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

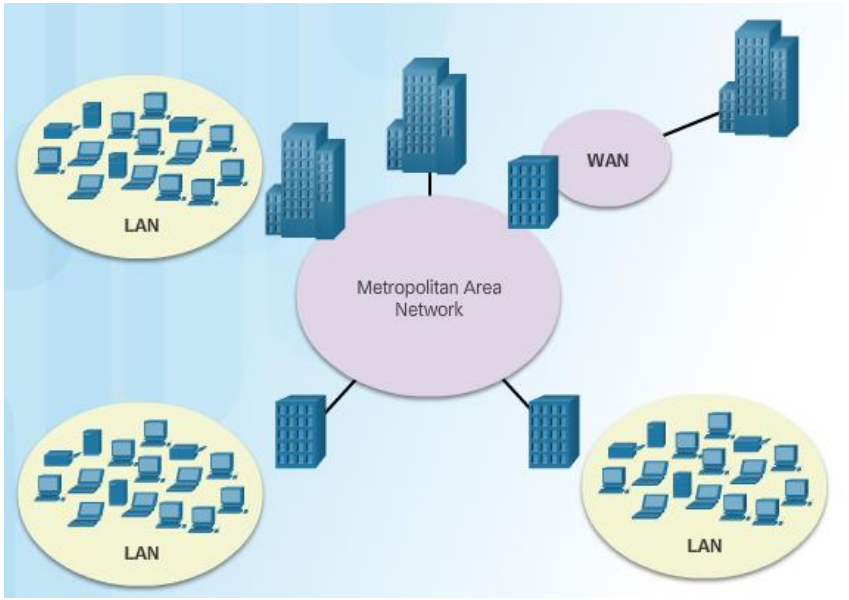
7.1 Principles of Networking

Cisco | Networking Academy®
Mind Wide Open™

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



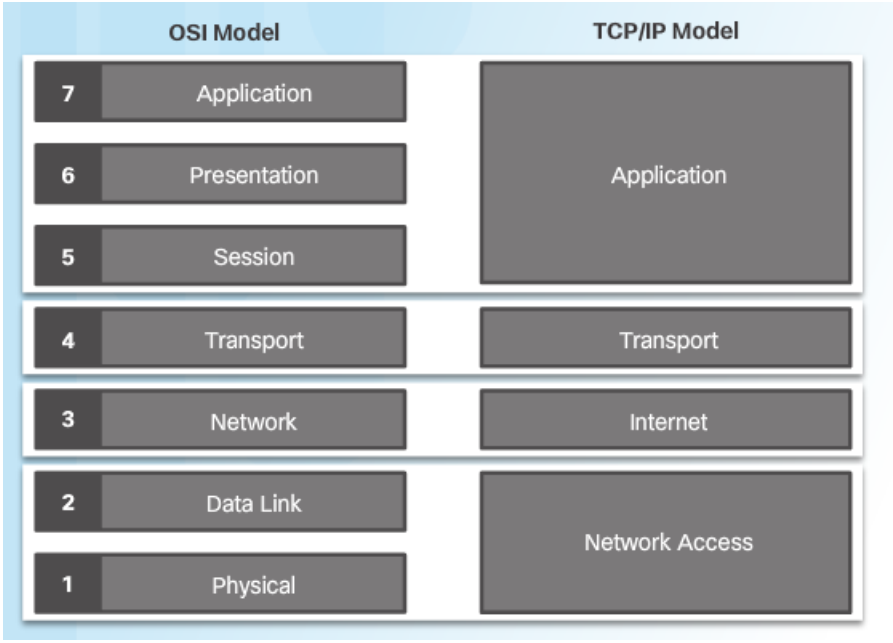
- Major types of networks include:
  - Local Area Networks (LANs)
  - Wireless Local Area Networks (WLANs)
  - Personal Area Networks (PANs)
  - Metropolitan Area Networks (MANs)
  - Wide Area Networks (WANs)
- Peer-to-Peer Networks
  - No dedicated servers
  - Each computer decides which resources to share
  - No central administration or security
- Client-Server Networks
  - Server with software installed for client access
  - Resources controlled by centralized administrator

7.2 Networking Standards

Cisco | Networking Academy®
Mind Wide Open™

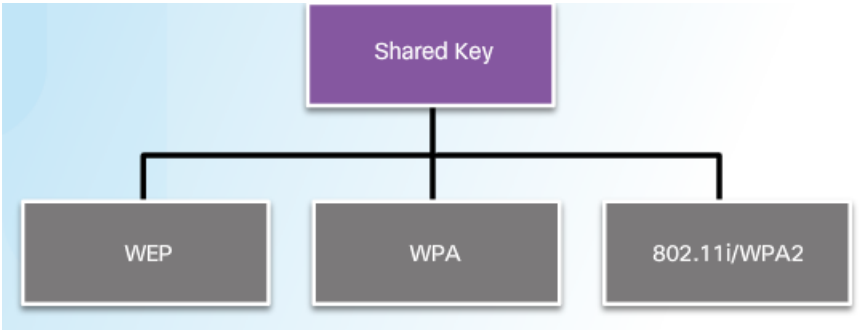
Reference Models

- 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.



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.

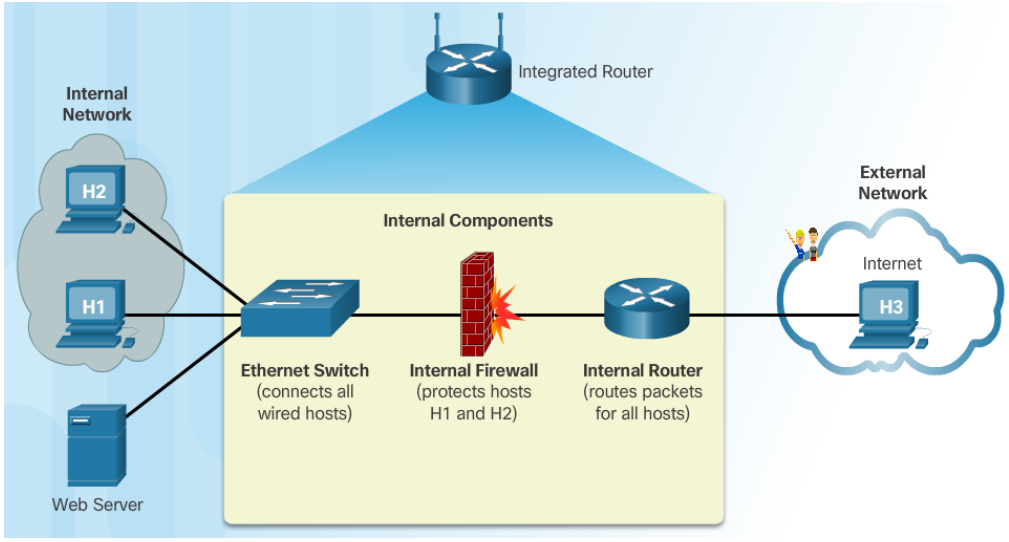


7.3 Physical Components of a Network

Cisco | Networking Academy®
Mind Wide Open™

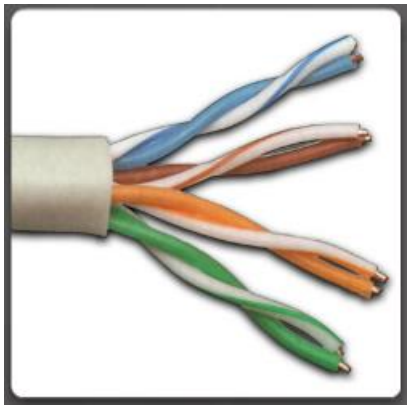
Network Devices

- Modems convert a computer's digital data into a format that can be transmitted on the ISP's network.
- Switches microsegment LANs by sending data only to the computer that needs it.
- Wireless access points (APs) connect wireless devices. Routers use IP addresses to forward traffic to other networks.
- In a home or small office, a route often includes a switch, a firewall, and an AP.



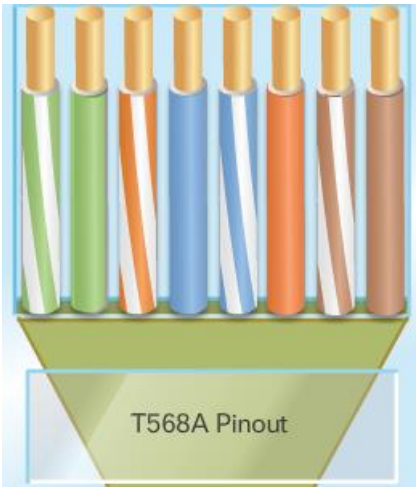
Cables and Connectors

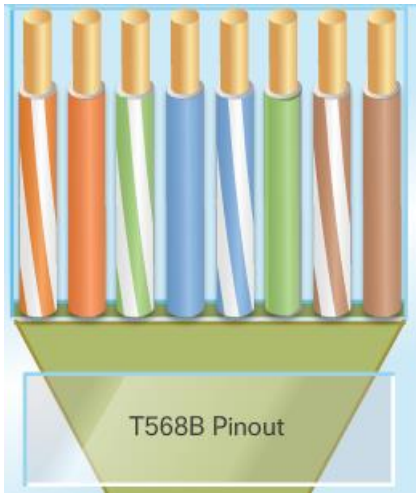
- Coaxial and twisted-pair cables use electrical signals over copper to transmit data. Fiber-optic cables use light signals to transmit data. These cables differ in bandwidth, size, and cost.
- There are several types of coaxial cable: 10Base5 (thicknet), 10Base2 (thinnet), RG-59 (cable TV), RG-6 (better than RG-59)
- Twisted-pair cables are terminated with an RJ-45 connector. Twisted-pair comes in two types:
  - Unshielded Twisted-Pair (UTP)
  - Shielded Twisted-Pair (STP)
- Fiber-optic cables are broadly classified into two types:
  - 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.



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.
- 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 and a crossover cable.
- A straight-through cable is the most common cable type. The wiring scheme is the same on both sides.
- A crossover cable uses both wiring schemes. T568A on one end of the cable and T568B on the other end of the same cable.





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

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

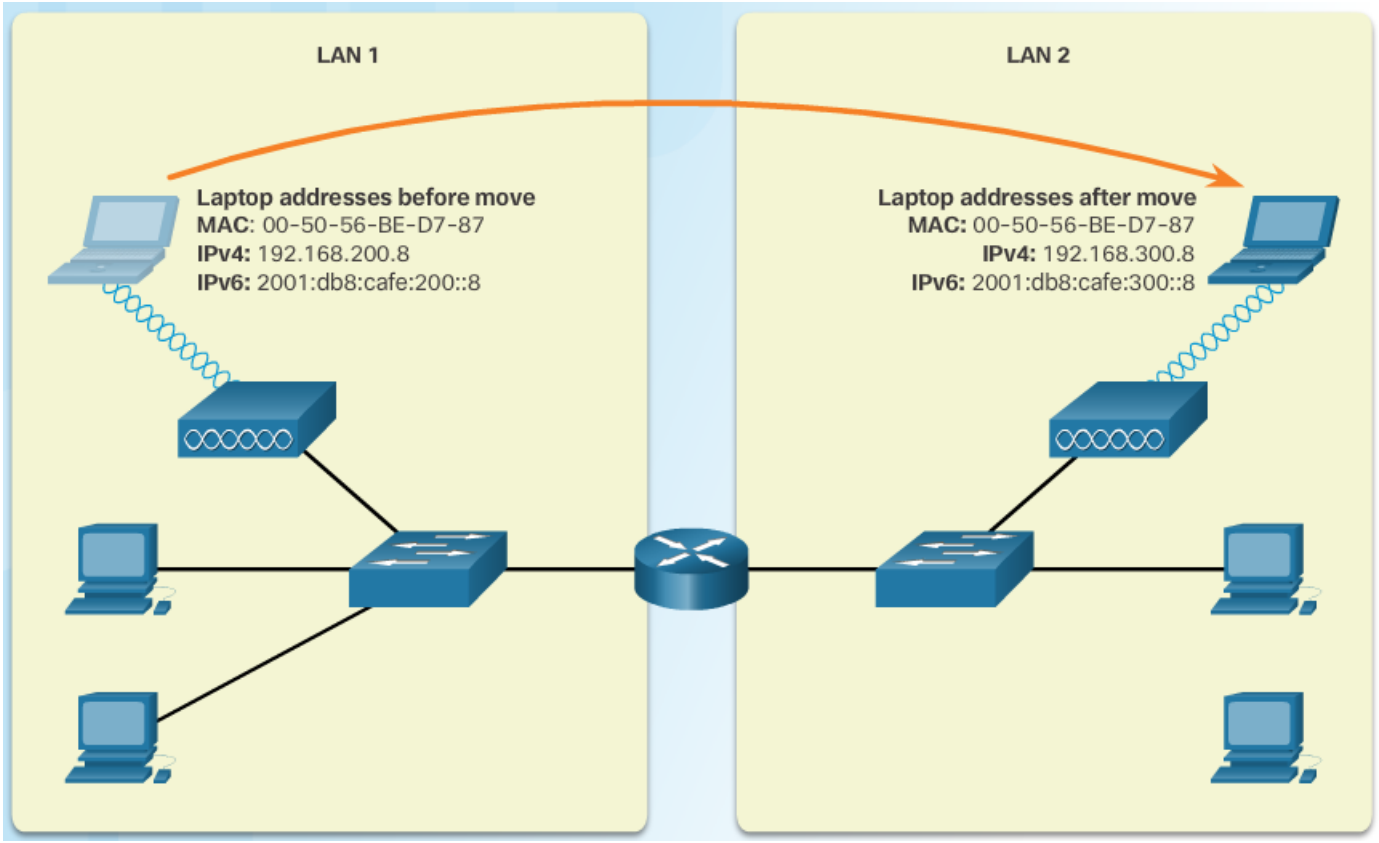
2001:0DB8:CAFE:0200:0000:0000:0000:0008

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.



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

Networked Equipment Addressing

- Two rules help reduce the number of digits needed to represent an IPv6 address.
  - Rule 1 - Omit Leading 0s
  - Rule 2 – Omit All 0 Segments

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

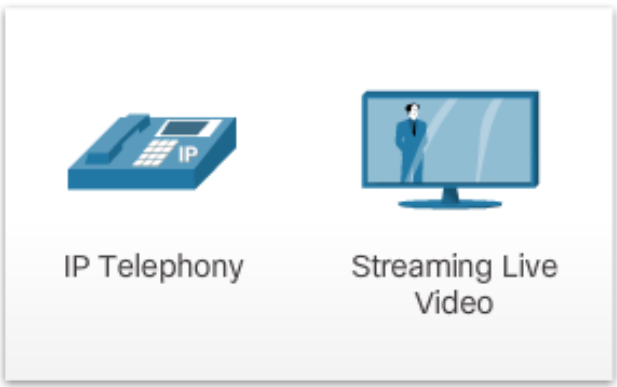
Transport Layer Protocols

- 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 acknowledgments
- 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.