Boson®

ICND1 Curriculum

100-105

Interconnecting Cisco Networking Devices Part 1

Version 3.0

Labs powered by

NetSim®
NETWORK SIMULATOR®

Boson

Interconnecting Cisco Networking Devices Part 1

100-105 Curriculum

LM20160804/BV3.0

Boson® NetSim® NETWORK SIMULATOR®

25 Century Blvd., Ste. 500, Nashville, TN 37214 | Boson.com

The labs referenced in this book have been printed in the Boson Lab Guide, which is included with the purchase of the curriculum. These labs can be performed with real Cisco hardware or in the Boson NetSim Network Simulator version 9 or later. To learn more about the benefits of using NetSim or to purchase the software, please visit www.boson.com/netsim.

Content in these modules is available in the full version of the curriculum. Please visit www.boson.com for more information.

Content in these modules is available in the full version of the curriculum. Please visit www.boson.com for more information.

Boson

Content in these modules is available in the full version of the curriculum. Please visit www.boson.com for more information.

Content in these modules is available in the full version of the curriculum. Please visit www.boson.com for more information.

Module 1

Networking Basics

Networking Basics Overview

- Network types
- Topologies
- Devices
- Physical media

Overview

Computer networks are used for a variety of reasons to facilitate many different objectives, from simple home networks consisting of just a few computers to corporate networks consisting of thousands of computers. When more than one computing device is connected in a way that allows for the sharing of information and hardware, a network is formed. This module covers the basics of networking, highlights the different types of environments, and discusses some of the characteristics and equipment involved in creating the environments in which communications and transfer of data are achieved.

Objectives

After completing this module, you should have the basic knowledge required to complete all of the following tasks:

- Understand major network types.
- Analyze the differences between various network topologies.
- Identify the common devices and physical media used in networks.

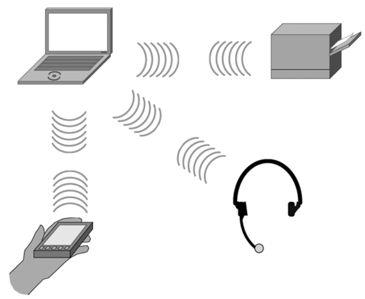
Network Types

- PANs
- LANs
- MANs
- WANs

Network Types

This section covers four basic network types: personal area networks (PANs), local area networks (LANs), metropolitan area networks (MANs), and wide area networks (WANs).

Personal Area Networks



- Bluetooth
- ZigBee

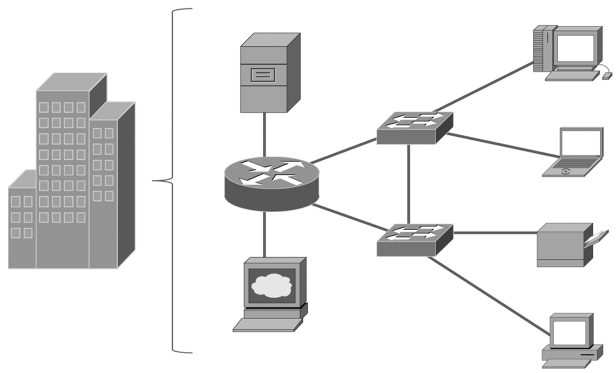
Personal Area Networks

A PAN can be used to connect and share data among devices that are located within a very close proximity of each other. For example, a personal computer, a telephone, a printer, and a wireless headset might all be a part of a home office setup using a PAN. Bluetooth and ZigBee are two technologies commonly used in a PAN setting.

Bluetooth is a short-range wireless technology that can be used to securely connect devices together. For example, Bluetooth can be used to transfer voice and data traffic between fixed or mobile devices. Bluetooth devices transmit data at the 2.4 to 2.485 gigahertz (GHz) frequency range. You can use Bluetooth to connect devices such as a mouse, a set of speakers, a scanner, a cell phone, and a printer to a computer. Several versions of Bluetooth exist. Bluetooth 1.2 supports a theoretical maximum data transfer speed of 1 megabit per second (Mbps), whereas Bluetooth 2.1 supports a theoretical maximum data transfer speed of up to 3 Mbps.

ZigBee is a wireless communications protocol used in electronics such as switches, timers, remote controls, and sensors. The protocol was developed as a low-cost alternative to other wireless PANs, and it can be less costly, mainly because of the low power and battery consumption requirements of the devices it is used in. For example, a sensor for a home lawn sprinkler system using ZigBee will be in sleep mode while not in use and will use power at only the scheduled time in order to activate the sprinklers, thus saving power and reducing the battery capacity required to operate for long periods of time.

Local Area Networks



• Ethernet

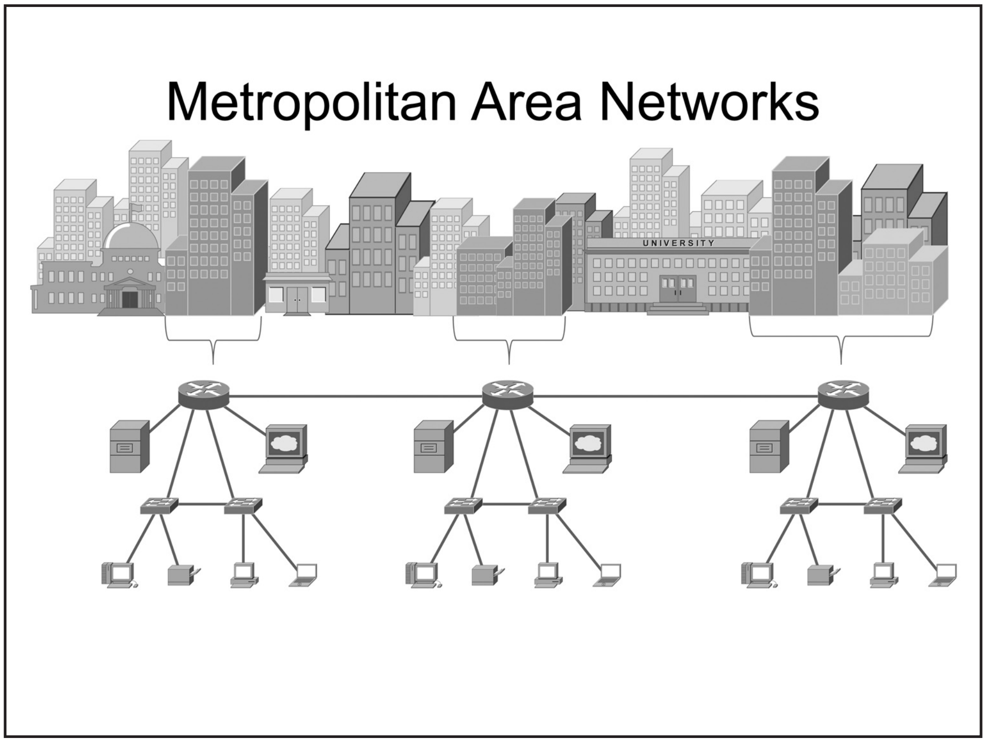
• Token Ring

Local Area Networks

LANs are typically used for communications within a single group or organization and typically within a single building or site where buildings are within close proximity of each other. Two common types of LANs include Ethernet networks and Token Ring networks.

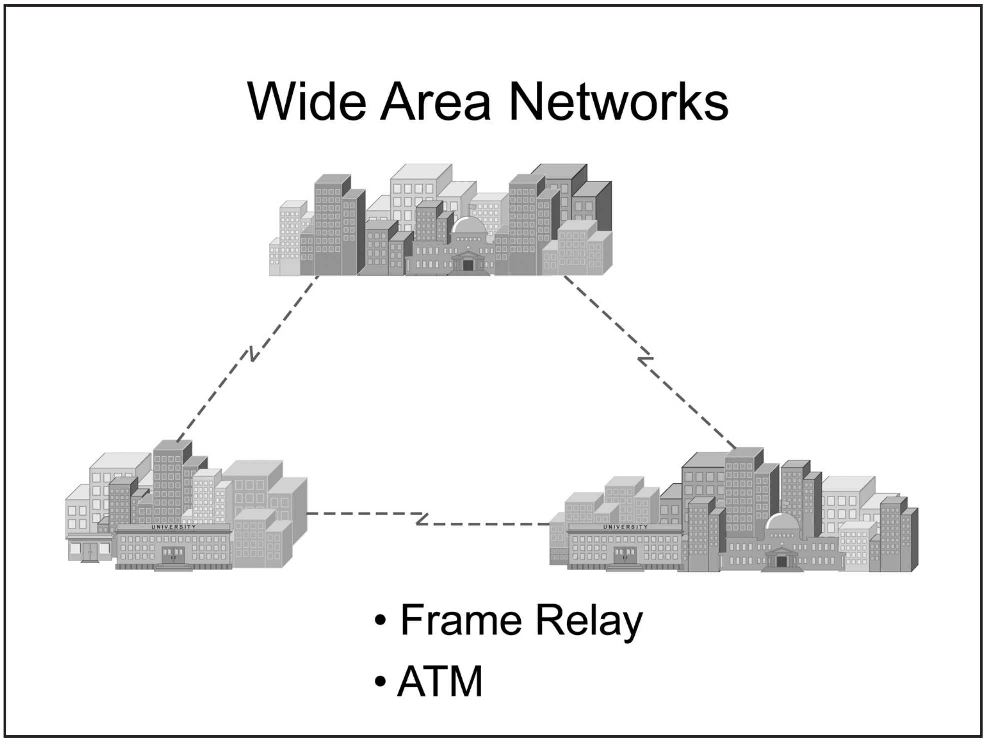
Ethernet networks originated with the use of coaxial cable. However, most modern Ethernet networks use unshielded twisted-pair (UTP) cables because they are inexpensive, are easy to install, and typically support network speeds of up to 1 gigabit per second (Gbps). UTP cables typically use RJ-45 connectors. The Ethernet cabling scheme uses one pair of wires to transmit data and another pair to receive data from end-station devices, such as computers or IP telephones, and networking devices, such as switches, hubs, or routers.

Token Ring networks use token passing to control media access. When token passing is used, a single token is sent around the ring from device to device. Because a device must wait until it has possession of the token before it can send data, only one device can transmit at a time. After the device has sent the data, the token is passed to the next device in the ring.



Metropolitan Area Networks

A MAN can be used to connect networks that reside within a single metropolitan area. For example, if a company has multiple locations within the same city, the company could configure a MAN to connect the LANs in each office together.



Wide Area Networks

A WAN is a network that covers a large geographical area. Often, a WAN is spread across multiple cities and even multiple countries. Computers connected to a WAN are typically connected through public networks, leased lines, or satellites. The largest example of a WAN is the Internet.

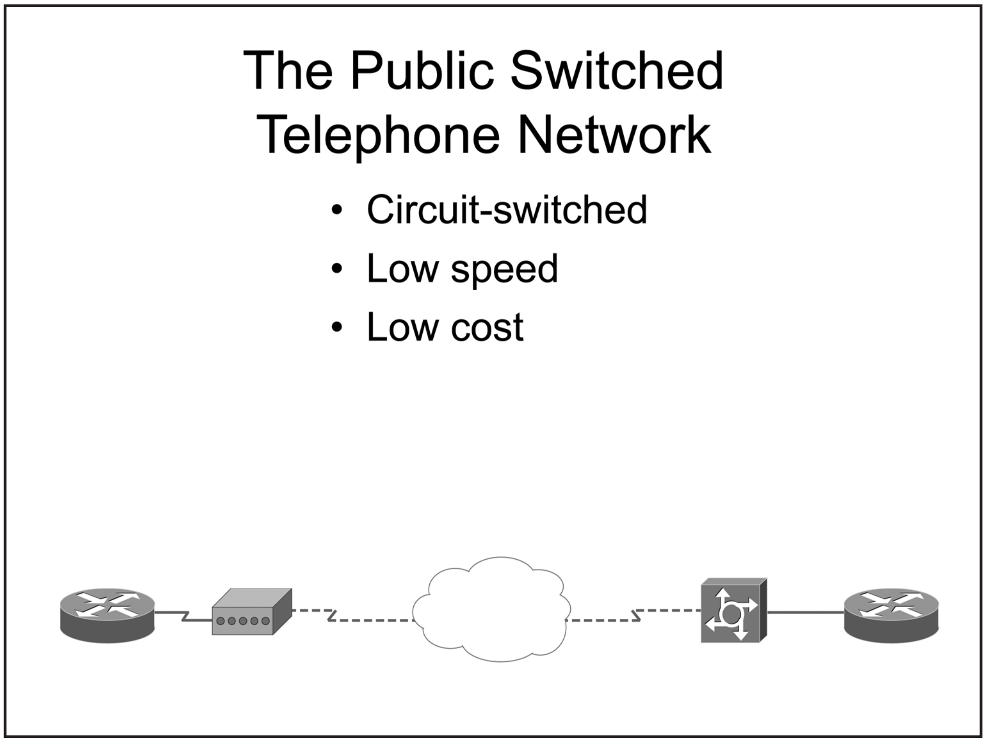
Understanding WAN Technologies

- PSTNs
- Leased lines
- Frame Relay
- ATM
- DSL
- Cable

Understanding WAN Technologies

Various access technologies can be used to enable WAN connectivity between remote sites. These technologies differ in many ways, including link speed, link latency, and cost. Some of the more common WAN access technologies are the following:

- Public Switched Telephone Networks (PSTNs)
- Leased lines
- Frame Relay
- Asynchronous Transfer Mode (ATM)
- Digital Subscriber Line (DSL)
- Cable

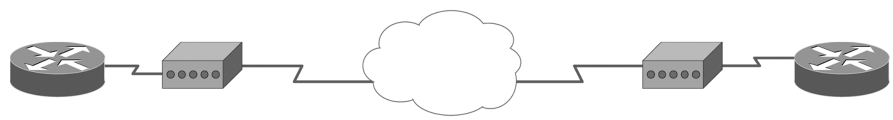


The Public Switched Telephone Network

The low-cost PSTN is a circuit-switched network commonly used for telephone service. Although the PSTN was designed for voice services, several methods have been developed to use the PSTN infrastructure for data services as well. The most common method for data service uses a modem to translate the digital signals used in computer networks into an analog signal that can be transported across the PSTN. However, because the PSTN was not designed for data services, the methods used to transport digital data are limited by the capabilities of the existing infrastructure. For example, data speeds on the PSTN typically do not exceed 56 kilobits per second (Kbps) because the infrastructure was not designed to support speeds beyond 64 Kbps.

Leased Lines

- Dedicated link
- High speed
- High cost

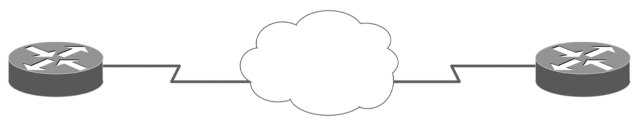


Leased Lines

Leased lines are dedicated circuits that are typically used as endpoint connections between sites. Because the circuits are dedicated and not switched, leased lines are more expensive for service providers to implement than switched circuits are. Leased lines are commonly available in a variety of speeds, such as 56 Kbps, 1.544 Mbps, and 45 Mbps.

Frame Relay

- Packet-switched
- Medium speed
- Medium cost

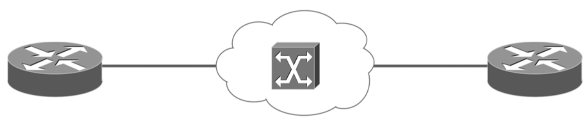


Frame Relay

Frame Relay is a cost-effective packet-switching technology that is suitable for data-only, medium-speed requirements. Frame Relay, which operates at the Data Link and Physical layers of the Open Systems Interconnection (OSI) model, uses statistical multiplexing and variable frame size to ensure network access and efficient delivery. Furthermore, Frame Relay allows multiple connections via virtual circuits (VCs) through a single interface. Frame Relay links are typically purchased in full or fractional T1 configurations.

ATM

- Cell-switched
- High speed
- High cost

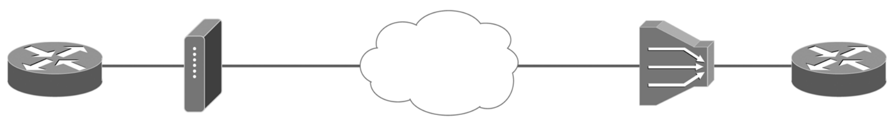


Asynchronous Transfer Mode

ATM is a high-speed packet switching technology similar to Frame Relay. However, ATM supports video and voice as well as data traffic. The most common ATM link speed is 155 Mbps; however, gigabit speeds are used between ATM switches. Because of their high speed, these connections are typically more expensive than Frame Relay.

DSL

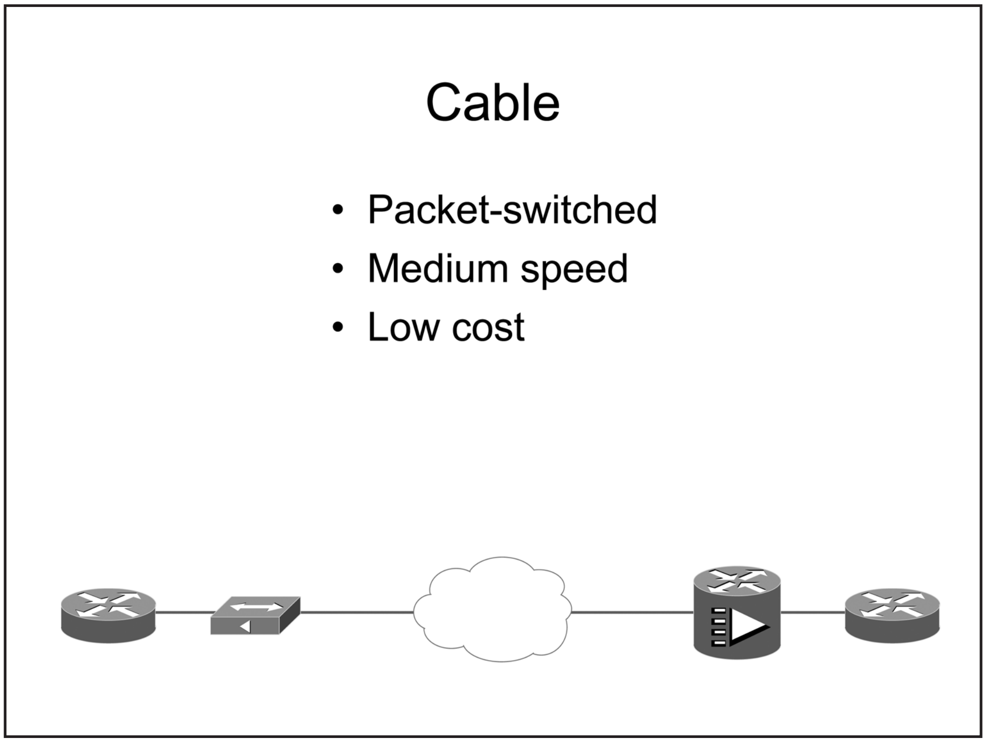
- Packet-switched
- Low speed
- Low cost



Digital Subscriber Line

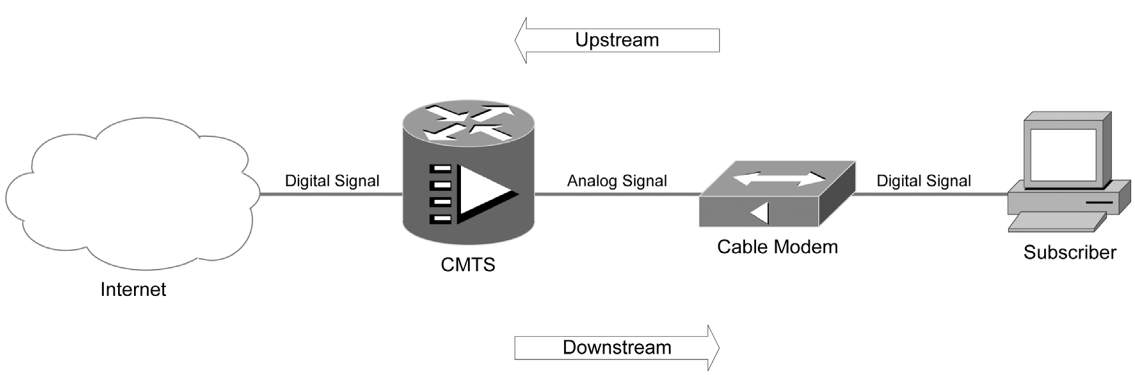
DSL is a WAN technology that offers low bandwidth and high latency relative to other WAN technologies. For example, Asymmetric DSL (ADSL) typically offers up to 12 Mbps of bandwidth in the downstream direction, which is the direction from the provider to the subscriber. However, because of its asymmetric nature, ADSL typically offers up to only 1 Mbps in the upstream direction, which is the direction from the subscriber to the provider. These speeds are miniscule when compared with WAN technologies, such as Synchronous Optical Network (SONET), which can offer up to 10 Gbps of synchronous bandwidth.

ADSL has a low initial cost and a low monthly cost. Because ADSL is a consumer-oriented WAN technology that offers limited bandwidth, the monthly cost, or tariff, is relatively low. Additionally, because a service provider can deliver ADSL to a subscriber's site without the addition of hardware such as repeaters, the initial cost of ADSL installation is also relatively low. However, because ADSL is typically implemented on existing copper lines, the reliability of an ADSL connection cannot be guaranteed. Thus ADSL cannot be considered a highly reliable WAN technology.



Cable

Cable networks are medium-speed, low-cost packet-switched networks. In a cable network, a cable modem termination system (CMTS) receives analog signals from the coaxial cable line and converts them into digital signals. The CMTS generally resides at the provider's location, or head end, and demodulates analog signals received from the coaxial cable line into digital signals suitable for transmission throughout the provider's network. The signals that pass to the CMTS from the coaxial cable are considered upstream signals and originate from the cable modem (CM) at the subscriber site, as illustrated below:

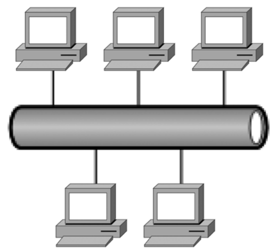


Conversely, the signals that pass to the CMTS from the provider network are considered downstream signals. The CMTS converts digital signals from the provider network into modulated analog signals that can be transmitted onto the coaxial cable line. The modulated analog signals are received by a CM at the subscriber site, where they are demodulated into a digital data stream suitable for transmission directly to the subscriber.

Network Topologies

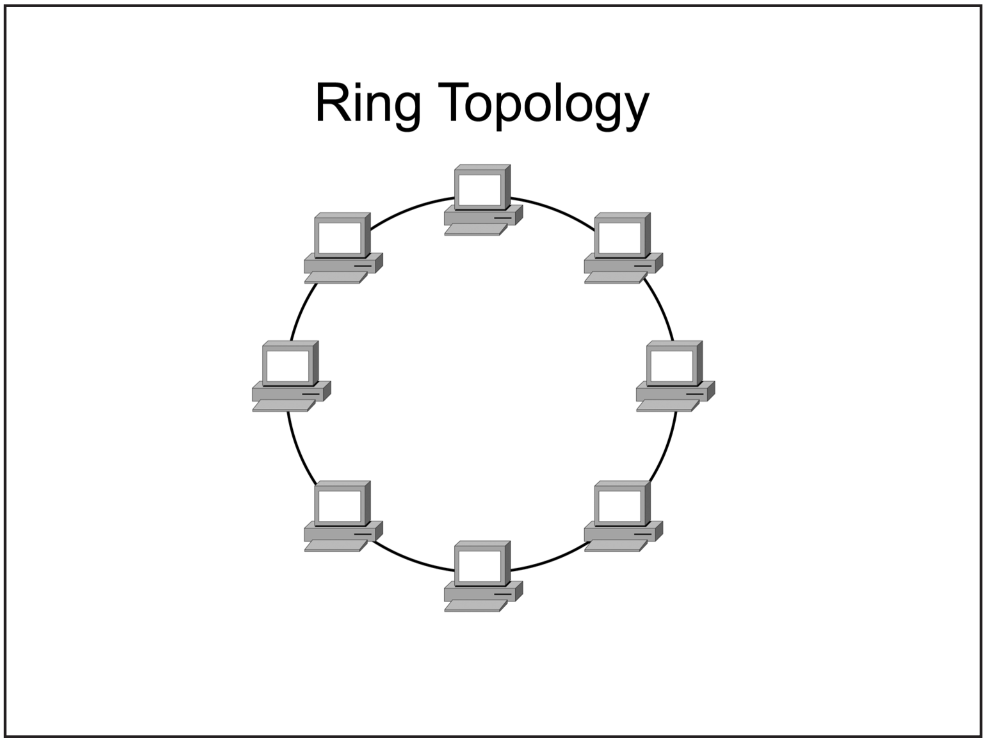
This section covers some basic network topologies: bus, ring, dual-ring, star, extended star, full-mesh, and partial-mesh. Additionally, it includes basic differences between physical topologies and logical topologies.

Bus Topology



Bus Topology

A bus topology has a single main line to which all computers on the network are attached. Bus topologies typically use coaxial cable and have several disadvantages, such as limited cable length and a limited number of hosts. Another disadvantage to a bus topology is that a failure on the main cable affects every host on the network.

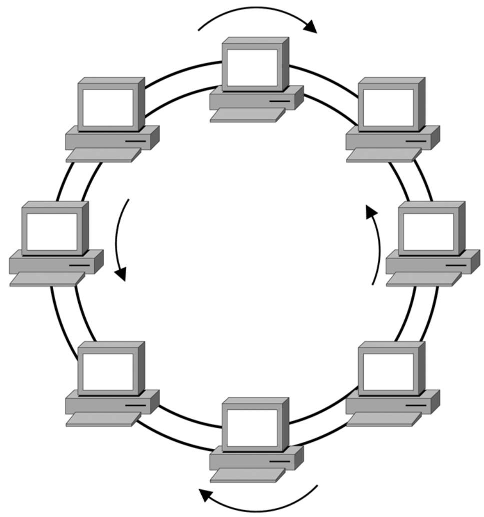


Ring Topology

A ring topology has a central ring of cable to which all hosts on the network connect. In a ring topology, each host is connected to exactly two other hosts. The flow of traffic in a ring topology goes in a single direction, with each node on the network handling each packet then passing it off to the next node in the ring. Similar to a bus topology, a failure in the ring affects every host on the network. The failure could be within the cable or one of the nodes. If a failure occurs, traffic flow will be disrupted until the issue is repaired or the faulty node is removed from the ring.

For some simpler network environments, the ring topology has advantages over a more complex topology; one advantage is the ability to connect computers and share data without the need to purchase costly servers.

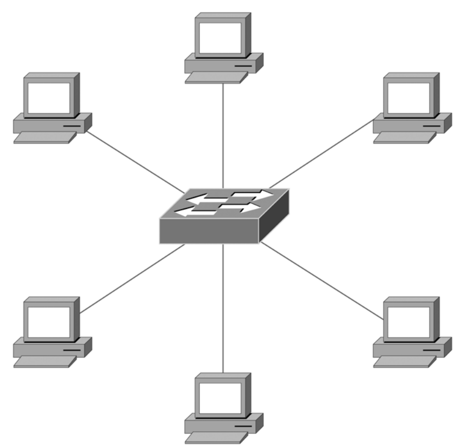
Dual-Ring Topology



Dual-Ring Topology

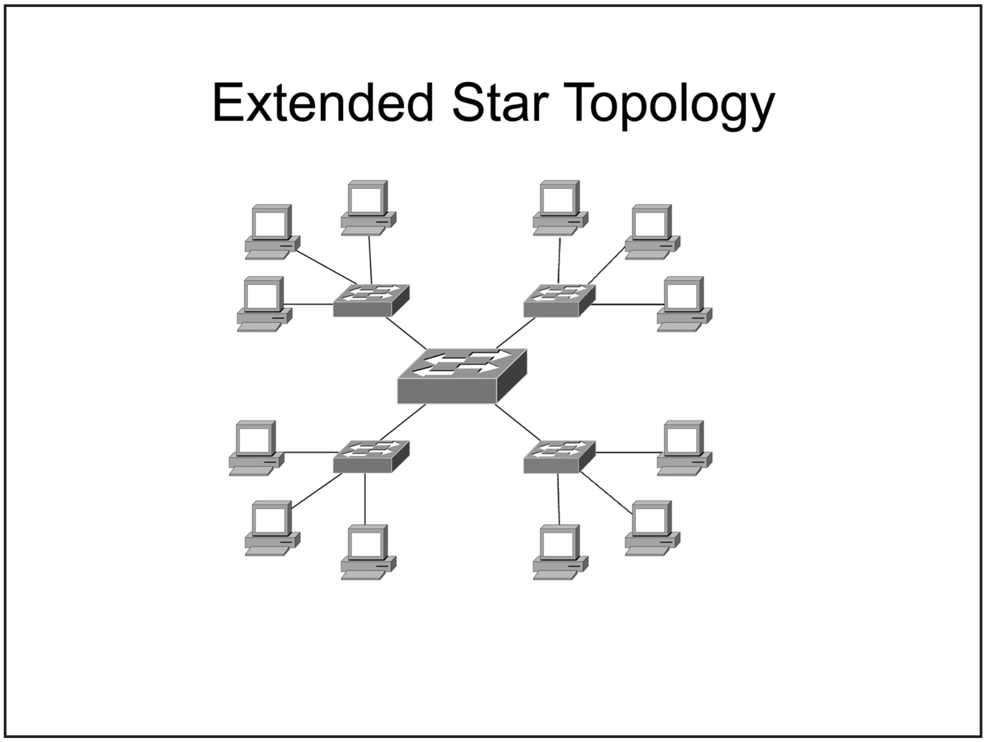
As compared to a standard ring topology, a dual-ring topology has a secondary ring which allows traffic to flow in the opposite direction of the first ring so that traffic can flow in both directions at the same time. This additional ring creates a backup path for traffic; in the event that one ring fails, traffic can still flow on the other ring. Having this redundancy does improve the reliability of the ring topology; however, this is limited to protecting against damage to the cables. If one of the nodes on the ring goes down, the traffic flow will still be interrupted on both rings.

Star Topology



Star Topology

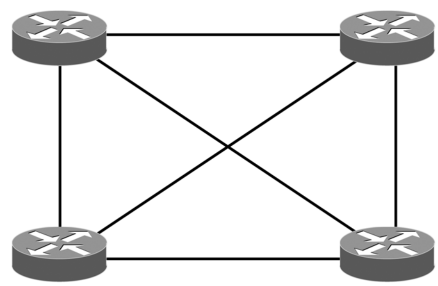
A star topology is the most common home and office network topology and is typically used on UTP Ethernet networks, but it can also be used with fiber-optic and coaxial cables. A star topology has a central connectivity device, such as a hub or a switch, to which all hosts on the network segment connect. In a very basic star topology scenario, data from one node on the network has to pass through only the central connectivity device before being sent to the intended recipient; traffic does not have to flow through all nodes in a star topology in order to reach the intended recipient. Not only can this topology improve performance, since data does not have to travel through unnecessary nodes, it also reduces the points of failure. Any given node on the network, or segment of cable, could fail and the rest of the network would still be able to communicate. However, a disadvantage of having this single point of failure is that if the central connectivity device fails, all traffic flow will stop until it has been repaired.



Extended Star Topology

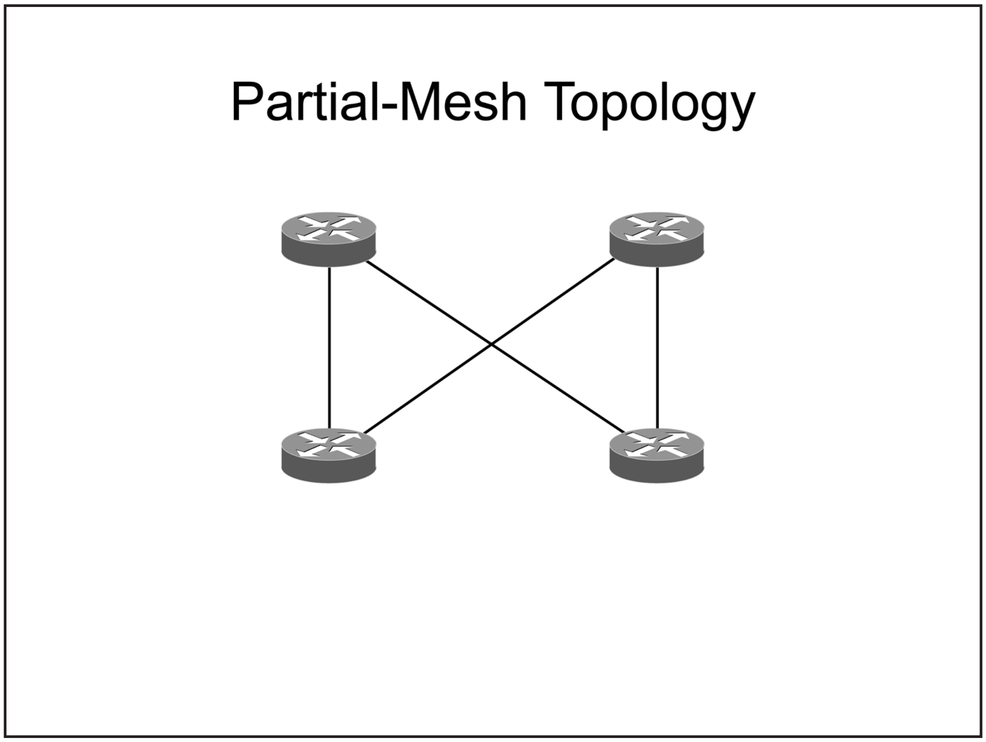
An extended star topology offers the same performance and reliability found in a star topology with the addition of the ability to cover greater distances from the central switch to the end nodes by adding repeaters or additional connectivity devices to the segments. The extended star topology makes more sense in a larger physical environment and allows you to reduce degradation of signal in places such as the far reaches of a large corporate office. Although additional points of failure are added with each extension device, the points of failure on any given segment of the network remain fairly easy to pinpoint. If one segment becomes unavailable in an extended star topology, hosts connected to other devices in the topology will still be able to communicate. By contrast, if the central device in a star topology fails, no devices will be able to communicate on the network.

Full-Mesh Topology



Full-Mesh Topology

A full-mesh topology is a very reliable network topology because of the redundancy built into it. For example, in a full-mesh network topology, each host is connected to every other host on the network. Reliability of this topology is greatly increased over other topologies because if even one segment or connection from a host to another host is down or inoperable, another path should be available for data to travel. However, even though a full-mesh topology is highly reliable, it is very difficult and expensive to implement, especially on networks that have many hosts. Thus, a full-mesh topology might be suitable for a small network environment, but it would be more costly and difficult to maintain as the network grew in physical size as well as number of nodes on the network.



Partial-Mesh Topology

Unlike a full-mesh topology, in a partial-mesh topology, each host does not connect to all other hosts on the network. Instead, in a partial-mesh topology, each host connects to only some of the other hosts, which reduces full redundancy yet maintains some failsafe reliability. Using a partial-mesh topology can reduce the maintenance and cost of cabling while still providing additional paths for traffic to flow in the event that one path becomes unavailable.

Physical vs. Logical Topologies

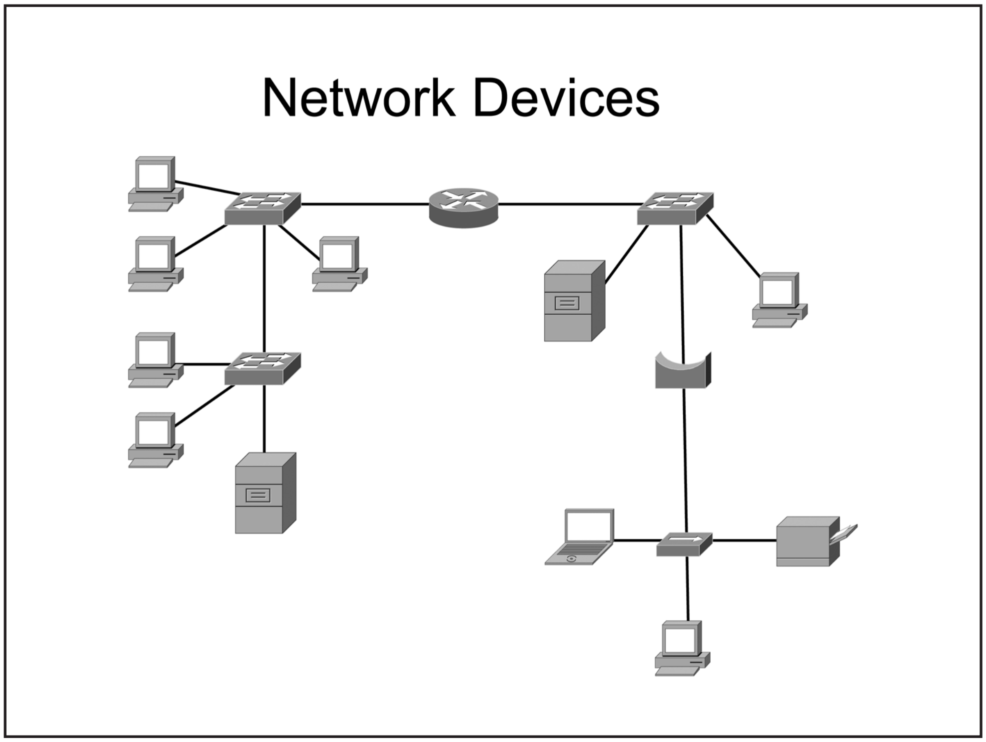
- Physical – Based on actual arrangement of devices and cables, or hardware-structured
- Logical – Based on the actual path of data flow, or protocol-structured

The physical topology of a network does not necessarily have to match the logical topology.

Physical vs. Logical Topologies

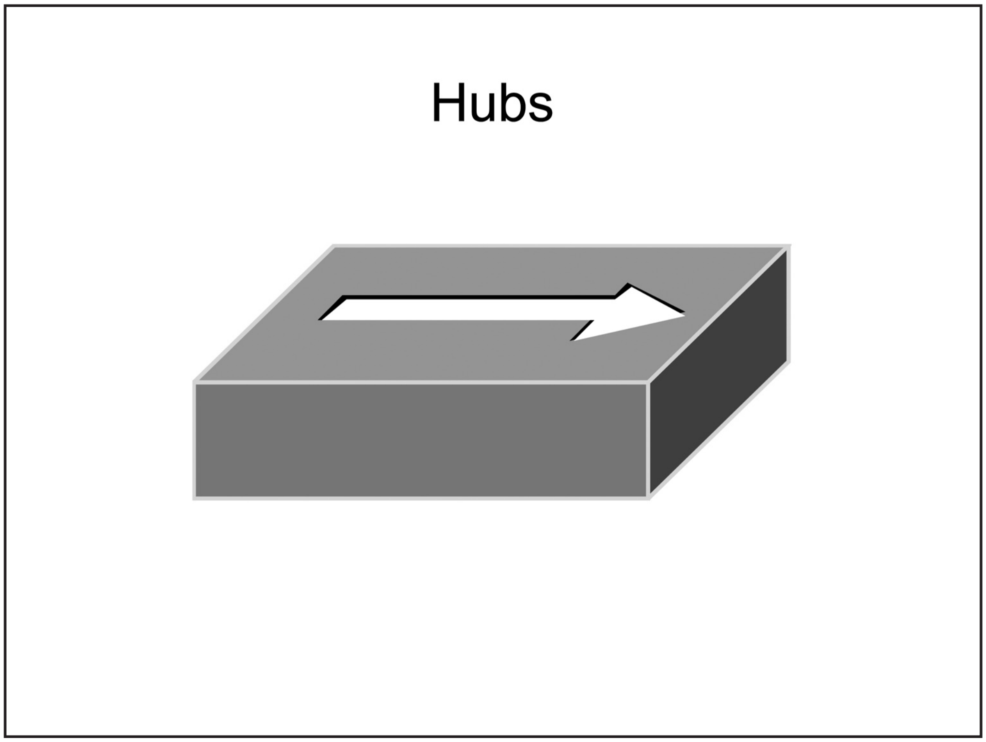
The physical topology refers to the hardware structure of the network and how the devices and cables are physically arranged. For example, a physical star topology consists of a central device, such as a hub or a switch, to which all other devices are physically connected. A physical ring topology consists of devices that are connected together in a ring; each device is connected to two other devices. In a bus topology, devices are physically connected in a bus layout.

The logical topology refers to the path the data follows as it moves around the network, without regard to how the hardware is physically configured. For example, data in a physical star topology could flow across the network in a ring network. In such a scenario, the logical topology would be that of a ring network, whereas the physical topology would be a star network. It is also possible for the physical and logical topologies to be the same, such as when data travels linearly from each computer in a physical bus topology.



Network Devices

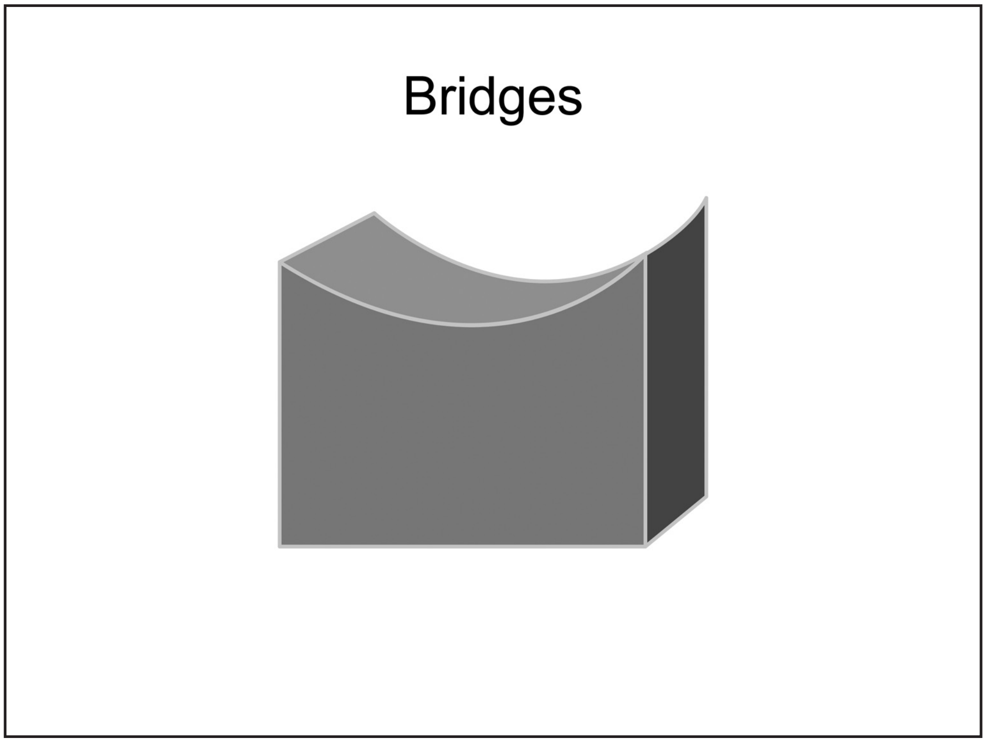
This section covers the basic network devices: hubs, bridges, switches, routers, servers, and hosts.



Hubs

A hub is a multiport physical repeater that is used primarily to connect end-user workstations. An incoming frame received on any hub port is simply rebroadcast out all the other ports except the port on which the frame was received. Hubs are inexpensive devices that do not create separate broadcast or collision domains.

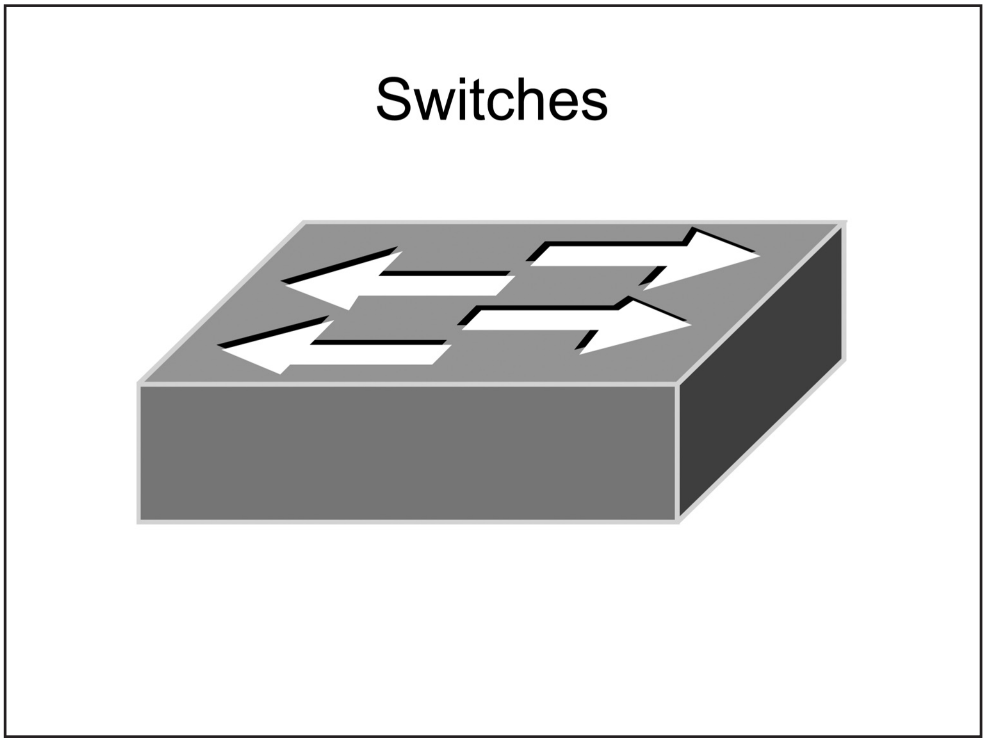
A collision domain is a network segment where collisions can occur when frames are sent among the devices on that network segment. For example, if four computers are connected to a hub, all four devices share the same bandwidth and each device can use only a portion of the total available bandwidth; therefore, collisions can occur when frames are sent simultaneously by multiple computers attached to the hub. A hub does not make any forwarding decisions based on Media Access Control (MAC) address or IP address. When connected to a hub, Ethernet devices rely on Carrier Sense Multiple Access with Collision Detection (CSMA/CD) to mitigate collision. With CSMA/CD, a transmitting device listens to the network segment before attempting to send data. If no transmissions are detected, the transmitting device sends its data and then listens to determine whether a collision occurs. If a collision is detected, each of the transmitting devices involved in the collision waits a random period of time before attempting to retransmit its data. Collision detection can function only when the devices do not attempt to transmit and receive at the same time; thus hubs are restricted to half-duplex mode. Devices connected to hubs cannot transmit and receive at the same time and therefore must also operate in half-duplex mode.



Bridges

Like a hub, a network bridge is a device to which endpoint devices can be connected. A bridge uses the MAC addresses of data recipients to deliver frames. Bridges maintain a forwarding database in which the MAC addresses of the attached hosts are stored. When a packet is received by a bridge, the sender's MAC address is recorded in the forwarding database, if it is not already there. If the recipient's address is also stored in the forwarding database, the packet will be sent directly to the recipient. However, if the recipient's MAC address is not in the forwarding database, the packet will be broadcast out all the ports with the exception of the port the packet arrived on. Each host will receive the packet and then use the MAC address to determine whether or not the data was intended for that host; if not, the host will discard the packet. When the intended recipient responds to the packet, the bridge will send the reply directly to the original sender because the original sender's MAC address is already stored in the forwarding database.

Bridges can be used to increase the number of collision domains. Each port on a bridge creates a separate collision domain. However, bridges do not create separate broadcast domains; all devices connected to a bridge will reside in the same broadcast domain.

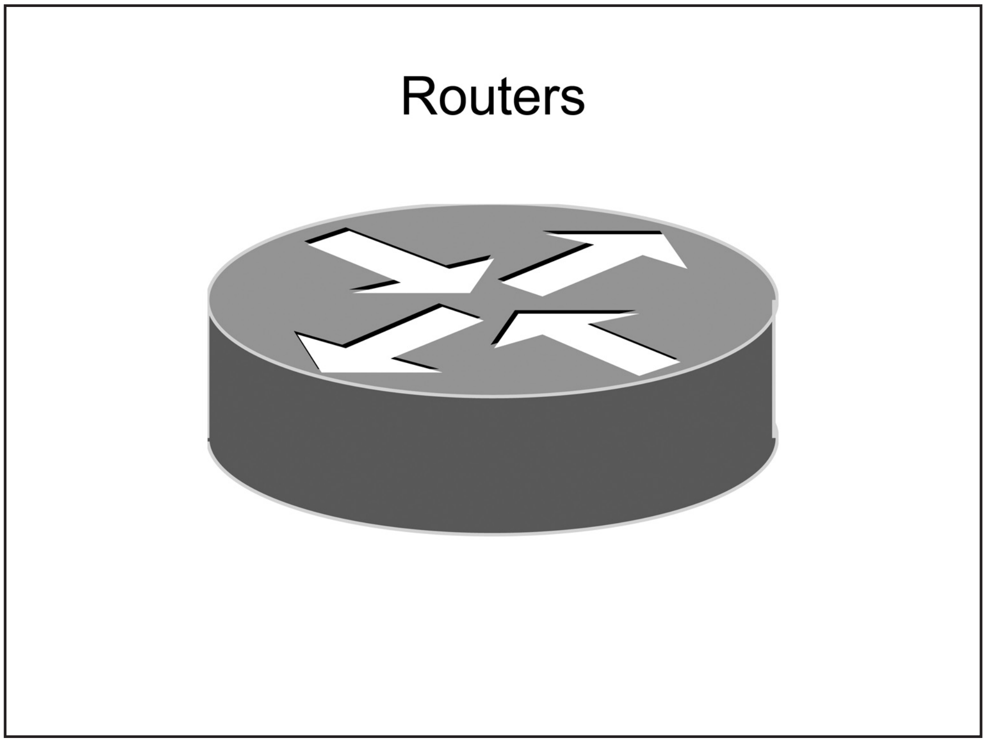


Switches

Like bridges, switches can be used to provide network connectivity to endpoint devices. Switches also function similarly to bridges. A switch uses information in the data packet headers to forward packets to the correct ports. This results in fewer collisions, improved traffic flow, and faster performance. Switches essentially break a large network into smaller networks. Switches perform microsegmentation of collision domains, which creates a separate, dedicated network segment for each switch port.

Switches use physical addresses, known as MAC addresses, to carry out their primary responsibility of switching frames. Switches store known MAC addresses in a special area of memory known as the Content Addressable Memory (CAM) table or switching table. The switching table associates MAC addresses with the physical interface through which those addresses can be reached. MAC addresses are dynamically learned as the switch forwards traffic between Ethernet devices. For example, when a switch receives a frame, the switch adds the source MAC address to the switching table, if the address does not already exist, so that the switch knows to which port to send frames that are destined for that MAC address. Then the switch will check the switching table to see if the destination MAC address in the received frame is listed. If so, the switch will direct the frame to the appropriate port. If the destination MAC address is not listed, the switch will broadcast the frame out all ports except the port from which the frame was received.

If four computers are connected to a switch, each computer will reside in its own collision domain, so all four computers can send data to the switch simultaneously. However, because switches forward broadcasts, all devices connected to a switch will reside within a single broadcast domain unless virtual LANs (VLANs) are used to separate the broadcast domains.

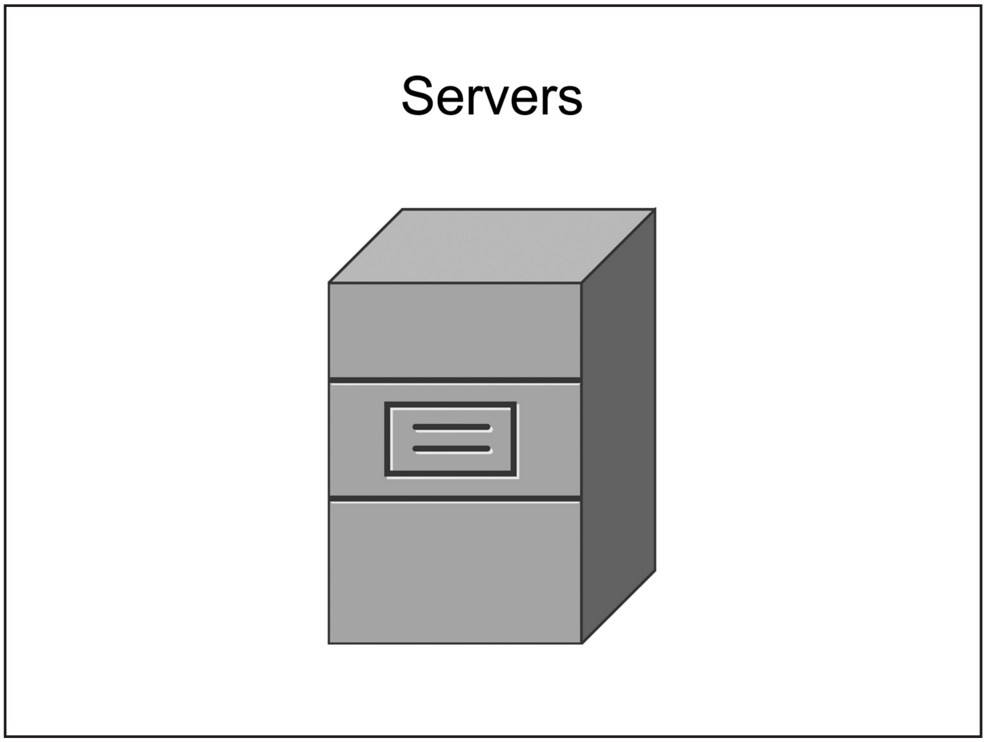


Routers

A router is used to forward packets between computer networks. Unlike switches, which create separate collision domains, routers create separate broadcast domains. Devices that are connected to a router reside in a separate broadcast domain. A broadcast that is sent on one network segment attached to the router will not be forwarded to any other network segments attached to the router. Layer 3 switches share many features and capabilities with dedicated routers; therefore, in this module and throughout the rest of the curriculum, the general term *router* refers to any device capable of processing packets at Layer 3.

A router makes path decisions based on logical addresses, such as IP addresses. Routers store IP address information in a routing table. The routing table is stored in a special section of memory known as a Ternary CAM (TCAM) table. Like the CAM table on a Layer 2 switch, a TCAM table is used to provide wire speed access to data for queries. However, unlike the CAM table, which can provide only exact, binary matches for queries, a TCAM table can provide a nonexact match for a particular query. Routers can implement multiple TCAM tables, and these tables are commonly used to facilitate the implementation of access control list (ACL) rules, Quality of Service (QoS) policies, and other Layer 3 operations that rely on table queries, such as routing table lookups.

When a router receives a packet, it will forward the packet to the destination network based on information in the routing table. If a router receives a packet that is destined for a remote network that is not listed in the routing table, and neither a static default route nor a gateway of last resort has been configured, then the packet is dropped and an Internet Control Message Protocol (ICMP) Destination Unreachable error message is sent to the interface from which the packet was received.

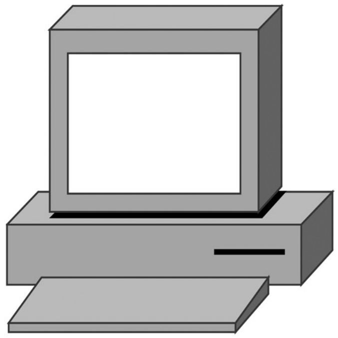


Servers

There are many different types of network servers and various functions associated with them. A server can be either a specific piece of hardware or a software program and is typically set up to provide specific services to a group of other computers on a network. Servers provide a centralized way to control, manage, and distribute a variety of technologies, such as simple data files, applications, security policies, and network addresses. Some examples of servers include the following:

- **File servers** – You can configure a file server to allow users to access shared files or folders stored on the server. File servers are used as a central storage location of shared files and folders.
- **Domain servers** – You can configure a domain server to manage the resources that are available on the domain. For example, you can use a domain server to configure access and security policies for users on a network.
- **Print servers** – You can set up a print server to provide access to a limited number of printers to many computer users, rather than requiring a local printer to be installed at each computer.
- **DHCP servers** – You could use a Dynamic Host Configuration Protocol (DHCP) server to automatically provide IP addresses to client computers. When a DHCP server is configured on the network, client computers can connect to the server and automatically obtain an IP address, rather than requiring an administrator to manually configure an IP address on each computer.
- **Web servers** – You could use a web server to allow customers to access your company's website. Web servers typically contain content that is viewable in a web browser, such as Internet Explorer.
- **Proxy servers** – You can configure a proxy server as an intermediary between a web browser and the Internet. When a computer on the internal network attempts to connect to the Internet, the computer first connects to the proxy server. Then the proxy server performs one of the following actions: the server forwards the traffic to the Internet, the server blocks the traffic, or the server returns a cached version of the requested webpage to the computer.

Hosts



Hosts

The hosts on a network are the individual computing devices that access the services available on the network. A host could be a personal computer (PC), a personal digital assistant (PDA), a laptop, or even a thin client or a terminal. The hosts act as the user interface, or the endpoint at which the user can access the data or other devices that are available on a network.

Physical Media

This section covers basic physical media used in networks, such as copper cables and fiber-optic cables.

Copper Cables

Copper Cables

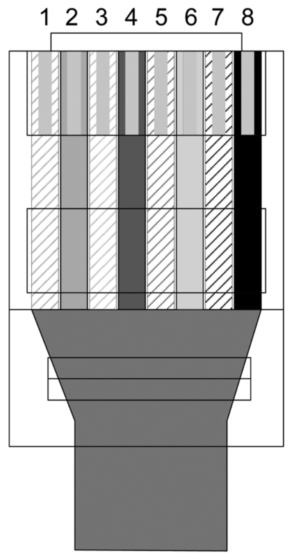
Copper is a soft metal that is an excellent conductor of both heat and electricity. Copper wires are used to transmit data as electrical signals. For example, Ethernet, Token Ring, and Copper Distributed Data Interface (CDDI) networks all use copper cabling to transmit data. Most modern Ethernet networks use copper UTP cables because they are inexpensive, are easy to install, and typically support network speeds of up to 1 Gbps. UTP cable segments should be no more than 100 meters in length.

UTP cables are segregated into different category ratings. A minimum rating of Category 3 is required to achieve a data transmission rate of up to 10 Mbps, which is also known as 10BaseT Ethernet. A minimum of Category 5 is required to achieve data rates of 100 Mbps, which is also known as Fast Ethernet or 100BaseTX Ethernet, or 1 Gbps, which is also known as Gigabit Ethernet or 1000BaseT Ethernet.

In the past, coaxial cables, which are another kind of copper cable, were used to connect devices together. Coaxial cables support longer segment runs than UTP cables. However, because of the low cost and high speeds of UTP cables, most modern Ethernet networks no longer use coaxial cables.

Connecting UTP with RJ-45

- Connectors contain eight pins
- Pins are numbered from left to right as you view the face of the connector, which is the side opposite of the clip
- Pins 1 and 2 are transmit pins for Ethernet and Fast Ethernet connections
- Pins 3 and 6 are receive pins for Ethernet and Fast Ethernet connections
- Gigabit Ethernet uses all eight pins and cable wires



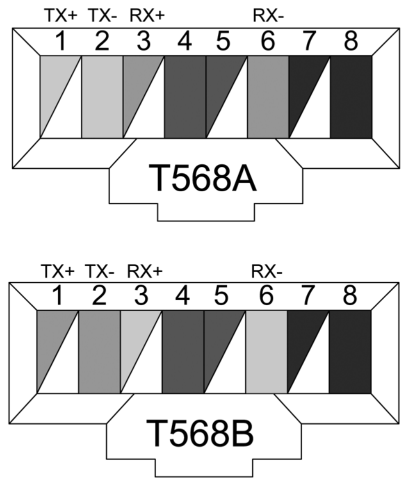
Connecting UTP with RJ-45

UTP cables contain four pairs of color-coded wires: white/green and green, white/blue and blue, white/orange and orange, and white/brown and brown. The eight total wires must be crimped into the eight pins within an RJ-45 connector, which is a connector that resembles an oversized telephone cable connector. The pins in the RJ-45 connector are arranged in order from left to right if you are viewing the face of the connector and have the connector positioned so that the row of pins is at the top.

In a typical Ethernet or Fast Ethernet cabling scheme, the wires that are connected to Pin 1 and Pin 2 transmit data and the wires that are connected to Pin 3 and Pin 6 receive data. By contrast, Gigabit Ethernet transmits and receives data on all four pairs of wires.

Connecting UTP with RJ-45

- Wires connect to pins based on one of two color-coded standards
- The transmit and receive wires in the T568A standard are inverse in the T568B standard



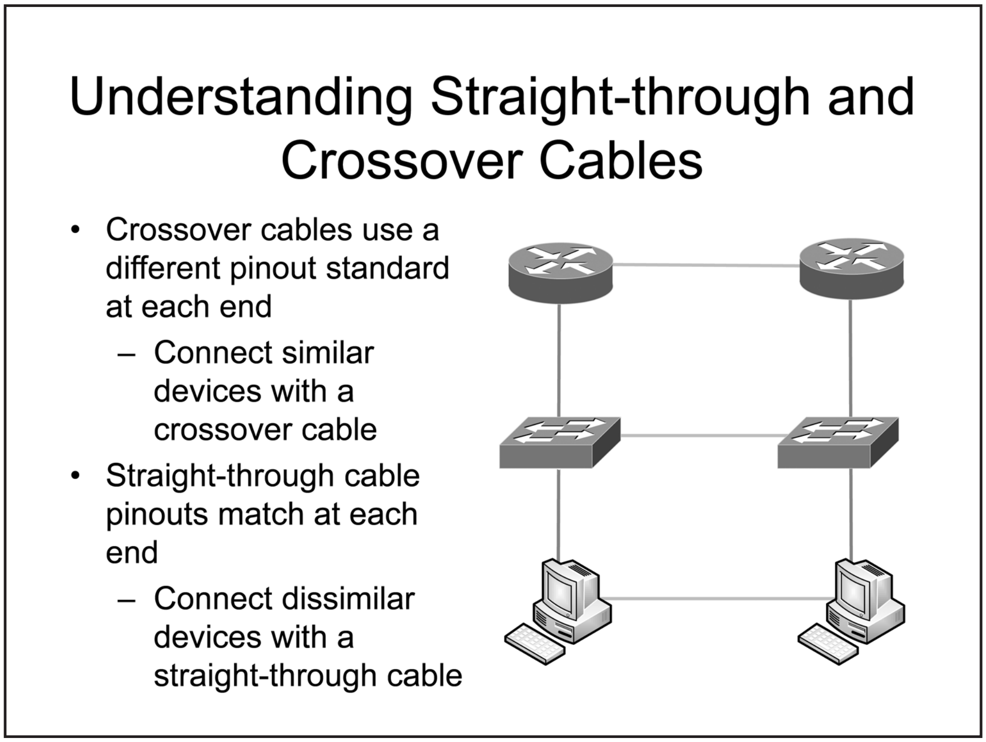
There are two different Telecommunications Industry Association (TIA) wire termination standards for an RJ-45 Ethernet connector: T568A and T568B. The T568A standard is compatible with Integrated Services Digital Network (ISDN) cabling standards. However, the T568B standard is compatible with a standard established by AT&T.

The difference between the two standards is that the wires used for transmit and receive in one standard are inverse in the other.

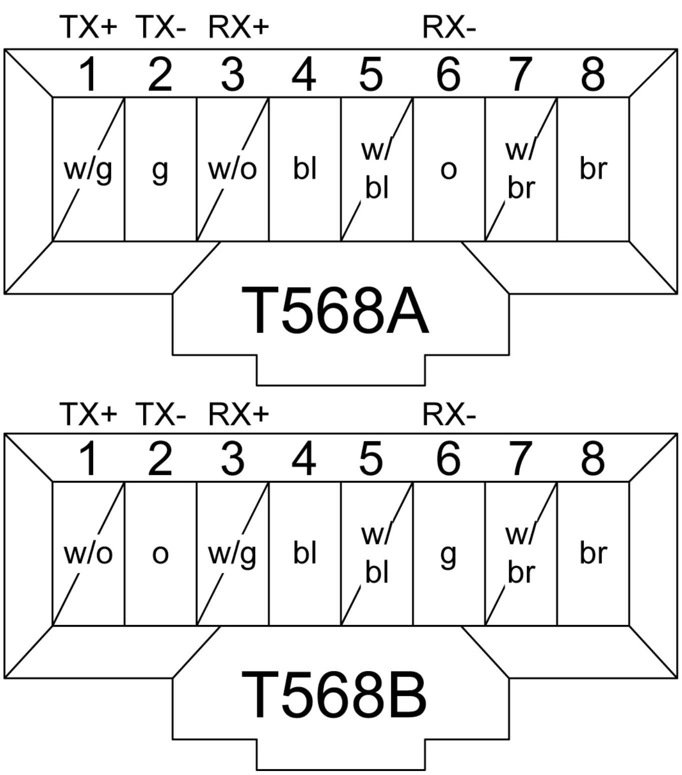
The T568A standard uses the white/green and green wires for Pins 1 and 2, respectively, and uses the white/orange and orange wires for Pins 3 and 6, respectively. Therefore, the T568A standard transmits over the white/green and green wires and receives over the white/orange and orange wires.

The T568B standard uses the white/orange and orange wires for Pins 1 and 2, respectively and uses the white/green and green wires for Pins 3 and 6, respectively. Therefore, the T568B standard transmits over white/orange and orange and receives over white/green and green.

The white/blue and blue and white/brown and brown wires are typically connected to the same pin regardless of which standard you use.



Understanding Straight-through and Crossover Cables

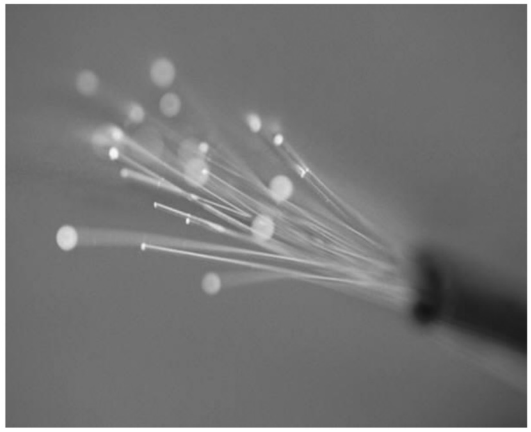


There are times when you should use the T568A-standard pinout on one side of a UTP Ethernet cable and the T568B-standard pinout on the other side of the cable. A crossover cable uses a different standard at each end. A crossover cable should be used to connect two workstations, two switches, or two routers together over the same Ethernet cable. By contrast, dissimilar Ethernet devices, such as a router and a switch, or a switch and a workstation, must be connected with a straight-through Ethernet cable. A straight-through cable uses the same pinout standard at each end.

If two dissimilar networking devices are connected with a straight-through Ethernet cable, the transmit pair on one device is connected to the receive pair on the other device. However, if two similar networking devices are connected with a straight-through Ethernet cable, the transmit pins on one device are connected to the transmit pins on the other device, and the devices will not be able to communicate. When you are troubleshooting network connectivity problems, a basic first approach is to verify that the cable that connects the two devices is the correct type and then reseat all cable connectors.

Because Gigabit Ethernet uses all eight wires of a UTP cable, the crossover pinout for a cable that is to be used over a Gigabit Ethernet connection is slightly more complex than an inverse T568-standard pinout. In addition to inverting the T586-standard transmit and receive wires, the white/blue and blue wires on one end of the cable should be inverse to the white/brown and brown wires on the other end of the cable.

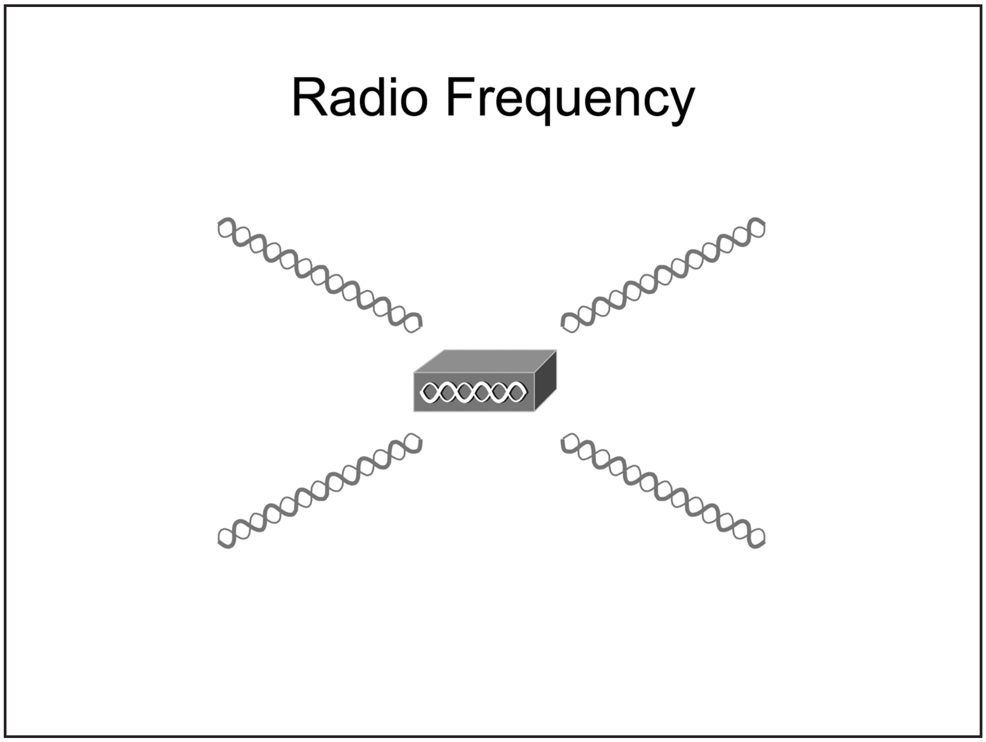
Fiber-Optic Cables



Fiber-Optic Cables

Unlike copper cables, which transmit data as electrical signals, fiber-optic cables transmit data as pulses of light; in addition, fiber-optic cables are not susceptible to radio frequency interference (RFI) or electromagnetic interference (EMI). Therefore, implementing fiber-optic cabling can be useful in buildings that contain sources of electrical or magnetic interference. Fiber-optic cables are also useful for connecting buildings that are electrically incompatible.

Because fiber-optic cables support greater bandwidth and longer segment distances than UTP cables, fiber-optic cables are commonly used for network backbones and for high-speed data transfer. Fiber-optic cables can be used to create Fiber Distributed Data Interface (FDDI) LANs, which are 100-Mbps dual-ring LANs. However, Cisco switches and Cisco routers do not require fiber-optic cable connections in order to communicate with each other. Although fiber-optic cables are useful in situations where there are problems or incompatibilities related to electrical issues, fiber-optic cables typically cost more than copper UTP, shielded twisted-pair (STP), or coaxial cables.



Radio Frequency

RF is an electrical signal that is sent over the air. RF signals are typically received by radio antennas and can be used to transmit video, audio, and data. Wireless LANs (WLANs) typically use RF signals to transmit data between devices. In WLANs, hosts connect to access points (APs), which provide the hosts with access to the rest of the network. In medium-to-large Cisco networks, a wireless LAN controller (WLC) can be used along with Lightweight Access Point Protocol (LWAPP) to manage APs. Cisco WLCs allow an administrator to centralize security configurations among APs and to provide mobility services at both Layer 2 and Layer 3 of the OSI model.

RF networks are susceptible to electrical interference. Electrical devices in your office building could cause interference to occur. Wireless devices that are close to the source of the interference could experience a disruption in wireless connectivity. Sources of interference can include microwave ovens, cordless phones, and high-power electric lines. Metal shelves, cabinets, and machinery can also block a wireless signal. To ensure that the devices on your network do not lose connectivity due to interference or signal blockage, you should install multiple APs on the network.

Review Question 1

Which of the following network types is typically used to share data among devices that are in close physical proximity?

A. LAN

B. MAN

C. PAN

D. WAN

Review Question 1

Which of the following network types is typically used to share data among devices that are in close physical proximity?

A. LAN
B. MAN
C. PAN
D. WAN

A personal area network (PAN) can be used to connect and share data among devices that are located within a very close proximity of each other. For example, a personal computer, a telephone, a printer, and a wireless headset might all be a part of a home office setup using a PAN.

Review Question 2

Which of the following network topologies offers the most redundancy?

A. star
B. extended star
C. full-mesh
D. dual ring

Review Question 2

Which of the following network topologies offers the most redundancy?

A. star

B. extended star

C. full-mesh

D. dual ring

A full-mesh topology is a very reliable network topology because of the redundancy built into it. For example, in a full-mesh network topology, each host is connected to every other host on the network. Reliability of this topology is greatly increased over other topologies because if even one segment or connection from a host to another host is down or inoperable, another path should be available for data to travel.

Index

Index

Symbols

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

Certification Candidates

Boson Software’s ExSim-Max practice exams are designed to simulate the complete exam experience. These practice exams have been written by in-house authors who have over 30 years combined experience writing practice exams. ExSim-Max is designed to simulate the live exam, including topics covered, question types, question difficulty, and time allowed, so you know what to expect. To learn more about ExSim-Max practice exams, please visit www.boson.com/exsim-max-practice-exams or contact Boson Software.

Organizational and Volume Customers

Boson Software’s outstanding IT training tools serve the skill development needs of organizations such as colleges, technical training educators, corporations, and governmental agencies. If your organization would like to inquire about volume opportunities and discounts, please contact Boson Software at orgsales@boson.com.

Contact Information

E-Mail: support@boson.com
Phone: 877-333-EXAM (3926)
615-889-0121
Fax: 615-889-0122
Address: 25 Century Blvd., Ste. 500
Nashville, TN 37214

Boson®

Boson.com

877.333.3926 support@boson.com