Network Fundamentals Full Notes

Network Fundamentals (University of Technology Sydney)

INTRODUCTION TO NETWORKS

CHAPTER 1 – Exploring the Network

1.1 Globally Connected

Networking Today

No Boundaries

- The immediate nature of communications over the internet encourages the creation of global communities – independent of location or time zone
- The human network → centres on the impact of the internet and networks on people and business

Networks Support the Way We Learn

- Access to high quality instruction not limited to proximity
- Removed geographic barriers + ↑ student opportunity

Networks Support the Way We Communicate

- Forms of Communication:
  - Texting
  - Social Media
  - Collaboration Tools
  - Blogs
  - Wikis
  - Podcasting
  - Peer-to-Peer (P2P) File Sharing

Networks Support the Way We Work

- Efficient and cost-effective
- Online learning ↓ time and cost

Networks Support the Way We Play

- Internet created online games + add to gaming experience

Providing Resources in a Network

Networks of Many Sizes

- Networks allow for sharing of resources
- Consolidation of storage and access to information
- The internet is the largest network

Clients and Servers

- Hosts: End devices. Computers connected to a network that participate directly in network communication
- Servers: Computers with software that enable them to provide information to other end devices. Provide services simultaneously to many clients.
- Clients: computers with software that enables them to request and display information obtained from the server.
  - Web Client and Server: The Web Server runs web server software and clients use their browser software (Windows, IE) to access web pages on the server.
  - File Client and Server: The File Server stores corporate and user files in a central location. The client devices access these files with client software (Windows Explorer)
  - Email Client and Server: The Email Server runs email server software and clients user their mail client software (Microsoft Outlook) to access email on the server

Peer-to-Peer

- Client and server software running on one computer to carry out both roles at the same time.

ADVANTAGES	DISADVANTAGES
+ Easy to set up + Less complexity + Lower cost since network devices and dedicated servers may not be required + Can be used for simple tasks such as transferring files and sharing printers	– No centralized administration – Not as secure – Not scalable – All devices may act as both clients and servers which can slow their performance

1.2 LANs, WANs and the Internet

Network Components

Overview of Network Components

- Network infrastructure
  - Devices – hardware, visible components of the network platform.
  - Media – hardware, eg. Laptop, PC, switch, router, WAP, cabling.
  - Services – common network applications (email, web hosting). Provide functionality that directs and moves the messages through the network.

End Devices

- End Device examples
  - Desktop computer
  - Laptop
  - IP Phone
  - Tablet
  - Printer
  - Interactive whiteboard
- Either source or destination
- Each end device is distinguished by an address → when ED initiates communication, uses address of destination

Intermediary Network Devices

- Connect individual ED to the network and can connect multiple individual networks to form an internetwork
- Provide connectivity and ensure data flow
- Use destination and device address + information about network interconnections to determine path for message
- Intermediary device examples
  - Wireless router
  - LAN switch
  - Firewall appliance
  - Multilayer switch
  - Router
- IND perform (some/ all) these functions
  - Regenerate and retransmit data signals
  - Maintain information about what pathways exist through the network
  - Notify other devices of errors and communication failures
  - Direct data along alternate pathways when there is a link failure
  - Classify and direct messages according to priorities
  - Permit or deny flow of data (based on security settings)

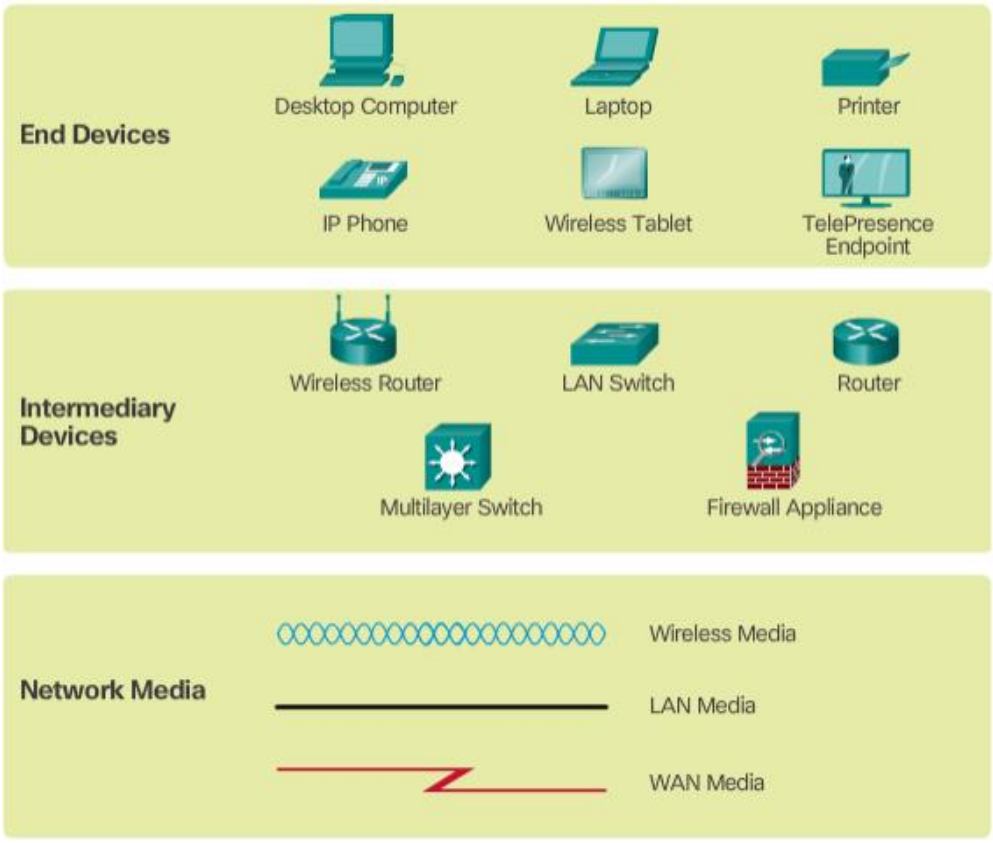
Network Media

- 3 types of media to interconnect devices + provide pathway for transmission
  - Metallic Wires → data encoded into electrical impulses
  - Glass or Plastic → data encoded as pulses of light
  - Wireless → data encoded using wavelengths from the electromagnetic spectrum
- What to use and when?
  - What is the maximum distance the media can successfully carry a signal?
  - Into what type of environment will the media be installed?
  - What is the amount of data and the speed at which it must be transmitted?
  - What is the cost of the media and installation?

Network Representations

- Terms:
  - Network Interface Card (NIC): Or LAN adapter, provides physical connection to the network from PC or other ED.
  - Physical Port: Connector or outlet on networking device where the media is connected to ED or other networking device.
  - Interface: Specialised ports on a networking device that connect to individual networks. Ports on a router are referred to as network interfaces.

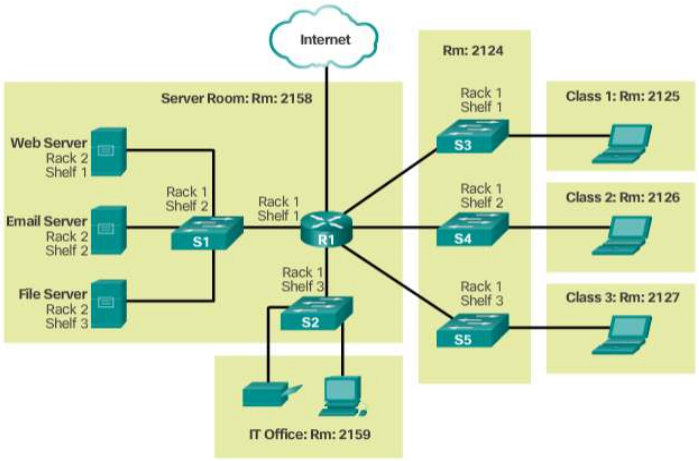
TOPOLOGY DIAGRAM SYMBOLS



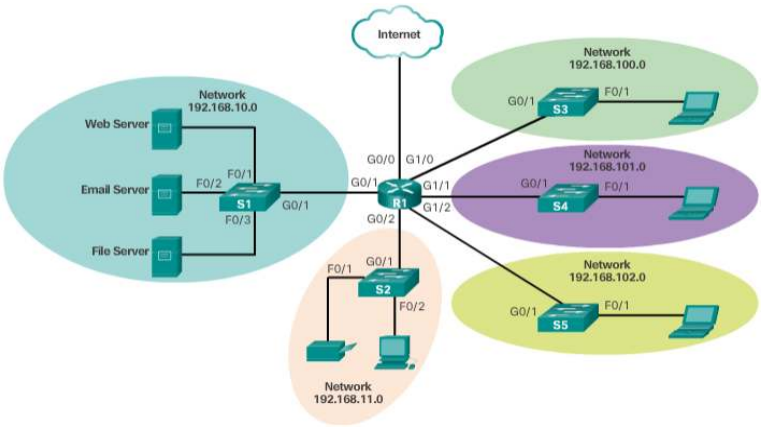
Topology Diagrams

- Visual Map of how the network is connected
- 2 types:
  - Physical → identify the physical location of ID and cable installation
  - Logical → identify devices, ports, and addressing scheme.

PHYSICA



LOGICAL



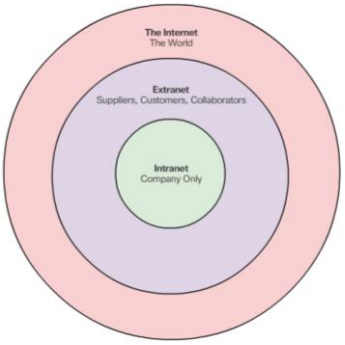
LANs and WANs

Types of Networks

- Infrastructure can vary greatly (Size of area, number of users, numbers of services, etc.)
- Local Area Network (LAN): Network infrastructure that provides access to users and ED in a small geographical area.
    - LANs interconnect ED in a limited area → home, school, office, campus.
    - Usually administered by a single org/ individual
    - Provide high speed bandwidth to internal ED and ID
- Wide Area Network (WAN): Network infrastructure that provides access to other networks over a wide geographical area.
    - WANs interconnect LANs over a wide geographical area → cities, states, provinces
    - Usually administered by multiple Service Providers or Internet Service Providers
    - Typically slower speed links between LANS
- Metropolitan Area Network (MAN): Network infrastructure that spans a physical area larger than a LAN but smaller than a WAN.
- Wireless LAN (WLAN): Similar to a LAN but wirelessly interconnects users and end points in a small geographical area.
- Storage Area Network (SAN): Network Infrastructure designed to support file servers and provide data storage, retrieval and replication.

The Internet, Intranets, and Extranets

The Internet



- Worldwide collection of interconnected networks
- Interconnection of LANs and WANs
- Organizations that help to maintain structure and standardization of Internet protocols and processes:
    - Internet Engineering Task Force (IETF)
    - Internet Corporation for Assigned Names and Numbers (ICANN)
    - Internet Architecture Board (IAB), plus many others.

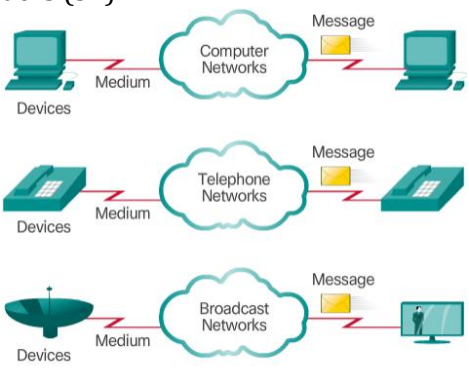
Intranets & Extranets

- Intranet: A private connection of LANs and WANs that belongs to an organisation, designed to be accessible only by the organisation's members, employees, or others with authorisation.
- Extranet: May be used by an organisation to provide secure and safe access to individuals who work for a different organisation, but require access to the organisation's data
    - A company providing access to outside suppliers and contractors.
    - A hospital providing a booking system to doctors to make appointments for patients.
    - A local office of education providing budget and personnel information to the schools in its district.

Internet Connections

Internet Access Technologies

- Home users, teleworkers (remote workers), and small offices typically require a connection to an Internet Service Provider (ISP)
    - Broadband cable, broadband (DSL), wireless WANs, and mobile services.
- Business-class interconnections are usually provided by service providers (SP)
    - Popular business-class services include business DSL, leased lines, and Metro Ethernet.



Home and Small Office Internet Connections

- Cable
    - Offered by cable television SPs
    - Internet data signal is carried on the same cable that delivers cable TV
    - High bandwidth
- DSL
    - Digital Subscriber Line
    - High bandwith
    - Runs over telephone line
    - Asymmetrical DSL → download speed is faster than the upload speed
- Cellular
    - Uses cell phone network → wherever there is a signal, internet is available
    - Performance is limited to phone capabilities and the cell tower it is connected to
- Satellite
    - Satellite dishes require clear line of sight to the satellite
    - Benefit to areas where internet connevity is low/ none
- Dial-Up Telephone
    - Any phone line and modem
    - Inexpensive
    - Low bandwidth
    - Not sufficient for large data transfer
    - Useful for mobile access while traveling
- Homes and small offices are more commonly being connected directly with fiber optic cables → enables an ISP to provide higher bandwidth speeds and support more services

Businesses Internet Connections

- Dedicated Leased Line
    - Reserved circuits within the SPs network
    - Connect geographically separated offices for private voice and data networking
    - Rented monthly/ yearly
    - Expensive
- Ethernet WAN
    - Extend LAN access technology into the WAN
- DSL
    - Business DSL
        - Symmetric Digital Subscriber Lines (SDSL)
        - Provides uploads and downloads at the same speeds
- Satellite
    - Provides connection when a wired solution is unavailable

1.3 The Network as a Platform

Converged Networks

Traditional Separate Networks

- Traditionally, separate networks could not communicate with each other.

The Converging Network

- Unlike dedicated networks → capable of delivering data, voice, and video between different types of devices over the same network infrastructure.

Reliable Network

Network Architecture

- The technologies that support the infrastructure and the programmed services and rules/ protocols that move data around the network.

Characteristics:

- Fault Tolerance
  - Limits the impact of failure so fewer devices are affected
  - Quick recovery
  - Multiple message paths
  - Implementation of a packet-switched network → a single message is broken into multiple message blocks
  - Circuit-switched network → the opposite – a dedicated circuit between source and destination
- Scalability
  - Can expand quickly to support new users and applications without impacting the performance of the service being delivered to users
  - New network can be added to the existing one
  - Following protocol so that everyone has the same rules
- Quality of Service (QoS)
  - Primary mechanism for managing congestion and ensuring reliable delivery of content
  - Demand for excessive network bandwidth + volume of traffic is greater than what can be transported across the network → creates network congestion
- Security
  - Network infrastructure security + information security
  - Physical security of devices + preventing unauthorised access
  - Protecting information
  - Confidentiality (only intended + authorised recipients have access), Integrity (assurance that the information has not been tampered with), Availability (assurance of timely and reliable access to data services).

1.4 The Changing Network Environment

Network Trends

New Trends

- Bring Your Own Device (BYOD)
  - Users having the freedom to use personal tools to access the information and communicate across a business/ campus network
  - ↑ in consumer devices & ↓ in cost = expected use
  - Eg. Laptops, notebooks, tablets, smartphones, e-readers
  - Any device, with any ownership, used anywhere
  - Flexibility in learning options
- Online Collaboration
  - Collaboration tools – Eg. Cosco WebEx
  - Instantly connect, interact + achieve objectives
  - Businesses - Critical + strategic priority to remain competitive
  - Education – assist each other in learning, develop team skills, work together on group based projects.
- Video Communication
  - For communication, entertainment and collaboration
  - Anywhere with network connection
  - Video conferencing – powerful tool

    - Becoming a critical requirement for effective collaboration
- Cloud Computing
    - Changing the way we access and store data
    - Allows storage and backup of files over the internet
    - Use of applications
    - Extends IT's capabilities without requiring investment in new infrastructure, training new personnel, or licensing new software
    - Possible due to data centres
    - Types of Clouds
        - Public → Available to general population, may be free or pay-per-use, uses the internet to provide services.
        - Private → intended for a specific organisation/ entity eg. Government, can be expensive to maintain, can be managed by outside org.
        - Custom → built to meet the needs of a specific industry, can be private or public.
        - Hybrid → made up of two or more clouds (part custom, part public), each part remains a distinctive object, both connected using a single architecture, users have differing degrees of access based on access rights

Networking Technologies for the Home

Technology Trends in the Home

- 'Smart home technology' → integrated into everyday appliances to make them more automated
- Smart home technology will become more of a reality as home networking and high-speed Internet technology becomes more widespread.

Powerline Networking

- Emerging trend for home networking that uses existing electrical wiring to connect devices
- Concept of 'no new wires' → ability to connect device to the network (LAN) wherever there is an electrical outlet
- Saves cost of installing data cable without additional cost
- Sends information by sending data on certain frequencies
- Useful when wireless is unavailable
- Not designed to be a substitute – an alternative when data network cables/ wireless are not a viable option

Wireless Broadband

- Wireless Internet Service Provider (WISP)
    - ISP that connects subscribers to a designated access point/ hot spot using similar technologies such as WLANs.
    - Commonly found in rural environments where DSL/ cable services are unavailable
    - Antenna is attached to existing elevated structure → dish on roof
- Wireless Broadband Service
    - Same cellular technology
    - Antenna installed outside the house
    - Wired/ wireless connectivity for devices
    - Home wireless broadband competes directly with DSL and cable services

Network Security

Security Threats

1. Network security implemented must take into account the environment, tools and requirements of the network
2. Secure data whilst still allowing QoS that is expected
3. Involves protocols, technologies, devices, tools and techniques to mitigate threats
4. Threat vectors may be internal or external
5. Common external threats:
    - Viruses, worms and Trojan horses

- Spyware and adware
- Zero-day attacks/ Zero-hour attacks
- Hacker attacks
- Denial of Service attacks
- Data interception and theft
- Identity theft

6. Internal
    - Lost/ stolen devices
    - Accidental/ purposeful misuse by employees
    - BYOD – corporate data is more vulnerable

Security Solutions

- Multiple layers
- Home → end devices, point of connection, contracted services from the ISP
- Business → many components built into the network to monitor and filter traffic
- Security components:
    - Antivirus spyware
    - Firewall filtering
    - Dedicated firewall systems
    - Access Control Lists (ACL)
    - Intrusion prevention Systems (IPS)
    - Virtual Private Networks (VPN)
- Take into account environment, applications and computing requirements
- Must be adaptable to the growing trends

CHAPTER 2 – Configure a Network Operating System

2.1 IOS Bootcamp

Cisco IOS

Operating Systems

- A Network Operating System (NOS) enables hardware to function and provides an interface for users to interact.
- Kernel, shell, hardware
- CLI → user interacts directly with system in text-based environment by entering commands
- GUI → interact using graphical icons, menus and windows
- Network devices are typically accessed through CLI (less chance of failure or wrong command executed, more stable)
- OS on home routers is called firmware

Purpose of OS

- Enables the user to:
  - Make selections and run programs
  - Enter text-based commands
  - View output on a monitor

Cisco IOS Access

Access Methods

- Cisco IOS switch can switch data between connected devices → devices instantly have connectivity with one another
  Common methods to access CLI + configure the device:
- Console:
  - Physical management port that provides out-of-band access to device (access via a dedicated management channel that is used for device maintenance purposes only).
  - Advantage: using a console port is that the device is accessible even if no networking services have been configured (eg. When performing initial config.)
- Secure Shell (SSH):
  - Remotely establishing a secure CLI connection through a virtual interface, over a network.
  - Requires active networking services on the device including an active interface configured with an address.
  - Recommended method for remote management → a secure connection
  - Provides encrypted password authentication and transport of session data (keeps data private)
  - Best practice is to use SSH for remote management CLI connections
- Telnet:
  - Insecure method of remotely establishing a CLI session through a virtual interface over a network
  - Does not provide a securely encrypted connect
  - Authentication is sent over the network in plain text
- Some devices may also support a legacy auxiliary port that was used to establish a CLI session remotely using a modem. The AUX port is out-of-band and does not require networking services to be configured/ available.

Terminal Emulation Programs

- Available programs for connecting to a networking device:
  - PuTTY
  - Tera Term
  - SecureCRT
  - OS X Terminal

Navigate the IOS

Primary Command Modes

Management access is separated into two command modes:

- User EXEC Mode:
  - Has limited capabilities but useful for basic operations.
  - Allows limited number of basic monitoring commands
  - Often referred to as a 'view-only' mode.
  - Identified by the CLI prompt that ends with the ">"
- Privileged EXEC Mode:
  - Access to all commands and features
  - The user can use any monitoring commands and execute configuration and management commands
  - To execute configuration commands, a network admin must access this mode
  - Higher configuration modes (eg. Global config mode)
  - Identified by the CLI prompt ending with "#" symbol.

Configuration Command Modes

- From Global Config Mode (GCM) CLI configuration changes that are made affect the operation of the device as a whole.
- Identified by a prompt that ends with "(config)#" after the device name
- Accessed before other specific config modes → user can enter other different sub-configuration modes
  - Line Configuration Mode → configures console, SSH, telnet, AUX ("Switch(config-line)#")
  - Interface Configuration Mode → configures switch port or router network interface ("Switch(config-if)#")
- When using CLI, the mode is identified by the command-line prompt

Navigate between IOS Modes

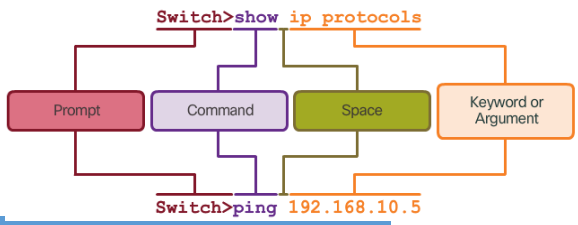
- Commands are used to move in and out of command prompts
  - User EXEC → privileged EXEC ~ *enable* command
-
  - privileged EXEC → user EXEC ~ *disable* command
  - privileged EXEC → GCM ~ *configure terminal*
  - GCM → privileged EXEC ~ *exit* command
  - GCM → Line sub-config mode ~ *line* command + *management line type & number*
  - Sub-config mode → GCM ~ *exit* command
  - Sub-config mode → privileged EXEC ~ *end* command + *ctrl+Z*
  - Sub-config mode → Sub-config mode ~ *name of configuration mode*

The Command Structure

Basic IOS Command Structure

- General syntax for a command → command followed by any appropriate keywords and arguments
  - Keyword: specific parameter defined in the OS
  - Argument: (not predefined) a value/ variable defined by the user

IOS Command Syntax



Command Conventions	
Convention	**Description**
boldface	Indicates commands and keywords that you enter literally as shown
italics	Indicates arguments for which you supply values
[x]	Indicates an optional element (keyword or argument)
{x}	Indicates a required element (keyword or argument)

[x {y | z}]	Indicates a required choice within and optional element

- Examples:
  - **ping** *ip-address* → command is **ping** and the user defined argument is the *ip-address* of the destination of the device.
  - **traceroute** *ip-address* → the command is **traceroute** and the user-defined argument is the *ip-address* of the destination device.

IOS Help Features

- Two forms of help
  - Context-Sensitive Help
    - Find available commands
    - Which commands start with specific characters
    - Which arguments and keywords are available to particular commands
    - "?"
  - Command Syntax Check
    - Verifies that a valid command was entered
    - Command line interpreter evaluates the command

Hotkeys and Shortcuts

CLI Line Editing	
Hotkey/ Shortcut	**Function**
Tab	Completes a partial command name entry
Backspace	Erases the character to the left of cursor
Ctrl-D	Erases the character at the cursor
Ctrl-K	Erases all characters from the cursor to the end of the command line
Esc D	Erases all characters from the cursor to the end of the world
Ctrl-U / Ctrl-X	Erases all characters from the cursor back to the beginning of the command line
Ctrl-W	Erases the word to the left of the cursor
Ctrl-A	Moves the cursor o the beginning of the line
Left Arrow / Ctrl-B	Moves the cursor one character to the left
Esc B	Moves the cursor back one word to the left
Esc F	Moves the cursor forward one word to the right
Right Arrow / Ctrl-F	Moves the cursor one character to the right
Ctrl-E	Moves the cursor to the end of the command line
Up Arrow / Ctrl-P	Recalls command in the history buffer, beginning with the most recent commands
Ctrl-R / Ctrl-I / Ctrl-L	Redisplays the system prompt and command line after a console message is received.

At the "-----More-----" prompt	
Hotkey/ Shortcut	**Function**
Enter Key	Displays the next line
Space Bar	Displays the next screen
Any Key	Ends the display string, returning to privileged EXEC mode

CLI Line Editing	
Hotkey/ Shortcut	**Function**
Ctrl-C	When in any config mode, ends the configuration mode and returns to privileged EXEC mode. When in setup mode, aborts back to the command prompt
Ctrl-Z	When in any config mode, ends the configuration mode and returns to privileged EXEC mode
Ctrl-Shift-6	All-purpose break sequence. Use to abort DNS lookups, traceroutes, pings.

2.2 Basic Device Configuration

Hostnames

Device Names

- Guidelines for choosing a hostname
  - Start with a letter
  - Contain no spaces

- End with a letter or digit
- Use only letters, digits, and dashes
- Be less than 64 characters in length

Configure Hostnames

1. From privileged EXEC mode, access the GCM
2. Enter command **hostname** followed by the name of the switch
3. Press Enter

Note: To remove, use command **no hostname**

```
Switch# configure terminal
Switch(config)# hostname SW-Floor-1
Sw-Floor-1(config)#
```

Limit Access to Device Configuration

Secure Device Access

- Limiting Device Access
  - Secure privileged EXEC access with a password
  - Secure user EXEC access with a password
  - Secure remote Telnet access with a password
  - Encrypt all passwords
  - Provide legal notification
- Password choosing guidelines
  - Use passwords that are more than 8 characters in length
  - Use a combination of upper and lowercase letters, numbers, special characters, and/or numeric sequences
  - Avoid using the same password for all devices
  - Don't use common words because these are easily guessed

Configure Passwords

- Most important password to configure is access to the privileged EXEC mode.

```
Sw-Floor-1> enable
Sw-Floor-1#
Sw-Floor-1# conf termainal
Sw-Floor-1(config)# enable secret password
Sw-Floor-1(config)# exit
Sw-Floor-1#
Sw-Floor-1# disable
Sw-Floor-1> enable
Password:
Sw-Floor-1#
```

- User EXEC access

```
Sw-Floor-1(config)# line console 0
Sw-Floor-1(config-line)# password password
Sw-Floor-1(config-line)# login
Sw-Floor-1(config)# exit
Sw-Floor-1(config)#
```

- VTY Line access – VTY lines enable remote access to the device.

```
Sw-Floor-1(config)# line vty 0 15
Sw-Floor-1(config-line)# password password
Sw-Floor-1(config-line)# login
Sw-Floor-1(config-line)#
```

Encrypt Passwords

- Service password-encryption global config command
    - Applies weak encryption to all unencrypted passwords

```
Switch(config)# service password-encryption
Switch(config)# exit
Switch# show running-config
**You successfully encrypted the plaintext passwords**
```

Banner Messages

- Banner messages inform the user of certain circumstances and display important messages – eg. Declaring only authorised personnel should attempt to gain entry into the device
- "#" → the delimiting character (can actually be any character not used within the message"
- Banners can include scheduled system shutdowns and other information that affects all network users

```
Switch(config)# banner motd # the message of the day #
```

Save Configurations

Save the Running Configuration File

Two system files that store device configuration:

- Startup-config
    - File stored in Non-Volatile Random Access Memory (NVRAM) that contains all of the commands that will be used by the device upon startup
    - NVRAM does not lose its contents when the device is powered up
- Running-config
    - File stores in Random Accessed Memory (RAM) that reflects the current configuration.
    - Modifying it affects the operation of the device immediately
    - RAM is volatile memory → it loses all of its content when the device is off

```
Switch# show running-config
```

Alter the Running Configuration

- Restore the device's previous configuration with **reload** command
    - Causes network downtime
- Clear all the configurations with **erase start-up config** command.

Capture Configuration to a Text File

1. Open PuTTY
2. Enable logging and assign a name and file location to save the log file
3. Execute the **show running-config show** or **startup-config** command. The text displayed with be placed into the chosen file.

2.3 Address Schemes

Ports and Addresses

IP Addresses

- Use of IP addresses is to enable devices to locate one another and establish end-to-end communication over the internet.
- The structure of an IPv4 address is called dotted decimal notation → represented by four decimal numbers between 0 and 255.
- Subnet mask: special type of IPv4 address. Coupled with the IPv4 address, the subnet mask determines which particular subnet the device is a member of
- Default gateway: the IP address of the router that the host will use to access remote networks
- IP addresses can be assigned to both physical ports and virtual interfaces

Interfaces and Ports

- Cable connecting to the interface must be designed to match the physical standards of the interface.
- Types of network media: twisted-pair copper cables, fiber-optic cables, coaxial cables or wireless
- Differences between types of media:
  - Distance the media can successfully carry a signal
  - Environment in which the media is to be installed
  - Amount of data and he speed at which it must be trsansmitted
  - Cost of media and installation
- Switches have one or more Switch Virtual Interfaces (SVIs) → provides means to remotely manage a switch over a network using IPv4

Configure IP Addressing

Manual IP Address Configuration for End Devices

- IP address information can be entered into devices manually, or automatically using Dynamic Host Configuration Protocol (DHCP)
- To manually configure IP address on a Windows host:

1. Control Panel > Network Sharing Centre > Change adapter setting
2. Right click and select properties to display the Local Area Connection Properties
3. Highlight Internet Protocol Version 4 (TCP/IPv4) and click properties to open them
4. Configure the IPv4 address and subnet mask information and default gateway

Automatic IP Address Configuration for End Devices

- DHCP enables automatic IPv4 address configuration for every end device that has DHCP enabled.
- To configure DHCP on a Windows PC → select “Obtain an IP address automatically" and “Obtain DNS server address automatically". The PC will search out a DHCP server and be assigned the address settings necessary to communicate on the network.
- Display the IP configuration settings by using **ipconfig** command.
  - Output: the IP address, subnet mask and gateway information from the DHCP server

Switch Virtual Interface

- To access the switch remotely, an IP address and a subnet mask must be configured on the SVI
- To configure an SVI on a switch:

1. Use the **interface vlan 1** command on GCM
2. Assign an IPv4 address using the **ip address** *ip-address subnet-mask* command
3. Enable using the **no shutdown** command.

```
Switch(config)# interface vlan 1
Switch(config-if)# ip address 192.168.10.2 255.255.255.0
Switch(config-if)# no shutdown
%LINK-5-CHANGED: Interface Vlan1, changed state to up
```

Verifying Connectivity

Interface Addressing Verification

- **Show ip interface brief** command → verifies the interfaces and address settings (condition) of intermediary devices like switches and routers

- **ping** command → used to test connectivity to another device on the network or a website on the internet

CHAPTER 3 – Network Protocols and Communication

3.1 Rules of Communication

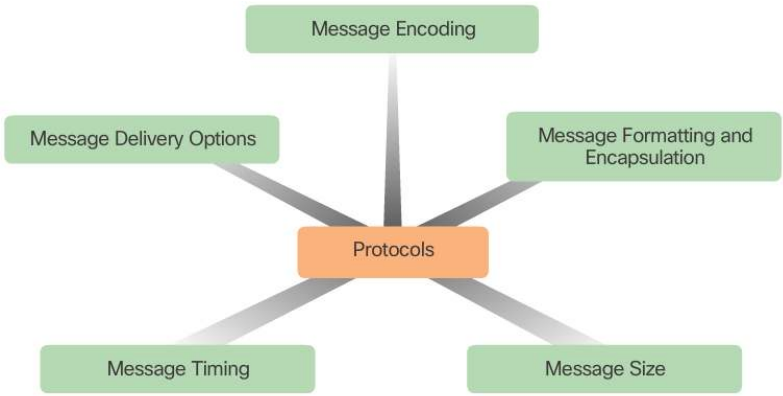
The Rules

Communication Fundamentals

- Simply having a wired/ wireless physical connection between devices is not enough to enable communication → the devices must know 'how' to communicate
- Elements of communication:
  - Message source (people, devices)
  - Destination (receiver – interprets)
  - Channel (media that provides the pathway)
- Communication begins with a message and is governed by protocols (rules)
- Protocols are specific to the type of communication method

Rule Establishment

- Protocols are necessary for effective communication
- Protocols must be followed in order for the message to be successfully delivered and understood
- Computer and network protocols define the details of hoe a message is transmitted across a network
- Must have the following:
  - An identified sender and receiver
  - Common language and grammar
  - Speed and timing of delivery
  - Confirmation or acknowledgement requirements.



Message Encoding

- First step to sending a message
- Encoding: the process of converting information into another acceptable form, for transmission.
- Decoding reverses this process to interpret the information
- Encoding between hosts must be in an appropriate format for the medium
- Messages sent across the network:

1. Converted into bits by the sending host → encoded into a pattern of sounds, light waves, or electrical impulses depending on the network media
2. Destination host receives and decodes the signals.

Message Formatting and Encapsulation

- When message is sent from source to destination, it must have specific format/ structure
  - Depend on the type of message and the channel that is used
- The process of placing one message format inside another message format is called encapsulation
- De-encapsulation occurs when the process is reversed by the recipient
- Each computer message is encapsulated in a specific format (frame) before it is sent over the network
- Frame → provides the address of the destination and the address of the source host
- The frame has source and destination in both the frame addressing and in the encapsulated message
- Messages that are not correctly formatted are not successfully delivered/ processed by the destination host.

Destination (physical / hardware address)	Source (physical / hardware address)	Start Flag (start of message indicator)	Recipient (destination identifier)	Sender (source identifier)	Encapsulated Data (bits)	End of Frame (end of message indicator)
Frame Addressing		Encapsulated Message				

Message Size

- Size is a rule of communication
- A long message must be broken into smaller pieces
- The size of pieces/ frames rules are strict
  - Frames that are too long or too short are not delivered
- Size restrictions require the host to break a long message into individual pieces that meet the minimum and maximum requirements
- Sent in frames → each containing a piece of the original message, addressing information
- The receiving host reconstructs the individual pieces of the message into the original message.

Message Timing

Rules of engagement for message timing:

- Access Method
  - Determines when someone is able to send a message
  - If two are talking at the same time – collision of information occurs
  - Hosts on a network need to know when to begin sending messages and how to respond when errors occur
- Flow Control
  - Timing also affects how much information can be sent and the speed that it can be delivered
  - Source and destination hosts use flow control methods to negotiate correct timing for successful communication
- Response Timeout
  - Hosts on the network have rules that specify how long to wait for responses and what action to take if a response timeout occurs.

Message Delivery Options

- The sender of a message can specify whether the recipient needs to return an acknowledgement to the sender
  Delivery options:
- Unicast
  - One-to-one
  - Single destination for the message
- Multicast
  - One-to-many
  - Same message to a group of host destinations simultaneously
- Broadcast
  - One-to-all
  - All hosts on the network receive the message at the same time
  - Some may need to acknowledge the receipt of the message, others do not.

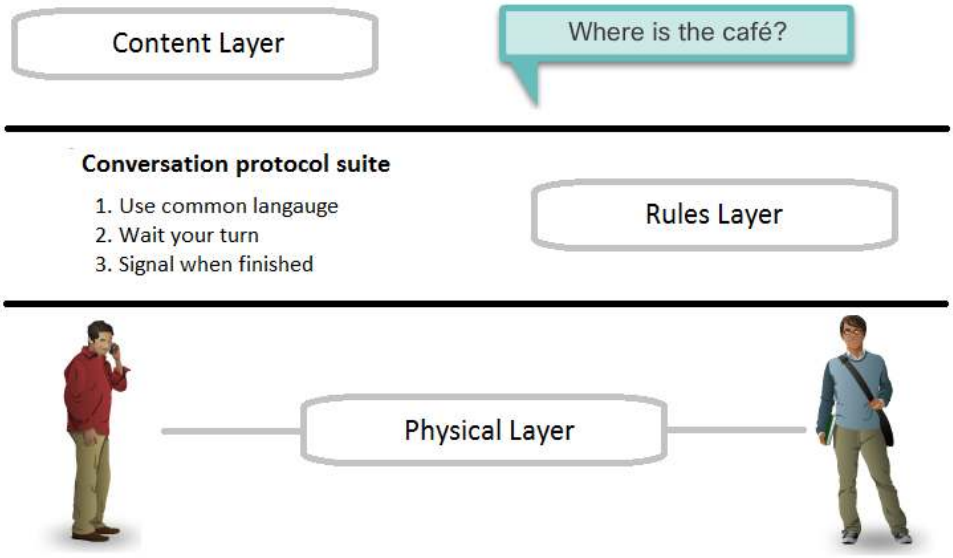
3.2 Network Protocols and Standards

Protocols

Rules that Govern Communications

- Protocol Suite: a group of inter-related protocols necessary to perform a communication function
  - Implemented by hosts and networking devices
- Protocols are viewed in terms of layers, each higher level service depending on the functionality defined by the protocols in the lower levels

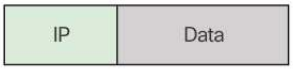
- Lower layers → concerned with moving data over the network + providing services to the upper layers
- Upper layers → focused on the content of the message being sent
- Protocol suites are sets of rules that work together to help solve a problem

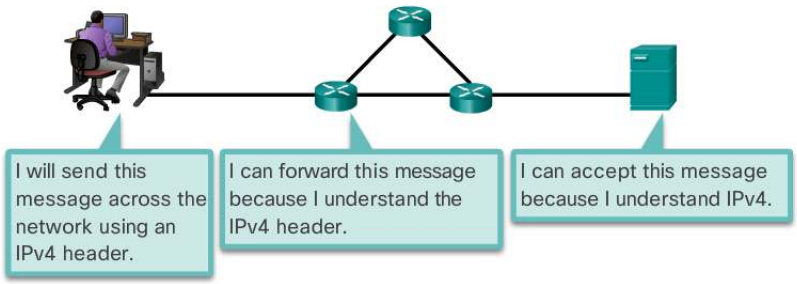


Network *Protocols*

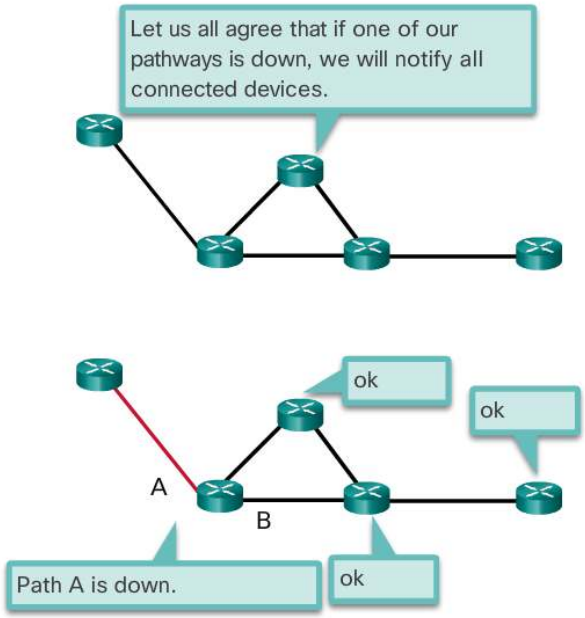
- For devices to successfully communicate, a network protocol suite must describe precise requirements and interactions
- Common networking protocols:
  - Hypertext Transfer Protocol (HTTP)
  - Transmission Control Protocol (TCP)
  - Internet Protocol (IP)
- Processes:

How the message is formatted

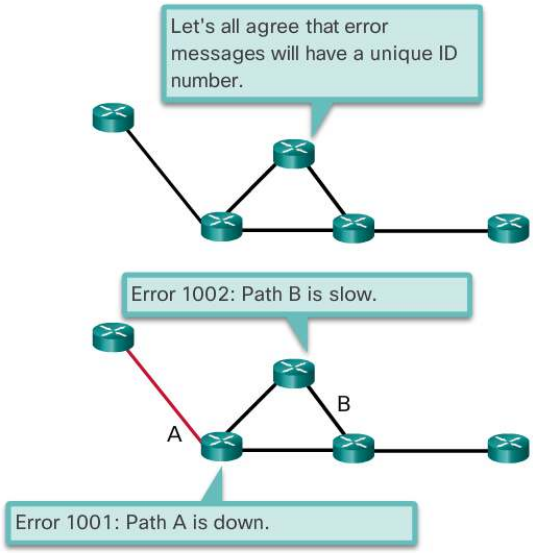




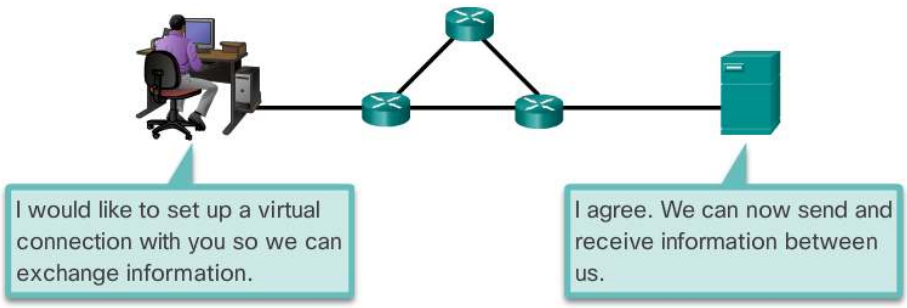
How networking devices share information about pathways with other networks



How and when error and system messages are passed between devices



Setup and termination of data transfer sessions



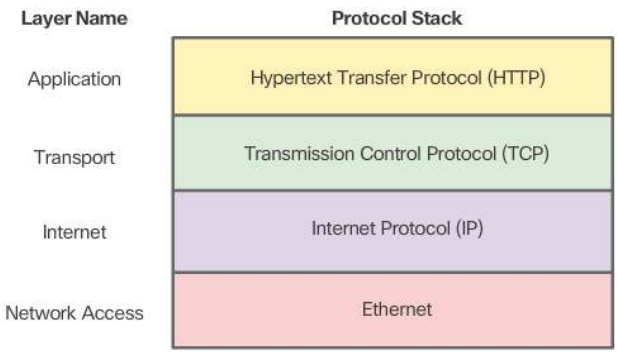
Protocol Interaction

Communication between a web server and web client is an example of an interaction between several protocols.

- HTTP
  - Application protocol that governs the way a web server and a web client interact.
  - Defines the content and formatting of the requests and responses that are exchanged between client and server

- Both web client and web server implement
- HTTP relies on other protocols to govern how the messages are transported between client and server.

- TCP
  - Transport protocol that manages the individual conversations.
  - Divides the HTTP messages into smaller pieces (segments) → sent between the web server and client processes running at the destination host
  - Also responsible for controlling the size and rate at which messages are exchanged between server and client.
- IP
  - Responsible for:
    - Taking the formatted segments from TCP
    - Encapsulating them into packets
    - Assigning them to the appropriate addresses
    - Delivering them to the destination host



- Ethernet
  - Network access protocol that describes 2 primary functions:
    - Communication over a data link
    - The physical transmission of data on the network media
  - Network access protocols are responsible for taking the packets from IP and formatting them to be transmitted over the media.

Protocol Suits

Protocol Suites and Industry Standards

- A protocol suite may be specified by a standards organisation or developed by a vendor
- The TCP/IP Protocol Suite → An open standard = freely available to the public, any vendor is able to implement these protocols on their hardware/ software
- Standards-based protocol → process that has been endorsed by the networking industry and approved by a standards organisation
- Use of standards ensures that products from different manufacturers can interoperate successfully.
- Some protocols are proprietary → one company/ vendor controls he definition of the protocol and how it functions

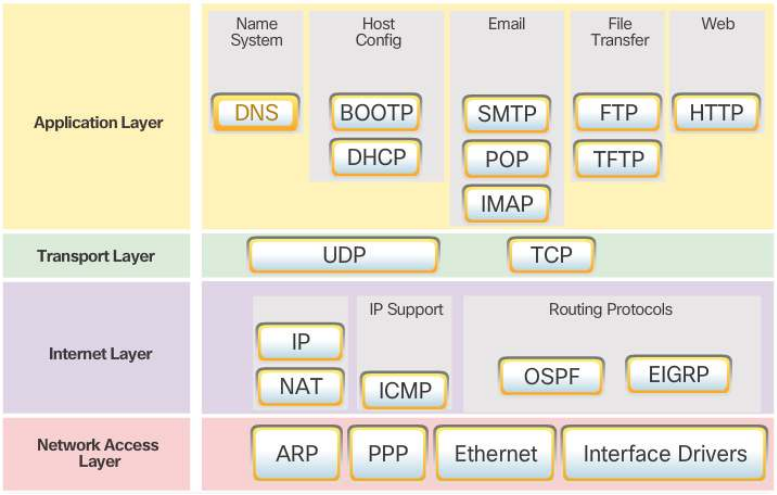
Development of TCP/IP

1969 → 1st packet switching network by Advanced Research Projects Agency Network (ARPANET) by connecting mainframe computers at four locations.
1970 → 1st packet radio network by Norman Abramson
1972 → Telnet specification written (RFC 318)
→ 1st email management program by Larry Roberts
→ '@' symbol chosen by Ray Tomlinson to signify the recipient's destination
1981 → TCP and IP protocols are formalised (RFC 793 and RFC 791)
1982 → The Exterior Gateway Protocol (EGP) is developed to all routers to exchange network information (RFC 827)
1984 → The Domain Name Service (DNS) is introduced
1985 → The File Transfer Protocol (FTP) is documented (RFC 765)
1986 → Cisco launches its 1st routing innovation, AGS multi-protocol router
1988 → The Internet Relay Chat (IRC) is developed by Jarkko Oikarinen
1991 → Release of specifications of WWW by Tim Berners-Lee and Robert Cailliau
1993 → 1st web browser, MOSAIC is developed by Marc Andreessen
1995 → 1st specifications for IPv6 released (RFC 1883)
2011 → 1st World IPv6 Day – websites and internet service providers (including Google, Facebook, Yahoo!) participated for a worldwide trial of IPv6.

TCP/IP Protocol Suite

- The TCP/IP protocol suite is implemented as a stack on both the sending and receiving hosts to provide end-to-end delivery of applications over a network

Application Layer



DNS → Domain Name System (or Service)
Translates domain names into IP address

BOOTP → Bootstrap Protocol
Enables a diskless workstation to discover its own IP address, the IP address of a BOOTP server on the network, and a file to be loaded into memory to boot the machine. Is being superseded by DHCP

DHCP → Dynamic Host Configuration Protocol
Dynamically assigns IP addresses to client stations at start-up. Allows address to be re-used when no longer needed.

SMTP → Simple Mail Transfer Protocol
Enables clients to send email to a mail server. Enables servers to send email to other servers.

POP → Post Office Protocol version 3 (POP3)
Enables clients to retrieve email from a mail server. Downloads email from the mail server to the desktop.

IMAP → Internet Message Access Protocol
Enables clients to access email stored on a mail server. Maintains email on the server.

FTP → File Transfer Protocol
Sets rules that enable a user on one host to access and transfer file to and from another host over a network. Reliable, connection-oriented, and acknowledged file delivery protocol.

TFTP → Trivial File Transfer Protocol
Simple, connectionless file transfer protocol. A best-effort, unacknowledged file delivery protocol. Utilises less overhead then FTP.

HTTP → Hypertext Transfer Protocol
Set of rules for exchanging text, graphic images, sound, video, and other multimedia files on the www.

Transport Layer

UDP → User Datagram Protocol
Enables a process running on one host to send packets to a process running on another host. Does not confirm successful datagram transmission.

TCP → Transmission Control Protocol
Enables reliable communication between processes running on separate hosts. Reliable, acknowledged transmissions that confirm successful delivery.

Internet Layer

IP → Internet Protocol
Receives message segments from the transport layer. Packages messages into packets. Addresses packets for end-to-end delivery over an Internetwork.

NAT → Network Address Translation
Translates IP addresses from a private network into globally unique public IP addresses

ICMP → Internet Control Message Protocol
Provides feedback from a destination host to a source host about errors in packet delivery

OSPF → Open Shortest Path First
Link-state routing protocol. Hierarchal design based on areas. Open standard interior routing protocol.

EIGRP → Enhanced Interior Gateway Routing Protocol
Cisco proprietary routing protocol. Uses composite metric based on bandwidth, delay, load and reliability.

Network Access Layer

ARP → Address Resolution Protocol
Provides dynamic address mapping between an IP address and a hardware address.

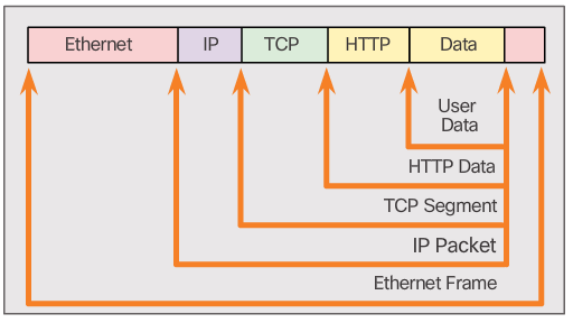
PPP → Point-to-Point Protocol
Provides a means of encapsulating packets for transmission over a serial link

Ethernet
Defines the rules for wiring and signalling standards of the network access layer

Interface Drivers
Provides instruction to a machine for the control of a specific interface on a network device.

TCP/IP Communication Process

1. Web server prepares the HTML page as data to be sent
2. The application protocol HTTP header is added to the front of the HTML data (header contains various information, including the HTTP version the server is using and a status code indicating it had information for the web client).
3. The HTTP application layer protocol delivers the HTML to the transport layer. The TCP transport layer protocol is used to manage individual conversations.
4. IP information is added to the front of the TCP information. IP assigns the appropriate source and destination IP addresses → known as IP packet
5. Ethernet protocol adds information to both ends of the IP packet → known as data link frame. Frame is delivered to the nearest router along the path towards the web client. This router removes the Ethernet connection, analyses IP packet, determines the best path for the packet, inserts the packet into a new frame, and sends it to the next neighbouring router towards the destination. Each router removes and adds new data link information before forwarding the packet.
6. This data is now transported through the internetwork (media and intermediary devices)
7. Client receives the data link frames that contain the data. Each protocol header is processed and then removed in the opposite order it was added. Ethernet information is processed and removed, followed by IP protocol information, the TCP information and finally the HTTP info.
8. The web page information is then passed on to the client's web browser software.



Standard Organisations

Open Standards

- Encourage interoperability, competition, and innovation
- Guarantee that no single company's product can monopolise the market or have an unfair advantage
- Standards organisation (SO) may draft a set of rules or select a proprietary protocol as the basis for the standard.
- SOs are usually vendor-neutral, non-profit and established to develop and promote the concept of open standards.

Internet Standards

- **Internet Society (ISOC)** → Responsible for promoting the open development and evolution of Internet use throughout the world.
- **Internet Architecture Board (IAB)** → Responsible for the overall management and development of Internet standards.
- **Internet Engineering Task Force (IETF)** → Develops, updates, and maintains Internet and TCP/IP technologies. This includes the process and documents for developing new protocols and updating existing protocols know as Request for Comments (RFC) documents.

- **Internet Research Task Force (IRTF)** → Focused on long-term research related to Internet and TCP/IP protocols such as Anti-Spam Research Group (ASRG), Crypto Forum Research Group (CFRG), and Peer-to-Peer Research Group (P2PRG).
- **Internet Corporation for Assigned Names and Numbers (ICANN)** → Based in the United States, coordinates IP address allocation, the management of domain names, and assignment of other information used TCP/IP protocols.
- **Internet Assigned Numbers Authority (IANA)** → Responsible for overseeing and managing IP address allocation, domain name management, and protocol identifiers for ICANN.

Electronics and Communications Standards Organisations

Responsibility for promoting and creating the electronic and communication standards used to deliver the IP packets as electronic signals over a wired or wireless medium.

- **Institute of Electrical and Electronics Engineers (IEEE)** → Organization of electrical engineering and electronics dedicated to advancing technological innovation and creating standards in a wide area of industries including power and energy, healthcare, telecommunications, and networking.
- **Electronic Industries Alliance (EIA)** → Best known for its standards related to electrical wiring, connectors, and the 19-inch racks used to mount networking equipment.
- **Telecommunications Industry Association (TIA)** → Responsible for developing communication standards in a variety of areas including radio equipment, cellular towers, Voice over IP (VoIP) devices, satellite communications, and more.
- **International Telecommunications Union-Telecommunication Standardization Sector (ITU-T)** → One of the largest and oldest communication standard organizations. The ITU-T defines standards for video compression, Internet Protocol Television (IPTV), and broadband communications, such as a digital subscriber line (DSL).

Reference Models

The Benefits of Using a Layered Model

Benefits include:

+ Assisting in protocol design because protocols that operate at a specific layer have defined information that they act upon and a defined interface to the layers above and below
+ Fostering competition
+ Preventing technology or capability changes in one layer from affecting other layers
+ Providing a common language to describe networking functions and capabilities

- TCP/IP model and Open Systems Interconnection (OSI) model are primary models used when discussing network functionality
- Basic types of layered networking models:
  - Protocol Model → closely matches the structure of a particular protocol suite. TCP/IP is a protocol model because it describes the functions that occur at each layer of protocols in the suite.
  - Reference Model → Provides consistency within all types of network protocols and services by describing what has to be done at a particular layer, but not prescribing how it is to be accomplished.

The OSI Reference Model

- Provides an extensive list of functions and services that can occur at each layer
- Describes the interaction of each layer with the layers above and below

The OSI Reference Model:

7. **Application**
   The application layer contains protocols used for process-to-process communications.
6. **Presentation**
   The presentation layer provides for common representation of the data transferred between application layer services.
5. **Session**

The session layer provides services to the presentation layer to organise its dialogue and to manage data exchange.

4. **Transport**
   The transport layer defines services to segment, transfer, and reassemble the data for individual communications between end devices.
3. **Network**
   The network layer provides services to exchange the individual pieces of data over the network between identified end devices.
2. **Data Link**
   The data link layer protocols describe methods for exchanging data frames between devices over a common media.
1. **Physical**
   The physical layer protocols describe the mechanical, electrical, functional, and procedural means to activate, maintain and de-activate physical connections for a bit transmission to and from a network device.

The TCP/IP Protocol Model

- Sometimes referred to as the internet model
- Defines four categories of functions that must occur for communications to be successful
- Architecture of the TCP/IP protocol suite follows the structure of this model
- Is an open standard

The TCP/IP Model:

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

OSI Model and TCP/IP Model Comparison

SIMILARITIES	DIFFERENCES
• OSI network layer → maps directly to the TCP/IP Internet layer. This layer is used to describe protocols that address and route messages through an internetwork. • OSI transport layer → maps directly to the TCP/IP Transport layer. This layer describes general services and functions that provide ordered and reliable delivery of data between source and destination hosts. • Both the TCP/IP and OSI models are commonly used when referring to protocols at varioAus layers. Because the OSI model separates the data link layer from the physical layer, it is commonly used when referring to these lower layers.	○ *Network access layer* → TCP/IP protocol suite does not specify which protocols to use when transmitting over a physical medium; it only describes the handoff from the internet layer to the physical network protocols. *OSI Layers 1 and 2* → discuss the necessary procedures to access the media and the physical means to send data over a network. ○ *TCP/IP application layer* → includes a number of protocols that provide specific functionality to a variety of end user applications. ○ *OSI model Layers 5, 6, and 7* → used as references for application software developers and vendors to produce products that operate on networks.

3.3 Data Transfer in the Network

Data Encapsulation

Message Segmentation

- Dividing the data into smaller, more manageable pieces to send over the network
- Primary benefits:
  - Many different conversations can be interleaved on the network (multiplexing)
  - Increases the efficiency of network communications. If part of the message fails to make it to the destination, only the missing parts need to be transmitted.
- Challenge is the level of complexity that is added to the process → each segment of the message must ensure it gets to the correct destination and can be reassembled into the content of the original message.

Protocol Data Units

- Encapsulation Process: as application data is passed down the protocol stack on its way to be transmitted across the network media, various protocol information is added at each level.
- The form of that piece of data at any layer is a **Protocol Data Unit** (PDU).
- At each stage, a PDU has a different name to reflect new functions

Passing down the stack

Data → General term for the PDU used at the application level

Segment → Transport layer PDU

Packet → Network layer PDU

Frame → Data Link layer PDU

Bits → A physical layer PDU used when physically transmitting data over the medium

Encapsulation

- When sending a message, the process works from top to bottom
- At each layer, the upper information is considered data within the encapsulated protocol

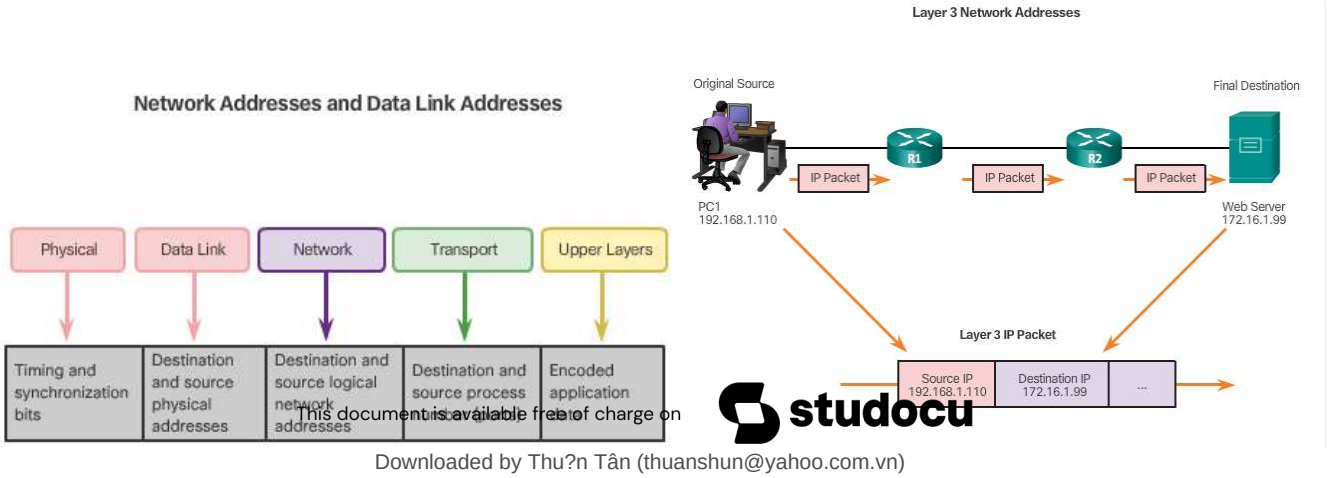
De-encapsulation

- This process is reversed at the receiving host (de-encapsulation)
- The process used by a receiving device → removes one or more of the protocol headers
- De-encapsulated as it moves up the stack toward end user application

Data Access

Network Addresses

- Network and data link layers are responsible for delivering the data form the source to destination
  - *Network layer source and destination address* → responsible for delivering the IP packet from the original source to the final destination.
  - *Data link layer source and destination addresses* → responsible for delivering the data link frame from one network interface card (NIC) to another NIC on the same address.
- The IP packet contains two IP addresses:
  - *Source IP address*
  - *Destination IP address*



Data Link Addresses

- Purpose of data link (layer 2) address is to deliver the data link frame from one NIC to another NIC on the same network
- Before IP packet can be sent, it must be encapsulated in a data link frame so it can be transmitted over the physical medium
- IP packet travel: host-to-router → router-to-router → router-to-host
    - Each point along the way the IP packet is encapsulated in a new data link frame
    - Each data link frame contains the source data link address of the NIC card sending the frame and the destination data link address of the NIC receiving the frame.
- IP packet encapsulated in a data link frame contains:
    - *Source data link address*
    - *Destination data link address*
- Data link frame also contains a trailer

Devices on the Same Network

Role of the Network Layer Addresses

- Network layer addresses (IP addresses) indicate original source and final destination
- Contains two parts:
    - *Network portion* → left most part of the address that indicates which network the IP address is a member. All devices on the same network will have the same portion.
    - *Host portion* → the remaining part of the address identifies specific device. Host portion is unique for each device.
- The subnet mask is used to identify the network portion of an address from the host portion.

Role of the Data Link Layer Addresses

- When on same network, data link frame is sent directly to the receiving device
- On Ethernet network, data link addresses are known as Ethernet (Media Access Control) addresses. MAC addressees are physically embedded on the Ethernet NIC
    - *Source MAC address* → data link address/ Ethernet MAC address of the device that sends the data link frame with the encapsulated IP packet. Written in hexadecimal notation
    - *Destination MAC address* → data link address of the receiving device. Also written in hexadecimal notation.

Devices on a Remote Network

Role of the Network Layer Addresses

- When on differing networks, the source and destination IP addresses will respresent hosts on different networks
- Indicated by the network portion of the IP address of the destination host.
    - *Source IP address*
    - *Destination IP address*

Role of the Data Link Layer Addresses

- Ethernet data link frame cannot be sent directly to the destination host → the Ethernet frame myst be sent to another device known as the router or default gateway.
    - *Source MAC address*
    - *Destination MAC address* → the sending device uses the Ethernet MAC address of the default gateway or router.
- It is important that the IP address of the default gateway be configured on each host on the local network → all packets to a destination on remote networks are sent to the default gateway.

CHAPTER 4 – Network Access

4.1 Physical Layer Protocols

Physical Layer Connection

Types of Connections

- Before any network communications can occur, a physical connection to a local network must be established
- Wired/ wireless transmitted using radio waves
  - Wireless capability requires a wireless access point
- Switch devices and wireless access points are often two separate dedicated devices within a network implementation
- In homes Integrated Service Routers (ISRs) are being implemented
  - Offer a switching component with multiple ports, allowing multiple devices to be connected to the LAN using cables
  - Many also include an AP

Network Interface Cards

- Connect a device to the network
- Ethernet NICs are used for a wired connection
- WLAN NICs are used for wireless
- Not all physical connections are equal (performance level) when connecting to a network
  - Wireless device may experience degradation in performance based on distance from AP
  - Slower network performance may occur as more wireless devices access the network simultaneously.
  - A wired connection will not degrade in performance, wired devices do not need to share their access to the network with other devices.
- A *wireless range extender* can be used to regenerate the wireless signal to other parts of the house that are too far from the wireless access point.

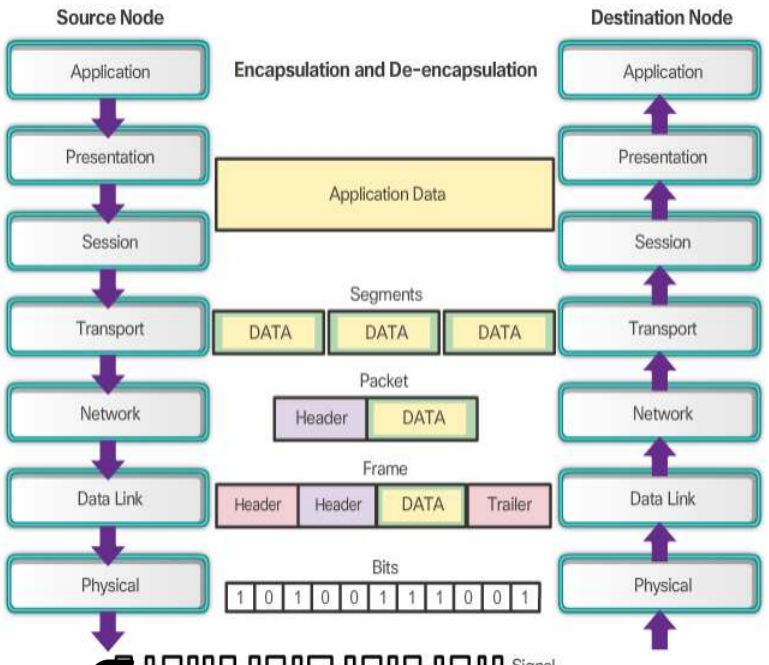
Purpose of the Physical Layer

The Physical Layer

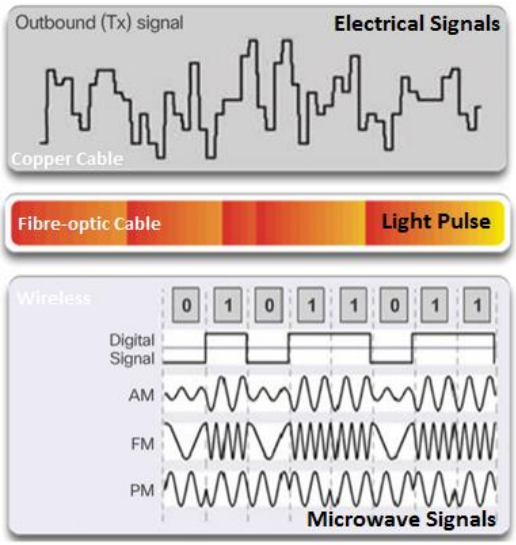
- Provides the means to transport the bits that make up a data link layer frame across network media
- Accepts a complete frame from the data link layer and encodes it as a series of signals that are transmitted onto the local media

Process of data from source → destination

1. User data is segmented by transport layer, placed in packets by network layer and encapsulated into frames by data link layer
2. Physical layer encodes the frames and creates the electrical, optical, or radio wave signals that represent the bits in each frame
3. Signals are sent on the media, one at a time
4. Destination node physical layer retrieves individual signals and restores them to their bit representations then passes the bits up to the data link layer as a complete frame.



Physical Layer Media



- Three basic forms of network media
- The physical layer produces the representation and groupings of bits for each type of media as:
  - Copper cable: patterns of electric pulses
  - Fibre Optic cable: patterns of light
  - Wireless: patterns of microwave transmissions

Physical Layer Standards

- The services and protocols in the TCP/IP suite are defined by the Internet Engineering Task Force (IETF)
- The physical layer consists of:
  - Electronic circuitry
  - Media
  - Connectors developed by engineers
- Physical layer hardware, media, encoding and signalling standards are defined + governed by:
  - International Organization for Standardization (ISO)
  - Telecommunications Industry Association/Electronic Industries Association (TIA/EIA)
  - International Telecommunication Union (ITU)
  - American National Standards Institute (ANSI)
  - Institute of Electrical and Electronics Engineers (IEEE)
  - National telecommunications regulatory authorities including the Federal Communication Commission (FCC) in the USA and the European Telecommunications Standards Institute (ETSI)

Physical Layer Characteristics

Functions

Physical components

- Physical components are:
  - electronic hardware devices
  - media
  - other connectors that transmit and carry the signals to represent the bits
- Examples in the physical layer:
  - NICs
  - Interfaces and connectors
  - Cable materials
  - Cable designs
  - Ports

Encoding

- Method of converting a stream of data bits into a predefined 'code'
- Groupings of bits used to provide a predictable pattern that can be recognised by both sender and receiver

Signalling

- The physical layer must generate the electrical, optical, or wireless signals that represent the 1 and 0 on the media
- Standards must define what type of signal represents a 1 and a 0
- Example: Modulation techniques → characteristic of one wave (the signal) modifies another wave (the carrier).
- Nature of signals representing bits on media will depend on signalling method

Bandwidth

- Bandwidth is the capacity of a medium to carry data → measures the amount of data that can flow from one place to another in a given amount of time.
- Different physical media support the transfer of bits at different rates
- Typically measured in:
  - Kilobits per second (kb/s)
  - Megabits per second (Mb/s)
  - Gigabits per second (Gb/s)
- Factors that determine bandwidth:
  - Properties of the physical media
  - Technologies chosen for signalling and detecting network signals

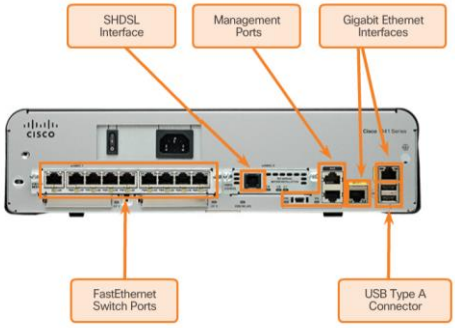
Unit of Bandwidth	Abbreviation	Equivalence
Bits per second	b/s	1 b/s = fundamental unit of bandwidth
Kilobits per second	kb/s	1 kb/s = 1,000 bps = 10^3 bps
Megabits per second	Mb/s	1 Mb/s = 1,000,000 bps = 10^6 bps
Gigabits per second	Gb/s	1 Gb/s = 1,000,000,000 bps = 10^9 bps
Terabits per second	Tb/s	1 Tb/s = 1,000,000,000,000 bps = 10^12 bps

Throughput

- Throughput is the measure of the transfer of bits across the media over a given period of time
- Usually does not match the specified bandwidth in physical layer implementations
- Factors that influence throughput:
  - Amount of traffic
  - Type of traffic
  - Latency (amount of time for data to travel from one point to the other) created by the number of network devices encountered between source + destination
- Throughput cannot be faster than the slowest link in the path
  - Slow segment creates a bottleneck to the throughput of the entire network
- Goodput → measure of usable data transferred over a given period of time. Throughput minus traffic

Types of Physical Media

- Physical layer produces the representations of bits as voltages, radio frequencies or light pulses.
- **E.g.** Standards for copper media:
  - Type of copper cabling used
  - Bandwidth of the communication
  - Pinout and colour codes of connections to media
  - Maximum distance of the media

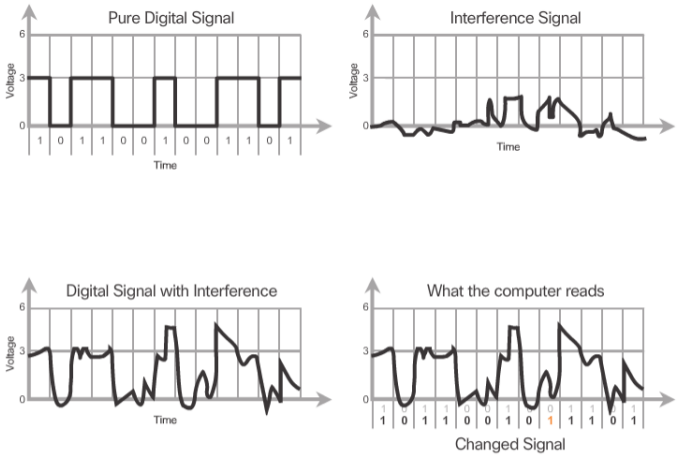


4.2 Network Media

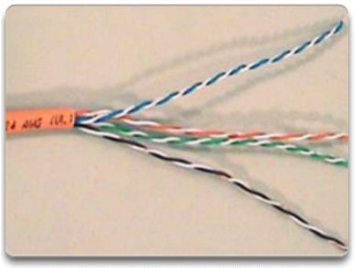
Copper Cabling

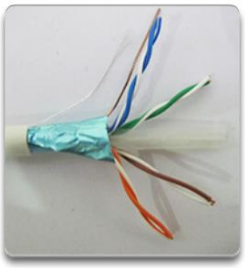
Characteristics of Copper Cabling

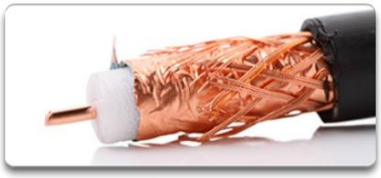
- Networks use copper media because it is inexpensive, easy to install and has low resistance to electrical current
- Although, limited by distance and signal interference
- Transmitted as electrical pulses
- A detector must receive a signal that is decoded to match the signal sent
- Longer signal is sent → more it deteriorates (attenuation)
- Timing and voltage values of electrical pulses are susceptible to interference from:
  - *Electromagnetic interference (EMI)/ Radio frequency interference (RFI)* → can distort and corrupt data signals being carried
  - *s* → disturbance caused by the electric or magnetic field of a signal on one wire to an adjacent wire. When an electrical current flows through a wire, creates a small, circular magnetic field around the wire, which is picked up by an adjacent wire.



- To counter EMI and RFI → some cables are wrapped in metallic shielding and require proper grounding connections.
- To counter crosstalk → some cables have opposing circuit wire pairs twisted together
- Susceptibility can be limited by:
  - Selecting cabling most suited to the environment
  - Designing cable infrastructure to avoid sources of interference
  - Cabling techniques that include proper handling and termination of the cables

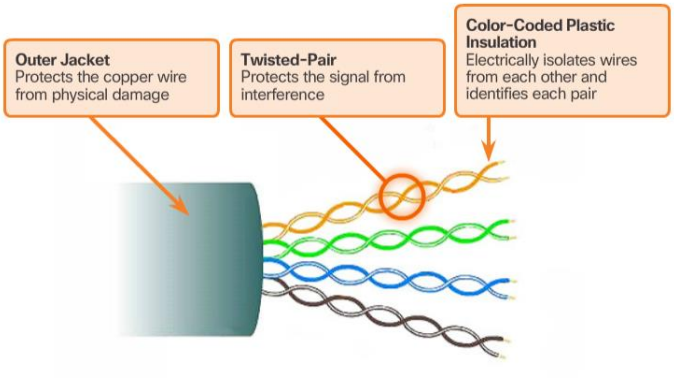

Unshielded Twisted-Pair (UTP) cable


Shielded Twisted-Pair (STP) cable


Coaxial cable

Copper Media

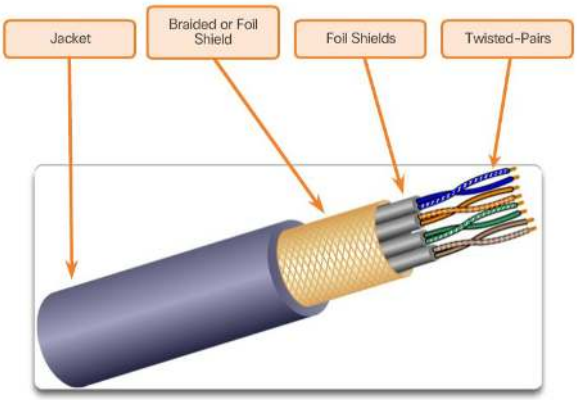
- Three main types of copper media:
  - Unshielded Twisted-Pair (UTP)
  - Shielded Twisted-Pair (STP)
  - Coaxial
- Used to interconnect nodes on a LAN and infrastructure devices
- Different physical layer standards specify the use of different connectors.
- A single type of physical connector may be used for multiple types of connections



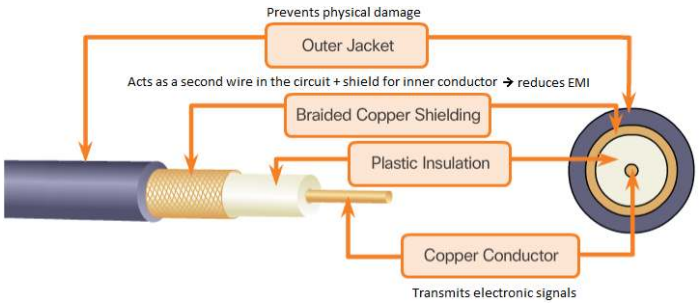
Unshielded Twisted-Pair Cable

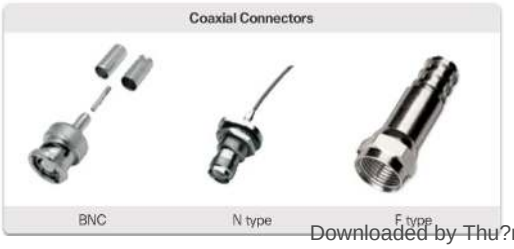
- Most common
- Terminated with RJ-45 connectors
- Used for interconnecting network hosts with intermediary networking devices
- In LANs → UTP cable consists of four pairs of colour-coded wires that are twisted and then encased in flexible plastic sheath (protects from minor damage).

Shielded Twisted-Pair Cable



- Better noise protection
- Significantly more expensive + difficult to install
- Uses RJ-45 connector
- shielding to counter EMI + RFI and wire twisting to counter crosstalk
- Terminated with special shielded STP data connectors
- If improperly grounded, the shield may act as an antenna and pick up unwanted signals.





Coaxial Cable

- Two conductors share the same axis
- Consists of:
- Different types of connectors used
- Used in:
  - Wireless installations → coax cable carries RF energy between antennas + radio equipment
  - Cable Internet installations → cable service providers provide internet to their customers by replacing portions of coax cable and supporting amplification elements with fibre-optic cable. Wiring inside customers premises is still coax cable.

Copper Media Safety

- Fire hazards
  - Cable insulation sheaths may be flammable
  - Produce toxic fumes when heated/ burned
- Electrical hazards
  - Copper wires conduct electricity in undesirable ways
  - Could present undesirable voltage levels when used to connect devices that have power sources with different ground potentials
  - May conduct voltages caused by lightning strikes to network devices.
- Result
  - Damage to network devices and connected computers
  - Injury to personnel
- Cabling practices to prevent potential hazards:
  - Separation of data and electrical power cabling must comply with safety codes
  - Cables must be connected correctly
  - Installations must be inspected for damage
  - Equipment must be grounded correctly

UTP Cabling

Properties of UTP Cabling

- Consists of four pairs of color-coded copper wires that have been twisted together and then encased in a flexible plastic sheath
- Small size = advantageous during installation
- Limit crosstalk by:
  - *Cancellation*
    Pairing wires in a circuit. Two wires are placed close together = magnetic fields are the exact opposite of each other → magnetic fields cancel each other any EMI and RFI signals
  - *Varying the number of twists per wire*
    must follow precise specifications on how many twists per meter of cable. Each coloured pair is twisted a different number of times.

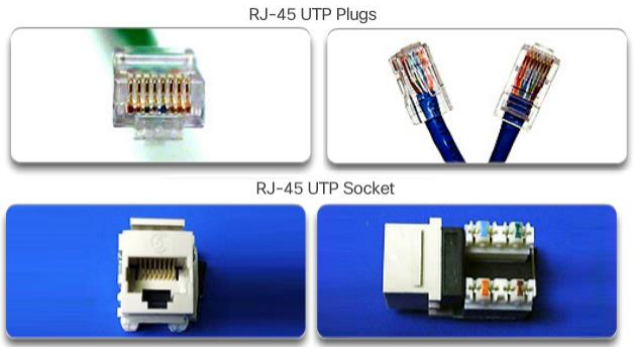
UTP Cabling Standards

- Standards by TIA/EIA
- TIA/EIA-568 → commercial cabling standards for LAN installations. Elements:
  - Cable types
  - Cable lengths
  - Connectors
  - Cable termination
  - Methods of testing cable
- IEEE categories for cabling → based on ability to carry higher bandwidth rates
  - *Category 3 Cable (UTP)*
    - Used for voice communication
    - Most often used for phone lines
  - *Category 5 and 5e Cable (UTP)*
    - Used for data transmission
    - Cat5 supports 100 Mb/s and 1000 Mb/s (not recommended)
    - Cat5e supports 1000 Mb/s
  - *Category 6 Cable (UTP)*
    - Used for data transmission
    - Added separator between each pair of wires allowing it to function at higher speeds
    - Supports 1000 Mb/s – 10 Gb/s (not recommended)

UTP Connectors

- UTP cable is usually terminated with an RJ-45 connector
  - Used for range of physical layer specifications, i.e. Ethernet

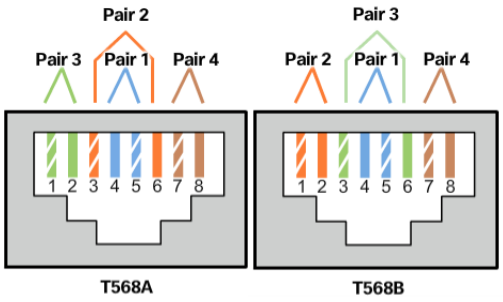
- TIA/EIA-568 → wire colour codes to pin assignments (pinouts) for Ethernet cables.
- RJ-45 connector → the socket (network device, wall, cubicle partition outlet, or patch panel)
- When copper cabling is terminated; possibility of signal loss and the introduction of noise into the communication circuit
  - When terminated improperly, each cable is a potential source of physical layer performance degradation → essential that all copper media terminations be high quality to ensure future optimum performance



Types of UTP Cable

- Different situations = differing wiring conventions
- Types:
  - *Ethernet Straight-Through*
    - Most common
    - To interconnect host to a switch and switch to a router
  - *Ethernet Crossover*
    - Interconnect similar devices → **e.g.** switch to switch, host to host
  - *Rollover*
    - Cisco proprietary cable
    - Connect workstation to a router/ switch or switch to console port
- Using crossover or straight-through incorrectly will not allow connectivity.

Cable Type	Standard	Application
Ethernet Straight-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
Rollover	Cisco proprietary	Connects a workstation serial port to a router console port, using an adapter.



Testing UTP Cables

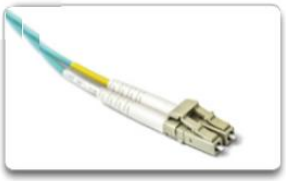
- UTP cable testing should test for the following parameters:
  - Wire map
  - Cable length
  - Signal loss due to attenuation
  - Crosstalk

Fibre-Optic Cabling

Properties of Fibre-Optic Cabling

- Transmit data over long distances + higher bandwidths than any other network media
- Transmit signals with less attenuation + completely immune to EMI and RFI
- Commonly used to interconnect network devices
- Flexible, thin, transparent strand of pure glass
- Bits are encoded on the fibre as light impulses → acts as a waveguide/ 'light pipe' to transmit light with minimal loss of signal
- Used in four types of industry:
  - Enterprise Networks → backbone cabling applications + interconnecting infrastructure devices
  - Fibre-to-the-Home (FTTH) → always-on broadband services to homes + small businesses
  - Long-Haul Networks → connect countries and cities

- Submarine Networks → reliable high-speed, high-capacity solutions capable fo surving in harsh undersea to transoceanic distances



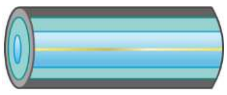
Duplex Multimode LC Connectors

Fibre Media Cable Design

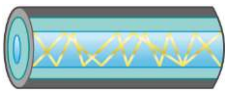
- Thin + susceptible to sharp bends, its properties make it very strong
- Durable and deployed in harsh environmental conditions
- Components:
  - **Core**
    The light transmission element at the centre of the optical fibre. Typically silica or glass. Light pulses travel through the fibre core.
  - **Cladding**
    Made from slightly different chemicals than those used to create the core. Acts like a mirror by reflecting light back into the core. Keeps light in the core as it travels down the fibre.
  - **Buffer**
    Used to help shield the core and cladding from damage
  - **Strengthening material**
    Surrounds the buffer, prevents the fibre cable from being stretched when it is being pulled. The material used is often the same material used to produce bullet proof vests.
  - **Jacket**
    Typically a PVC jacket that protects the fibre against abrasion, moisture, and other containments. This outer jacket composition can vary depending on the cable usage.

Types of Fibre Media

- Light pulses are generated by:
  - Lasers
  - Light emitting diodes (LEDs)
- Electronic semiconductor devices (photodiodes) detect the light pulses and convert them to voltages.
- Fibre-optic cables are classified into 2 types:
  - **Single-mode fibre (SMF)**
    Very small core and uses expensive laser technology to send a single ray of light. Popular for long-distance.



  - **Multimode fibre (MMF)**
    Larger core and uses LED emitters to send light pulses. Light from LED enters the multimode fibre at different angles. Popular in LANS because they are low-cost.
    Provides bandwidth up to 10 Gb/s over link lengths of up to 550 meters.



- Difference between them is the amount of dispersion → the spreading of a light pulse over time; the more dispersion, the greater the loss of signal strength.

Fibre-Optic Connectors

- Optical fibre connector terminates the end of an optical fibre
- Main differences are dimensions and methods of coupling
- Types of Fibre-optic connectors:
  - **Straight-Tip (ST) Connectors**
    - One of the first types used
    - Locks securely with a “twist-on-twist-off” bayonet style mechanism

ST Connectors

  - **Subscriber Connector (SC) Connectors**
    - Referred to as a square/ standard connector
    - Widely adopted LAN and WAN connector
    - Uses a push-pull mechanism to ensure insertion
    - Used with multimode and sing-mode fibre

LC Connector

  - **Lucent Connector (LC) Connectors**
    - Smaller version of fibre-optic SC connector
    - Called little/ local connector
    - Quickly growing in popularity due to smaller size
  - **Duplex Multimode LC Connectors**

SC Connectors

    - Similar to LC simplex connector, but using a duplex connector

- Light can only travel in one direction over optical fiber → two fibers are required to support the full duplex operation
    - Patch cables bundle together two optical fiber cables and terminate them with a pair of standard single fiber connectors
    - Some fibre connectors accept both the transmitting and receiving fibres in a single connector (duplex connnector)
- Fibre patch cords are required for interconnecting infrastructure devices
    - Use of colour distinguishes between single mode and multimode patch cords → Yellow jacket is for single-mode fiber cables and orange (or aqua) for multimode fiber cables.

Testing Fibre Cables

- Incorrect termination of fibre-optic media will result in diminished signalling distances or complete transmission failure.
- Common Fibre-optic termination and splicing errors are:
    - *Misalignment* → fibre-optic media are not precisely aligned to one another when joined
    - *End gap*→ media does not completely touch at the splice/ connection
    - *End finish* → media ends are not well polished, or dirt is present at the termination
- Test: Shining a bright flashlight into one end of the fibre while observing the other end → Tell if broken, but not performance
- Test: An Optical Time Domain Reflectometer (OTDR) can be used to test each cable segment. Injects a test pulse of light into the cable and measures backscatter and reflection of light as a function of time. → Will calculate the approximate distance at which these faults are detected along the length of the cable.

Fibre VS Copper

- Most enterprise environments use optical fibre → primarily used as backbone cabling for high-traffic point-to-point connections between data distribution facilities and for the interconnection of buildings in multi-building campuses. Because optical fiber does not conduct electricity and has a low signal loss, it is well suited for these uses.

Implementation Issues	UTP Cabling	Fibre-Optic Cabling
Bandwidth supported	10 Mb/s – 10 Gb/s	10 Mb/s – 100 Gb/s
Distance	Relatively short (1 – 100m)	Relatively high (1 – 100,000m)
Immunity to EMI and RFI	Low	High (completely immune)
Immunity to electric hazards	Low	High (completely immune)
Media and connector costs	Lowest	Highest
Installation skills required	Lowest	Highest
Safety precautions	Lowest	Highest

Wireless Media

Properties of Wireless Media

- Wireless media carry electromagnetic signals that represent the binary digits of data communications using radio or microwave frequencies.
- Greatest mobility option

- Copper and fibre are still the most popular physical layer media for network deployments.
- Areas of concern:
    - **Converge area**
      Certain construction materials used in buildings and structures, and the local terrain, will limit the effective coverage
    - **Interference**
      Susceptible to interference and can be disrupted by such common devices as household cordless phones, some types of fluorescent lights, microwave ovens, and other wireless communications.
    - **Security**
      Requires no access to a physical strand of media → non-authorised devices and users can gain access to the transmission. Network security is a major component of wireless network administration.
    - **Shared medium**
      WLANs operate in half-duplex, which means only one device can send or receive at a time. The wireless medium is shared amongst all wireless users. The more users needing to access the WLAN simultaneously, results in less bandwidth for each user.

Types of Wireless Media

- IEEE + telecommunications industry standards for wireless data communication:
    - **Wi-Fi:** *Standard IEEE 802.11*
        - WLAN
        - WLAN uses a contention-based protocol known as Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) → Wireless NIC must listen before transmitting to determine if the radio channel is clear. If another wireless device is transmitting, then the NIC must wait until the channel is clear.
    - **Bluetooth:** *Standard IEEE 802.15*
        - Wireless Personal Area Network (WPAN)
        - A device pairing process to communicate over distances from 1 to 100m
    - **WiMAX:** *Standard IEEE 802.16*
        - Worldwide Interoperability for Microwave Access (WiMAX)
        - Point-to-multipoint topology to provide wireless broadband access
- In each of these standards, physical layer specifications are applied to areas that include:
    - Data to radio signal encoding
    - Frequency and power of transmission
    - Signal reception and decoding requirements
    - Antenna design and construction
- Wi-Fi is a trademark of the Wi-Fi Alliance

Wireless LAN

- Wireless LAN requires the following network devices:
    - **Wireless Access Point**
      Concentrates the wireless signals from users and connects to the existing copper-based network infrastructure. Wireless routers integrate the functions of a router, switch, and access point into one device.
    - **Wireless NIC adapters**
      Provide wireless communication capability to each network host.
- Benefits include: savings on costly premises wiring and the convenience of host mobility
- Network administrators need to develop and apply stringent security policies and processes to protect wireless LANs from unauthorised access and damage.

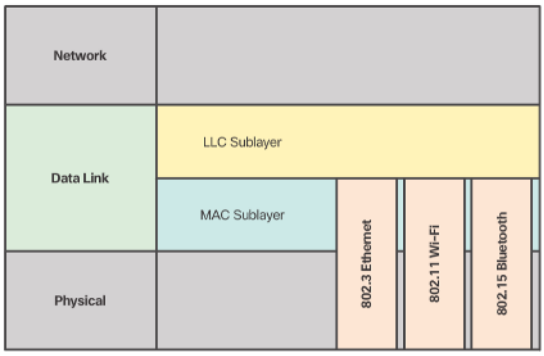
4.3 Data Link Layer Protocols

Purpose of the Data Link Layer

The Data Link Layer

- The data link layer prepare network data for the physical network
- The data link layer is responsible for:
  - Allowing the upper layers to access the media
  - Accepting Layer 3 packets and packaging them into frames
  - Preparing network data for the physical network
  - Controlling how data is placed and received on the media
  - Exchanging frames between nodes over a physical network media (such as UTP, fibre-optic)
  - Receiving and directing packets to an upper layer protocol
  - Performing error detection
- The Layer 2 notation for network devices connected to a common media is called a node → Nodes build and forward frames
- The data link layer effectively separates the media transitions that occur as the packet is forwarded from the communication processes of the higher layers
- The data link layer receives packets from and directs packets to an upper layer protocol

Data Link Sublayers



Divided into two sublayers:

- **Logical Link Control (LLC)**
  - Upper sublayer communicates with the network layer
  - Places information in the frame that identifies which network layer protocol is being used for the frame
  - Information allows multiple Layer 3 protocols to utilise the same network interface and media.
- **Media Access Control (MAC)**
  - Lower sublayer defines the media access processes performed by the hardware.
  - Provides data link layer addressing and access to various network technologies.
- The LLC communicates with the network layer while the MAC sublayer allows various network access technologies
- The MAC sublayer also communicates with wireless technologies such as Wi-Fi and Bluetooth to send and receive frames wirelessly.

Media Access Control

- Layer 2 protocols specify the encapsulation of a packet into a frame and the techniques for getting the encapsulated packet on and off each medium
- Data link layer protocols govern how to format a frame for use on different media
- Media Access Control method→ technique used for getting the frame on and off the media
- Without the data link layer, network layer protocols such as IP, would have to make provisions for connecting to every type of media that could exist along a delivery path → IP would have to adapt every time a new network technology or medium was developed
  - This is a key reason for using a layered approach to networking.

Providing Access to Media

- Router interfaces encapsulate the packet into the appropriate frame, and a suitable media access control method is used to access each link.
- At each stop along the path, a router:
  - Accepts a frame from a medium
  - De-encapsulates the frame
  - Re-encapsulates the packet into a new frame
  - Forwards the new frame appropriate to the medium of that segment of the physical network

Data Link Layer Standards

- Data link layer protocols are generally not defined by Request for Comments (RFCs)
- Internet Engineering Task Force (IETF) maintains the functional protocols and services for the TCP/IP protocol suite in the upper layers → does not define functions and operation of the model's network access layer
- Engineering organisations that define the open standard protocols that apply to the layer include:

- Institute of Electrical and Electronics Engineers (IEEE)
- International Telecommunication Union (ITU)
- International Organization for Standardization (ISO)
- American National Standards Institute (ANSI)

4.4 Media Access Control

Topologies

Controlling Access to the Media

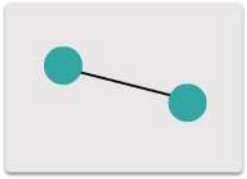
- Regulating the placement of data frames onto the media is controlled by the media access control sublayer
- The protocols at the data link layer define the rules for access to different media
- Define if and how the nodes share the media.
- Media access control method used depends on:
  - *Topology* → how the connection between the nodes appears to the data link layer
  - *Media sharing* → how the nodes share the media. Point-to-point or shared.

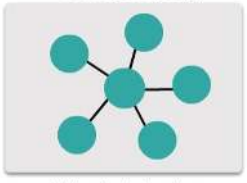
Physical and Logical Topologies

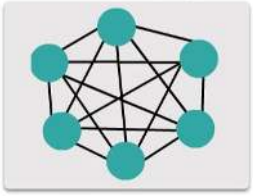
- The topology of a network is the arrangement or relationship of the network devices
- It is the logical topology that influences the type of network framing and media access control used.
- Viewed in two ways:
  - **Physical topology**
    - Physical connections and identifies how end devices and infrastructure devices such as routers, switches, and wireless access points are interconnected
    - Usually point-to-point or star.
  - **Logical topology**
    - The way a network transfers frames from one node to the next.
    - Consists of virtual connections between the nodes of a network.
    - These logical signal paths are defined by data link layer protocols.
    - The logical topology of point-to-point links is relatively simple while shared media offers different access control methods

WAN Topologies

Common Physical WAN Topologies

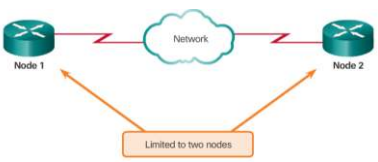

Point-to-point topology


Hub and spoke topology


Full mesh topology

- Interconnected using the following physical topologies:
  - **Point-to-Point**
    - Simplest
    - Permanent link between two endpoints
    - Very popular for WAN topologies
  - **Hub and Spoke**
    - WAN version of the star topology
    - Central site interconnects branch sites using point-to-point links
  - **Mesh**
    - High availability
    - Requires that every end system be interconnected to every other system
    - Significant administrative and physical costs
    - Each link is essentially a point-to-point link to the other node
    - Variation is a partial mesh – some but not all end devices are interconnected

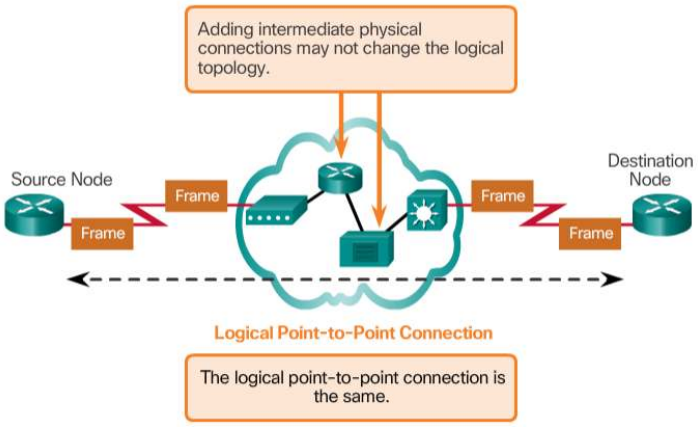
Physical Point-to-Point Topology



- Directly connect two nodes → simple, only travels between two nodes
- Do not have to share the media with other hosts →media one end to the other
- Does not have to make any determination whether incoming frame is for another node

Logical Point-to-Point Topology

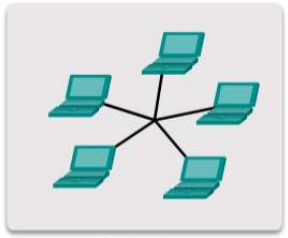
- Can be physically connected via a number of intermediate device
- Use of physical devices in the network does not affect the logical topology
- Virtual circuit → a logical connection created within a network between two network devices.
- Media access method used by the data link protocol is determined by the logical point-to-point topology → logical point-to-point connection between two nodes may not necessarily be between two physical nodes at each end of a single physical link.

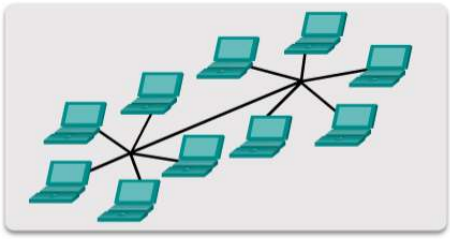


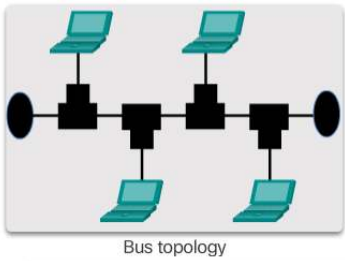
LAN Topologies

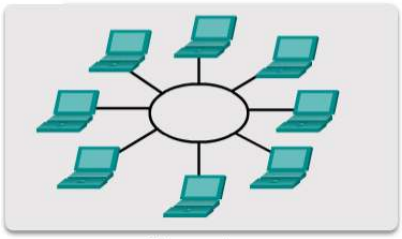
Physical LAN Topologies

- In LANs, end devices can be interconnected using:
  - **Star**
    - End devices are connected to a central intermediate device
    - Used to use Ethernet hubs → now use Ethernet switches
    - Easy to install, scalable and easy to troubleshoot.
  - **Extended Star**
    - Ethernet switches interconnect other star topologies
  - **Bus**
    - All end systems are chained to each other and terminated in some form on each end.
    - Infrastructure devices (switches) are not required to interconnect the end devices.
    - Use coax cables were used in legacy Ethernet networks because it was inexpensive and easy to set up.
  - **Ring**
    - End systems are connected to their respective neighbour forming a ring.
    - Unlike the bus topology→ ring does not need to be terminated
    - Used in legacy Fibre Distributed Data Interface (FDDI) and Token Ring networks.


Star topology


Extended star topology


Bus topology

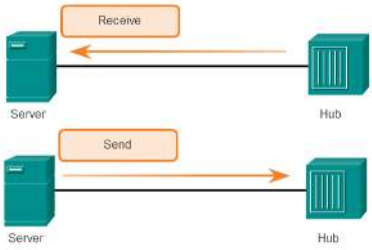

Ring topology

Half and Full Duplex

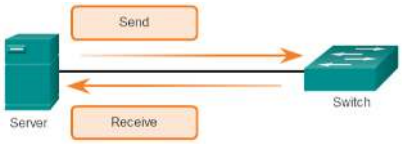
- Refer to the direction of data transmission between two devices.
- Half-duplex → restrict the exchange of data to one direction at a time
- Full-duplex → allows only one device to send or receive data to happen simultaneously
- Two interconnected interfaces operate using the same duplex mode → creates inefficiency and latency on the link.

Half-duplex communication

- Both devices can transmit and receive on the media but cannot do so simultaneously
- Used in legacy bus topologies and with Ethernet hub
- WLANs operate in half-duplex
- Allows only one device to send or receive at a time on the shared medium and is used with contention-based access methods.



Full-duplex communication



- Both devices can transmit and receive on the media at the same time
- Data link layer assumes that the media is available for transmission for both nodes at any time
- Ethernet switches operate in full-duplex mode by default, but can operate in half-duplex if connecting to a device such as an Ethernet hub.

Media Access Control Methods

- Multi-access methods → share a common medium with multiple nodes
  - **E.g.** LANs and WLANs
- Access control methods for shared media:
  - **Contention-based access**
    - All nodes operating in half-duplex compete for the use of the medium → there is a process if more than one device transmits at the same time.
    - **E.g.** Ethernet LANs using hubs and WLANs
  - **Controlled access**
    - Each node has its own time to use the medium
    - Deterministic types of networks are inefficient → device must wait its turn to access the medium
    - **E.g.** Legacy Token Ring LANs

*Contention-Based Access – CSMA/**CD***

- The Carrier Sense Multiple Access/**Collision Detection** (CSMA/CD)
- Process to govern when a device can send and what happens when multiple devices send at the same time
- **E.g.** LANs, Ethernet LANs with hubs, and legacy Ethernet bus networks

Process:

1. PC1 has an Ethernet frame to send to PC3
2. PC1's NIC needs to determine if anyone is transmitting on the medium. If it does not detect signal, it will assume the network is available to send
3. PC1's NIC sends the Ethernet frame
4. Ethernet hub (multiport repeater) receives the frame. Any bits received on an incoming port are regenerated and sent out to all other ports
5. If PC2 wants to transmit, but is currently receiving a frame, it must wait until the channel is clear
6. All devices attached to the hub will receive the frame. Frame has a destination data link address for PC3 so only that device will accept and copy in the entire frame → All other devices' NICs will ignore the frame

- If two devices transmit at the same time, a collision will occur.
  - NIC compares data transmitted with data received, or by recognising the signal amplitude is higher than normal on the media
  - Data sent by both devices will be corrupted and will need to be resent.

*Contention-Based Access – CSMA/**CA***

- Carrier Sense Multiple Access/**Collision Avoidance** (CSMA/CA)
- Uses a method similar to CSMA/CD to detect if the media is clear
- Additional techniques:
  - Does not detect collisions but attempts to avoid them by waiting before transmitting → each device that transmits includes the time duration that it needs for the transmission
  - Receiver returns an acknowledgment so that the sender knows the frame arrived.
- Contention-based systems do not scale well under heavy media use

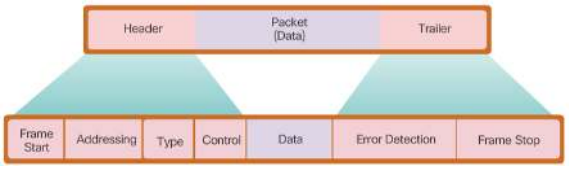
Data Link Frame

The Frame

- Frame → data link layer prepares a packet for transport across the local media by encapsulating it with a header and a trailer
- Description of a frame is a key element of each data link layer protocol
- 3 parts:
  - *Header*
  - *Data*
  - *Trailer*
- Structure of frame and fields contained in the header and trailer vary
- In a fragile environment more controls are needed to ensure delivery → header and trailer fields are larger as more control information is needed

Frame Fields

- Framing breaks the stream into decipherable groupings
- Control information in header and trailer
- Format gives physical signals a structure that can be received by nodes and decoded
- Field types:
  - **Frame start and stop indicator flags**
    Identifies beginning and end limits of the frame
  - **Addressing**
    Indicates source and destination nodes on the media
  - **Type**
    Identifies layer 3 protocol in the data field
  - **Control**
    Identifies special flow control services (such as QoS)
  - **Data**
    Contains frame payload (packet header, segment header, data)
  - **Error Detection**
    Used for error detection and are included after the data to form the trailer



- Not all include these fields
- Trailer → added from the data link layer, used to determine if the frame arrived without error. Placing a logical or mathematical summary of the bits that comprise the frame in the trailer to find error.
  - Added at the data link layer because the signals on the media could be subject to interference, distortion, or loss that would substantially change the bit values that those signals represent.

Layer 2 Address

- The data link layer provides addressing that is used in transporting a frame across a shared local media
- Device addresses at this layer are referred to as physical addresses
- Data link addressing is contained within frame header → frame destination node and source
- Physical addresses do not indicate on what network the network device is located → unique to device
- A device-specific address cannot be used to locate a device on large networks
- Addresses at this layer have no meaning beyond the local network.
- If the data must pass onto another network segment, an intermediate device, such as a router, is necessary.

LAN and WAN Frames

- Each protocol performs media access control for specified Layer 2 logical topologies → number of different network devices can act as nodes that operate at the data link layer when implementing protocols
- Layer 2 protocol used for a particular network topology is determined by the technology used to implement that topology → also determined by the size of the network
- LAN typically uses a high bandwidth → carrying signals for WANs over distances results in low bandwidth

- Data link layer protocols include:
  - Ethernet
  - 802.11 Wireless
  - Point-to-Point Protocol (PPP)
  - HDLC
  - Frame Relay

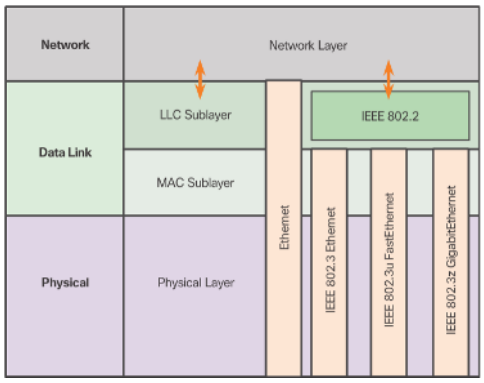
CHAPTER 5 – Ethernet

5.1 Ethernet Protocol

Ethernet Frame

Ethernet Encapsulation

- Ethernet is the most widely used LAN technology
- Ethernet is defined by data link layer and physical layer protocols
- It is a family of networking technologies that are defined in the IEEE 802.2 and 802.3 standards
- Supports bandwidths of:
  - 10 Mb/s
  - 100 Mb/s
  - 1000 Mb/s (1 Gb/s)
  - 10,000 Mb/s (10 Gb/s)
  - 40,000 Mb/s (40 Gb/s)
  - 100,000 Mb/s (100 Gb/s)



- Ethernet relies on the two separate sublayers of the DLL to operate
- **LLC Sublayer**
  - Handles the communication between the upper layers and lower layers → networking software and device hardware
  - Takes the network protocol data and adds control information to help deliver the packet to the destination node
  - Communicates with upper layers and transitions packet to lower layers
  - Implemented in software and is independent of hardware
  -
- **MAC Sublayer**
  - Implemented by hardware → typically in computer NIC

MAC Sub layer

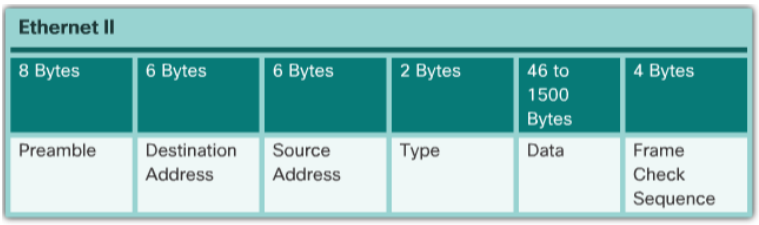
Two primary responsibilities:

- **Data encapsulation**
  - Frame assembly before transmission, frame disassembly upon reception of a frame
  - Adds a header and trailer to the network layer PDU
  - Primary functions:
    - *Frame delimiting*
      - Provides important delimiters used to identify a group of bits that make up a frame → provide synchronisation between transmitting and receiving nodes
    - *Addressing*
      - Encapsulation process contains Layer 3 PDU
      - Data link layer addressing
    - *Error detection*
      - Every frame has a trailer used to detect any errors in transmissions
  - Use of frame aids in transmission of bits and as they are placed on the media + groupings of bits at receiving node
- **Media access control**
  - Responsible for placement and removal of frames on the media
  - Controls access to the media
  - Communicates directly with the physical layer
  - Logical topology of Ethernet is a multi-access bus → all nodes (devices) on a single network segment share the medium
  - Contention-based (any device can try to transmit data across the shared medium whenever it has data to send)
  - Ethernet LANs use full-duplex switches → allow multiple devices to send and receive simultaneously with no collisions.

Ethernet Evolution

- **1973** → creation of Ethernet
- Popular – ability to improve over time
- At DDL, frame structure is nearly identical for all speeds of Ethernet
- Ethernet II is the Ethernet frame format used in TCP/IP networks.

Ethernet II Frame Structure and Field Size



Timeline of Ethernet

Year	Standard	Description
1973	Ethernet	Ethernet invented by Dr Robert Metcalf of Xerox corp
1980	DIX standard Ethernet II	Digital Equipment Corp, Intel and Xerox (DIX) release a standard for 10 Mb/s Ethernet over coaxial cable
1983	IEEE 802.3 10 BASE-5	10 Mb/s Ethernet over thick coaxial cable
1985	IEEE 802.3a 10 BASE-2	10 Mb/s Ethernet over thin coaxial cable
1990	IEEE 802.3i 10 BASE-T	10 Mb/s Ethernet over TP
1993	IEEE 802.3j 10 BASE-F	10 Mb/s Ethernet over fibre-optic
1995	IEEE 802.3u 100 BASE-xx	Fast Ethernet: 100 Mb/s Ethernet over TP and fibre (various standards)
1998	IEEE 802.3z 1000 BASE-X	Gigabit Ethernet over fibre-optic
1999	IEEE 802.3ab 10 BASE-T	Gigabit over TP
2002	IEEE 802.3ae 10G BASE-xx	10 Gigabit Ethernet over fibre (various standards)
2006	IEEE 802.3an 10G BASE-T	10 Gigabit Ethernet over TP

Ethernet Frame Fields

- Minimum frame size is 64 bytes (one with less is known as a RUNT frame or collision fragment)
- Maximum frame size is 1518 bytes
  - Includes destination MAC address field
  - Preamble field is not included
- Frame < 64 bytes → "collision fragment", "runt frame" and automatically discarded
- Frame > 1500 bytes → "jumbo", "baby giant frames" receiving device drops the frame
  - *Dropped frames* are result of collisions or other unwanted signals

Preamble & Start Frame Delimiter

- 7 bytes
- Used for synchronisation between the sending and receiving **devices**
- Used to get the attention of the receiving nodes → tell the receivers to get ready to receive a new frame

Destination MAC Address

- 6 bytes
- Identifier for the intended recipient
- Used by layer 2 to assist devices in determining if a frame is addressed to them
- Address in frame is compared to the MAC address in the device → if a match, the device accepts the frame
- Unicast, multicast or broadcast (because the desination can be one or many)

Source MAC Address

- 6 bytes
- Identifies the frame's originating NIC or interface
- Must be a unicast address (only one originating source)

Ether Type

- 2 bytes
- Identifies the upper layer protocol encapsulated in the Ethernet frame
- Common value are (hexadecimal)
  - 0x800 for IPv4
  - 0x86DD for IPv6
  - 0x806 for ARP

Data

- 46 – 1500 bytes
- Contains encapsulated data from a higher layer (generic layer 3 PDU or IPv4 packet)
- Must be at least 64 bytes long
- If small → additional bits (called a pad) are used to increase the size of the frame to min size

Frame Check Sequence (FCS)

- 4 bytes
- Used to detect errors in a frame
- Uses a cyclic redundancy check (CRC)
  - Sending device includes the results of a CRC in the FCS field
  - Receiving device receives the frame and generates a CRC to look for errors
  - If calculations match → no error occurred.
  - If calculations do not match → indication that the data has changed – frame is then dropped
  - Change in data could be result of a disruption of the electrical signals that represent the bits

Ethernet MAC Addresses

MAC Addresses and Hexadecimal

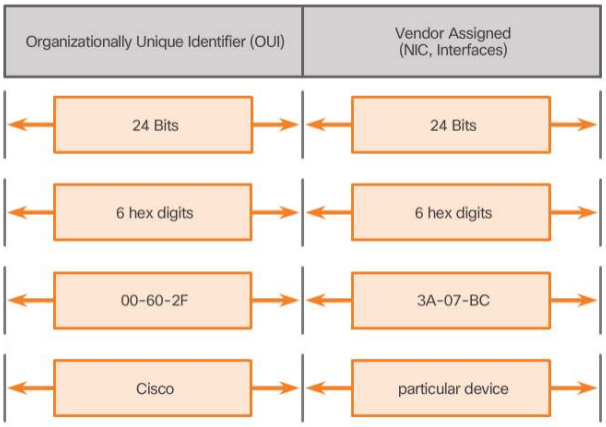
- Ethernet MAC Address is 48-bit binary value expressed as 12 hexadecimal digits
- Common representation of hexadecimal is preceded with "0x"

MAC Address: Ethernet Identity

- In Ethernet, every network device is connected to the same, shared media
  - All nodes would receive every frame transmitted
  - To prevent excessive overhead involved in processing every frame → MAC addresses were created to identify source + destination
- MAC addressing provides method for device identification at the lower layer

MAC Address Structure

- MAC Address value is a direct result of IEEE enforced rules for vendors
- IEEE assigns a 3-byte code → Organisationally Unique Identifier (OUI)
- Rules:
    - All MAC Addresses assigned to a NIC or other Ethernet devices must use that vendor's assigned OUI as the first 3 bytes
    - All MAC Addresses with the same OUI must be assigned a unique value in the last 3 bytes



Frame Processing

- MAC Address → Burned-In Address (BIA)
- When computer first boots → NIC copies MAC address from ROM into RAM
- When NIC receives a frame → examines the destination MAC address stored in RAM
- If there is no match, the device discards the frame
    - If there is a match, passed the frame up the layer
- Ethernet NICs will also accept frames if the destination MAC address is a broadcast or a multicast group of which the host is a member.
- Any device that can be the source or destination of an Ethernet frame must be assigned a MAC address

MAC Address Representations

- Different hardware and software manufacturers represent MAC addresses in different hexadecimal formats:
    - 00-05-9A-3C-78-00 (dashes)
    - 00:05:9A:3C:78:00 (colons)
    - 0005.9A3C.7800 (periods)
- **Ipconfig /all** → used to identify MAC address of an Ethernet adapter

Unicast MAC Address

- Different MAC addresses are used for Layer 2 unicast, broadcast, and multicast communications
- Unicast MAC address → unique address used when a frame is sent from a single transmitting device to a single destination device
- The IP address and MAC address combine to deliver data to one specific destination host
- **Address Resolution Protocol (ARP)**→ process that a source host uses to determine the destination MAC address
- Source MAC address must always be a unicast.

Broadcast MAC Address

- Broadcast packet contains a destination IPv4 address that has all ones (1s) in the host portion
    - All the hosts on that local network (broadcast domain) will receive and process the packet
- When broadcast packet is encapsulated in the Ethernet frame, destination MAC address is the broadcast MAC address of FF-FF-FF-FF-FF-FF in hexadecimal (48 ones in binary).

Multicast MAC Address

- Devices that belong to a multicast group are assigned a multicast group IP address
    - Range of IPv4 multicast addresses is 224.0.0.0 to 239.255.255.255
- **E.g.** a multicast address would be remote gaming
- Requires corresponding multicast MAC address
    - MAC address begins with 01-00-5E
    - Remaining portion is created by converting the lower 23 bits of the IP multicast group address into 6 hexadecimal characters

5.2 LAN Switches

The MAC Address Table

Switch Fundamentals

- Ethernet switch is Layer 2 device → uses MAC addresses for forwarding decisions
- Unaware of protocol being carried in the data portion of the frame
- Consults a MAC address table (MAT) to make a forwarding decision for each frame
    - Can be referred to as a content addressable memory (CAM) table

Learning MAC Addresses

- Switch dynamically builds the MAC address table (MAT) by examining the source MAC address of the frames received on a port
- Forwards the frames by searching for a match between the destination MAC address in the frame and an entry in the MAT
  Process of every frame that enters a switch:
- **Learn – Examining the Source MAC Address**
  Every frame is checked for new information to learn → examines frame's source MAC Address and port number where the frame entered the switch.
    - If source MAC address does not exist → added to the table with incoming port number
    - If source MAC address does exist → updates the refresh timer for the entry. Default time an entry in MAT is for 5 minutes.
- **Forward – Examining the Destination MAC Address**
  If the destination MAC address is a unicast address, switch will look for a match between destination MAC Address of the frame and an entry in MAT
    - If destination MAC address is in MAT → frame will be forwarded to specified port
    - If destination MAC address is not in MAT → frame will be forwarded out all ports except the incoming port (known as an unknown unicast)
- If the destination MAC address is a broadcast or a multicast: frame is also flooded out all ports except the incoming port.

Filtering Frames

- Switch populates its MAT as it receives frames from different devices and examines their source address
    - When the switch's MAT contains the destination MAC address, it is able to filter the frame and forward out a single port.

Switch Forwarding Methods

Frame Forwarding Methods

Forwarding methods for switching data between network ports:

- **Store-and-forward switching**
    - When switch receives the frame → stores data and buffers until the frame has been received
    - During storage process → switch analyses frame for information about its destination + CRC for error detection
    - After confirming integrity of the frame → forwarded out to appropriate port
        - If error is detected, switch discards the frame (doing this reduces the amount of bandwidth consumed by corrupt data)
    - Store-and-forward switching is required for Quality of Service (QoS) analysis on converged networks
- **Cut-through switching**
    - Switch acts upon the data as soon as its received (even if transmission is not complete)
    - Switch buffers just enough of the frame to read the destination MAC address so that it can determine which port to forward the data
    - Looks up destination MAC address in MAT → determines outgoing port → forwards the frame
    - No error checking
      Two types:

- *Fast-forward switching*
  - Lowest level of latency
  - Immediately forwards packet after reading the destination
  - Packets are sometimes relayed with errors
    - Happens infrequently, destination network adapter discards the faulty packet upon receipt
  - typical cut-through method of switching
- *Fragment-free switching*
  - Stores the first 64 bytes of the frame before forwarding → most network errors and collisions occur during the first 64 bytes
  - Tries to enhance fast-forward switching by performing a small error check
  - Known as a compromise between store-and-forward and fast-forward switching
- Some switches are configured to perform cut-through switching on a per-port basis until a user-defined error threshold is reached, and then they automatically change to store-and-forward → when the error rate falls below the threshold, the port automatically changes back to cut-through switching.

Memory Buffering on Switches

- Ethernet switch may use a buffering technique to store frames before forwarding them
  - Buffering may also be used when the destination port is busy due to congestion and the switch stores the frame until it can be transmitted

Methods of memory buffering:

- **Port-based Memory Buffering**
  - Frames are stored in queues that are linked to specific incoming and outgoing ports
  - Frame is transmitted to outgoing port only when the frames ahead of it in the queue have been successful
  - Delay if there is a busy destination port
    - Even if the other frames could be transmitted to open destination ports
- **Shared Memory Buffering**
  - Deposits all frames into a common memory buffer that all the ports on switch share
  - Buffer memory is dynamically allocated
  - Allows packet to be received on one port and then transmitted on another port → without moving to another queue
- Switch keeps a map of frame to port links → map link is cleared after the frame has been successfully transmitted.
- Number of frames stored in the buffer is restricted by the size of the entire memory buffer and not limited to a single port buffer
- Important to *asymmetric switching* → allows for different data rates on different ports

Switch Port Settings

Duplex and Speed Settings

- Critical that the duplex and bandwidth settings match between the switch port and the connected device

Two types of duplex settings:

- **Full-duplex** → both ends of the connection can send and receive simultaneously
- **Half-duplex** → only one end of the connection can send at a time
- Autonegotiation → optional function found on most Ethernet switches and NICs
  - Enables two devices to automatically exchange information about speed and duplex capabilities
  - Switch and device choose the highest performance mode
- **Duplex Mismatch**
  - Common cause of performance issues on 10/100 Mb/s Ethernet links
  - When one port on the link operates at half-duplex and the other runs full-duplex
  - Occurs when port/s are reset and autonegotiation process is not configured, or when only one side has been reconfigured

Auto-MDIX

- Necessary to have the correct cable type defined for each port
- MDIX auto detects the type of connection required and configures the interface accordingly
    - The switch detects the type of cable attached to the port, and configures the interfaces accordingly
    - Either a crossover or a straight-through cable can be used for connections to a copper 10/100/1000 port on the switch, regardless of the type of device on the other end of the connection.

5.3 Address Resolution Protocol

MAC and IP

Destination on Same Network

Two primary addresses assigned to a device on an Ethernet LAN:

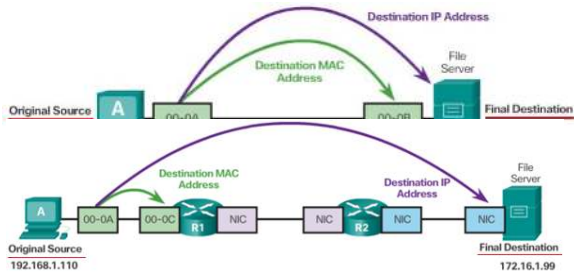
- **Physical Address (MAC)** → used for Ethernet NIC to Ethernet NIC communications on the same network
- **Logical Address (IP)** → used to send the packet from the original source to the final destination
- Most applications use DNS to determine the IP address

Layer 2 Ethernet frame contains

- **Destination MAC Address** → MAC address of the file server's Ethernet NIC
- **Source MAC Address** → MAC address of the device's Ethernet NIC

Layer 3 IP packet contains:

- **Source IP Address** → IP address of the original source
- **Destination IP address** → IP address of the final destination



Destination Remote Network

- Destination MAC address will be the address of the default gateway, the router's NIC.
- Routers examine the destination IP address to determine the best path to forward the IP packet
- When router receives the Ethernet frame, it de-encapsulates Layer 2 information
- Using the destination IP address → determines the next-hop device and then encapsulates the IP packet in a new data link frame for the outgoing interface
- Along each link in the path, IP packet is encapsulated in a frame specific to the particular data link technology associated with that link
- If next-hop device is the final destination → destination MAC address will be that of the device's Ethernet NIC
- Address Resolution Protocol (ARP) → how the IP addresses of the IP packets in a data flow are associated with the MAC addresses on each link along the path

ARP

Introduction to ARP

When a device sends an Ethernet frame, it contains two addresses:

    - Destination MAC Address
    - Source MAC Address
- To determine the destination MAC address, the device uses ARP
  ARP provides functions:
- Resolving IPv4 addresses to MAC addresses
- Maintaining a table of mappings

ARP Functions

Resolving IPv4 Addresses to MAC Addresses

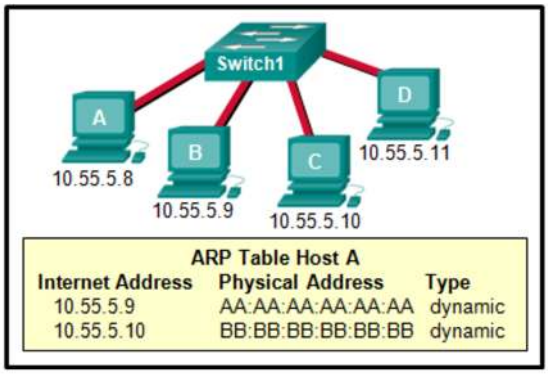
- ARP table/cache

- When packet is sent to the data link layer to be encapsulated→ device refers to a table in its memory to find the MAC address that is mapped to the IPv4 address
- Stored in RAM

- Sending device will search ARP table for a destination IPv4 address and a corresponding MAC address
  - If destination address is on the same network → device will search ARP table for the address
  - If destination address is on a different network → device will search ARP table for the address of the default gateway
- Search is for an IPv4 address and a corresponding MAC address for the device
- Table binds an IPv4 address with a MAC address
  - Relationship between two values is called a *map* → can locate an IPv4 address and discover MAC address
  - Temporarily saves (caches) the mapping for the devices on the LAN
- If there is no entry is found, then the device sends an ARP request.

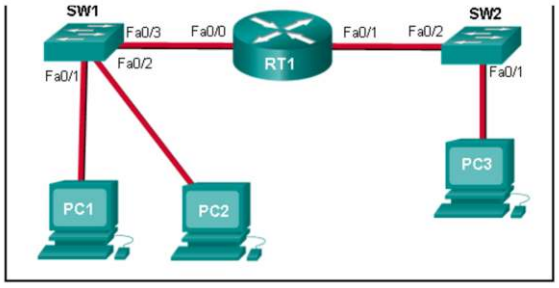
ARP Request

- An ARP request is sent when a device needs a MAC address associated with an IPv4 address
- ARP messages are encapsulated directly within an Ethernet frame
- No IPv4 header
- Includes:
  - Target IPv4 address → requires a corresponding MAC address
  - Target MAC address → unknown MAC address (empty in the ARP request message)
- Encapsulated in an Ethernet frame using header information:
  - Destination MAC address
  - Source MAC address
  - Type → ARP messages have a type field of 0x806 (informs the receiving NIC that the data portion of the frame needs to be passed to the ARP process)
- ARP requests are broadcasts → flooded out all ports by the switch except the receiving port
- Every device must process the ARP request to see if the target IPv4 address matches its own
- Now, look at the below example. If the address of a device is not in the table yet then a broadcast will be sent out to all devices. → the host wanted then specifies its MAC



Refer to the exhibit. A switch with a default configuration connects four hosts. The ARP table for host A is shown. What happens when host A wants to send an IP packet to host D?

- Host A sends out a broadcast of FF:FF:FF:FF:FF:FF. Every other host connected to the switch receives the broadcast and host D responds with its MAC address.



Refer to the exhibit. PC1 issues an ARP request because it needs to send a packet to PC2. In this scenario, what will happen next?

- RT1 will send an ARP reply with its Fa0/0 MAC address.
- SW1 will send an ARP reply with its Fa0/1 MAC address.
- SW1 will send an ARP reply with the PC2 MAC address.
- PC2 will send an ARP reply with its MAC address.

Removing Entries from an ARP Table

- ARP cache timer removes ARP entries that have not been used for a specified period of time
  - Times differ for the devices OS
- Commands can also be used to manually remove all/ some of the entries in the table
- After entry is removed, process for sending ARP request + receiving an ARP reply must occur again to enter the map in the ARP table

ARP Tables

On a cisco router

- **show ip arp** → displays ARP table

Windows PC

- **arp –a** → displays ARP table

ARP Issues

ARP Broadcasts

- As a broadcast frame, an ARP request is received and processed by every device on the local network
- Generally have minimal impact on network performance
  - However, if a large number of devices were to all start accessing network services at the same time → could be some reduction in performance for a short period of time
- Impact on the network will be minimised after the devices send out the initial ARP broadcasts and have learned the necessary MAC addresses.

ARP Spoofing

- Use of ARP can lead to a potential security risk → *ARP spoofing*, or *ARP poisoning*
  - Technique used by an attacker to reply to an ARP request for an IPv4 address belonging to another device
  - Attacker sends an ARP reply with its own MAC address
  - Receiver adds the wrong MAC address to its table and will then send the packets to the attack
- Enterprise level switches include mitigation techniques known as dynamic ARP inspection (DAI)

CHAPTER 6 – Network Layer

6.1 Network Layer Protocols

Network Layer in Communications

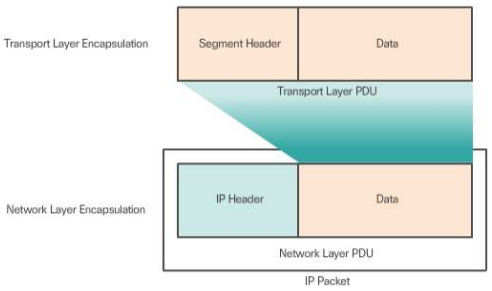
The Network Layer

- Provides services to allow end devices to exchange data across the network
- To accomplish end-to-end transport, layer uses four basic processes:
- **Addressing end devices**
  - Unique IP address for identification on the network
- **Encapsulation**
  - Network layer encapsulates the PDU from the transport layer into a packet
  - Process adds IP header information → Source and destination IP
- **Routing**
  - Network layer provides services to direct packet to the destination
  - To travel to other networks → must be processed by the router
  - Routing → router selects best path and directs the packet to destination host
  - Each router that a packet crosses is called a hop
- **De-encapsulation**
  - When packet arrives at destination → the host checks the IP header of the packet
  - If destination IP = own IP → IP header is removed from the packet
  - After de-encapsulation, Layer 4 PDU is passed up to appropriate service at transport layer
- NL protocols specify the packet structure and processing used to carry the data from one host to another
- Operating without regard of data carried in the packet allows the NL to carry packets for multiple types of communications between multiple hosts

Network Layer Protocols

- IPv4
- IPv6

Characteristics of the IP Protocol



Encapsulating IP

- Encapsulates the transport layer segment by adding an IP header
  - Header used to deliver the packet to the destination host
- Encapsulation enables the services at the different layers to develop and scale without affecting the other layers
- Routers can implement the different network layer protocols to operate concurrently over a network
- Routing performed by intermediate devices only considers the contents of the network layer packet header
- Data portion/ encapsulated transport layer PDU remains unchanged in the process

Characteristics of IP

- Designed to have low overhead
- Provides only the functions that are necessary to deliver a packet
- Does not track and manage the flow of packets
- **Connectionless**
  - No connection with the destination is established before sending data packet
- **Best Effort**
  - IP is inherently unreliable because packet delivery is not guaranteed
- **Media Independent**
  - Operation is independent of the medium – carrying the data

IP – Connectionless

- No dedicated end-to-end connection is created before data is sent → requires no initial exchange of control information to establish an end-to-end connection before packets are forwarded
- Process reduces the overhead of IP
- Senders are unaware whether destination devices are present and functional when sending packets or whether destination receives the packet.

IP – Best Effort Delivery

- IP does not guarantee that all packets that are delivered are received
- Does not have the capability to manage and recover from undelivered/ corrupt packets
    - They contain no information that can inform the sender whether or not it was successful
- Can arrive corrupted or out of sequence
    - If out-of-order or missing, then applications using the data must resolve issues
    - Allows IP to function very efficiently

IP – Media Independent

- IP operates independently of the media that carry the data at lower layers of the protocol stack
- Not limited to any particular medium
- It is the responsibility of the DDL to prepare the packet for transmission
- Does consider the size of the PDU that the medium can transport
    - Maximum Transmission Unit (TMU)
    - Control communication between DDL and NL is the establishment of the max size of a packet
    - DDL passes MTU value to the NL → NL determines how large packet can be
- Fragmentation → when a router must split up a packet when forwarding it from one medium to another

IPv4 Packet

IPv4 Packet Header

- Consists of fields containing important information about the packet
    - Binary numbers which are examined by the Layer 3 process
    - Identify various settings of the IP packet

Fields of IPv4 header:

- **Version**
    - Contains 4-bit value set to 0100 that identifies this as an IP version 4 packet
- **Differentiated Services (DS)**
    - 8-bit field used to determine the priority of each packet
- **Time-to-Live(TTL)**
    - 8-bit value used to limit the lifetime of a packet
    - Sender sets the initial TTL value → decreased by one each time its processed by a router
    - When it gets to 0 the router discards the packet and sends an ICMP Time exceeded message to the source IP
- **Protocol**
    - 8-bit binary value indicates the data payload type that the packet is carrying → enables the NL to pass the data to appropriate upper-layer protocol
- **Source IP Address**
    - 32-bit binary value that represents the source IP address
- **Destination IP Address**
    - 32-bit binary value that represents the destination IP address
- The Internet Header Length (IHL), Total Length, and Header Checksum fields are used to identify and validate the packet
- IPv4 packet uses Identification, Flags, and Fragment Offset fields to keep track of the fragments

IPv6 Packet

Limitations of IPv4

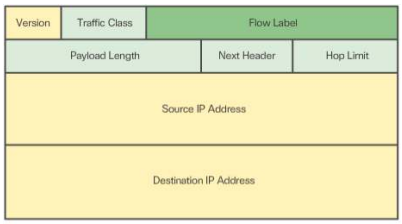
- **IP address depletion**
  - Limited number of unique public IPv4 addresses available
  - Approx. 4 billion IPv4 addresses
  - Potential growth of the world
- **Internet routing table expansion**
  - Number of servers connected to the Internet increases = number of network routes
  - IPv4 routes consume a great deal of memory and processor resources on Internet routers
- **Lack of end-to-end connectivity**
  - Network Address Translation (NAT) → technology commonly implemented within IPv4 networks
  - Provides way for multiple devices to share a single public IPv4 address
    - Because the public IPv4 address is shared, the IPv4 address of an internal network host is hidden. This can be problematic for technologies that require end-to-end connectivity.

Introducing IPv6

- Internet Engineering Task Force (IETF) grew concerned about the issues with IPv4
- IPv6 overcomes the limitations of IPv4 + powerful enhancement with features that better suit current and foreseeable network demands
- Improvements:
  - **Increased address space**
    IPv6 based on 128-bit hierarchal addressing as opposed to 32-bit. IPv6 address space provides 340 undecillion addresses (equivalent to every grain of sand on Earth)
  - **Improved packet handling**
    IPv6 header is simplified with fewer fields
  - **Eliminates the need for NAT**
    Not needed because of so many more addresses. Also avoids some of the NAT-induced application problems experienced

Encapsulating IPv6

- Simplified IPv6 header
  - Efficient packet handling
  - Larger payload for increased throughput and transport efficiency
  - Hierarchal network architecture for routing efficiency
  - Auto-configuration for addresses
  - Elimination of need for NAT between private and public addresses



IPv6 Packet Header

- **Version**
  - 4-bit binary value set to 0110 that identifies packet as IPv6
- **Traffic Class**
  - 8-bit
  - Equivalent to DS field
- **Flow Label**
  - 20-bit
  - Suggests that all packets with the same flow label receive the same type of handling from routers
- **Payload Length**
  - 16-bit
  - Equivalent to the data portion/ payload
- **Next Header**
  - 8-bit
  - Equivalent to the IPv4 Protocol field
  - Indicates the data payload type that the packet is carrying → enabling NL to pass the data to the appropriate upper-layer protocol
- **Hop Limit**
  - 8-bit

    - Replaces IPv4 TTL field
    - Value is decremented by 1 from each router that forwards the packet
    - When counter reaches 0, packet is discarded, and an ICMPv6 Time Exceeded message is forwarded to the sending host → indicating packet did not reach its destination because the hop limit was exceeded
- **Source address**
    - 128-bit
    - Address of sending host
- **Destination address**
    - 128-bit
    - Address of the receiving host
- Can also contain Extension Header (EH) → provide optional NL information
    - Placed in between header and payload
    - For fragmentation, security, support mobility, etc.

6.2 Routing

How a Host Routes

Host Forwarding Decision

- NL directs packets between hosts
- Host can send a packet to:
    - **Itself**
      Host can ping itself →special IPv4 address of 127.0.0.1, (loopback)
    - **Local host**
      Host on the same network (share the same network address)
    - **Remote host**
      Host on a different network
- Whether packet is destined for a local host or remote host → determined by the IPv4 address and subnet mask combination – the source device compared to the IPv4 address and subnet mask of the destination device
- The router connected to the local network segment is referred to as the *default gateway*

Default Gateway

- Network device that can route traffic to other networks → the router that can route traffic out of the local network
- Routes traffic to other networks
- Has a local IP address in the same address range as other hosts on the network
- Can take data in and forward data out

Using the Default Gateway

- Host's routing table will typically include a default gateway
- Host receives the IPv4 address of the default gateway either dynamically (DHCP) or configured manually
- Having a default gateway configured creates a default route in the routing table of the PC
- Default route is the route or pathway your computer will take when it tries to contact a remote network.
    - The default route is derived from the default gateway configuration and is placed in the host computer's routing table

Host Routing Tables

- **route print** or **netstat –r** command displays the routing table
- Displays three sections related to the current TCP/IP network connections:
    - **Interface List**
        - Lists the MAC addresses and the assigned interface number of every network-capable interface on the host (Ethernet, wifi and Bluetooth)
    - **IPv4 Route Table**

- Lists all known IPv4 routes → direct connections, local network and default routes
- **IPv6 Route Table**
  - Lists all known IPv6 routes → direct connections, local network and default routes

Router Routing Tables

Router Packet Forwarding Decision

- When a host sends a packet to another host, it will use its routing table to determine where to send the packet
  - If destination host is on a remote network, packet is forwarded to the default gateway
- When packet arrives at the default gateway (which is usually a router) → router looks at its routing table to determine where to forward packets
- Routing table stores information about:
  - **Directly-connected routes**
    - Routes come from the active router interfaces
    - Routers add a directly connected route when an interface is configured with an IP address + is activated
    - Each of router's interfaces is connected to a different network segment
  - **Remote routes**
    - Routes come from remote networks connected to other routers
    - Can be configured manually/ dynamically
  - **Default route**
    - Default route as a last resort if there is no other route to the desired network in the table

IPv4 Router Routing Table

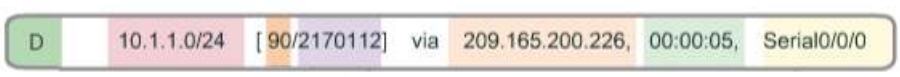
- **show ip route** command is used to display the router's routing table
- Routing table also has information on how the route was learned, the trustworthiness and rating of the route, when the route was last updated, and which interface to use to reach the requested destination.
- When packet arrives at the router interface→ router examines the packet header to determine the destination network
  - If the destination network matches a route in the routing table, the router forwards the packet using the information specified in the routing table.
- If there are two or more possible routes to the same destination, the metric is used to decide which route appears in the routing table.

Directly Connected Routing Table Entries

- When a router interface is configured with an IPv4 address, a subnet mask, and is activated, the following two routing table entries are automatically created:
  - **C** - Identifies a directly-connected network. Directly-connected networks are automatically created when an interface is configured with an IP address and activated
  - **L** - Identifies that this is a local interface. This is the IPv4 address of the interface on the router

Remote Network Routing Table Entries

- Router typically has multiple interfaces configured
- Routing table stores information about both directly-connected networks and remote networks



1. **Route Source**
   Identifies how the network was learned by the router. Common route sources include:
   - S (static route)
   - D (Enhanced Interior Gateway Routing Protocol or EIGRP)
   - O (Open Shortest Path First or OSPF)
2. **Destination Network**
3. **Administrative Distance**

Identifies the administrative distance (i.e., trustworthiness) of the router source. Lower values indicate increased trustworthiness of the route source

4. **Metric**
   Identifies the value assigned to reach the remote network. Lower values indicate preferred routes.
5. **Next-Hop**
   Identifies the IP address of the next router to forward the packet.
6. **Route Timestamp**
   Identifies the last time the route was updated (in hours:minutes:seconds).
7. **Outgoing Interface**
   Identifies the exit interface to use to forward a packet toward the final destination.

Next-Hop Address

- When a packet destined for a remote network arrives at the router, the router matches the destination network to a route in the routing table → if match is found, the router forwards the packet to the next hop address out of the identified interface.
- Directly connected networks with a route source of C and L have no next-hop address → router can forward packets directly to hosts on these networks using the designated interface
- Packets cannot be forwarded by the router without a route for the destination network in the routing table
  - If a route representing the destination network is not in the routing table→ the packet is dropped

6.3 Routers

Anatomy of a Router

A Router is a Computer

- Types of businesses and networks
  - Branch → teleworkers, small businesses, medium-sized branch sites
  - WAN → large businesses, organisations, enterprises
  - Service Providers
- All computers → regardless of their function, size or complexity
- Require:
  - CPUs
  - OSs
  - Memory (RAM, ROM and NVRAM)

Router CPU and OS

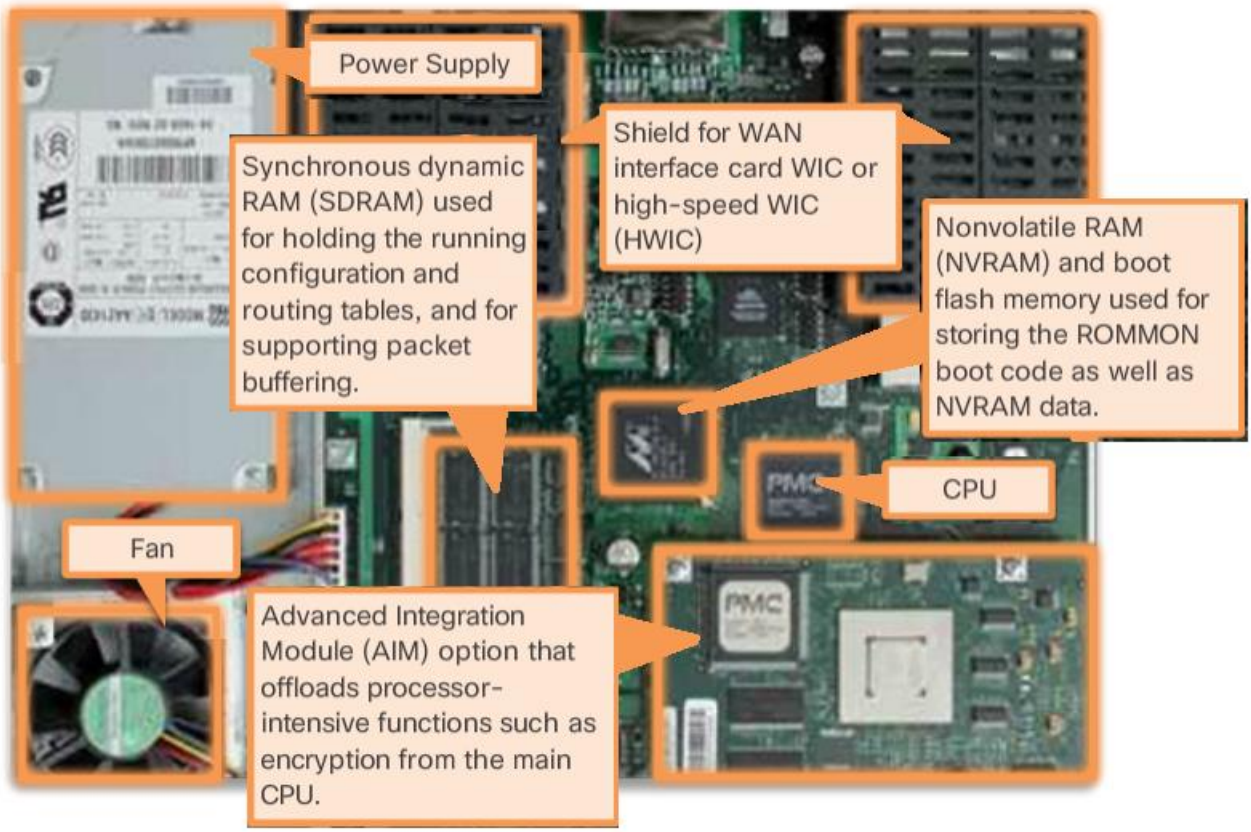
- Router devices require a CPU to execute OS instructions (such as initialisation, routing functions and switching functions)
- The *heatsink* helps dissipate the heat generated by the CPU
- Cisco Internetwork Operating System (IOS) is the system software for most devices
  - Used for routers, LAN switches, small wireless access points, large routers with dozens of interfaces and other devices

Router Memory

- Access to volatile or non-volatile memory storage
  4 types of memory
- **RAM**
  - To store applications, processes, and data needed to be executed by the CPU
  - Cisco routers use a fast type of RAM called synchronous dynamic random access memory (SDRAM)
  - RAM uses the following applications and processes:
    - The IOS image and running configuration file
    - The routing table used to determine the best path to use to forward packets
    - The ARP cache used to map IPv4 addresses to MAC addresses

        - The Packet buffer used to temporarily store packets before forwarding to the destination
- **ROM**
    - Non-volatile memory used to store crucial operational instructions and a limited IOS
    - Firmware embedded on an integrated circuit inside the router only able to be altered by Cisco
    - ROM stores:
        - Bootup information that provides the startup instructions
        - Power-on self-test (POST) that tests all the hardware components
        - Limited IOS to provide a backup version of the IOS. It is used for loading a full feature IOS when it has been deleted or corrupted.
- **NVRAM**
    - Used as the permanent storage for the startup configuration file
- **Flash**
    - Non-volatile computer memory used as permanent storage for the IOS and other system related files (log files, voice config files, HTML files, backup configs, etc)
    - When router is rebooted → IOS is copied from flash into RAM
- Flash is upgradable

Inside a Router



Connect to a router

Enhanced High-speed WAN Interface Card (eHWIC) slots labeled as eHWIC 0 and eHWIC 1 to provide modularity and flexibility by enabling the router to support different types of interface modules, including serial, digital subscriber line (DSL), switch port, and wireless.

Compact Flash slots labeled as CF0 and CF1 to provide increased storage flash space upgradable to 4 GB compact flash card per slot. By default, CF0 is populated with a 256 MB compact flash card and is the default boot location.

Auxiliary (AUX) RJ-45 port for remote management access similar to the Console port. Now considered a legacy port as it was used to provide support for dial-up modems.

Console ports for the initial configuration and command-line interface (CLI) management access. Two ports are available; the commonly used regular RJ-45 port and a new USB Type-B (mini-B USB) connector. However, the console can only be accessed by one port at a time.

Gigabit Ethernet interfaces labeled as GE0/0 and GE0/1. Typically used to provide LAN access by connecting to switches and users, or to interconnect to another router.

USB ports labeled as USB 0 and USB 1 to provide additional storage space similar to flash.

LAN and WAN Interfaces

- Connections can be grouped:
  - In-band router interfaces
    - LAN (i.e. Gigabit Ethernet) and WAN (i.e., eHWICs) interfaces
    - Configured with IP addressing to carry user traffic.
    - Ethernet interfaces are the most common LAN connections, while common WAN connections include serial and DSL interfaces
  - Management ports
    - Console and AUX ports
    - Used to configure, manage, and troubleshoot the router
    - Unlike LAN and WAN interfaces, management ports are not used for packet forwarding user traffic
- Several ways to access user exec mode:
  - Console
    - Physical management port
    - Provides out-of-band (access via a dedicated management channel that is used for device maintenance purposes only) access to a device
  - Secure Shell (SSH)
    - For remotely establishing a secure CLI connection through a virtual interface, over a network
    - Unlike console connection, SSH connections require active networking services on the device including an active interface configured with an address.
  - Telnet
    - Telnet is an insecure method of remotely establishing a CLI session through a virtual interface, over a network
    - Unlike SSH, Telnet does not provide a securely encrypted connection→ user authentication, passwords, and commands are sent over the network in plaintext
- Telnet + SSH require an inband network connection → an administrator must access the router through one of the WAN or LAN interfaces.
- Inband interfaces receive and forward IP packets
- Every configured and active interface on the router is a member or host on a different IP network
- Each interface must be configured with an IPv4 address and subnet mask of a different network
- Cisco IOS does not allow two active interfaces on the same router to belong to the same network.

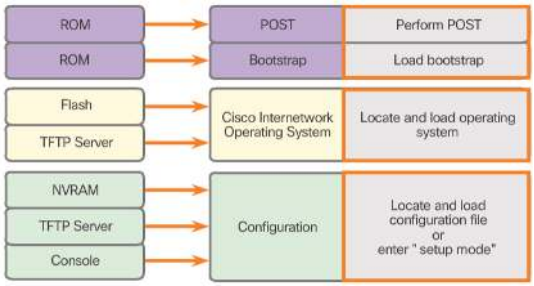
Router Boot-Up

Bootset Files

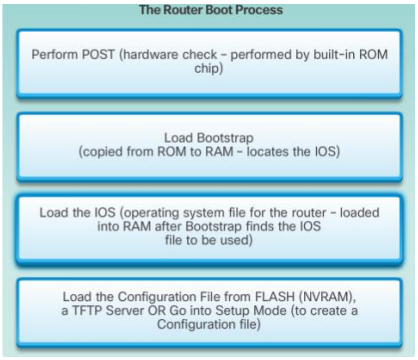
- Routers + switches load IOS image and startup config file into RAM when booted
- Running configuration is modified when the network administrator performs device configurations
- Changes made to the running-config file should be saved to the startup configuration file in NVRAM → in case the router is restarted or loses power.

Router Bootup Process

1. **Performing POST and Load Bootstrap Program**
   - During the Power-On Self-Test (POST) → router executes diagnostics from ROM on several hardware components (CPU, RAM, and NVRAM)
   - After the POST, the bootstrap program is copied from ROM into RAM
   - Main task of the bootstrap program is to locate the Cisco IOS and load it into RAM.
   - *Note*: At this point, if you have a console connection to the router, you begin to see the output on the screen.



2. **Locating and Loading Cisco IOS**
   - IOS is typically stored in flash memory and is copied into RAM for execution by the CPU
   - If the IOS image is not located in flash, then the router may look for it using a Trivial File Transfer Protocol (TFTP) server
   - If full IOS image cannot be located → limited IOS is copied into RAM, which can be used to diagnose problems and transfer a full IOS into Flash memory



3. **Locating and Loading Configuration File**
   - The bootstrap program then copies the startup configuration file from NVRAM into RAM
     → Becomes the running configuration
   - If the startup configuration file does not exist in NVRAM, the router may be configured to search for a TFTP server → If a TFTP server is not found, then the router displays the setup mode prompt.

Show Version Output

- e
- **Show version** command displays information about:
  - Version of the Cisco IOS software currently running on the router
  - Version of bootstrap program
  - Information about hardware configuration – amount of system memory

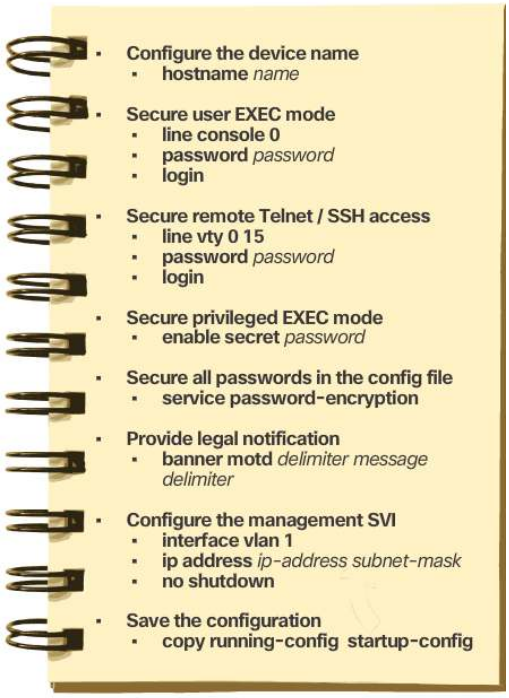
6.4 Configure a Cisco Router

Configure Initial Settings

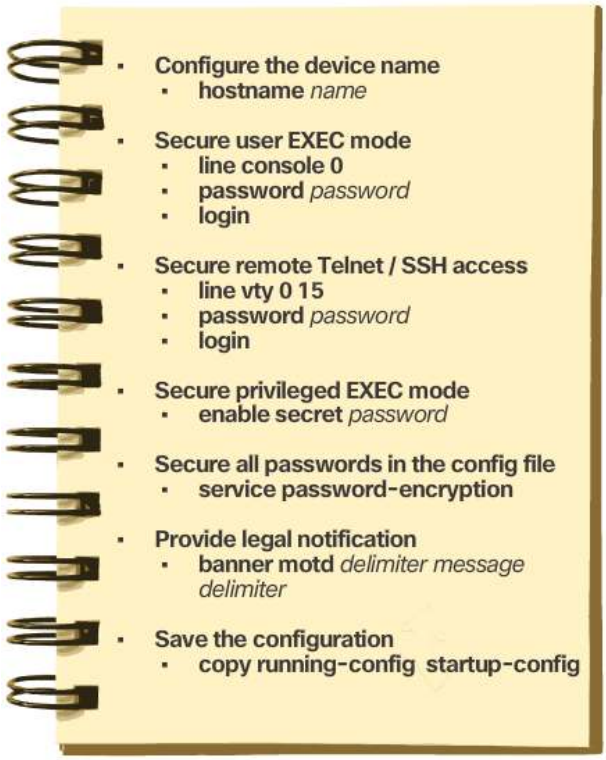
Basic Switch Configuration Steps

- Routers and switches have similar OSs, support similar command structures and support many of the same commands

- Have identical initial configuration steps when implemented in a network



Basic Router Configuration Steps



Configure Interfaces

Configure Router Interfaces

- For routers to be reachable – in-band router interfaces must be configured
- **E.g.** Cisco 1941 router:
  - *Two Gigabit Ethernet interfaces*
  - *A serial WAN interface card (WIC)*
- Good practice to configure a description on each interface to help document the network information
- **no shutdown** command activates the interface
- The interface must also be connected to another device (a hub, a switch, or another router) for the physical layer to be active

```
R1# configure terminal
R1(config)# interface GigabitEthernet 0/0
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# description LAN-10
R1(config-if)# no shutdown
```

Verify Interface Configuration

- **show ip interface brief** command verifies interface configuration
  - **displays all interfaces, IPv4 address and current status**
  - **status 'up' or 'down'**
- **ping** command verifies connectivity
- **show ip route** command displays the contents of the IPv4 routing table stored in RAM
- **show interfaces** command displays statistics for all interfaces on the device
- **show ip interface** command displays the IPv4 statistics for all interfaces on a router

Configure the Default Gateway

Default Gateway for a Host

- Default gateway is only used when the host wants to send a packet to a device on another network
- Default gateway address is generally the router interface address attached to the local network of the host

Default Gateway for a Switch

- A workgroup switch that interconnects client computers is a Layer 2 device
- A Layer 2 switch does not require an IP address to function properly
  - To connect to the switch and administratively manage it over multiple networks → need to configure the SVI with an IPv4 address, subnet mask, and default gateway address
- **ip default-gateway** GC command to configure a default gateway on a switch
  - IP address configured is that of the router interface of the connected switch

CHAPTER 7 – IP Addressing

7.1 IPv4 Network Addresses

Binary and Decimal Conversion

IPv4 Addresses

- Hosts, servers, and network devices use binary addressing
  - Binary IPv4 addressing
- Address consists of a string of 32 bits divided into four sections called *octets*
  - Octet → contains 8 bits/ a byte separated with a dot
  - **E.g.** 11000000.10101000.00001010.00001010
- Addresses are expressed in decimal notation for ease of use

Positional Notation

- A digit represents different values depending on the "position" the digit occupies in the sequence of numbers
- Matches a given number to its positional value

Radix	10	10	10	10
Position in #	3	2	1	0
Calculate	(10^3)	(10^2)	(10^1)	(10^0)
Positional Value	1000	100	10	1

1. **Radix** → First row: identifies the number base/ radix (The decimal notation system is based on 10, therefore the radix is 10)
2. **Position in #** → 2nd row: considers the position of the decimal number starting with, from right to left, 0 (1st position), 1 (2nd position), 2 (3rd position), 3 (4th position). These numbers also represent the exponential value that will be used to calculate the positional value (4th row).
3. **Calculate** → 3rd row: calculates the positional value by taking the radix and raising it by the exponential value of its position. Note: n^0 is always = 1
4. **Positional Value** → first row identifies the number base or radix. Therefore the value listed, from left to right, represents units of thousands, hundreds, tens, and ones.

Decimal Positional Notation (1234)

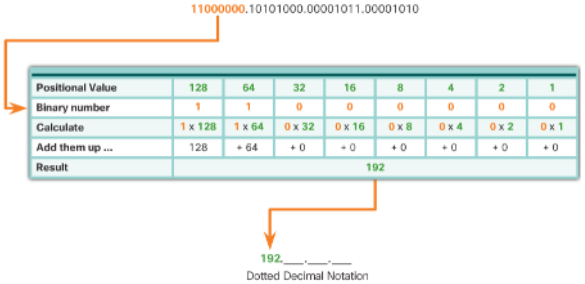
	Thousands	Hundreds	Tens	Ones
Positional Value	1000	100	10	1
Decimal Number	1	2	3	4
Calculate	1 x1000	2 x100	3 x10	4 x1
Add them up ...	1000	+ 200	+ 30	+ 4
Result	1,234			

Binary Positional Notation (11000000)

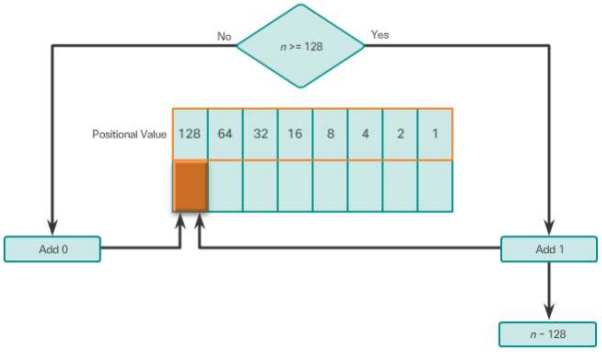
Positional Value	128	64	32	16	8	4	2	1
Binary number	1	1	0	0	0	0	0	0
Calculate	1 x 128	1 x 64	0 x 32	0 x 16	0 x 8	0 x 4	0 x 2	0 x 1
Add them up ...	128	+ 64	+ 0	+ 0	+ 0	+ 0	+ 0	+ 0
Result	192							

Binary to Decimal Conversion

1. Divide the IPv4 address into four 8-bit octets
2. Apply the binary positional value to the first octet binary number and calculate accordingly



Decimal to Binary Conversion



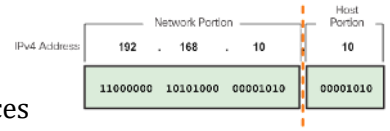
- Useful tool to use is the binary positional value table

1. Is the decimal number octet (n) >= the most-significant bit (128). If no, then enter binary 0 in the 128 positional value. If yes, then add a binary 1 in the 128 positional value and subtract 128 from the decimal number.
2. Is the remainder (n) => the next most-significant bit (64). If no, then add a binary 0 in the 64 positional value, otherwise add binary 1 and subtract 64 from the decimal.
3. Is the remainder (n) => next most-significant bit (32). If no, then add a binary 0 in the 32 positional value, otherwise add binary 1 and subtract 32 from the decimal.

IPv4 Address Structure

Network and Host Portions

- Understanding binary notation → to determine if two hosts are in the same network
  - IPv4 address is a hierarchical address that is made up of a network portion and a host portion
- Within the 32-bit stream:
  - Portion of the bits identify the network
  - Portion of the bits identify the host
- Bits within the network portion of the address must be identical for all devices that reside in the same network
- Bits within the host portion of the address must be unique to identify a specific host within a network



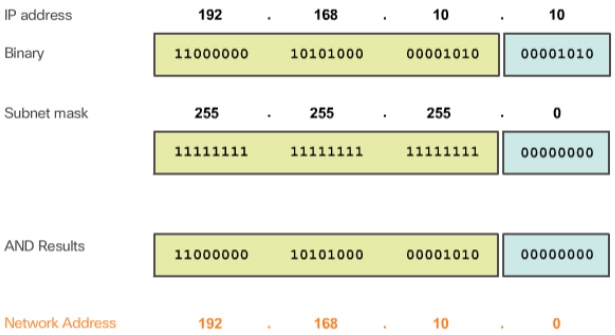
The Subnet Mask

- 3 decimal IPv4 addresses must be configured when assigning an IPv4 configuration to host:
  - **IPv4 address** → Unique IPv4 address of the host
  - **Subnet mask** → Used to identify the network/host portion of the IPv4 address
  - **Default gateway** → Identifies the local gateway (**i.e**. local router interface IPv4 address) to reach remote networks
- The Subnet Mask is used to determine the network address where the device belongs
- Network address represents all devices on the same network
- 32-bit subnet mask: sequence of 1 bits followed by a sequence of 0 bits
- To identify network and host portions of the IPv4 address, subnet mask is compared to the address bit for bit (left to right)
- Subnet mask does not actually contain the network or host portion of an IPv4 address → just tells the computer where to look for these portions in a given IPv4 address

ANDing

- ANDing is one of three basic binary operations used in digital logic (others are OR and NOT)
- Only AND is used in determining network address
- Logical AND is the comparison of two bits

```
1 AND 1 = 1
0 AND 1 = 0
0 AND 0 = 0
1 AND 0 = 0
```



- To identify the network address of an IPv4 host, address is logically ANDed, bit by bit, with the subnet mask

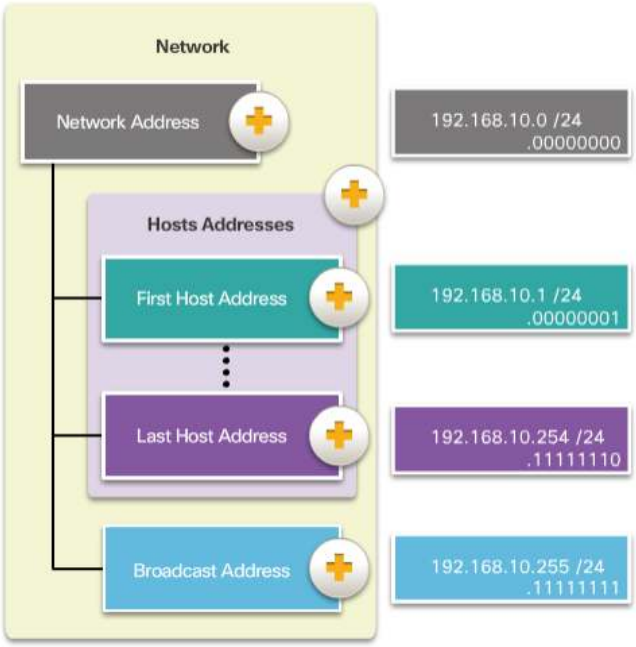
The Prefix Length

- Shorthand method of identifying subnet mask → 'prefix length'
- Number of bits set to 1 in the subnet mask
- Written in 'slash notation' '/' followed by number of bits set to1
- **E.g.** figure →

Subnet Mask	32-bit Address	Prefix Length
255.0.0.0	11111111.00000000.00000000.00000000	/8
255.255.0.0	11111111.11111111.00000000.00000000	/16
255.255.255.0	11111111.11111111.11111111.00000000	/24

Network, Host, and Broadcast Addresses

- Each network address contains (or identifies) host addresses and a broadcast address



Network Address → Address and subnet mask refer to a network. All hosts within the network share the same network address. The host portion is all 0s.

***Host Addresses* →** Unique IP addresses assigned to hosts and devices. The host portion always contains assorted 0s and 1s but never all 0s or all 1s.

First → First available host IP address in that network. The host portion always has all 0s and ends with a 1.

Last → Last available host IP address in that network. The host portion always has all 1s and ends with a 0.

Broadcast Address → A special address that communicates with all hosts in a network. When a host sends a packet to the network broadcast IPv4 address, all other hosts in the network receive the packet. The broadcast address uses the highest address in the network range. The host portion is all 1s.

IPv4 Unicast, Broadcast, and Multicast

Static IPv4 Addresses Assignment to a Host

- Devices can be assigned an IP address either statically or dynamically
- Some devices require a fixed IP address (**E.g.** printers, servers, and networking devices need an IP address that does not change)
  - Therefore given a static IP address
- Assigning hosts static IP addresses is acceptable in small networks
  - Would be time-consuming to enter static addresses on each host in a large network
- Important to maintain an accurate list of static IP addresses assigned to each device.

Dynamic IPv4 Address Assignment to a Host

- In most data networks → user population and their devices change frequently
  - Impractical to statically assign IPv4 addresses for each device
- Use Dynamic Host Configuration Protocol (DHCP)
  - Obtain IP addressing information automatically
  - The host is a DHCP client and requests IP address information from a DHCP server
  - The DHCP server provides an IP address, subnet mask, default gateway, and other configuration information
- Generally the preferred method of assigning IPv4 addresses on large networks
- Not permanent → "leased"
  - When host is taken off the network, address is returned to pool for reuse

IPv4 Communication

- **Unicast**
  Sending a packet from one host to an individual host
- **Broadcast**
  Sending a packet from one host to all hosts
- **Multicast**
  Sending a packet from one host to a selected group of hosts, possibly in different networks

Unicast Transmission

- Used for host-to-host in both client/ server and peer-to-peer network

- Packets use the address of the destination device as destination address and can be routed through an internetwork
- Host address → unicast address applied to end device
- The addresses assigned to the two end devices are used as the source and destination IPv4 addresses
- Source host's IPv4 address = source address, destination host's IPv4 address = destination address.
- Source address is always the unicast address of the originating host
- IPv4 unicast host addresses are in the address range of 0.0.0.0 - 223.255.255.255.

Broadcast Transmission

- Packet contains a destination IPv4 address with all ones (1s) in the host portion
  - All hosts on that local network (broadcast domain) will receive and look at the packet
- Host processes packet as it would a packet addressed to its unicast address
- May be:
  - Directed→ sent to all hosts on a specific network
  - Limited → sent to 255.255.255.255. By default, routers do not forward broadcasts
- Broadcast traffic should be limited so that it does not affect the performance of the network or devices
- Routers separate broadcast domains → subdividing networks can improve network performance by eliminating excessive broadcast traffic

Multicast Transmission

- Reduces traffic by allowing a host to send a single packet to a selected set of hosts that subscribe to a multicast group
- IPv4 has reserved the 224.0.0.0 - 239.255.255.255 addresses as a multicast range
- IPv4 multicast addresses 224.0.0.0 to 224.0.0.255 are reserved for multicasting on the local network
  - A router connected to the local network recognises that the packets are addressed to a local network multicast group and does not forwards them further
- Use of reserved local network multicast address: in routing protocols using multicast transmission to exchange routing information
- Hosts that receive particular multicast data are called multicast clients
- Each multicast group is represented by a single IPv4 multicast destination address → hosts subscribe to the group

Types of IPv4 Addresses

Public and Private IPv4 Addresses

- Public IPv4 addresses are addresses which are globally routed between ISP routers
- Blocks of addresses, *private addresses,* are used by most organizations to assign IPv4 addresses to internal hosts
  - Introduced because in the mid-1990s, there was a depletion of IPv4 address space
  - Not unique
  - Can be used by internal network
- Private address blocks are:
  - 10.0.0.0 /8 or 10.0.0.0 to 10.255.255.255
  - 172.16.0.0 /12 or 172.16.0.0 to 172.31.255.255
  - 192.168.0.0 /16 or 192.168.0.0 to 192.168.255.255
- These addresses are not allowed on the Internet and must be filtered (discarded) by Internet routers
- Most organizations use private IPv4 addresses for their internal hosts
- Private addresses are defined in RFC 1918.
  - RFC 1918 address are not routable in the Internet and must be translated to a public IPv4 address
- Network Address Translation (NAT) → used to translate between private IPv4 and public IPv4 addresses
- Home routers provide the same capability

Special User IPv4 Addresses

- Certain addresses such as the network address and broadcast address cannot be assigned to hosts

- **Loopback addresses (127.0.0.0 /8 or 127.0.0.1 to 127.255.255.254)**
  - Commonly identified as only 127.0.0.1
  - Used by a host to direct traffic to itself
  - **E.g.** Used to test id TCP/IP config is operational
- Link-Local addresses (169.254.0.0 /16 or 169.254.0.1 to 169.254.255.254)
  - Automatic Private IP Addressing (APIPA)
  - Used by a Windows DHCP client to self-configure in the event that there are no DHCP servers available
  - Useful in a peer-to-peer connection
- **TEST-NET addresses (192.0.2.0/24 or 192.0.2.0 to 192.0.2.255)**
  - These addresses are set aside for teaching and learning purposes and can be used in documentation and network examples

Legacy Classful Addressing

- 1981 → Internet IPv4 addresses were assigned using *classful addressing* defined in RFC 790 Divided the unicast ranges into specific classes:
- **Class A (0.0.0.0/8 to 127.0.0.0/8)**
  - to support extremely large networks with more than 16 million host addresses
  - Used a fixed /8 prefix with the first octet to indicate the network address and the remaining three octets for host addresses
  - All class A addresses required that the most significant bit of the high-order octet be a zero → total of 128 possible class A networks.

Class A Specifics	
Address block	0.0.0.0 – 127.0.0.0*
Default Subnet Mask	/8 (255.0.0.0)
Maximum Number of Networks	128
Number of Host per Network	16,777,214
High order bit	0xxxxxxx

- **Class B (128.0.0.0 /16 – 191.255.0.0 /16)**
  - To support the needs of moderate to large size networks with up to approximately 65,000 host addresses.
  - Used a fixed /16 prefix with the two high-order octets to indicate the network address and the remaining two octets for host addresses

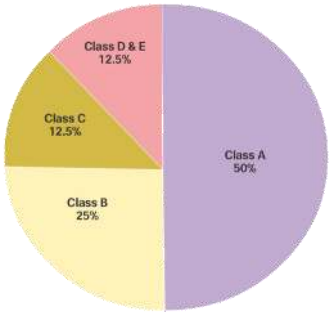
Class B Specifics	
Address block	128.0.0.0 – 191.255.0.0
Default Subnet Mask	/16 (255.255.0.0)
Maximum Number of Networks	16,384
Number of Host per Network	65,534
High order bit	10xxxxxx

- **Class C (192.0.0.0 /24 – 223.255.255.0 /24)**
  -
  - To support small networks with a maximum of 254 hosts.
  - Used a fixed /24 prefix with the first three octets to indicate the network and the remaining octet for the host addresses.
  - The most significant three bits of the high-order octet must be 110 creating over 2 million possible networks.

Class C Specifics	
Address block	192.0.0.0 – 223.255.255.0
Default Subnet Mask	/24 (255.255.255.0)
Maximum Number of Networks	2,097,152
Number of Host per Network	254
High order bit	110xxxxx

- Class D multicast block consisting of 224.0.0.0 - 239.0.0.0
- Class E experimental address block consisting of 240.0.0.0 – 255.0.0.0.

Classless Addressing



- This wasted a great deal of addresses and exhausted the availability of IPv4 addresses
- Not all organizations' requirements fit well into one of these three classes
- Classful addressing was abandoned in the late 1990s → still classful remnants in networks today
- System in use today is referred to as *classless addressing*
- Classless Inter-Domain Routing (CIDR)
- 1993→ IETF created a new set of standards that allowed service providers to allocate IPv4 addresses on any address bit boundary (prefix length) instead of only by a class A, B, or C address. This was to help delay the depletion and eventual exhaustion of IPv4 addresses.

Assignment of IP Addresses

- Public addresses must be unique, and use of these public addresses is regulated and allocated to each organisation separately→ IPv4 and IPv6 addresses
- IPv4 and IPv6 addresses are managed by the Internet Assigned Numbers Authority (IANA)

- IANA manages and allocates blocks of IP addresses to the Regional Internet Registries (RIRs)
- RIRs are responsible for allocating IP addresses to ISPs who in turn provide IPv4 address blocks to organizations and smaller ISPs

7.2 IPv6 Network Addresses

IPv4 Issues

The need for IPv6

- Successor of IPv4
- Larger 128-bit address space
- Provides for 340 undecillion addresses
- Internet Control Message Protocol version 6 (ICMPv6)→ includes address resolution and address auto-configuration not found in ICMP for IPv4
- The depletion of IPv4 address space was motivation for moving to IPv6 → not enough IPv4 addresses to accommodate this growth → IPv4 has a theoretical maximum of 4.3 billion addresses
  - Private addresses + NAT have been instrumental in slowing the depletion of IPv4 address space
  - NAT breaks many applications and has limitations that severely impede peer-to-peer communications.

  Internet of Everything
- No longer just devices like computers and phones → everything from automobiles and biomedical devices, to household appliances and natural ecosystems.

IPv4 and IPv6 Coexistence

- IPv4 and IPv6 will coexist
- Transition is expected to take years
- Migration techniques:
  - **Dual Stack**
    Allows IPv4 and IPv6 to coexist on the same network segment. Dual stack devices run both IPv4 and IPv6 protocol stacks simultaneously.
  - **Tunnelling**
    Method of transporting an IPv6 packet over an IPv4 network. The IPv6 packet is encapsulated inside an IPv4 packet, similar to other types of data.
  - **Translation**
    (NAT64) allows IPv6-enabled devices to communicate with IPv4-enabled devices using a translation technique similar to NAT for IPv4. An IPv6 packet is translated to an IPv4 packet and vice versa.

IPv6 Addressing

IPv6 Address Representation

- Written as a string of hexadecimal values
- Format: x:x:x:x:x:x:x:x (each "x" consisting of four hexadecimal values)
- *Hextet* is the unofficial term used to refer to a segment of 16 bits or four hexadecimal values → each "x" is a sing hextet

***Rule 1** – Omit Leading 0s*

- To help reduce notation → omit any lead 0s in any hextet
  - **E.g.** 01AB → 1AB, 09F0 → 9F0, 0A00 → A00
- Only leading 0s, not trailing 0s

***Rule 2** – Omit all 0 Segments*

- A double colon (::) can replace any single, contiguous string of one or more hextets consisting of all 0s.
  - **E.g.** FE80:0:0:0:123:4567:89AB:CDEF → FE80::123:4567:89AB:CDEF
- Can only be used once within an address
- With both rules applied – compressed format

- **E.g.** 2001:0DB8:0000:1111:0000:0000:0200 → 2001: DB8:0:1111:0:0:0:200 → 2001:DB8:0:1111::200

Types of IPv6 Addresses

IPv6 Address Types

- **Unicast**
  - Uniquely identifies an interface on an IPv6-enabled device.
- **Multicast**
  - Used to send a single IPv6 packet to multiple destinations
- **Anycast**
  - Any IPv6 unicast address that can be assigned to multiple devices. A packet sent to an anycast address is routed to the nearest device having that address
- IPv6 does not have a broadcast address → there is an IPv6 all-nodes multicast address that essentially gives the same result

IPv6 Prefix Length

- IPv6 uses the prefix length to represent the prefix portion of the address
- Does not use the dotted-decimal subnet mask notation
- Prefix length is used to indicate the network portion of an IPv6 address\
- Range from 0 – 128
  - Typical IPv6 prefix length for LANs and most other types of networks is /64
- Prefix/ network portion of the address is 64 bits in length
  - Leaving another 64 bits for the interface ID (host portion) of the address

IPv6 Unicast Addresses

- Most common types of IPv6 unicast addresses are global unicast addresses (GUA) and link-local unicast addresses.
- **Global unicast**
  - Similar to a public IPv4 address
  - Globally unique
  - Internet routable
  - Can be configured statically or assigned dynamically
- **Link-local**
  - Used to communicate with other devices on the same local link (subnet)
  - Their uniqueness must only be confirmed on that link because they are not routable beyond the link
  - Range of FE80::/10
- **Unique local**
  - Have some similarity to RFC 1918 private addresses for IPv4
  - Used for local addressing within a site or between a limited number of sites
  - Should not be routable, should not be translated to a global IPv6 address
  - Range of FC00::/7 to FDFF::/7.

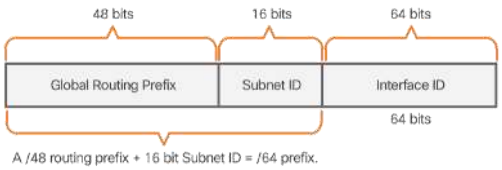
IPv6 Link-Local Unicast Addresses

- An IPv6 link-local address → communicate with other IPv6-enabled devices on the same link and only on that link (subnet)
- Cannot be routed beyond the link from which the packet originated
- Global unicast address is not a requirement → every IPv6-enabled network interface is required to have a link-local address
- If link-local address is not configured manually → device will automatically create its own without communicating with a DHCP server
- IPv6-enabled hosts create an IPv6 link-local address even if the device has not been assigned a global unicast IPv6 address

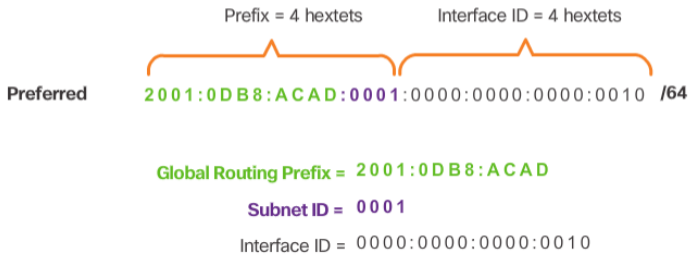
IPv6 Unicast Addresses

Structure of an IPv6 Global Unicast Address

- Globally unique and routable on the IPv6 Internet
- Equivalent to public IPv4 addresses
- ICANN allocates IPv6 address blocks to the five RIRs
- Currently, only global unicast addresses with the first three bits of 001 or 2000::/3 are being assigned (1/8th of the total available IPv6 address space)



- **Global Routing Prefix**
  - GRP, or network, portion of the address that is assigned by the provider, to a customer or site
  - Typically, RIRs assign a /48 global routing prefix to customers
  - The size of the global routing prefix determines the size of the subnet ID.
- **Subnet ID**
  - The Subnet ID is used by an organization to identify subnets within its site
  - The larger the subnet ID, the more subnets available
- **Interface**
  - Equivalent to the host portion of an IPv4 address
  - Interface ID: because a single host may have multiple interfaces, each having one or more IPv6 addresses



Static Configuration of a Global Unicast Address

- **Router Configuration**
  - Most IPv6 configuration and verification commands are similar to IPv4 ones
  - ipv6 → ip
  - command to configure IPv6 global unicast address → **ipv6 address** *ipv6-address/prefix-length*
    - **E.g.** 2001:0DB8:ACAD:0001:/64 (or 2001:DB8:ACAD:1::/64)

```
R1(config)# interface gigabitethernet 0/0
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface gigabitethernet 0/1
R1(config-if)# ipv6 address 2001:db8:acad:2::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface serial 0/0/0
R1(config-if)# ipv6 address 2001:db8:acad:3::1/64
R1(config-if)# clock rate 56000
R1(config-if)# no shutdown
```

- **Host Configuration**
  - Manually configuring the IPv6 address on a host is similar to configuring an IPv4 address
    - Default gateway address configured is the global unicast address of the interface on the same network
    - Default gateway address can be configured to match the link-local address of the interface
- Most network administrators in an IPv6 network will enable dynamic assignment of IPv6 addresses.
- Ways a device can obtain an IPv6 global unicast address automatically:
  - Stateless Address Autoconfiguration (SLAAC)
  - DHCPv6

Dynamic Configuration – SLAAC

- Stateless Address Autoconfiguration (SLAAC)
- Method that allows a device to obtain its prefix, prefix length, default gateway address, and other information from an IPv6 router without the use of a DHCPv6 server
- Relies on the local router's ICMPv6 Router Advertisement (RA) messages to obtain the necessary information.

- IPv6 routers periodically send out ICMPv6 RA messages (every 200 seconds), to all IPv6-enabled devices on the network → RA message will also be sent in response to a host sending an ICMPv6 Router Solicitation (RS) message.
- To enable a router → **ipv6 unicast-routing** command
- The ICMPv6 RA message is a suggestion to a device on how to obtain an IPv6 global unicast address
- RA message includes:
    - **Network prefix + prefix length**
      Tells the device which network it belongs to
    - **Default gateway address**
      IPv6 link-local address → source IPv6 address of the RA message
    - **DNS addresses and domain name**
      Addresses of DNS servers and domain name

  Three options for RA messages:
- *Option 1:* **SLAAC**
    - RA message suggests that the receiving device use the information in the RA message to create its own IPv6 global unicast address and for all other information
    - Stateless → no central server
    - Client device uses the information in the RA message to create its own global unicast address
    - Two parts of the address are created:
        - Prefix → received in the RA message
        - Interface ID → Uses the EUI-64 process/ generates a random 64 bit number

Dynamic Configuration – DHCPv6

- Default for RA message is SLAAC
- Can be configured
- *Option 2:* **SLAAC with a stateless DCHPv6 server**
    - RA message suggests devices use:
        - SLAAC to create its own IPv6 global unicast address
        - The router's link-local address, the RA's source IPv6 address for the DG address
        - A stateless DHCPv6 server to obtain other information such as a DNS server address and a domain name
    - A stateless DHCPv6 server distributes DNS server addresses and domain names. It does not allocate global unicast addresses.
- *Option 3:* **Stateful DHCPv6 (No SLAAC)**
    - Similar to DHCP for IPv4
    - Device can automatically receive its addressing information (including a global unicast address, prefix length, and the addresses of DNS servers) using the services of a stateful DHCPv6 server.
    - RA message suggests devices use:
        - The router's link-local address, the RA's source IPv6 address for the default gateway address.
        - A stateful DHCPv6 server to obtain a global unicast address, DNS server address, domain name and all other information.
    - A stateful DHCPv6 server allocates and maintains a list of which device receives which IPv6 address.

EUI-64 Process and Randomly Generated

- When the RA message is either SLAAC → the client must generate its own Interface ID
    - Only knows the prefix portion of the address
- IEEE defined the Extended Unique Identifier (EUI) or modified EUI-64 process
- Process uses a client's 48-bit Ethernet MAC address, and inserts another 16 bits in the middle of the 48-bit MAC address → creates a 64-bit Interface ID
- EUI is made up of three parts:
    - 24-bit OUI from the client MAC address, but the 7th bit (the Universally/Locally (U/L) bit) is reversed. This means that if the 7th bit is a 0, it becomes a 1, and vice versa.
    - The inserted 16-bit value FFFE (in hexadecimal)
    - 24-bit Device Identifier from the client MAC address

- EUI-64 process:

  Step 1: Divide the MAC address between the OUI and device identifier.
  Step 2: Insert the hexadecimal value FFFE, which in binary is: 1111 1111 1111 1110.
  Step 3: Convert the first 2 hexadecimal values of the OUI to binary and flip the U/L bit (bit 7).

- Advantage of EUI-64 is the Ethernet MAC address can be used to determine the Interface ID → allowing network administrators to easily track IPv6 address to an end-device using the MAC
- **Randomly Generated Interface IDs**
  - Device may use a randomly generated Interface ID instead of using the MAC address and the EUI-64 process (for privacy reasons)
- After the Interface ID is established → can be combined with an IPv6 prefix in RA message to create a global unicast address
- To ensure the uniqueness of any IPv6 unicast address: client may use a process known as Duplicate Address Detection (DAD). (This is similar to an ARP request - for its own address. If there isn't a reply, then the address is unique).

Dynamic Link-Local Addresses

- link-local address is dynamically created using the FE80::/10 prefix and the Interface ID using the EUI-64 process/ randomly generated 64-bit number
- Cisco routers automatically create an IPv6 link-local address whenever a global unicast address is assigned to the interface
- For serial interfaces, the router will use the MAC address of an Ethernet interface
- Drawback to using the dynamically assigned link-local address is its length → challenging to identify and remember assigned addresses
- Common to statically configure IPv6 link-local addresses on routers

Static Link-Local Addresses

- Configuring manually provides the ability to create an address that is recognizable and easier to remember
- Configured using **ipv6 address** *ipv6-address/prefix-length* **link-local**

```
R1(config)# interface gigabitethernet 0/0
R1(config-if)# ipv6 address fe80::1 ?
       Link-local Use link-local address

R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# exit
R1(config)# interface gigabitethernet 0/1
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# exit
R1(config)# interface serial 0/0/0
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)#
```

Verifying IPv6 Address Configuration

- The **show interface** command verifies the IPv6 interface configuration
- The **show ipv6 interface brief** command displays abbreviated output for each of the interfaces
- [up/up] → indicates the Layer 1/Layer 2 interface state
- Each interface has 2 IPv6 addresses:
  1st → link-local unicast address for the interface
  2nd → address for each interface is the global unicast address that was configured
- The link-local address of the router interface is typically the default gateway address for devices on that link or network
- To verify that IPv6 networks and specific IPv6 interface addresses have been installed in the IPv6 routing table → **show ipv6 route** command
  - In a route table, a C next to a route indicates that this is a directly connected network
  - IPv6 is added to the routing table as a connected route if when the router interface is configured with a global unicast address and is in the "up/up" state

- local route has a /128 prefix → used by the routing table to efficiently process packets with a destination address of the router's interface address
- **ping** command is identical to IPv4

IPv6 Multicast Addresses

Assigned IPv6 Multicast Addresses

- IPv6 multicast addresses have the prefix FF00::/8
- Two types: Assigned multicast and Solicited node multicast
- **Assigned Multicast**
  - AM addresses are reserved multicast addresses for predefined groups of devices
  - A single address used to reach a group of devices running a common protocol or service
  - Used in context with specific protocols (such as DHCPv6)
  - Common IPv6 assigned multicast groups:
    FF02::1 All-nodes multicast group
    - All IPv6-enabled devices join
    - packet sent to this group is received and processed by all IPv6 interfaces on the link or network → same effect as broadcast address in IPv4
    - An IPv6 router sends Internet Control Message Protocol version 6 (ICMPv6) RA messages to the all-node multicast group
    - RA message informs all IPv6-enabled devices on the network about addressing information

    FF02::2 All-routers multicast group
    - all IPv6 routers join
    - becomes a member with **ipv6 unicast-routing** GCM command
    - Packet sent to this group is received and processed by all IPv6 routers on the link or network.
  - IPv6-enabled devices send ICMPv6 Router Solicitation (RS) messages to the all-routers multicast address → RS message requests an RA message from the IPv6 router to assist the device in its address configuration

Solicited-Node IPv6 Multicast Addresses

- Similar to the all-nodes multicast address
- Advantage of the address - is mapped to a special Ethernet multicast address
  - Allows Ethernet NIC to filter the frame by examining the destination MAC address without sending it to the IPv6 process to see if the device is the intended target of the IPv6 packet

7.3 Connectivity Verification

ICMP

ICMPv4 and ICMPv6

- Messages (such as in the event of certain errors) are sent using the services of ICMP
- ICMP messages are not required and are often not allowed within a network for security reasons
- Available for both IPv4 and IPv6
- ICMPv6 provides these same services as for ICMPv4 + additional functionality
  Common messages include:
- **Host confirmation**
  - ICMP Echo Message can be used to determine if a host is operational
  - If host is available → responds with an Echo Reply
- **Destination or Service Unreachable**
  - If a host/gateway receives a packet that it cannot deliver→ uses ICMP Destination Unreachable message to notify the source that the destination or service is unreachable
  - Codes for Destination Unreachable:
    - 0 – Net unreachable
    - 1 – Host unreachable

        - 2 – Protocol unreachable
        - 3 – Port unreachable
    - ICMPv6 has similar but slightly different codes for Destination Unreachable messages.
- **Time exceeded**
    - ICMPv4 Time Exceeded message is used by a router to indicate that a packet cannot be forwarded because the Time to Live (TTL) field of the packet was decremented to 0 → router discards the packet and sends a Time Exceeded message to the source host.
    - ICMPv6 sends a Time Exceeded message if the router cannot forward an IPv6 packet because the packet has expired →does not have a TTL field; it uses the hop limit field to determine if the packet has expired.
- **Route redirection**

ICMPv6 Router Solicitation and Router Advertisement Messages

- ICMPv6 includes four new protocols as part of the Neighbour Discovery Protocol (ND or NDP)
- *Messaging between an IPv6 router and an IPv6 device*
    - **Router Solicitation (RS) message**
    - **Router Advertisement (RA) message**
- *Messaging between IPv6 devices*
    - **Neighbour Solicitation message**
    - **Neighbour Advertisement message**
- Neighbor Solicitation and Neighbor Advertisement messages are used for Address resolution and Duplicate Address Detection (DAD)
- **Address Resolution**
    - Used when a device on the LAN knows the IPv6 unicast address of a destination but does not know its Ethernet MAC address
    - To determine MAC - device sends NS message to the solicited node address →device that has the targeted IPv6 address will respond with NA message containing its Ethernet MAC address
- **Duplicate Address Detection**
    - When a device is assigned a global unicast or link-local unicast address → recommended that DAD is performed on the address to ensure that it is unique
    - Device will send an NS message with its own IPv6 address as the targeted IPv6 address → if another device has this address, it will respond with NA message (notifies that address is in use)

Testing and Verification

***Ping** – Testing the Local Stack*

- Testing utility that uses ICMP echo request and echo reply messages to test connectivity between hosts
- To test connectivity to another host on a network, an echo request is sent to the host address using the this command → destination device responds with echo reply
- Ping provides feedback → measures network performance
- Has timeout value → indicative of a problem
- Provides summary
- *Pinging the Local Loopback*
    - For testing the internal configuration of IP on the local host → ping the local loopback address of 127.0.0.1 for IPv4 (::1 for IPv6)
    - Response indicates that IP is properly installed on the host (this response comes from the network layer). Simply tests IP down through the network layer of IP, no that anything else is properly configured

***Ping** – Testing Connectivity to the Local LAN*

- Ping to test the ability of a host to communicate on the local network
- Done by pinging the IP address of the gateway of the host → ping to the gateway indicates that the host and the router interface serving as the gateway are both operational on the local network
- The gateway address is most often used because the router is normally always operational

- If either the gateway or another host responds, then the local host can successfully communicate over the local network
- If the gateway does not respond but another host does, this could indicate a problem with the router interface serving as the gateway
    - Wrong gateway address has been configured on the host
    - Router interface may be fully operational but have security applied to it that prevents it from processing or responding to ping requests

Ping *– Testing Connectivity to Remote*

- Test the ability of a local host to communicate across an internetwork
- If successful, the operation of a large piece of the internetwork can be verified.
- Confirms communication on:
    - The local network,
    - The operation of the router serving as the gateway
    - The operation of all other routers that might be in the path between the local network and the network of the remote host
    - Functionality of the remote host can be verified → If the remote host could not communicate outside of its local network, it would not have responded

Traceroute *– Testing the Path*

- Traceroute (tracert) is a utility that generates a list of hops that were successfully reached along the path
    - Provide important verification and troubleshooting information
    - If the data reaches the destination, then the trace lists the interface of every router in the path between the hosts
    - If the data fails at some hop along the way, the address of the last router that responded to the trace can provide an indication of where the problem or security restrictions are found
- **Round Trip Time**
    - Using traceroute provides round trip time for each hop along the path and indicates if a hop fails to respond
    - Time a packet takes to reach the remote host and for the response from the host to return
    - An asterisk (*) is used to indicate a lost or unreplied packet
    - Locates problematic router
- **IPv4 TTL and IPv6 Hop Limit**
    - Traceroute then progressively increments the TTL field (2, 3, 4...) for each sequence of messages
    - Provides the trace with the address of each hop as the packets timeout further down the path
    - TTL field continues to be increased until the destination is reached, or it is incremented to a predefined maximum

CHAPTER 8 – Subnetting IP Networks

8.1

Network Segmentation

Broadcast Domains

- Devices use broadcasts to locate:
  - Other devices
    A device uses ARP which sends layer 2 broadcasts to a known Ipv4 address on the local network to discover the associated MAC address
  - Services
    Host typically acquires it IP address configuration using DHCP which sends broadcasts on the local network to locate DHCP server
- Switches propagate broadcasts out all interfaces except the interface on which it was received
- Routers do not propagate broadcasts at all
- Router interface connects to a broadcast domain → broadcasts are only propagated within a specific broadcast domain

Problems with Large Broadcast Domains

- Large broadcast domain is a network that connects many hosts
- These hosts generate excessive broadcasts and negatively affect the network
  - Slow network operations due to the significant amount of traffic
  - Slow device operations because a device must accept and process each broadcast packet
- Solution: reduce the size of the network to create smaller broadcast domains → 'subnetting'
- Broadcasts are only propagated within the smaller broadcast domains → **E.g.** a broadcast in LAN 1 would not propagate to LAN 2
- Prefix length has changes → the basis of subnetting; using host bits to create additional subnets

Reasons for Subnetting

- Reduces overall network traffic and improves network performance
- Enables administrator to implement security policies → which subnets are allowed or not allowed to communicate
- Managing network devices by grouping into subnets that are determined by:
  - Location
  - Organisational unit
  - Device type
  - Etc.

Subnetting an IPv4 Network

Octet Boundaries

- IP address and subnet mask configured on the router interface are used to identify the specific broadcast domain
- Pv4 subnets are created by using one or more of the host bits as network bits
  - By extending the subnet mask to borrow some of the bits from the host portion of the address to create additional network bits
  - More bits borrowed → more subnets can be defined
- Most easily subnetted at the octet boundary (/8, /16 and /24

Prefix Length	Subnet Mask	Subnet Mask in Binary (n = network, h = host)	# of hosts
/8	255.0.0.0	nnnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh 11111111.00000000.00000000.00000000	16,777,214
/16	255.255.0.0	nnnnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh 11111111.11111111.00000000.00000000	65,534
/24	255.255.255.0	nnnnnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh 11111111.11111111.11111111.00000000	254

Subnetting on the Octet Boundary

Example

- An enterprise has chosen the private address 10.0.0.0/8 as its internal network address. That network address can connect 16,777,214 hosts in one broadcast domain.

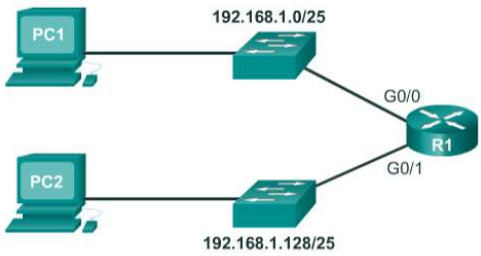
- Subnet the 10.0.0.0/8 address at the octet boundary of /16 → would provide the enterprise the ability to define up to 256 subnets (i.e., 10.0.0.0/16 – 10.255.0.0/16) with each subnet capable of connecting 65,534 hosts.
- First two octets identify the network portion of the address while the last two octets are for host IP addresses.
  OR:
- Enterprise could choose to subnet at the /24 octet boundary → would enable them to define 65,536 subnets each capable of connecting 254 hosts.

- The /24 boundary is very popular in subnetting because it accommodates a reasonable number of hosts and conveniently subnets at the octet boundary.

Classless Subnetting

- Subnets can borrow bits from any host bit position to create other masks
- Flexibility when assigning network addresses to a smaller number of end devices:
  - /25 row - Borrowing 1 bit from the fourth octet creates 2 subnets supporting 126 hosts each.
  - /26 row - Borrowing 2 bits creates 4 subnets supporting 62 hosts each.
  - /27 row – Borrowing 3 bits creates 8 subnets supporting 30 hosts each.
  - /28 row – Borrowing 4 bits creates 16 subnets supporting 14 hosts each.
  - /29 row – Borrowing 5 bits creates 32 subnets supporting 6 hosts each.
  - /30 row – Borrowing 6 bits creates 64 subnets supporting 2 hosts each.
- For each bit borrowed in the fourth octet, number of subnetworks available is doubled while reducing the number of host addresses per subnet.
- Higher the prefix length → more subnets
- Lower the prefix length → more hosts

Creating 2 Subnets



- From a /25 subnet
- Router interfaces must be assigned an IP address within the valid host range for the assigned subnet.
  - This is the address that hosts on that network will use as their default gateway

Subnetting Formulas

- To calculate the number of subnets that can be created from the bits borrowed:

  $$\mathbf{2^n}$$

  n = bits borrowed
- The last two bits cannot be borrowed from the last octet because there would be no host addresses available
  - Longest prefix length possible when subnetting is /30 or 255.255.255.252
- To calculate the number of hosts that can be supported:

  $$\mathbf{2^n - 2}$$

  n = the number of bits remaining in the host field
  - There are two subnet addresses that cannot be assigned to a host, the network address and the broadcast address = subtract 2

Creating 4 Subnets

- Subnets can only be created in powers of 2
- Magic number – each subnet goes up by 64 because the binary digit is in the 64's place → creating 4 equal subnets

Subnetting a /16 and /8 Prefix

Creating Subnets with a /16 Prefix

- For a larger number of subnets, an IP network needs hosts bits to borrow from
- 16 bits in the network portion and 16 bits in the host portion

- 8 additional bits that can be borrowed, and, therefore, the number of subnets and hosts are larger.

Creating 100 Subnets with a /16 Network

- Large enterprise that requires at least 100 subnets with private address 172.16.0.0
  - Start borrowing bits in the third octet
  - Borrow a single bit at a time until the number of bits necessary to create 100 subnets is reached
  - Up to 14 host bits that can be borrowed
  - 7 bits (i.e., 2^7 = 128 subnets) would need to be borrowed

Calculating the Hosts

- To calculate the number of hosts a subnet can support → examine third and fourth octet
- Use formula
  - **E.g.** if 9 bits were borrowed → 2^9-2 = 510 hosts per subnet

Creating 1000 Subnets with a /8 Network

- Network address 10.0.0.0 has a default subnet mask of 255.0.0.0 or /8
  - There are 8 bits in the network portion and 24 host bits available to borrow toward subnetting → small ISP will subnet the 10.0.0.0/8 network
  - Must borrow 10 bits to create > 1000 (1024) subnets
    - 2^{10} = 1024 subnets
    - 2^{14} -2 = 16382 hosts on each subnet

Subnetting to Meet Requirements

Subnetting Based on Host Requirements

- Considerations when planning subnets:
  - Number of host addresses required for each network
  - Number of individual subnets needed
- Inverse relationship for number of subnets and number of hosts
  - More bits borrowed to create subnets, the fewer host bits available
  - If more host addresses are needed, more host bits are required, resulting in fewer subnets
- Always cannot use two addresses

Subnetting Based on Network Requirements

- Sometimes required number of subnets (less emphasis on number of hosts)
  - **E.g.** Organisation chooses to separate network traffic based on internal structure/ department setup
- Number of subnets is most important in determining how many bits to borrow
- Formula (2^n) → the key to balance the number of subnets needed and the number of hosts required for the largest subnet
- More bits borrowed to create additional subnets means fewer hosts available per subnet.

Benefits of Variable Length Subnet Masking

Traditional Subnetting Wastes Addresses

- Using traditional subnetting, the same number of addresses is allocated for each subnet → if all the subnets have the same requirements for the number of hosts, these fixed size address blocks would be efficient
- Traditional subnetting meets the needs of the largest LAN and divides the address space into an adequate number of subnets → results in significant waste of unused addresses
  - **E.g.** Only two addresses are needed in each subnet for the three WAN links. Because each subnet has 30 usable addresses = 28 unused addresses in each of these subnets x 3
- Limits future growth by reducing the total number of subnets available

- Variable Length Subnet Mask (VLSM), was designed to avoid wasting addresses.

Variable Length Subnet Masks (VLSM)

- Traditional subnetting creates subnets of equal size → uses the same subnet mask
- VLSM allows a network space to be divided into unequal parts
  - Subnet mask will vary depending on how many bits have been borrowed for a particular subnet
  - Thus the "variable" part of the VLSM
- Formulas to calculate the number of hosts per subnet and the number of subnets created still apply
- VLSM → the network is first subnetted, and then the subnets are subnetted again
  - Process can be repeated multiple times to create subnets of various sizes
  - Always begin by satisfying the host requirements of the largest subnet. Continue subnetting until the host requirements of the smallest subnet are satisfied.

Basic VLSM

- To create smaller subnets, one of the subnets will be divided
  - **E.g.** *Address 192.168.20.224/27*
    - 5 host bits in the subnetted address space, 3 more bits can be borrowed, leaving 2 bits in the host portion
    - Calculations are the same as traditional subnetting → bits are borrowed, and the subnet ranges are determined
- Scheme reduces the number of addresses per subnet to a size appropriate for WANS

VLSM Chart

- An addressing chart can be used to identify which blocks of addresses are available for use and which ones are already assigned
  - Helps to prevent assigning addresses that have already been allocated
- To use the address space more efficiently, /30 subnets are created for WAN links
  - To keep the unused blocks of addresses together in a block of contiguous address space, the last /27 subnet was further subnetted to create the /30 subnets.
  - The first 3 subnets were assigned to WAN links
  - Designing the addressing scheme in this way leaves 3 unused, contiguous /27 subnets and 5 unused contiguous /30 subnets

8.2 Addressing Schemes

Structured Design

Network Address Planning

- Address assignment should not be random → well designed and meaningful
- Planning network subnets requires examination of both the needs of an organization's network usage, and how the subnets will be structured
- Network requirement study
  - Looking at the entire network and how it will be segmented
  - Address plan – determining needs of each subnet in size, hosts per subnet, how host addresses are assigned, which hosts require static IPs, which use DHCP, etc.
- The size of the subnet involves planning the number of hosts that will require IP host addresses in each subnet of the subdivided private network
- Must take into account future expansion

Planning to Address the Network

Primary considerations for planning address allocation:

- Prevent Duplication of Addresses
  - Each host in an internetwork must have a unique address
  - Without proper planning and documentation, an address could be assigned to multiple hosts → access issues for both

- Provide and Control Access
  - Some hosts (**e.g.** servers) provide resources to internal hosts and external hosts
  - Layer 3 address assigned to a server can be used to control access to that server
    - If the address is randomly assigned and not well documented, controlling access is more difficult
- Monitor Security and Performance
  - Network traffic is examined for source IP addresses that are generating or receiving excessive packets
  - If there is proper planning and documentation, of the network addressing, problematic network devices should easily be found

Assigning Addresses to Devices

Different types of devices that require addresses:

- End User Clients
  - Mostly through DHCP → reduces the burden on network support staff + eliminates entry errors
  - Addresses are leased for a period of time
  - Changing the subnetting scheme means that the DHCP server needs to be reconfigured, and the clients must renew their IP addresses
- Servers and peripherals
  - Should have predictable static IPs
  - Use a consistent numbering system
- Servers that are accessible from the Internet
  - Remote
  - Assigned private addresses internally
  - Router/ firewall at the perimeter of the network must be configured to translate the internal address into a public address
- Intermediary devices
  - Assigned addresses for network management, monitoring and security
  - Because we must know how to communicate with them → should have predictable, statically assigned addresses
- Gateway
  - Routers and firewall devices have an IP address assigned to each interface → serves as the gateway for the hosts in that network
  - Typically router interface uses the lowest or highest address in the network
- Generally recommended to have a set pattern of how addresses are allocated → benefits administrators when adding/ removing devices, filtering traffic based on IP + simplifies documentation.

8.3 Design Considerations for IPv6

Subnetting an IPv6 Network

The IPv6 Global Unicast Address

- Different to IPv4 → so many addresses that the reason for subnetting is different
- Limiting broadcast domains + managing address scarcity
- Determining subnet mask and use of VLSM is done to conserve IPv4 addresses → IPv6 is unconcerned with this, subnet ID includes more than enough
- IPv6 subnetting is about building an addressing hierarchy based on the number of subnetworks needed
- Link-local addresses are never subnetted because only exists on local link
- IPv6 global unicast can be subnetted
  - Usually consists of /48 global routing prefix, 16 but subnet ID and 64 bit interface ID

Subnetting Using the Subnet ID

- 16 bit subnet ID of IPv6 global unicast address can be used by organisation to create internal subnets
- Subnet ID provides more than enough subnets and host support – 16 bit section can:
    - Create up to 65536 /64 subnets (without borrowing any bits from interface ID)
    - Support up to 18 quintillion host addresses per subnet
- Easier to implement than IPv4 → no conversion to binary required

IPv6 Subnet Allocation

- Task of the network administrator: design a logical scheme to address the network
- with IPv6 the WAN link subnet will not be subnetted further
    - This may “waste” addresses, that is not a concern when using IPv6
- Each /64 subnet will provide more addresses than will ever be needed
- Each LAN segment and the WAN link is assigned a /64 subnet
- Each of the router interfaces has been configured to be on a different IPv6 subnet

CHAPTER 9 – Application Layer

91. Transport Layer Protocols

Transportation of Data

Role of the Transport Layer

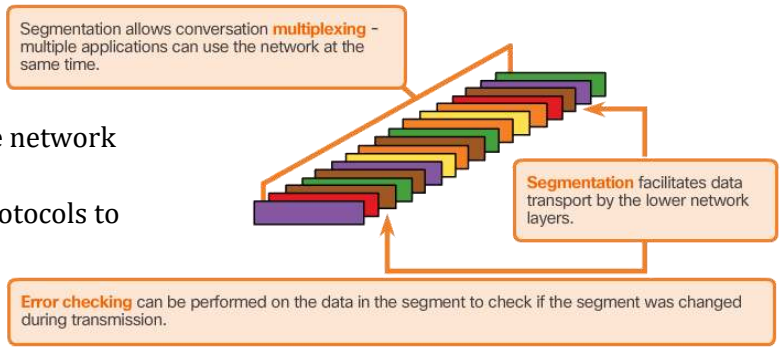
- The transport layer is responsible for establishing a temporary communication session between two applications and delivering data between them
- Application generates data that is sent from an application on a source host to an application on a destination host
    - Without regard to the destination host type, type of media, path taken or size of network

Transport Layer Responsibilities

- **Tracking Individual Conversations**
    - *Conversation* → each set of data flowing between a source application and a destination application
    - Host may have multiple applications communicating simultaneously
    - Many to many
    - Responsibility of the transport layer to maintain and track the multiple conversation
- **Segmenting Data and Reassembling Segments**
    - Transport layer protocols have services that segment the application data into blocks that are an appropriate size → encapsulation
    - Header attached
        - Used for reassembly
        - To track the data stream
    - At destination, TL reconstructs pieces of data into complete data stream to be used by application layer
    - Protocols describe how the TL header information is used to reassemble the data pieces
- **Identifying the Applications**
    - TL identifies target application
        - TL assigns each application an identifier → *port number*
        - Software process that needs to access the network is assigned a port number - unique

Conversation Multiplexing

- Segmenting data into smaller chunks enables many different communications from many users to be interleaved on the same network → not consume all of the available bandwidth
- Values in the header field enable various TL protocols to perform different functions in managing data communication



Transport Layer Reliability

- TL manages reliability requirements of a conversation
- Different applications have different transport reliability requirements
- IP is concerned only with the structure, addressing, and routing of packets (not with how the delivery takes place) → TCP/IP provides two transport layer protocol
- **TCP**
    - Considered a reliable, full-featured transport layer protocol
    - Ensures that all of the data arrives at the destination
- **UDP**
    - Very simple transport layer protocol
    - Does not provide for any reliability

TCP (Transmission Control Protocol)

- A connection-oriented protocol

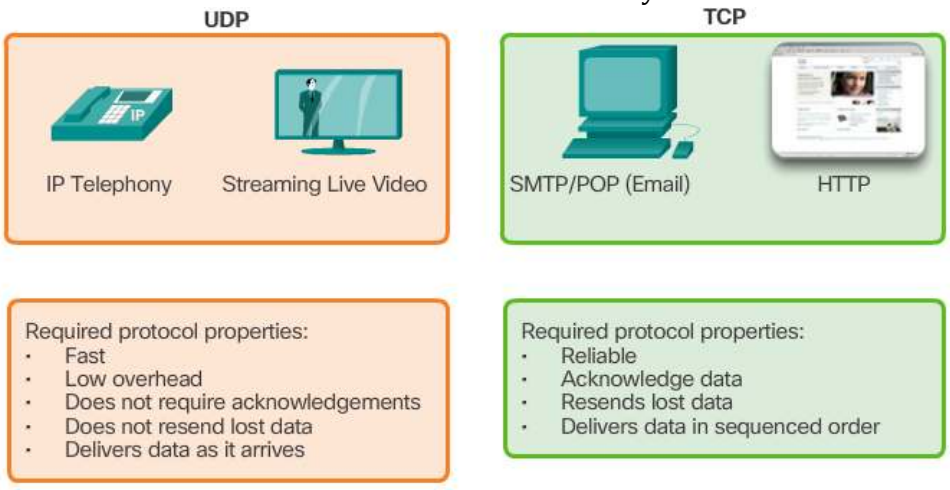
    - Negotiates and establishes a permanent connection (or session) between source and destination devices prior to forwarding any traffic.
- Sends packages that are tracked from source to destination
- Basic operations of reliability:
    - Numbering and tracking data segments transmitted to a specific host from a specific application
    - Acknowledging received data
    - Retransmitting any unacknowledged data after a certain period of time
- Incur additional overhead and possible delays in transmission → trade-off between the value of reliability and the burden it places on network resource

UDP (User Datagram Protocol)

- UDP provides the basic functions for delivering data segments between the appropriate applications,
- Very little overhead and data checking
- best-effort delivery protocol (unreliable because there is no acknowledgment that the data is received at the destination)

The Right Transport Layer Protocol for the Right Application

- Some applications need segments to arrive in a very specific sequence to be processed successfully
- Application developers must choose which transport protocol type is appropriate based on the requirements of the applications
- Applications such as databases, web browsers and email clients need all data to arrive at destination → TCP → missing data could cause a corrupt communication that is either incomplete or unreadable
- Applications such as streaming live audio, live video, and Voice over IP can tolerate some data loss during transmission over the network, but delays in transmission are unacceptable → UDP → acknowledgments and retransmission would slow down delivery



TCP and UDP

TCP Features

- **Establishing a session**
    - Through session establishment, the devices negotiate the amount of traffic that can be forwarded at a given time, and the communication data between the two can be closely managed

- **Reliable Delivery**
  - Ensuring that each segment that the source sends arrives at the destination
  - Possibility of a segment to become corrupted or lost completely, as it is transmitted over the network.
- **Same-Oder Delivery**
  - Data can arrive in the wrong order (networks may provide multiple routes that can have different transmission rates)
  - TCP numbers and sequences segments → ensure that these segments are reassembled into the proper order
- **Flow Control**
  - Network hosts have limited resources → when TCP is aware that these resources are overtaxed, it can request that the sending application reduce the rate of data flow
  - TCP regulates the amount of data the source transmits
  - Prevents the need for retransmission of the data when the receiving host's resources are overwhelmed.

Establishing a session ensures the application is ready to receive the data.

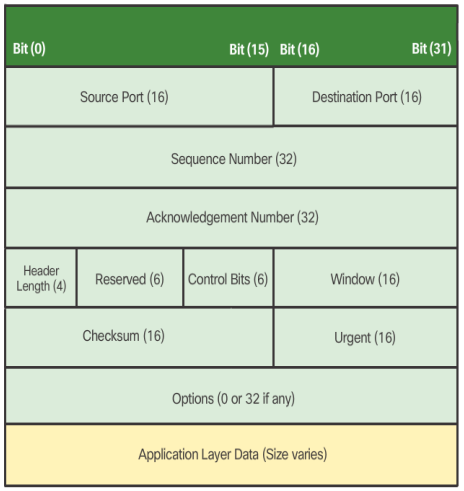
Reliable delivery means lost segments are resent so the data is received complete.

Same order delivery ensures that the segments are reassembled into the proper order.

Flow control ensures that the receiver is able to process the data received.

TCP Header

- TCP is a stateful protocol → keeps track of the state of the communication session
  - Records which information it has sent and which information has been acknowledged
- 20 bytes
  - **Source Port** (16 bits) & **Destination Port** (16 bits) - Used to identify the application.
  - **Sequence number** (32 bits) - Used for data reassembly purposes.
  - **Acknowledgment number** (32 bits) - Indicates the data that has been received.
  - **Header length** (4 bits) - Known as "data offset". Indicates the length of the TCP segment header.
  - **Reserved** (6 bits) - This field is reserved for the future.
  - **Control bits** (6 bits) - Includes bit codes, or flags, which indicate the purpose and function of the TCP segment.
  - **Window size** (16 bits) - Indicates the number of bytes that can be accepted at one time.
  - **Checksum** (16 bits) - Used for error checking of the segment header and data.
  - **Urgent** (16 bits) - Indicates if data is urgent.



UDP Features

- UDP is a lightweight transport protocol → offers the same data segmentation and reassembly as TCP, but without TCP reliability and flow control

No Ordered Data Reconstruction
Data is reconstructed in the order that it is received.

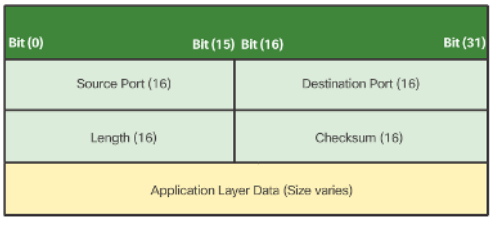
Connectionless
No session establishment.

Unreliable Delivery
Any segments lost are not resent.

No Flow Control
Does not inform the sender about resource availability.

UDP Header

- Stateless protocol → neither the client, nor the server, is obligated to keep track of the state of the communication session
- One of the most important requirements is that data continues to flow quickly
- Pieces of communication in UDP are called datagrams
- 8 bytes



Multiple Separate Conversations

- The transport layer must be able to separate and manage multiple communications with different transport requirement needs
- TCP and UDP manage these multiple simultaneous conversations by using header fields that can uniquely identify these applications → port numbers.

Port Numbers

- Source port number → originating application on the local host
- Destination port number → destination application on the remote host
- **Source Port**
  - Dynamically generated by the sending device
  - Process allows multiple conversations to occur simultaneously
  - Common for a device to send multiple HTTP service requests to a web server at the same time → each are tracked
- **Destination Port**
  - Client places a destination port number in the segment to tell the destination server what service is being requested

Socket Pairs

- Source/ Destination IP address **+** source/ destination port number **=** socket
- Socket is used to identify the server and service being requested by the client
- Socket Pair = client and server IP address and port
- Sockets enable multiple processes to distinguish themselves from each other
- The source port number acts as a return address for the requesting application
- TL keeps track of this port and the application that initiated the request so that when a response is returned, it can be forwarded to the correct application
- **E.g.** 192.168.1.5:1099, 192.168.1.7:80

Port Number Groups

- IANA is responsible for assigning various addressing standards, including port numbers
- Some applications may use both TCP and UDP
- **Well-known Ports (0 - 1023)**
  - Reserved for services and applications
  - Commonly used for applications such as web browsers, email clients, and remote access clients
  - By defining these well-known ports for server applications → client applications can be programmed to request a connection to that specific port and its associated service.
- **Registered Ports (1024 - 49151)**
  - Assigned by IANA to a requesting entity to use with specific processes or applications
  - Primarily individual applications that a user has chosen to install
  - **E.g.** Cisco has registered port 1985 for its Hot Standby Routing Protocol (HSRP) process.
- **Dynamic or Private Ports (49152 - 65535)**
  - AKA Ephemeral ports
  - Usually assigned dynamically by the client's OS when a connection to a service is initiated
  - Dynamic port is then used to identify the client application during communication

The netstat Command

- Unexplained TCP connections can pose a major security threat
- Can be necessary to know which active TCP connections are open and running on a networked host
- Netstat is an important network utility that can be used to verify connections
- ***Netstat** command* → list the protocols in use, the local address and port numbers, the foreign address and port numbers, and the connection state.
  - Will attempt to resolve IP addresses to domain names and port numbers to well-known applications
  - ***-n*** option can be used to display IP addresses and port numbers in their numerical form

9.2 TCP and UDP

TCP Communication Process

TCP Server Processes

- Each application process running on the server is configured to use a port number
- An individual server cannot have two services assigned to the same port number within the same transport layer services
- **E.g.** web server application and file transfer application cannot be configured to use the same port
- An active server application assigned to a specific port is considered to be open, which means that the transport layer accepts and processes segments addressed to that port
- There can be many ports open simultaneously on a server, one for each active server application.

TCP Connection Establishment

- TCP connection is established in three steps:
  1. Initiating client requests a client-to-server communication session with the server
  2. The server acknowledges the client-to-server communication session and requests a server-to-client communication session
  3. Initiating client acknowledges the server-to-client communication session

TCP Session Termination

- To close a connection, the Finish (FIN) control flag must be set in the segment header
  - To end each one-way TCP session, consisting of a FIN segment and an Acknowledgment (ACK) segment, is used.
- Steps to terminate a session between any two hosts:
  1. When data transfer is finished, client sends a segment with the FIN flag set
  2. Server sends and ACK to acknowledge receipt of the FIN to terminate the session
  3. Server sends a FIN to the client to terminate the server-to-client sessions
  4. Client responds with an ACK to acknowledge FIN from the server
     When all segments have been acknowledged, the session is closed.

TCP Three-way Handshake Analysis

- Hosts track each data segment within a session and exchange information about what data is received using the information in the TCP header
- TCP is full-duplex protocol → two way
- To establish a connection, hosts perform a three-way handshake
- Control bits in the TCP header indicate the progress and status of the connection
- 3-way handshake:
  - Establishes destination device that is present on the network
  - Verifies that the destination device has an active service and is accepting requests on the destination port number that the initiating client intends to use
  - Informs the destination device that the source client intends to establish a communication session on that port number
- The connection and session mechanisms enable TCP's reliability function.
- Flags → 6 bits in the Control Bit field of the TCP segment header
  - Set to on and off
  - 6 flags:
    - URG - Urgent pointer field significant
    - ACK - Acknowledgement field significant
    - PSH - Push function
    - RST - Reset the connection
    - SYN - Synchronize sequence numbers
    - FIN - No more data from sender

Reliability and Flow Control

TCP Reliability – Ordered Delivery

- TCP segments may arrive at their destination out of order → Sequence numbers are assigned in the header of each packet to be able to reassemble
- During session setup, an initial sequence number (ISN) is set
    - ISN represents the starting value of the bytes for this session that is transmitted to the receiving application
    - Sequence number is incremented by the number of bytes that have been transmitted
    - Enables each segment to be uniquely identified and acknowledged (missing segments can be found)
    - ISN begins at a random number (prevents malicious attacks)
- The receiving TCP process places the data from a segment into a receiving buffer
    - Segments are placed in the proper sequence order and passed to the application layer when reassembled

TCP Flow Control – Window Size and Acknowledgements

- The amount of data that the destination can receive and process reliably
- Flow control helps maintain the reliability of TCP transmission by adjusting the rate of data flow between source and destination for a given session
- Window Size → 16-bit field in TCP header
    - The window size is the number of bytes that the destination device of a TCP session can accept and process at one time
    - Included in every TCP segment so the destination can modify the window size at any time depending on buffer availability
- Destination will not wait for all the bytes for its window size to be received before replying with an acknowledgment
- Sliding windows → process of the destination sending acknowledgments as it processes bytes received and the continual adjustment of the source's send window

TCP Flow Control – Congestion Avoidance

- Congestion = packets disregarded, and left unacknowledged
- By determining the rate at which TCP segments are sent but not acknowledged, the source can assume a certain level of network congestion
- When there is congestion → retransmission of lost TCP segments from the source
    - If the retransmission is not properly controlled, the additional retransmission of the TCP segments can make the congestion even worse
- TCP employs several congestion handling mechanisms, timers, and algorithms
    - If the source determines that the TCP segments are either not being acknowledged or not acknowledged in a timely manner, then it can reduce the number of bytes it sends before receiving an acknowledgment

UDP Communication

UDP Low Overhead versus Reliability

- Lower overhead → not connection-oriented, does not offer the sophisticated retransmission, sequencing and flow control mechanisms
- Not inferior – just not provided by transport layer protocol and must implemented elsewhere
- Low overhead makes it desirable for protocols that's makes it simple to request and reply transactions

UDP Datagram Reassembly

- UDP does not track sequence numbers → no way to reorder the datagrams into transmission order
- UDP simply reassembles the data in the order that it was received and forwards it to the application
    - If the data sequence is important to the application, the application must identify the proper sequence and determine how the data should be processed

UDP Server Processes and Requests

- UDP-based server applications are assigned well-known or registered port numbers
    - Applications accept the data matched with the assigned port number

- UDP receives a datagram destined for one of these ports, it forwards the application data to the appropriate application based on its port number

UDP Client Processes

- Client-server communication is initiated by a client application that requests data from a server process
- The UDP client process dynamically selects a port number from the range of port numbers and uses this as the source port for the conversation
- After a client has selected the source and destination ports, the same pair of ports is used in the header of all datagrams used in the transaction

TCP or UDP

Applications that use TCP

- TCP handles all tasks associated with:
  - Dividing the data stream into segments
  - Providing reliability
  - Controlling data flow
  - Reordering of segments
- TCP frees the application from having to manage any of these tasks → Applications can simply send the data stream to the transport layer and use the services of TCP.

Applications that use UDP

- Applications best suited for UDP:
  - **Live video and multimedia applications**
    - Can tolerate some data loss, but require little or no delay.
    - **E.g.** VoIP and live streaming video.
  - **Simple request and reply applications**
    - Applications with simple transactions where a host sends a request and may or may not receive a reply.
    - **E.g.** DNS and DHCP.
  - **Applications that handle reliability themselves**
    - Unidirectional communications where flow control, error detection, acknowledgments, and error recovery is not required or can be handled by the application
    - **E.g.** SNMP and TFTP.
- Although DNS and SNMP use UDP by default, both can also use TCP
  - DNS will use TCP if the DNS request or DNS response is more than 512 bytes
  - Under some situations the network administrator may want to configure SNMP to use TCP.

CHAPTER 10 – Application Layer

10.1 Application Layer Protocols

Application, Presentation and Session

Application Layer

- Closest layer to the user
- The layer that provides the interface between the applications used to communicate and the underlying network over which messages are transmitted
- Used to exchange data between programs running on the source and destination hosts
- The upper three layers of the OSI model (application, presentation, and session) = single TCP/IP application layer
- Application layer protocols:
  - HTTP
  - FTP
  - TFTP
  - IMAP
  - DNS

Presentation and Session Layer

Presentation Layer

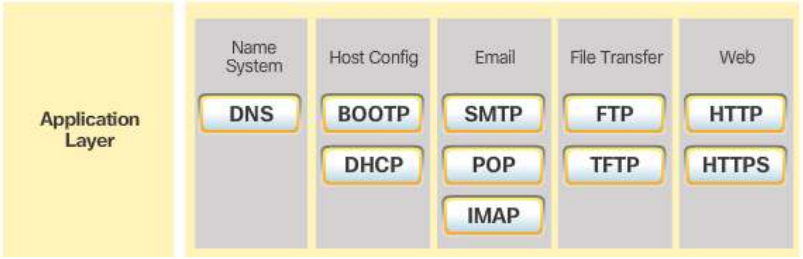
- 3 primary functions:
  - Formatting/ presenting data at the source device into a compatible form for receipt by the destination device
  - Compressing data in a way that can be decompressed by destination device
  - Encrypting data for transmission and decrypting data upon receipt
- Formats data for the application layer
- Sets standards for file formats
  - **E.g.** JPEG, GIF, PNG, MPEG

Session Layer

- Functions create and maintain dialogs between source and destination applications
- Handles exchange of information to:
  - Initiate dialogs
  - Keep them active
  - Restart sessions that are disrupted/ idle for a long period of time

TCP/IP Application Layer Protocols

- Specify the format and control information necessary for many common Internet communication functions
- Used by both the source and destination devices during a communication session → therefor must have compatible protocols



Name System

- **DNS → Domain Name System/ Service (TCP, UDP 53)**
  Translates domain names into IP address

Host Config

- **BOOTP → Bootstrap Protocol (UDP client 69, server 67)**
  Enables a diskless workstation to discover its own IP address, the IP address of a BOOTP server on the network, and a file to be loaded into memory to boot the machine. Is being superseded by DHCP
  DHCP → Dynamic Host Configuration Protocol (UDP client 68, server 67)
  Dynamically assigns IP addresses to client stations at start-up. Allows address to be re-used when no longer needed.

Email

- **SMTP → Simple Mail Transfer Protocol (TCP 25)**
  Enables clients to send email to a mail server. Enables servers to send email to other servers.
- **POP → Post Office Protocol version 3 (TCP 110)**
  Enables clients to retrieve email from a mail server. Downloads email from the mail server to the desktop.
- **IMAP → Internet Message Access Protocol (TCP 143)**
  Enables clients to access email stored on a mail server. Maintains email on the server.

File Transfer

- **FTP → File Transfer Protocol (TCP 20-21)**
  Sets rules that enable a user on one host to access and transfer file to and from another host over a network. Reliable, connection-oriented, and acknowledged file delivery protocol.
- **TFTP → Trivial File Transfer Protocol (UDP 69)**
  Simple, connectionless file transfer protocol. A best-effort, unacknowledged file delivery protocol. Utilises less overhead then FTP.

Web

- **HTTP → Hypertext Transfer Protocol (TCP 80, 8080)**
  Set of rules for exchanging text, graphic images, sound, video, and other multimedia files on the www.
- **HTTPS → Hypertext Transfer Protocol Secure (TCP, UDP 443)**
  Browser uses encryption to secure HTTP communications. It authenticates the website to which you are connecting to your browser

How Application Protocols Interact with End-User Applications

Client-Server Model

- Client = device requesting information
- Server = device responding to the request
- Client begins exchange by requesting data from server → responds which one/ more streams of data
- AL protocols describe the format of the requests and responses between clients and servers
- Exchange may also require use authentication before transmission

Pee-to-Peer Networks

- When the data is accessed from a peer device without the use of a dedicated server
- 2 parts → P2P networks and P2P applications
- P2P network
  - 2 or more computers are connected via network
  - Share resources without dedicated server
  - Any end device can be both a server and a client
  - Per request basis

Peer-to-Peer Applications

- Allows a device to act as both a client and a server within the same communication
- Require that each end device provide a user interface and run a background service
- Hybrid system P2P applications
  - Decentralised resource sharing → indexes point to resource locations stored in centralised directory

Common P2P Applications

- Common P2P networks include:
  - eDonkey
  - G2
  - BitTorrent
  - Bitcoin
- Sharing whole files with other users → based of Gnutella protocol
  - Allows users to connect to Gnutella services over the Internet and to locate and access resources shared by other Gnutella peers
  - **i.e.** gtk-gnutella, WireShare, Shareaza, and Bearshare.
- Sharing pieces of many files with each other at the same time
  - Use torrent file to locate other users who have pieces that they need so that they can connect directly to them
  - **i.e.** BitTorrent, uTorrent, Frostwire, and qBittorrent.

10.2 Well-Known Application Layer Protocols and Services

Web and Email Protocols

Hypertext Transfer Protocol and Hypertext Markup Language

- URL typed into web browser → web browser establishes connection → web service runs server using the HTTP protocol
- 3 parts of URL that browser interprets:
  1. **http** (the protocol or scheme)
  2. **www.cisco.com** (the server name)
  3. **index.html** (the specific filename requested)
- Next:
  - Coverts server name into numeric address → to connect with server
  - Browser sends GET request to the server → asks for index.html file
  - Server sends HTML code for webpage to the browser
  - Browser deciphers the HTML code and formats the page for the browser window

HTTP and HTTPS

HTTP

- Request/response protocol
- Specifies the message types used for that communication
- Three common message types:
  - **GET** → client request for data
    Client (web browser) sends the GET message to the web server to request HTML pages
  - **POST** → uploads data files to the web server
  - **PUT** → uploads resources/ content to the web server
- Flexible but not secure
  - Request messages send information to the server in plain text that can be intercepted and read.
  - Server responses, typically HTML pages, are also unencrypted

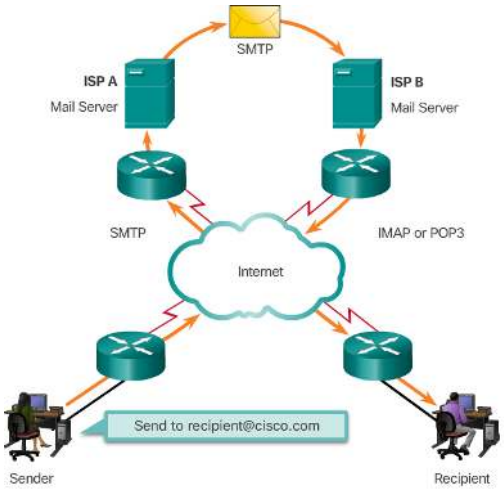
HTTPS

- Uses authentication and encryption to secure data as it travels between the client and server
- Same client request-server response process as HTTP → but the data stream is encrypted with Secure Socket Layer (SSL) before being transported across the network

Email Protocols

- Email is a store-and-forward method of sending, storing, and retrieving electronic messages across a network
- Stored in databases on mail servers
- Email clients communicate with mail servers to send and receive email

- Mail servers communicate with other mail servers to transport messages from one domain to another
    - Email client does not communicate directly with another email client when sending email
- Supports 3 separate protocols for operation:
    - SMTP
    - POP
    - IMAP
    - Only retrieves using POP or IMAP



SMTP Operation

- Format require a message header and a message body
- Body can have whatever
- Header must have a properly formatted recipient email address and a sender address
- Port 25
- When client sends email → connects with SMTP server
- Must have connection
- Places the message in a local account or forwards the message to another mail server for delivery
- Periodically, the server checks the queue for messages and attempts to send them again
    - If still not delivered after a predetermined expiration time, it is returned to the sender as undeliverable

POP Operation

- Retrieves mail from mail server
- Mail is downloaded from the server to the client and then deleted on the server
- The server starts the POP service by passively listening on TCP for client connection requests
- Port 110
- Client sends request to establish TCP connection with server
- Established = POP sends greeting
- Client and POP exchange commands + responses until connection is terminated
- Messages are downloaded to the client and removed from server
    - Undesirable for small business (no backup)

IMAP Operation

- Retrieves mail
- When the user connects to an IMAP-capable server, copies of the messages are downloaded to the client application
- Original messages are kept on the server until manually deleted
- Client sorting of messages is duplicated on email client also

IP Addressing Services

Domain Name Service

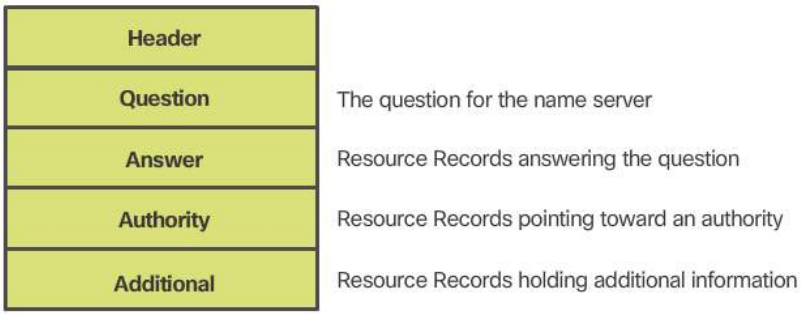
- Domain names were created to convert the numeric address into a simple, recognizable name
- If server decides to change the numeric address, it is transparent to the user because the domain name remains the same.
- DNS protocol defines an automated service that matches resource names with the required numeric network address
    - Format for queries, responses, and data
- DNS communications use a single format called a message → used for all types of client queries and server responses, error messages, and the transfer of resource record information between servers.

DNS Message Format

- Record types:

- **A** → An end device IPv4 address
- **NS** → An authoritative name server
- **AAAA** → An end device IPv6 address (pronounced quad-A)
- **MX** → A mail exchange record

- If DNS is unable to resolve the name using its stored records, it contacts other servers to resolve the name
- After match is found and returned to the original requesting server, server temporarily stores the numbered address in the event that the same name is requested again



DNS Hierarchy

- DNS protocol uses a hierarchical system to create a database to provide name resolution
- Broken down → each DNS server maintains a specific database file and only responsible for managing name-to-IP mappings for that small portion of the entire DNS structure
  - When a DNS server receives a request for a name translation that is not within its DNS zone → server forwards the request to another DNS server
- **E.g.** of top-level domains
  - .com - a business or industry
  - .org - a non-profit organization
  - .au - Australia
  - .co - Colombia

The nslookup Command

- ***nslookup*** command allows the user to manually query the name servers to resolve a given host name
- Can also be used to troubleshoot name resolution issues and to verify the current status of the name servers

Dynamic Host Configuration Protocol

- DHCP automates the assignment of IPv4 addresses, subnet masks, gateways, and other IPv4 networking parameters → dynamic addressing
- Host connects to the network→ the DHCP server is contacted, and an address is requested to lease
- Preferred for larger networks
- DHCP-distributed addresses are leased for a set period of time→ when the lease is expired, the address is returned to the pool for reuse if the host has been powered down or taken off the network
- Both:
  - DHCP is used for general purpose hosts, such as end user devices
  - Static addressing is used for network devices, such as gateways, switches, servers, and printers
- DHCPv6
  - Provides similar services for IPv6 clients
  - Important difference is that DHCPv6 does not provide a default gateway address → can only be obtained dynamically from the router's RA message

DHCP Operation

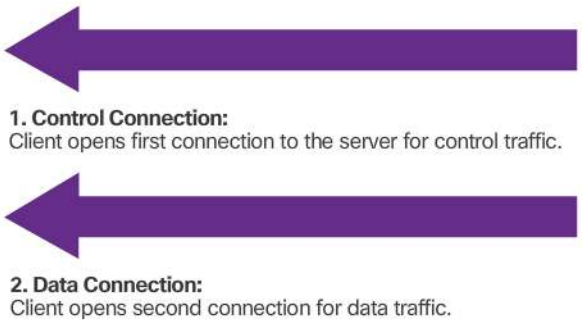
- Process:
  - DHCP-configured device boots up or connects to the network, client broadcasts a DHCP discover (DHCPDISCOVER) message to identify any available DHCP servers on the network
  - DHCP server replies with a DHCP offer (DHCPOFFER) message, offering a lease to the client.
- Message contains:
  - IPv4 address and subnet mask to be assigned

    - IPv4 address of the DNS server,
    - IPv4 address of the default gateway
    - Duration of the lease
- Client may DHCP request (DHCPREQUEST) message that identifies the explicit server and lease offer that the client is accepting – if multiple DHCPOFFERs
- If address requested is still available, the server returns a DHCP acknowledgment (DHCPACK) → finalises lease
- If no longer valid, DHCP server responds with a negative acknowledgment (DHCPNAK) message
    - And selection process begins again
- DHCP ensures all IP addresses are unique
- DHCPv6 messages are SOLICIT, ADVERTISE, INFORMATION REQUEST, and REPLY

File Sharing Services

File Transfer Protocol

- Allows for data transfers between a client and a server
- An FTP client is an application that runs on a computer that is used to push and pull data from a server running an FTP daemon (FTPd).
- Process:
    - Client establishes the first connection to the server for control traffic using TCP port 21 (client commands + server replies)
    - Client establishes the second connection to the server for the actual data transfer using TCP port 20 (connection is created every time there is data to be transferred)
- Transfer can be either direction
- Pull/push and download/upload



Server Message Block (SMB)

- Client/server file sharing protocol
- Describes the structure of shared network resources
    - **i.e** directories, files, printers, and serial ports
- Request-response protocol
- Format includes fixed-sized header, followed by a variable-sized parameter and data component
- SMB messages can:
    - Start, authenticate, and terminate sessions
    - Control file and printer access
    - Allow an application to send or receive messages to or from another device
- SMB file-sharing and print services have become the mainstay of Microsoft networking
- Unlike the file sharing supported by FTP, clients establish a long-term connection to servers

CHAPTER 11 – Build a Small Network

11.1 Network Design

Devices in a Small Network

Small Network Topologies

- Simple → single router, one or more switches
- Maybe a wireless access point
- Internet → single WAN connection provided by DSL, cable, or an Ethernet connection.
- Work is focused on:
  - Maintenance and troubleshooting of existing equipment
  - Securing devices and information on the network
- Done by employee or contractor

Device Selection for a Small Network

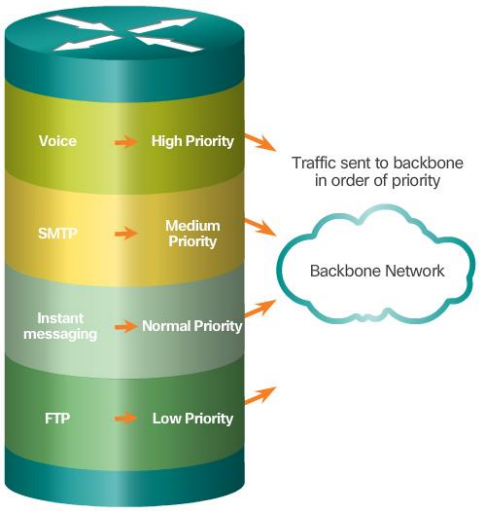
- Involves planning and design
- When deciding on intermediate devices, factors to consider:
  - **Cost**
    - Determined by capacity and features
    - Capacity includes number and types of ports available and backplane spped
    - Management capabilities
    - Embedded security technologies
    - Expense of cable running
    - Amount of redundancy
  - **Speed and Types of Ports/ Interfaces**
    - Choosing Layer 2 devices that can accommodate increased speeds allows the network to evolve without replacing central devices
  - **Expandability**
    - Fixed or modular
    - Modular → have expansion slots that provide the flexibility to add new modules as requirements evolve
    - Switches are available with additional ports for high-speed uplinks
    - Routers can be used to connect different types of networks
  - **Operating System Features and Services**
    - Network device can have features:
      - Security
      - Quality of Service
      - VoIP
      - Layer 3 switching
      - Network Address Translation
      - DHCP

IP Addressing for a Small Network

- Planning the IP address space
- All unique
- Planned, documented and maintained → based on the type of device receiving the address
- Factor of ip design should be for:
  - End devices for users
  - Servers and peripherals
  - Hosts that are accessible from the Internet
  - Intermediary devices
- Documenting and planning scheme helps administrator track device types
  - Useful when troubleshooting network traffic using protocol analyser
  - Better able to control access to resources on the network
  - Especially important for hosts that provide resources to internal and external network

Redundancy in a Small Network

- Reliability is important → businesses heavily rely on them
- Failure = costly
- In order to maintain a high degree of reliability, redundancy is required in the network design
    - Redundancy helps to eliminate single points of failure
- Can be accomplished by:
    - Installing duplicate equipment
    - Supplying duplicate network links for critical areas:
        - Routers
            - Ensure that application transmissions received from external traffic can be handled in the event of router failure
        - Switches
            - Avoid switching failure
        - Servers
            - If a server fails there is another to handle customer requests
- Second service provider as backup



Traffic Management

- routers and switches in a small network should be configured to support real-time traffic
    - **E.g.** voice and video
- Good network design classifies traffic according to priority
- Minimises network downtime

Small Network Applications and Protocols

Common Applications

- **Network Applications**
    - software programs used to communicate over the network\
    - Can be end-user applications are network-aware → implement application layer protocols and communicate directly with the lower layers of the protocol stack (**e.g.** email clients and web browsers)
- **Application Layer Services**
    - Programs that need the assistance of application layer services (**e.g.** le transfer or network print spooling)
    - Interface with the network and prepare the data for transfer

Common Protocols

- Network protocols support the applications and services used by employees in a small network
- Common protocols used:
    - DNS Server
    - Telnet
    - Email Server
    - DHCP Server
    - Web Server
    - FTP Server
- Each of these network protocols define:
    - Processes on either end of a communication session
    - Types of messages
    - Syntax of the messages
    - Meaning of informational fields
    - How messages are sent and the expected response
    - Interaction with the next lower layer
- Establish a policy of using secure versions of these protocols whenever possible

Voice and Video Applications

- Ensure the proper equipment is installed in the network and that the network devices are configured to ensure priority deliver
- **Infrastructure**
  - Must accommodate the characteristics of each type of traffic
  - Must determine whether the existing switches and cabling can support the traffic that will be added to the network.
- **VoIP**
  - The device could be an analog telephone adapter (ATA) that is attached between a traditional analog phone and the Ethernet switch → after the signals are converted into IP packets, the router sends those packets between corresponding location
- **IP Telephony**
  - IP phone itself performs voice-to-IP conversion
  - IP phones use a dedicated server for call control and signalling
- **Real-Time Applications**
  - Must be able to support applications that require delay-sensitive delivery
  - Real-Time Transport Protocol (RTP)
  - Real-Time Transport Control Protocol (RTCP)
    - RTP and RTCP enable control and scalability of the network resources by allowing Quality of Service (QoS)

Scale to Larger Networks

Small Network Growth

- To scale a network:
  - **Network documentation** - physical and logical topology
  - **Device inventory** - list of devices that use or comprise the network
  - **Budget** - itemised IT budget, including fiscal year equipment purchasing budget
  - **Traffic analysis** - protocols, applications, and services and their respective traffic requirements, should be documented

Protocol Analysis

- Understand the type of traffic that is crossing the network as well as the current traffic flow
- To determine traffic flow patterns, it is important to:
  - Capture traffic during peak utilization times to get a good representation of the different traffic types
  - Perform the capture on different network segments; some traffic will be local to a particular segment
- Information gathered is evaluated based on the source and destination of the traffic, as well as the type of traffic being sent
  - used to make decisions on how to manage the traffic more efficiently

Employee Network Utilisation

- Network administrator must also be aware of how network use is changing
- Does this through “snapshots”
  - OS and OS Version
  - Non-Network Applications
  - Network Applications
  - CPU Utilization
  - Drive Utilization
  - RAM Utilization
- Informing the network administrator of evolving protocol requirements and associated traffic flows

11.2 Network Security

Security Threats and Vulnerabilities

Types of Threats

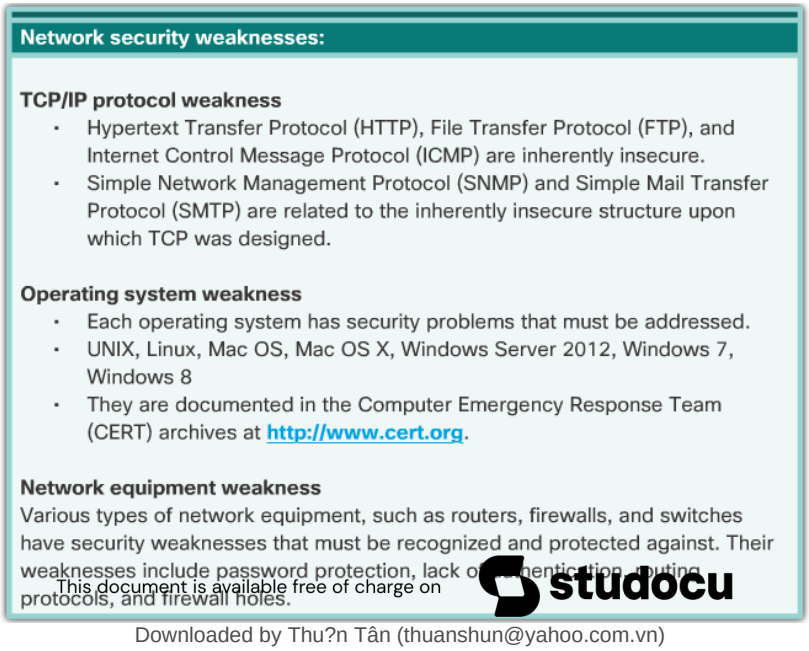
- Intrusion by an unauthorized person can result in costly network outages and loss of work
- Intruders can gain access to a network through software vulnerabilities, hardware attacks or through guessing someone's username and password
- After the hacker gains access to the network, four types of threats may arise:
    - **Information Theft**
        - Breaking into a computer to obtain confidential information
        - Information can be used or sold for various purposes
    - **Data Loss and Manipulation**
        - Breaking into a computer to destroy or alter data records
        - **E.g.** data loss: sending a virus that reformats a computer's hard drive.
        - **E.g.** manipulation: breaking into a records system to change information, such as the price of an item.
    - **Identity Theft**
        - Form of information theft where personal information is stolen for the purpose of taking over someone's identity
        - Using this information, an individual can obtain legal documents, apply for credit, and make unauthorized online purchases
    - **Disruption of Service**
        - Preventing legitimate users from accessing services to which they should be entitled
        - **E.g.** DoS attacks on servers, network devices, or network communications links

Physical Security

- The four classes of physical threats are:
    - **Hardware threats** - physical damage to servers, routers, switches, cabling plant, and workstations
    - **Environmental threats** - temperature extremes (too hot or too cold) or humidity extremes (too wet or too dry)
    - **Electrical threats** - voltage spikes, insufficient supply voltage (brownouts), unconditioned power (noise), and total power loss
    - **Maintenance threats** - poor handling of key electrical components (electrostatic discharge), lack of critical spare parts, poor cabling, and poor labelling
- Plan physical security to limit damage to the equipment:
    - Lock up equipment and prevent unauthorized access from the doors, ceiling, raised floor, windows, ducts, and vents
    - Monitor and control closet entry with electronic logs
    - Use security cameras

Types of Vulnerabilities

- There are three primary vulnerabilities/ weaknesses:
    - **Technological**



- **Configuration**

Configuration Weakness	How the weakness is exploited
Unsecured user accounts	User account information may be transmitted insecurely across the network, exposing usernames and passwords to snoopers.
System accounts with easily guessed passwords	This common problem is the result of poorly selected and easily guessed user passwords.
Misconfigured Internet services	A common problem is to turn on JavaScript in Web browsers, enabling attacks by way of hostile JavaScript when accessing untrusted sites. IIS, FTP, and Terminal Services also pose problems.
Unsecured default settings within products	Many products have default settings that enable security holes.
Misconfigured network equipment	Misconfigurations of the equipment itself can cause significant security problems. For example, misconfigured access lists, routing protocols, or SNMP community strings can open up large security holes.

- **Security policy**

Policy Weakness	How the weakness is exploited
Lack of written security policy	An unwritten policy cannot be consistently applied or enforced.
Politics	Political battles and turf wars can make it difficult to implement a consistent security policy.
Lack of authentication continuity	Poorly chosen, easily cracked, or default passwords can allow unauthorized access to the network.
Logical access controls not applied	Inadequate monitoring and auditing allow attacks and unauthorized use to continue, wasting company resources. This could result in legal action or termination against IT technicians, IT management, or even company leadership that allows these unsafe conditions to persist.
Software and hardware installation and changes do not follow policy	Unauthorized changes to the network topology or installation of unapproved applications create security holes.
Disaster recovery plan is nonexistent	The lack of a disaster recovery plan allows chaos, panic, and confusion to occur when someone attacks the enterprise.

Network Attacks

Types of Malware

- Code or software that is specifically designed to damage, disrupt, steal, or inflict “bad” or illegitimate action on data, hosts, or network

- **Viruses**
  - Propagates by inserting a copy of itself into, and becoming part of, another program
  - Spreads from one computer to another, leaving infections as it travels
  - Almost all viruses are attached to an executable file, which means the virus may exist on a system but will not be active or able to spread until a user runs or opens the malicious host file or program
  - Viruses spread when the software or document they are attached to is transferred from one computer to another using the network, a disk, file sharing, or infected e-mail attachments
- **Worms**
  - worms are standalone software and do not require a host program or human help to propagate
  - Worms take advantage of system features to travel through the network unaided
- **Trojan Horses**
  - Harmful piece of software that looks legitimate → users are tricked into executing it
  - After its activated, it can achieve any number of attacks on the host:
    - Irritating the user (popping up windows or changing desktops) to damaging the host (deleting files, stealing data, or activating and spreading other malware, such as viruses)
  - Known to create back doors to give malicious users access to the system

Network attacks can be classified into three major categories:

Reconnaissance Attacks

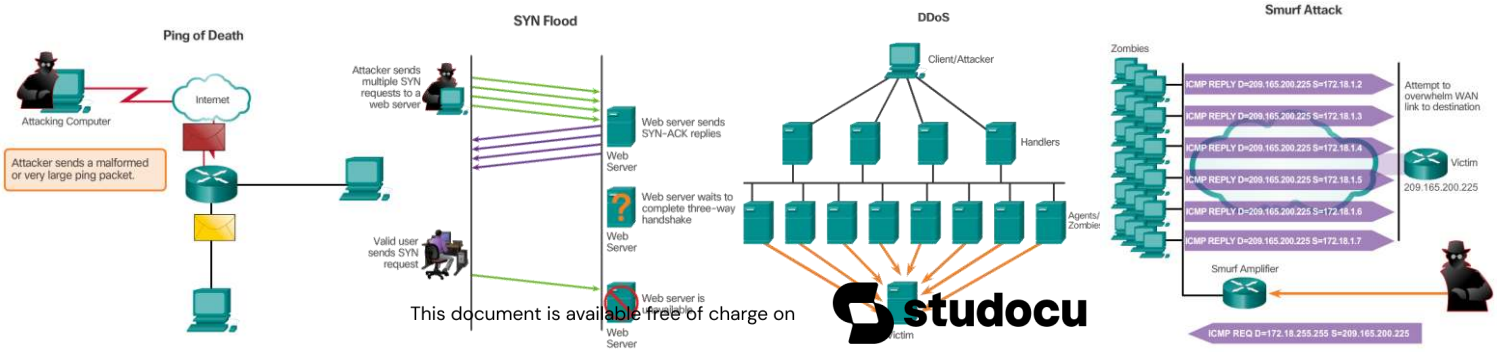
- The discovery and mapping of systems, services, or vulnerabilities
- External attackers can use Internet tools to easily determine the IP address space assigned to a given corporation or entity
- After the IP address space is determined, an attacker can then ping the publicly available IP addresses to identify the addresses that are active

Access Attacks

- Access attacks exploit known vulnerabilities in:
  - Authentication services
  - FTP services
  - Web services to gain entry to web accounts, confidential databases, and other sensitive information
- Classified into four types:
  - Password attacks
  - Trust Exploitation
  - Port Redirection
  - Man-in-the-Middle

Denial of Service Attacks

- Prevent authorized people from using a service by consuming system resources
- Most difficult to eliminate
- Stay up to date with the latest security updates for operating systems and application
- **E.g.** ping of death, SYN Flood, DDos, Smurf Attack



Network Attack Mitigation

Backup, Upgrade, Update and Patch

- Keeping up-to-date → more effective defence against network attacks
- most effective way to mitigate a worm attack is to download security updates from the operating system vendor and patch all vulnerable systems
- Security requirements change and already deployed systems may need to have updated security patches installed
- One solution to the management of critical security patches is to create a central patch server that all systems must communicate with after a set period of time

Authentication, Authorisation and Accounting

- AAA network security services provide the primary framework to set up access control on a network device
- Way to control:
    - Who is permitted to access a network (authenticate)
    - What they can do while they are there (authorise)
    - What actions they perform while accessing the network (accounting)

Firewalls

- One of the most effective security tools available for protecting users from external threats
- Network firewalls reside between two or more networks, control the traffic between them, and help prevent unauthorized access
- Host-based firewalls or personal firewalls are installed on end systems
- Firewall techniques are:
    - **Packet filtering** - Prevents or allows access based on IP or MAC addresses
    - **Application filtering** - Prevents or allows access by specific application types based on port numbers
    - URL filtering - Prevents or allows access to websites based on specific URLs or keywords
    - **Stateful packet inspection (SPI)** - Incoming packets must be legitimate responses to requests from internal hosts. Unsolicited packets are blocked unless permitted specifically. SPI can also include the capability to recognize and filter out specific types of attacks, such as denial of service (DoS)
- Firewall products:
    - **Cisco Security Appliances**
        - Dedicated firewall devices are specialised computers that do not have peripherals or hard drives. Appliance-based firewalls can inspect traffic faster and are less prone to failure
    - **Server-Based Firewall**
        - Firewall applications provide a solution that combines an SPI firewall and access control based on IP address or application
        - Server-based firewalls can be less secure than dedicated, appliance-based firewalls because of the security weaknesses of the general purpose OS
    - **Cisco WRP500 Wireless Broadband Router**
        - Higher-end routers that run special operating systems like Cisco Internetwork Operating System (IOS) also have firewall capabilities that can be configured
    - **Personal Firewall**
        - Client-side firewalls that typically filter using SPI
        - The user may be prompted to allow certain applications to connect or may define a list of automatic exceptions
        - Often used when a host device is connected directly to an ISP modem → may interfere with Internet access if not properly configured
        - Not recommended to use more than one personal firewall at a time since they can conflict with one another.

Endpoint Security

- A company must have well-documented policies in place and employees must be aware of these rules
  - Employees need to be trained on proper use of the network
  - Policies often include the use of antivirus software and host intrusion prevention

Device Security

Device Security Overview

- ***auto secure*** command → used to assist securing the system
- Simple steps that should be taken that apply to most operating systems:
  - Default usernames and passwords should be changed immediately
  - Access to system resources should be restricted to only the individuals that are authorized to use those resources
  - Any unnecessary services and applications should be turned off and uninstalled when possible
- Also it is important to update any software and install any security patches prior to implementation.

Passwords

- Guideline for good passwords:
  - Length >= 8 characters
  - Complex
  - Mix of uppercase and lowercase letters, numbers, symbols, and spaces
  - Avoid repetition, common dictionary words, letter or number sequences, usernames, relative or pet names, biographical information, such as birthdates, ID numbers, ancestor names, or other easily identifiable pieces of information.
  - Deliberately misspell a password. **E.g.** Smith = Smyth = 5mYth or Security = 5ecur1ty.
  - Change passwords often
  - Do not write passwords down

Basic Security Practices

- **Additional Password Security**
  - ***service password-encryption*** command → prevents unauthorized individuals from viewing passwords in plain text in the configuration file
  - ***security passwords min-length*** command → ensure that all configured passwords are a minimum of a specified length
  - ***login block-for 120 attempts 3 within 60*** command → blocking login attempts to the device if a set number of failures occur within a specific amount of time.
- **Exec Timeout**
  - ***exec-timeout*** command → sets executive timeouts. By setting the exec timeout, you are telling the Cisco device to automatically disconnect users

Enable SSH

Step 1. Ensure router has a unique hostname, and then configure the IP domain name of the network using the **ip domain-name** command in global configuration mode.

Step 2. To generate the SSH key, use the **crypto key generate rsa general-keys** command in global configuration mode. The modulus determines the size of the key and can be configured from 360 bits to 2048 bits. The larger the modulus, the more secure the key, but the longer it takes to encrypt and decrypt information. The minimum recommended modulus length is 1024 bits.

Step 3. Create a local database username entry using the **username** global configuration command.

Step 4. Enable inbound SSH sessions using the line vty commands **login local** and **transport input ssh**.

Backup and Restore Configuration Files

Router File Systems

- Cisco (IFS) allows the administrator to navigate to different directories and list the files in a directory, and to create subdirectories in flash memory or on a disk.
- ***show file systems*** command → lists all of the available file systems on a Cisco 1941 router
  - provides amount of available and free memory, the type of file system, and its permissions

- **The Flash File System**
  - ***dir*** command → flash is the default file system, the ***dir*** command lists the contents of flash. Several files are located in flash, but of specific interest is the last listing. This is the name of the current Cisco IOS file image that is running in RAM.
- **The NVRAM File System**
  - Must change the current default file system using the **cd**(change directory) command. The **pwd** (present working directory) command verifies that we are viewing the NVRAM directory. Finally, the **dir** (directory) command lists the contents of NVRAM.

Switch File Systems

- ***show file systems*** command → view the file systems on a Catalyst switch is the same as on a Cisco router

Backing Up and Restoring Using Text Files

- **Backup Configurations with Text Capture (Tera Term)**
  - Configuration files can be saved/archived to a text file using Tera Term.
    Step 1. On the File menu, click **Log**.
    Step 2. Choose the location to save the file. Tera Term will begin capturing text.
    Step 3. After capture has been started, execute the **show running-config** or **show startup-config** command at the privileged EXEC prompt. Text displayed in the terminal window will be directed to the chosen file.
    Step 4. When the capture is complete, select **Close** in the Tera Term: Log window.
    Step 5. View the file to verify that it was not corrupted
- **Restoring Text Configurations**
  - A configuration can be copied from a file to a device → the file will require editing to ensure that encrypted passwords are in plain text and that non-command text such as "--More--" and IOS messages are removed
    Step 1. On the File menu, click **Send** file.
    Step 2. Locate the file to be copied into the device and click **Open**.
    Step 3. Tera Term will paste the file into the device

Backing Up and Restoring TFTP

- **Backup Configurations with TFTP**
  - Configuration files can be stored on a Trivial File Transfer Protocol (TFTP) server or a USB drive
  - ***copy running-config tftp*** or ***copy startup-config tftp*** command → save the running configuration or the startup configuration to a TFTP server
    - **Step 1.** Enter the ***copy running-config tftp*** command.
    - **Step 2**. Enter the IP address of the host where the configuration file will be stored.
    - **Step 3**. Enter the name to assign to the configuration file.
    - **Step 4**. Press Enter to confirm each choice.
- **Restoring Configurations with TFTP**
  - ***copy tftp running-config*** or ***copy tftp startup-config*** command → To restore the running configuration or the startup configuration from a TFTP server\
    - **Step 1**. Enter the ***copy tftp running-config*** command.
    - **Step 2**. Enter the IP address of the host where the configuration file is stored.
    - **Step 3**. Enter the name to assign to the configuration file.
    - **Step 4**. Press **Enter** to confirm each choice

Using USB Ports on a Cisco Router

- The USB flash feature provides an optional secondary storage capability and an additional boot device
- Images, configurations, and other files can be copied to or from the Cisco USB flash memory with the same reliability as storing and retrieving files using the Compact Flash card
- Modular integrated services routers can boot any Cisco IOS Software image saved on USB flash memory
- ***dir*** command → view the contents of the USB flash drive

Backing Up and Restoring using a USB

- **Backup Configurations with a USB Flash Drive**
  - ***show file systems*** command → to verify that the USB drive is there and confirm the name
  - ***copy run usbflash0:/*** command → to copy the configuration file to the USB flash drive
  - ***dir*** command → to see the file on the USB drive
  - ***more*** command → to see the contents
- **Restore Configurations with a USB Flash Drive**
  - ***copy usbflash0:/[file name] running-config*** command → to restore a running configuration

11.3 Basic Network Performance

The ping Command

Interpreting ping Results

- Tests connectivity
- Uses the Internet Control Message Protocol (ICMP) and verifies Layer 3 connectivity
- Helps to identify the source of the problem → help to troubleshoot network failure
- **IOS Ping Indicators**
  - **!** → receipt of an ICMP echo reply message
  - **.** → time expired while waiting for an ICMP echo reply message
    - Connectivity problem occurred somewhere along the path
    - May indicate that a router along the path did not have a route to the destination
    - May be blocked by device security
  - **U** → an ICMP unreachable message was received
    - The router either did not have a route to the destination address or that the ping request was blocked
- **Testing the Loopback**
  - Pinging the loopback address (127.0.0.1) → verifies the internal IP configuration on the local host
  - Verifies the proper operation of the protocol stack from the network layer to the physical layer

Extended ping

- ***ping [without destination IP address]*** command (in privileged exec mode) → extended ping
- Network administrator can verify from R2 that R1 has a route to R1

Network Baseline

- Network baseline → one of the most effective tools for monitoring and troubleshooting network performance
- Creating a picture of overall network performance
  - Measuring performance at measuring times
  - Over time
  - Loads
- The output derived from network commands can contribute data to the network baseline
- Starting a baseline:
  - Copy and paste results from ping, trace, etc. → time and date stamp saved into an archive
  - Error messages
  - Response times
- Companies should have extensive baselines → software

The traceroute and tracert Command

Interpreting Trace Messages

- returns a list of hops as a packet is routed through a network
- form of the command depends on where the command is issued

- ***tracert*** command on computer
- ***traceroute*** command on a router
- No response/ timeout = failure in the internetwork

Show Commands

Common show Commands Revisited

- ***show*** commands display:
  - Relevant information about the configuration and operation of the device
  - Viewing configuration files
  - Checking the status of device interfaces and processes
  - Verifying the device operational status
- ***show*** commands are:
  - show ***running-config***
  - show ***interfaces***
  - show ***arp***
  - show ***ip route***
  - show ***protocols***
  - show ***version***

Host and IOS Commands

The ipconfig Command

- ***ipconfig*** command → IP address of the default gateway of a host
- ***ipconfig /all*** command → MAC address as well as a number of details regarding the Layer 3 addressing of the device
- ***ipconfig /displaydns*** command → cached DNS entries on a Windows computer system
  - DNS Client service on Windows PCs optimizes the performance of DNS name resolution by storing previously resolved names in memory, as well. As shown if Figure 3, the

The arp Command

- ***arp*** command
- ***arp –a*** command → lists all devices currently in the ARP cache of the host
  - Includes the IPv4 address, physical address, and the type of addressing (static/dynamic)
- ***arp -d**** command → cache can be cleared in the event the network administrator wants to repopulate the cache with updated information
- The ARP cache only contains information from devices that have been recently accessed → to ensure ARP cache is populated, ping a device so that it will have an entry in the ARP table

The show cdp neighbors command

- Cisco Discovery Protocol (CDP) is a Cisco-proprietary protocol that runs at the data link layer
- Runs on bootup → CDP automatically discovers neighboring Cisco devices running CDP, regardless of which Layer 3 protocol or suites are running
- ***show cdp neighbors detail*** command → reveals the IP address of a neighbouring device
- provides the information:
  - *Device identifiers* - For example, the configured host name of a switch
  - *Address list* - Up to one network layer address for each protocol supported
  - *Port identifier* - The name of the local and remote port in the form of an ASCII character string, such as FastEthernet 0/0
  - *Capabilities list* - For example, whether this device is a router or a switch
  - *Platform* - The hardware platform of the device; for example, a Cisco 1841 series router
- Can have security risks
- ***No cdp run*** command → disable

The show ip interface brief Command

- **Verifying Router Interfaces**

- ***show ip interface brief*** command → provides a more abbreviated output and a summary of the key information for all the network interfaces on a router

- **Verifying the Switch Interfaces**
  - ***show ip interface brief*** command → used to verify the status of the switch interfaces