Chapter 7: Networking Concepts

IT Essentials v6.0

Cisco | Networking Academy®
Mind Wide Open™

Chapter 7 - Sections & Objectives

- 7.1 Principles of Networking
  - Explain components and types of computer networks.
- 7.2 Networking Standards
  - Explain the purpose and characteristics of networking standards.
- 7.3 Physical Components of a Network
  - Explain the purpose of physical components of a network.
- 7.4 Basic Networking Concepts and Technologies
  - Configure network connectivity between PCs.
- 7.5 Chapter Summary

7.1 Principles of Networking

Cisco | Networking Academy®
Mind Wide Open™

Principles of Networking

- Networks are systems that are formed by links.
- People use different types of networks every day:
  - Mail delivery system
  - Telephone system
  - Public transportation system
  - Corporate computer network
  - The Internet

- Computers can be linked by networks to share data and resources.
- A network can be as simple as two computers connected by a single cable or as complex as hundreds of computers connected to devices that control the flow of information.

Computer Networks

- A computer data network is a collection of hosts connected by networking devices such as computers, printers, scanners, smartphones, and file and print servers.
- Resources shared across networks include different types of services, storage devices, and applications.
- Network devices link together using a variety of connections:
  - Copper cabling
  - Fiber-optic cabling
  - Wireless connection
- Benefits from networking include:
  - Fewer peripherals needed
  - Increased communication capabilities
  - Avoid file duplication and corruption
  - Lower cost licensing
  - Centralized administration
  - Conservation of resources

Computer Networks

- Computer Network Devices and Components
  - Host Devices – any device that sends and receives information on the network (computer, printer, etc.)
  - Intermediary Devices – exist in between host devices
  - Media – component over which the message travels from source to destination
- Can you name each device or component shown here?






Types of Networks

- **LAN (Local Area Network):** A group of interconnected computers under one administrative control group that governs the security and access control policies that are in force on the network.
- **WLAN (Wireless Local Area Network):** A group of wireless devices that connect to access points within a specified area. Access points are typically connected to the network using copper cabling.
- **PAN (Personal Area Network):** Network that connects devices, such as mice, keyboards, printers, smartphones, and tablets within the range of an individual person. PANs are most often connected with Bluetooth technology.

Types of Networks

- **MAN (Metropolitan Area Network):** Network that spans across a large campus or a city. Consisting of various buildings interconnected through wireless or fiber optic backbones.
- **WAN (Wide Area Network):** Connections of multiple smaller networks such as LANs that are in geographically separated locations. The most common example of a WAN is the Internet.

Types of Networks

- **Peer-to-Peer Networks**
  - No dedicated servers
  - Each computer decides which resources to share
  - No central administration or security
- **Client-Server Networks**
  - Server with software installed for client access
  - Resources controlled by centralized administrator
  - Secure access to confidential information
  - A centralized storage
  - Critical data should be backed up on a regular basis.

Bandwidth and Latency

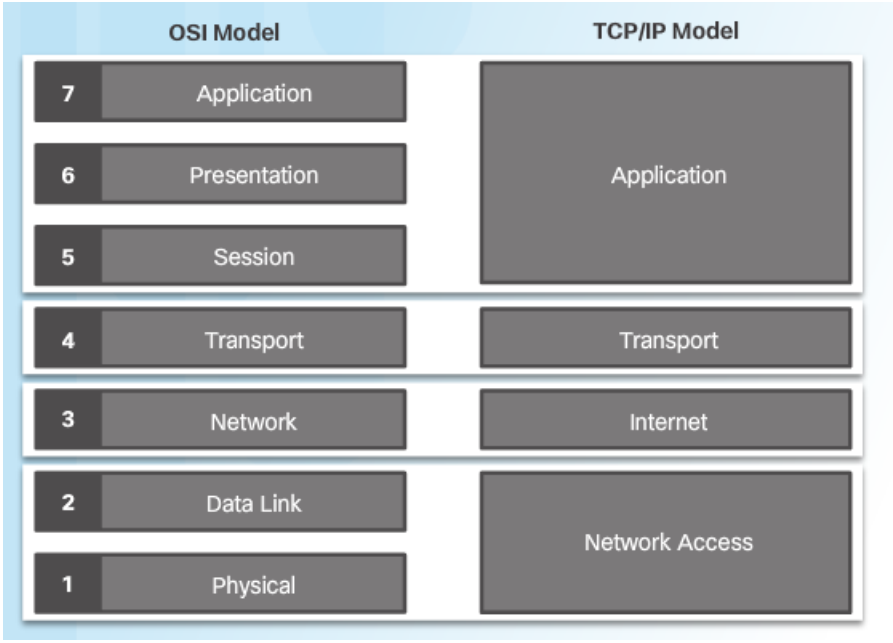
- **Bandwidth** is the amount of data that can be transmitted within a fixed time period.
- Bandwidth is measured in bits per second and is usually denoted by the following:
  - bps - bits per second
  - Kbps - kilobits per second
  - Mbps - megabits per second
  - Gbps - gigabits per second
- **Latency** is the amount of time it takes data to travel from source to destination.
- Data is transmitted in one of three modes:
  - **Simplex** (Unidirectional transmission) is a single, one-way transmission.
  - **Half-duplex** allows data to flow in one direction at a time.
  - **Full-duplex** allows data to flow in both directions at the same time.

7.2 Networking Standards

Cisco | Networking Academy®
Mind Wide Open™

Reference Models

- Organizations, such as IEEE, IETF, and ISO, develop open standards for networks so that any client running any operating system can access network resources.
- The OSI model and the TCP/IP model are both reference models used to describe the data communication process.
- As application data is passed down through the layers, protocol information is added at each level. This is known as the encapsulation process.



Standards Organizations

	Name	Type	Standards	Established
ITU-T	ITU Telecommunication Standardization Sector (formerly CCITT)	one of the three Sectors of the International Telecommunication Union	Standards covering all fields of telecommunications	Became ITU-T in 1992
IEEE	Institute of Electrical and Electronics Engineers	A non-profit, technical professional association	Standards for the computer and electronics industry	1884
ISO	International Organization for Standardization	A network of the national standards institutes of 157 countries	Promote the development of international standards agreements	1947
IAB	Internet Architecture Board	A committee; an advisory body	Oversees the technical and engineering development of the Internet	1979; first named ICCB
IEC	International Electrotechnical Commission	Global organization	Standards for all electrical, electronic, and related technologies	1906
ANSI	American National Standards Institute	Private, non-profit organization	Seeks to establish consensus among groups	1918
TIA/EIA	Telecommunications Industry Association / Electronic Industries Alliance	Trade associations	Standards for voice and data wiring for LANs	After the deregulation of the U.S. telephone industry in 1984

Ethernet Standards

- Ethernet protocols describe the rules that control how communication occurs on an Ethernet network.
- **IEEE 802.3** Ethernet standard specifies that a network implement the **Carrier Sense Multiple Access with Collision Detection (CSMA/CD)** access control method.
- In **CSMA/CD**, all end stations "listen" to the network wire for clearance to send data. When the end station detects that no other host is transmitting, the end station will attempt to send data. Unfortunately collisions might occur.
- Any device connected to a network is considered a host/node.

Ethernet Technologies

- 10BASE-T
  - The ten (10) represents a maximum bandwidth of 10 Mbps
  - The BASE represents baseband transmission
  - The T represents twisted-pair cabling.

Ethernet Standards

Ethernet Standards	Media	Transfer Rates
10BASE-T	Category 3	Transfers data at a rate of 10 Mb/s.
100BASE-TX	Category 5	At 100 Mb/s, transfer rates of 100BASE-TX are ten times that of 10BASE-T.
1000BASE-T	Category 5e, 6	The 1000BASE-T architecture supports data transfer rates of 1 Gb/s.
10GBASE-T	Category 6a, 7	The 10GBASE-T architecture supports data transfer rates of 10 Gb/s.

Wireless Ethernet Standards

- **IEEE 802.11** is the standard that specifies connectivity for wireless networks.
- **Wi-Fi** (wireless fidelity), refers to the 802.11 family
  - **802.11** (the original specification)
  - **802.11a**
  - **802.11b**
  - **802.11g**
  - **802.11n**
  - These protocols specify the frequencies, speeds, and other capabilities of the different Wi-Fi standards.

Wireless Ethernet Standards

	Bandwidth	Frequency	Range	Interoperability
802.11a	Up to 54 Mbps	5 GHz band	100 feet (30 meters)	Not interoperable with 802.11b, 802.11g, or 802.11n
802.11b	Up to 11 Mbps	2.4 GHz band	100 feet (30 meters)	Interoperable with 802.11g
802.11g	Up to 54 Mbps	2.4 GHz band	100 feet (30 meters)	Interoperable with 802.11b
802.11n	Up to 540 Mbps	2.4 GHz band	164 feet (50 meters)	Interoperable with 802.11b and 802.11g
802.15.1 Bluetooth	Up to 2 Mbps	2.4 GHz band or 5 GHz band	30 feet (10 meters)	Not interoperable with any other 802.11

Bluetooth can support up to 7 devices simultaneously to a Personal Area Network (PAN).

The TCP/IP Reference Model

- Frame of reference used to develop the Internet's protocols.
- Consists of layers that perform functions necessary to prepare data for transmission over a network.

	Description	Protocols
Application	**Provides network services to user applications**	**HTTP, HTML, Telnet, FTP, SMTP, DNS**
Transport	**Provides end-to-end management of data and divides data into segments**	**TCP, UDP**
Internet	**Provides connectivity between hosts in the network. IP addressing and routing here.**	**IP, ICMP, RIP, ARP**
Network Access	**Where Mac addressing and physical components exist**	

The OSI Model

- The OSI model is an industry standard framework that is used to divide network communications into seven layers.
- Although other models exist, most network vendors today build their products using this framework.
- A protocol stack is a system that implements protocol behavior using a series of layers.
  - Protocol stacks can be implemented either in hardware or software, or in a combination of both.
  - Typically, only the lower layers are implemented in hardware, and the higher layers are implemented in software.

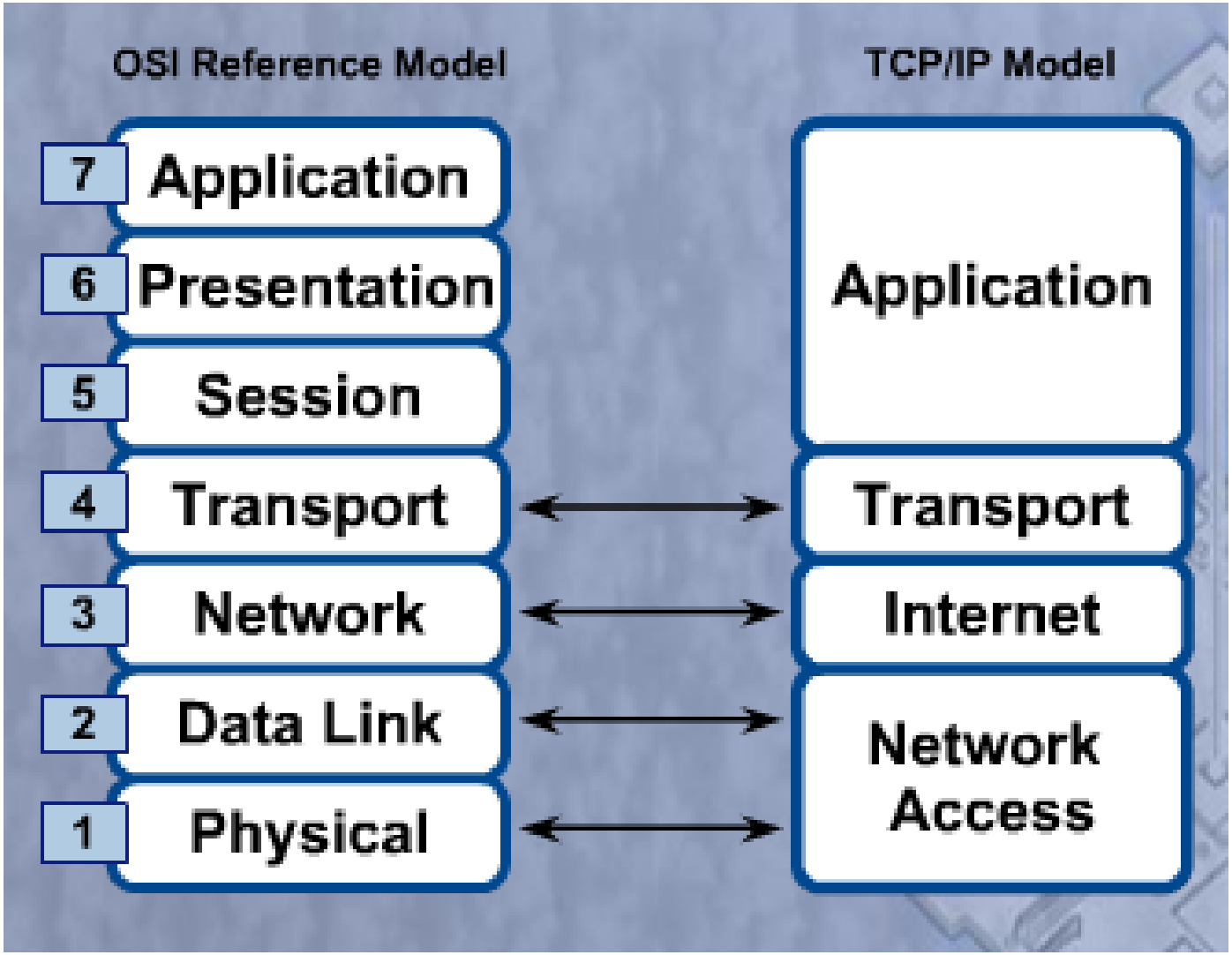
The OSI Model

	Layer	Description
Application	7	Responsible for network services to applications
Presentation	6	Transforms data formats to provide a standard interface for the Application layer
Session	5	Establishes, manages and terminates the connections between the local and remote application
Transport	4	Provides reliable transport and flow control across a network
Network	3	Responsible for logical addressing and the domain of routing
Data Link	2	Provides physical addressing and media access procedures
Physical	1	Defines all the electrical and physical specifications for devices

Remember the OSI layers with this mnemonic:

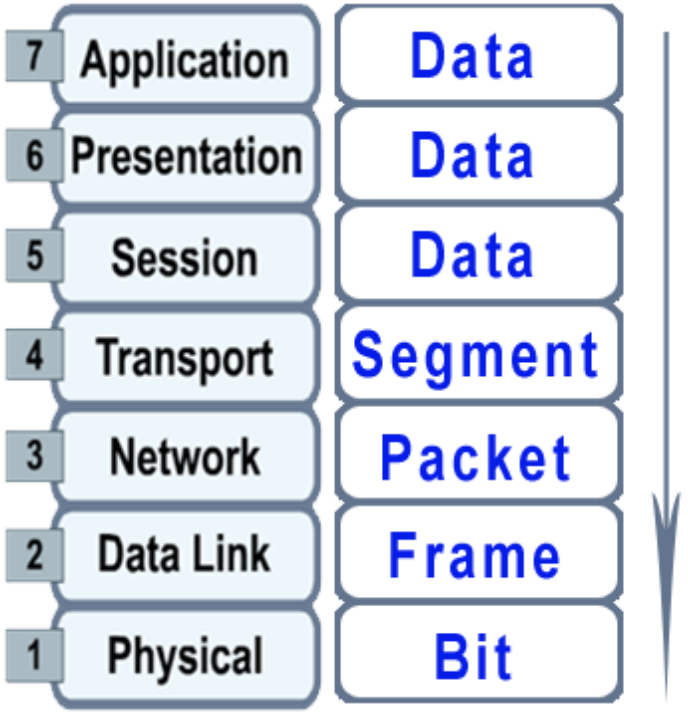
"Please Do Not Throw Sausage Pizza Away"

Compare OSI and TCP/IP Models



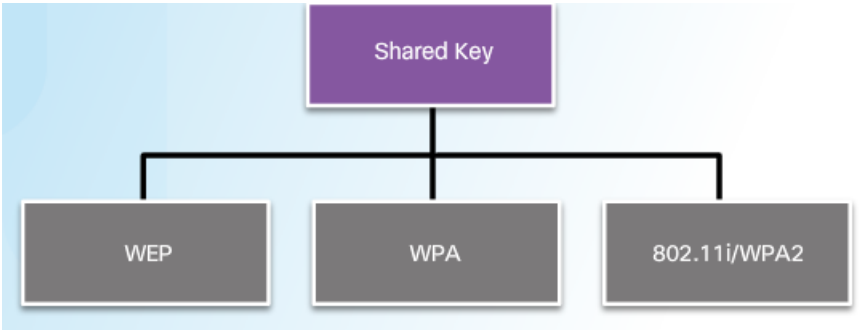
Encapsulation

- Process of placing one message format into another format so that the message can be delivered
- Receives headers, footers, and other information
- Five step process:
  - Data
  - Segments
  - Packets
  - Frames
  - Bits



Wired and Wireless Standards

- When Ethernet operates in half-duplex, the IEEE 802.3 standard specifies that a network implement the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) access control method.
- The 802.3 standard also specifies cable types for Ethernet including:
  - 10Base-T
  - 100Base-TX
  - 1000Base-T
  - 10GBase-T
- The IEEE 802.11 standard specifies that wireless LANs use Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA).
- WLAN standards include 802.11a, 802.11b, 802.11g, 802.11n, and 802.11ac
- When configuring an 802.11 WLAN, use the strongest encryption available.
- Since 2006, the strongest encryption has been WPA2.



7.3 Physical Components of a Network

Cisco | Networking Academy®
Mind Wide Open™

Physical Network Components

- Network devices:
  - Computers
  - Hubs
  - Switches
  - Routers
  - Wireless access points
- Network media:
  - Twisted-pair copper cabling
  - Fiber-optic cabling
  - Radio waves

Physical Network Components

A **Modem** is an electronic device that connects to the Internet via an ISP.

- A modem converts digital data to analog signals for transmission over a phone line.
- Internal modems plug into an expansion slot on the motherboard.
- External modems connect to a computer through the serial and USB ports.

Network Devices

- **Hub**
  - Extend the range of a signal by receiving then regenerating it and sending it out all other ports.
  - Allow for **collisions** on the network segment and are often not a good solution.
  - Also called **concentrators** because they serve as a central connection point for a LAN.
- **Bridges and Switches**
  - Makes forwarding decisions based on the destination MAC address that is contained in the frame.
  - A **bridge** has the intelligence to determine if an incoming frame is to be sent to a different segment, or dropped. A bridge has two ports.
  - A **switch** (multiport bridge) has several ports and refers to a table of MAC addresses to determine which port to use to forward the frame.
- **Power over Ethernet (PoE)**
  - PoE switch transfers small amounts of DC current over Ethernet cable, along with data, to power PoE devices such as Wi-Fi access points.

Network Devices (Continued)

- **Routers**
  - Devices that connect entire networks to each other.
  - They use IP addresses to forward packets to other networks.
  - A router can be a computer with special network software installed or can be a device built by network equipment manufacturers.
  - Routers contain tables of IP addresses along with optimal routes to other networks.

- **Wireless Access Points (WAP)**
  - Provide network access to wireless devices such as laptops and PDAs.
  - Use radio waves to communicate with radios in computers, PDAs, and other wireless access points.
  - Have limited range of coverage.

Network Devices (Continued)

- **Multipurpose Devices**
  - Perform more than one function.
  - More convenient to purchase and configure just one device.
  - Combines the functions of a switch, a router and a wireless access point into one device.
  - The Linksys E2500 is an example of a multipurpose device.
  - Integrated Service Router
    - Router
    - Switch
    - Wireless Access Point

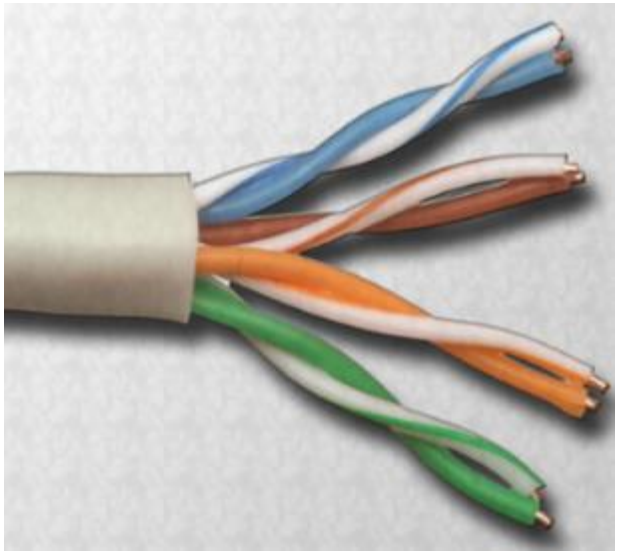
Coaxial Cable

- A copper-cored network cable surrounded by a heavy shielding.

- Types of coaxial cable:
  - **Thicknet** or **10Base5** - Coaxial cable that was used in networks and operated at 10 megabits per second with a maximum length of 500 m
  - **Thinnet** or **10Base2** - Coaxial cable that was used in networks and operated at 10 megabits per second with a maximum length of 185 m
  - **RG-59** - Most commonly used for cable television in the US
  - **RG-6** - Higher quality cable than RG-59 with more bandwidth and less susceptibility to interference

Twisted-Pair Cabling

- A pair of twisted wires forms a circuit that transmits data.
- The twisted wires provide protection against crosstalk (electrical noise) because of the cancellation effect.
- Pairs of copper wires are encased in color-coded plastic insulation and twisted together.



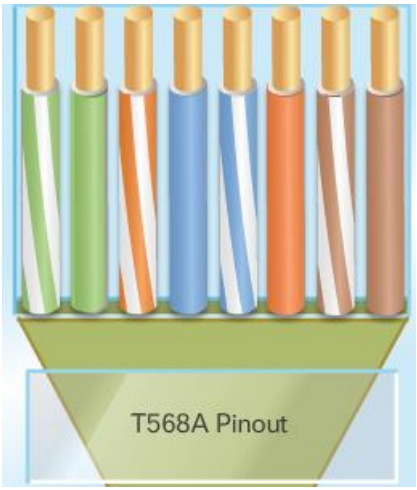
- An outer jacket of poly-vinyl chloride (PVC) protects the bundles of twisted pairs.
- There are two types of this cable:
  - **Unshielded twisted-pair (UTP)**

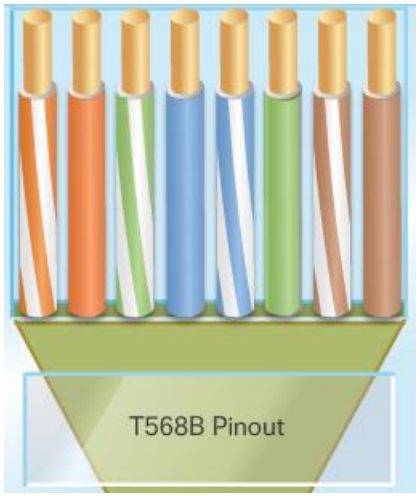
    (Cat 3, Cat 5, 5e ,Cat 6 and Cat 7)
  - **Shielded twisted-pair (STP)**

    Reduces RFI and EMI

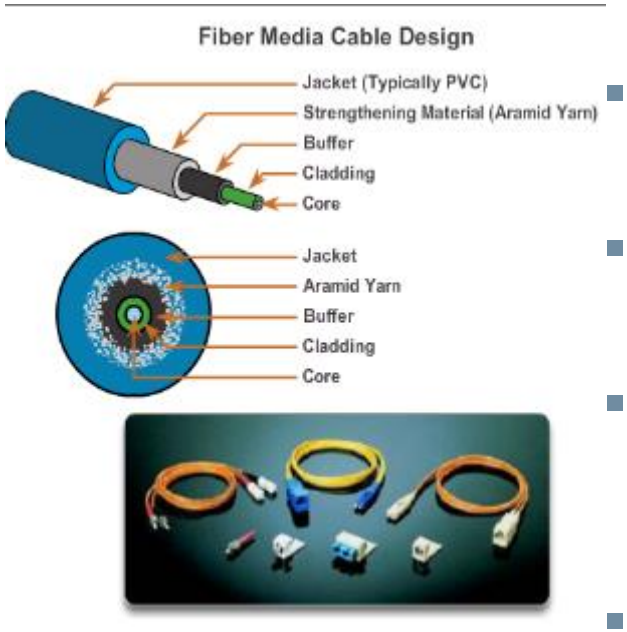
Cables and Connectors

- Twisted-pair is the most popular type of cabling used in LANs today.
- There are two different twisted-pair wiring schemes: called T568A and T568B.
  - The green and orange wires change termination order.
  - Each wiring scheme defines the pinout, or order of wire connections, on the end of the cable.
- Two types of cables can be created:
  - A **straight-through** cable is the most common cable type. The wiring scheme is the same on both sides. Connect unlike devices.
  - A **crossover** cable uses both wiring schemes. T568A on one end of the cable and T568B on the other end of the same cable. Connect like devices.



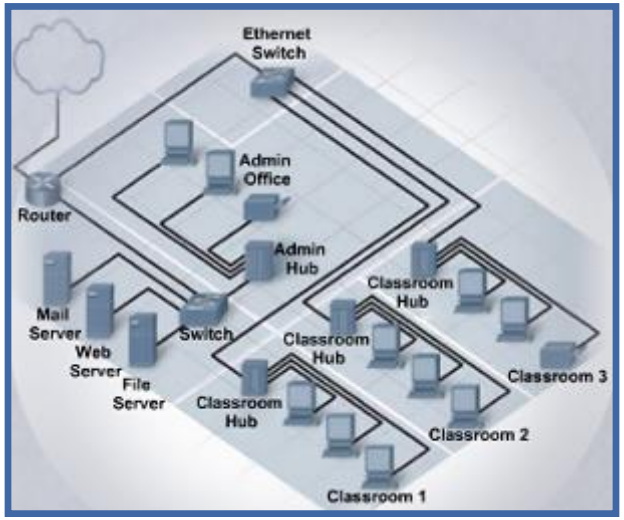


Fiber-Optic Cable

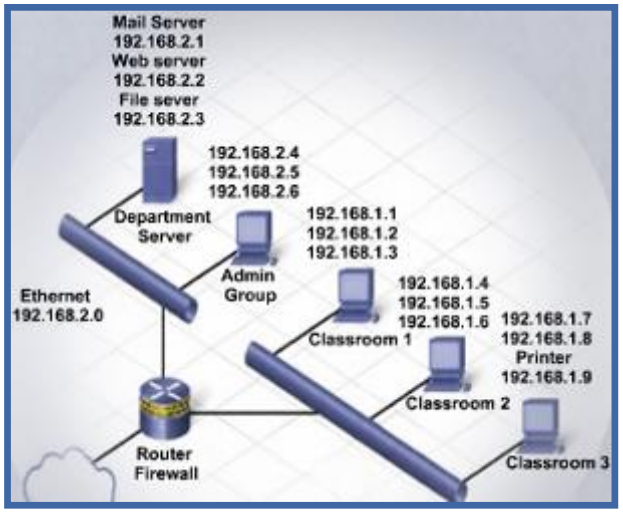


- A glass or plastic strand that transmits information using light and is made up of one or more optical fibers enclosed together in a sheath or jacket.
- Not affected by electromagnetic or radio frequency interference.
- Signals are clearer, can go farther, and have greater bandwidth than with copper cable.
- Usually more expensive than copper cabling and the connectors are more costly and harder to assemble.
- Two types of glass fiber-optic cable:
  - **Single-mode fiber** (SMF) - Uses lasers to send a single ray of light that can travel hundreds of kilometers.
  - **Multimode fiber** (MMF) - Uses LEDs to send multiple light signals that can travel up to 550 meters.

Two Types of LAN Topologies



Physical topology is the physical layout of the components on the network.



Logical topology determines how the hosts access the medium to communicate across the network.

Logical Topologies

- The two most common types of logical topologies are **broadcast and token passing**.

  - **Broadcast topology**- A host broadcasts a message to all hosts on the same network segment. There is no order that hosts must follow to transmit data. Messages are sent on a First In, First Out (FIFO). Ethernet is based on this topology.

  - **Token passing** controls network access by passing an electronic token sequentially to each host. When a host receives the token, it can send data on the network. If the host has no data to send, it passes the token to the next host and the process repeats itself.

LAN Physical Topologies

- A physical topology defines the way in which computers, printers, and other devices are connected to a network.
- **Bus**
  - Each computer connects to a common cable The ends of the cable have a **terminator** installed to prevent signal reflections and network errors.
  - Only one computer can transmit data at a time or frames will collide and be destroyed.
- **Ring**
  - Hosts are connected in a physical ring or circle.
  - A special frame, a **token**, travels around the ring, stopping at each host to allow data transmission.
  - There are two types of ring topologies:
    - Single-ring and Dual-ring

LAN Physical Topologies (Continued)

- **Star**
  - Has a central connection point : a hub, switch, or router.
  - Easy to troubleshoot, since each host is connected to the central device with its own wire.
- **Hierarchical or Extended Star Topology**
  - A star network with an additional networking device connected to the main networking device to increase the size of the network.
  - Used for larger networks.
- **Mesh Topology**
  - Connects all devices to each other.
  - Used in WANs that interconnect LANs. The Internet is an example of a mesh topology.
- **Hybrid**
  - A hybrid topology is a combination of two or more basic network topologies, such as a star-bus, or star-ring topology. The advantage of a hybrid topology is that it can be implemented for a number of different network environments.

7.4 Basic Networking Concepts and Technologies

Cisco | Networking Academy®
Mind Wide Open™

Networked Equipment Addressing

- The MAC address is hard coded onto the network interface card (NIC) by the manufacturer.
  - The MAC address is 48 bits represented in hexadecimal
  - OSI-Data Link Layer; TCP/IP-Network Access Layer

Address Format	Description
00-50-56-BE-D7-87	Two hexadecimal digits separated by hyphens
00:50:56:BE:D7:87	Two hexadecimal digits separated by colons
0050.56BE.D787	Four hexadecimal digits separated by periods

- The Internet Protocol (IP) address is assigned by network administrators based on the location within the network.
- Two versions of Internet Protocol (IP) Addressing:
  - IPv4: 32-bit represented in dotted-decimal
  - IPv6: 128-bit represented in hexadecimal

IPv4 Address Format

32 bits in dotted decimal notation

192.168.200.8

IPv6 Address Format

128 bits in preferred format

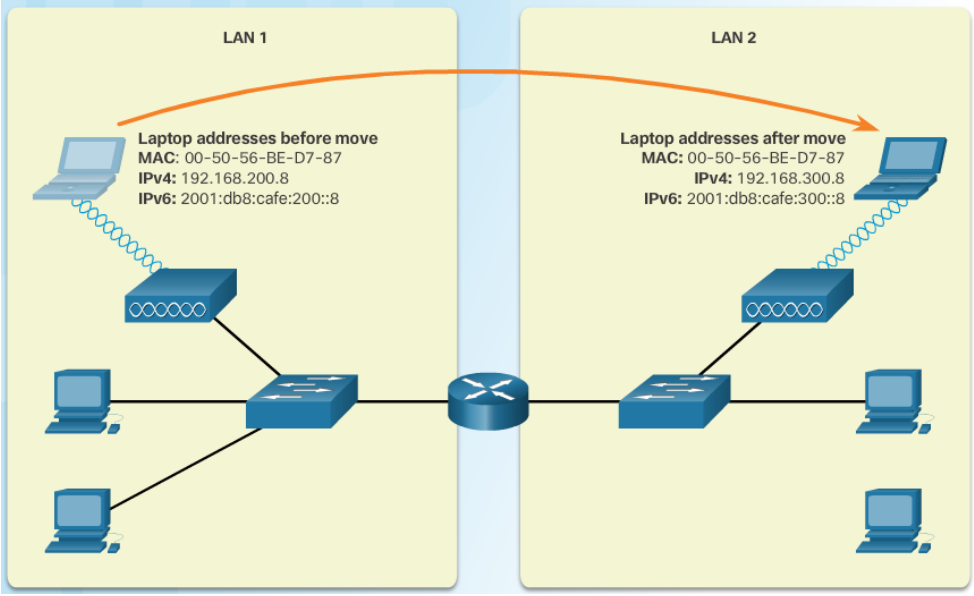
2001:0DB8:CAFE:0200:0000:0000:0000:0008

128 bits in compressed format

2001:DB8:CAFE:200::8

Networked Equipment Addressing

- Host devices need both addresses to communicate on the network.
  - MAC addresses do not change when devices move from one network to another.
  - IP addresses change because they are based on where the device is in the network.



IP Addressing - IPV4

- An IP address is a unique number that is used to identify a network device and is represented as a 32-bit binary number, divided into four **octets** (groups of eight bits):
  - Example: 10111110.01100100.00000101.00110110
- An IP address is also represented in a **dotted decimal** format.
  - Example: 190.100.5.54
- When a host is configured with an IP address, it is entered as a dotted decimal number, such as 192.168.1.5. This IP address must be unique on a network to ensure data can be sent/received.
- IP Classes
  - Class A: Large networks, implemented by large companies and some countries (16,777,214 usable)
  - Class B: Medium-sized networks, implemented by universities (65,534 usable)
  - Class C: Small networks, implemented by ISP for customer subscriptions (254 usable)
  - Class D: Special use for multicasting
  - Class E: Used for experimental testing

IP Addressing – IPV4

- **Private Addresses** - IETF reserved some Internet address space for private networks.
- Private networks have no connection to public networks.
- Private network addresses are not routed across the Internet.
  - **Class A** - 10.0.0.0 to 10.255.255.255
  - **Class B** - 172.16.0.0 to 172.31.255.255
  - **Class C** - 192.168.0.0 to 192.168.255.255

- **Automatic Private IP Addressing (APIPA)**
  - Feature of modern operating systems
  - Automatically self-configures an IP address and subnet mask when a DHCP server isn't available
  - IP address range: 169.254.0.1 through 169.254.255.254
  - Configures a default class B subnet mask of 255.255.0.0

Subnet Masks

- The subnet mask is used to indicate the network and the host portion of an IP address.
- The default subnet masks for three classes of IP addresses.
  - **255.0.0.0** - Class A, which indicates that the first octet of the IPv4 address is the network portion.
  - **255.255.0.0** - Class B, which indicates that the first two octets of the IPv4 address is the network portion.
  - **255.255.255.0** - Class C, which indicates that the first three octets of the IPv4 address is the network portion.

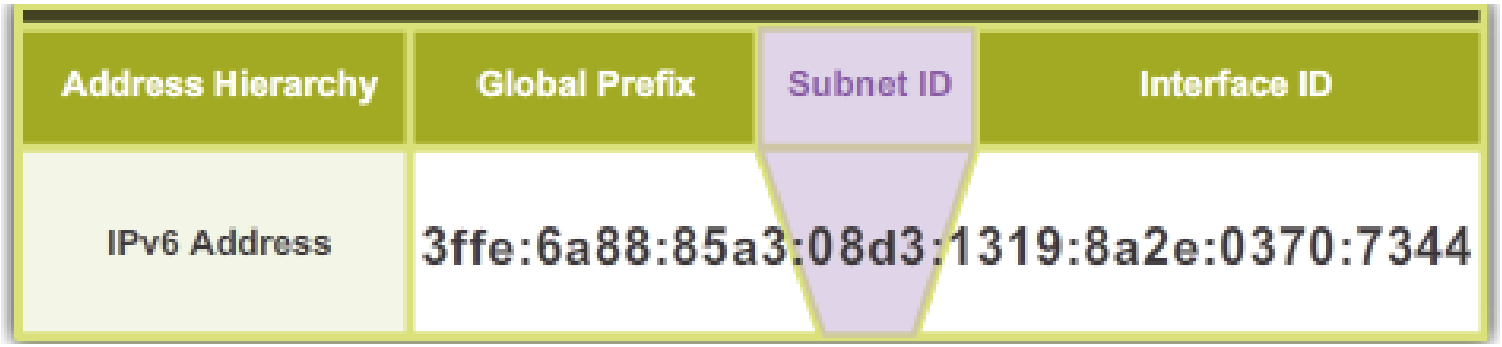
Networked Equipment Addressing

- An IPv4 address is composed of two parts. The first part identifies the network. The second part identifies a host on that network.
- Computers and routers use the subnet mask to calculate the network portion of the destination IPv4 address.
- A one bit in the subnet mask means that bit is part of the network portion. So the first 24 bits of the 192.168.200.8 address are network bits. The last 8 bits are host bits.

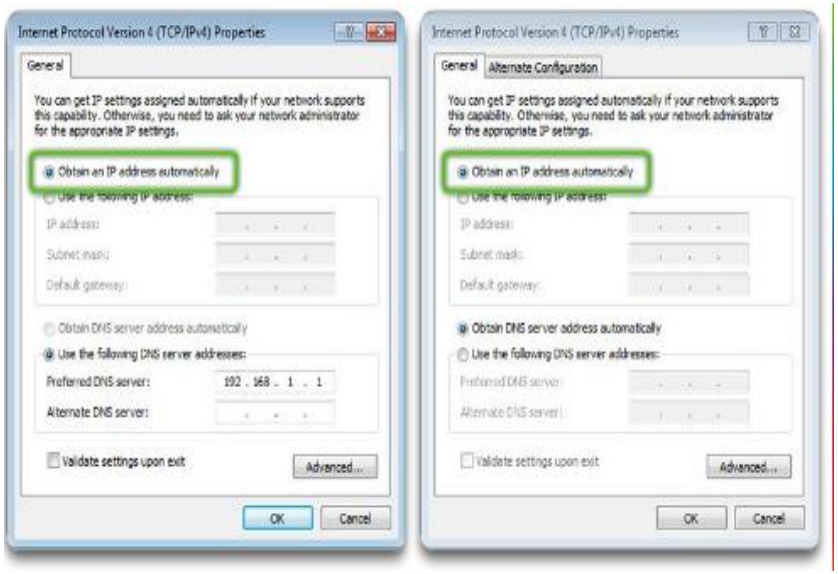
	Network Portion		Host Portion
192.168.200.8	11000000.10101000.11001000	.	00001000
255.255.255.0	11111111.11111111.11111111	.	00000000
192.168.200.0	11000000.10101000.11001000	.	00000000

IP Addressing – IPV6

- IPv6 address - 128 bits or 32 hexadecimal values.
  - 32 hexadecimal values are further subdivided into eight fields of four hexadecimal values separated by colons.
- IPv6 address has a three-part hierarchy
  - **Global prefix**, also called a site prefix, is the first three blocks of the address.
  - **Subnet ID** includes the fourth block of the address.
  - **Interface ID** or **host identifier** includes the last four blocks of the address.



Dynamic Host Configuration Protocol (DHCP)



- DHCP automatically provides computers with an IP address.
- The DHCP server can assign these to hosts:
  - IP address
  - Subnet mask
  - Default gateway
  - Domain Name System (DNS) server address

Internet Control Message Protocol (ICMP)

- **Internet Control Message Protocol (ICMP)** is used by devices on a network to send control and error messages to computers and servers.
- **PING (Packet Internet Groper)** is a simple command line utility used to test connections between computers.
  - Used to determine whether a specific IP address is accessible.
  - Used with either the hostname or the IP address.
  - Works by sending an ICMP echo request to a destination computer.
  - Receiving device sends back an ICMP echo reply message.
- Four ICMP echo requests (pings) are sent to the destination computer to determine the reliability and reachability of the destination computer.

Internet Protocols

- A **protocol** is a set of rules. Internet protocols govern communication within and between computers on a network.
- Many protocols consist of a **suite** (or group) of protocols stacked in layers.
  - Devices and computers connected to the Internet use a protocol suite called **TCP/IP** to communicate with each other.
- The main functions of protocols:
  - Identifying errors
  - Compressing data
  - Deciding how data is to be sent
  - Addressing data
  - Deciding how to announce sent and received data
- The information is transmitted most often via two protocols, TCP and UDP.

Networked Equipment Addressing

- THREE rules help reduce the number of digits needed to represent an IPv6 address.
  - Rule 1 – Omit Leading 0s
  - Rule 2 – Omit All 0 Segments
  - Rule 3 – You can use a double colon only once

Fully expanded	2001:0DB8:0000:1111:0000:0000:0000:0200
No leading 0s	2001: DB8: 0:1111: 0: 0: 0: 200
Compressed	2001:DB8:0:1111::200

Fully expanded	FE80:0000:0000:0000:0123:4567:89AB:CDEF
No leading 0s	FE80: 0: 0: 0: 123:4567:89AB:CDEF
Compressed	FE80::123:4567:89AB:CDEF

Fully expanded	FF02:0000:0000:0000:0000:0000:0000:0001
No leading 0s	FF02: 0: 0: 0: 0: 0: 0: 1
Compressed	FF02::1

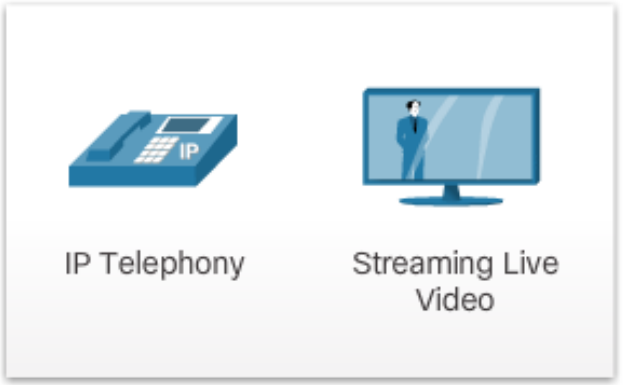
Transport Layer Protocols

- The two protocols that operate at the transport layer are Transport Control Protocol (TCP) and User Datagram Protocol (UDP)
  - TCP is considered reliable, because it ensures that all of the data arrives at the destination.
  - UDP does not provide for any reliability.

TCP

Required protocol properties:
- Reliable
- Acknowledge data
- Resends lost data
- Delivers data in sequenced order

UDP



Required protocol properties:
- Fast
- Low overhead
- Does not require acknowledgements
- Does not resend lost data
- Delivers data as it arrives

Transport Layer Protocols

- TCP and UDP use a source and destination port number to keep track of application conversations.
- The destination port number is associated with the destination application on the remote device.
- The source port number is dynamically generated by the sending device.

Port Number	Protocol	Application	Acronym
20	TCP	File Transfer Protocol (data)	FTP
21	TCP	File Transfer Protocol (control)	FTP
22	TCP	Secure Shell	SSH
23	TCP	Telnet	–
25	TCP	Simple Mail Transfer Protocol	SMTP
53	UDP, TCP	Domain Name Service	DNS
67	UDP	Dynamic Host Configuration Protocol (server)	DHCP
68	UDP	Dynamic Host Configuration Protocol (client)	DHCP
69	UDP	Trivial File Transfer Protocol	TFTP
80	TCP	Hypertext Transfer Protocol	HTTP
110	TCP	Post Office Protocol version 3	POP3
143	TCP	Internet Message Access Protocol	IMAP
161	UDP	Simple Network Management Protocol	SNMP
443	TCP	Hypertext Transfer Protocol Secure	HTTPS
137-139, 445	TCP	Server Message Block	SMB
548/427	TCP	Apple Filing Protocol	AFP
3389	TCP, UDP	Remote Desktop Protocol	RDP

7.5 Chapter Summary

Cisco | Networking Academy®
Mind Wide Open™

Summary

This chapter introduced the operation of computer networks. The following concepts from this chapter are important to remember:

- Computer devices and components include host devices, intermediary devices, and media.
- Major network types include LANs, WLANs, PANs, MANs, WANs, Peer-to-Peer, and Client-Server
- Networking standards are conceptually organized into two reference models: the OSI model and the TCP/IP model
- Wired networks use CSMA/CD when operating in half-duplex. Wireless networks use CSMA/CA.
- Network devices include modems, switches, wireless APs, routers, and firewalls.
- Network media includes coaxial cables, twisted-pair cables, and fiber-optic cables. Wireless signals are also considered media.
- The two twisted-pair wiring schemes are T568A and T568B.
- Devices need a physical address (MAC) and a logical address (IP) to communicate on the network.
- The transport layer includes the two protocols, TCP and UDP. TCP is reliable but introduces overhead that is not used with UDP.
- The transport layer tracks conversations between applications using source and destination port numbers.


Cisco | Networking Academy®
Mind Wide Open™


CISCO