

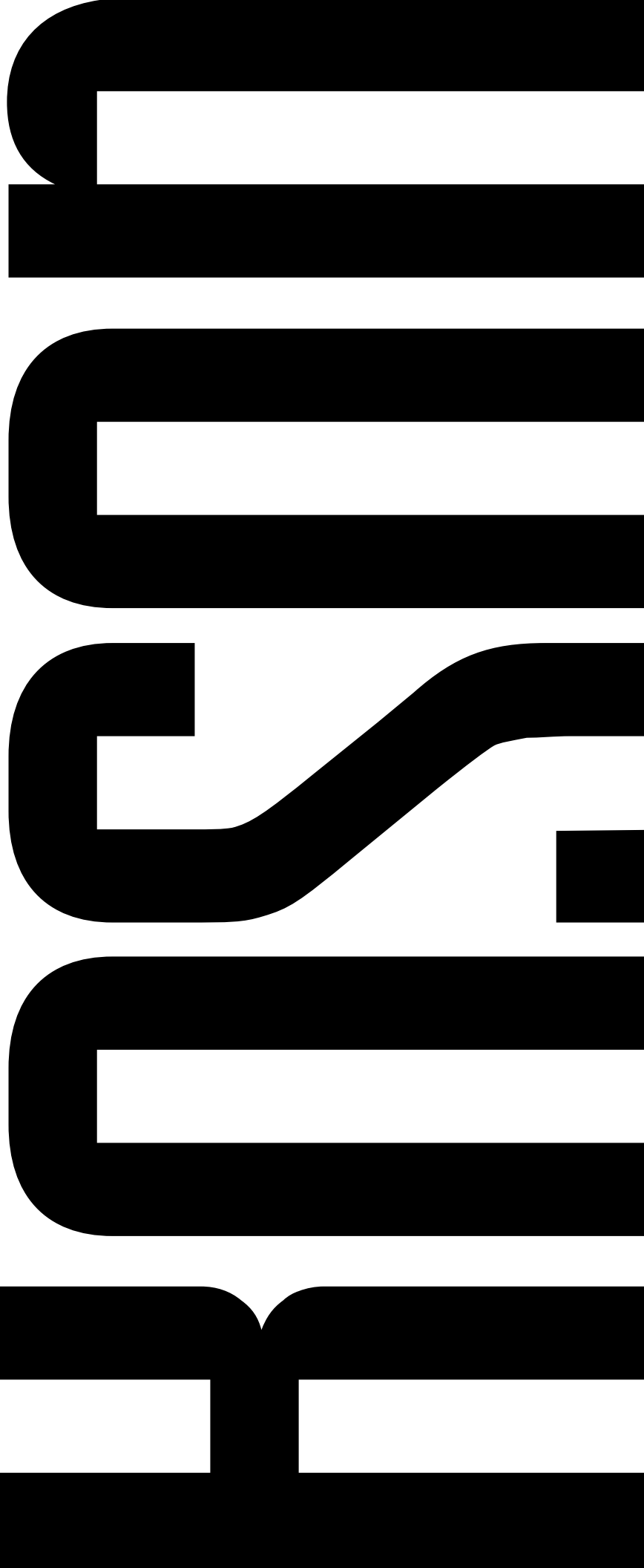


ICND1 Curriculum

640-822

Interconnecting Cisco Networking Devices Part 1
Version: Beta

Labs powered by



Interconnecting Cisco Networking Devices Part 1

640-822 Curriculum



25 Century Blvd. Ste. 500
Nashville, TN 37214
www.boson.com



The labs referenced in this book correspond to some of the labs available in the Boson NetSim 8 Network Simulator and have been printed in the Boson Lab Guide, which is available for purchase. To learn more about the Boson NetSim or to purchase and download the software, please visit www.boson.com/netsim-cisco-network-simulator.

Copyright © 2012 Boson Software, LLC. All rights reserved. Boson, Boson NetSim, Boson Network Simulator, and Boson Software are trademarks or registered trademarks of Boson Software, LLC. Catalyst, Cisco, and Cisco IOS are trademarks or registered trademarks of Cisco Systems, Inc. in the United States and certain other countries. Media elements, including images and clip art, are the property of Microsoft. All other trademarks and/or registered trademarks are the property of their respective owners. Any use of a third-party trademark does not constitute a challenge to said mark. Any use of a product name or company name herein does not imply any sponsorship of, recommendation of, endorsement of, or affiliation with Boson, its licensors, licensees, partners, affiliates, and/or publishers.

Module 1: Networking Basics	1
Overview	2
Objectives	2
Network Types	3
Personal Area Networks.....	4
Local Area Networks	5
Metropolitan Area Networks.....	6
Wide Area Networks	7
Network Topologies	8
Bus Topology.....	9
Ring Topology.....	10
Dual-Ring Topology.....	11
Star Topology	12
Extended Star Topology.....	13
Full-Mesh Topology	14
Partial-Mesh Topology	15
Physical vs. Logical Topologies.....	16
Network Devices.....	17
Hubs	18
Bridges	19
Switches	20
Routers.....	21
Servers.....	22
Hosts	24
Printers	25
Physical Media.....	26
Copper Cables	27
Connecting UTP with RJ-45.....	28
Understanding Straight-through and Crossover Cables.....	30
Fiber-Optic Cables	31
Radio Frequency	32
Review Question 1	33
Review Question 2.....	35
Module 2: Networking Models	37
Overview	38
Objectives	38
The OSI Model.....	39
Application Layer.....	40
Presentation Layer	41
Session Layer.....	42
Transport Layer	43

Network Layer	44
Data Link Layer	45
Physical Layer	46
Using the OSI Model to Troubleshoot Networks.....	47
Understanding the Bottom Up Troubleshooting Technique.....	47
Understanding the Top Down Troubleshooting Technique.....	47
Understanding the Divide and Conquer Troubleshooting Technique	48
TCP/IP Model.....	49
Application Layer.....	50
Transport Layer	51
Internet Layer	52
Network Access Layer.....	53
Network Model Comparison	54
Hierarchical Network Design Model	55
The Core Layer.....	56
The Distribution Layer	57
The Access Layer.....	58
Review Question 1.....	59
Review Question 2.....	61
Module 3: Network Addressing	63
Overview	64
Objectives	64
Layer 2 Addressing	65
Ethernet Overview.....	66
MAC Address	68
Layer 3 Addressing	70
IPv4 Overview	71
Binary Overview	73
Dotted Decimal Overview.....	74
Converting from Binary to Decimal	75
Converting from Decimal to Binary	77
Classful Networks	80
Classless Networks	82
Subnetting	84
Layer 4 Addressing	87
UDP.....	88
TCP	90
Review Question 1.....	92
Review Question 2.....	94
Lab Exercises	96
Module 4: Packet Delivery	97

Overview	98
Objectives	98
Devices in the Packet Delivery Process	99
Hubs	100
Switches	101
Routers	102
Gateways	104
Hosts	105
The Flow of Data	106
PDUs and SDUs	107
Intra-layer Communication	108
Inter-layer Communication	109
The Packet Delivery Process in Action	110
The Application Layer	111
The Transport Layer	112
<i>UDP</i>	113
<i>TCP</i>	114
<i>The TCP Three-Way Handshake</i>	115
<i>Windowing</i>	117
<i>Sliding Windowing</i>	118
The Internet Layer	119
<i>The Protocol Field</i>	119
<i>ARP</i>	120
The Network Access Layer	121
Host-to-Host Packet Delivery Example	122
Review Question 1	134
Review Question 2	136
Review Question 3	138
Module 5: Device Management	141
Overview	142
Objectives	142
Accessing Cisco Devices	143
Console Access	144
AUX Port Access	145
vty Access	146
<i>Telnet</i>	146
<i>SSH</i>	146
IOS Overview	148
Device Modes	149
<i>User EXEC Mode</i>	149
<i>Privileged EXEC Mode</i>	149
<i>Global Configuration Mode</i>	150

<i>Interface Configuration Mode</i>	150
<i>Line Configuration Mode</i>	150
<i>Router Configuration Mode</i>	150
CLI Features	151
<i>Context-sensitive Help</i>	151
<i>Command History</i>	151
<i>Syntax Verification</i>	152
<i>Abbreviated Entry</i>	152
<i>Enhanced Editing</i>	152
IOS Boot Process	153
Loading IOS Images	154
Changing the IOS Image Load Location	155
Using the Configuration Register	156
Handling IOS Load Errors	157
Upgrading IOS	158
<i>Troubleshooting IOS Upgrades</i>	159
Initial Device Setup	160
Automated Setup	160
Manual Setup	161
Configuration Management	162
Cisco Discovery Protocol	163
The show cdp neighbors Command	164
The show cdp neighbors detail Command	165
The show cdp entry Command	167
Disabling CDP	169
Using IOS to Troubleshoot Networks	170
Understanding show Commands	171
Understanding debug Commands	172
Understanding the ping Command	173
Understanding the traceroute Command	174
Review Question 1	175
Review Question 2	177
Lab Exercises	179
Module 6: Network Security Basics	181
Overview	182
Objectives	182
Adversaries	183
Goals and Motivations	184
Classes of Attacks	185
Common Threats	186
Physical Threats	187
<i>Electrical Threats</i>	188

<i>Hardware Threats</i>	189
<i>Environmental Threats</i>	190
<i>Administrative Threats</i>	191
Reconnaissance Attacks.....	192
<i>Packet Sniffing</i>	193
<i>Ping Sweeps</i>	194
<i>Port Scans</i>	195
Access Attacks.....	196
<i>Password Attacks</i>	197
<i>Buffer Overflow Attacks</i>	198
Protecting Assets.....	199
Securing Cisco Devices.....	200
Warning Banners.....	201
<i>Login Banners</i>	202
<i>MOTD Banners</i>	203
<i>EXEC Banners</i>	204
Securing Access.....	205
<i>Requiring Authentication</i>	206
<i>Configuring User Names and Passwords</i>	207
<i>Forcing SSH Access</i>	208
<i>Configuring an Enable Password</i>	209
Review Question 1.....	210
Review Question 2.....	212
Review Question 3.....	214
Lab Exercises	216
Module 7: Switches	217
Overview.....	218
Objectives.....	218
Benefits of Switches	219
Physical Attributes of Switches.....	221
Switch LEDs.....	222
Switch Port Types.....	224
<i>Ethernet</i>	224
<i>Console</i>	224
Switching Modes.....	225
Store-and-Forward Switching	226
Cut-Through Switching	227
Adaptive Cut-Through Switching	228
FragmentFree Switching	229
Switch Interface Configuration.....	230
Configuring Interface Duplex.....	231
Configuring Interface Speed	233

Verifying Switch Configuration	234
<i>The show interfaces Command</i>	235
<i>The show running-config Command</i>	237
Troubleshooting Switches	238
<i>Excessive Noise</i>	239
<i>Collisions</i>	241
<i>Late Collisions</i>	243
<i>Duplex Mismatch</i>	245
<i>Speed Mismatch</i>	247
Basic Switch Security	249
Disabling Unused Ports.....	250
Configuring Port Security	251
Spanning Tree Protocol	253
Review Question 1	254
Review Question 2.....	256
Lab Exercises	258
Module 8: Routers	259
Overview	260
Objectives	260
Router Benefits	261
Layer 3 Forwarding.....	261
Broadcast Domains	262
Common Router Features	263
<i>Modularity</i>	263
<i>Number of Physical Ports</i>	263
<i>Routed Ports</i>	263
<i>AUX Ports</i>	264
<i>Compact Flash Storage</i>	264
Understanding the Routing Process	265
Route Types	266
Directly Connected Routes.....	267
<i>Verifying a Directly Connected Route</i>	268
Static Routes	269
<i>Configuring a Static Route</i>	270
<i>Verifying a Static Route</i>	271
Dynamic Routes	273
<i>Routing Metrics</i>	273
<i>Administrative Distance</i>	274
<i>Dynamic Routing Protocols</i>	275
<i>Interior or Exterior Routing Protocols</i>	276
<i>Common Routing Protocols</i>	277
<i>Classful or Classless Routing Protocols</i>	278

<i>Distance-Vector or Link-State Routing Protocols</i>	279
Default Routes	286
<i>Configuring a Default Route</i>	287
<i>Verifying a Default Route</i>	288
Understanding WAN Technologies	289
The PSTN	290
Leased Lines	291
Frame Relay	292
ATM	293
DSL	294
Cable	295
Configuring Router Interfaces	296
Interface Overview	296
<i>Modular Routers</i>	297
<i>Expansion Modules</i>	298
Configuring a LAN Interface	300
<i>Configuring an Ethernet Interface</i>	301
<i>Verifying an Ethernet Interface</i>	302
<i>Troubleshooting an Ethernet Interface</i>	303
Configuring a WAN Interface	305
<i>Common WAN Encapsulation Protocols</i>	305
<i>Configuring a Serial Interface</i>	307
<i>Verifying a Serial Interface</i>	308
<i>Troubleshooting a Serial Interface</i>	309
Configuring a PPP Interface	311
Understanding DNS	312
Configuring a DNS Client	313
Configuring a DNS Server	314
Understanding DHCP	315
DHCP Discover	316
DHCP Offer	317
DHCP Request	318
DHCP Acknowledgment	319
Configuring a DHCP Client	320
Configuring a DHCP Server	321
Configuring DHCP Server Options	322
Understanding NAT/PAT	323
NAT Methods	323
NAT/PAT Address Terminology	324
Translation Methods	326
Static NAT	327
Dynamic NAT	328
PAT	330

Configuring Interfaces for NAT/PAT	331
Configuring Static NAT	332
Configuring Dynamic NAT	333
Configuring PAT	335
Review Question 1	337
Review Question 2	339
Review Question 3	341
Lab Exercises	343
Module 9: WLANs	345
Overview	346
Objectives	346
WLAN Basics	347
Wireless Standards Organizations	348
Wireless Standards	349
802.11a	350
802.11b	351
802.11g	352
802.11n	353
Other Wireless Standards	354
WiMAX	354
Infrared	354
Bluetooth	354
Wireless Components	355
Access Points	356
Wireless Clients	357
Wireless Operation	358
Wireless Topologies	359
<i>IBSS</i>	359
<i>BSS</i>	360
<i>ESS</i>	361
Associating with Wireless Clients	362
Wireless Security	363
WEP	364
WPA	365
WPA2	366
802.1X	367
Troubleshooting WLANs	368
Review Question 1	369
Review Question 2	371
Index	373

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. In this module, we discuss the basics of networking, highlight the different types of environments, and discuss 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:

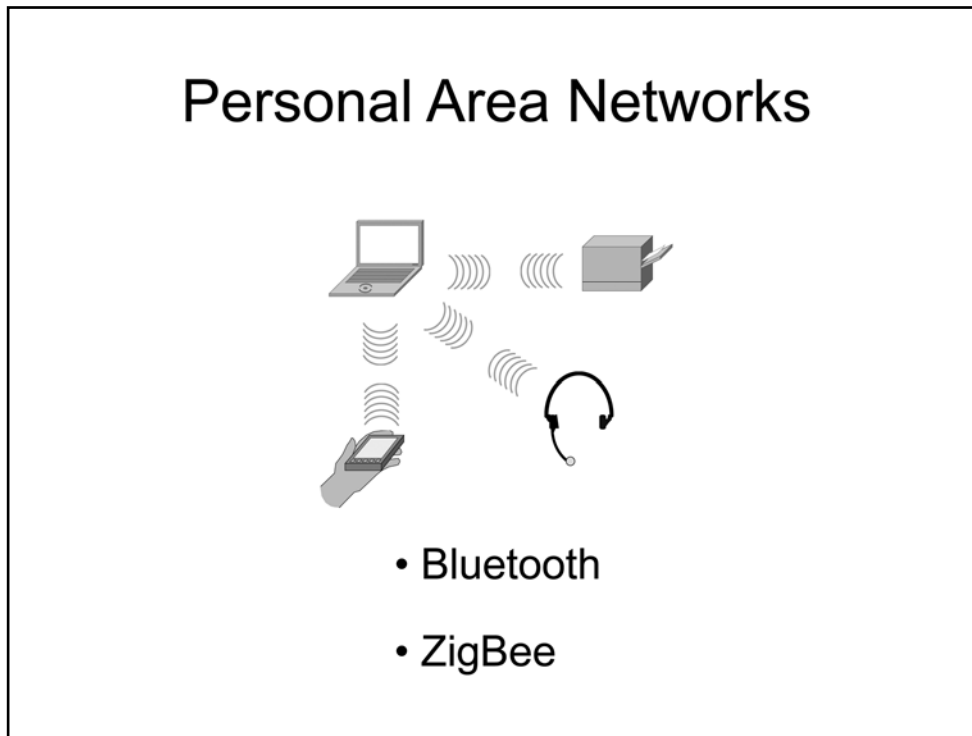
- Understand major network types.
- Analyze the differences between various network topologies.
- Identify the common devices and physical media used in networks.

Network Types

- PANs
- LANs
- MANs
- WANs

Network Types

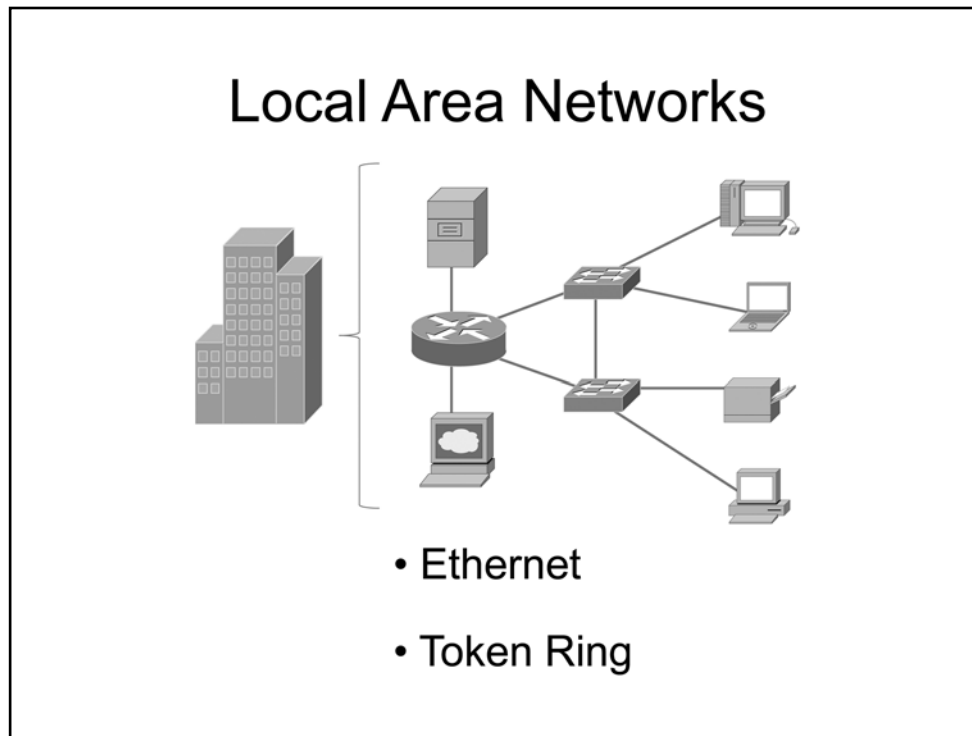
In this section, we will cover four basic network types: personal area networks (PANs), local area networks (LANs), metropolitan area networks (MANs), and wide area networks (WANs).



Personal Area Networks

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. Bluetooth and ZigBee are two technologies commonly used in a PAN setting.

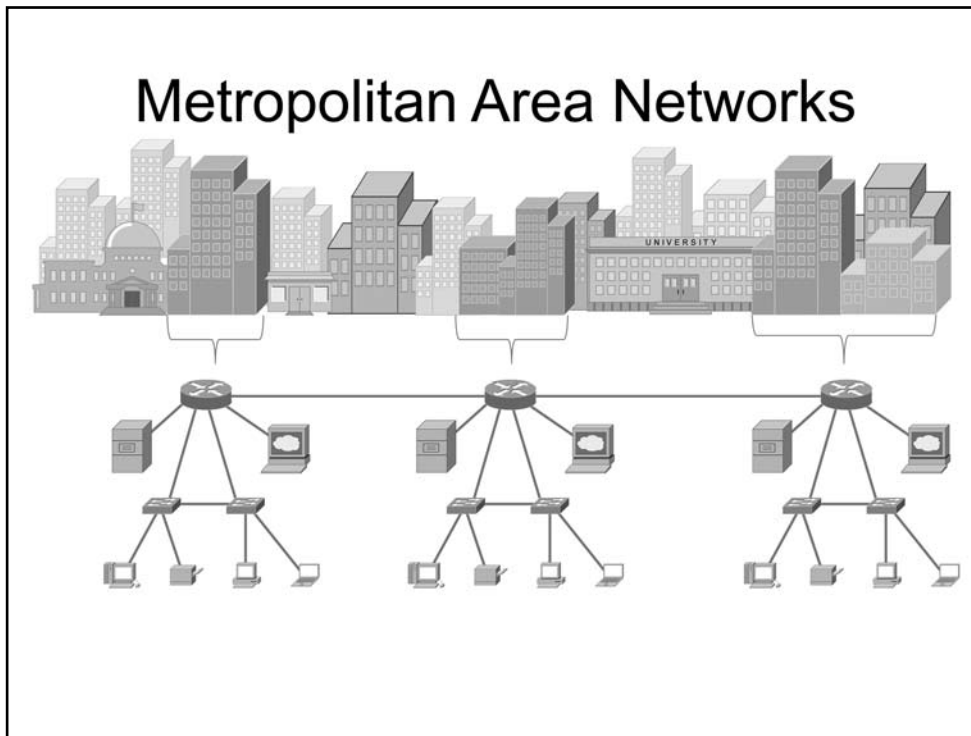
- Bluetooth is a short-range wireless technology that can be used to securely connect devices together. For example, Bluetooth can be used to transfer voice and data traffic between fixed or mobile devices. Bluetooth devices transmit data at the 2.4 to 2.485 gigahertz (GHz) frequency range. You can use Bluetooth to connect devices such as a mouse, speakers, scanners, cell phones, and printers 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

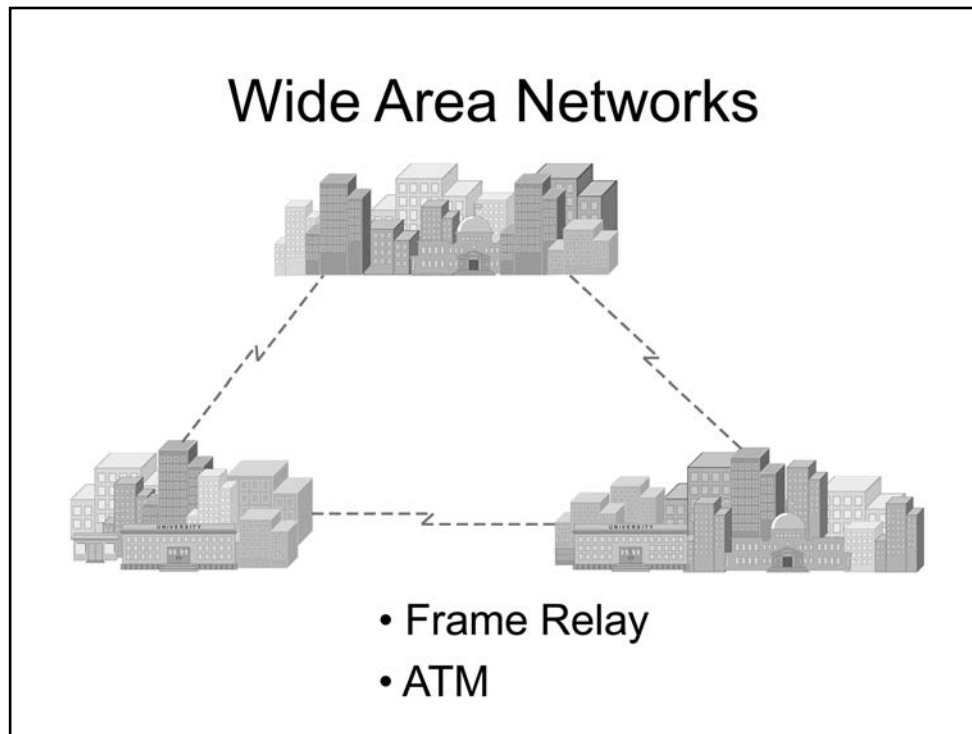
Local area networks (LANs) are typically used for communications within a single group or organization and typically within a single building or site where buildings are within close proximity of each other. Two common types of LANs include Ethernet networks and Token Ring networks.

- 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 metropolitan area network (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 wide area network (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. Frame Relay and Asynchronous Transfer Mode (ATM) are technologies used to create WANs.

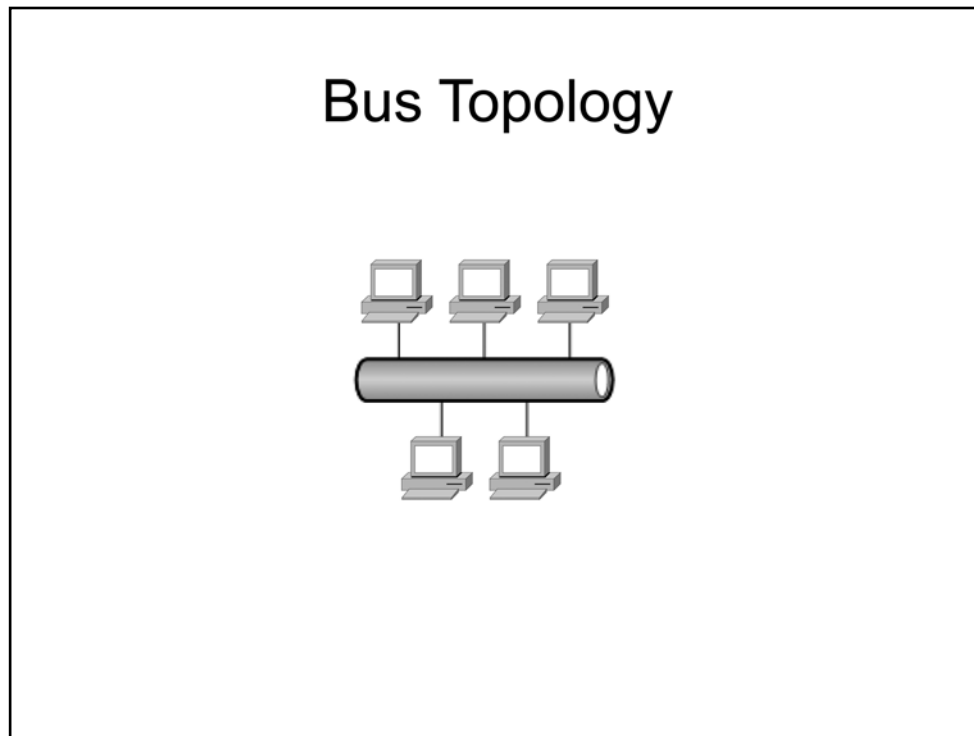
- Frame Relay is a cost-effective packet-switching technology that is suitable for data-only, medium-speed requirements. Frame Relay is a WAN encapsulation technology that can be used to implement a nonbroadcast multiaccess (NBMA) network. An NBMA network does not support broadcasts, but it does support multiple devices being connected to the network. Frame Relay uses statistical multiplexing and variable frame size to ensure network access and efficient delivery. Furthermore, Frame Relay allows multiple connections via virtual circuits through a single interface. Frame Relay links are typically purchased in full or fractional T1 configurations.
- ATM is a WAN technology that transports its payload in a series of fixed-sized 53-byte cells. ATM has the unique ability to transport different types of traffic, including IP packets, traditional circuit-switched voice, and video, while still maintaining a high quality of service for delay-sensitive traffic, such as voice and video.

Network Topologies

- Types of topologies
 - Bus
 - Ring / dual-ring
 - Star / extended star
 - Full-mesh / partial-mesh
- Physical vs. logical topologies

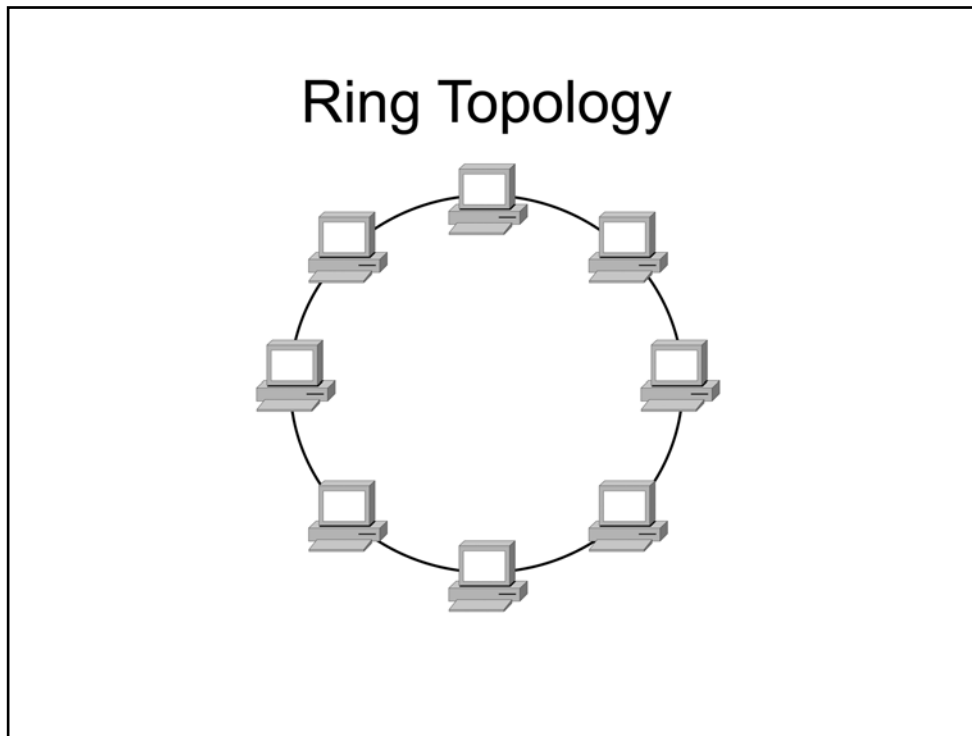
Network Topologies

In this section, we will cover some basic network topologies: bus, ring, dual-ring, star, extended star, full-mesh, and partial-mesh. Additionally, we will discuss some basic differences between physical topologies and logical topologies.



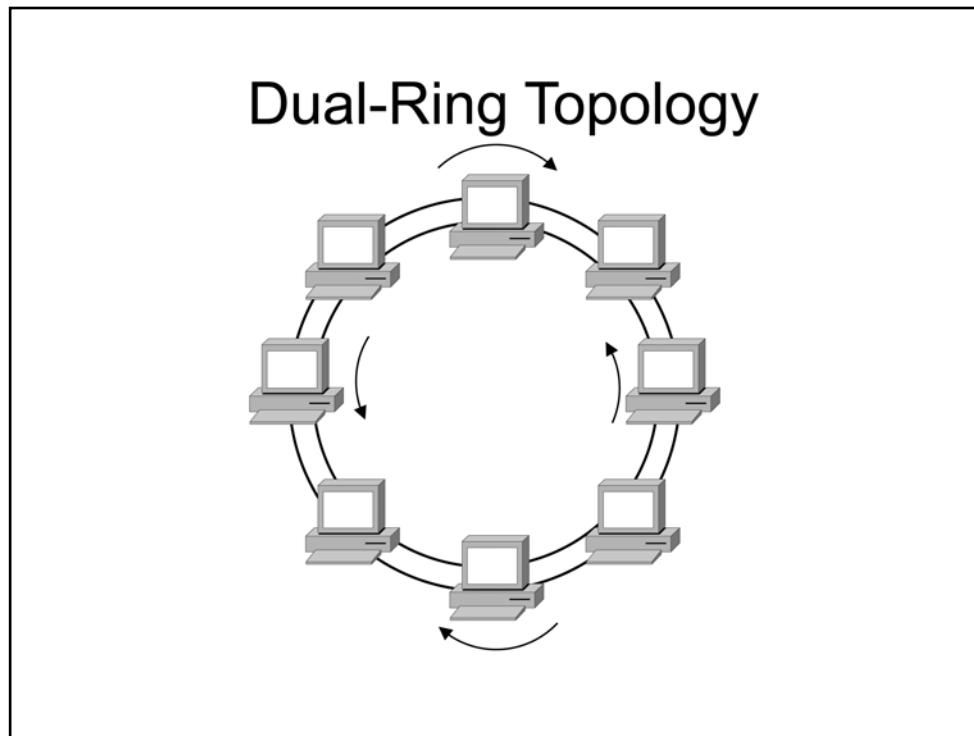
Bus Topology

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.



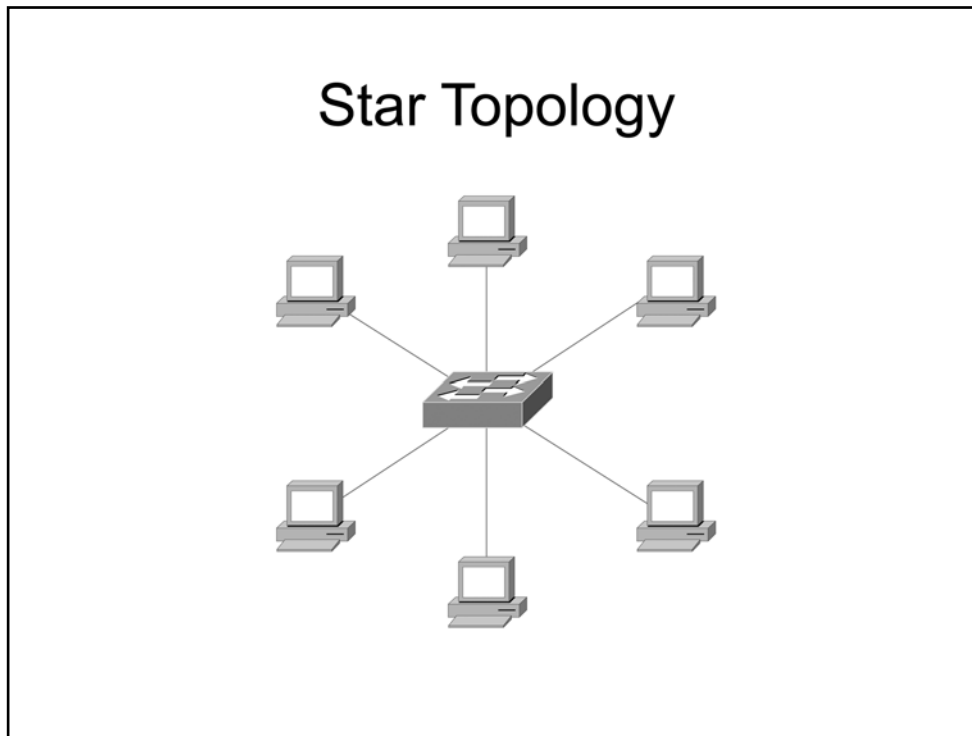
Ring Topology

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.



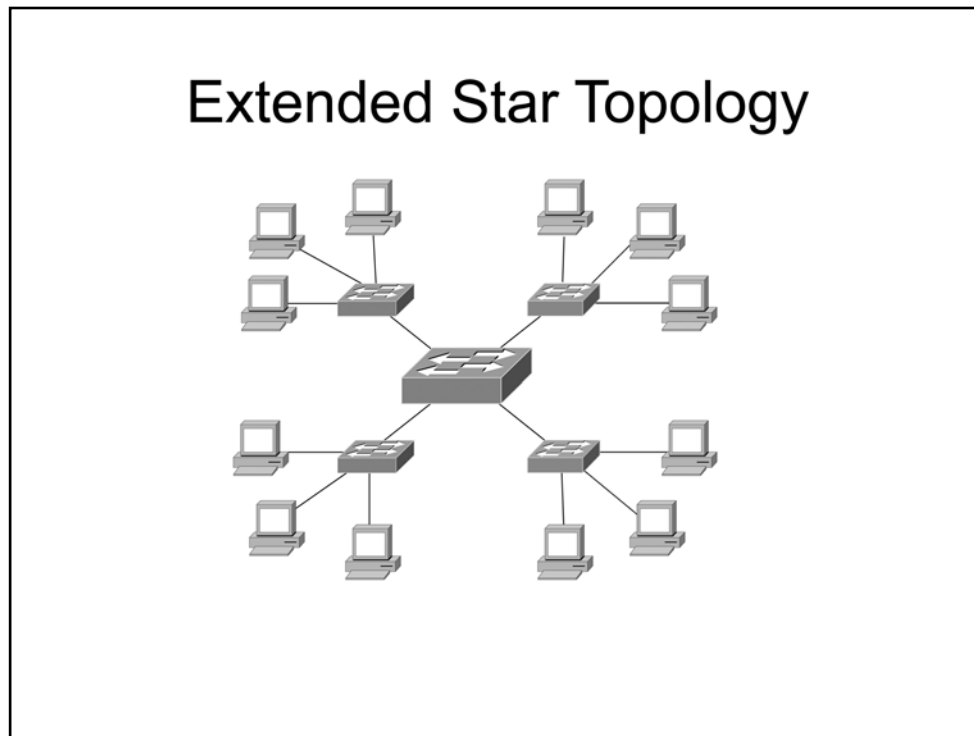
Dual-Ring Topology

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 for the entire ring.



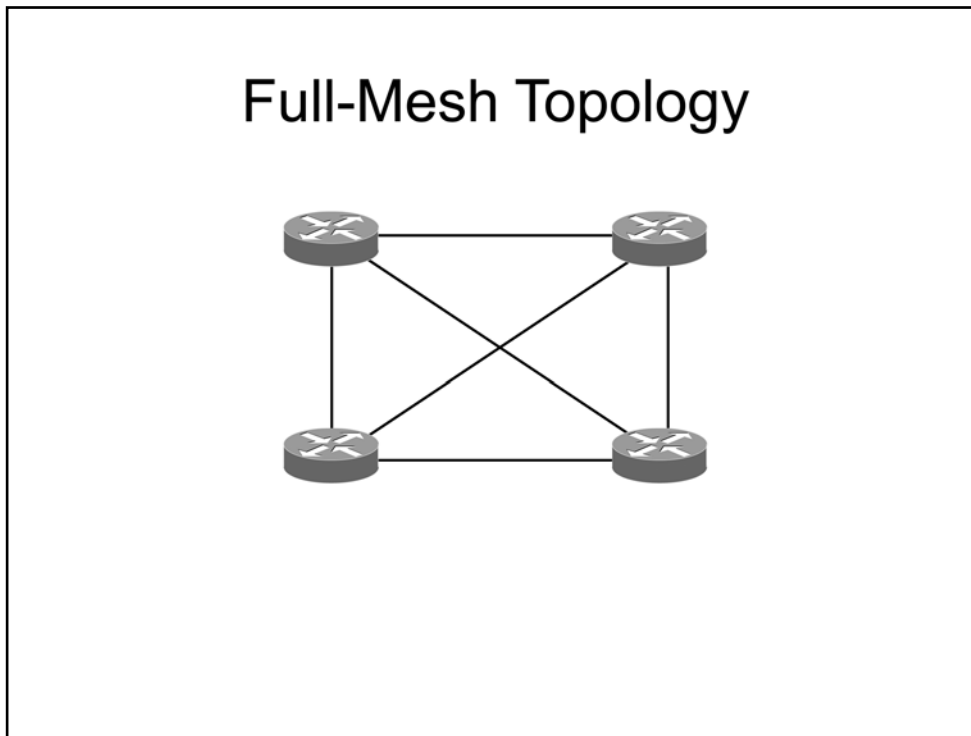
Star Topology

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.



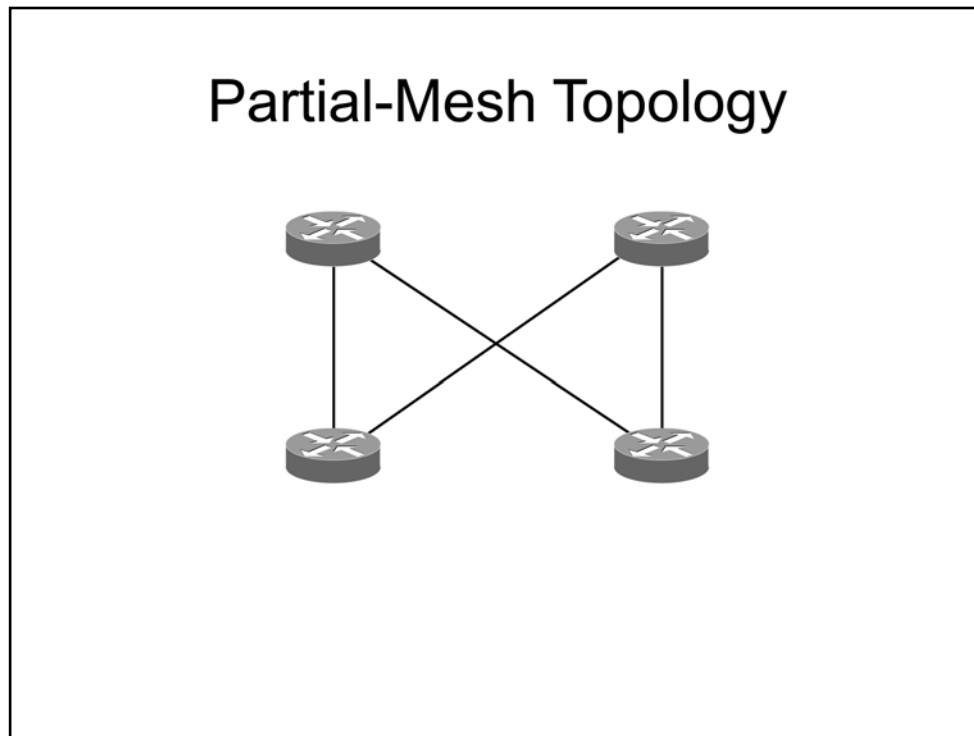
Extended Star Topology

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

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

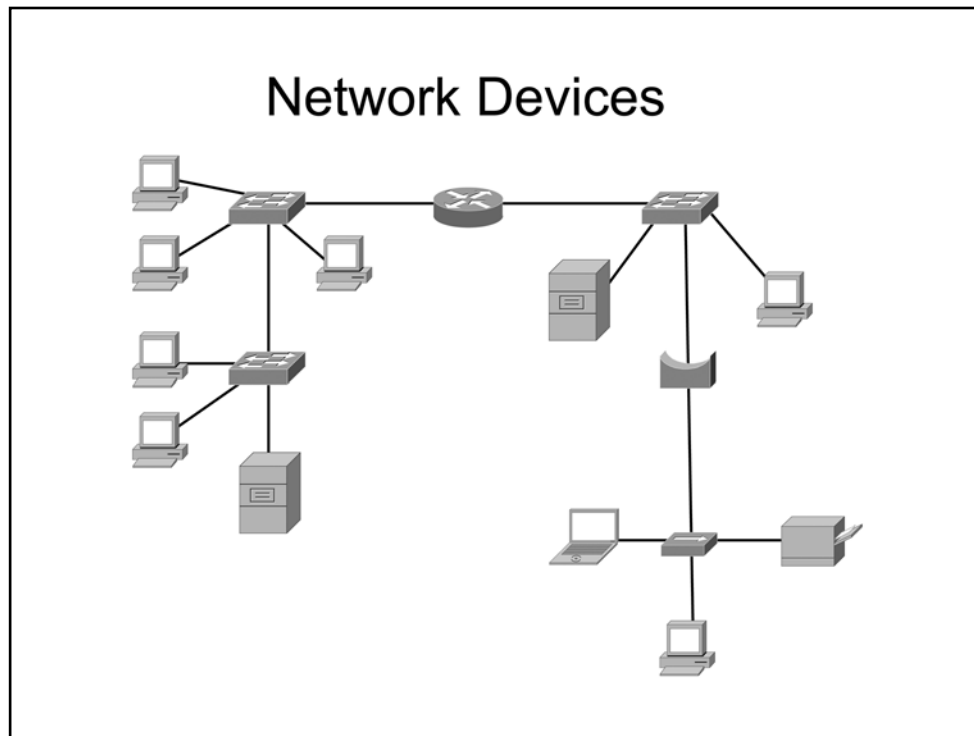
- Physical – Based on actual arrangement of devices and cables, or hardware-structured
- Logical – Based on the actual path of data flow, or protocol-structured

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

Physical vs. Logical Topologies

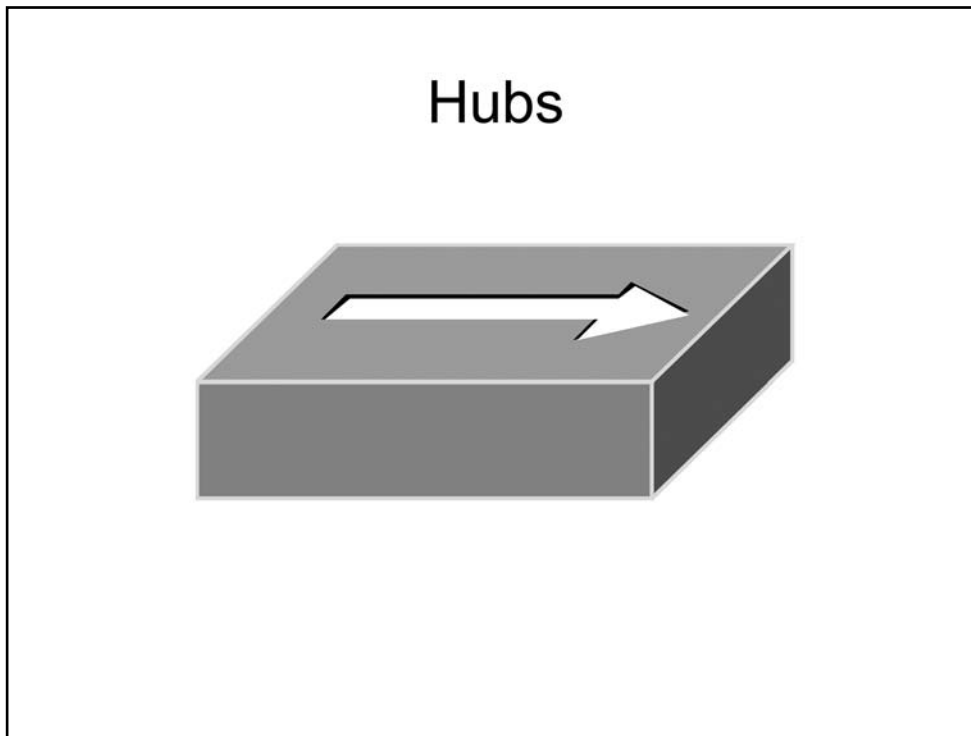
The physical topology refers to the hardware structure of the network and how the devices and cables are physically arranged. For example, a physical star topology consists of a central device, such as a hub or a switch, to which all other devices are physically connected. A physical ring topology consists 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

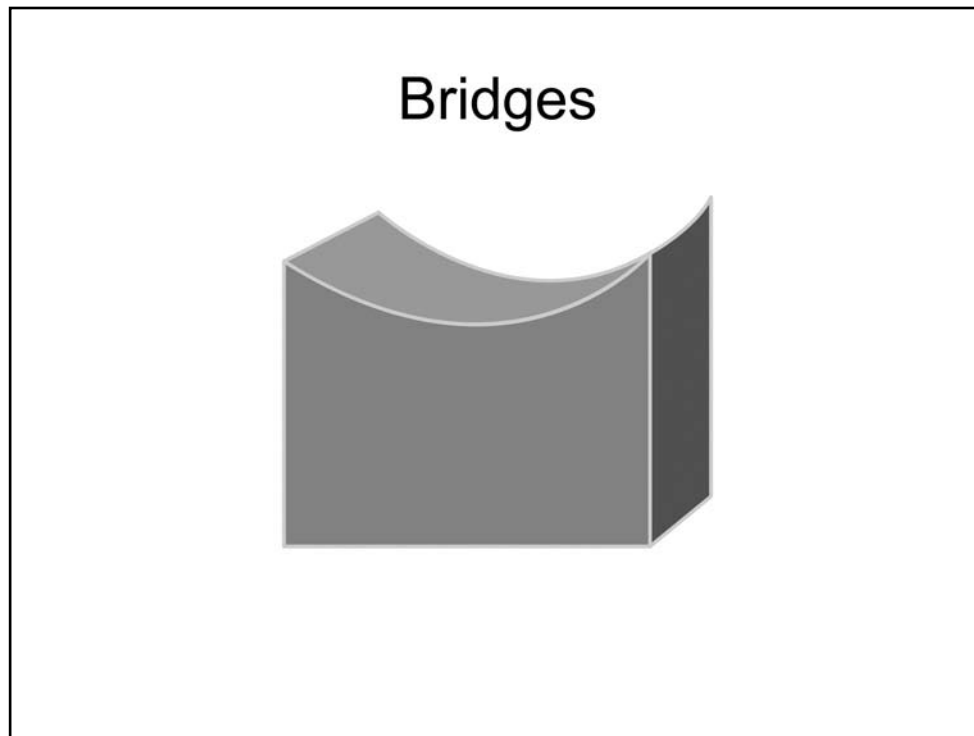
In this section, we will discuss the basic network devices: hubs, bridges, switches, routers, servers, hosts, and printers.



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.

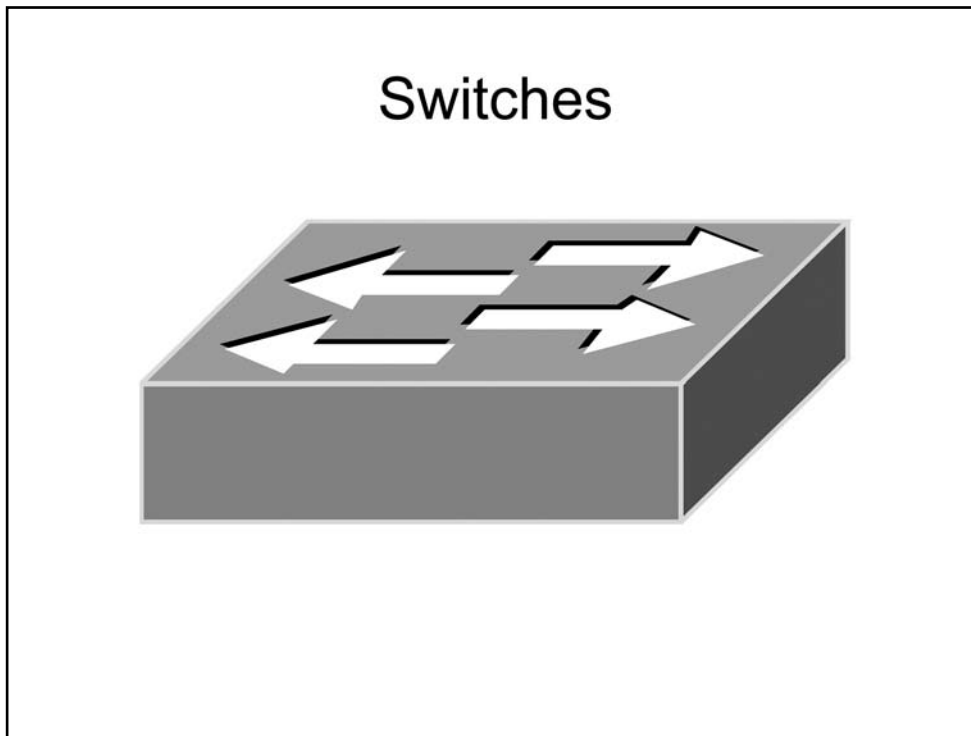
A collision domain is a network segment where collisions can occur when frames are sent among the devices on that network segment. For example, if four computers are connected to a hub, all four devices share the same bandwidth and each device can use only a portion of the total available bandwidth; 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 must rely on collision detection and retransmission to recover from errors that occur when two devices attempt to transmit a frame at the same time. 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.

Similar to switches, 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.

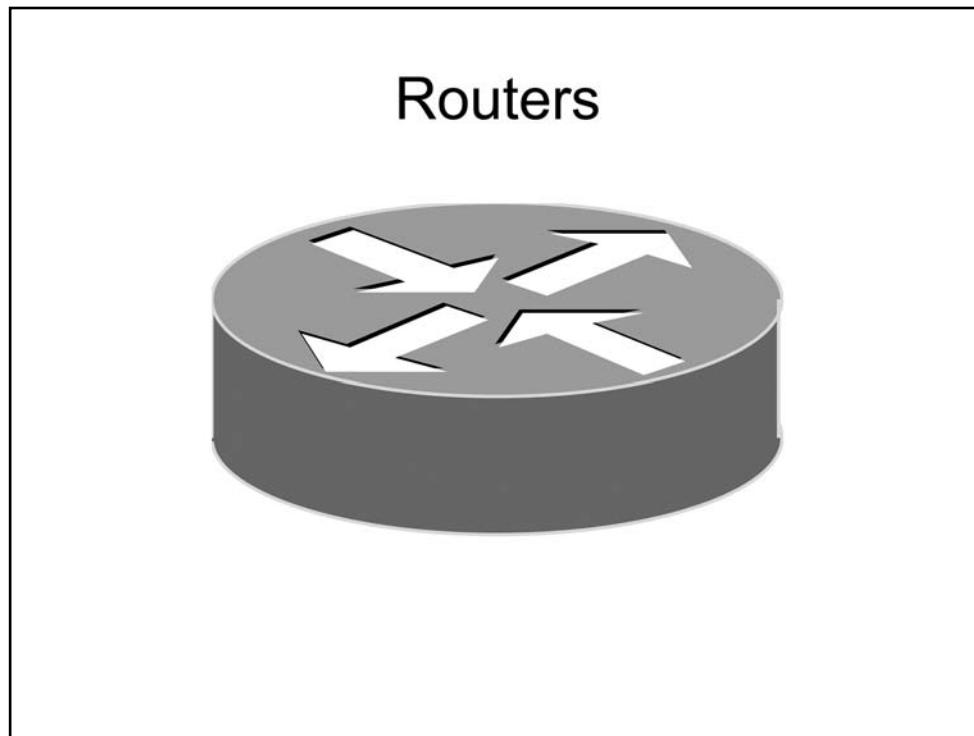


Switches

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, such as MAC addresses, to carry out their primary responsibility of switching frames. 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 address. Then the switch will check the switching table to see if the destination MAC address is listed. If so, the switch will direct the frame to the appropriate port. If the destination address is not listed, the switch will broadcast the frame out all ports except the port from which the frame was received.

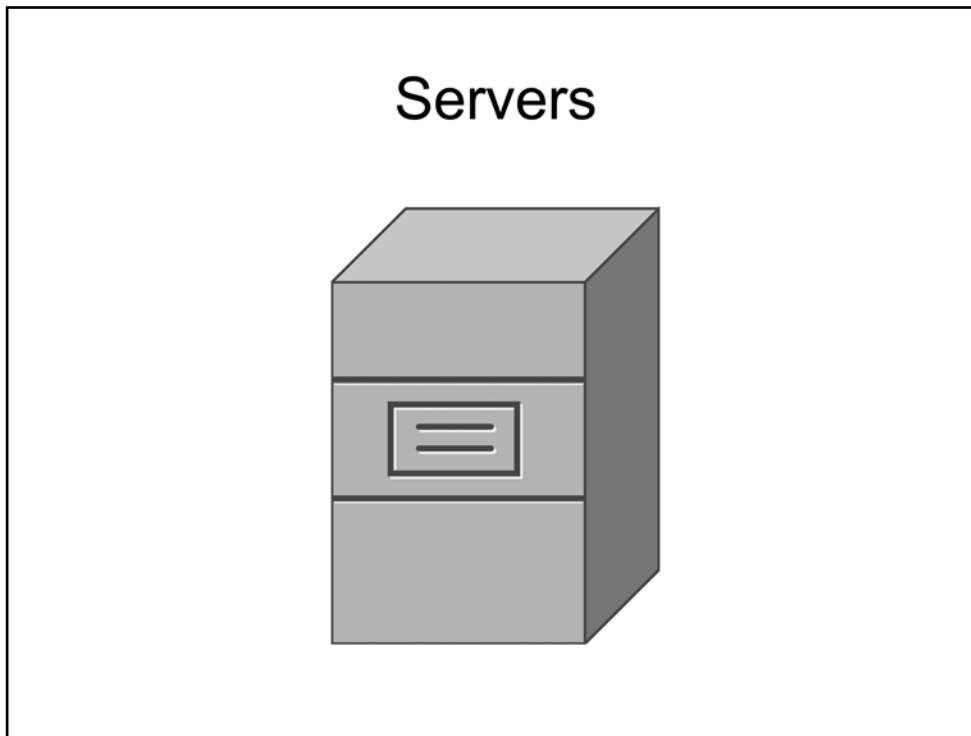
If four computers are connected to a switch, each computer will reside in its own collision domain, so all four computers can send data to the switch simultaneously. However, because switches forward broadcasts, all devices connected to a switch will reside within a single broadcast domain unless virtual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

A router makes path decisions based on logical addresses, such as IP addresses. Routers store IP address information in a routing table. 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.

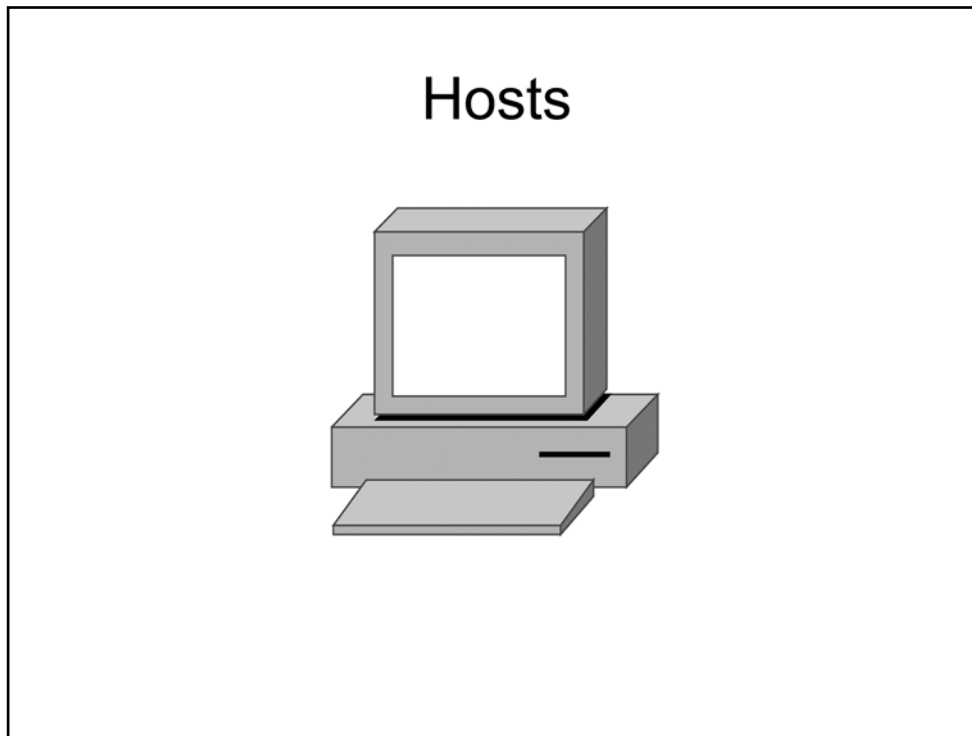


Servers

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:

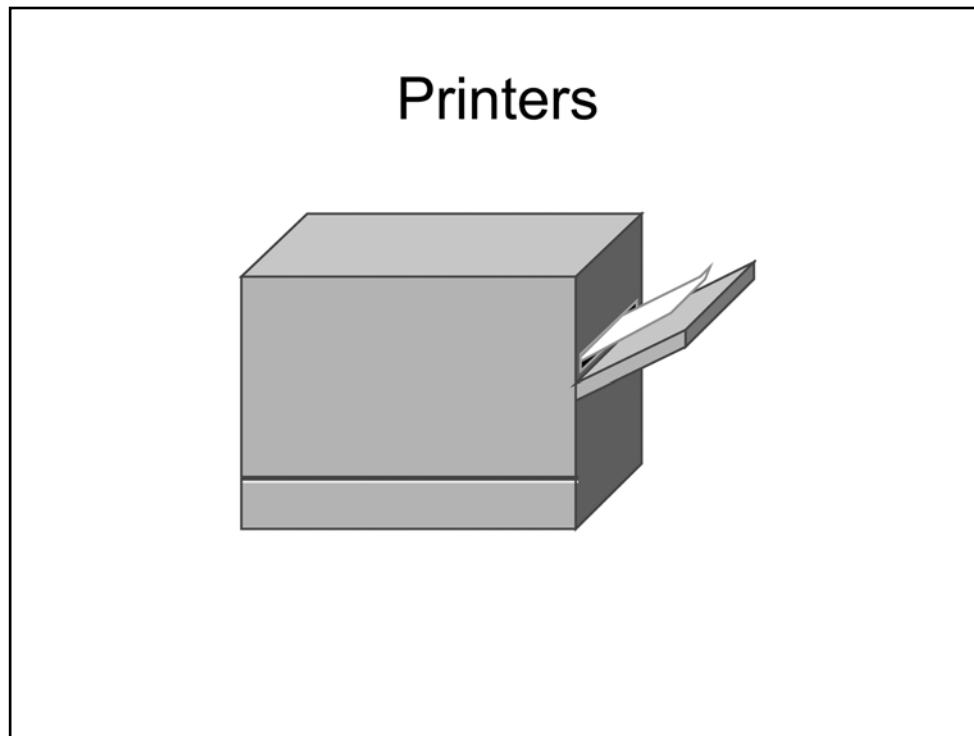
- **File servers** – You can configure a file server to allow users to access shared files or folders stored on the server. File servers are used as a central storage location of shared files and folders.
- **Domain servers** – You can configure a domain server to manage the resources that are available on the domain. For example, you can use a domain server to configure access and security policies for users on a network.
- **Print servers** – A print server is typically set up 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 Web site. Web servers typically contain content that is viewable in a Web browser, such as Internet Explorer.

- **Proxy servers** – A proxy server works 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 Web page to the computer.



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.



Printers

A printer is a type of software called a driver that is used to communicate with a print device. Local print devices are connected to a computer's parallel, universal serial bus (USB), or FireWire ports. Network printers are typically installed in central locations and are accessed by several users through the services of a print server.

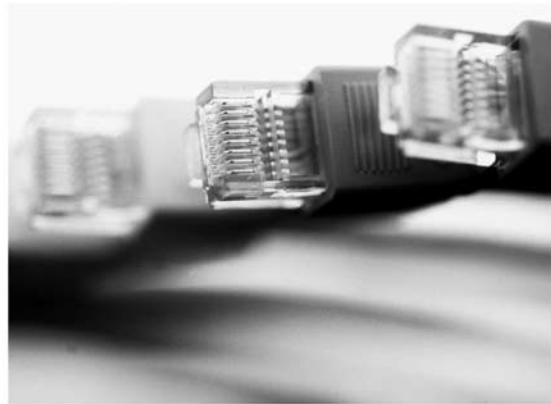
Physical Media

- Copper cables
- Fiber-optic cables
- RF

Physical Media

In this section, we will cover basic physical media used in networks: copper cables, fiber-optic cables, and radio frequency (RF).

Copper Cables



Copper Cables

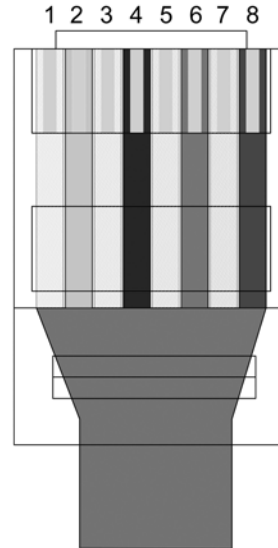
Copper is a soft metal that is an excellent conductor of both heat and electricity. Copper wires are used to transmit data as electrical signals. For example, Ethernet, Token Ring, and Copper Distributed Data Interface (CDDI) networks all use copper cabling to transmit data. Most modern Ethernet networks 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



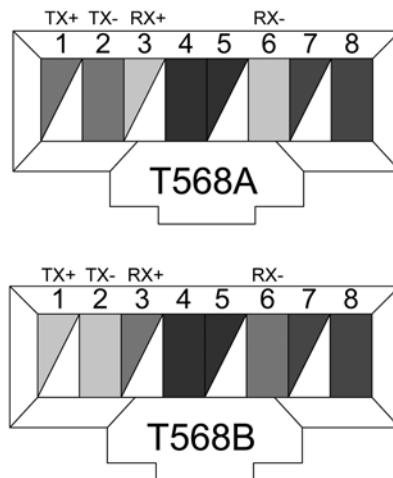
Connecting UTP with RJ-45

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



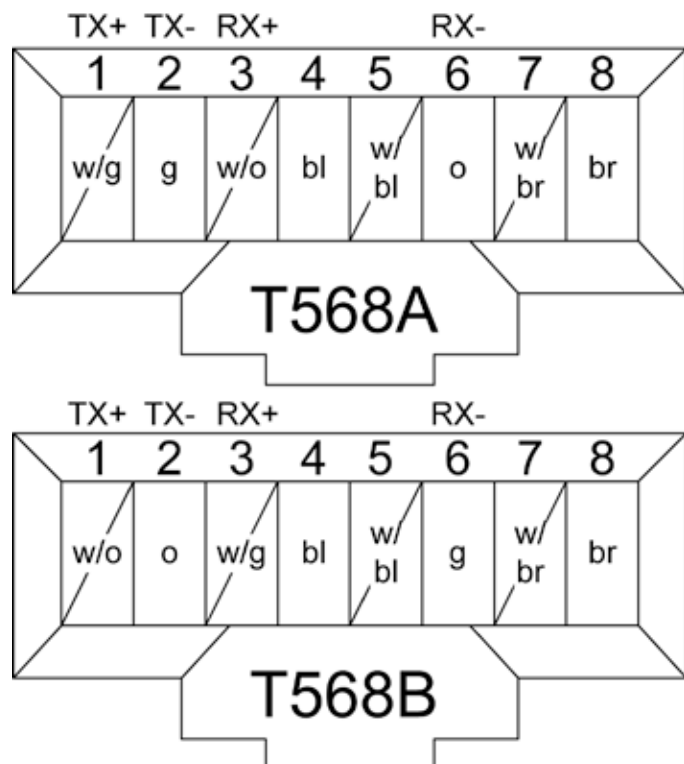
There are two different Telecommunications Industry Association (TIA) wire termination standards for an RJ-45 Ethernet connector: T568A and T568B. The T568A standard is compatible with Integrated Services Digital Network (ISDN) cabling standards. However, the T568B standard is compatible with a standard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

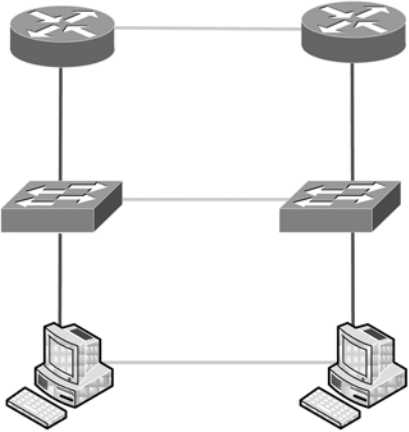
The T568B standard uses the white/orange and orange wires for Pins 1 and 2, respectively and uses the white/green and green wires for Pins 3 and 6, respectively. Therefore, the T568B standard transmits over white/orange and orange and receives over white/green and green.

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

- Crossover cables use a different pinout standard at each end
 - Connect similar devices with a crossover cable
- Straight-through cable pinouts match at each end
 - Connect dissimilar devices with a straight-through cable



The diagram shows two identical vertical stacks of network devices. Each stack consists of a router at the top, a switch in the middle, and a workstation at the bottom. A horizontal line connects the two routers, representing a crossover cable connection between similar devices. Another horizontal line connects the two switches, also representing a crossover cable connection between similar devices. A third horizontal line connects the two workstations, representing a straight-through cable connection between dissimilar devices (workstation to workstation).

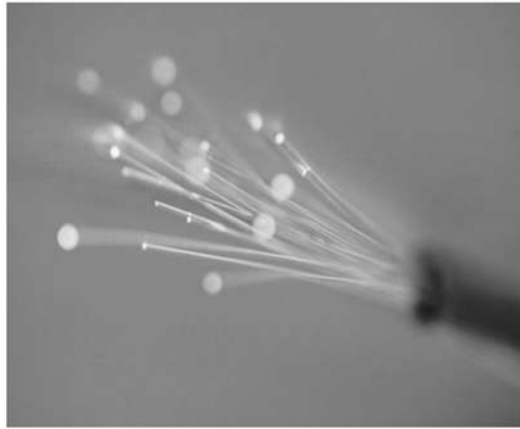
Understanding Straight-through and Crossover Cables

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 cable that uses an inverse standard at each end is called a crossover cable. A crossover cable should be used to connect two workstations, two switches, or two routers together over the same Ethernet cable. By contrast, dissimilar devices, such as a router and a switch, or a switch and a workstation, must be connected with a straight-through 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 reseal 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.

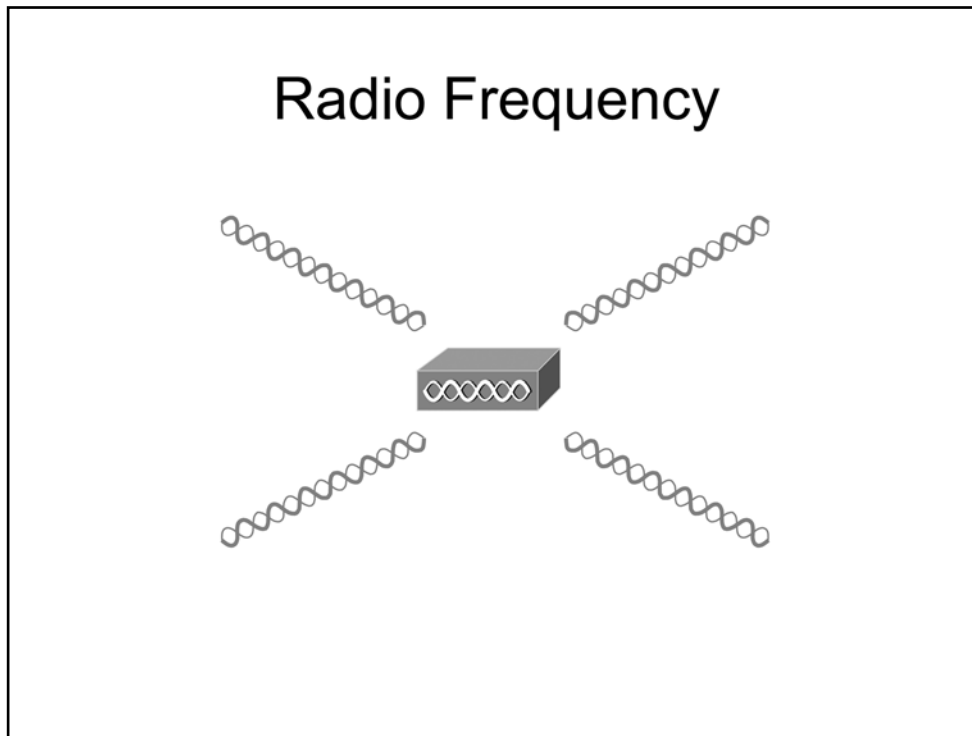
Fiber-Optic Cables



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 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. 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

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.

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

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

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.

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





b o s o n . c o m

8 7 7 . 3 3 3 . 3 9 2 6 s u p p o r t @ b o s o n . c o m

© Copyright 2012 Boson Software, LLC. All rights reserved. 3-15-12