Network Addressing and Basic Troubleshooting

Module 1:Physical Layer

Introduction

Added Note: The course doesn't specifically state this, so I'm putting it here. When looking at IP addressing in a CLI, when you see [up/up] or [down/down] or any combination, here is what that means:

In Cisco IOS terminology, the `[up/up]` status represents the **Layer 1 (Physical)** and **Layer 2 (Data Link)** states of an interface.

The Two-Part Status

The status is read as **[Status / Protocol]**:

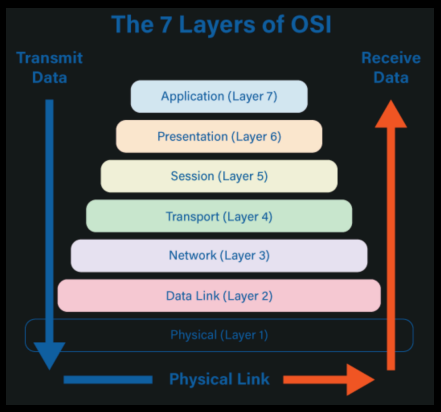
1. **Status (Physical Layer):** Indicates if the hardware is receiving a signal (e.g., cable is plugged in, electricity is flowing).
2. **Protocol (Data Link Layer):** Indicates if the software "keepalives" or framing (like Ethernet or PPP) are successfully communicating with the device on the other end.

Status	Meaning	Typical Cause
up / up	Fully operational.	Normal working state.
down / down	Physical failure.	Cable unplugged, device at other end is off, or interface is `shutdown`.
up / down	Physical is fine; Layer 2 failed.	Encapsulation mismatch (e.g., HDLC vs PPP), clock rate issues on Serial, or authentication failure.
down / up	**Impossible.**	Software protocol cannot be active if the physical hardware is not detecting a signal.
admin down / down	Manually disabled.	You (the admin) issued the `shutdown` command.

The Physical Connection

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



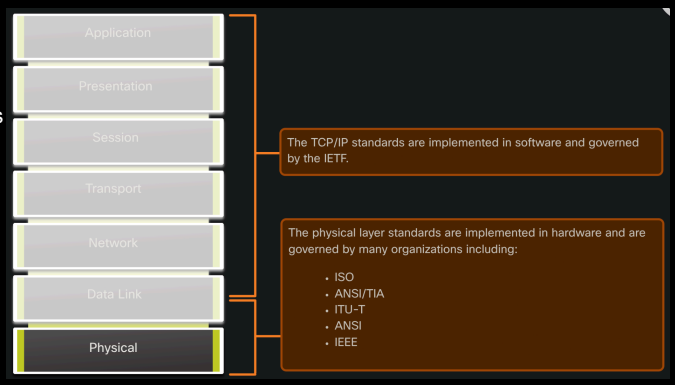
Similar to a corporate office, most homes offer both wired and wireless connectivity to the network. The figures show a home router and a laptop connecting to the local area network (LAN).
Network Interface Cards

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.

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.

Press 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.

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**)
- American National Standards Institute (**ANSI**)/Telecommunications Industry Association (**TIA**)
- International Telecommunication Union (**ITU**)
- 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.

Physical Components

The physical layer standards address three functional areas:

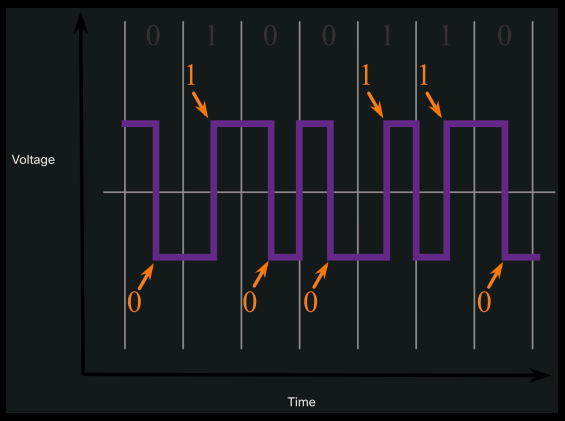
- Physical Components
- Encoding
- Signaling

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.

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.



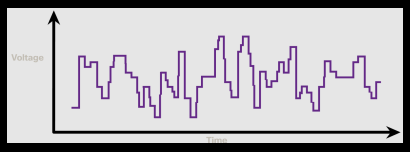
For example, Manchester encoding represents a 0 bit by a high to low voltage transition, and a 1 bit is represented as a low to high voltage transition. An example of Manchester encoding is illustrated in the figure. The transition occurs at the middle of each bit period. This type of encoding is used 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.

Signaling

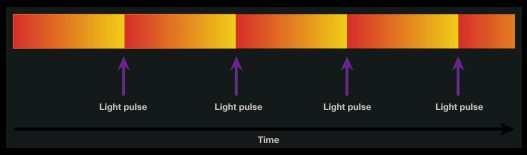
The physical layer must generate the electrical, optical, or wireless signals that represent the "1" and "0" on the media. The way that bits are represented is called the signaling method. The physical layer standards must define what type of signal represents a "1" and what type of signal represents 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.

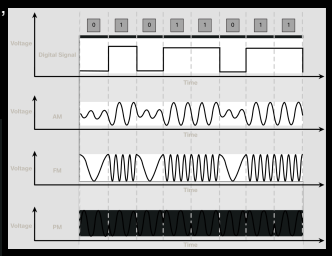
This is similar to the signaling method used in Morse code, which may use a series of on-off tones, lights, or clicks to send text over telephone wires or between ships at sea.

This is Copper Cable



This is Fiber Optic





This is Microwave Signals over Wireless

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.

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

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.

Copper Cabling

Characteristics of Copper Cabling

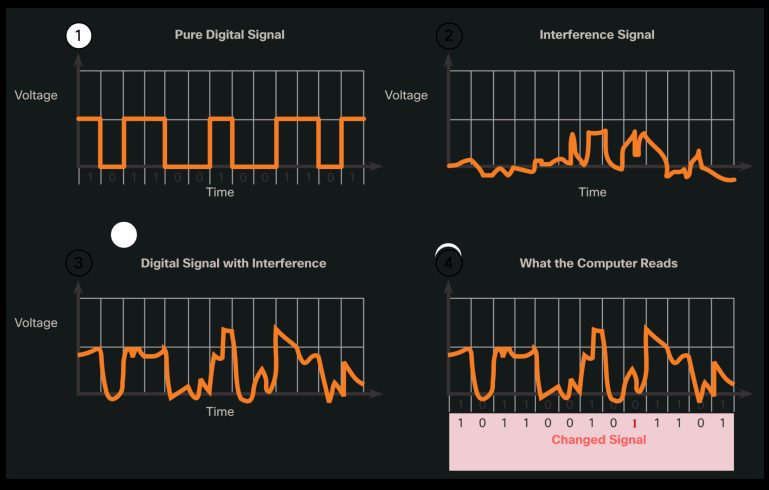
Copper cabling is the most common type of cabling used in networks today. In fact, copper cabling is not just one type of cable. There are three different types of copper cabling that are each used in specific situations.

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.

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:

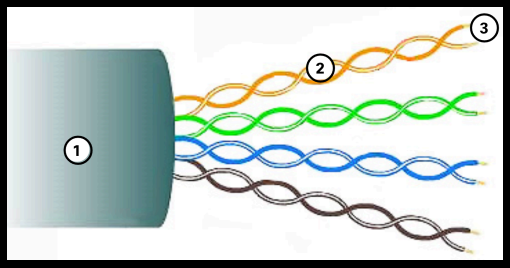
- Selecting the cable type or category most suited to a given networking environment
- Designing a cable infrastructure to avoid known and potential sources of interference in the building structure
- Using cabling techniques that include the proper handling and termination of the cables

Types of Copper Cabling

There are 3 main types

1. UTP
2. STP
3. Coaxial

Unshielded Twisted-Pair (UTP)

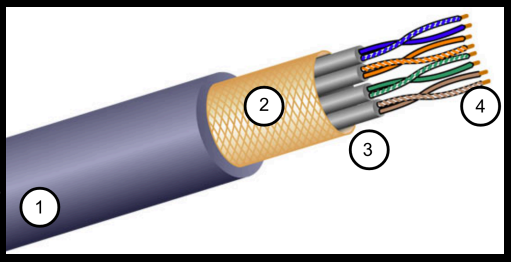


Unshielded twisted-pair (UTP) cabling is the most common networking media. UTP cabling, terminated with RJ-45 connectors, is used for interconnecting network hosts with intermediary networking devices, such as switches and routers.

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 the wires 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 to aid in cable termination.

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.

Coaxial Cable

UTP Cabling

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:

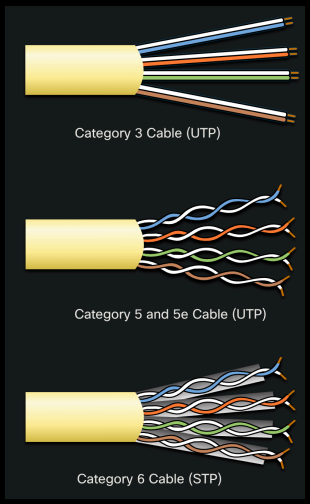
- Cancellation - Designers now pair wires in a circuit. When two wires in an electrical circuit are placed close together, their magnetic fields are the exact opposite of each other. Therefore, the two magnetic fields cancel each other and also cancel out any outside EMI and RFI signals.
- Varying the 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.

UTP Cabling Standards and Connectors

UTP cabling conforms to the standards established jointly by the ANSI/TIA. Specifically, ANSI/TIA-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 (5e), 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 are 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.

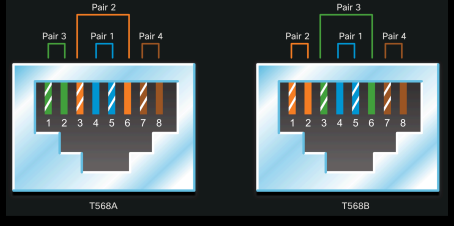
Some manufacturers are making cables exceeding the ANSI/TIACategory 6a specifications and refer to these as Category 7.

Straight-through and Crossover UTP Cables

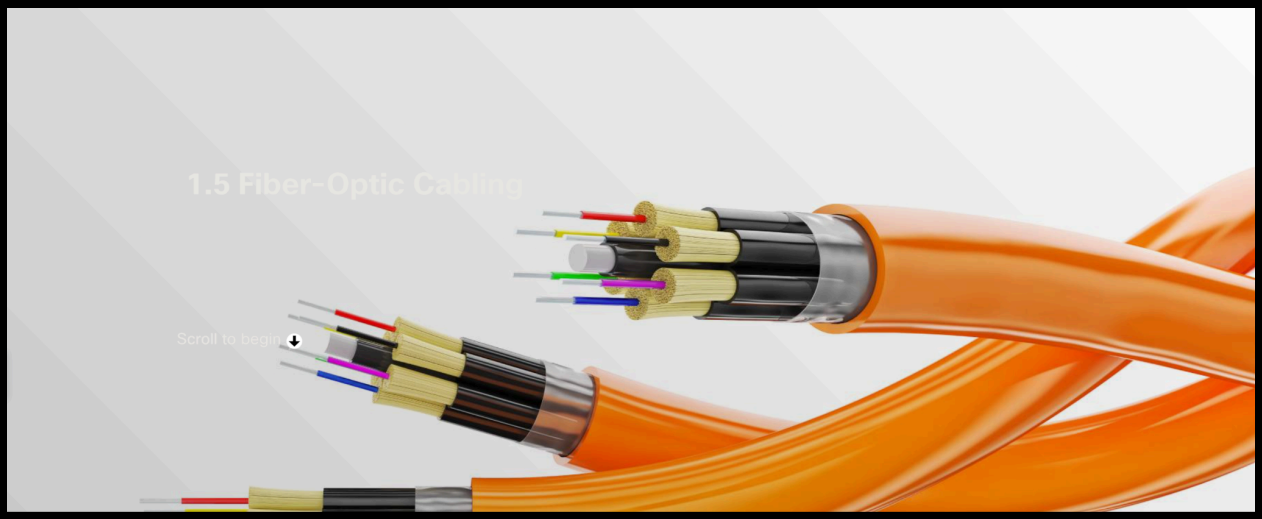
Different situations may require UTP cables to be wired according to different wiring conventions. This means that the individual wires in the cable have to be connected in different orders to different sets of pins in the RJ-45 connectors.
The following are the main cable types that are obtained by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



T568A and T568B Standards



[Fiber optic Cabling]

Properties of Fiber-Optic Cabling

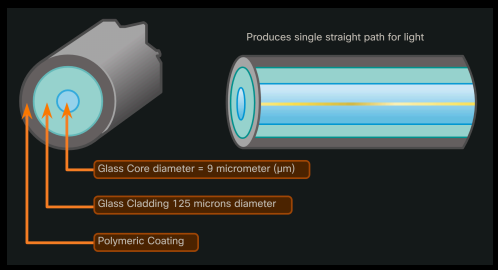
As you have learned, fiber-optic cabling is the other type of cabling used in networks. Because it is expensive, it is not as commonly used as the various types of copper cabling. But fiber-optic cabling has certain properties that make it the best option in certain situations, which you will discover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

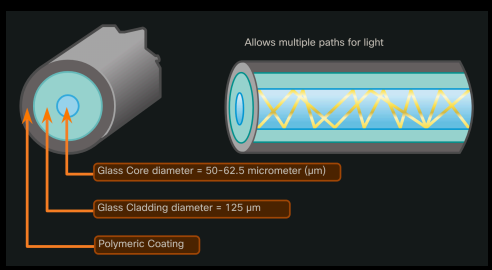
As an analogy, consider an empty paper towel roll with the inside coated like a mirror. It is a thousand meters in length, and a small laser pointer is used to send Morse code signals at the speed of light. Essentially that is how a fiber-optic cable operates, except that it is smaller in diameter and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

Types of Fiber Media



Fiber-optic cables are broadly classified into two types:

- Single-mode fiber (SMF)
  - 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.



- Multimode fiber (MMF)
  - MMF consists of a larger core and uses LED emitters to send light pulses. Specifically, light from an LED enters the multimode fiber at different angles, as shown in the figure. MMFs are popular in LANs because they can be powered by low-cost LEDs. It provides bandwidth up to 10 Gbps over link lengths of up to 550 meters.

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.

Fiber-Optic Cabling Usage

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

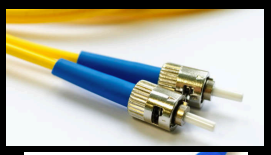
- Enterprise Networks - This is used for backbone cabling applications and interconnecting infrastructure devices.
- Fiber-to-the-Home (FTTH) - This is used to provide always-on broadband services to homes and small businesses.
- Long-Haul Networks - This is used by service providers to connect countries and cities.
- Submarine Cable Networks - This is 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.

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.



Straight-Tip (ST) Connectors

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

Subscriber Connector (SC) Connectors

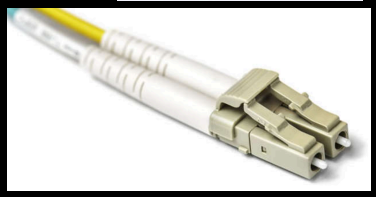
- SC connectors are sometimes referred to as 'square connectors' or 'standard connectors'. They are a widely-adopted LAN and WAN connector that uses a push-pull mechanism to ensure positive insertion. This connector type is used with multimode and single-mode fiber.

Lucent Connector (LC) Simplex Connectors

- LC simplex connectors are a smaller version of the SC connector. These are sometimes called little or local connectors and are quickly growing in popularity due to their smaller size.

Duplex Multimode LC Connectors

- A duplex multimode LC connector is similar to an LC simplex connector, but uses a duplex connector.



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.

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.

Fiber versus Copper

There are many advantages to using fiber-optic cable compared to copper cable. 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

Implementation Issues	UTP Cabling	Fiber-Optic Cabling
Bandwidth supported	10 Mbps - 10 Gbps	10 Mbps - 100 Gbps
Distance	Relatively short (1 - 100 meters)	Relatively long (1 - 100,000 meters)
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

Module 2: Data Link Layer

Topologies

Physical and Logical Topologies

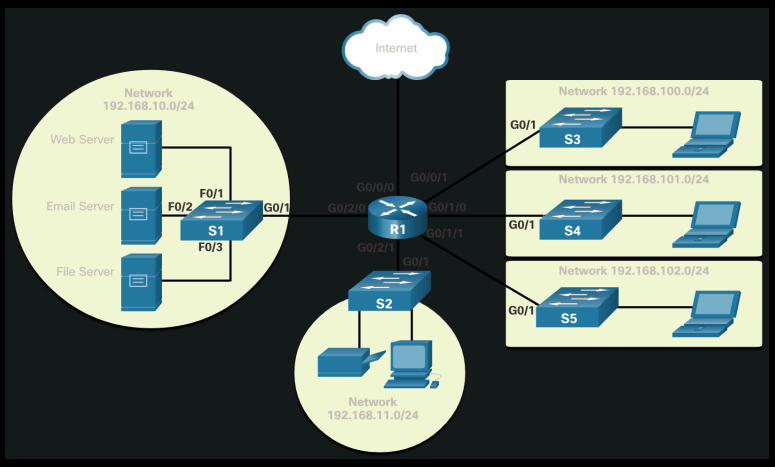
The topology of a network is the arrangement, or the relationship, of the network devices and the interconnections between them.

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

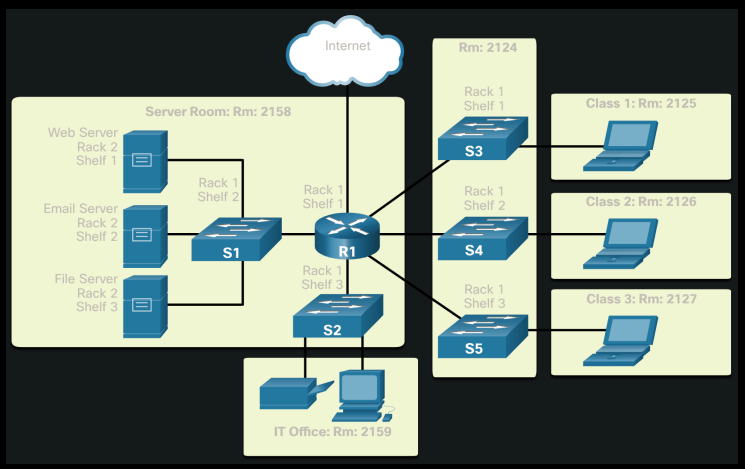
- Physical topology – Identifies the physical connections and how end devices and intermediary devices (i.e, routers, switches, and wireless access points) are interconnected. The topology may also include specific device location such as room number and location on the equipment rack. Physical topologies 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.
Physical Topology

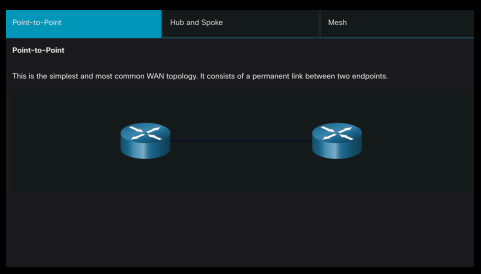
Logical Topology

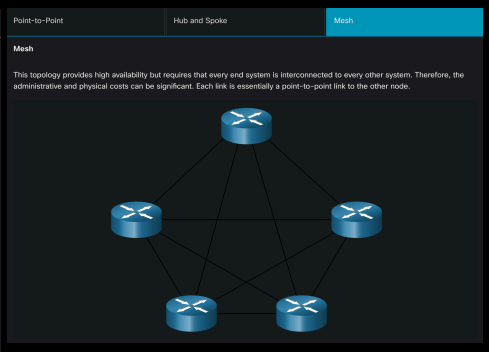


Physical Topology



WAN Topologies





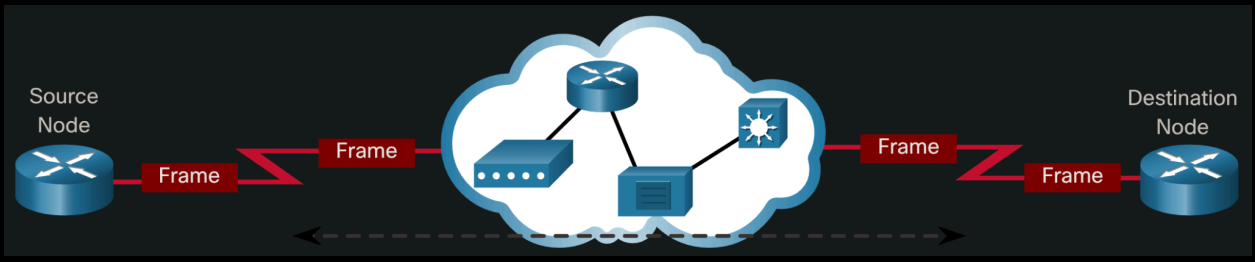
- Point-to-Point
- Hub and Spoke
- Mesh

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.

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

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.



LAN Topologies

Media Access Control Methods

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.

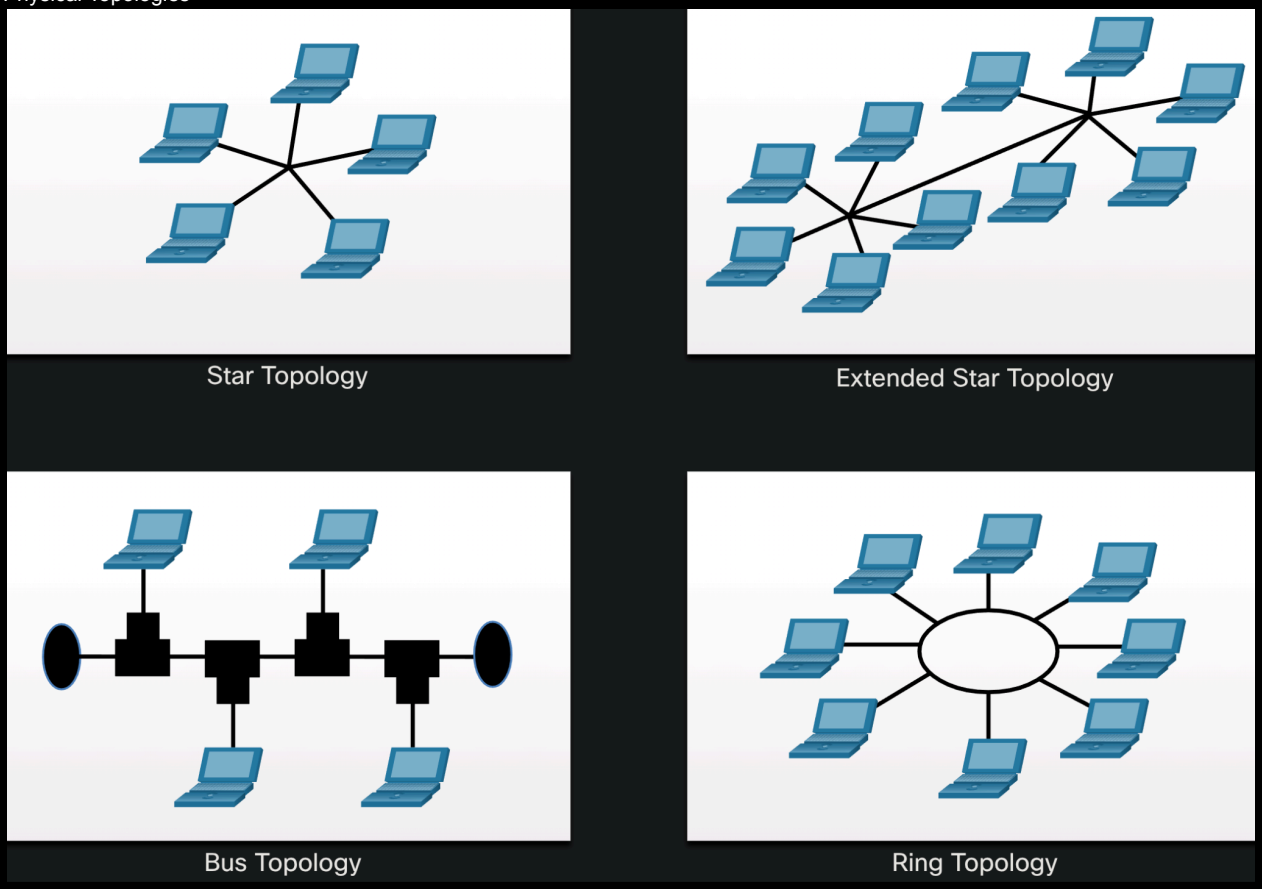
Legacy LAN Topologies

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 neighbors 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.

Physical Topologies



Media Access Control Methods

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. Press play in the figure to see the animation showing half-duplex communication.

- **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. Press play in the figure to see the animation showing full-duplex communication.

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.

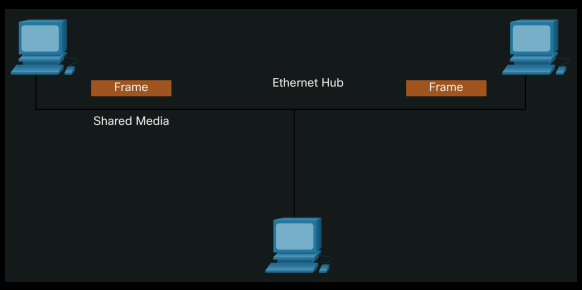
Access Control Methods

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

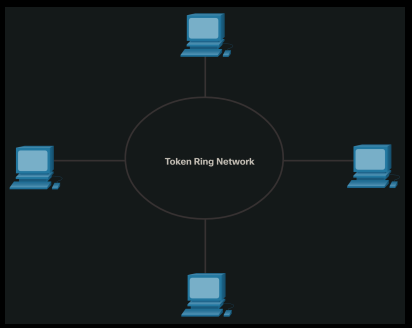
In contention-based multiaccess networks, all nodes are operating in half-duplex, competing for the use of the medium. However, only one device can send at a time. Therefore, there is a process if more than one device transmits at the same time. Examples of contention-based access methods include the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



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



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.

Contention-Based Access - CSMA/CD

Examples of contention-based access networks include the following:

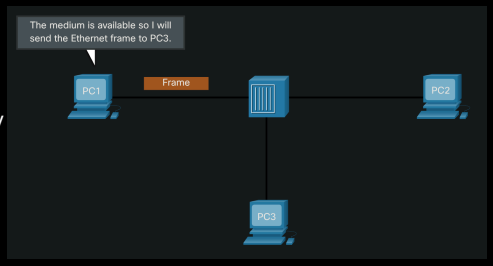
- Wireless LAN (uses CSMA/CA)
- Legacy bus-topology Ethernet LAN (uses CSMA/CD)
- Legacy Ethernet LAN using a hub (uses CSMA/CD)

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.

1. PC1 Sends a 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.

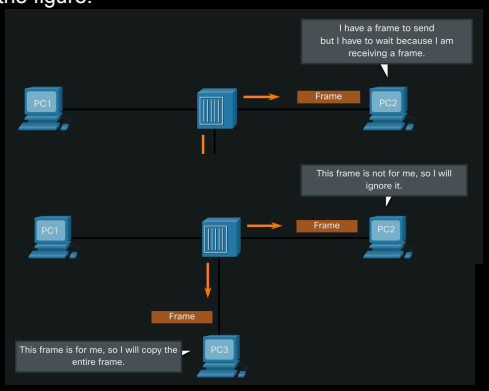


The PC1 NIC sends the Ethernet Frame when the medium is available, as shown in the figure.

2. The Hub Receives the Frame

The Ethernet hub receives and sends the frame. An Ethernet hub is also known as a multiport repeater. Any bits received on an incoming port are regenerated and sent out all other ports, as shown in the figure.

If another device, such as PC2, wants to transmit, but is currently receiving a frame, it must wait until the channel is clear, as shown in the figure.



3. The Hub Sends the Frame

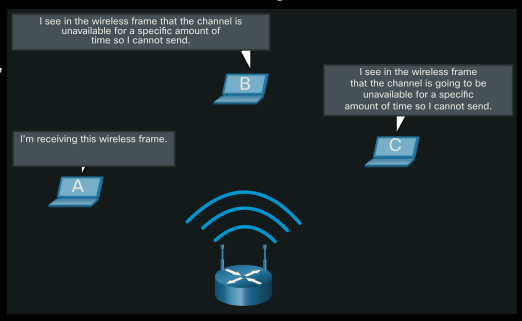
All devices attached to the hub will receive the frame. However, because the frame has a destination data link address for PC3, only that device will accept and copy in the entire frame. All other device NICs will ignore the frame, as shown in the figure.

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.



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.

Module 3: Routing at the Network Layer

How a host routes

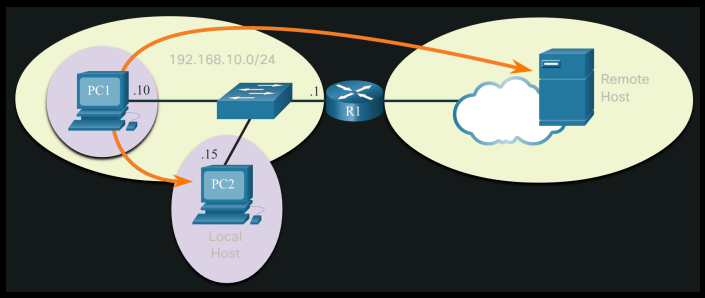
Host Forwarding Decision

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.



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.

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:

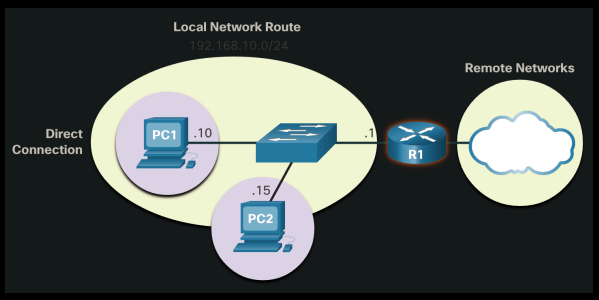
- It has a local IP address in the same address range as other hosts on the local network.
- It can accept data into the local network and forward data out of the local network.
- It routes traffic to other networks.

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.

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.



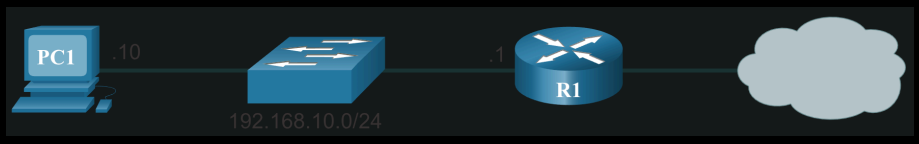
Having a default gateway configured creates a default route in the routing table of the PC. A default route is the route or pathway your computer will take when it tries to contact a remote network.

Both PC1 and PC2 will have a default route to send all traffic destined to remote networks to R1.

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.



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.

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)
```

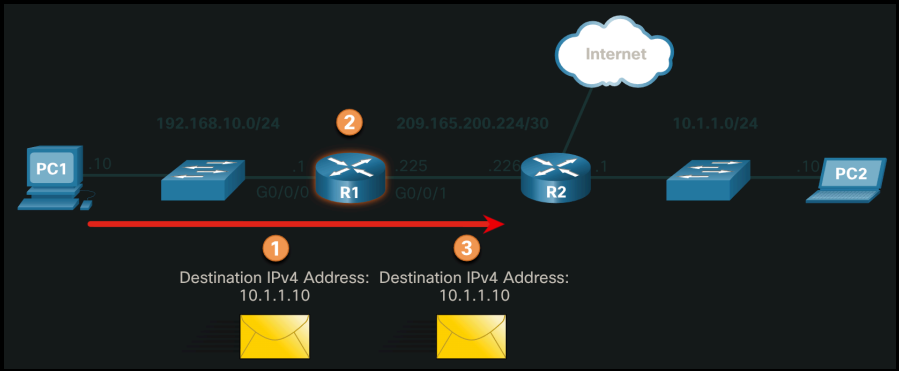
Routing Tables

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.



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.*

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**
Default Route 0.0.0.0/0	via R2

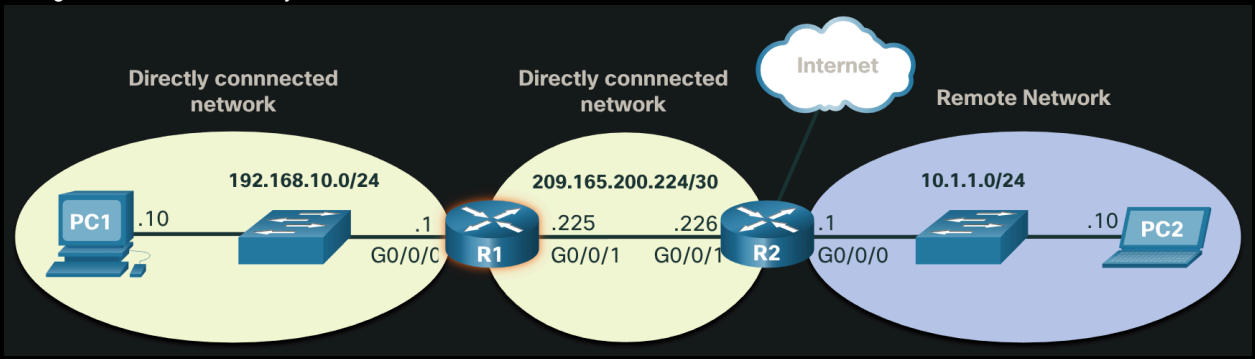
IP Router Routing Table

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.



R1 has two directly connected networks:

- *192.168.10.0/24*
- *209.165.200.224/30*

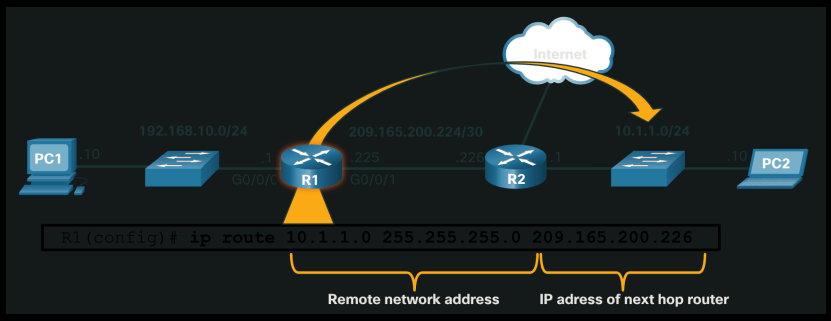
R1 also has remote networks (i.e. 10.1.1.0/24 and the internet) that it can learn about.

A router can learn about remote networks in one of two ways:

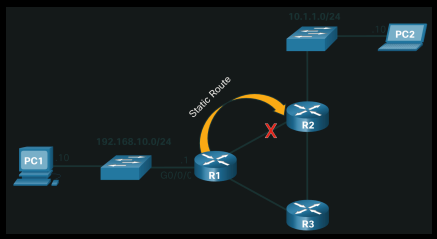
- **Manually** - Remote networks are manually entered into the route table using static routes.
- **Dynamically** - Remote routes are automatically learned using a dynamic routing protocol.

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.



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.

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.

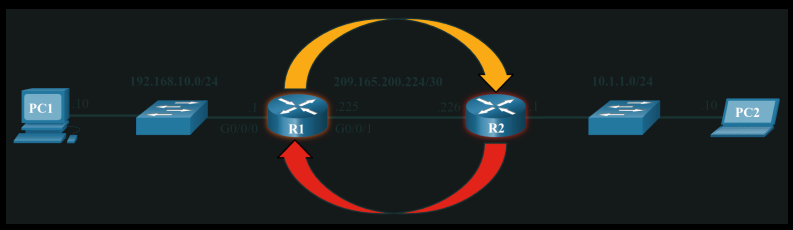
Static routing has the following characteristics:

- 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.

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 Open Shortest Path First (**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.

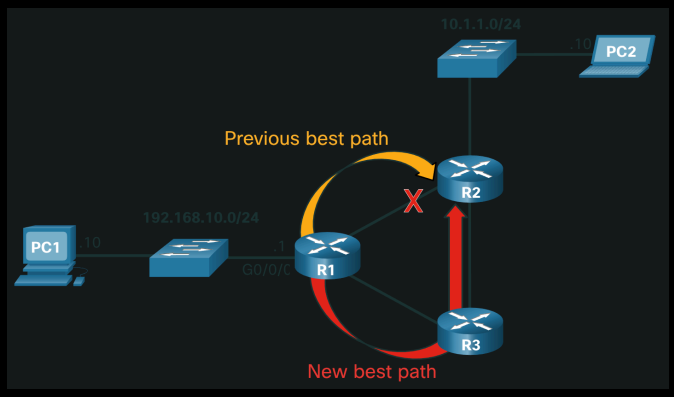


- R1 is using the routing protocol OSPF to let R2 know about the 192.168.10.0/24 network.
- R2 is using the routing protocol OSPF to let R1 know about the 10.1.1.0/24 network.

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.



R1, R2, and R3 are using the dynamic routing protocol Open Shortest Path First (**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.

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 Open Shortest Path First (**OSPF**) routing to advertise directly connected networks.

```
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        192.168.10.1/24 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** - Open Shortest Path First (**OSPF**)
- **D** - Enhanced Interior Gateway Routing Protocol (**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.

Module 4: IPv6 Addressing

IPv6 Address Types

Unicast, Multicast, Anycast

As with IPv4, there are different types of IPv6 addresses. In fact, there are three broad categories of IPv6 addresses:

- Unicast - An IPv6 unicast address uniquely identifies an interface on an IPv6-enabled device.
- Multicast - An IPv6 multicast address is used to send a single IPv6 packet to multiple destinations.
- Anycast - An IPv6 anycast address is any IPv6 unicast address that can be assigned to multiple devices. A packet sent to an anycast address is routed to the nearest device having that address. Anycast addresses are beyond the scope of this course.

Unlike IPv4, IPv6 does not have a broadcast address. However, there is an IPv6 all-nodes multicast address that essentially gives the same result.

IPv6 Prefix Length

The prefix, or network portion, of an IPv4 address can be identified by a dotted-decimal subnet mask or prefix length (slash notation). For example, an IPv4 address of 192.168.1.10 with dotted-decimal subnet mask 255.255.255.0 is equivalent to 192.168.1.10/24.

In IPv6 it is only called the prefix length. IPv6 does not use the dotted-decimal subnet mask notation. Like IPv4, the prefix length is represented in slash notation and is used to indicate the network portion of an IPv6 address.

The prefix length can range from 0 to 128. The recommended IPv6 prefix length for LANs and most other types of networks is /64, as shown in the figure.

IPv6 Prefix Length →

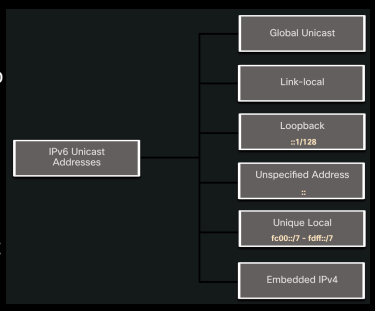
The prefix or network portion of the address is 64 bits in length, leaving another 64 bits for the interface ID (host portion) of the address.

It is strongly recommended to use a 64-bit Interface ID for most networks. This is because stateless address autoconfiguration (**SLAAC**) uses 64 bits for the Interface ID. It also makes subnetting easier to create and manage.

Types of IPv6 Unicast Addresses

An IPv6 unicast address uniquely identifies an interface on an IPv6-enabled device. A packet sent to a unicast address is received by the interface which is assigned that address. Similar to IPv4, a source IPv6 address must be a unicast address. The destination IPv6 address can be either a unicast or a multicast address. The figure shows the different types of IPv6 unicast addresses.

IPv6 Unicast Addresses →



Unlike IPv4 devices that have only a single address, IPv6 addresses typically have two unicast addresses:

- Global Unicast Address (**GUA**) - This is similar to a public IPv4 address. These are globally unique, internet-routable addresses. GUAs can be configured statically or assigned dynamically.
- Link-Local Address (**LLA**) - This is required for every IPv6-enabled device. LLAs are used to communicate with other devices on the same local link. With IPv6, the term link refers to a subnet. LLAs are confined to a single link. Their uniqueness must only be confirmed on that link because they are not routable beyond the link. In other words, routers will not forward packets with a link-local source or destination address.

Gemini said:

To put this in perspective for your next deployment, think of these like your office's communication systems: the **GUA** is your direct-dial external phone number, while the **LLA** is the internal intercom system that works even if the building's external lines are cut.

Per **IETF RFC 4291** and **Cisco IPv6 Implementation SOPs**, here is the technical breakdown:

IPv6 Address Type Comparison

Feature	Global Unicast Address (GUA)	Link-Local Address (LLA)
IPv4 Equivalent	Public IP	APIPA ($169.254.x.x$) - *but mandatory*
Prefix Range	$2000::/3$	$fe80::/10$
Scope	Global (Internet)	Local Link (Subnet)
Routability	Fully Routable	Non-routable (Dropped by routers)
Requirement	Optional (context-dependent)	**Mandatory** for every IPv6 interface

Key Technical Distinctions

- **GUA (Global Unicast):** These are currently allocated from the $2000::/3$ block. In a Cisco environment, these are what you'll route across your core and out to the ISP. They allow for end-to-end reachability without the need for NAT66 (though NAT66 exists, it's generally discouraged in standard IPv6 design).
- **LLA (Link-Local):** These are automatically generated (SLAAC) or manually configured the moment IPv6 is enabled on an interface. They are the backbone of the **Neighbor Discovery Protocol (NDP)**. If you try to ping a GUA on a remote segment, your router actually uses the LLA of the next-hop router to get the packet there.

I have verified these details against the current **IANA IPv6 Address Space registry** and **Cisco IOS XE documentation** for 2026 standards.

A note about the Unique Local Address

Unique local addresses (range fc00::/7 to fdff::/7) are not yet commonly implemented. Therefore, this module only covers GUA and LLA configuration. However, unique local addresses may eventually be used to address devices that should not be accessible from the outside, such as internal servers and printers.

The IPv6 unique local addresses have some similarity to RFC 1918 private addresses for IPv4, but there are significant differences:

- Unique local addresses are used for local addressing within a site or between a limited number of sites.
- Unique local addresses can be used for devices that will never need to access another network.
- Unique local addresses are not globally routed or translated to a global IPv6 address.

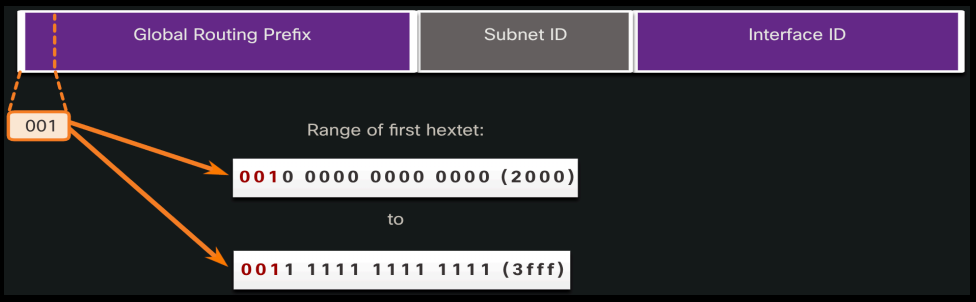
Note: Many sites also use the private nature of RFC 1918 addresses to attempt to secure or hide their network from potential security risks. However, this was never the intended use of these technologies, and the IETF has always recommended that sites take the proper security precautions on their internet-facing router.

IPv6 GUA

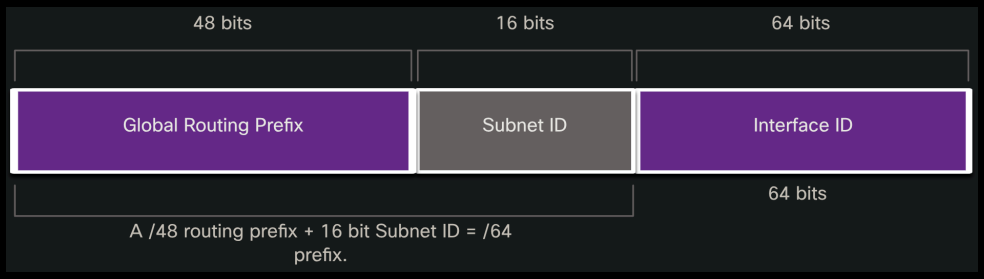
IPv6 global unicast addresses (GUAs) are globally unique and routable on the IPv6 internet. These addresses are equivalent to public IPv4 addresses. The Internet Committee for Assigned Names and Numbers (**ICANN**), the operator for Internet Assigned Numbers Authority (**IANA**), allocates IPv6 address blocks to the five RIRs. Currently, only GUAs with the first three bits of 001 or 2000::/3 are being assigned, as shown in the figure.

The figure shows the range of values for the first hextet where the first hexadecimal digit for currently available GUAs begins with a 2 or a 3. This is only 1/8th of the total available IPv6 address space, excluding only a very small portion for other types of unicast and multicast addresses.

Note: The 2001:db8::/32 address has been reserved for documentation purposes, including use in examples.



The next figure shows the structure and range of a GUA.



IPv6 Address with a /48 Global Routing Prefix and /64 Prefix

A GUA has three parts:

- Global Routing Prefix
- Subnet ID
- Interface ID

IPv6 GUA Structure

Global Routing Prefix

The global routing prefix is the prefix, or network, portion of the address that is assigned by the provider, such as an ISP, to a customer or site. For example, it is common for ISPs to assign a /48 global routing prefix to its customers. The global routing prefix will usually vary depending on the policies of the ISP.

The previous figure shows a GUA using a /48 global routing prefix. /48 prefixes are a common global routing prefix that is assigned and will be used in most of the examples throughout this course.

For example, the IPv6 address 2001:db8:acad::/48 has a global routing prefix that indicates that the first 48 bits (3 hextets) (2001:db8:acad) is how the ISP knows of this prefix (network). The double colon (::) following the /48 prefix length means the rest of the address contains all 0s. The size of the global routing prefix determines the size of the subnet ID.

Subnet ID

The subnet ID field is the area between the global routing prefix and the interface ID. Unlike IPv4 where you must borrow bits from the host portion to create subnets, IPv6 was designed with subnetting in mind. The subnet ID is used by an organization to identify subnets within its site. The larger the subnet ID, the more subnets available.

Note: Many organizations are receiving a /32 global routing prefix. Using the recommended /64 prefix in order to create a 64-bit interface ID, leaves a 32 bit subnet ID. This means an organization with a /32 global routing prefix and a 32-bit subnet ID will have 4.3 billion subnets, each with 18 quintillion devices per subnet. That is as many subnets as there are public IPv4 addresses!
The IPv6 address in the previous figure has a /48 global routing prefix, which is common among many enterprise networks. This makes it especially easy to examine the different parts of the address. Using a typical /64 prefix length, the first four hextets are for the network portion of the address, with the fourth hextet indicating the subnet ID. The remaining four hextets are for the interface ID.

Interface ID

The IPv6 interface ID is equivalent to the host portion of an IPv4 address. The term interface ID is used because a single host may have multiple interfaces, each having one or more IPv6 addresses. The figure shows an example of the structure of an IPv6 GUA. It is strongly recommended that in most cases /64 subnets should be used, which creates a 64-bit interface ID. A 64-bit interface ID allows for 18 quintillion devices or hosts per subnet.

A /64 subnet or prefix (global routing prefix + subnet ID) leaves 64 bits for the interface ID. This is recommended to allow SLAAC-enabled devices to create their own 64-bit interface ID. It also makes developing an IPv6 addressing plan simple and effective.

Note: Unlike IPv4, in IPv6, the all-0s and all-1s host addresses can be assigned to a device. The all-1s address can be used because broadcast addresses are not used within IPv6. The all-0s address can also be used, but is reserved as a subnet-router anycast address, and should be assigned only to routers.

IPv6 LLA

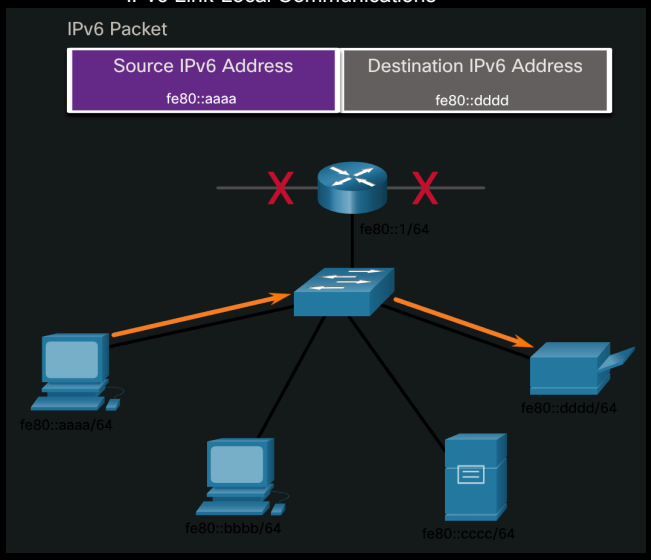
An IPv6 link-local address (LLA) enables a device to communicate with other IPv6-enabled devices on the same link and only on that link (subnet). Packets with a source or destination LLA cannot be routed beyond the link from which the packet originated.

The GUA is not a requirement. However, every IPv6-enabled network interface must have an LLA.

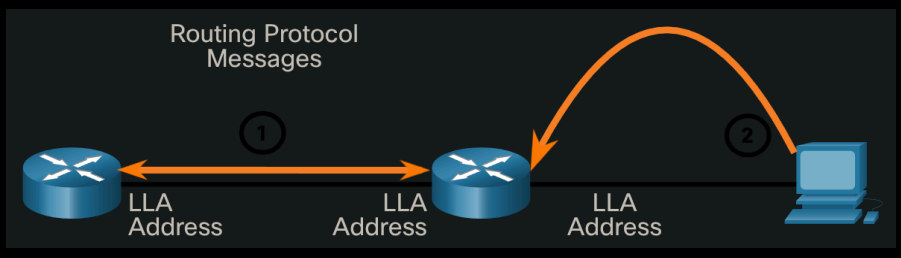
If an LLA is not configured manually on an interface, the device will automatically create its own without communicating with a DHCP server. IPv6-enabled hosts create an IPv6 LLA even if the device has not been assigned a global unicast IPv6 address. This allows IPv6-enabled devices to communicate with other IPv6-enabled devices on the same subnet. This includes communication with the default gateway (router).

IPv6 LLAs are in the fe80::/10 range. The /10 indicates that the first 10 bits are 1111 1110 10xx xxxx. The first hextet has a range of 1111 1110 1000 0000 (fe80) to 1111 1110 1011 1111 (febf).
The figure shows an example of communication using IPv6 LLAs. The PC is able to communicate directly with the printer using the LLAs.

IPv6 Link-Local Communications



The next figure shows some of the uses for IPv6 LLAs.



i. *Routers use the LLA of neighbor routers to send routing updates.*
ii. *Hosts use the LLA of a local router as the default-gateway.*

The prefix or network portion of the address is 64 bits in length, leaving another 64 bits for the interface ID (host portion) of the address.

It is strongly recommended to use a 64-bit Interface ID for most networks. This is because stateless address autoconfiguration (SLAAC) uses 64 bits for the Interface ID. It also makes subnetting easier to create and manage.

GUA and LLA Static Configuration

Static GUA Configuration on a Router

As you learned in the previous topic, IPv6 GUAs are the same as public IPv4 addresses. They are globally unique and routable on the IPv6 internet. An IPv6 LLA lets two IPv6-enabled devices communicate with each other on the same link (subnet). It is easy to statically configure IPv6 GUAs and LLAs on routers to help you create an IPv6 network. This topic teaches you how to do just that!

Most IPv6 configuration and verification commands in the Cisco IOS are similar to their IPv4 counterparts. In many cases, the only difference is the use of ipv6 in place of ip within the commands.

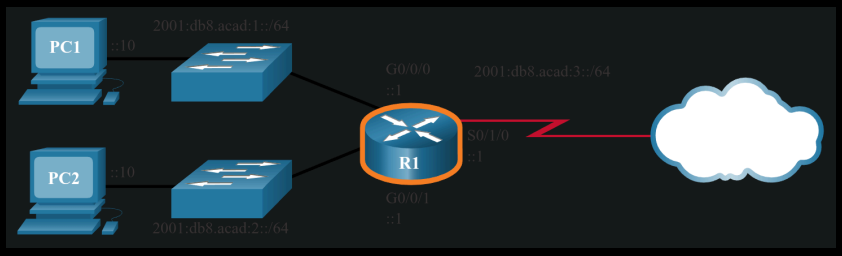
For example, the Cisco IOS command to configure an IPv4 address on an interface is ip address ip-address subnet-mask. In contrast, the command to configure an IPv6 GUA on an interface is ipv6 address ipv6-address/prefix-length.

Notice that there is no space between ipv6-address and prefix-length.

The example configuration uses the topology shown in the figure and these IPv6 subnets:

- 2001:db8:acad:1::/64
- 2001:db8:acad:2::/64
- 2001:db8:acad:3::/64

Example Topology:



The example shows the commands required to configure the IPv6 GUA on GigabitEthernet 0/0/0, GigabitEthernet 0/0/1, and the Serial 0/1/0 interface of R1.

IPv6 GUA Configuration on Router R1

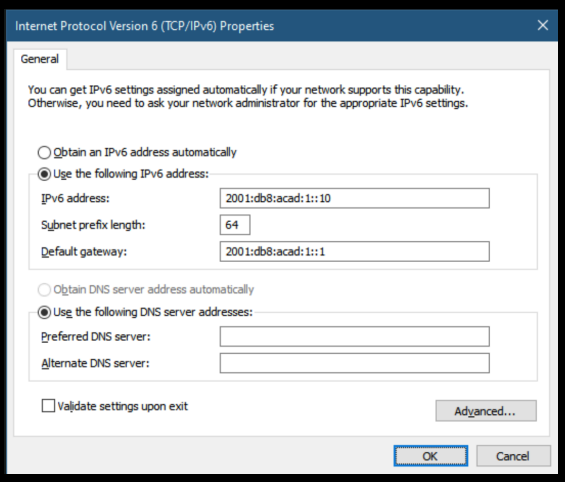
```
R1(config)# interface gigabitethernet 0/0/0
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface gigabitethernet 0/0/1
R1(config-if)# ipv6 address 2001:db8:acad:2::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface serial 0/1/0
R1(config-if)# ipv6 address 2001:db8:acad:3::1/64
R1(config-if)# no shutdown
```

Static GUA Configuration on a Windows Host

Manually configuring the IPv6 address on a host is similar to configuring an IPv4 address.

As shown in the figure, the default gateway address configured for PC1 is 2001:db8:acad:1::1. This is the GUA of the R1 GigabitEthernet interface on the same network. Alternatively, the default gateway address can be configured to match the LLA of the GigabitEthernet interface. Using the LLA of the router as the default gateway address is considered best practice. Either configuration will work.

Just as with IPv4, configuring static addresses on clients does not scale to larger environments. For this reason, most network administrators in an IPv6 network will enable dynamic assignment of IPv6 addresses.



There are two ways in which a device can obtain an IPv6 GUA automatically:

- Stateless address autoconfiguration (**SLAAC**)
- **Stateful DHCPv6**

SLAAC and DHCPv6 are covered in the next topic.

Note: When DHCPv6 or SLAAC is used, the LLA of the router will automatically be specified as the default gateway address.

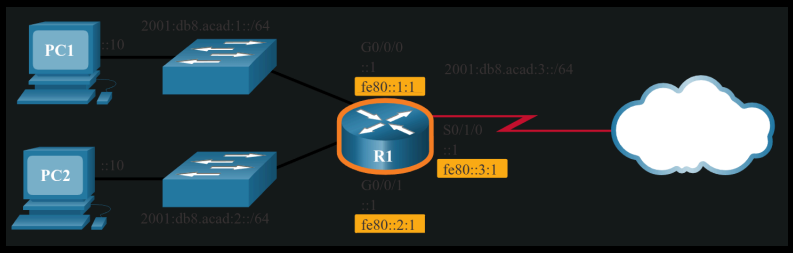
Static Configuration of a Link-Local Unicast Address

Configuring the LLA manually lets you create an address that is recognizable and easier to remember. Typically, it is only necessary to create recognizable LLAs on routers. This is beneficial because router LLAs are used as default gateway addresses and in routing advertisement messages.

LLAs can be configured manually using the ipv6 address ipv6-link-local-address link-local command. When an address begins with this hextet within the range of **fe80** to **febf**, the link-local parameter must follow the address.

The figure shows an example topology with LLAs on each interface.

Example Topology with LLAs



The example shows the configuration of an LLA on router R1.

```
R1(config)# interface gigabitethernet 0/0/0
R1(config-if)# ipv6 address fe80::1:1 link-local
R1(config-if)# exit
R1(config)# interface gigabitethernet 0/0/1
R1(config-if)# ipv6 address fe80::2:1 link-local
R1(config-if)# exit
R1(config)# interface serial 0/1/0
R1(config-if)# ipv6 address fe80::3:1 link-local
R1(config-if)# exit
```

Statically configured LLAs are used to make them more easily recognizable as belonging to router R1. In this example, all the interfaces of router R1 have been configured with an LLA that begins with fe80::n:1.

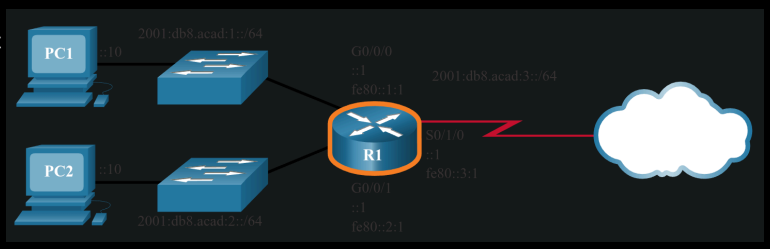
Note: The exact same LLA could be configured on each link as long as it is unique on that link. This is because LLAs only have to be unique on that link. However, common practice is to create a different LLA on each interface of the router to make it easy to identify the router and the specific interface.

Syntax Checker - GUA and LLA Static Configuration

Assign IPv6 GUAs and LLAs to the specified interfaces on router R1.

Configure and activate IPv6 on the GigabitEthernet 0/0/0 interface with the following addresses:

- Use g0/0/0 as the interface name
- LLA - fe80::1:1
- GUA - 2001:db8:acad:1::1/64
- Activate the interface
- Exit interface configuration mode

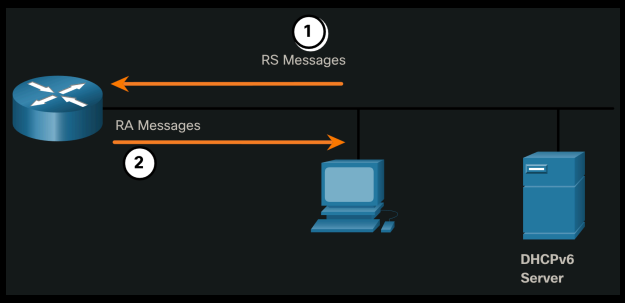


Dynamic Addressing for IPv6 GUAs

RS and RA Messages

If you do not want to statically configure IPv6 GUAs, no need to worry. Most devices obtain their IPv6 GUAs dynamically. This topic explains how this process works using Router Advertisement (**RA**) and Router Solicitation (**RS**) messages. This topic gets rather technical, but when you understand the difference between the three methods that a router advertisement can use, as well as how the EUI-64 process for creating an interface ID differs from a randomly generated process, you will have made a huge leap in your IPv6 expertise!

For the GUA, a device obtains the address dynamically through Internet Control Message Protocol version 6 (ICMPv6) messages. IPv6 routers periodically send out ICMPv6 **RA** messages, every 200 seconds, to all IPv6-enabled devices on the network. An **RA** message will also be sent in response to a host sending an ICMPv6 RS message, which is a request for an **RA** message. Both messages are shown in the figure.



ICMPv6 **RS** and **RA** Messages

RA messages are on IPv6 router Ethernet interfaces. The router must be enabled for IPv6 routing, which is not enabled by default. To enable a router as an IPv6 router, the ipv6 unicast-routing global configuration command must be used.

The ICMPv6 **RA** message is a suggestion to a device on how to obtain an IPv6 GUA. The ultimate decision is up to the device operating system.

1. *RS messages are sent to all IPv6 routers by hosts requesting addressing information.*
2. *RA messages are sent to all IPv6 nodes. If Method 1 (SLAAC only) is used, the RA includes network prefix, prefix-length, and default-gateway information.*

The ICMPv6 **RA** message includes the following:

- Network prefix and prefix length - This tells the device which network it belongs to.
- Default gateway address - This is an IPv6 LLA, the source IPv6 address of the **RA** message.
- DNS addresses and domain name - These are the addresses of DNS servers and a domain name.

There are three methods for **RA** messages:

- Method 1: SLAAC - “I have everything you need including the prefix, prefix length, and default gateway address.”
- Method 2: SLAAC with a stateless DHCPv6 server - “Here is my information but you need to get other information such as DNS addresses from a stateless DHCPv6 server.”
- Method 3: Stateful DHCPv6 (no SLAAC) - “I can give you your default gateway address. You need to ask a stateful DHCPv6 server for all your other information.”

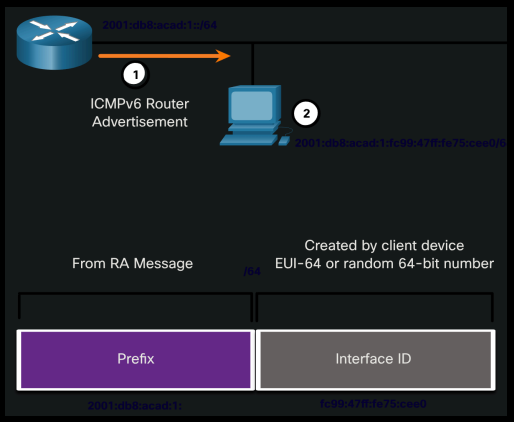
Method 1: SLAAC

SLAAC is a method that allows a device to create its own GUA without the services of DHCPv6. Using SLAAC, devices rely on the ICMPv6 RA messages of the local router to obtain the necessary information.

By default, the RA message suggests that the receiving device use the information in the RA message to create its own IPv6 GUA and all other necessary information. The services of a DHCPv6 server are not required.

SLAAC is stateless, which means there is no central server (for example, a stateful DHCPv6 server) allocating GUAs and keeping a list of devices and their addresses. With SLAAC, the client device uses the information in the RA message to create its own GUA. As shown in the figure, the two parts of the address are created as follows:

- Prefix - This is advertised in the RA message.
- Interface ID - This uses the EUI-64 process or by generating a random 64-bit number, depending on the device operating system.



1. *The router sends an RA message with the prefix for the local link.*
2. *The PC uses SLAAC to obtain a prefix from the RA message and creates its own Interface ID.*

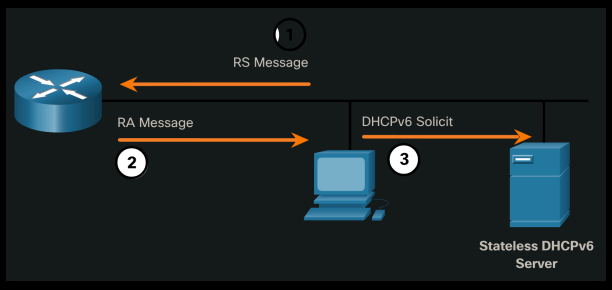
Method 2: SLAAC and Stateless DHCPv6

A router interface can be configured to send a router advertisement using SLAAC and stateless DHCPv6.

As shown in the figure, with this method, the RA message suggests devices use the following:

- SLAAC to create its own IPv6 GUA
- The router LLA, which is the RA source IPv6 address, as the default gateway address
- A stateless DHCPv6 server to obtain other information such as a DNS server address and a domain name

Note: A stateless DHCPv6 server distributes DNS server addresses and domain names. It does not allocate GUAs.



1. *The PC sends an RS to all IPv6 routers, "I need addressing information."*
2. *The router sends an RA message to all IPv6 nodes with Method 2 (SLAAC and DHCPv6) specified. "Here is your prefix, prefix-length, and default gateway information. But you will need to get DNS information from a DHCPv6 server."*
3. *The PC sends a DHCPv6 Solicit message to all DHCPv6 servers. "I used SLAAC to create my IPv6 address and get my default gateway address, but I need other information from a stateless DHCPv6 server."*

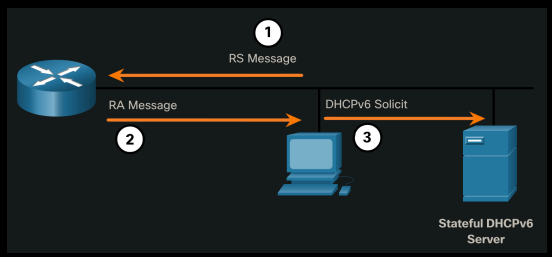
Method 3: Stateful DHCPv6

A router interface can be configured to send an RA using stateful DHCPv6 only.

Stateful DHCPv6 is similar to DHCP for IPv4. A device can automatically receive its addressing information including a GUA, prefix length, and the addresses of DNS servers from a stateful DHCPv6 server.

As shown in the figure, with this method, the RA message suggests devices use the following:

- The router LLA, which is the RA source IPv6 address, for the default gateway address.
- A stateful DHCPv6 server to obtain a GUA, DNS server address, domain name and other necessary information.



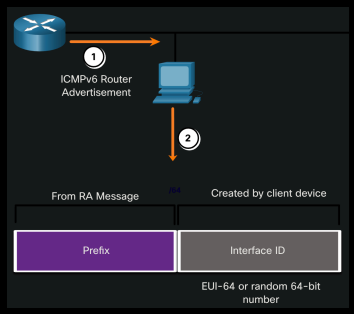
- *The PC sends an RS to all IPv6 routers, "I need addressing information."*
- *The router sends an RA message to all IPv6 nodes with Method 3 (Stateful DHCPv6) specified, "I am your default gateway, but you need to ask a stateful DHCPv6 server for your IPv6 address and other addressing information."*
- *The PC sends a DHCPv6 Solicit message to all DHCPv6 servers, " I received my default gateway address from the RA message, but I need an IPv6 address and all other addressing information from a stateful DHCPv6 server."*

A stateful DHCPv6 server allocates and maintains a list of which device receives which IPv6 address. DHCP for IPv4 is stateful.

Note: The default gateway address can only be obtained dynamically from the RA message. The stateless or stateful DHCPv6 server does not provide the default gateway address.

EUI-64 Process vs. Randomly Generated

When the RA message is either SLAAC or SLAAC with stateless DHCPv6, the client must generate its own interface ID. The client knows the prefix portion of the address from the RA message, but must create its own interface ID. The interface ID can be created using the EUI-64 process or a randomly generated 64-bit number, as shown in the figure.



Dynamically Creating an Interface ID

1. *The router sends an RA message.*
2. *The PC uses the prefix in the RA message and uses either EUI-64 or a random 64-bit number to generate an interface ID.*

EUI-64 Process

IEEE defined the Extended Unique Identifier (**EUI**) or modified EUI-64 process.

- This process uses the 48-bit Ethernet MAC address of a client, and inserts another 16 bits in the middle of the 48-bit MAC address to create a 64-bit interface ID.

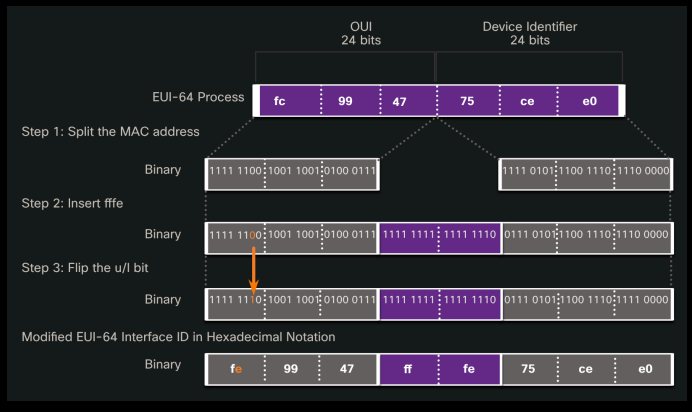
Ethernet MAC addresses are usually represented in hexadecimal and are made up of two parts:

- Organizationally Unique Identifier (**OUI**) - The OUI is a 24-bit (6 hexadecimal digits) vendor code assigned by IEEE.
- Device Identifier - The device identifier is a unique 24-bit (6 hexadecimal digits) value within a common OUI.

An EUI-64 interface ID is represented in binary and is made up of three parts:

- 24-bit OUI from the client MAC address, but **the 7th bit (the Universally/Locally (U/L) bit) is reversed**. This means that if the 7th bit is a 0, it becomes a 1, and vice versa.
- The inserted 16-bit value fffe (in hexadecimal).
- 24-bit device identifier from the client MAC address.

The EUI-64 process is illustrated in the figure, using the R1 GigabitEthernet MAC address of fc99:4775:cee0.



Step 1: Divide the MAC address between the OUI and device identifier.

Step 2: Insert the hexadecimal value fffe, which in binary is: 1111 1111 1111 1110.

Step 3: Convert the first 2 hexadecimal values of the OUI to binary and flip the U/L bit (bit 7). In this example, the 0 in bit 7 is changed to a 1.

The result is an EUI-64 generated interface ID of fe99:47ff:fe75:cee0.

Note: The use of the U/L bit, and the reasons for reversing its value, are discussed in RFC 5342.

The example output for the ipconfig command shows the IPv6 GUA being dynamically created using SLAAC and the EUI-64 process. An easy way to identify that an address was probably created using EUI-64 is by observing the fffe located in the middle of the interface ID.

The advantage of EUI-64 is that the Ethernet MAC address can be used to determine the interface ID. It also allows network administrators to easily track an IPv6 address to an end-device using the unique MAC address. However, this has caused privacy concerns among many users who worried that their packets could be traced to the actual physical computer. Due to these concerns, a randomly generated interface ID may be used instead.

EUI-64 Generated Interface ID

```
C:\> ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
   Connection-specific DNS Suffix . :
   IPv6 Address. . . . . . . . . . . :
2001:db8:acad:1:
fc99:47
ff:fe
75:cee0
   Link-local IPv6 Address . . . . . : fe80::fc99:47ff:fe75:cee0
   Default Gateway . . . . . . . . . : fe80::1
C:\>
```

Randomly Generated Interface IDs

Depending upon the operating system, a device may use a randomly generated interface ID instead of using the MAC address and the EUI-64 process. Beginning with Windows Vista, Windows uses a randomly generated interface ID instead of one created with EUI-64. Windows XP and previous Windows operating systems used EUI-64.

After the interface ID is established, either through the EUI-64 process or through random generation, it can be combined with an IPv6 prefix in the RA message to create a GUA, as shown in the figure.

Random 64-Bit Generated Interface ID

```
C:\> ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . :
2001:db8:acad:1:
50a5:8a35:a5bb:66e1
   Link-local IPv6 Address . . . . . : fe80::50a5:8a35:a5bb:66e1
   Default Gateway . . . . . . . . . : fe80::1
C:\>
```

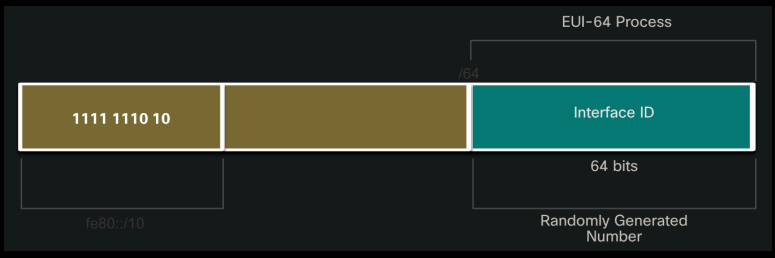
Note: To ensure the uniqueness of any IPv6 unicast address, the client may use a process known as duplicate address detection (DAD). This is similar to an ARP request for its own address. If there is no reply, then the address is unique.

Dynamic Addressing for IPv6 LLAs

Dynamic LLAs

All IPv6 devices must have an IPv6 LLA. Like IPv6 GUAs, you can also create LLAs dynamically. Regardless of how you create your LLAs (and your GUAs), it is important that you verify all IPv6 address configuration. This topic explains dynamically generated LLAs and IPv6 configuration verification.

The figure shows the LLA is dynamically created using the fe80::/10 prefix and the interface ID using the EUI-64 process, or a randomly generated 64-bit number.



Dynamic LLAs on Windows

Operating systems, such as Windows, will typically use the same method for both a SLAAC-created GUA and a dynamically assigned LLA. See the highlighted areas in the following examples that were shown previously.

EUI-64 Generated Interface ID

```
C:\> ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
IPv6 Address. . . . . . . . . . . : 2001:db8:acad:1:
fc99:47
ff:fe
75:cee0
Link-local IPv6 Address . . . . . : fe80::
fc99:47
ff:fe
75:cee0
Default Gateway . . . . . . . . . : fe80::1
C:\>
```

Random 64-Bit Generated Interface ID

```
C:\> ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:db8:acad:1:
50a5:8a35:a5bb:66e1
   Link-local IPv6 Address . . . . . : fe80::
50a5:8a35:a5bb:66e1
   Default Gateway . . . . . . . . . : fe80::1
C:\>
```

Dynamic LLAs on Cisco Routers

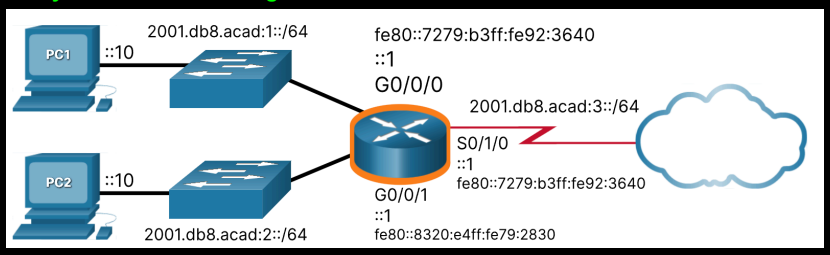
IPv6 LLA Using EUI-64 on Router R1 →

Cisco routers automatically create an IPv6 LLA whenever a GUA is assigned to the interface. By default, Cisco IOS routers use EUI-64 to generate the interface ID for all LLAs on IPv6 interfaces. For serial interfaces, the router will use the MAC address of an Ethernet interface. Recall that an LLA must be unique only on that link or network. However, a drawback to using the dynamically assigned LLA is its long interface ID, which makes it challenging to identify and remember assigned addresses. The example displays the MAC address on the GigabitEthernet 0/0/0 interface of router R1. This address is used to dynamically create the LLA on the same interface, and also for the Serial 0/1/0 interface.

To make it easier to recognize and remember these addresses on routers, it is common to statically configure IPv6 LLAs on routers.

```
R1# show interface gigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Hardware is ISR4221-2x1GE, address is
7079.b392.3640
 (bia 7079.b392.3640)
(Output omitted)
R1# show ipv6 interface brief
GigabitEthernet0/0/0   [up/up]
    FE80::
7279:B3
FF:FE
92:3640
    2001:DB8:ACAD:1::1
GigabitEthernet0/0/1   [up/up]
    FE80::
7279:B3
FF:FE
92:3641
    2001:DB8:ACAD:2::1
Serial0/1/0            [up/up]
    FE80::
7279:B3
FF:FE
92:3640
    2001:DB8:ACAD:3::1
Serial0/1/1            [down/down]
    unassigned
R1#
```

Verify IPv6 Address Configuration




```
# show ipv6 interface brief
```

The `show ipv6 interface brief` Command on R1 →

On Linux: `$ ip -6 addr show`

The show ipv6 interface brief command displays the IPv6 address of the Ethernet interfaces. EUI-64 uses this MAC address to generate the interface ID for the LLA. Additionally, the show ipv6 interface brief command displays abbreviated output for each of the interfaces. The [up/up] output on the same line as the interface indicates the Layer 1/Layer 2 interface state. This is the same as the Status and Protocol columns in the equivalent IPv4 command.

Notice that each interface has two IPv6 addresses. The second address for each interface is the GUA that was configured. The first address, the one that begins with fe80, is the link-local unicast address for the interface. Recall that the LLA is automatically added to the interface when a GUA is assigned.

```
R1# show ipv6 interface brief
GigabitEthernet0/0/0   [up/up]
    FE80::1:1
    2001:DB8:ACAD:1::1
GigabitEthernet0/0/1   [up/up]
    FE80::1:2
    2001:DB8:ACAD:2::1
Serial0/1/0            [up/up]
    FE80::1:3
    2001:DB8:ACAD:3::1
Serial0/1/1            [down/down]
unassigned
R1#
```

Also, notice that the R1 Serial 0/1/0 LLA is the same as its GigabitEthernet 0/0/0 interface. Serial interfaces do not have Ethernet MAC addresses, so Cisco IOS uses the MAC address of the first available Ethernet interface. This is possible because link-local interfaces only have to be unique on that link.

 # show ipv6 route

On Linux: **$ ip -6 route show**

The `show ipv6 route` Command on R1

```
R1# show ipv6 route
IPv6 Routing Table - default - 7 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route

C   2001:DB8:ACAD:1::/64 [0/0]
     via GigabitEthernet0/0/0, directly connected
L   2001:DB8:ACAD:1::1/128 [0/0]
     via GigabitEthernet0/0/0, receive
C   2001:DB8:ACAD:2::/64 [0/0]
     via GigabitEthernet0/0/1, directly connected
L   2001:DB8:ACAD:2::1/128 [0/0]
     via GigabitEthernet0/0/1, receive
C   2001:DB8:ACAD:3::/64 [0/0]
     via Serial0/1/0, directly connected
L   2001:DB8:ACAD:3::1/128 [0/0]
     via Serial0/1/0, receive
L   FF00::/8 [0/0]
     via Null0, receive
R1#
```

As shown in the example, the show ipv6 route command can be used to verify that IPv6 networks and specific IPv6 interface addresses have been installed in the IPv6 routing table. The show ipv6 route command will only display IPv6 networks, not IPv4 networks.

Within the route table, a C next to a route indicates that this is a directly connected network. When the router interface is configured with a GUA and is in the “up/up” state, the IPv6 prefix and prefix length is added to the IPv6 routing table as a connected route.

Note: The L indicates a local route, the specific IPv6 address assigned to the interface. This is not an LLA. LLAs are not included in the routing table of the router because they are not routable addresses.

The IPv6 GUA configured on the interface is also installed in the routing table as a local route. The local route has a /128 prefix. Local routes are used by the routing table to efficiently process packets with a destination address of the router interface address.

 # ping

The ping command for IPv6 is identical to the command used with IPv4, except that an IPv6 address is used. As shown in the example, the command is used to verify Layer 3 connectivity between R1 and PC1. When pinging an LLA from a router, Cisco IOS will prompt the user for the exit interface. Because the destination LLA can be on one or more of its links or networks, the router needs to know which interface to send the ping to.

```
R1# ping 2001:db8:acad:1::10
Type escape sequence to abort.
Sending 5, 100-
byte ICMP Echos to 2001:DB8:ACAD:1::10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
R1#
```

IPv6 Multicast Addresses

Assigned IPv6 Multicast Addresses

Earlier in this module, you learned that there are three broad categories of IPv6 addresses: unicast, anycast, and multicast. This topic goes into more detail about multicast addresses.

IPv6 multicast addresses are similar to IPv4 multicast addresses. Recall that a multicast address is used to send a single packet to one or more destinations (multicast group). IPv6 multicast addresses have the prefix ff00::/8.

Note: Multicast addresses can only be destination addresses and not source addresses.

There are two types of IPv6 multicast addresses:

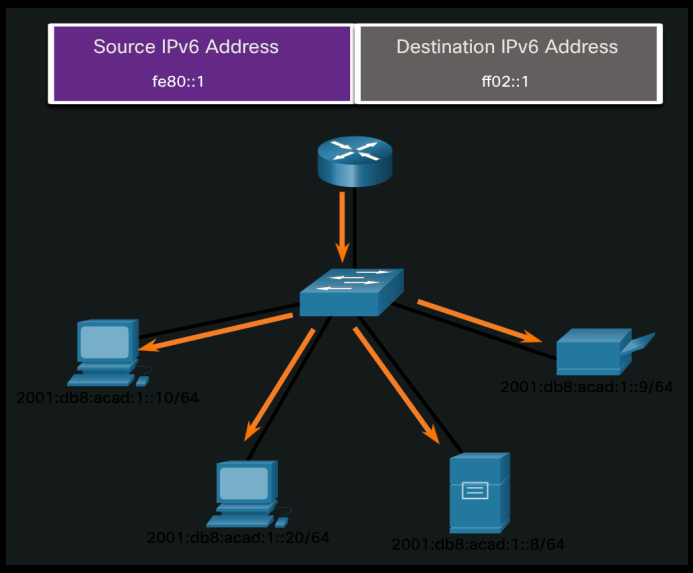
- Well-known multicast addresses
- Solicited-node multicast addresses

Well-Known IPv6 Multicast Addresses

Well-known IPv6 multicast addresses are assigned. Assigned multicast addresses are reserved multicast addresses for predefined groups of devices. An assigned multicast address is a single address used to reach a group of devices running a common protocol or service. Assigned multicast addresses are used in context with specific protocols such as DHCPv6.

These are two common IPv6 assigned multicast groups:

- ff02::1 All-nodes multicast group - This is a multicast group that all IPv6-enabled devices join. A packet sent to this group is received and processed by all IPv6 interfaces on the link or network. This has the same effect as a broadcast address in IPv4. The figure shows an example of communication using the all-nodes multicast address. An IPv6 router sends ICMPv6 RA messages to the all-node multicast group.
- ff02::2 All-routers multicast group - This is a multicast group that all IPv6 routers join. A router becomes a member of this group when it is enabled as an IPv6 router with the ipv6 unicast-routing global configuration command. A packet sent to this group is received and processed by all IPv6 routers on the link or network.

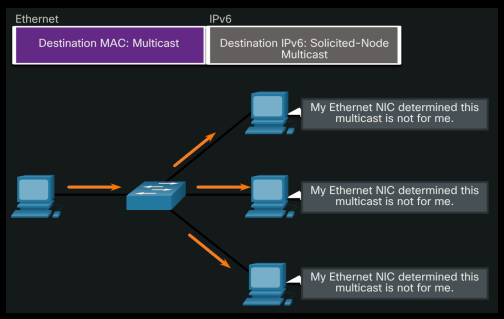


IPv6 All-Nodes Multicast: RA Message

IPv6-enabled devices send ICMPv6 RS messages to the all-routers multicast address. The RS message requests an RA message from the IPv6 router to assist the device in its address configuration. The IPv6 router responds with an RA message, as shown.

Solicited-Node IPv6 Multicast

A solicited-node multicast address is similar to the all-nodes multicast address. The advantage of a solicited-node multicast address is that it is mapped to a special Ethernet multicast address. This allows the Ethernet NIC to filter the frame by examining the destination MAC address without sending it to the IPv6 process to see if the device is the intended target of the IPv6 packet.



Module 5: IPv6 Neighbor Discovery

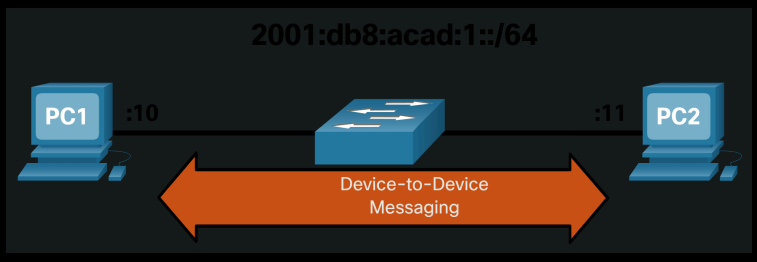
Neighbor Discovery Operation

Neighbor Discovery Messages

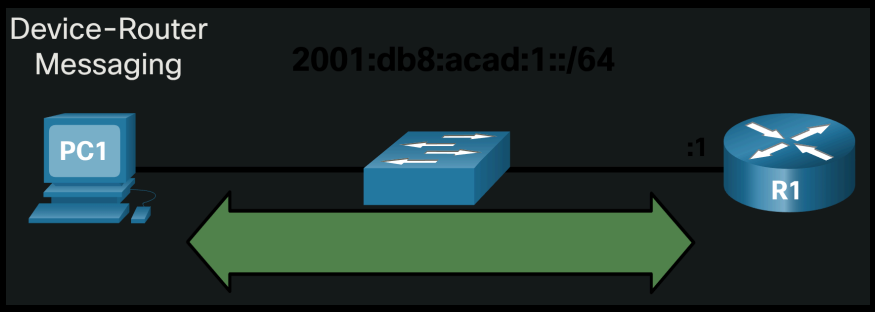
IPv6 neighbor discovery protocol is sometimes referred to as ND or NDP. In this course, we will refer to it as ND. ND provides address resolution, router discovery, and redirection services for IPv6 using ICMPv6. ICMPv6 ND uses five ICMPv6 messages to perform these services:

- **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.



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).



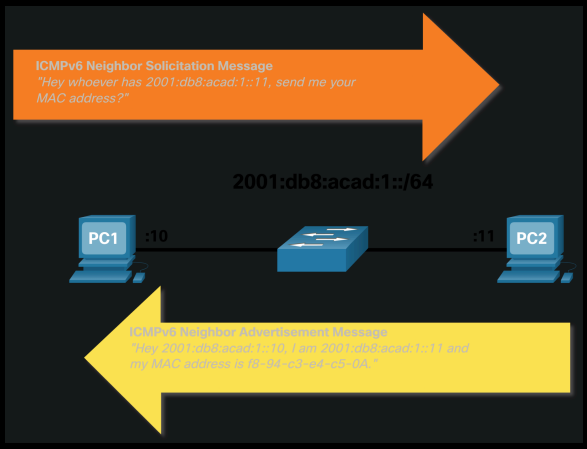
Note: The fifth ICMPv6 ND message is a redirect message which is used for better next-hop selection. This is beyond the scope of this course.

IPv6 ND is defined in the IETF RFC 4861.

IPv6 Neighbor Discovery - Address

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.



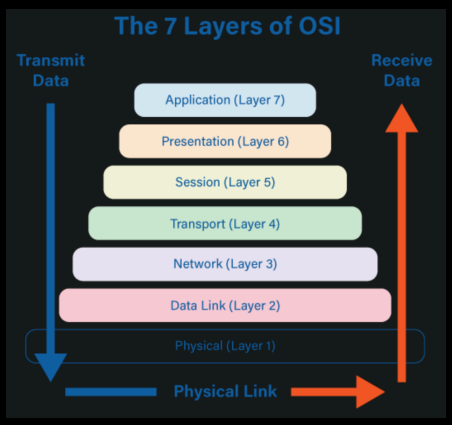
ICMPv6 neighbor solicitation messages are sent using special Ethernet and IPv6 multicast addresses. This allows the Ethernet NIC of the receiving device to determine whether the neighbor solicitation message is for itself without having to send it to the operating system for processing.

PC2 replies to the request with an ICMPv6 neighbor advertisement message which includes its MAC address.

Module 6: Cisco Switches and Routers

Cisco Switches

Connect More Devices



Home and small business networks usually do not require more than one or two networking devices in order to function efficiently. A wireless router, equipped with wireless connections and a few wired connections, is the only piece of networking equipment that is necessary in order to provide sufficient connectivity for the average small group of users. These routers are configured through a web browser and have an easy to use graphical user interface (GUI) that guides you through the most common configuration items.

Wireless routers that are designed primarily for home use are not appropriate for most business networks that must support more than a few users. Modern networks use a variety of devices for connectivity. Each device has certain capabilities for controlling the flow of data across a network. A general rule is that the higher the device is in the OSI model, the more intelligent it is. What this means is that a higher level device can better analyze the data traffic and forward it based on information not available at lower layers. As an example, a Layer 2 switch can filter the data and send it only out of the port that is connected to the destination, based on the MAC address.

As switches and routers evolve, the distinction between them may seem blurred. One simple distinction remains: LAN switches provide connectivity within the local-area networks of the organization, while routers interconnect local networks and are needed in a wide area network (WAN) environment. In other words, a switch is used to connect devices on the same network. A router is used to connect multiple networks to each other.

In addition to switches and routers, there are other connectivity options available for LANs. Wireless access points that are deployed in enterprises enable computers and other devices, such as IP phones, to wirelessly connect to the network, or share broadband connectivity. Firewalls guard against network threats and provide security, network control, and containment.

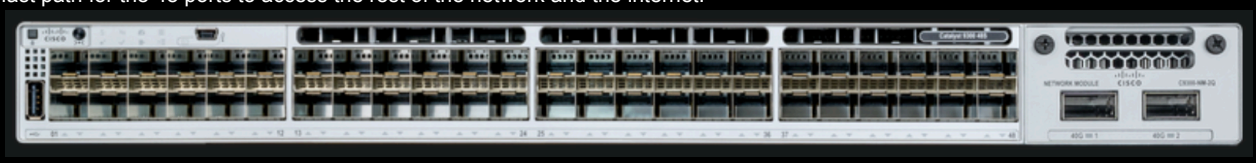
Cisco LAN Switches

When a LAN network grows to the point where the four Ethernet ports provided by the wireless router are not enough for all of the devices that need to attach to the wired network, it is time to add a LAN switch to the network. A switch can provide connectivity at the access layer of a network, connecting devices to a LAN. A switch can allow the network to grow without replacing central devices. When choosing a switch, there are a number of factors to consider, including the following:

- Type of ports
- Speed required
- Expandability
- Manageability

Type of Ports
When selecting a switch for your LAN, choosing the appropriate number and type of ports is critical. Most lower-cost switches support only copper twisted-pair interface ports. Higher priced switches may have fiber-optic connections. These are used to link the switch to other switches that may be located over long distances. The Cisco Catalyst 9300 series has a variety of options depending on your environment.

Speed Required
Ethernet twisted-pair interfaces on a switch have defined speeds. A 10/100 Ethernet port can only function at either 10 megabits per second (Mbps), or at 100 Mbps. What this means is that even if the device that you are connecting to the 10/100 switch interface port is capable of connecting at gigabit speeds, the maximum speed at which it will be able to communicate will be 100 Mbps. Switches may also include gigabit Ethernet ports. If your internet connection is more than 100 Mbps, then a gigabit port is necessary to take advantage of the higher internet bandwidth. Gigabit Ethernet ports will also operate at 10/100 Mbps. Gigabit Ethernet is sometimes represented as 1000 Mbps. The Cisco Catalyst 9300 48S switch in the figure has two 40 Gbps uplink ports to provide a fast path for the 48 ports to access the rest of the network and the internet.



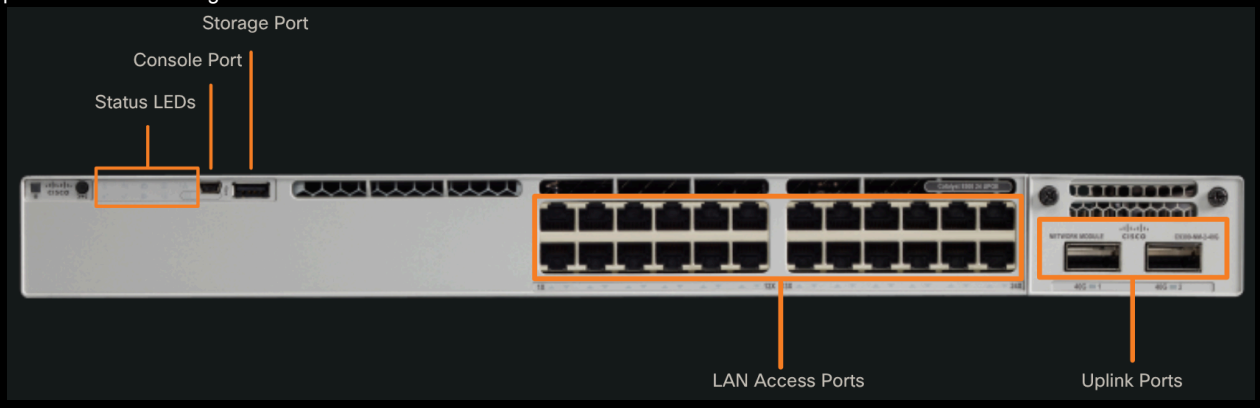
Similar to a switch port, Ethernet NICs operate at specific bandwidths such as 10/100 or 10/100/1000 Mbps. The actual bandwidth of the attached device will be the highest common bandwidth between the NIC on the device and the switch port.

Expandability
Networking devices come in both fixed and modular physical configurations. Fixed configurations have a specific type and number of ports or interfaces. Modular devices have expansion slots that provide the flexibility to add new modules as required. The figure shows a Cisco Catalyst 9600 chassis in which you can install different configurations of hardware to address your particular environment.

Many basic, inexpensive switches are not configurable. A managed switch that uses a Cisco operating system enables control over individual ports or over the switch as a whole. Controls include the ability to change the settings for a device, add port security, and monitor performance. The network administrator in the figure is directly connecting to a Cisco Catalyst switch using a console cable.

Lan Switch Components

The Cisco Catalyst 9300 switch shown in the figure is suitable for small and medium-sized networks. It provides 24 1 Gbps data ports with Power over Ethernet (PoE) so that some device types can be directly powered from the switch. It also has two modular 40 Gbps uplink ports. The LEDs indicate the port and system status of the switch. The switch is equipped with a console and storage ports for device management.



Switch Speeds and Forwarding Methods

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(Cyclic Redundancy Check)**. 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.

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.

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.

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:

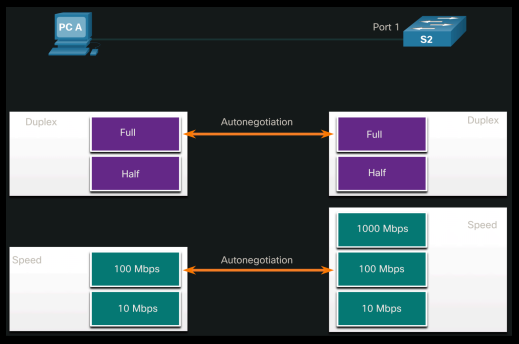
Memory Buffering Methods

Method	Description
Port-based memory	• 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 a busy destination port. • This delay occurs even if the other frames could be transmitted to open destination ports.
Shared memory	• Deposits all frames into a common memory buffer shared by all switch ports and the amount of buffer 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

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:

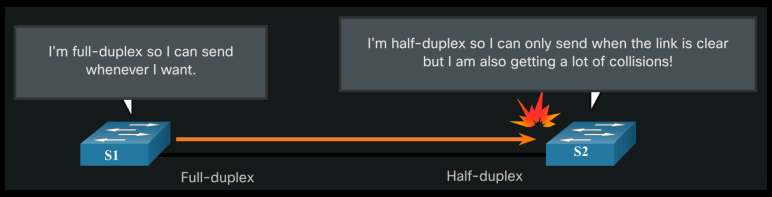
- Full-duplex - Both ends of the connection can send and receive simultaneously.
- Half-duplex - Only one end of the connection can send at a time.

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.

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.



S2 will continually experience collisions because S1 keeps sending frames any time it has something to send.

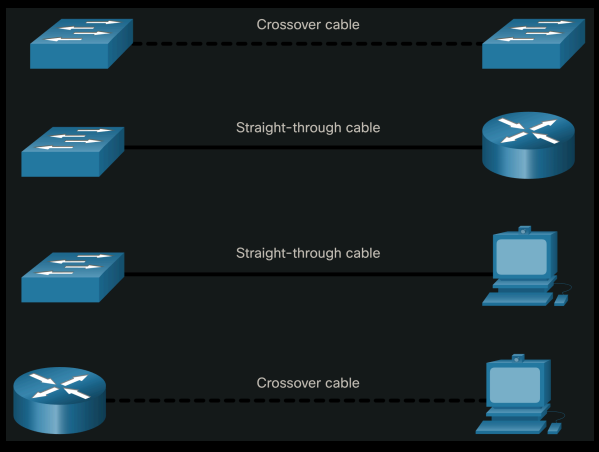
Duplex mismatch occurs when one or both ports on a link are reset, and the autonegotiation process does not result in both link partners having the same configuration. It also can occur when users reconfigure one side of a link and forget to reconfigure the other. Both sides of a link should have autonegotiation on, or both sides should have it off. Best practice is to configure both Ethernet switch ports as full-duplex.

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.



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.

Switch Boot Process

Note: in-band activity is when you have remote connectivity to a device, out of band management where remote access is not possible, but physical access is.

Power Up the Switch

Cisco switches, like most switches, are preconfigured to operate in a LAN as soon as they are powered on. All of the interface ports on the switch are active and will begin forwarding traffic immediately when devices are plugged into them. It is important to remember that no security settings are enabled by default. You will need to configure the basic security settings before placing the switch into the network.

The three basic steps for powering up a switch are as follows:

Step 1. Check the components.

- Ensure all the components that came with the switch are available. These could include a console cable, power cord, Ethernet cable, and switch documentation.

Step 2. Connect the cables to the switch.

- Connect the PC to the switch with a console cable and start a terminal emulation session. Connect the AC power cord to the switch and to a grounded AC outlet.

Step 3. Power up the switch.

- Some Cisco switch models do not have an on/off switch, like the Cisco Catalyst 9300 48S switch shown in the figure. To power on the switch, plug one end of the AC power cord into the switch AC power connector, and plug the other end into an AC power outlet.

- Note: The Cisco Catalyst 9300 switch in the figure has redundant power supplies in case one fails.

Back Panel of the Cisco Catalyst 9300 48S

Note: You can also attach cables after power is applied.

When the switch is on, the power-on self-test (POST) begins. During POST, the LEDs blink while a series of tests determine that the switch is functioning properly.

POST is completed when the SYST LED rapidly blinks green. If the switch fails POST, the SYST LED turns amber. When a switch fails POST, it is necessary to return the switch for repairs.

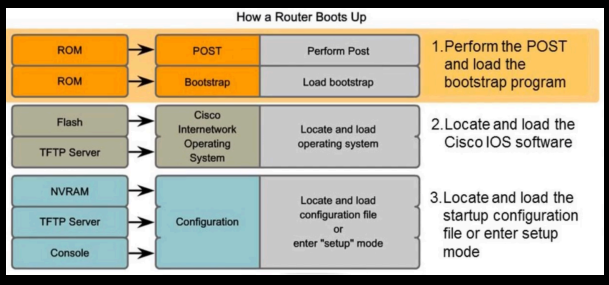
When all startup procedures are finished, the Cisco switch is ready to configure.

IOS Startup Files

As shown in the figure, a Cisco device loads the following two files into RAM when it is booted:

- IOS image file - The IOS facilitates the basic operation of the device's hardware components. The IOS image file is stored in flash memory.

- Startup configuration file - The startup configuration file contains commands that are used to initially configure a router and switch and create the running configuration file stored in RAM. The startup configuration file is stored in NVRAM**(Non-Volatile Random-Access Memory)**. All configuration changes are stored in the running configuration file and are implemented immediately by the IOS.



The running configuration file is modified when the network administrator performs device configuration. When changes are made to the running-config file, it should be saved to NVRAM as the startup configuration file in case the router is restarted or loses power.

Cisco Routers

Router Components

Regardless of their function, size, or complexity, all router models are essentially computers. Just like computers, tablets, and smart devices, routers also require the following:

- Operating system (OS)
- Central processing unit (CPU)
- Random-access memory (RAM)
- Read-only memory (ROM)
- Nonvolatile random-access memory (NVRAM)

Like all computers, tablets, and smart devices, Cisco routers require a CPU to execute OS instructions, such as system initialization, routing functions, and switching functions.

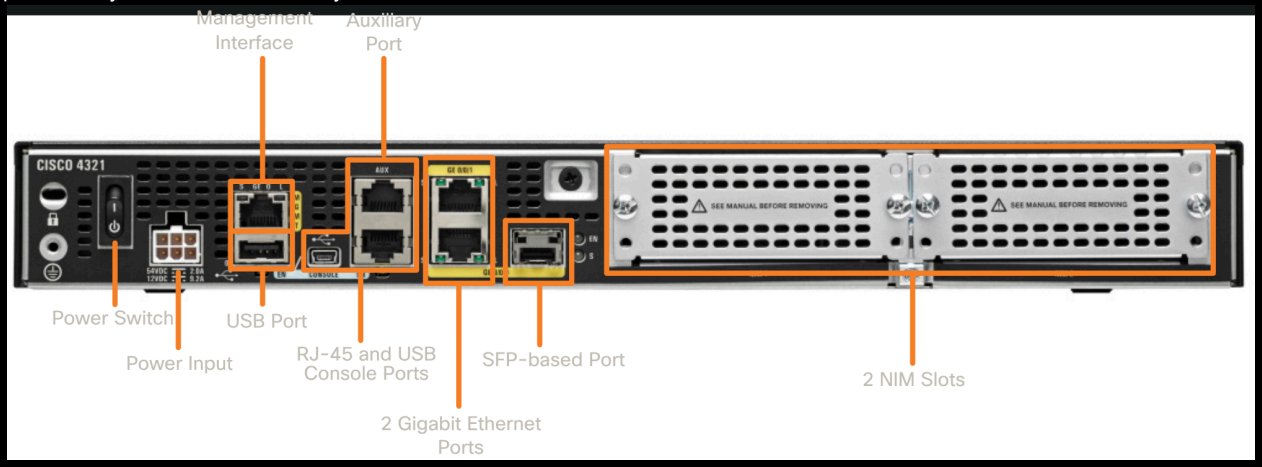
The CPU requires an OS to provide routing and switching functions. The Cisco Internetwork Operating System (IOS) is the system software used for most Cisco devices, regardless of the size and type of the device. It is used for routers, LAN switches, small wireless access points, large routers with dozens of interfaces, and many other devices.

Router Interface Ports

Although there are several different types and models of routers, every Cisco router has the same general hardware components. The figure shows a Cisco 4321 Integrated Services Router (ISR). The router includes the following connections:

- Console ports - Two console ports for the initial configuration and command-line interface (CLI) management access using a regular RJ-45 port and a USB Type-B (mini-B USB) connector.
- Two LAN interfaces - Two Gigabit Ethernet interfaces for LAN access labeled GE 0/0/0 and GE 0/0/1. The GE 0/0/0 port can be accessed through an RJ-45 connection or by using a small form-factor pluggable (SFP) attachment to provide a fiber-optics connection.
- Network Interface Modules (NIMs) - Two NIM expansion slots that provide modularity and flexibility by enabling the router to support different types of interface modules, including serial, digital subscriber line (DSL), switch ports, and wireless.

The Cisco 4321 ISR also has a USB port, a management interface, and an auxiliary port. The USB port can be use for file transfers. The management port can be used for remote management access when the two Gigabit Ethernet interfaces are unavailable. The auxiliary port provides legacy support for a method for connecting a dial-up modem to the router for remote access. The auxiliary port is rarely used in networks today.



Router Boot Process

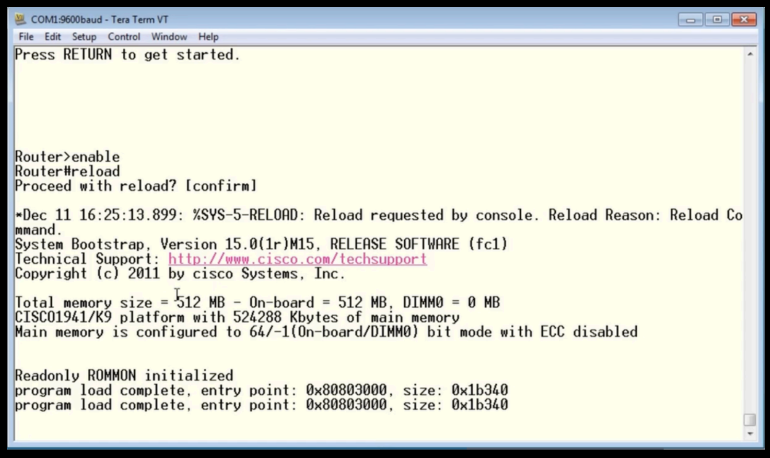
Power Up the Router

There are 6 main steps to the process:

1. Securely mount the device to the rack
2. Ground the device from electrical overloads
3. Plug the power cord in
4. Plug in the console cable
5. Turn the device on
6. Observe the startup messages on the laptop as the router boots up

Router Bootup Messages

```
Located isr4200-universalk9_ias.16.09.04.SPA.bin
#################################################....
(output omitted)

Package header rev 3 structure detected
IsoSize = 486723584
Calculating SHA-1 hash...Validate package: SHA-1 hash:
        calculated 4155409B:CC0DB23E:6D72A6AE:EA887F82:AC94DC6A
        expected   4155409B:CC0DB23E:6D72A6AE:EA887F82:AC94DC6A
RSA Signed RELEASE Image Signature Verification Successful.
Image validated

             Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

           Cisco Systems, Inc.
           170 West Tasman Drive
           San Jose, California 95134-1706



Cisco IOS Software [Fuji], ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9_IAS-
M), Version 16.9.4, RELEASE
SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
Compiled Thu 22-Aug-19 18:09 by mcpre

(output omitted)
```



Management Ports

Similar to a Cisco switch, there are several ways to access the command line interface on a Cisco router. The most common methods are as follows:

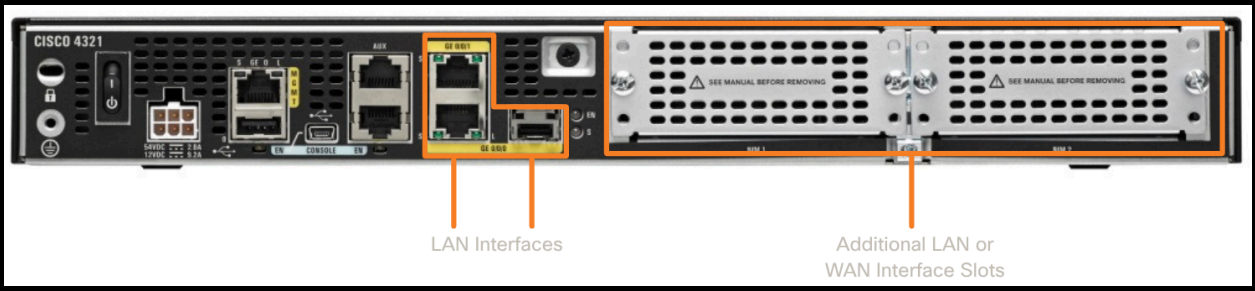
- Console - Uses a low speed serial or USB connection to provide direct connect, out-of-band management access to a Cisco device.
- SSH - Method for remotely accessing a CLI session across an active network interface, including the management interface.
- AUX port - Used for remote management of the router using a dial-up telephone line and modem.

The console port is a physical port located on the router. When using SSH, there must be an active network interface that is configured with a valid IP address for the network. This can be one of the active network interfaces used for network traffic or it can be the management interface.

Management Configuration Access

In addition to these management ports, routers also have network interfaces to receive and forward IP packets. Most routers have multiple interfaces that are used to connect to multiple networks. Typically, the interfaces connect to various types of networks, as shown in the figure, which means that different types of media and connectors are required.

LAN and WAN Interfaces



Module 7: Troubleshoot Common Network Problems

Network Troubleshooting Overview

Troubleshooting is the process of identifying, locating and correcting problems. Experienced individuals often rely on instinct to troubleshoot. However, there are structured techniques that can be used to determine the most probable cause and solution.

When troubleshooting, proper documentation must be maintained. This documentation should include as much information as possible about the following:

- The problem encountered
- Steps taken to determine the cause of the problem
- Steps to correct the problem and ensure that it will not reoccur

Document all steps taken in troubleshooting, even the ones that did not solve the issue. This documentation becomes a valuable reference should the same or similar problem occur again. Even in a small home network, good documentation saves hours of trying to remember how a problem was fixed in the past.

Gather Information

When a problem is first discovered in the network, it is important to verify it and determine how much of the network is affected by it. After the problem is confirmed, the first step in troubleshooting is to gather information. The following checklist provides some of the important information you should check.

Nature of problem

- End-user reports
- Problem verification report

Equipment

- Manufacturer
- Make / model
- Firmware version
- Operating system version
- Ownership / warranty information

Configuration and Topology

- Physical and logical topology
- Configuration files
- Log files

Previous Troubleshooting

- Steps taken
- Results achieved

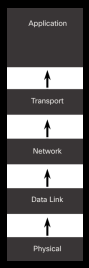
One of the first ways to gather information is to question the individual who reported the problem, as well as any other affected users. Questions can include end user experiences, observed symptoms, error messages, and information about recent configuration changes to devices or applications.

Next, collect information about any equipment that may be affected. This can be gathered from documentation. A copy of all log files and a listing of any recent changes made to equipment configurations is also necessary. Log files are generated by the equipment itself and are usually obtainable through the management software. Other information on the equipment includes the manufacturer, make and model of devices affected, as well as ownership and warranty information. The version of any firmware or software on the device is also important because there may be compatibility problems with particular hardware platforms.
Information about the network can also be gathered using network monitoring tools. Network monitoring tools are complex applications often used on large networks to continually gather information about the state of the network and network devices. These tools may not be available for smaller networks.

After all necessary information is gathered, start the troubleshooting process.

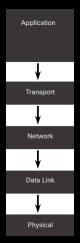
Structured Troubleshooting Methods

There are several structured troubleshooting approaches that can be used. Which one to use will depend on the situation. Each approach has its advantages and disadvantages. This topic describes methods and provides guidelines for choosing the best method for a specific situation.



Bottom-Up

In bottom-up troubleshooting, you start with the physical layer and the physical components of the network as shown in the figure, and move up through the layers of the OSI model until the cause of the problem is identified.
Bottom-up troubleshooting is a good approach to use when the problem is suspected to be a physical one. Most networking problems reside at the lower levels, so implementing the bottom-up approach is often effective.
The disadvantage with the bottom-up troubleshooting approach is it requires that you check every device and interface on the network until the possible cause of the problem is found. Remember that each conclusion and possibility must be documented so there can be a lot of paper work associated with this approach. A further challenge is to determine which devices to start examining first.

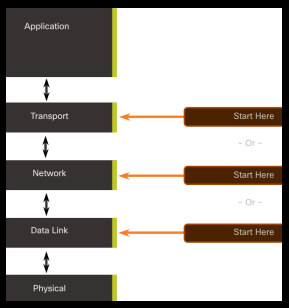


Top-Down

As shown in the figure, top-down troubleshooting starts with the end-user applications and moves down through the layers of the OSI model until the cause of the problem has been identified.
End-user applications of an end system are tested before tackling the more specific networking pieces. Use this approach for simpler problems, or when you think the problem is with a piece of software.
The disadvantage with the top-down approach is it requires checking every network application until the possible cause of the problem is found. Each conclusion and possibility must be documented. The challenge is to determine which application to start examining first.

Divide-and-Conquer

The figure shows the divide-and-conquer approach to troubleshooting a networking problem.
The network administrator selects a layer and tests in both directions from that layer.
In divide-and-conquer troubleshooting, you start by collecting user experiences of the problem, document the symptoms and then, using that information, make an informed guess as to which OSI layer to start your investigation. When a layer is verified to be functioning properly, it can be assumed that the layers below it are functioning. The administrator can work up the OSI layers. If an OSI layer is not functioning properly, the administrator can work down the OSI layer model.
For example, if users cannot access the web server, but they can ping the server, then the problem is above Layer 3. If pinging the server is unsuccessful, then the problem is likely at a lower OSI layer.



Follow-the-Path

This is one of the most basic troubleshooting techniques. The approach first discovers the traffic path all the way from source to destination. The scope of troubleshooting is reduced to just the links and devices that are in the forwarding path. The objective is to eliminate the links and devices that are irrelevant to the troubleshooting task at hand. This approach usually complements one of the other approaches.

Substitution

This approach is also called swap-the-component because you physically swap the problematic device with a known, working one. If the problem is fixed, then the problem is with the removed device. If the problem remains, then the cause may be elsewhere.
In specific situations, this can be an ideal method for quick problem resolution, such as with a critical single point of failure. For example, a border router goes down. It may be more beneficial to simply replace the device and restore service, rather than to troubleshoot the issue.
If the problem lies within multiple devices, it may not be possible to correctly isolate the problem.

Comparison

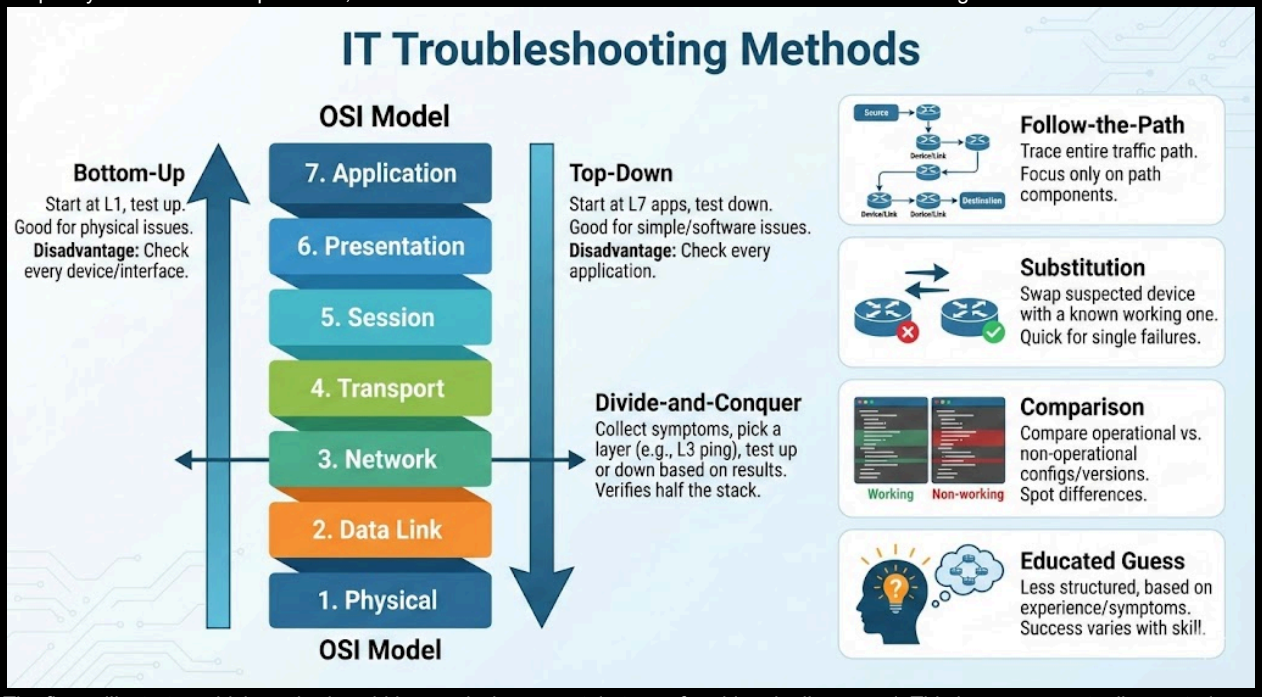
This approach is also called the spot-the-differences approach and attempts to resolve the problem by changing the nonoperational elements to be consistent with the working ones. You compare configurations, software versions, hardware, or other device properties, links, or processes between working and nonworking situations and spot significant differences between them.
The weakness of this method is that it might lead to a working solution, without clearly revealing the root cause of the problem.

Educated Guess

This approach is also called the shoot-from-the-hip troubleshooting approach. This is a less-structured troubleshooting method that uses an educated guess based on the symptoms of the problem. Success of this method varies based on your troubleshooting experience and ability. Seasoned technicians are more successful because they can rely on their extensive knowledge and experience to decisively isolate and solve network issues. With a less-experienced network administrator, this troubleshooting method may be too random to be effective.

Guidelines for Selecting a Troubleshooting Method

To quickly resolve network problems, take the time to select the most effective network troubleshooting method.



The figure illustrates which method could be used when a certain type of problem is discovered. This image was actually created with ChatGPT because the original was garbagio. Gar-BAGIO!

For instance, software problems are often solved using a top-down approach, while hardware-based problems are solved using the bottom-up approach. New problems may be solved by an experienced technician using the divide-and-conquer method. Otherwise, the bottom-up approach may be used.
Troubleshooting is a skill that is developed by doing it. Every network problem you identify and solve adds to your skill set.