MAC have the following roles in the data link layer:

- **LLC Sublayer** - This IEEE 802.2 sublayer communicates between the networking software at the upper layers and the device hardware at the lower layers. It places information in the frame that identifies which network layer protocol is being used for the frame. This information allows multiple Layer 3 protocols, such as IPv4 and IPv6, to use the same network interface and media.
- **MAC Sublayer** - This sublayer (IEEE 802.3, 802.11, or 802.15 for example) is implemented in hardware and is responsible for data encapsulation and media access control. It provides data link layer addressing and is integrated with various physical layer technologies.

The diagram shows the OSI network, data link, and physical layers. It also shows the data link layer LLC and MAC sublayers and various LAN/WAN protocols. At the top of the diagram is the network layer and the network layer protocol. Below that is the data link layer and its sublayers. The top sublayer is the LLC sublayer as specified in IEEE 802.2. Next is the MAC sublayer with three columns representing different types of network technologies. The first column is Ethernet IEEE 802.3 at the upper part of the MAC sublayer. Below this are various Ethernet standards for Fast Ethernet, Gigabit Ethernet, etc. that span across the lower part of the MAC sublayer and the entire OSI physical layer. The next column is WLAN IEEE 802.11 at the upper part of the MAC sublayer. Below this are the various WLAN standards for different types of wireless communications that span across the lower part of the MAC sublayer and the entire OSI physical layer. The last column is WPAN IEEE 802.15 at the upper part of the MAC sublayer. Below this are various WPAN standards for Bluetooth, RFID, etc. that span across the lower part of the MAC sublayer and the entire OSI physical layer.

MAC Sublayer

The MAC sublayer is responsible for data encapsulation and accessing the media.

Data Encapsulation

IEEE 802.3 data encapsulation includes the following:

- **Ethernet frame** - This is the internal structure of the Ethernet frame.
- **Ethernet Addressing** - The Ethernet frame includes both a source and destination MAC address to deliver the Ethernet frame from Ethernet NIC to Ethernet NIC on the same LAN.
- **Ethernet Error detection** - The Ethernet frame includes a frame check sequence (FCS) trailer used for error detection.

Accessing the Media

As shown in the figure, the IEEE 802.3 MAC sublayer includes the specifications for different Ethernet communications standards over various types of media including copper and fiber.

The diagram is showing various Ethernet standards in the MAC sublayer. At the top of the diagram is the network layer and the network layer protocol. Below that is the data link layer and its sublayers. The top sublayer is the IEEE 802.2 LLC sublayer. Next is the Ethernet IEEE 802.3 MAC sublayer. Below that are five columns with various Ethernet standards and media types that span the lower part of the MAC sublayer and the entire OSI physical layer. From left to right the columns are: IEEE 802.3u Fast Ethernet; IEEE 802.3z Gigabit Ethernet over Fiber; IEEE 802.ab Gigabit Ethernet over Copper; IEEE 802.3ae 10 Gigabit Ethernet over Fiber; and Etc.

Ethernet Standards in the MAC Sublayer

Recall that legacy Ethernet using a bus topology or hubs, is a shared, half-duplex medium. Ethernet over a half-duplex medium uses a contention-based access method, carrier sense multiple access/collision detection (CSMA/CD) This ensures that only one device is transmitting at a time. CSMA/CD allows multiple devices to share the same half-duplex medium, detecting a collision when more than one device attempts to transmit simultaneously. It also provides a back-off algorithm for retransmission.

Ethernet LANs of today use switches that operate in full-duplex. Full-duplex communications with Ethernet switches do not require access control through CSMA/CD.

7.1.4

Ethernet Frame Fields

The minimum Ethernet frame size is 64 bytes and the expected maximum is 1518 bytes. This includes all bytes from the destination MAC address field through the frame check sequence (FCS) field. The preamble field is not included when describing the size of the frame.

Note: The frame size may be larger if additional requirements are included, such as VLAN tagging. VLAN tagging is beyond the scope of this course.

Any frame less than 64 bytes in length is considered a “collision fragment” or “runt frame” and is automatically discarded by receiving stations. Frames with more than 1500 bytes of data are considered “jumbo” or “baby giant frames”.

If the size of a transmitted frame is less than the minimum, or greater than the maximum, the receiving device drops the frame. Dropped frames are likely to be the result of collisions or other unwanted signals. They are considered invalid. Jumbo frames are usually supported by most Fast Ethernet and Gigabit Ethernet switches and NICs.

The figure shows each field in the Ethernet frame. Refer to the table for more information about the function of each field.

The diagram shows the fields of an Ethernet frame. From left to right the fields and their length are: Preamble and SFD, 8 bytes; destination MAC address, 6 bytes; source MAC address, 6 bytes; type / length, 2 bytes; data, 46 - 1500 bytes; and F C S, 4 bytes. Excluding the first field, the total number of bytes in the remaining fields is between 64 – 1518 bytes.

Ethernet Frame Fields

bytes64-1518 bytes

8 bytes6 bytes6 bytes2 bytes46-1500 bytes4

Ethernet Frame Fields Detail

Table caption	
Field	Description
Preamble and Start Frame Delimiter Fields	The Preamble (7 bytes) and Start Frame Delimiter (SFD), also called the Start of Frame (1 byte), fields are used for synchronization between the sending and receiving devices. These first eight bytes of the frame are used to get the attention of the receiving nodes. Essentially, the first few bytes tell the receivers to get ready to receive a new frame.
Destination MAC Address Field	This 6-byte field is the identifier for the intended recipient. As you will recall, this address is used by Layer 2 to assist devices in determining if a frame is addressed to them. The address in the frame is compared to the MAC address in the device. If there is a match, the device accepts the frame. Can be a unicast, multicast or broadcast address.
Source MAC Address Field	This 6-byte field identifies the originating NIC or interface of the frame.
Type / Length	This 2-byte field identifies the upper layer protocol encapsulated in the Ethernet frame. Common values are, in hexadecimal, 0x800 for IPv4, 0x86DD for IPv6 and 0x806 for ARP. Note: You may also see this field referred to as EtherType, Type, or Length.
Data Field	This field (46 - 1500 bytes) contains the encapsulated data from a higher layer, which is a generic Layer 3 PDU, or more commonly, an IPv4 packet. All frames must be at least 64 bytes long. If a small packet is encapsulated, additional bits called a pad are used to increase the size of the frame to this minimum size.
Frame Check Sequence Field	The Frame Check Sequence (FCS) field (4 bytes) is used to detect errors in a frame. It uses a cyclic redundancy check (CRC). The sending device includes the results of a CRC in the FCS field of the frame. The receiving device receives the frame and generates a CRC to look for errors. If the calculations match, no error occurred. Calculations that do not match are an indication that the data has changed; therefore, the frame is dropped. A change in the data could be the result of a disruption of the electrical signals that represent the bits.

7.2.1

MAC Address and Hexadecimal

In networking, IPv4 addresses are represented using the decimal base ten number system and the binary base 2 number system. IPv6 addresses and Ethernet addresses are represented using the hexadecimal base sixteen number system. To understand hexadecimal, you must first be very familiar with binary and decimal.

The hexadecimal numbering system uses the numbers 0 to 9 and the letters A to F.

An Ethernet MAC address consists of a 48-bit binary value. Hexadecimal is used to identify an Ethernet address because a single hexadecimal digit represents four binary bits. Therefore, a 48-bit Ethernet MAC address can be expressed using only 12 hexadecimal values.

The figure compares the equivalent decimal and hexadecimal values for binary 0000 to 1111.

The figure is three columns showing the decimal and hexadecimal equivalents of select 4-bit binary numbers. From left to right, the column headings are: decimal, binary, and hexadecimal. Each column has 16 rows below the header.

Decimal and Binary Equivalents of 0 to F Hexadecimal

015345678910111213142100001111001101000101011001111000100110101011110011011110001000010F3456789ABCDE21

DecimalBinaryHexadecimal

Given that 8 bits (one byte) is a common binary grouping, binary 00000000 to 11111111 can be represented in hexadecimal as the range 00 to FF, as shown in the next figure.

The figure is three columns showing the decimal and hexadecimal equivalents of select 8-bit binary numbers. From left to right, the column headings are: decimal, binary, and hexadecimal. Each column has 18 rows below the header.

Selected Decimal, Binary, and Hexadecimal Equivalents

02553571015321281922022402181664640000 00001111 11110000 00110000 01010000 01110000 10100000 11110010 00001000 00001100 00001100 10101111 00000000 00100000 00010000 10000001 00000100 00000000 01100000 010000FF0305070A0F2080C0CAF002010810400604

DecimalBinaryHexadecimal

When using hexadecimal, leading zeroes are always displayed to complete the 8-bit representation. For example, in the table, the binary value 0000 1010 is shown in hexadecimal as 0A.

Hexadecimal numbers are often represented by the value preceded by the value preceded by **0x** (e.g., 0x73) to distinguish between decimal and hexadecimal values in documentation.

Hexadecimal may also be represented by a subscript 16, or the hex number followed by an H (e.g., 73H).

You may have to convert between decimal and hexadecimal values. If such conversions are required, convert the decimal or hexadecimal value to binary, and then to convert the binary value to either decimal or hexadecimal as appropriate.

7.2.2

Ethernet MAC Address

In an Ethernet LAN, every network device is connected to the same, shared media. The MAC address is used to identify the physical source and destination devices (NICs) on the local network segment. MAC addressing provides a method for device identification at the data link layer of the OSI model.

An Ethernet MAC address is a 48-bit address expressed using 12 hexadecimal digits, as shown in the figure. Because a byte equals 8 bits, we can also say that a MAC address is 6 bytes in length.

The diagram shows that MAC address are composed of 48 bits total. These 48 bits can be divided into twelve 4-bit groupings, or 12 hex digits. Combining two hex digits together makes a byte, therefore the 48 bits is also equivalent to 6 bytes.

1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111

ByteByteByteByteByteByte= 6 bytesHexHexHexHexHexHexHexHexHexHexHexHex= 12 hex= 48 bits

All MAC addresses must be unique to the Ethernet device or Ethernet interface. To ensure this, all vendors that sell Ethernet devices must register with the IEEE to obtain a unique 6 hexadecimal (i.e., 24-bit or 3-byte) code called the organizationally unique identifier (OUI).

When a vendor assigns a MAC address to a device or Ethernet interface, the vendor must do as follows:

- Use its assigned OUI as the first 6 hexadecimal digits.
- Assign a unique value in the last 6 hexadecimal digits.

Therefore, an Ethernet MAC address consists of a 6 hexadecimal vendor OUI code followed by a 6 hexadecimal vendor-assigned value, as shown in the figure.

the first six hex digits of a MAC address (AKA first 6 hex digits or first 3 bytes) is the organizational unique identifier and the last six hex digits is vendor assigned

111

ByteByteByteByteByteByteHexHexHexHexHexHexOrganizational Unique Identifier (OUI)HexHexHexHexHexHexVendor AssignedHex

For example, assume that Cisco needs to assign a unique MAC address to a new device. The IEEE has assigned Cisco a OUI of **00-60-2F**. Cisco would then configure the device with a unique vendor code such as **3A-07-BC**. Therefore, the Ethernet MAC address of that device would be **00-60-2F-3A-07-BC**.

It is the responsibility of the vendor to ensure that none of its devices be assigned the same MAC address. However, it is possible for duplicate MAC addresses to exist because of mistakes made during manufacturing, mistakes made in some virtual machine implementation methods, or modifications made using one of several software tools. In any case, it will be necessary to modify the MAC address with a new NIC or make modifications via software.

7.2.3

Frame Processing

Sometimes the MAC address is referred to as a burned-in address (BIA) because the address is hard coded into read-only memory (ROM) on the NIC. This means that the address is encoded into the ROM chip permanently.

Note: On modern PC operating systems and NICs, it is possible to change the MAC address in software. This is useful when attempting to gain access to a network that filters based on BIA. Consequently, filtering or controlling traffic based on the MAC address is no longer as secure.

When the computer boots up, the NIC copies its MAC address from ROM into RAM. When a device is forwarding a message to an Ethernet network, the Ethernet header includes these:

- **Source MAC address** - This is the MAC address of the source device NIC.
- **Destination MAC address** - This is the MAC address of the destination device NIC.

Click Play in the animation to view the frame forwarding process.

The animation has a topology consisting of a switch with links to four host PCs labeled, H1, H2, H3 and H4. H1 says I need to send information to H3. A frame appears on the screen of the PC and an expanded view of the frame appears above the PC. The frame consists of the framing addressing and data. The destination address CC:CC:CC:CC:CC:CC, the source address AA:AA:AA:AA:AA:AA and the data part of the frame is encapsulated. The frame from H1 is forwarded to the switch. The switch then forwards the frame out every interface but the interface connected to H1. When H2 and H4 receive the frame and they say This is not addressed to me. I shall ignore it. When H3 receives the frame it says This is mine.

This is not addressed to me. I shall ignore it.

This is not addressed to me. I shall ignore it.

This is mine.

I need to send information to H3.

When a NIC receives an Ethernet frame, it examines the destination MAC address to see if it matches the physical MAC address that is stored in RAM. If there is no match, the device discards the frame. If there is a match, it passes the frame up the OSI layers, where the de-encapsulation process takes place.

Note: Ethernet NICs will also accept frames if the destination MAC address is a broadcast or a multicast group of which the host is a member.

Any device that is the source or destination of an Ethernet frame, will have an Ethernet NIC and therefore, a MAC address. This includes workstations, servers, printers, mobile devices, and routers.

7.2.4

Unicast MAC Address

In Ethernet, different MAC addresses are used for Layer 2 unicast, broadcast, and multicast communications.

A unicast MAC address is the unique address that is used when a frame is sent from a single transmitting device to a single destination device.

Click Play in the animation to view how a unicast frame is processed. In this example the destination MAC address and the destination IP address are both unicast.

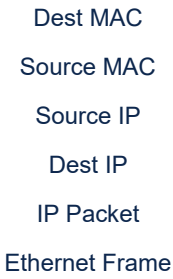
The animation shows a host with IPv4 address 192.168.1.5 (source) requesting a web page from a server at IPv4 unicast address 192.168.1.200. The animation has a topology consisting of a host PC named H1 linked to a switch. The switch has connections to three other host PCs and two servers. At the bottom of the animation is an expanded view of an ethernet frame. The frame consists of the destination MAC 00-07-E9-42-AC-28, source MAC 00-07-E9-63-CE-53, Source IP 192.168.1.5, destination IP address 192.168.1.200, user data and trailer. The IP packet portion of the frame is the source IP, destination IP address, and user data. In the animation, H1 says I need to send this frame to Server. A frame is sent from H1 to the switch. The switch then forwards the frame to the server with the IP and MAC matching the destination IP and MAC address.

Server

IP: 192.168.1.200
MAC: 00-07-E9-42-AC-28

Source Host

IP: 192.168.1.5
MAC: 00-07-E9-63-CE-53



In the example shown in the animation, a host with IPv4 address 192.168.1.5 (source) requests a web page from the server at IPv4 unicast address 192.168.1.200. For a unicast packet to be sent and received, a destination IP address must be in the IP packet header. A corresponding destination MAC address must also be present in the Ethernet frame header. The IP address and MAC address combine to deliver data to one specific destination host.

The process that a source host uses to determine the destination MAC address associated with an IPv4 address is known as Address Resolution Protocol (ARP). The process that a source host uses to determine the destination MAC address associated with an IPv6 address is known as Neighbor Discovery (ND).

Note: The source MAC address must always be a unicast.

7.2.5

Broadcast MAC Address

An Ethernet broadcast frame is received and processed by every device on the Ethernet LAN. The features of an Ethernet broadcast are as follows:

- It has a destination MAC address of FF-FF-FF-FF-FF-FF in hexadecimal (48 ones in binary).
- It is flooded out all Ethernet switch ports except the incoming port.
- It is not forwarded by a router.

If the encapsulated data is an IPv4 broadcast packet, this means the packet contains a destination IPv4 address that has all ones (1s) in the host portion. This numbering in the address means that all hosts on that local network (broadcast domain) will receive and process the packet.

Click Play in the animation to view how a broadcast frame is processed. In this example the destination MAC address and destination IP address are both broadcasts.

The animation shows a source host sending an IPv4 broadcast packet to all devices on its network. The animation has a topology consisting of a host PC named H1 linked to a switch. The switch has connections to three other host PCs and two servers. At the bottom of the animation is an expanded view of an ethernet frame. The frame consists of the destination MAC FF-FF-FF-FF-FF-FF, source MAC 00-07-E9-63-CE-53, Source IP 192.168.1.5, destination IP address 192.168.1.255, user data and trailer. The IP packet portion of the frame is the source IP, destination IP address, and user data. In the animation, H1 says I need to send data to all hosts on the network. A frame is sent from H1 to the switch. The switch then forwards the frame out all its interfaces except the one connected to H1. The three other PC hosts and the two servers receive the frames.

Destination
Host Group

Source Host
IP: 192.168.1.5
MAC: 00-07-E9-63-CE-53

Dest MAC

Source MAC

Source IP

Dest IP

IP Packet

Ethernet Frame

As shown in the animation, the source host sends an IPv4 broadcast packet to all devices on its network. The IPv4 destination address is a broadcast address, 192.168.1.255. When the IPv4 broadcast packet is encapsulated in the Ethernet frame, the destination MAC address is the broadcast MAC address of FF-FF-FF-FF-FF-FF in hexadecimal (48 ones in binary).

DHCP for IPv4 is an example of a protocol that uses Ethernet and IPv4 broadcast addresses.

However, not all Ethernet broadcasts carry an IPv4 broadcast packet. For example, ARP Requests do not use IPv4, but the ARP message is sent as an Ethernet broadcast.

7.2.6

Multicast MAC Address

An Ethernet multicast frame is received and processed by a group of devices on the Ethernet LAN that belong to the same multicast group. The features of an Ethernet multicast are as follows:

- There is a destination MAC address of 01-00-5E when the encapsulated data is an IPv4 multicast packet and a destination MAC address of 33-33 when the encapsulated data is an IPv6 multicast packet.
- There are other reserved multicast destination MAC addresses for when the encapsulated data is not IP, such as Spanning Tree Protocol (STP) and Link Layer Discovery Protocol (LLDP).
- It is flooded out all Ethernet switch ports except the incoming port, unless the switch is configured for multicast snooping.
- It is not forwarded by a router, unless the router is configured to route multicast packets.

If the encapsulated data is an IP multicast packet, the devices that belong to a multicast group are assigned a multicast group IP address. The range of IPv4 multicast addresses is 224.0.0.0 to 239.255.255.255. The range of IPv6 multicast addresses begins with ff00::/8. Because multicast addresses represent a group of addresses (sometimes called a host group), they can only be used as the destination of a packet. The source will always be a unicast address.

As with the unicast and broadcast addresses, the multicast IP address requires a corresponding multicast MAC address to deliver frames on a local network. The multicast MAC address is associated with, and uses addressing information from, the IPv4 or IPv6 multicast address.

Click Play in the animation to view how a multicast frame is processed. In this example, the destination MAC address and destination IP address are both multicasts.

The animation shows a source host sending a multicast frame to devices that belong to the multicast group. The animation has a topology consisting of a host PC named H1 linked to a switch. The switch has connections to three other host PCs and two servers. At the bottom of the animation is an expanded view of an ethernet frame. The frame consists of the destination MAC 01-00-5E-00-00-C8, source MAC 00-07-E9-63-CE-53, Source IP 192.168.1.5, destination IP address 224.0.0.200, user data and trailer. The IP packet portion of the frame is the source IP, destination IP address, and user data. In the animation, H1 says I need to send to a group of hosts on the network. A frame is sent from H1 to the switch. The switch then forwards the frame out to only the devices in the multicast group. Two of the three PC hosts and one server receive the multicast frame.

Destination Host Group

Source Host
IP: 192.168.1.5
MAC: 00-07-E9-63-CE-53

- Dest MAC
- Source MAC
- Source IP
- Dest IP
- IP Packet
- Ethernet Frame

Routing protocols and other network protocols use multicast addressing. Applications such as video and imaging software may also use multicast addressing, although multicast applications are not as common.

7.3.1

Switch Fundamentals

Now that you know all about Ethernet MAC addresses, it is time to talk about how a switch uses these addresses to forward (or discard) frames to other devices on a network. If a switch just forwarded every frame it received out all ports, your network would be so congested that it would probably come to a complete halt.

A Layer 2 Ethernet switch uses Layer 2 MAC addresses to make forwarding decisions. It is completely unaware of the data (protocol) being carried in the data portion of the frame, such as an IPv4 packet, an ARP message, or an IPv6 ND packet. The switch makes its forwarding decisions based solely on the Layer 2 Ethernet MAC addresses.

An Ethernet switch examines its MAC address table to make a forwarding decision for each frame, unlike legacy Ethernet hubs that repeat bits out all ports except the incoming port. In the figure, the four-port switch was just powered on. The table shows the MAC Address Table which has not yet learned the MAC addresses for the four attached PCs.

Note: MAC addresses are shortened throughout this topic for demonstration purposes.

The diagram shows four hosts, along with their associated MAC addresses, connected to ports 1 - 4 on a switch. The MAC address table which maps ports to MAC addresses is currently empty.

ABCD1234

Table caption	
MAC Address Table	
Port	MAC Address

MAC
00-0AMAC
00-0BMAC
00-0CMAC
00-0D

The switch MAC address table is empty.

Note: The MAC address table is sometimes referred to as a content addressable memory (CAM) table. While the term CAM table is fairly common, for the purposes of this course, we will refer to it as a MAC address table.

7.3.2

Switch Learning and Forwarding

The switch dynamically builds the MAC address table by examining the source MAC address of the frames received on a port. The switch forwards frames by searching for a match between the destination MAC address in the frame and an entry in the MAC address table.

Click the Learn and Forward buttons for an illustration and explanation of this process.

Learn

Forward

Examine the Source MAC Address

Every frame that enters a switch is checked for new information to learn. It does this by examining the source MAC address of the frame and the port number where the frame entered the switch. If the source MAC address does not exist, it is added to the table along with the incoming port number. If the source MAC address does exist, the switch updates the refresh timer for that entry in the table. By default, most Ethernet switches keep an entry in the table for 5 minutes.

In the figure for example, PC-A is sending an Ethernet frame to PC-D. The table shows the switch adds the MAC address for PC-A to the MAC Address Table.

Note: If the source MAC address does exist in the table but on a different port, the switch treats this as a new entry. The entry is replaced using the same MAC address but with the more current port number.

The figure shows four hosts, A - D, are connected to a switch at ports 1 - 4. Host A with MAC address 00-0A (simplified in this example) is connected to the switch at port 1. Host A sends a frame with a destination MAC address of 00-0D. The source MAC in the frame is 00-0A. The switch maps port 1 to MAC address 00-0A in its MAC address table.

ABCD1234

Table caption	
MAC Address Table	
Port	MAC Address
1	00-0A

Table caption	
MAC Address Table	
Port	MAC Address

MAC
00-0AMAC
00-0BMAC
00-0CMAC
00-0D

1. PC-A sends an Ethernet frame.
2. The switch adds the port number and MAC address for PC-A to the MAC Address Table.

7.3.3

Filtering Frames

As a switch receives frames from different devices, it is able to populate its MAC address table by examining the source MAC address of every frame. When the MAC address table of the switch contains the destination MAC address, it is able to filter the frame and forward out a single port.

Click each button for an illustration and explanation of how a switch filters frames.

PC-D to Switch

Switch to PC-A

PC-A to Switch to PC-D

In the figure, PC-D is replying back to PC-A. The switch sees the MAC address of PC-D in the incoming frame on port 4. The switch then puts the MAC address of PC-D into the MAC Address Table associated with port 4.

The figure shows four hosts, A - D, are connected to a switch at ports 1 - 4. Host D with MAC address 00-0D is connected to the switch at port 4. Host D sends a frame with a destination MAC address of 00-0A and a source MAC of 00-0D. The switch maps port 4 to MAC address 00-0D in its MAC address table.

ABCD1234

Table caption	
MAC Address Table	
Port	MAC Address
1	00-0A
4	00-0D

MAC
00-0AMAC
00-0BMAC
00-0CMAC
00-0D

The switch adds the port number and MAC address for PC-D to its MAC address table.

7.3.4

Video - MAC Address Tables on Connected Switches

A switch can have multiple MAC addresses associated with a single port. This is common when the switch is connected to another switch. The switch will have a separate MAC address table entry for each frame received with a different source MAC address.

Click Play in the figure to view a demonstration of how two connected switches build MAC address tables.

Play Video

7.3.5

Video - Sending the Frame to the Default Gateway

When a device has an IP address that is on a remote network, the Ethernet frame cannot be sent directly to the destination device. Instead, the Ethernet frame is sent to the MAC address of the default gateway, the router.

Click Play in the figure to view a demonstration of how PC-A communicates with its default gateway.

Note: In the video, the IP packet that is sent from PC-A to a destination on a remote network has a source IP address of PC-A and a destination IP address of the remote host. The returning IP packet will have the source IP address of remote host and the destination IP address will be that of PC-A.

Play Video

7.3.6

Activity - Switch It!

Determine how the switch forwards a frame based on the source MAC address, the destination MAC address, and information in the switch MAC table. Answer the questions using the information provided.

Frame

Preamble	Destination MAC	Source MAC	Type / Length	Frame	End of Frame
	0F	0C			

MAC Table

Fa1	Fa2	Fa3	Fa4	Fa5	Fa6	Fa7	Fa8	Fa9	Fa10	Fa11	Fa12
		0B				0D		0F			

Question 1 - Where will the switch forward the frame?

- Fa1
- Fa2
- Fa3
- Fa4
- Fa5
- Fa6
- Fa7
- Fa8
- Fa9

Fa10

Fa11

Fa12

Question 2 - **When the switch forwards the frame, which statement(s) are true?**

- Switch adds the source MAC address which is currently not in the MAC address table.
- Frame is a broadcast frame and will be forwarded to all ports.
- Frame is a unicast frame and will be sent to specific port only.
- Frame is a unicast frame and will be flooded to all ports.
- Frame is a unicast frame but it will be dropped at the switch.

CheckNew ProblemShow MeHelp

7.3.7

Lab - View the Switch MAC Address Table

In this lab, you will complete the following objectives:

- Part 1: Build and Configure the Network
- Part 2: Examine the Switch MAC Address Table

View the Switch MAC Address Table

7.2

Ethernet MAC Address

7.4

Switch Speeds and Forwarding Methods

7.4.1

Frame Forwarding Methods on Cisco Switches

As you learned in the previous topic, switches use their MAC address tables to determine which port to use to forward frames. With Cisco switches, there are actually two frame forwarding methods and there are good reasons to use one instead of the other, depending on the situation.

Switches use one of the following forwarding methods for switching data between network ports:

- **Store-and-forward switching** - This frame forwarding method receives the entire frame and computes the CRC. CRC uses a mathematical formula, based on the number of bits (1s) in the frame, to determine whether the received frame has an error. If the CRC is valid, the switch looks up the destination address, which determines the outgoing interface. Then the frame is forwarded out of the correct port.
- **Cut-through switching** - This frame forwarding method forwards the frame before it is entirely received. At a minimum, the destination address of the frame must be read before the frame can be forwarded.

A big advantage of store-and-forward switching is that it determines if a frame has errors before propagating the frame. When an error is detected in a frame, the switch discards the frame. Discarding frames with errors reduces the amount of bandwidth consumed by corrupt data. Store-and-forward switching is required for quality of service (QoS) analysis on converged networks where frame classification for traffic prioritization is necessary. For example, voice over IP (VoIP) data streams need to have priority over web-browsing traffic.

Click Play in the animation for a demonstration of the store-and-forward process.

The animation shows as source host sending a frame to a cut-through switch. The animation has a topology consisting of a Source host linked to a switch. The switch has a link to a destination host and a server. In the animation, the source host forwards a frame to the switch. The switch receives the frame and looks at its switching table to determine which interface to forward the frame. The switch then sends the frame to the destination host.



7.4.2

Cut-Through Switching

In cut-through switching, the switch acts upon the data as soon as it is received, even if the transmission is not complete. The switch buffers just enough of the frame to read the destination MAC address so that it can determine to which port it should forward out the data. The destination MAC address is located in the first 6 bytes of the frame following the preamble. The switch looks up the destination MAC address in its switching table, determines the outgoing interface port, and forwards the frame onto its destination through the designated switch port. The switch does not perform any error checking on the frame.

Click Play in the animation for a demonstration of the cut-through switching process.

The animation shows as source host sending a frame to a store-and-forward switch. The switch computes the CRC and if valid sends the frame to the destination host. The animation has a topology consisting of a Source host linked to a switch. The switch has a link to a destination host and a server. In the animation, the source host shows the contents of the frame consisting of a destination address, source address, data and CRC. The frame is forwarded to the switch from the source host. The switch receives the frame and computes the CRC in the frame. The CRC in the packet is 435869123 and the computed CRC is 435869123, both matching. The switch says Frame is good and then looks at its switching table to determine which interface to forward the frame. The switch then sends the frame to the destination host.



There are two variants of cut-through switching:

- **Fast-forward switching** - Fast-forward switching offers the lowest level of latency. Fast-forward switching immediately forwards a packet after reading the destination address. Because fast-forward switching starts forwarding before the entire packet has been received, there may be times when packets are relayed with errors. This occurs infrequently, and the destination NIC discards the faulty packet upon receipt. In fast-forward mode, latency is measured from the first bit received to the first bit transmitted. Fast-forward switching is the typical cut-through method of switching.
- **Fragment-free switching** - In fragment-free switching, the switch stores the first 64 bytes of the frame before forwarding. Fragment-free switching can be viewed as a compromise between store-and-forward switching and fast-forward switching. The reason fragment-free switching stores only the first 64 bytes of the frame is that most network errors and collisions occur during the first 64 bytes. Fragment-free switching tries to enhance fast-forward switching by performing a small error check on the first 64 bytes of the frame to ensure that a collision has not occurred before forwarding the frame. Fragment-free switching is a compromise between the high latency and high integrity of store-and-forward switching, and the low latency and reduced integrity of fast-forward switching.

Some switches are configured to perform cut-through switching on a per-port basis until a user-defined error threshold is reached, and then they automatically change to store-and-forward. When the error rate falls below the threshold, the port automatically changes back to cut-through switching.

7.4.3

Memory Buffering on Switches

An Ethernet switch may use a buffering technique to store frames before forwarding them. Buffering may also be used when the destination port is busy because of congestion. The switch stores the frame until it can be transmitted.

As shown in the table, there are two methods of memory buffering:

Memory Buffering Methods

Table caption	
Method	Description
Port-based memory	<ul style="list-style-type: none">Frames are stored in queues that are linked to specific incoming and outgoing ports.A frame is transmitted to the outgoing port only when all the frames ahead in the queue have been successfully transmitted.It is possible for a single frame to delay the transmission of all the frames in memory because of the destination port.This delay occurs even if the other frames could be transmitted to open destination ports.
Shared memory	<ul style="list-style-type: none">Deposits all frames into a common memory buffer shared by all switch ports and the amount of memory required by a port is dynamically allocated.The frames in the buffer are dynamically linked to the destination port enabling a packet to be received on one port and then transmitted on another port, without moving it to a different queue.

Shared memory buffering also results in the ability to store larger frames with potentially fewer dropped frames. This is important with asymmetric switching which allows for different data rates on different ports such as when connecting a server to a 10 Gbps switch port and PCs to 1 Gbps ports.

7.4.4

Duplex and Speed Settings

Two of the most basic settings on a switch are the bandwidth (sometimes referred to as “speed”) and duplex settings for each individual switch port. It is critical that the duplex and bandwidth settings match between the switch port and the connected devices, such as a computer or another switch.

There are two types of duplex settings used for communications on an Ethernet network:

- Full-duplex** - Both ends of the connection can send and receive simultaneously.
- Half-duplex** - Only one end of the connection can send at a time.

Autonegotiation is an optional function found on most Ethernet switches and NICs. It enables two devices to automatically negotiate the best speed and duplex capabilities. Full-duplex is chosen if both devices have the capability along with their highest common bandwidth.

In the figure, the Ethernet NIC for PC-A can operate in full-duplex or half-duplex, and in 10 Mbps or 100 Mbps.

S2PC A

DuplexDuplexSpeedSpeedPort 1AutonegotiationAutonegotiation

PC-A is connected to switch S2 on port 1, which can operate in full-duplex or half-duplex, and in 10 Mbps, 100 Mbps or 1000 Mbps (1 Gbps). If both devices are using autonegotiation, the operating mode will be full-duplex and 100 Mbps.

Note: Most Cisco switches and Ethernet NICs default to autonegotiation for speed and duplex. Gigabit Ethernet ports only operate in full-duplex.

Duplex mismatch is one of the most common causes of performance issues on 10/100 Mbps Ethernet links. It occurs when one port on the link operates at half-duplex while the other port operates at full-duplex, as shown in the figure.

Switch S1 is connected to switch S2. S1 is operating in full-duplex and S2 is operating in half-duplex. A callout above S1 reads: Im full duplex so I can send whenever I want. A callout above S2 reads: Im half duplex so I can only send when the link is clear but I am also getting a lot of collisions! The graphic shows both switches sending data at the same time that has resulted in a collision.

S1S2

Half-duplexFull-duplexI'm half-duplex so I can only send when the link is clear but I am also getting a lot of collisions!I'm full-duplex so I can send whenever I want.

S2 will continually experience collisions because S1 keeps sending frames any time it has something to send.

Duplex mismatch occurs when one or both ports on a link are reset, and the autonegotiation process does not result in both link partners having the same configuration. It also can occur when users reconfigure one side of a link and forget to reconfigure the other. Both sides of a link should have autonegotiation on, or both sides should have it off. Best practice is to configure both Ethernet switch ports as full-duplex.

7.4.5

Auto-MDIX

Connections between devices once required the use of either a crossover or straight-through cable. The type of cable required depended on the type of interconnecting devices.

For example, the figure identifies the correct cable type required to interconnect switch-to-switch, switch-to-router, switch-to-host, or router-to-host devices. A crossover cable is used when connecting like devices, and a straight-through cable is used for connecting unlike devices.

Note: A direct connection between a router and a host requires a cross-over connection.

The diagram shows the correct cable type to use when connecting various types of networking devices together. From top to bottom, the devices and cable types are: switch to switch is a crossover cable; switch to router is a straight-through cable; switch to host is a straight-through cable; and router to host is a crossover cable.

Crossover cableStraight-through cableStraight-through cableCrossover cable

Most switch devices now support the automatic medium-dependent interface crossover (auto-MDIX) feature. When enabled, the switch automatically detects the type of cable attached to the port and configures the interfaces accordingly. Therefore, you can use either a crossover or a straight-through cable for connections to a copper 10/100/1000 port on the switch, regardless of the type of device on the other end of the connection.

The auto-MDIX feature is enabled by default on switches running Cisco IOS Release 12.2(18)SE or later. However, the feature could be disabled. For this reason, you should always use the correct cable type and not rely on the auto-MDIX feature. Auto-MDIX can be re-enabled using the **mdix auto** interface configuration command.

8.1.1

The Network Layer

The network layer, or OSI Layer 3, provides services to allow end devices to exchange data across networks. As shown in the figure, IP version 4 (IPv4) and IP version 6 (IPv6) are the principle network layer communication protocols. Other network layer protocols include routing protocols such as Open Shortest Path First (OSPF) and messaging protocols such as Internet Control Message Protocol (ICMP).

Network Layer Protocols

7654321

- Internet Protocol version 4 (IPv4)
- Internet Protocol version 6 (IPv6)

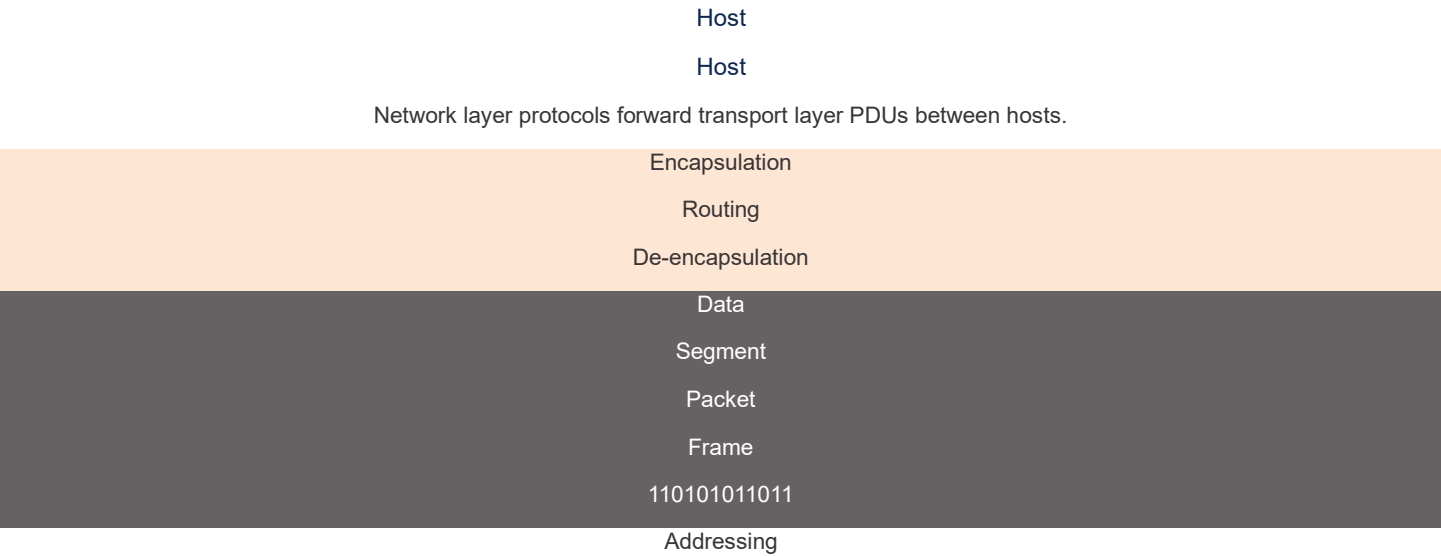
To accomplish end-to-end communications across network boundaries, network layer protocols perform four basic operations:

- **Addressing end devices** - End devices must be configured with a unique IP address for identification on the network.
- **Encapsulation** - The network layer encapsulates the protocol data unit (PDU) from the transport layer into a packet. The encapsulation process adds IP header information, such as the IP address of the source (sending) and destination (receiving) hosts. The encapsulation process is performed by the source of the IP packet.
- **Routing** - The network layer provides services to direct the packets to a destination host on another network. To travel to other networks, the packet must be processed by a router. The role of the router is to select the best path and direct packets toward the destination host in a process known as routing. A packet may cross many routers before reaching the destination host. Each router a packet crosses to reach the destination host is called a hop.
- **De-encapsulation** - When the packet arrives at the network layer of the destination host, the host checks the IP header of the packet. If the destination IP address within the header matches its own IP address, the

IP header is removed from the packet. After the packet is de-encapsulated by the network layer, the resulting Layer 4 PDU is passed up to the appropriate service at the transport layer. The de-encapsulation process is performed by the destination host of the IP packet.

Unlike the transport layer (OSI Layer 4), which manages the data transport between the processes running on each host, network layer communication protocols (i.e., IPv4 and IPv6) specify the packet structure and processing used to carry the data from one host to another host. Operating without regard to the data carried in each packet allows the network layer to carry packets for multiple types of communications between multiple hosts.

Click Play in the figure to view an animation that demonstrates the exchange of data.



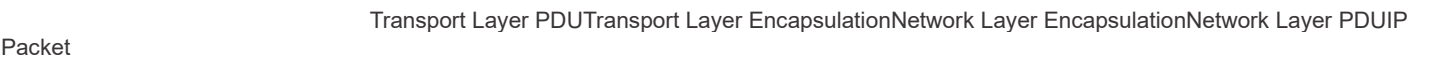
8.1.2

IP Encapsulation

IP encapsulates the transport layer (the layer just above the network layer) segment or other data by adding an IP header. The IP header is used to deliver the packet to the destination host.

The figure illustrates how the transport layer PDU is encapsulated by the network layer PDU to create an IP packet.

The illustration shows the transport layer PDU being encapsulated into an IP packet. At the top of the graphic is the transport layer encapsulation. It shows the segment header followed by data. This comprises the transport layer PDU. This is passed down to the network layer for further encapsulation and becomes the data part of the network layer PDU. An IP header is added in front of the data to create the IP packet.



The process of encapsulating data layer by layer enables the services at the different layers to develop and scale without affecting the other layers. This means the transport layer segments can be readily packaged by IPv4 or IPv6 or by any new protocol that might be developed in the future.

The IP header is examined by Layer 3 devices (i.e., routers and Layer 3 switches) as it travels across a network to its destination. It is important to note, that the IP addressing information remains the same from the time the packet leaves the source host until it arrives at the destination host, except when translated by the device performing Network Address Translation (NAT) for IPv4.

Note: NAT is discussed in later modules.

Routers implement routing protocols to route packets between networks. The routing performed by these intermediary devices examines the network layer addressing in the packet header. In all cases, the data portion of the packet, that is, the encapsulated transport layer PDU or other data, remains unchanged during the network layer processes.

8.1.3

Characteristics of IP

IP was designed as a protocol with low overhead. It provides only the functions that are necessary to deliver a packet from a source to a destination over an interconnected system of networks. The protocol was not designed to track and manage the flow of packets. These functions, if required, are performed by other protocols at other layers, primarily TCP at Layer 4.

These are the basic characteristics of IP:

- **Connectionless** - There is no connection with the destination established before sending data packets.
- **Best Effort** - IP is inherently unreliable because packet delivery is not guaranteed.
- **Media Independent** - Operation is independent of the medium (i.e., copper, fiber-optic, or wireless) carrying the data.

8.1.4

Connectionless

IP is connectionless, meaning that no dedicated end-to-end connection is created by IP before data is sent. Connectionless communication is conceptually similar to sending a letter to someone without notifying the recipient in advance. The figure summarizes this key point.

a packet, consisting of an IP header and segment, is sent from a source on one network to a destination on another network

Connectionless - Analogy

A letter is sent.LetterLetterMail box

Connectionless data communications work on the same principle. As shown in the figure, IP requires no initial exchange of control information to establish an end-to-end connection before packets are forwarded.

Connectionless - Network

A packet is sent.

8.1.5

Best Effort

IP also does not require additional fields in the header to maintain an established connection. This process greatly reduces the overhead of IP. However, with no pre-established end-to-end connection, senders are unaware whether destination devices are present and functional when sending packets, nor are they aware if the destination receives the packet, or if the destination device is able to access and read the packet.

The IP protocol does not guarantee that all packets that are delivered are, in fact, received. The figure illustrates the unreliable or best-effort delivery characteristic of the IP protocol.

The diagram shows a source on one network and a destination on another network. Between the two hosts is a cloud consisting of four routers in a mesh topology. Three IP packets leave the source host but only two arrive at the destination host. Text in the graphic reads: Packets are routed through the network quickly; Some Packets may be lost en route.

Packets are routed through the network quicklySome Packets may be lost en route IP PacketIP PacketIP PacketIP PacketIP Packet

As an unreliable network layer protocol, IP does not guarantee that all sent packets will be received. Other protocols manage the process of tracking packets and ensuring their delivery.

8.1.6

Media Independent

Unreliable means that IP does not have the capability to manage and recover from undelivered or corrupt packets. This is because while IP packets are sent with information about the location of delivery, they do not contain information that can be processed to inform the sender whether delivery was successful. Packets may arrive at the destination corrupted, out of sequence, or not at all. IP provides no capability for packet retransmissions if errors occur.

If out-of-order packets are delivered, or packets are missing, then applications using the data, or upper layer services, must resolve these issues. This allows IP to function very efficiently. In the TCP/IP protocol suite, reliability is the role of the TCP protocol at the transport layer.

IP operates independently of the media that carry the data at lower layers of the protocol stack. As shown in the figure, IP packets can be communicated as electronic signals over copper cable, as optical signals over fiber, or wirelessly as radio signals.

The diagram shows a network topology within a cloud with a packet traveling over various media types between two hosts. An IP packet is shown moving between a host and a router over a copper Ethernet connection. The first router is connected to second router via a copper serial connection. An IP packet is shown moving between the second router and a third router over an optical fiber connection. The third router is connected to a fourth router, which is a wireless router. An IP packet is shown moving between the fourth router and a host over a wireless connection.

IP PacketIP PacketIP PacketCopper EthernetCopper SerialOptical FiberWirelessCopper Ethernet

IP packets can travel over different media.

The OSI data link layer is responsible for taking an IP packet and preparing it for transmission over the communications medium. This means that the delivery of IP packets is not limited to any particular medium.

There is, however, one major characteristic of the media that the network layer considers: the maximum size of the PDU that each medium can transport. This characteristic is referred to as the maximum transmission unit (MTU). Part of the control communication between the data link layer and the network layer is the establishment of a maximum size for the packet. The data link layer passes the MTU value up to the network layer. The network layer then determines how large packets can be.

In some cases, an intermediate device, usually a router, must split up an IPv4 packet when forwarding it from one medium to another medium with a smaller MTU. This process is called fragmenting the packet, or fragmentation. Fragmentation causes latency. IPv6 packets cannot be fragmented by the router.

8.2.1

IPv4 Packet Header

IPv4 is one of the primary network layer communication protocols. The IPv4 packet header is used to ensure that this packet is delivered to its next stop on the way to its destination end device.

An IPv4 packet header consists of fields containing important information about the packet. These fields contain binary numbers which are examined by the Layer 3 process.

8.2.2

IPv4 Packet Header Fields

The binary values of each field identify various settings of the IP packet. Protocol header diagrams, which are read left to right, and top down, provide a visual to refer to when discussing protocol fields. The IP protocol header diagram in the figure identifies the fields of an IPv4 packet.

names and bit length of fields in an IPv4 packet header

Fields in the IPv4 Packet Header

Byte 1Byte 2Byte 3Byte 4
20 Bytes

Significant fields in the IPv4 header include the following:

- **Version** - Contains a 4-bit binary value set to 0100 that identifies this as an IPv4 packet.
- **Differentiated Services or DiffServ (DS)** - Formerly called the type of service (ToS) field, the DS field is an 8-bit field used to determine the priority of each packet. The six most significant bits of the DiffServ field are the differentiated services code point (DSCP) bits and the last two bits are the explicit congestion notification (ECN) bits.
- **Time to Live (TTL)** – TTL contains an 8-bit binary value that is used to limit the lifetime of a packet. The source device of the IPv4 packet sets the initial TTL value. It is decreased by one each time the packet is processed by a router. If the TTL field decrements to zero, the router discards the packet and sends an Internet Control Message Protocol (ICMP) Time Exceeded message to the source IP address. Because the router decrements the TTL of each packet, the router must also recalculate the Header Checksum.

- **Protocol** – This field is used to identify the next level protocol. This 8-bit binary value indicates the data payload type that the packet is carrying, which enables the network layer to pass the data to the appropriate upper-layer protocol. Common values include ICMP (1), TCP (6), and UDP (17).
- **Header Checksum** – This is used to detect corruption in the IPv4 header.
- **Source IPv4 Address** – This contains a 32-bit binary value that represents the source IPv4 address of the packet. The source IPv4 address is always a unicast address.
- **Destination IPv4 Address** – This contains a 32-bit binary value that represents the destination IPv4 address of the packet. The destination IPv4 address is a unicast, multicast, or broadcast address.

The two most commonly referenced fields are the source and destination IP addresses. These fields identify where the packet is coming from and where it is going. Typically, these addresses do not change while travelling from the source to the destination.

The Internet Header Length (IHL), Total Length, and Header Checksum fields are used to identify and validate the packet.

Other fields are used to reorder a fragmented packet. Specifically, the IPv4 packet uses Identification, Flags, and Fragment Offset fields to keep track of the fragments. A router may have to fragment an IPv4 packet when forwarding it from one medium to another with a smaller MTU.

The Options and Padding fields are rarely used and are beyond the scope of this module.

8.3.1

Limitations of IPv4

IPv4 is still in use today. This topic is about IPv6, which will eventually replace IPv4. To better understand why you need to know the IPv6 protocol, it helps to know the limitations of IPv4 and the advantages of IPv6.

Through the years, additional protocols and processes have been developed to address new challenges. However, even with changes, IPv4 still has three major issues:

- **IPv4 address depletion** - IPv4 has a limited number of unique public addresses available. Although there are approximately 4 billion IPv4 addresses, the increasing number of new IP-enabled devices, always-on connections, and the potential growth of less-developed regions have increased the need for more addresses.
- **Lack of end-to-end connectivity** - Network Address Translation (NAT) is a technology commonly implemented within IPv4 networks. NAT provides a way for multiple devices to share a single public IPv4 address. However, because the public IPv4 address is shared, the IPv4 address of an internal network host is hidden. This can be problematic for technologies that require end-to-end connectivity.
- **Increased network complexity** – While NAT has extended the lifespan of IPv4 it was only meant as a transition mechanism to IPv6. NAT in its various implementation creates additional complexity in the network, creating latency and making troubleshooting more difficult.

8.3.2

IPv6 Overview

In the early 1990s, the Internet Engineering Task Force (IETF) grew concerned about the issues with IPv4 and began to look for a replacement. This activity led to the development of IP version 6 (IPv6). IPv6 overcomes the limitations of IPv4 and is a powerful enhancement with features that better suit current and foreseeable network demands.

Improvements that IPv6 provides include the following:

- **Increased address space** - IPv6 addresses are based on 128-bit hierarchical addressing as opposed to IPv4 with 32 bits.
- **Improved packet handling** - The IPv6 header has been simplified with fewer fields.
- **Eliminates the need for NAT** - With such a large number of public IPv6 addresses, NAT between a private IPv4 address and a public IPv4 is not needed. This avoids some of the NAT-induced problems experienced by applications that require end-to-end connectivity.

The 32-bit IPv4 address space provides approximately 4,294,967,296 unique addresses. IPv6 address space provides 340,282,366,920,938,463,463,374,607,431,768,211,456, or 340 undecillion addresses. This is roughly equivalent to every grain of sand on Earth.

The figure provides a visual to compare the IPv4 and IPv6 address space.

IPv4 and IPv6 Address Space Comparison

Number Name	Scientific Notation	Number of Zeros
1 Thousand	10^3	1,000
1 Million	10^6	1,000,000
1 Billion	10^9	1,000,000,000
1 Trillion	10^12	1,000,000,000,000
1 Quadrillion	10^15	1,000,000,000,000,000
1 Quintillion	10^18	1,000,000,000,000,000,000
1 Sextillion	10^21	1,000,000,000,000,000,000,000
1 Septillion	10^24	1,000,000,000,000,000,000,000,000
1 Octillion	10^27	1,000,000,000,000,000,000,000,000,000
1 Nonillion	10^30	1,000,000,000,000,000,000,000,000,000,000
1 Decillion	10^33	1,000,000,000,000,000,000,000,000,000,000,000
1 Undecillion	10^36	1,000,000,000,000,000,000,000,000,000,000,000,000

LegendThere are 4 billion IPv4 addressesThere are 340 undecillion IPv6 addresses

8.3.3

IPv4 Packet Header Fields in the IPv6 Packet Header

One of the major design improvements of IPv6 over IPv4 is the simplified IPv6 header.

For example, the IPv4 header consists of a variable length header of 20 octets (up to 60 bytes if the Options field is used) and 12 basic header fields, not including the Options field and Padding field.

For IPv6, some fields have remained the same, some fields have changed names and positions, and some IPv4 fields are no longer required, as highlighted in the figure.

The diagram shows an IPv4 packet header and indicates which fields kept the same name, which fields changed names and position, and which fields were not kept in IPv6. The fields that kept the same name are: version, source address, and destination address. The fields that changed names and position are: type of service, total length, time-to-live, and protocol. The fields that were not kept in IPv6 are: IHL, identification, flags, fragment offset, header checksum, options, and padding.

IPv4 Packet Header



The figure shows IPv4 packet header fields that were kept, moved, changed, as well as those that were not kept in the IPv6 packet header.

In contrast, the simplified IPv6 header shown the next figure consists of a fixed length header of 40 octets (largely due to the length of the source and destination IPv6 addresses).

The IPv6 simplified header allows for more efficient processing of IPv6 headers.

The diagram shows an IPv6 packet header and indicates which fields kept the same name from IPv4 to IPv6, which fields changed names and position in IPv6, which fields were not kept in IPv6, and new fields in IPv6. The field names that were kept the same are: version, source IP address, and destination IP address. The fields that changed names and position in IPv6 are: traffic class, payload length, next header, and hop limit. The field that is NEW to IPv6 is flow label.

IPv6 Packet Header

Byte 1Byte 2Byte 3Byte 4

name kept from IPv4 to IPv6- Name and position changed in IPv6- Fields no longer required in IPv6

Legend40 bytes

- Fields

The figure shows the IPv4 packet header fields that were kept or moved along with the new IPv6 packet header fields.

8.3.4

IPv6 Packet Header

The IP protocol header diagram in the figure identifies the fields of an IPv6 packet.

names and bit length of fields in an IPv6 header

Fields in the IPv6 Packet Header

Byte 1Byte 2Byte 3Byte 4

Bytes

40

The fields in the IPv6 packet header include the following:

- **Version** - This field contains a 4-bit binary value set to 0110 that identifies this as an IP version 6 packet.
- **Traffic Class** - This 8-bit field is equivalent to the IPv4 Differentiated Services (DS) field.
- **Flow Label** - This 20-bit field suggests that all packets with the same flow label receive the same type of handling by routers.
- **Payload Length** - This 16-bit field indicates the length of the data portion or payload of the IPv6 packet. This does not include the length of the IPv6 header, which is a fixed 40-byte header.
- **Next Header** - This 8-bit field is equivalent to the IPv4 Protocol field. It indicates the data payload type that the packet is carrying, enabling the network layer to pass the data to the appropriate upper-layer protocol.
- **Hop Limit** - This 8-bit field replaces the IPv4 TTL field. This value is decremented by a value of 1 by each router that forwards the packet. When the counter reaches 0, the packet is discarded, and an ICMPv6 Time Exceeded message is forwarded to the sending host,. This indicates that the packet did not reach its destination because the hop limit was exceeded. Unlike IPv4, IPv6 does not include an IPv6 Header Checksum, because this function is performed at both the lower and upper layers. This means the checksum does not need to be recalculated by each router when it decrements the Hop Limit field, which also improves network performance.
- **Source IPv6 Address** - This 128-bit field identifies the IPv6 address of the sending host.
- **Destination IPv6 Address** - This 128-bit field identifies the IPv6 address of the receiving host.

An IPv6 packet may also contain extension headers (EH), which provide optional network layer information. Extension headers are optional and are placed between the IPv6 header and the payload. EHs are used for fragmentation, security, to support mobility and more.

Unlike IPv4, routers do not fragment routed IPv6 packets.

8.4.1

Host Forwarding Decision

With both IPv4 and IPv6, packets are always created at the source host. The source host must be able to direct the packet to the destination host. To do this, host end devices create their own routing table. This topic discusses how end devices use routing tables.

Another role of the network layer is to direct packets between hosts. A host can send a packet to the following:

- **Itself** - A host can ping itself by sending a packet to a special IPv4 address of 127.0.0.1 or an IPv6 address ::1, which is referred to as the loopback interface. Pinging the loopback interface tests the TCP/IP protocol stack on the host.
- **Local host** - This is a destination host that is on the same local network as the sending host. The source and destination hosts share the same network address.
- **Remote host** - This is a destination host on a remote network. The source and destination hosts do not share the same network address.

The figure illustrates PC1 connecting to a local host on the same network, and to a remote host located on another network.

The diagram shows a host, PC1, connecting to a local host, PC2, on the same network and to a remote host, a server, on another network. PC1 and PC2 are connected to a switch on network 192.168.10.0/24. PC1 has an address of .10 and PC2 has an address of .15. The switch is connected to a router, R1, at address .1. On the other side of the R1 is a connection to the cloud where the remote host resides.

PC1R1.10.1PC2.15

Local
HostRemote
Host192.168.10.0/24

Whether a packet is destined for a local host or a remote host is determined by the source end device. The source end device determines whether the destination IP address is on the same network that the source device itself is on. The method of determination varies by IP version:

- **In IPv4** - The source device uses its own subnet mask along with its own IPv4 address and the destination IPv4 address to make this determination.
- **In IPv6** - The local router advertises the local network address (prefix) to all devices on the network.

In a home or business network, you may have several wired and wireless devices interconnected together using an intermediary device, such as a LAN switch or a wireless access point (WAP). This intermediary device provides interconnections between local hosts on the local network. Local hosts can reach each other and share information without the need for any additional devices. If a host is sending a packet to a device that is configured with the same IP network as the host device, the packet is simply forwarded out of the host interface, through the intermediary device, and to the destination device directly.

Of course, in most situations we want our devices to be able to connect beyond the local network segment, such as out to other homes, businesses, and the internet. Devices that are beyond the local network segment are known as remote hosts. When a source device sends a packet to a remote destination device, then the help of routers and routing is needed. Routing is the process of identifying the best path to a destination. The router connected to the local network segment is referred to as the default gateway.

8.4.2

Default Gateway

The default gateway is the network device (i.e., router or Layer 3 switch) that can route traffic to other networks. If you use the analogy that a network is like a room, then the default gateway is like a doorway. If you want to get to another room or network you need to find the doorway.

On a network, a default gateway is usually a router with these features:

- It has a local IP address in the same address range as other hosts on the local network.
- It can accept data into the local network and forward data out of the local network.
- It routes traffic to other networks.

A default gateway is required to send traffic outside of the local network. Traffic cannot be forwarded outside the local network if there is no default gateway, the default gateway address is not configured, or the default gateway is down.

8.4.3

A Host Routes to the Default Gateway

A host routing table will typically include a default gateway. In IPv4, the host receives the IPv4 address of the default gateway either dynamically from Dynamic Host Configuration Protocol (DHCP) or configured manually. In IPv6, the router advertises the default gateway address or the host can be configured manually.

In the figure, PC1 and PC2 are configured with the IPv4 address of 192.168.10.1 as the default gateway.

The diagram shows two hosts, PC1 and PC2, connected to a switch on network 192.168.10.0/24, the local network route. The switch is connected to a router, R1, which is then connected to the cloud representing remote networks. PC1 has an address of .10, PC2 has an address of .15, and the router interface to which the switch is connected has an address of .1. The PCs, the switch, and the router interface all have a direct connection.

.10.1192.168.10.0/24.15PC1R1PC2

Local Network RouteRemote NetworksDirect Connection

Having a default gateway configured creates a default route in the routing table of the PC. A default route is the route or pathway your computer will take when it tries to contact a remote network.

Both PC1 and PC2 will have a default route to send all traffic destined to remote networks to R1.

8.4.4

Host Routing Tables

On a Windows host, the **route print** or **netstat -r** command can be used to display the host routing table. Both commands generate the same output. The output may seem overwhelming at first, but is fairly simple to understand.

The figure displays a sample topology and the output generated by the **netstat -r** command.

The diagram shows a network topology consisting of a host, PC1, connected to a switch on network 192.168.10.0/24. The switch is connected to a router, R1, which is then connected to the cloud. PC1 has an address of .10 and the router interface to which the switch is connected has an address of .1.

192.168.10.0/24.10.1PC1R1

IPv4 Routing Table for PC1

```
C:\Users\PC1> netstat -r
```

```
(output omitted)
```

```
IPv4 Route Table
```

=====				
Active Routes:				
Network Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	192.168.10.1	192.168.10.10	25
127.0.0.0	255.0.0.0	On-link	127.0.0.1	306
127.0.0.1	255.255.255.255	On-link	127.0.0.1	306
127.255.255.255	255.255.255.255	On-link	127.0.0.1	306
192.168.10.0	255.255.255.0	On-link	192.168.10.10	281
192.168.10.10	255.255.255.255	On-link	192.168.10.10	281
192.168.10.255	255.255.255.255	On-link	192.168.10.10	281
224.0.0.0	240.0.0.0	On-link	127.0.0.1	306
224.0.0.0	240.0.0.0	On-link	192.168.10.10	281
255.255.255.255	255.255.255.255	On-link	127.0.0.1	306
255.255.255.255	255.255.255.255	On-link	192.168.10.10	281

(output omitted)

Note: The output only displays the IPv4 route table.

Entering the **netstat -r** command or the equivalent **route print** command displays three sections related to the current TCP/IP network connections:

- **Interface List** - Lists the Media Access Control (MAC) address and assigned interface number of every network-capable interface on the host, including Ethernet, Wi-Fi, and Bluetooth adapters.
- **IPv4 Route Table** - Lists all known IPv4 routes, including direct connections, local network, and local default routes.
- **IPv6 Route Table** - Lists all known IPv6 routes, including direct connections, local network, and local default routes.

8.5.1

Router Packet Forwarding Decision

The previous topic discussed host routing tables. Most networks also contain routers, which are intermediary devices. Routers also contain routing tables. This topic covers router operations at the network layer. When a host sends a packet to another host, it consults its routing table to determine where to send the packet. If the destination host is on a remote network, the packet is forwarded to the default gateway, which is usually the local router.

What happens when a packet arrives on a router interface?

The router examines the destination IP address of the packet and searches its routing table to determine where to forward the packet. The routing table contains a list of all known network addresses (prefixes) and where to forward the packet. These entries are known as route entries or routes. The router will forward the packet using the best (longest) matching route entry.

The diagram is a network topology showing what happens to an IPv4 packet as it is routed between networks. Host PC1, with an address of .10, is connected to a switch on network 192.168.10.0/24 which is connected to the G0/0/0 interface of router R1 with an address of .1. Network 209.165.200.224/30 connects the G0/0/1 interface on R1, address .225, to another router, R2 at address .226. R2 is connected to a switch on network 10.1.1.0/24 to which host PC2, address .10, is connected. R2 also has a connection to the Internet cloud. A packet with destination IPv4 address 10.1.1.10 is sent from PC1 to R1. R1 then sends the packet with destination IPv4 address 10.1.1.10 to R2.

132PC2R2.10.1.1G0/0/1.226.10209.165.200.224/30192.168.10.0/2410.1.1.0/24R1.225G0/0/0PC1

InternetDestination IPv4 Address:
10.1.1.10Destination IPv4 Address:
10.1.1.10

1. Packet arrives on the Gigabit Ethernet 0/0/0 interface of router R1. R1 de-encapsulates the Layer 2 Ethernet header and trailer.
2. Router R1 examines the destination IPv4 address of the packet and searches for the best match in its IPv4 routing table. The route entry indicates that this packet is to be forwarded to router R2.
3. Router R1 encapsulates the packet into a new Ethernet header and trailer, and forwards the packet to the next hop router R2.

The following table shows the pertinent information from the R1 routing table.

R1 Routing Table

Table caption	
Route	Next Hop or Exit Interface
192.168.10.0 /24	G0/0/0
209.165.200.224/30	G0/0/1
10.1.1.0/24	via R2

Table caption	
Route	Next Hop or Exit Interface
Default Route 0.0.0.0/0	via R2

8.5.2

IP Router Routing Table

The routing table of the router contains network route entries listing all the possible known network destinations.

The routing table stores three types of route entries:

- **Directly-connected networks** - These network route entries are active router interfaces. Routers add a directly connected route when an interface is configured with an IP address and is activated. Each router interface is connected to a different network segment. In the figure, the directly-connected networks in the R1 IPv4 routing table would be 192.168.10.0/24 and 209.165.200.224/30.
- **Remote networks** - These network route entries are connected to other routers. Routers learn about remote networks either by being explicitly configured by an administrator or by exchanging route information using a dynamic routing protocol. In the figure, the remote network in the R1 IPv4 routing table would be 10.1.1.0/24.
- **Default route** – Like a host, most routers also include a default route entry, a gateway of last resort. The default route is used when there is no better (longer) match in the IP routing table. In the figure, the R1 IPv4 routing table would most likely include a default route to forward all packets to router R2.

The figure identifies the directly connected and remote networks of router R1.

The diagram is a network topology identifying directly connected networks and remote networks of a router. Host PC1, with an address of .10, is connected to a switch on network 192.168.10.0/24 which is connected to the G0/0/0 interface of router R1 with an address of .1. Network 209.165.200.224/30 connects the G0/0/1 interface on R1, address .225, to another router, R2 at address .226 on G0/0/1. R2 is connected to a switch on network 10.1.1.0/24 to which host PC2, address .10, is connected. R2 also has a connection to the Internet cloud. Networks 192.168.10.0/24 and 209.165.200.224/30 are shown as directly connected networks to R1 and network 10.1.2.0/24 (should this be 10.1.1.0/24?) is shown as a remote network to R2.

.10.1.1G0/0/1.226.10209.165.200.224/30192.168.10.0/2410.1.1.0/24.225G0/0/0G0/0/0G0/0/1PC2R2R1PC1

InternetDirectly connected networkDirectly connnected networkRemote Network

R1 has two directly connected networks:

- 192.168.10.0/24
- 209.165.200.224/30

R1 also has remote networks (i.e. 10.1.1.0/24 and the internet) that it can learn about.

A router can learn about remote networks in one of two ways:

- **Manually** - Remote networks are manually entered into the route table using static routes.
- **Dynamically** - Remote routes are automatically learned using a dynamic routing protocol.

8.5.3

Static Routing

Static routes are route entries that are manually configured. The figure shows an example of a static route that was manually configured on router R1. The static route includes the remote network address and the IP address of the next hop router.

The diagram is a network topology showing a static route configuration to reach a remote network. Host PC1, with an address of .10, is connected to a switch on network 192.168.10.0/24 which is connected to the G0/0/0 interface of router R1 with an address of .1. Network 209.165.200.224/30 connects the G0/0/1 interface on R1, address .225, to another router, R2 at address .226. R2 has an interface with address .1 connected to a switch on network 10.1.1.0/24 to which host PC2, address .10, is connected. R2 also has a connection to the Internet cloud. A static route configuration on R1 to the network 10.1.1.0/24 reads: R1(config)#ip route 10.1.1.0 255.255.255.0 209.165.200.226. In the configuration, 10.1.1.0 255.255.255.0 is labeled remote network and 209.165.200.226 is labeled IP address of next hop router.

```
R1(config)# ip route 10.1.1.0 255.255.255.0 209.165.200.226
.10.1.1G0/0/1.226.10209.165.200.224/30192.168.10.0/2410.1.1.0/24.225G0/0/0PC2R2R1PC1
```

InternetRemote network addressIP adress of next hop router

R1 is manually configured with a static route to reach the 10.1.1.0/24 network. If this path changes, R1 will require a new static route.

If there is a change in the network topology, the static route is not automatically updated and must be manually reconfigured. For example, in the figure R1 has a static route to reach the 10.1.1.0/24 network via R2. If that path is no longer available, R1 would need to be reconfigured with a new static route to the 10.1.1.0/24 network via R3. Router R3 would therefore need to have a route entry in its routing table to send packets destined for 10.1.1.0/24 to R2.

The diagram is a network topology showing a failed link in a static route. Host PC1, with an address of .10, is connected to a switch on network 192.168.10.0/24 which is connected to the G0/0/0 interface of router R1 with an address of .1. R1 is connected to router R2 and router R3 which are also directed connected. R2 is connected to a switch on network 10.1.1.0/24 to which host PC2, address .10, is connected. A static route has been configured on R1 that points to R2 as the next hop. A red X indicates that this link has failed.

```
.10.1192.168.10.0/24G0/0/0PC2R2R1PC1R310.1.1.0/24.10
```

Static Route

If the route from R1 via R2 is no longer available, a new static route via R3 would need to be configured. A static route does not automatically adjust for topology changes.

Static routing has the following characteristics:

- A static route must be configured manually.
- The administrator needs to reconfigure a static route if there is a change in the topology and the static route is no longer viable.
- A static route is appropriate for a small network and when there are few or no redundant links.

8.5.4

Dynamic Routing

A dynamic routing protocol allows the routers to automatically learn about remote networks, including a default route, from other routers. Routers that use dynamic routing protocols automatically share routing information with other routers and compensate for any topology changes without involving the network administrator. If there is a change in the network topology, routers share this information using the dynamic routing protocol and automatically update their routing tables.

Dynamic routing protocols include OSPF and Enhanced Interior Gateway Routing Protocol (EIGRP). The figure shows an example of routers R1 and R2 automatically sharing network information using the routing protocol OSPF.

The diagram is a network topology showing routers using dynamic routing protocols to exchange information. Host PC1, with an address of .10, is connected to a switch on network 192.168.10.0/24 which is connected to the G0/0/0 interface of router R1 with an address of .1. Network 209.165.200.224/30 connects the G0/0/1 interface on R1, address .225, to another router, R2 at address .226. R2 has an interface with address .1 connected to a switch on network 10.1.1.0/24 to which host PC2, address .10, is connected. Arrows show R1 and R2 sharing information with each other.

```
.10.1.1G0/0/1.226.10209.165.200.224/30192.168.10.0/2410.1.1.0/24.225G0/0/0PC2R2R1PC1
```

- R1 is using the routing protocol OSPF to let R2 know about the 192.168.10.0/24 network.
- R2 is using the routing protocol OSPF to let R1 know about the 10.1.1.0/24 network.

Basic configuration only requires the network administrator to enable the directly connected networks within the dynamic routing protocol. The dynamic routing protocol will automatically do as follows:

- Discover remote networks
- Maintain up-to-date routing information
- Choose the best path to destination networks
- Attempt to find a new best path if the current path is no longer available

When a router is manually configured with a static route or learns about a remote network dynamically using a dynamic routing protocol, the remote network address and next hop address are entered into the IP routing table. As shown in the figure, if there is a change in the network topology, the routers will automatically adjust and attempt to find a new best path.

The diagram shows a network topology in which routers using dynamic routing protocols are adjusting best paths after a topology change. Host PC1, with an address of .10, is connected to a switch on network 192.168.10.0/24 which is connected to the G0/0/0 interface of router R1 with an address of .1. R1 is connected to router R2 and router R3 which are also directed connected. R2 is connected to a switch on network 10.1.1.0/24 to which host PC2, address .10, is connected. A red X indicates that the link between R1 and R2, labeled as the previous best path, has failed. A new best path is shown going from R1 to R3 to R2.

.10.1192.168.10.0/24G0/0/0PC2R2R1PC1R310.1.1.0/24.10

Previous best pathNew best path

R1, R2, and R3 are using the dynamic routing protocol OSPF. If there is a network topology change, they can automatically adjust to find a new best path.

Note: It is common for some routers to use a combination of both static routes and a dynamic routing protocol.

8.5.5

Video- IPv4 Router Routing Tables

Unlike a host computer routing table, there are no column headings identifying the information contained in the routing table of a router. It is important to learn the meaning of the different items included in each entry of the routing table.

Click Play in the figure to view an introduction to the IPv4 routing table.

Play Video

8.5.6

Introduction to an IPv4 Routing Table

Notice in the figure that R2 is connected to the internet. Therefore, the administrator configured R1 with a default static route sending packets to R2 when there is no specific entry in the routing table that matches the destination IP address. R1 and R2 are also using OSPF routing to advertise directly connected networks.

Host PC1, with an address of .10, is connected to a switch on network 192.168.10.0/24 which is connected to the G0/0/0 interface of router R1 with an address of .1. Network 209.165.200.224/30 connects the G0/0/1 interface on R1, address .225, to another router, R2 at address .226. R2 is connected to a switch on network 10.1.1.0/24 to which host PC2, address .10, is connected. R2 also has a connection to the Internet cloud.

.10.1.1G0/0/1.226.10209.165.200.224/30192.168.10.0/2410.1.1.0/24.225G0/0/0PC2R2R1PC1

Internet

```
R1# show ip route
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
```

```
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
```

```
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
E1 - OSPF external type 1, E2 - OSPF external type 2
```

```
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
```

```
ia - IS-IS inter area, * - candidate default, U - per-user static route
```

```
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
```

```
a - application route
```

+ - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is 209.165.200.226 to network 0.0.0.0

S* 0.0.0.0/0 [1/0] via 209.165.200.226, GigabitEthernet0/0/1

10.0.0.0/24 is subnetted, 1 subnets

O 10.1.1.0 [110/2] via 209.165.200.226, 00:02:45, GigabitEthernet0/0/1

192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.10.0/24 is directly connected, GigabitEthernet0/0/0

L 192.168.10.1/32 is directly connected, GigabitEthernet0/0/0

209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks

C 209.165.200.224/30 is directly connected, GigabitEthernet0/0/1

L 209.165.200.225/32 is directly connected, GigabitEthernet0/0/1

R1#

The **show ip route** privileged EXEC mode command is used to view the IPv4 routing table on a Cisco IOS router. The example shows the IPv4 routing table of router R1. At the beginning of each routing table entry is a code that is used to identify the type of route or how the route was learned. Common route sources (codes) include these:

- **L** - Directly connected local interface IP address
- **C** – Directly connected network
- **S** – Static route was manually configured by an administrator
- **O** - OSPF
- **D** - EIGRP

The routing table displays all of the known IPv4 destination routes for R1.

A directly connected route is automatically created when a router interface is configured with IP address information and is activated. The router adds two route entries with the codes **C** (i.e., the connected network) and **L** (i.e., the local interface IP address of the connected network). The route entries also identify the exit interface to use to reach the network. The two directly connected networks in this example are 192.168.10.0/24 and 209.165.200.224/30.

Routers R1 and R2 are also using the OSPF dynamic routing protocol to exchange router information. In the example routing table, R1 has a route entry for the 10.1.1.0/24 network that it learned dynamically from router R2 via the OSPF routing protocol.

A default route has a network address of all zeroes. For example, the IPv4 network address is 0.0.0.0. A static route entry in the routing table begins with a code of **S***, as highlighted in the example.

Destination on Same Network

Sometimes a host must send a message, but it only knows the IP address of the destination device. The host needs to know the MAC address of that device, but how can it be discovered? That is where address resolution becomes critical.

There are two primary addresses assigned to a device on an Ethernet LAN:

- **Physical address (the MAC address)** – Used for NIC to NIC communications on the same Ethernet network.
- **Logical address (the IP address)** – Used to send the packet from the source device to the destination device. The destination IP address may be on the same IP network as the source or it may be on a remote network.

Layer 2 physical addresses (i.e., Ethernet MAC addresses) are used to deliver the data link frame with the encapsulated IP packet from one NIC to another NIC that is on the same network. If the destination IP address is on the same network, the destination MAC address will be that of the destination device.

Consider the following example using simplified MAC address representations.

The image is a network diagram with PC 1 at IP 192.168.10.10/24 with simplified MAC aa-aa-aa, connected to a switch at IP 192.168.10.0/24, connected to PC 2 at IP 192.168.10.11/24 with simplified MAC 55-55-55. Below the diagram are four boxes reading from left to right: Destination MAC 55-55-55, Source MAC aa-aa-aa, Source IPv4 192.168.10.10, and Destination IPv4 192.168.10.11.

Destination MAC	Source MAC	Source IPv4	Destination IPv4
55-55-55	aa-aa-aa	192.168.10.10	192.168.10.11
55-55-55aa-aa-aa	192.168.10.10/24192.168.10.0/24192.168.10.11/24		

In this example, PC1 wants to send a packet to PC2. The figure displays the Layer 2 destination and source MAC addresses and the Layer 3 IPv4 addressing that would be included in the packet sent from PC1.

The Layer 2 Ethernet frame contains the following:

- **Destination MAC address** – This is the simplified MAC address of PC2, 55-55-55.
- **Source MAC address** – This is the simplified MAC address of the Ethernet NIC on PC1, aa-aa-aa.

The Layer 3 IP packet contains the following:

- **Source IPv4 address** – This is the IPv4 address of PC1, 192.168.10.10.
- **Destination IPv4 address** – This is the IPv4 address of PC2, 192.168.10.11.

9.1.2

Destination on Remote Network

When the destination IP address (IPv4 or IPv6) is on a remote network, the destination MAC address will be the address of the host default gateway (i.e., the router interface).

Consider the following example using a simplified MAC address representation.

The image is a network diagram showing the source and destination MAC and IPv4 addressing for the first hop when information is sent from a PC on one network to a destination on a remote network. The description that follows are the names, connections, and addressing of devices from left to right. PC 1 is connected to a switch which is connected to router R1 interface G0/0/0 on network 192.168.10.0/24. PC 1 has an IP of 192.168.10.10 and MAC of aa-aa-aa. The R1 G0/0/0 interface has an IP of 192.168.10.1 and MAC of bb-bb-bb. R1 has a G0/0/1 interface connected to router R2 interface G0/0/1 on network 209.165.200.224/30. The R1 G0/0/1 interface has an IP of 209.165.200.225 and MAC cc-cc-cc. The R2 G0/0/1 interface has an IP of 209.165.200.226 and MAC dd-dd-dd. R2 has a G0/0/0 interface connected to a switch connected to PC 2 on network 10.1.1.0/24. The R2 G0/0/0 interface has an IP of 10.1.1.1 and MAC ee-ee-ee. PC 2 has an IP of 10.10.10.10 and MAC 55-55-55. R2 also has a connection at the top leading to the Internet cloud. Below the diagram under network 192.168.10.0/24 are four boxes reading from left to right: Destination MAC bb-bb-bb, Source MAC aa-aa-aa, Source IPv4 192.168.10.10, and Destination IPv4 10.1.1.10.

R1R2PC 2 PC 1.10.1.225.226.1.10G0/0/1G0/0/1G0/0/0G0/0/0

Destination MAC	Source MAC	Source IPv4	Destination IPv4
bb-bb-bb	aa-aa-aa	192.168.10.10	10.1.1.10
55-55-55aa-aa-aa	192.168.10.0/24209.165.200.224/3010.1.1.0/24Internetbb-bb-bbcc-cc-ccdd-dd-ddee-ee-ee		

In this example, PC1 wants to send a packet to PC2. PC2 is located on remote network. Because the destination IPv4 address is not on the same local network as PC1, the destination MAC address is that of the local default gateway on the router.

Routers examine the destination IPv4 address to determine the best path to forward the IPv4 packet. When the router receives the Ethernet frame, it de-encapsulates the Layer 2 information. Using the destination IPv4 address, it determines the next-hop device, and then encapsulates the IPv4 packet in a new data link frame for the outgoing interface.

In our example, R1 would now encapsulate the packet with new Layer 2 address information as shown in the figure.

The image is a network diagram showing the source and destination MAC and IPv4 addressing when information is passed between two routers as it is sent from a PC on one network to a destination on a remote network. The description that follows are the names, connections, and addressing of devices from left to right. PC 1 is connected to a switch which is connected to router R1 interface G0/0/0 on network 192.168.10.0/24. PC 1 has an IP of 192.168.10.10 and MAC of aa-aa-aa. The R1 G0/0/0 interface has an IP of 192.168.10.1 and MAC of bb-bb-bb. R1 has a G0/0/1 interface connected to router R2 interface G0/0/1 on network 209.165.200.224/30. The R1 G0/0/1 interface has an IP of 209.165.200.225 and MAC cc-cc-cc. The R2 G0/0/1 interface has an IP of 209.165.200.226 and MAC dd-dd-dd. R2 has a G0/0/0 interface connected to a switch connected to PC 2 on network 10.1.1.0/24. The R2 G0/0/0 interface has an IP of 10.1.1.1 and MAC ee-ee-ee. PC 2 has an IP of 10.10.10.10 and MAC 55-55-55. R2 also has a connection at the top leading to the Internet cloud. Below the diagram under network 209.165.200.224/30 are four boxes reading from left to right: Destination MAC dd-dd-dd, Source MAC cc-cc-cc, Source IPv4 192.168.10.10, and Destination IPv4 10.1.1.10.

R1R2PC 2 PC 1.10.1.225.226.1.10G0/0/1G0/0/1G0/0/0G0/0/0

Destination MAC	Source MAC	Source IPv4	Destination IPv4
dd-dd-dd	cc-cc-cc	192.168.10.10	10.1.1.10

55-55-55aa-aa-aa192.168.10.0/24209.165.200.224/3010.1.1.0/24Internetbb-bb-bbcc-cc-ccdd-dd-ddeee-ee-ee

The new destination MAC address would be that of the R2 G0/0/1 interface and the new source MAC address would be that of the R1 G0/0/1 interface.

Along each link in a path, an IP packet is encapsulated in a frame. The frame is specific to the data link technology that is associated with that link, such as Ethernet. If the next-hop device is the final destination, the destination MAC address will be that of the device Ethernet NIC, as shown in the figure.

The image is a network diagram showing the source and destination MAC and IPv4 addressing when information exits a router to the final destination as it is sent from a PC on one network to a destination on a remote network. The description that follows are the names, connections, and addressing of devices from left to right. PC 1 is connected to a switch which is connected to router R1 interface G0/0/0 on network 192.168.10.0/24. PC 1 has an IP of 192.168.10.10 and MAC of aa-aa-aa. The R1 G0/0/0 interface has an IP of 192.168.10.1 and MAC of bb-bb-bb. R1 has a G0/0/1 interface connected to router R2 interface G0/0/1 on network 209.165.200.224/30. The R1 G0/0/1 interface has an IP of 209.165.200.225 and MAC cc-cc-cc. The R2 G0/0/1 interface has an IP of 209.165.200.226 and MAC dd-dd-dd. R2 has a G0/0/0 interface connected to a switch connected to PC 2 on network 10.1.1.0/24. The R2 G0/0/0 interface has an IP of 10.1.1.1 and MAC ee-ee-ee. PC 2 has an IP of 10.10.10.10 and MAC 55-55-55. R2 also has a connection at the top leading to the Internet cloud. Below the diagram under network 10.1.1.0/24 are four boxes reading from left to right: Destination MAC 55-55-55, Source MAC ee-ee-ee, Source IPv4 192.168.10.10, and Destination IPv4 10.1.1.10.

R1R2PC 2 PC 1.10.1.225.226.1.10G0/0/1G0/0/1G0/0/0G0/0/0

Destination MAC	Source MAC	Source IPv4	Destination IPv4
55-55-55	ee-ee-ee	192.168.10.10	10.1.1.10

55-55-55aa-aa-aa192.168.10.0/24209.165.200.224/3010.1.1.0/24Internetbb-bb-bbcc-cc-ccdd-dd-ddeee-ee-ee

How are the IP addresses of the IP packets in a data flow associated with the MAC addresses on each link along the path to the destination? For IPv4 packets, this is done through a process called Address Resolution Protocol (ARP). For IPv6 packets, the process is ICMPv6 Neighbor Discovery (ND).

ARP Overview

If your network is using the IPv4 communications protocol, the Address Resolution Protocol, or ARP, is what you need to map IPv4 addresses to MAC addresses. This topic explains how ARP works.

Every IP device on an Ethernet network has a unique Ethernet MAC address. When a device sends an Ethernet Layer 2 frame, it contains these two addresses:

- **Destination MAC address** - The Ethernet MAC address of the destination device on the same local network segment. If the destination host is on another network, then the destination address in the frame would be that of the default gateway (i.e., router).
- **Source MAC address** - The MAC address of the Ethernet NIC on the source host.

The figure illustrates the problem when sending a frame to another host on the same segment on an IPv4 network.

Four hosts, H1, H2, H3, and H4, are connected to the same switch. H1 has an IP of 192.168.1.5/24, H2 has an IP of 192.168.1.6/24, H3 has an IP of 192.168.1.8/24, and H4 has an IP of 192.168.1.7/24. H1 has a callout that reads: I need to send information to 192.168.1.7, but I only have the IP address. I don't know the MAC address of the device that has that IP.



To send a packet to another host on the same local IPv4 network, a host must know the IPv4 address and the MAC address of the destination device. Device destination IPv4 addresses are either known or resolved by device name. However, MAC addresses must be discovered.

A device uses Address Resolution Protocol (ARP) to determine the destination MAC address of a local device when it knows its IPv4 address.

ARP provides two basic functions:

- Resolving IPv4 addresses to MAC addresses
- Maintaining a table of IPv4 to MAC address mappings

9.2.2

ARP Functions

When a packet is sent to the data link layer to be encapsulated into an Ethernet frame, the device refers to a table in its memory to find the MAC address that is mapped to the IPv4 address. This table is stored temporarily in RAM memory and called the ARP table or the ARP cache.

The sending device will search its ARP table for a destination IPv4 address and a corresponding MAC address.

- If the packet's destination IPv4 address is on the same network as the source IPv4 address, the device will search the ARP table for the destination IPv4 address.
- If the destination IPv4 address is on a different network than the source IPv4 address, the device will search the ARP table for the IPv4 address of the default gateway.

In both cases, the search is for an IPv4 address and a corresponding MAC address for the device.

Each entry, or row, of the ARP table binds an IPv4 address with a MAC address. We call the relationship between the two values a map. This simply means that you can locate an IPv4 address in the table and discover the corresponding MAC address. The ARP table temporarily saves (caches) the mapping for the devices on the LAN.

If the device locates the IPv4 address, its corresponding MAC address is used as the destination MAC address in the frame. If there is no entry is found, then the device sends an ARP request.

Click Play in the figure to see an animation of the ARP function.

This animation illustrates how a host will use A R P to discover the MAC address of a known I P address. Host H1 needs to send some information to a host with IP address 192 dot 168 dot 1 dot 7. However, H1 does not have the MAC address for that address. Therefore, it sends an A R P request to I P address 192.168.1.7. All hosts on the network will receive the A R P request. However, only host H4 with IP address 192.168.1.7 will send an A R P reply containing its MAC address. Then H1 can send an envelope to the switch that goes directly to H4.

I must send out an ARP request to learn the MAC address of the host with the IP address of 192.168.1.7.

This isn't me.

This isn't me.

This is me, I will send back my MAC address.

Now I have the MAC. I can forward my information.

Thanks. I got it.

9.2.3

Video - ARP Request

An ARP request is sent when a device needs to determine the MAC address that is associated with an IPv4 address, and it does not have an entry for the IPv4 address in its ARP table.

ARP messages are encapsulated directly within an Ethernet frame. There is no IPv4 header. The ARP request is encapsulated in an Ethernet frame using the following header information:

- **Destination MAC address** – This is a broadcast address FF-FF-FF-FF-FF-FF requiring all Ethernet NICs on the LAN to accept and process the ARP request.
- **Source MAC address** – This is MAC address of the sender of the ARP request.
- **Type** - ARP messages have a type field of 0x806. This informs the receiving NIC that the data portion of the frame needs to be passed to the ARP process.

Because ARP requests are broadcasts, they are flooded out all ports by the switch, except the receiving port. All Ethernet NICs on the LAN process broadcasts and must deliver the ARP request to its operating system for processing. Every device must process the ARP request to see if the target IPv4 address matches its own. A router will not forward broadcasts out other interfaces.

Only one device on the LAN will have an IPv4 address that matches the target IPv4 address in the ARP request. All other devices will not reply.

Click Play in the figure to view a demonstration of an ARP request for a destination IPv4 address that is on the local network.

Play Video

9.2.4

Video - ARP Operation - ARP Reply

Only the device with the target IPv4 address associated with the ARP request will respond with an ARP reply. The ARP reply is encapsulated in an Ethernet frame using the following header information:

- **Destination MAC address** – This is the MAC address of the sender of the ARP request.
- **Source MAC address** – This is the MAC address of the sender of the ARP reply.
- **Type** - ARP messages have a type field of 0x806. This informs the receiving NIC that the data portion of the frame needs to be passed to the ARP process.

Only the device that originally sent the ARP request will receive the unicast ARP reply. After the ARP reply is received, the device will add the IPv4 address and the corresponding MAC address to its ARP table. Packets destined for that IPv4 address can now be encapsulated in frames using its corresponding MAC address.

If no device responds to the ARP request, the packet is dropped because a frame cannot be created.

Entries in the ARP table are time stamped. If a device does not receive a frame from a particular device before the timestamp expires, the entry for this device is removed from the ARP table.

Additionally, static map entries can be entered in an ARP table, but this is rarely done. Static ARP table entries do not expire over time and must be manually removed.

Note: IPv6 uses a similar process to ARP for IPv4, known as ICMPv6 Neighbor Discovery (ND). IPv6 uses neighbor solicitation and neighbor advertisement messages, similar to IPv4 ARP requests and ARP replies.

Click Play in the figure to view a demonstration of an ARP reply.

Play Video

9.2.5

Video - ARP Role in Remote Communications

When the destination IPv4 address is not on the same network as the source IPv4 address, the source device needs to send the frame to its default gateway. This is the interface of the local router. Whenever a source device has a packet with an IPv4 address on another network, it will encapsulate that packet in a frame using the destination MAC address of the router.

The IPv4 address of the default gateway is stored in the IPv4 configuration of the hosts. When a host creates a packet for a destination, it compares the destination IPv4 address and its own IPv4 address to determine if the two IPv4 addresses are located on the same Layer 3 network. If the destination host is not on its same network, the source checks its ARP table for an entry with the IPv4 address of the default gateway. If there is not an entry, it uses the ARP process to determine a MAC address of the default gateway.

Click Play to view a demonstration of an ARP request and ARP reply associated with the default gateway.

Play Video

9.2.6

Removing Entries from an ARP Table

For each device, an ARP cache timer removes ARP entries that have not been used for a specified period of time. The times differ depending on the operating system of the device. For example, newer Windows operating systems store ARP table entries between 15 and 45 seconds, as illustrated in the figure.

ACBR1S1G0/0/0
192.168.1.110/24
MAC 00-0A192.168.1.120/24
MAC 00-0B192.168.1.50/24
MAC 00-0C192.168.1.1/24
MAC 00-0D

I will remove this ARP entry if I have not used it within 15 to 45 seconds.

InternetNote: MAC addresses are shortened for demonstration purposes.

PC A's
ARP
Cache

IPv4 Address	MAC Address
192.168.1.1	00:0D

Commands may also be used to manually remove some or all of the entries in the ARP table. After an entry has been removed, the process for sending an ARP request and receiving an ARP reply must occur again to enter the map in the ARP table.

9.2.7

ARP Tables on Networking Devices

On a Cisco router, the **show ip arp** command is used to display the ARP table, as shown in the figure.

R1# show ip arp

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	192.168.10.1	-	a0e0.af0d.e140	ARPA	GigabitEthernet0/0/0
Internet	209.165.200.225	-	a0e0.af0d.e141	ARPA	GigabitEthernet0/0/1
Internet	209.165.200.226	1	a03d.6fe1.9d91	ARPA	GigabitEthernet0/0/1

R1#

On a Windows 10 PC, the **arp -a** command is used to display the ARP table, as shown in the figure.

C:\Users\PC> arp -a

Interface: 192.168.1.124 --- 0x10

Internet Address	Physical Address	Type
192.168.1.1	c8-d7-19-cc-a0-86	dynamic
192.168.1.101	08-3e-0c-f5-f7-77	dynamic
192.168.1.110	08-3e-0c-f5-f7-56	dynamic
192.168.1.112	ac-b3-13-4a-bd-d0	dynamic
192.168.1.117	08-3e-0c-f5-f7-5c	dynamic

192.168.1.126	24-77-03-45-5d-c4	dynamic
192.168.1.146	94-57-a5-0c-5b-02	dynamic
192.168.1.255	ff-ff-ff-ff-ff-ff	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.251	01-00-5e-00-00-fb	static
239.255.255.250	01-00-5e-7f-ff-fa	static
255.255.255.255	ff-ff-ff-ff-ff-ff	static

C:\Users\PC>

9.2.8

ARP Issues - ARP Broadcasts and ARP Spoofing

As a broadcast frame, an ARP request is received and processed by every device on the local network. On a typical business network, these broadcasts would probably have minimal impact on network performance. However, if a large number of devices were to be powered up and all start accessing network services at the same time, there could be some reduction in performance for a short period of time, as shown in the figure. After the devices send out the initial ARP broadcasts and have learned the necessary MAC addresses, any impact on the network will be minimized.

The diagram shows seven devices on shared media (multiple access) all powered on at the same time. A text box reads: ARP broadcasts can flood the local media.

All devices powered on at the same timeARP broadcasts can flood the local media.Shared Media (multiple access)

In some cases, the use of ARP can lead to a potential security risk. A threat actor can use ARP spoofing to perform an ARP poisoning attack. This is a technique used by a threat actor to reply to an ARP request for an IPv4 address that belongs to another device, such as the default gateway, as shown in the figure. The threat actor sends an ARP reply with its own MAC address. The receiver of the ARP reply will add the wrong MAC address to its ARP table and send these packets to the threat actor. Enterprise level switches include mitigation techniques known as dynamic ARP inspection (DAI). DAI is beyond the scope of this course.

The image is a network diagram showing two hosts, Host A with IP 192.168.1.110/24 and MAC 00-0A and Host B with IP 192.168.1.120/24 and MAC 00-0B, connected to switch S1 which is connected to router R1 at port G0/0/0 (the default gateway with IP 192.168.1.1/24 and MAC 00-0D) which is connected to the Internet cloud. Also connected to S1 is a threat actor at host C with IP 192.168.1.50/24 and MAC 00-0C. Host A has a callout that reads: ARP Request: I need the MAC address of default gateway, 192.168.1.1. The threat actor host C has a callout that reads: I will send an ARP reply and pretend to be the default gateway! Note: MAC addresses are shortened for demonstration purposes.

ABS1R1CA192.168.1.110/24MAC 00-0A192.168.1.120/24MAC 00-0B192.168.1.50/24MAC 00-0C192.168.1.1/24MAC 00-0D
G0/0/0
NetworkNote: MAC addresses are shortened for demonstration purposes. I will send an ARP reply and pretend to be the default gateway!ARP Request: I need the MAC address of default gateway, 192.168.1.1

9.2.9

9.3.1

Video - IPv6 Neighbor Discovery

If your network is using the IPv6 communications protocol, the Neighbor Discovery protocol, or ND, is what you need to match IPv6 addresses to MAC addresses. This topic explains how ND works.

Click Play in the figure to view a demonstration of IPv6 Neighbor Discovery.

Play Video

9.3.2

IPv6 Neighbor Discovery Messages

IPv6 Neighbor Discovery protocol is sometimes referred to as ND or NDP. In this course, we will refer to it as ND. ND provides address resolution, router discovery, and redirection services for IPv6 using ICMPv6. ICMPv6 ND uses five ICMPv6 messages to perform these services:

- Neighbor Solicitation messages
- Neighbor Advertisement messages
- Router Solicitation messages
- Router Advertisement messages
- Redirect Message

Neighbor Solicitation and Neighbor Advertisement messages are used for device-to-device messaging such as address resolution (similar to ARP for IPv4). Devices include both host computers and routers.

:11:102001:db8:acad:1::/64PC1PC2

Router Solicitation and Router Advertisement messages are for messaging between devices and routers. Typically router discovery is used for dynamic address allocation and stateless address autoconfiguration (SLAAC).

:12001:db8:acad:1::/64PC1R1

Note: The fifth ICMPv6 ND message is a redirect message which is used for better next-hop selection. This is beyond the scope of this course.

IPv6 ND is defined in the IETF RFC 4861.

9.3.3

IPv6 Neighbor Discovery - Address Resolution

Much like ARP for IPv4, IPv6 devices use IPv6 ND to determine the MAC address of a device that has a known IPv6 address.

ICMPv6 Neighbor Solicitation and Neighbor Advertisement messages are used for MAC address resolution. This is similar to ARP Requests and ARP Replies used by ARP for IPv4. For example, assume PC1 wants to ping PC2 at IPv6 address 2001:db8:acad::11. To determine the MAC address for the known IPv6 address, PC1 sends an ICMPv6 Neighbor Solicitation message as illustrated in the figure.

The diagram shows PC1 and PC2 connected to the same switch on network 2001:db8:acad:1::/64. PC1 has an IPv6 address 2001:db8:acad:1::10 and PC2 has an IPv6 address of 2001:db8:acad:1::11. PC1 is sending an ICMPv6 neighbor solicitation message that reads: Hey whoever has 2001:db8:acad:1::11, send me your MAC address? PC2 is replying with an ICMPv6 neighbor advertisement message that reads: Hey 2001:db8:acad:1::10, I am 2001:db8:acad:1::11 and my MAC address is f8-94-c3-e4-c5-0A.

:11:102001:db8:acad:1::/64PC1PC2

ICMPv6 Neighbor Advertisement Message

*"Hey 2001:db8:acad:1::10, I am 2001:db8:acad:1::11 and my MAC address is f8-94-c3-e4-c5-0A."***ICMPv6 Neighbor Solicitation Message**
"Hey whoever has 2001:db8:acad:1::11, send me your MAC address?"

ICMPv6 Neighbor Solicitation messages are sent using special Ethernet and IPv6 multicast addresses. This allows the Ethernet NIC of the receiving device to determine whether the Neighbor Solicitation message is for itself without having to send it to the operating system for processing.

PC2 replies to the request with an ICMPv6 Neighbor Advertisement message which includes its MAC address.

10.1.1

Basic Router Configuration Steps

The following tasks should be completed when configuring initial settings on a router.

1. Configure the device name.

```
Router(config)# hostname hostname
```

2. Secure privileged EXEC mode.

```
Router(config)# enable secret password
```

3. Secure user EXEC mode.

```
Router(config)# line console 0  
Router(config-line)# password password  
Router(config-line)# login
```

4. Secure remote Telnet / SSH access.

```
Router(config-line)# line vty 0 4  
Router(config-line)# password password  
Router(config-line)# login  
Router(config-line)# transport input {ssh | telnet}
```

5. Secure all passwords in the config file.

```
Router(config-line)# exit  
Router(config)# service password-encryption
```

6. Provide legal notification.

```
Router(config)# banner motd delimiter message delimiter
```

7. Save the configuration.

```
Router(config)# end  
Router# copy running-config startup-config
```

10.1.2

Basic Router Configuration Example

In this example, router R1 in the topology diagram will be configured with initial settings.

The figure shows a network topology diagram with two PCs, two switches, two routers, and an internet cloud. From left to right PC 1 connects to a switch which connects to R1 which connects to R2 which connects to a second switch, which connects to PC2. PC1 is on the 192.168.10.0/24 IPv4 network and has IPv4 address 192.168.10.10. PC1 also connects to the 2001:db8:acad:10::/64 IPv6 network and has IPv6 address 2001:db8:acad:10::10. Router R1 G0/0/0 interface is on the same network as PC1. The IPv4 and IPv6 address of the G0/0/0 interface of R1 is 192.168.10.1 and 2001:db8:acad:10::1. The IPv4 network connecting R1 and R2 is 209.165.200.224/30. The IPv6 network connecting R1 and R2 is 2001:db8:feed:224::/64. R1 connects to R2 over interface G0/0/1 which has IPv4 address 209.165.200. 225 and IPv6 address 2001:db8:feed:224::1. The IP addresses for R2 on the shared network with R1 are 209.165.200. 226 and 2001:db8:feed:224::2. PC2 and R2 are connected on IPv4 network 10.1.1.0/24 and IPv6 network 2001:db8:cafe:1::/64. PC1 has IPv4 address 10.1.1.10 and IPv6 address 2001:db8:cafe::10. R2 has IPv4 address 10.1.1.1 and IPv6 address 2001:db8:cafe::1.

.10::10192.168.10.0/24.1::1G0/0/0G0/0/1.225::1.226::2.1::1209.165.200.224/3010.1.1.0/24.10::102001:db8:acad:10::/642001:db8:feed:224::/642001:db8:cafe:1::/64PC1PC2R1R2
Internet

To configure the device name for R1, use the following commands.

```
Router> enable
```

```
Router# configure terminal
```

```
Enter configuration commands, one per line.
```

```
End with CNTL/Z.
```

```
Router(config)# hostname R1
```

```
R1(config)#
```

Note: Notice how the router prompt now displays the router hostname.

All router access should be secured. Privileged EXEC mode provides the user with complete access to the device and its configuration. Therefore, it is the most important mode to secure.

The following commands secure privileged EXEC mode and user EXEC mode, enable Telnet and SSH remote access, and encrypt all plaintext (i.e., user EXEC and VTY line) passwords.

```
R1(config)# enable secret class
```

```
R1(config)#
```

```
R1(config)# line console 0
```

```
R1(config-line)# password cisco
```

```
R1(config-line)# login
```

```
R1(config-line)# exit
```

```
R1(config)#
```

```
R1(config)# line vty 0 4
```

```
R1(config-line)# password cisco
```

```
R1(config-line)# login
```

```
R1(config-line)# transport input ssh telnet
```

```
R1(config-line)# exit
```

```
R1(config)#
```

```
R1(config)# service password-encryption
```

```
R1(config)#
```

The legal notification warns users that the device should only be accessed by permitted users. Legal notification is configured as follows.

```
R1(config)# banner motd #
```

```
Enter TEXT message. End with a new line and the #
```

```
*****
```

```
WARNING: Unauthorized access is prohibited!
```



```
*****
```

```
#
```

```
R1(config)#
```

If the previous commands were configured and the router accidently lost power, all configured commands would be lost. For this reason, it is important to save the configuration when changes are implemented. The following command saves the configuration to NVRAM.

```
R1# copy running-config startup-config
```

```
Destination filename [startup-config]?
```

```
Building configuration...
```

```
[OK]
```

```
R1#
```

10.1.3

Syntax Checker - Configure Initial Router Settings

Use this syntax checker to practice configuring the initial settings on a router.

- Configure the device name.
- Secure the privileged EXEC mode.
- Secure and enable remote SSH and Telnet access.
- Secure all plaintext passwords.
- Provide legal notification.

Enter global configuration mode to configure the name of the router as “R1”.

```
Router>
```

ResetShow MeShow All

10.2.1

Configure Router Interfaces

At this point, your routers have their basic configurations. The next step is to configure their interfaces. This is because routers are not reachable by end devices until the interfaces are configured. There are many different types of interfaces available on Cisco routers. For example, the Cisco ISR 4321 router is equipped with two Gigabit Ethernet interfaces:

- **GigabitEthernet 0/0/0 (G0/0/0)**
- **GigabitEthernet 0/0/1 (G0/0/1)**

The task to configure a router interface is very similar to a management SVI on a switch. Specifically, it includes issuing the following commands:

```
Router(config)# interface type-and-number
Router(config-if)# description description-text
Router(config-if)# ip address ipv4-address subnet-mask
Router(config-if)# ipv6 address ipv6-address/prefix-length
Router(config-if)# no shutdown
```

Note: When a router interface is enabled, information messages should be displayed confirming the enabled link.

Although the **description** command is not required to enable an interface, it is good practice to use it. It can be helpful in troubleshooting on production networks by providing information about the type of network connected. For example, if the interface connects to an ISP or service carrier, the **description** command would be helpful to enter the third-party connection and contact information.

Note: The *description-text* is limited to 240 characters.

Using the **no shutdown** command activates the interface and is similar to powering on the interface. The interface must also be connected to another device, such as a switch or a router, for the physical layer to be active.

Note: On inter-router connections where there is no Ethernet switch, both interconnecting interfaces must be configured and enabled.

10.2.2

Configure Router Interfaces Example

In this example, the directly connected interfaces of R1 in the topology diagram will be enabled.

The diagram is a network topology showing the IPv4 and IPv6 addressing of the network devices. What follows is a description of the topology from left to right. PC1 is connected to a switch connected to router R1. The network IPv4 address is 192.168.10.0/24 and the IPv6 address is 2001:db8:acad:10::/64. PC1 has an address of .10 and ::10. Interface G0/0/0 on R1 has an address of .1 and ::1. R1 interface G0/0/1 is then connected to router R2 on IPv4 network 209.165.200.224/30 and IPv6 network 2001:db8:feed:224::/64. Interface G0/0/1 on R1 has an address of .225 and ::1. The interface on R2 has an address of .226 and ::2. R2 is then connected to a switch which is connected to PC2 on IPv4 network 10.1.1.0/24 and IPv6 network 2001:db8:cafe:1::/64. The R2 interface has an address of .1 and ::1. PC2 has an address of .10 and ::10. R2 also has a connection to the Internet cloud.

.10::10192.168.10.0/24.1::1G0/0/0G0/0/1.225::1.226::2.1::1209.165.200.224/3010.1.1.0/24.10::102001:db8:acad:10::/642001:db8:feed:224::/642001:db8:cafe:1::/64PC1PC2R1R2
Internet

To configure the the interfaces on R1, use the following commands.

```
R1> enable
```

```
R1# configure terminal
```

```
Enter configuration commands, one per line.
```

```
End with CNTL/Z.
```

```
R1(config)# interface gigabitEthernet 0/0/0
```

```
R1(config-if)# description Link to LAN
```

```
R1(config-if)# ip address 192.168.10.1 255.255.255.0
```

```
R1(config-if)# ipv6 address 2001:db8:acad:10::1/64
```

```
R1(config-if)# no shutdown
```

```
R1(config-if)# exit
```

```
R1(config)#
```

```
*Aug  1 01:43:53.435: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, changed state to
down
```

```
*Aug  1 01:43:56.447: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, changed state to
up
```

```
*Aug  1 01:43:57.447: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0/0, changed state to up
```

```
R1(config)#
```

```
R1(config)#
```

```
R1(config)# interface gigabitEthernet 0/0/1
```

```
R1(config-if)# description Link to R2
```

```
R1(config-if)# ip address 209.165.200.225 255.255.255.252
```

```
R1(config-if)# ipv6 address 2001:db8:feed:224::1/64
```

```
R1(config-if)# no shutdown
```

```
R1(config-if)# exit
```

```
R1(config)#
```

```
*Aug  1 01:46:29.170: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/1, changed state to
down
```

```
*Aug  1 01:46:32.171: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/1, changed state to
up
```

```
*Aug  1 01:46:33.171: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0/1, changed state to up
```

```
R1(config)#
```

Note: Notice the informational messages informing us that G0/0/0 and G0/0/1 are enabled.

10.2.3

Verify Interface Configuration

There are several commands that can be used to verify interface configuration. The most useful of these is the **show ip interface brief** and **show ipv6 interface brief** commands, as shown in the example.

```
R1# show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
-----------	------------	-----	--------	--------	----------

GigabitEthernet0/0/0	192.168.10.1	YES	manual	up	up
----------------------	--------------	-----	--------	----	----

GigabitEthernet0/0/1	209.165.200.225	YES	manual	up	up
----------------------	-----------------	-----	--------	----	----

Vlan1	unassigned	YES	unset	administratively down	down
-------	------------	-----	-------	-----------------------	------

R1#	show ipv6 interface brief
-----	---------------------------

GigabitEthernet0/0/0	[up/up]
----------------------	---------

FE80::201:C9FF:FE89:4501

2001:DB8:ACAD:10::1

GigabitEthernet0/0/1	[up/up]
----------------------	---------

FE80::201:C9FF:FE89:4502

2001:DB8:FEED:224::1

Vlan1	[administratively down/down]
-------	------------------------------

unassigned

R1#

Configuration Verification Commands

The table summarizes the more popular **show** commands used to verify interface configuration.

Table caption	
Commands	Description
show ip interface brief show ipv6 interface brief	The output displays all interfaces, their IP addresses, and their current status. The configured and connected interfaces should display a Status of “up” and Protocol of “up”. Anything else would indicate a problem with either the configuration or the cabling.
show ip route show ipv6 route	Displays the contents of the IP routing tables stored in RAM.
show interfaces	Displays statistics for all interfaces on the device. However, this command will only display the IPv4 addressing information.
show ip interface	Displays the IPv4 statistics for all interfaces on a router.
show ipv6 interface	Displays the IPv6 statistics for all interfaces on a router.

Click each button to see the command output for each configuration verification command.

- show ip interface brief
- show ipv6 interface brief
- show ip route
- show ipv6 route
- show interfaces
- show ip interface
- show ipv6 interface

```
R1# show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0/0	192.168.10.1	YES	manual	up	up
GigabitEthernet0/0/1	209.165.200.225	YES	manual	up	up
Vlan1	unassigned	YES	unset	administratively down	down

```
R1#
```

10.2.5

Syntax Checker - Configure Interfaces

Use this syntax checker to practice configuring the GigabitEthemet 0/0 interface on a router.

- Describe the link as 'Link to LAN'.
- Configure the IPv4 address as 192.168.10.1 with the subnet mask 255.255.255.0.
- Configure the IPv6 address as 2001:db8:acad:10::1 with the /64 prefix length.
- Activate the interface.

```
Enter global configuration mode.  
  
R1#
```

10.3.1

Default Gateway on a Host

If your local network has only one router, it will be the gateway router and all hosts and switches on your network must be configured with this information. If your local network has multiple routers, you must select one of them to be the default gateway router. This topic explains how to configure the default gateway on hosts and switches.

For an end device to communicate over the network, it must be configured with the correct IP address information, including the default gateway address. The default gateway is only used when the host wants to send a packet to a device on another network. The default gateway address is generally the router interface address attached to the local network of the host. The IP address of the host device and the router interface address must be in the same network.

For example, assume an IPv4 network topology consisting of a router interconnecting two separate LANs. G0/0/0 is connected to network 192.168.10.0, while G0/0/1 is connected to network 192.168.11.0. Each host device is configured with the appropriate default gateway address.

In this example, if PC1 sends a packet to PC2, then the default gateway is not used. Instead, PC1 addresses the packet with the IPv4 address of PC2 and forwards the packet directly to PC2 through the switch.

The diagram is a network topology with one router, two switches, and four PCs showing the flow of information between devices on the same network. PC1 and PC2 are connected to the switch on network 192.168.10.0/24 at interface G0/0/0 on router R1. PC3 and PC4 are connected to another switch on network 192.168.11.0/24 at interface G0/0/1 on R1. An arrow shows the flow of information sent from PC1 passing through the attached switch on its way to PC2.

PC!PC!.10.11192.168.10.0/24.1G0/0/0G0/0/1.1.10.11192.168.11.0/24R1PC1PC2PC3PC4

What if PC1 sent a packet to PC3? PC1 would address the packet with the IPv4 address of PC3, but would forward the packet to its default gateway, which is the G0/0/0 interface of R1. The router accepts the packet and accesses its routing table to determine that G0/0/1 is the appropriate exit interface based on the destination address. R1 then forwards the packet out of the appropriate interface to reach PC3.

The diagram is a network topology with one router, two switches, and four PCs showing the flow of information between devices on different networks. PC1 and PC2 are connected to the switch on network 192.168.10.0/24 at interface G0/0/0 on router R1. PC3 and PC4 are connected to another switch on network 192.168.11.0/24 at interface G0/0/1 on R1. An arrow shows the flow of information sent from PC1 passing through R1 and onto PC3.

PC1PC2192.168.10.0/24192.168.11.0/24R1PC3PC4

The same process would occur on an IPv6 network, although this is not shown in the topology. Devices would use the IPv6 address of the local router as their default gateway.

10.3.2

Default Gateway on a Switch

A switch that interconnects client computers is typically a Layer 2 device. As such, a Layer 2 switch does not require an IP address to function properly. However, an IP configuration can be configured on a switch to give an administrator remote access to the switch.

To connect to and manage a switch over a local IP network, it must have a switch virtual interface (SVI) configured. The SVI is configured with an IPv4 address and subnet mask on the local LAN. The switch must also have a default gateway address configured to remotely manage the switch from another network.

The default gateway address is typically configured on all devices that will communicate beyond their local network.

To configure an IPv4 default gateway on a switch, use the **ip default-gateway ip-address** global configuration command. The *ip-address* that is configured is the IPv4 address of the local router interface connected to the switch.

The figure shows an administrator establishing a remote connection to switch S1 on another network.

The diagram is a network topology showing a router R1 connected to two switches, S1 on network 192.168.10.0/24, and S2 on network 192.168.11.0/24. A user is connected to S2 and an arrow shows the user is accessing S1 remotely. Above the user is a box showing the user has CLI access to S1 and is displaying the running configuration.

S1# show running-configBuilding configuration...!service password-encryption!hostname S1!Interface Vlan1 ip address 192.168.10.50 255.255.255.0!!ip default-gateway 192.168.10.11G0/0/0.1G0/0/1PC1PC2S2.10.11192.168.10.0/24192.168.11.0/24S1R1.50



In this example, the administrator host would use its default gateway to send the packet to the G0/0/1 interface of R1. R1 would forward the packet to S1 out of its G0/0/0 interface. Because the packet source IPv4 address came from another network, S1 would require a default gateway to forward the packet to the G0/0/0 interface of R1. Therefore, S1 must be configured with a default gateway to be able to reply and establish an SSH connection with the administrative host.

Note: Packets originating from host computers connected to the switch must already have the default gateway address configured on their host computer operating systems.

A workgroup switch can also be configured with an IPv6 address on an SVI. However, the switch does not require the IPv6 address of the default gateway to be configured manually. The switch will automatically receive its default gateway from the ICMPv6 Router Advertisement message from the router.

10.3.3

Syntax Checker - Configure the Default Gateway

Use this syntax checker to practice configuring the default gateway of a Layer 2 switch.

Enter global configuration mode.

S1#
ResetShow MeShow All