ملاحظة: المكثف بهدف لتلخيص اهم النقاط لشبكات الحاسوب, بس ما بظمنلك تجيب العلامة الكاملة, رح تستفيد من هاظ المكثف اكثر لو درست المادة قبل تدرس هان, و انا مش مسؤول عن اي حد ما جاب العلامة الي بدو اياها

Chapter 1

1. The amount of devices doubled from "fixed" computing to the mobile computing every 13 years to 200m devices
2. The amount of devices doubled from mobile computing to the internet of things every 1.4 years to 10b devices
3. The amount of devices doubled from internet of things to the internet of everything to 50b devices

Networks support the way we

1. Learn
2. communicate
3. work
4. play

Types of networks

1. Small home networks (one device to a printer)
2. Small office/Home office networks (two device next to each other)
3. Medium to large networks (a building)
4. World Wide networks (the world)

Clients and servers

All computers connected to a network are classified as hosts or end devices, depending on the software installed.

In modern networks, end devices can act as a client, a server, or both.

Hosts: devices that can send and receive messages on the network

Servers: hosts that have software installed that enable them to provide information, like email or web pages, to other hosts on the network. Each service requires software

Clients : computer hosts that have software installed that enable them to request and display the information obtained from the server. i.e. web browsers.

Peer to Peer networks

peer-to-peer network: a network where computers serve as both servers and clients, used mostly in home and small businesses, i.e a pc and a printer

Advantages

1. Easier to set up
2. less complex
3. Lower Costs (explain): as there is no need for dedicated servers and networks
4. can be used for simple tasks like sharing files and printers

Disadvantages

1. No centralized administration
2. Not as secure
3. Not Scalable
4. Can slow down devices, as they act as both servers and clients

---

Types of Networks

Components of a network

Components of a Network

Devices

- **Examples of End Devices:**
  - Computers (workstations, laptops, file servers, web servers)
  - Network printers
  - VoIP phones
  - TelePresence endpoint
  - Security cameras
  - Mobile handheld devices (such as smartphones, tablets, PDAs, and wireless debit/credit card readers and barcode scanners)
- **Examples of Intermediary Network Devices:**
  - Network Access Devices (switches, and wireless access points)
  - Internetworking Devices (routers)

- Security Devices (firewalls)

Media

- **Examples of Media:**
  - Copper
  - Fiber optics
  - Wireless

Services

Topology Diagrams

There are two types of topology diagrams

1. Physical: intermediary devices, configured ports, and cable installation.
2. Logical: devices, ports, and IP addressing scheme.

Networks depend on 3 factors

1. Area Size
2. Number of Users
3. Number and Types of Services

Main network types

1. Local Area Network (LAN): provides access to users and end devices in a small geographical area.
2. Wide Area Network (WAN): provides access to other networks over a wide geographical area.

Other Types

1. Metropolitan Area Network (MAN)
2. Wireless LAN (WLAN)
3. Storage Area Network (SAN)

Intranet and Extranet

Intranet: a private connection of LANs and WANs that belongs to an organization (only that org can use it)

Extranet: used by an organization to provide secure and safe access to individuals who work for a different organizations, but require company data.

Connecting Remote Users to the Internet

1. Broadband Digital Subscriber Line (DSL)
    - DSL runs over a telephone line
    - requires a special modem that separates the DSL signal from the telephone signal and provides an Ethernet connection to a host computer or LAN
    - depends mainly on the quality of the phone line and the distance from your phone company's central office
2. Cable
    - Offered by cable television service providers
    - the Internet data signal is carried on the same coaxial cable that delivers cable television.
    - A special cable modem separates the Internet data signal from the other signals carried on the cable
3. Cellular: uses a cell phone network to connect, Performance will be limited by the capabilities of the phone and the cell tower to which it is connected.
4. Satellite: a good option for homes or offices that do not have access to DSL or cable, Dishes require a clear line of sight to the satellite
5. Dial-up Telephone
    - An inexpensive option that uses any phone line and a modem.
    - To connect, a user calls the ISP access phone number.
    - The low bandwidth provided by a dialup modem connection is usually not sufficient for large data transfer

Connecting Businesses to the Internet

1. Dedicated Leased Line: a dedicated connection from the service provider to the customer premise. Leased lines are actually reserved circuits that connect geographically separated offices for private voice and/or data networking.
2. Metro Ethernet: typically available from a provider to the customer premise over a dedicated copper or fiber connection

---

The network as a platform

seperate/dispared networks: networks that can't communicate with each other

converged networks: networks that can deliver stuff between many different types of devices over the same communication channel and network structure

---

Supporting Network Architecture

there are four basic characteristics that need to addressed in order to meet user expectations

1. Fault Tolerance
    - The expectation is that the Internet is always available to the millions of users who rely on it.
    - A fault tolerant network is one that:
    1. limits the impact of a failure
    2. built to allow quick recovery when such a failure occurs
2. Scalability
- Thousands of new users and service providers connect to the Internet each week.
- for the Internet to support this. it must be scalable
- it can expand quickly to support new users and applications without impacting the performance of services to existing users.
- Scalability also refers to the ability to accept new products and applications
3. Providing QoS
- New applications available to users over internetworks create higher expectations for the quality of the delivered services.
- Networks must provide predictable, measurable, and at times, guaranteed services
4. Security

Chapter 2

Operating Systems

Networking equipment relies on operating systems (OS for short) for functionality.

Firmware: Name of the operating system used on a home router

Cisco devices utilize Cisco IOS, which encompasses a range of network operating systems.

Shell: The interface enabling users to request tasks from the computer, accessible via CLI or GUI.

Kernel: Facilitates communication between a computer's hardware and software, managing resource allocation.

Hardware: Physical components of a computer, encompassing its underlying electronics.

Purpose of Operating Systems

PC operating systems (Windows 8 and OS X) perform technical functions that enable:

- Use of a mouse
- View output
- Enter text

Switch or router IOS provides options to:

- Configure interfaces
- Enable routing and switching functions

Networking devices are equipped with a default IOS, which can be upgraded.

Location of the Cisco IOS

Cisco IOS is stored in Flash, providing non-volatile storage unaffected by power loss and allowing for easy modification. Flash memory accommodates multiple IOS versions, which can be copied to volatile RAM for execution. The quantity of flash and RAM determines the available IOS options for a device.

IOS Functions

- Security
- Routing
- QoS
- Addressing
- Managing Resources
- Interface

Console Access Method

1. Console Port:

- Allows access even without networking setup (out-of-band).
- Requires a specific console cable.
- Facilitates configuration input.
- Password setup is essential to thwart unauthorized entry.
- Best situated in a secure room to prevent easy access to the console port.

2. Telnet

- Enables remote CLI access over a network.
- Requires active networking services and at least one configured active interface.

3. Secure Shell (SSH)

- Remote login similar to Telnet, but utilizes more security
- Stronger password authentication
- Uses encryption when transporting data

4. Aux Port

- Out-of-band connection
- Uses telephone line
- Can be used like console port

Terminal Emulation Programs

Software for connecting to network devices:

- PuTTY
- Tera Term
- SecureCRT
- HyperTerminal
- OS X Terminal

Primary Modes (User vs Primary)

User EXEC mode permits only basic monitoring commands and is akin to a view-only mode (Switch>,Router>).

Privileged EXEC mode grants access to monitoring, configuration, and management commands by default (Switch#, Router#).

Cisco IOS Command Reference

To navigate to Cisco's IOS Command Reference to find a command:

1. Go to Cisco website
2. Click Support
3. Click Networking Software (IOS & NX-OS)
4. Click 15.2M&T
5. Click Reference Guides
6. Click Command References
7. Click the particular technology
8. Click the link on the left that alphabetically matches the command you referencing
9. Click the link for the command

Hot Keys and Shortcuts

- Tab – Completes the remainder of a partially typed command or keyword.
- Ctrl-R – Redisplays a line.
- Ctrl-A – Moves to the beginning of the line.
- Ctrl-Z – Exits the configuration mode and returns to user EXEC.
- Down Arrow – Allows the user to scroll forward through former commands.
- Up Arrow – Allows the user to scroll backward through former commands.
- Ctrl-shift-6 – Allows the user to interrupt an IOS process such as ping or traceroute.
- Ctrl-C – Exits the current configuration or aborts the current command.

Device Names

Some guidelines for naming conventions:

- Start with a letter
- Contains no spaces
- Ends with a letter or digit
- Uses only letters, digits, and dashes
- Be less than 64 characters in length

Without names, network devices are difficult to identify for configuration purposes.

Hostnames allow devices to be identified by network administrators over a network or the Internet.

Securing Device Access

These passwords are used to control access to different parts of a network device:

- **Enable Password:** Controls access to high-level configuration and operations.
- **Enable Secret:** A more secure version of the enable password, used for the same purpose.
- **Console Password:** Limits access through direct physical connections.
- **VTY Password:** Controls access over remote Telnet connections.

Choose Enable Secret' over Enable Password for better security. Enable Secret encrypts the password, while Enable Password stores it in plain text, making unauthorized access easier.

Securing the console port reduces the risk of unauthorized physical access to the device via cable insertion.

VTY lines enable Telnet access to Cisco devices. The number of supported VTY lines depends on the device type and IOS version.

Encrypting Password Display

Service Password Encryption

- Prevents passwords from showing up as plain text when viewing the configuration
- Keeps unauthorized individuals from viewing passwords in the configuration file
- Once applied, removing the encryption service does not reverse the encryption

---

Banner Messages

- Important part of the legal process in the event that someone is prosecuted for breaking into a device.
- Wording that implies that a login is "welcome" or "invited" is not appropriate.
- Often used for legal notification because it is displayed to all connected terminals.

1. `Switch# reload`: Initiates a reboot of the switch. Prompts whether to save the system configuration before proceeding. User selects 'n' to not save.

Switch# reload System configuration has been modified.
Save? [yes/no]: n
Proceed with reload? [confirm]

2. `Switch# erase startupconfig`: Clears the startup configuration stored in the switch's memory. This configuration is loaded upon booting, so erasing it resets the switch to default settings.

Switch# erase startupconfig

3. `Switch# delete vlan.dat`: Removes the VLAN database file from flash memory. This file holds VLAN configuration details. Deleting it wipes out all VLAN configurations.
   Switch# delete vlan.dat
   Delete filename [vlan.dat]?
   Delete flash:vlan.dat? [confirm]

IP Addressing of Devices

- Each device connected to a network needs to have an IP address configured.
- The format of an IPv4 address is termed as dotted decimal.
- An IPv4 address is represented in decimal notation with four numbers ranging from 0 to 255, separated by dots.
- Alongside the IP address, a subnet mask is essential for defining the network portion.
- IP addresses can be assigned to both physical ports and virtual interfaces.

Interfaces and Ports

- Network communications rely on interfaces of end user devices, networking devices, and the cables that link them.
- Network media can be twisted-pair copper cables, fiber-optic cables, coaxial cables, or wireless.
- Each type of network media offers distinct features and advantages.
- Ethernet stands out as the primary technology for local area networks (LANs).
- Ethernet ports are present on end user devices, switch devices, and other networking equipment.
- Cisco IOS switches feature physical ports for device connections, as well as switch virtual interfaces (SVIs) which are software-created and lack physical hardware.
- SVIs enable remote management of a switch over a network.

Configuring a Switch Virtual Interface

- IP address: When combined with a subnet mask, it uniquely identifies an end device on a network.

- Subnet mask: It determines which portion of a larger network is assigned to an IP address.
- Interface VLAN 1: Accessible in interface configuration mode.
- IP address 192.168.10.2 255.255.255.0: Sets the IP address and subnet mask for the switch.
- No shutdown: Activates the interface administratively.
- Additionally, physical ports of the switch need configuration, and VTY lines need to be set up for remote management.

Chapter 3

Rules of Communication

All communication methods have three elements in common: - Source or sender - Destination or receiver - Channel or media

Rules or protocols govern all methods of communication.

it goes: Message (source) > Signal (Transmitter) > Transmission Medium > Signal (Receiver) > Message (Message Destination)

Effective communication relies on protocols that encompass:

1. a sender and receiver.
2. common language and grammar.
3. speed and timing in delivery.
4. confirmation or acknowledgment procedures.
5. an agreed method of communication (face to face etc)

Protocols used in network communications also define:

A. Message Encoding

- Hosts encode messages to fit the medium.
- Messages are first converted into bits by the sending host.
- Each bit is then encoded into specific patterns of sounds, light waves, or electrical impulses, depending on the network media.
- The destination host receives and deciphers these signals to interpret the original message.

B. Message Formatting and Encapsulation

- Letters must adhere to a standardized format and proper addressing to ensure accurate delivery.
- Encapsulation involves placing the letter within its addressed envelope.
- Every computer message is encapsulated into a distinct format, known as a frame, prior to transmission across the network.
- Similar to an envelope, a frame supplies both destination and source addresses.

C. Message Size

- Humans divide lengthy messages into smaller parts or sentences.
- Extensive messages are broken into smaller pieces for network transmission.
- Each piece is sent in an individual frame.
- Each frame is equipped with its unique addressing information.
- Upon reception, a host reconstructs multiple frames into the original message.

D. Message Timing

Access Method:

- Hosts on a network require clear guidelines on when to initiate message transmission and how to handle collisions if they occur.

Flow Control:

- Source and destination hosts engage in flow control protocols to regulate the timing of data transfer, preventing overwhelm at the destination and ensuring successful reception of information.

Response Timeout:

- Network hosts adhere to predetermined rules dictating the duration to wait for responses and defining appropriate actions in the event of response timeouts.

E. Message Delivery Options

- Unicast Message (one to one)
- Multicast Message (one to many)
- Broadcast Message (one to all)

Network Protocols and Standards

Protocols: Rules that govern communication.

Protocol suites: Set of rules that work together to help solve a problem.

Example: Conversation Protocol suites:

1. Use a common language
2. Wait your turn
3. Signal when finished

Network Protocols:

How the message is formatted or structured

How networking devices share information about pathways with other networks

How and when error and system messages are passed between devices

The setup and termination of data transfer sessions

Interaction of Protocols

1. Application Protocol – Hypertext Transfer Protocol (HTTP)
2. Transport Protocol – Transmission Control Protocol (TCP)
3. Internet Protocol – Internet Protocol (IP)
4. Network Access Protocols – Data link & physical layers

Protocol Suites and Industry Standards

TCP	ISO	Apple Talk	Novell Software
HTTPS/DNS/DHCP/FTP	ACSE/ROSE/TRSE/SESE	AFP	NDS
TCP/UDP	TP0/TP1/TP2/TP3/TP4	ATP/AEP/NBP/RTMP	SPX
IPv4/IPv6/ICMPv4/ICMPv6	CONP/CMNS/CLNP/CLNS	AARP	IPX
Ethernet	PPP	Frame Relay	ATM/WLAN

Creation of Internet, Development of TCP/IP

- ARPANET (Advanced Research Projects Agency Network), established in 1969, was the precursor to the modern Internet, connecting mainframe computers at four locations. - Funded by the U.S. Department of Defense, ARPANET was intended for use by universities and research labs. - BBN (Bolt, Beranek and Newman) played a crucial role in ARPANET's development, creating the first router, called an Interface Message Processor (IMP). - In 1973, Robert Kahn and Vinton Cerf initiated work on TCP to improve upon ARPANET's existing Network Control Program (NCP). - TCP/IP, developed in 1978, replaced TCP and IP,

becoming the foundational protocol suite for the Internet. - Over time, additional protocols like Telnet, FTP, DNS, etc., were incorporated into the TCP/IP suite.

TCP/IP Protocol Suite and Communication

Layer Name	Examples
Application Layer	Name System (DNS)/ Host Config (BOOTP/DHCP) / Email(SMTP/POP/IMAP)/ Web(HTTP)
Transport Layer	UDP / TCP
Internet Layer	IP(NAT ARP)/ IP Support(ICMP) / Routing Protocols (RIP/OSPF/EIGRP/BGP)
Network Access Layer	ARP/ PPP/ Ethernet/ Interface Drivers

Standards Organizations

Open Standards

- The Internet Society (ISOC)
- The Internet Architecture Board (IAB)
- The Internet Engineering Task Force (IETF)
- Institute of Electrical and Electronics Engineers (IEEE)
- The International Organization for Standards (ISO)

The Internet Society controls The Internet Architecture Board which controls

1. The Internet Engineering Task Force (working groups)
2. The Internet Research Steering Group (IRSG) (Research Groups)

IEEE:

- 38 societies

- 130 journals
- 1,300 conferences each year
- 1,300 standards and projects
- 400,000 members
- 160 countries

Working group examples:

1. IEEE 802.3 (Ethernet Working Group)
2. IEEE 802.11 (Wireless LAN Working Group)

Other Standards Organization

- The Electronic Industries Alliance (EIA)
- The Telecommunications Industry Association (TIA)
- The International Telecommunications Union – Telecommunications Standardization Sector (ITU-T)
- The Internet Corporation for Assigned Names and Numbers (ICANN)
- The Internet Assigned Numbers Authority (IANA)

Reference Models

ISO/OSI Model

1. Physical
2. Data Link
3. Network
4. Transport
5. Session
6. Presentation
7. Application

TCP/IP Model

- Application: Represents data to the user, plus encoding and dialog control.
- Transport: Supports communication between diverse devices across diverse networks
- Internet: Determines the best path through the network.
- Network Access: Controls the hardware devices and media that make up the network.

OSI Model	TCP/IP Protocol Suite	TCP/IP Model
Application		Application
Presentation	HTTP, DNS, DHCP, FTP	
Session		
Transport	**TCP, UDP**	**Transport**
Network	**IPv4, IPv6, ICMPv4, ICMPv6**	**Internet**
Data Link	**PPP, Frame Relay, Ethernet**	
Physical		Physical

Moving Data in the Network

Communicating the Messages

- Segmenting message benefits :

1. Different conversations can be interleaved
2. Increased reliability of network communications.

- Segmenting message disadvantage: Increased level of complexity

Protocol Data Units (PDUs)

1. Data
2. Segment
3. Packet
4. Frame
5. Bits

Example:

Email Data (Data) --> Segment (Data/Data/Data --> Transport Header/Data) --> Packet(Network Header/Transport Header/Data) --> Frame(medium dependent) (Frame Header/Network Header/Transport Header/Data/Frame Header)

Accessing Local Resources

Network Addresses and Data Link Addresses

- Physical: Timing and synchronization bits.

- Data Link: Destination and source physical addresses.
- Network: Destination and source logical network addresses
- Transport: Destination and source process number (ports).
- Upper Layers: Encoded application data.

Chapter 4

Physical Layer

encapsulation and De-encapsulation

Source		Destination
Application		Application
Presentation	ApplicationData	Presentation
Session	Application Data	Session
Transport	Data / Data / Data	Transport
Network	Header/ Data	Network
Data Link	Header/Header/ Data/Trailer	Data Link
Physcial		Physcial
	Signal	

Physical Layer Standards

Standard Organization	Networking Standards
ISO	•ISO 8877: Officially adopted the RJ connectors (e.g., RJ-11, RJ-45) •ISO 11801: Network cabling standard similar to EIA/TIA 568.
EIA/TIA	•TIA-568-C: Telecommunications cabling standards, used by nearly all voice, video and data networks. •TIA-569-B: Commercial Building Standards for Telecommunications Pathways and Spaces •TIA-598-C: Fiber optic color coding •TIA-942: Telecommunications Infrastructure Standard for Data Centers
ANSI	•568-C: RJ-45 pinouts. Co-developed with EIA/TIA
ITU-T	•G.992: ADSL
IEEE	•802.3: Ethernet •802.11: Wireless LAN (WLAN) & Mesh (Wi-Fi certification) •802.15: Bluetooth

Physical Layer Fundamental Principles

Media	Physical Components	Frame Encoding Technique	Signalling Method
Copper Cable	•UTP •Coaxial •Connectors •NICs •Ports Interface	•Manchester Encoding •Non-Return to Zero (NRZ) techniques •4B/5B codes are used with Multi-Level Transition Level 3 (MLT-3) signaling •8B/10B PAM5	•Changes in the electromagnetic field •Intensity of the electromagnetic field •Phase of the electromagnetic wave
Fiber Optic Cable	•Single-mode Fiber •Multimode Fiber •Connectors •NICs •Interfaces •Lasers and LEDs •Photoreceptors	•Pulses of light •Wavelength multiplexing using different colors	•A pulse equals 1. •No pulse is 0.
Wireless Media	•Access Points •NICs •Radio •Antennae	•DSSS (direct-sequence spread-spectrum) •OFDM (orthogonal frequency division multiplexing)	•Radio waves

Bandwidth

Unit	Abbr	Speed
Bits per second	bps	1 bps
Kilobits per second	kbps	1^3 bps
Megabits per second	mbps	1^6 bps
Gigabits per second	gbps	1^9 bps
Terabits per second	tbps	1^12 bps

Network Media

Copper Media Types:

1. Unshielded Twisted Pair (UTP) Cable:
    - Outer Jacket: Protects the copper wire from physical damage
    - Twisted-Pair: Protects the signal from interference
    - Color-Coded Plastic: Insulation Electrically isolates wires from each other and identifies each pair
2. Shielded Twisted Pair (STP) Cable
    - Jacket
    - Braided or Foil Shield
    - Twisted Pair
3. Coaxial Cable
    - Outer Jacket
    - Braided Copper Shielding
    - Copper Conductor
    - Plastic Insulation
    - Coaxial Connectors:
        1. BNC
        2. N Type
        3. F Type

Cooper Media Safety

1. The separation of data and electrical power, cabling must comply with safety codes.
2. Cables must be connected correctly.
3. Installations must be inspected for damage.
4. Equipment must be grounded correctly.

UTP Cabling

UTP cable does not use shielding to counter the effects of EMI and RFI. Instead, cable designers have discovered that they can limit the negative effect of crosstalk by:

1. Cancellation
2. Varying the number of twists per wire pair

UTP Cabling Standards

1. Category 3 (UTP)
2. Category 7 (scTP)
3. Category 6 (UTP)
4. Category 5 and 5e (UTP):
    - . Used for Data transmission
    - Cat 5 supports 100 Mbps and can support 1000 Mbps but it is not recommended
    - Cat 5e supports 1000 Mbps

UTP Connectors is the RJ-45

UTP Cable Types

Type	Standard	Application
Ethernet Staright-through	Both ends T568A or both ends T568B	Connects a network host to a network device such as a switch or hub.
Ethernet Crossover	One end T568A, other end T568B	. Connects two network hosts . Connects two network intermediary devices (switch to switch, or router to router)
Rollover	Cisco proprietary	Connects a workstation serial port to a router console port, using an adapter.

After installation, UTP cables are checked for

1. Wire map
2. Cable length
3. Signal loss due to attenuation
4. Crosstalk

Fiber Optic Cabling

Fiber Optic Cabling Uses

1. Enterprise Networks
2. Fiber-to-the-home (FTTH) and Access Networks
3. Long-Haul Networks
4. Submarine Networks

Fiber Optic Cabling Design

1. Jacket (outer)

2. Strengthening Material
3. Buffer
4. Cladding
5. Core (Inner)

Fiber Media Types

1. Single Mode: Produces single straight path for light
    - Glass Core =9 microns
    - Glass Cladding 125 microns diameter
    - Polymeric coating
    - Small core
    - Less dispersion
    - Suited for long distance applications
    - Uses lasers as the light source
    - Commonly used with campus backbones for distances of several thousand meters

2. Multimode: Allows multiple paths for light
    - Glass Core=50/62.5 microns
    - Glass Cladding 125 microns diameter
    - Coating
    - Larger core than single mode cable
    - Allows greater dispersion and therefore, loss of signal
    - Suited for long distance applications, but shorter than single mode
    - Uses LEDs as the light source
    - Commonly used with LANs or distances of a couple hundred meters within a campus network

Network Fiber Connectors

1. ST Connector
2. SC Connector
3. LC Connector
4. Duplex Multimode LC Connector

Fiber versus Copper

Implementation Issues	Copper	Fiber
Bandwidth Supported	10 Mbps – 10 Gbps	10 Mbps – 100 Gbps

Implementation Issues	Copper	Fiber
Distance	Relatively short (1 – 100 meters)	Relatively High (1 – 100,000 meters)
Immunity To EMI And RFI	Low	High (Completely immune)
Immunity To Electrical Hazards	Low	High (Completely immune)
Media And Connector Costs	Lowest	Highest
Installation Skills Required	Lowest	Highest
Safety Precautions	Lowest	Highest

Wireless Media

Wireless Media areas of concern

- Coverage area
- Interference
- Security

Types of Wireless Media

WIFI	**•IEEE 802.11 standards** **•Commonly referred to as Wi-Fi.** **•Uses CSMA/CA** **•Variations include:** **•802.11a: 54 Mbps, 5 GHz** **•802.11b: 11 Mbps, 2.4 GHz** **•802.11g: 54 Mbps, 2.4 GHz** **•802.11n: 600 Mbps, 2.4 and 5 GHz** **•802.11ac: 1 Gbps, 5 GHz** **•802.11ad: 7 Gbps, 2.4 GHz, 5 GHz, and 60 GHz**

Bluetooth	•IEEE 802.15 standard •Supports speeds up to 3 Mb/s •Provides device pairing over distances from 1 to 100 meters.
WI MAX	•IEEE 802.16 standard •Provides speeds up to 1 Gbps •Uses a point-to-multipoint topology to provide wireless broadband access.

802.11 Wi-Fi Standards

Standard	Maximum Speed	Frequency	Backwards Compatible
802.11a	54 Mbps	5 GHz	No
802.11b	11 Mbps	2.4 GHz	No
802.11g	54 Mbps	2.4 GHz	802.11b
802.11n	600 Mbps	2.4 GHz or 5 GHz	802.11b/g
802.11ac	1.3 Gbps (1300 Mbps)	2.4 GHz and 5 GHz	802.11b/g/n
802.11ad	7 Gbps (7000 Mbps)	2.4 GHz, 5 GHz and 60 GHz	802.11b/g/n/ac

---

Data Link Layer Protocols

Data Link Sublayers

1. LLC Sublayer
2. Mac Sublayer
3. (between physical and data link is 802.3 Ethernet, 802.11 Wi-Fi, 802.15 Bluetooth)

Media Access Control

Data link layer protocols govern how to format a frame for use on different media.

Different protocols may be in use for different media.

At each hop along the path, an intermediary device accepts frames from one medium, decapsulates the frame and then forwards the packets in a new frame. The headers of each frame are formatted for the specific medium that it will cross.

The Data Link layer is responsible for controlling the transfer of frames across the media.

Formatting Data for Transmission

Header	Packet	Trailer
Frame Start/Addressing/Type/Quality Control	Data	Error Detection / Frame Stop
A specific Pattern at the start of the frame		another specific Pattern at the end of the frame

Data Link Layer Standards

Standard organization	Networking Standards
IEEE	•802.2: Logical Link Control (LLC) •802.3: Ethernet •802.4: Token bus •802.5: Token passing •802.11: Wireless LAN (WLAN) & Mesh (Wi-Fi certification) •802.15: Bluetooth 802.16: WiMax
ITU-T	•G.992: ADSL •G.8100 - G.8199: MPLS over Transport aspects •Q.921: ISDN Q.922: Frame Relay
ISO	•HDLC (High Level Data Link Control) •ISO 9314: FDDI Media Access Control (MAC)
ANSI	•X3T9.5 and X3T12: Fiber Distributed Data Interface (FDDI)

Common Physical WAN Topologies

1. Point-to-Point Topology (2 nodes only)
2. Hub and spoke topology
3. Full Mesh topology

Logical Point-to-Point Topology

Source Node -> Frames -> logical ptp connection -> Frames -> Destination Node

Adding intermediate physical connections may not change the logical topology.

The logical point-to-point connection is the same.

half and Full Duplex

Half: only the server can send to the switch

Full : the server and switch can send and receive

LAN Topologies

Physical LAN Topologies

1. Star 2. Extended Star 3. Bus 4. Ring

Logical Topology for Shared Media

1. Contention-Based Access

Characteristics	Contention-Based Technologies
•Stations can transmit at any time •Collision exist •There are mechanisms to resolve contention for the media	•CSMA/CD for 802.3 Ethernet networks •CSMA/CA for 802.11 wireless networks

2. Controlled Access

Characteristics	Contention-Based Technologies
•Only one station can transmit at a time •Devices wanting to transmit must wait their turn •No collisions •May use a token passing method	•Token Ring (IEEE 802.5) •FDDI

Data Link Frame

The Frame

In a fragile environment, more controls are needed to ensure delivery. The header and trailer fields are larger as more control information is needed.

(Greater effort needed to ensure delivery = higher overhead = slower transmission rates)

In a protected environment, we can count on the frame arriving at its destination. Fewer controls are needed, resulting in smaller fields and smaller frames.

(Less effort needed to ensure delivery = lower overhead = faster transmission rate)

The Header and The Trailer

Header Content

Start Frame	Address	Type/Length

Trailer Content

FCS	Stop Frame
This field is used for error checking. The source calculates a number based on the frame's data and places that number in the FCS field. The destination then recalculates the data to see if the FCS matches. If they don't match, the destination deletes the frame.	This field, also called the Frame Trailer, is an optional field that is used when the length of the frame is not specified in the Type/Length field. It indicates the end of the frame when transmitted.

Ethernet Frame

A common data link layer protocol for LANs

Field Name	Size
Preamble	8
Destination	6

Field Name	Size
Source	6
Type	2
Data	46-1500
Frame Check Sequence	4

Preamble - Used for synchronization; also contains a delimiter to mark the end of the timing information
Destination Address - 48-bit MAC address for the destination node
Source Address - 48-bit MAC address for the source node
Type - Value to indicate which upper layer protocol will receive the data after the Ethernet process is complete
Data or payload - This is the PDU, typically an IPv4 packet, that is to be transported over the media.
Frame Check Sequence (FCS) - A value used to check for damaged frames

---

Point-to-Point Protocol Frame

A common data link layer protocol for LANs

Field Name	Size
Flag	1
Address	1
Control	1
Protocol	2
Data	Var
Frame Check Sequence	2-4

Flag - A single byte that indicates the beginning or end of a frame. The flag field consists of the
binary sequence 01111110.
Address - A single byte that contains the standard PPP broadcast address. PPP does not assign individual station addresses.
Control - A single byte that contains the binary sequence 00000011, which calls for transmission of user data in an unsequenced frame.
Protocol - Two bytes that identify the protocol encapsulated in the data field of the frame.

The
most up-to-date values of the protocol field are specified in the most recent Assigned Numbers
Request For Comments (RFC).
Data - Zero or more bytes that contain the datagram for the protocol specified in the protocol field.
Frame Check Sequence (FCS) - Normally 16 bits (2 bytes). By prior agreement, consenting PPP implementations can use a 32-bit (4-byte) FCS for improved error detection.

Chapter 5

Ethernet Protocol

Ethernet: One of the most widely used LAN technologies ,Operates in the data link layer and the physical layer ,Family of networking technologies that are defined in the IEEE 802.2 and 802.3 standards

Supports data bandwidths

1. 10 Mbps
2. 100 Mbps
3. 1000 Mbps
4. 10,000 Mbps
5. 40,000 Mbps
6. 100,000 Mbps (100 Gbps)

Ethernet Standards

Define Layer 2 protocols and Layer 1 technologies

Two separate sub layers of the data link layer to operate – Logical link control (LLC) and the MAC sublayers.

LLC:

Handles communication between upper and lower layers.

Takes the network protocol data and adds control information to help deliver the packet to the destination.

MAC Suplayer

Constitutes the lower sublayer of the data link layer.

Implemented by hardware, typically in the computer NIC.

Two primary responsibilities:
1. Data encapsulation
2. Media access control

Data encapsulation

Frame assembly before transmission and frame disassembly upon reception of a frame.

MAC layer adds a header and trailer to the network layer PDU.

Provides three primary functions:

1. Frame delimiting – Identifies a group of bits that make up a frame, synchronization between the transmitting and receiving nodes.
2. Addressing – Each Ethernet header added in the frame contains the physical address (MAC address) that enables a frame to be delivered to a destination node.
3. Error detection – Each Ethernet frame contains a trailer with a cyclic redundancy check (CRC) of the frame contents.

MAC

Responsible for the placement of frames on the media and the removal of frames from the media

Communicates directly with the physical layer

If multiple devices on a single medium attempt to forward data simultaneously, the data will collide resulting in corrupted, unusable data

Ethernet provides a method for controlling how the nodes share access through the use a Carrier Sense Multiple Access (CSMA) technology

Physical Layer

Logical Link Control Sublayer							
802.3 Media Access Control							
Physical Signaling Sublayer	10BASE5 (500m) 50 Ohm	10BASE2 (185m) 50 Ohm	10BASE-T (100m)	100BASE-TX (100m)	1000BASE-CX (25m) 150 Ohm	1000BASE-T (100m)	1000 ST (2 550m

Logical Link Control Sublayer							
/ Physical Medium	Coax N-Style	Coax BNC	100 Ohm UTP RJ-45	100 Ohm UTP RJ-45	STP mini-DB-9	100 Ohm UTP RJ-45	MM F SC

Carrier Sense Multiple Access (CSMA) process

Used to first detect if the media is carrying a signal

If no carrier signal is detected, the device transmits its data

If two devices transmit at the same time - data collision

Contention-Based Access

- Stations can transmit at any time
- Collisions exist
- Mechanisms exist to resolve contention problems
- CSMA/CD for Ethernet networks
- CSMA/CA for 802.11 wireless networks

i.e :

1. Ethernet
2. Wireless

CSMA is usually implemented in conjunction with a method for resolving media contention. The two commonly used methods are: CSMA/Collision Detection and CSMA/Collision Avoidance

CSMA/Collision Detection:

- The device monitors the media for the presence of a data signal
- If a data signal is absent, indicating that the media is free, the device transmits the data
- If signals are then detected that show another device was transmitting at the same time, all devices stop sending & try again later
- While Ethernet networks are designed with CSMA/CD technology, with today's intermediate devices, collisions do not occur and the processes utilized by CSMA/CD are really unnecessary

- Wireless connections in a LAN environment still have to take collisions into account

CSMA/Collision Avoidance (CSMA/CA) media access method

- Device examines the media for the presence of data signal - if the media is free, the device sends a notification across the media of its intent to use it
- The device then sends the data.
- Used by 802.11 wireless networking technologies

MAC Address: Ethernet Identity

Layer 2 Ethernet MAC address is a 48-bit binary value expressed as 12 hexadecimal digits.

IEEE requires a vendor to follow these rules:
1. Must use that vendor's assigned OUI as the first 3 bytes.
2. All MAC addresses with the same OUI must be assigned a unique value in the last 3 bytes.

The Ethernet MAC Address Structure

Organizationally Unique Identifier (OUI)	**Vendor Assigned (NIC, Interfaces)**
24 bits	24 Bits
6 hex digits	6 hex digits
00-60-2F	3A-07-BC
Cisco	particular device

Frame Processing

MAC addresses assigned to workstations, servers, printers, switches, and routers.

Example MACs:
- 00-05-9A-3C-78-00
- 00:05:9A:3C:78:00
- 0005.9A3C.7800.

When a device is forwarding a message to an Ethernet network, attaches header information to the packet, contains the source and destination MAC address.

Each NIC views information to see if the destination MAC address in the frame matches the device’s physical MAC address stored in RAM.

No match, the device discards the frame.

Matches the destination MAC of the frame, the NIC passes the frame up the OSI layers, where the de-encapsulation process takes place.

Ethernet Encapsulation

Early versions of Ethernet were slow at 10 Mb/s.

Now operate at 10 Gb/s per second and faster.

Ethernet frame structure adds headers and trailers around the Layer 3 PDU to encapsulate the message being sent.

Ethernet II: the Ethernet frame format used in TCP/IP networks.

802.3 vs II Frame Structure and Size Field

IEE 802.3

7 Bytes	**1**	**6**	**6**	**2**	**46 to 1500**	**4**
Preamble	Start of Frame Delimiter	Destination Address	Source Address	Length	802.2 Header and Data	Frame Check Sequence

Preamble and Start Frame Delimiter Fields :Used for synchronization between the sending and receiving devices.

Length/Type Field: Defines the exact length of the frame's data field; describes which protocol is implemented.

Data and Pad Fields : Contains the encapsulated data from a higher layer, an IPv4 packet

Ethernet II

8	**6**	**6**	**2**	**46 to 1500**	**4**
Preamble	Destination Address	Source Address	Type	Data	Frame Check Sequence

Frame Check Sequence Field: Used to detect errors in a frame with cyclic redundancy check (4 bytes); if calculations match at source and receiver, no error occurred.

Ethernet II and IEEE 802.3 standards define the minimum frame size as 64 bytes and the maximum as 1518 bytes

Less than 64 bytes in length is considered a "collision fragment" or "runt frame”

If size of a transmitted frame is less than the minimum or greater than the maximum, the receiving device drops the frame

At the physical layer, different versions of Ethernet vary in their method for detecting and placing data on the media

extra 4 bytes allow for QoS and VLAN Tech

Destination Address	Source Address	802.1Q VLAN Tag	Type/len	Data	Frame Check

802.1Q VLAN Tag's 4 bytes are used

2 bytes for Tag Protocol ID 0x8100

and 2 bytes for

1. User Priority (3 Bits)
2. Canonical Format Indicator (1 Bit)
3. VLAN ID (12 Bits)

Decimal	Binary	Hexadecimal
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F
16	0001 0000	10

Decimal	Binary	Hexadecimal
32	0010 0000	20
64	0100 0000	40
128	1000 0000	80
192	1100 0000	C0
202	1100 1010	CA
240	1111 0000	F0
255	1111 1111	FF

Multicast MAC address is a special value that begins with 01-00-5E in hexadecimal

Range of IPV4 multicast addresses is 224.0.0.0 to 239.255.255.255

MAC and IP

MAC Address:

- does not change
- Similar to the name of a person
- Known as physical address because physically assigned to the host NIC

IP Address:

- Similar to the address of a person
- Based on where the host is actually located
- Known as a logical address because assigned logically
- Assigned to each host by a network administrator

Both are required for a computer to communicate just like both the name and address of a person are required to send a letter.

IP Packet Encapsulated in an Ethernet Frame

Destination MAC Address BB:BB:BB:BB:BB:BB	Source MAC Address AA:AA:AA:AA:AA:AA	Source IP Address 10.0.0.1	Destination IP Address 192.168.1.5	Data	Trailer
A swtich examins the mac address		A router examins the ip address			

The Data Link Layer

Data link layer protocols govern how to format a frame for use on different media.

Different protocols may be in use for different media.

At each hop along the path, an intermediary device accepts frames from one medium, de-encapsulates the frame and then forwards the packets in a new frame. The headers of each frame are formatted for the specific medium that it will cross.

Address Resolution Protocol

Introduction to ARP

Purpose: Sending node needs a way to find the MAC address of the destination for a given Ethernet link

Provides two basic functions:

1. Resolving IPv4 addresses to MAC addresses
2. Maintaining a table of mappings

ARP Table

Used to find the data link layer address that is mapped to the destination IPv4 address.

As a node receives frames from the media, it records the source IP and MAC address as a mapping in the ARP table.

ARP Request

Layer 2 broadcast to all devices on the Ethernet LAN.

The node that matches the IP address in the broadcast will reply.

If no device responds to the ARP request, the packet is dropped because a frame cannot be created.

Note:

Static map entries can be entered in an ARP table, but this is rarely done.

ARP Role in Remote Communication

- If the destination IPv4 host is on the local network, the frame will use the MAC address of this device as the destination MAC address.
- If the destination IPv4 host is not on the local network, the source uses the ARP process to determine a MAC address for the router interface serving as the gateway.
- In the event that the gateway entry is not in the table, an ARP request is used to retrieve the MAC address associated with the IP address of the router interface.

Removing Entries from an ARP Table

- The ARP cache timer removes ARP entries that have not been used for a specified period of time.
- Commands may also be used to manually remove all or some of the entries in the ARP table.

How ARP Can Create Problems

- ARP broadcasts can flood the local media
- Can Lead to some issues like
    1. Broadcast overhead on the media
    2. security

LAN Switches

Layer 2 Fundamentals

- Connects end devices to a central intermediate device on most Ethernet networks
- Performs switching and filtering based only on the MAC address
- Builds a MAC address table that it uses to make forwarding decisions
- Depends on routers to pass data between IP subnetworks

Switch MAC Address Table

1. The switch receives a broadcast frame from PC 1 on Port 1.

2. The switch enters the source MAC address and the switch port that received the frame into the address table.

3. Because the destination address is a broadcast, the switch floods the frame to all ports, except the port on which it received the frame.

4. The destination device replies to the broadcast with a unicast frame addressed to PC 1.

5. The switch enters the source MAC address of PC 2 and the port number of the switch port that received the frame into the address table. The destination address of the frame and its associated port is found in the MAC address table.

6. The switch can now forward frames between source and destination devices without flooding, because it has entries in the address table that identify the associated ports.

Duplex Settings

1. Half Duplex (CSMA/CD)

- Unidirectional data flow
- Higher potential for collision
- Hub connectivity

2. Full Duplex

- Point-to-point only
- Attached to dedicated switched port
- Requires full-duplex support on both ends
- Collision-free
- Collision detect circuit disabled

Auto-MDIX

Auto detects the type of connection required and configures the interface accordingly

---

Frame Forwarding Methods on Cisco Switches

1. Store-and-forward:
   Receives the entire frame, and computes the CRC. If the CRC is valid, the switch looks up the destination address, which determines the outgoing interface. The frame is then forwarded out the correct port.
2. Cut-through:
   Forwards the frame before it is entirely received. At a minimum, the destination address of the frame must be read before the frame can be forwarded.
3. Fast-forward switching:
   Lowest level of latency immediately forwards a packet after reading the destination address, typical cut-through method of switching

4. Fragment-free switching:
   Switch stores the first 64 bytes of the frame before forwarding, most network errors and collisions occur during the first 64 bytes

---

Memory Buffering on Switches

1. Port-based memory:
   In port-based memory buffering, frames are stored in queues that are linked to specific incoming and outgoing ports.
2. Shared memory:
   Shared memory buffering deposits all frames into a common memory buffer, which all the ports on the switch share.

Fixed versus Modular Configuration

1. Fixed Configuration Switches: Features and options are limited to those that originally come with the switch.
2. Modular Configuration Switches: The chassis accepts line cards that contain the ports.
3. Stackable Configuration Switches

Module Options for Cisco Switch Slots

1. Cisco Optical Gigabit Ethernet SFP
2. Cisco 1000BASE-T Copper SFP
3. Cisco 2-channel 1000BASE-BX Optical SFP

Cisco Express Forwarding

Cisco devices which support Layer 3 switching utilize Cisco Express Forwarding (CEF). Two main components of CEF operation are the:

1. Forwarding Information Base (FIB)
   - Conceptually it is similar to a routing table.
   - A networking device uses this lookup table to make destination-based switching decisions during Cisco Express Forwarding operation.
   - Updated when changes occur in the network and contains all routes known at the time.

2. Adjacency Tables
    - Maintain layer 2 next-hop addresses for all FIB entries.

The major types of Layer 3 interfaces are:

1. Switch Virtual Interface (SVI) – Logical interface on a switch associated with a virtual local-area network (VLAN).
2. Routed Port – Physical port on a Layer 3 switch configured to act as a router port. Configure routed ports by putting the interface into Layer 3 mode with the no switchport interface configuration command.
3. Layer 3 EtherChannel – Logical interface on a Cisco device associated with a bundle of routed ports.

Chapter 6

The Network Layer

provides services to allow end devices to exchange data across the network.

To accomplish this end-to-end transport, the network layer uses four basic processes:

1. Addressing end devices
2. Encapsulation
3. Routing
4. De-encapsulating

Common network layer protocols include:

1. IP version 4 (IPv4)
2. IP version 6 (IPv6)

Legacy network layer protocols include:

1. Novell Internetwork Packet Exchange (IPX)
2. AppleTalk
3. Connectionless Network Service (CLNS/DECNet)

Connectionless IP

No connection is established before sending data packets.

The sender doesn't know:

- if the receiver is present

- if the letter arrived
- if the receiver can read the letter

The receiver doesn't know:

- when it is coming

Best Effort (unreliable)

No overhead is used to guarantee packet delivery.

Packets are routed through the network quickly.

Some packets may be lost en route.

As an unreliable network layer protocol, IP does not guarantee that all sent packets will be received. Other protocols manage the process of tracking packets and ensuring their delivery.

Media Independent

Operates independently of the medium carrying the data.

- ip packets can travel through different media

IPv4 Packet Header

Contents of the IPv4 packet header

Byte 1:

1. Version
2. Internet Header Length
3. Identification
4. Time-to-Live
5. Source IP Address
6. Destination IP Address
7. Options (optional)

Byte 2:

1. Differentiated Services (DS)
2. DSCP
3. ECN

4. Identification
5. Protocol
6. Source IP Address
7. Destination IP Address
8. Options (optional)

Byte 3:

1. Total Length
2. Flag
3. Fragment Offset
4. Header Checksum
5. Source IP Address
6. Destination IP Address
7. Options (optional)
8. Padding

Byte 4:

1. Total Length
2. Flag
3. Fragment Offset
4. Header Checksum
5. Source IP Address
6. Destination IP Address
7. Padding

Contents of the IPv4 header files

Byte 1:

1. Intemet Header Length
2. Identification

Byte 2:

1. Identification

Byte 3 + 4:

1. Total Length
2. Flags (3 only)
3. Fragment Offset (4 only)
4. Header Checksum

Limitations of IPv4

1. IP Address depletion 2. Internet routing table expansion 3. Lack of end-to-end connectivity

---

IPv6

1. Increased address space
2. Improved packet handling
3. Eliminates the need for NAT
4. Integrated security
5. 4 billion IPv4 addresses (4,000,000,000)
6. 340 undecillion IPv6 addresses (340,000,000,000,000,000,000,000,000,000,000,000,000)

Field names kept from IPv4 to IPv6

1. Version 2. Source Address 3. Destination Address

Fields not kept in IPv6

1. IHL 2. Identification 3. Flags 4. Fragment Offset 5. Header Checksum 6. Options 7. Padding

Name & position changed in IPv6

Old 1. Type of Service 2. LengthTotal 3. Time to Live 4. Protocol

New

1. Traffic Class
2. Payload Length
3. Next Header
4. Hop Limit

New field in IPv6

1. Flow Label

IPv6 Packet Header

Byte 1: 1. Version 2. Traffic Class 3. Payload Length 4. Source IP Address 5. Destination IP Address

byte 2:

1. Traffic Class
2. Payload Length
3. Source IP Address
4. Destination IP Address

byte 3+4:

1. Flow Label
2. Next Header (3 only)
3. Hop Limit
4. Source IP Address
5. Destination IP Address

Routing

Default Gateway

- Hosts must maintain their own, local, routing table to ensure that network layer packets are directed to the correct destination network.
- The local table of the host typically contains
    1. Direct connection
    2. Local network route
    3. Local default route

Routers

Router Memory

Memory	Volatile / Non-Volatile	Stores
RAM	Volatile	1. Running IOS 2. Running configuration file 3. IP routing and ARP tables 4. Packet buffer

Memory	Volatile / Non-Volatile	Stores
ROM	Non-Volatile	1. Bootup instructions 2. Basic diagnostic software 3. Limited IOS
NRAM	Non-Volatile	1. Startup configuration file
Flash	Non-Volatile	1. IOS 2. Other system files

Components of a router

1. Power Supply 2. Shield for WIC 3. Fan 4. SDRAM 5. NVRAM 6. CPU 7. Advanced Integration Module (AIM)

Router Backplane

1. Double-Wide EHWIC slots 2. Two 4 GB Flash Card Slots 3. EHWIC 0 4. Console USB Type B 5. AUX Port 6. Console RJ45 7. LAN Interface 8. USB Ports

to connect to a router we can use

1. WAN Interface (Serial Interfaces)
2. Console USB Type B
3. Console RJ45
4. AUX Port
5. LAN Interface

Cisco IOS

it's operational details vary on different internetworking devices, depending on the device’s purpose and feature set.

Cisco IOS for routers provides the following::

1. Addressing
2. Interfaces
3. Routing
4. Security
5. QoS
6. Resources Management

Router Boot Process

1. ROM (Read-Only Memory)

- **POST (Power-On Self-Test)**: Perform POST

2. ROM

- **Bootstrap**: Load bootstrap

3. Flash + TFTP Server

- **Cisco Internetwork Operating System (IOS)**: Locate and load operating system

4. NVRAM + TFTP Server + Console

- **Configuration**: Locate and load configuration file or enter "setup mode"