CCNA Summary

# Module 1 - Networking today

## Network roles

* Augment and enhance human interactions.
* Facilitate the creation of global communities.
* Make possible cloud storage for mobile data access.

…plus many more.

## Network components

A computer network is a collection of data-sharing computers linked together.

Hosts (end devices) are computers connected to a network and directly participate in communication in the network. Some hosts are also called clients.

The term host is specifically used for a computer assigned a unique Internet Protocol (IP) address to distinguish it from others in the network. The address identifies host and network the host is attached to.

Servers are computers that serve information to other end devices. To do this, they need specialized server software for different kinds of services such as emails, webpages or files. Meanwhile, clients have software to request the server for data (for example, web browsers, email clients, file viewers…). Servers and clients can run multiple kinds of server/client softwares simultaneously.

A peer-to-peer network is a network in which one or many computers act as both a client and a server. This network type is often seen in small home and business networks.   
  
Advantages of P2P:

* Easy to build.
* Less complex.
* Cheaper since network devices and dedicated servers may not be required.
* Adequate for simple tasks.

Disadvantages:

* No centralized administration.
* Less secure.
* Not scalable.
* Potential performance slowdown as all devices may act both as clients and servers.

An end device is either the source or destination of data delivered over the network. End devices are distinguished from each other with a unique address.

Intermediary devices connect end devices to the network or networks to an internetwork. Intermediary devices use the destination address in tandem with info about network interconnections to determine a path for data transmission.

Some roles of intermed devices:

* Regenerate and retransmit communication signals.
* Maintain information about pathways.
* Inform other devices of errors.
* Direct data to alternative pathways on link failure.
* Classify and direct message according to priorities.
* Allow or deny data flow depending on settings.

Network media are the channels along which data transmits. For modern networks there are 3 main media:

* Metal wires within cables - Data as electrical impulses.
* Glass/plastic fibers within cables - Data as light pulses.
* Wireless - Data as modulation of specific frequencies of electromagnetic waves.

When choosing the appropriate medium, one should consider: the maximum distance permitted by the media, the environment where the media will be installed, the data amount and required speed, and the cost of media and installation.

## Network topology diagrams

Network topology diagrams help visualize the components within a network and their relationship with other components. Two types: physical and logical.

The physical type contains information about the physical locations at which the network devices will be installed.

The logical type contains information about the devices, ports and addressing scheme of the network.

Special terminology:

* Network Interface Card (NIC): Physically connects an end device to a network.
* Physical port: An outlet on a networking device where the media connects to an end device or another networking device.
* Interface: Specialized ports on a networking device that connect to individual networks. Router ports are referred to as network interfaces because routers connect networks together.

## Network types

Network sizes range from small home networks to worldwide networks. Two common types of network infrastructures are Local Area Networks (LAN) and Wide Area Networks (WAN).

LAN interconnects end devices in a small geographical area. LAN is often managed by an organization or individual. Administrative control is enforced at the network level and governs the security and access control policies. LAN provides high-speed bandwidth to ***internal*** devices.

WAN connects LANs over a large geographical area and is often managed by (internet) service providers. WAN often provides slower-speed links between LANs.

The Internet is a worldwide collection of interconnected networks. The Internet is not owned by anyone and thus, consistent, standardized practices and technologies are needed to ensure smooth communication over the Internet. Many organizations have been created to maintain standards for the Internet.

Intranets are private networks that belong to an organization. They are meant to be used in-house or accessible to outsiders only with authorization.

Extranets are controlled private networks that allow outside suppliers or collaborators to securely access data from an organization - typically a subset of the information accessible through its intranet.

## Internet connection options

For home and small office internet connections, a connection to the ISP is typically required. Connection options include:

* Cable: Offered by cable TV service providers, data travels along the same cable as that of cable TV. High-bandwidth, availability, always on internet connection.
* DSL (Digital Subscriber Lines) - Runs over a telephone line. Also high-bandwidth, high availability, always on internet connection. Generally asymmetrical DSL is used (download is faster than upload)
* Cellular - Uses a cellphone network to connect. Available whenever the user has access to a cellular signal. Performance is limited by phone and cell tower.
* Satellite - Dishes require a clear line of sight to the satellite. Give connection opportunities to areas that would otherwise have no connectivity.
* Dial-up telephone - Inexpensive option that involves a phone line and a modem. Low bandwidth, so useful only for lightweight use.

For corporations, higher bandwidth, dedicated bandwidth and managed services may be required. They have access to the following options:

* Dedicated Leased Line - Leased lines are reserved circuits within the SP’s network that connects separated offices together.
* Metro Ethernet (Ethernet WAN) - Extend LAN technology into WAN.
* Business DSL - Available in various formats. SDSL is popular, similar to consumer DSL but with equal download/upload speeds.
* Satellite: - When no wired option is available.

Previously, different kinds of information had to be transmitted on different networks. Now, they can be delivered on the same network, allowing multiple services to be run on one network (converging network). These networks must follow the same rulesets and standards.

## Network reliability

4 characteristics of a reliable network:

1. Fault tolerance: Limit the number of affected devices in a network failure. Relies on the existence of multiple paths between source and destination (redundancy). Packet switching is one way of achieving redundancy. It involves splitting the message into packets which can be delivered along different paths in the network.
2. Scalability: Supports new users and applications without compromising performance of existing services. Achieved by adhering to accepted standards and protocols.
3. Quality of Service: QoS policies ensure reliable data transmission across the network. Prioritize time-sensitive traffic (such as voice or video communication) when congestion occurs. Congestion happens when more bandwidth is needed than available.
4. Security: Two concerns - network infrastructure security and information security. Former involves physically securing networking devices and preventing unauthorized access to the management of these devices. Latter must meet three requirements: (1) confidentiality (data access restricted to intended and authorized recipients), (2) integrity (data remains unaltered throughout transmission), (3) availability (timely and reliable data access)

## Networking trends

Trends in computer networking:

1. Bring your own device (BYOD): Users have the freedom to use their personal devices to communicate across a business or campus network rather than having to use officially provided ones.
2. Online collaboration
3. Video communication
4. Cloud computing: Allows the storage of files on servers on the Internet. Made possible thanks to data centers, which are expensive to build and maintain. Distributed data centers used to ensure security, reliability and fault tolerance. Four types of clouds: (1) public clouds, (2) private clouds, (3) hybrid clouds, (4) community clouds.

Networking trends in the home - Smart home technology: Every-day appliances made “smarter” through connection with other devices.

Powerline networking: Make use of existing electrical wiring to connect devices.

Wireless broadband: When cable and DSL are not available. WISPs and Wireless Broadband Service.

## Network security

Security threats:

External:

1. Viruses, worms, trojan horses - malicious code
2. Spyware and adware - applications that secretly collect data.
3. Zero-day attacks - attacks on the first day a vulnerability becomes known
4. Threat actor attacks - malicious person attacks
5. Denial of service attacks - slowing or crashing applications
6. Data interception and theft - stealing private information from an organization
7. Identity theft - stealing login credentials to access private data.

Internal: lost/stolen devices, accidental misuse by employees, malicious employees…

Security solutions

For home users:

* Antivirus and antispyware - protect against malicious software
* Firewall filtering - blocks unauthorized access into and out of the network. Can be implemented on end devices or on routers.

For corporations:

* Dedicated firewall systems - advanced filtering capabilities for large volumes of traffic
* Access control lists (ACL) - filters access and traffic forwarding based on IP addresses and applications
* Intrusion prevention systems (IPS) - identifies fast-spreading threats
* Virtual private networks (VPN) - provides secure access for remote workers

…along with antivirus, antispyware and firewall filtering.

# Module 2 - Configuring switches and end devices

## Cisco IOS and access methods

An operating system is a piece of software that manages other software applications and hardware components. The kernel is a part of the OS that interacts directly with the hardware. The shell is the interface between the applications and the user. There are 2 types of user interface: command-line interface (CLI) and graphical user interface (GUI).

CLI lets users enter commands with a keyboard in a text-based environment. The system then executes the command, providing textual output. CLIs require little overhead but is more difficult and less user-friendly.

GUI lets users interact with the system through graphical icons and buttons. GUI is user-friendly, easy to use but may not provide all features and is generally less reliable than CLI.

Cisco networking devices use the Cisco IOS (Internetwork OS) of varying versions depending on the device type. Users can run commands on networking devices through the Cisco IOS.

Networking devices can be accessed with one of the following methods:

* Console: Requires a computer running terminal emulation software and a special console cable to establish a connection. The cable is plugged into a physical management port to provide out-of-band access to the device (access via a dedicated channel separated from normal network channels). Useful for when no networking devices are configured, such as in the initial configuration.
* Secure Shell (SSH): Allows users to securely establish remote CLI connections to the device. The connection is in-band and takes place over the network. Requires active networking services on the device, including an interface configured with an address.
* Telnet: Similar to SSH but without encryption. Sensitive data such as authentication and passwords is sent in plaintext. Should be used only in lab environments.
* Auxiliary Port (legacy): Remotely access a network device over a telephone connection using a modem.

## Command modes

Management access is separated into two command modes:

* User EXEC mode (>): Limited control, only a few monitoring commands available. Cannot run configuration commands.
* Privileged EXEC mode (#): Full control. Allows users to run configuration commands on the device. Other configuration modes only reachable if the user is in this mode.

To configure the network device or a specific part of it, the user must enter a configuration mode:

* Global configuration mode ((config)#): Changes impact entire device. From here users can enter specific configuration modes.
* Line configuration mode ((config-line)#): Configures console, SSH, Telnet or AUX access.
* Interface configuration mode ((config-if)#): Configures a switch port or router network interface.

Switching between modes:

| User EXEC | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| enable | | | ↓↑ | disable | | |
| Privileged EXEC | | | | | | |
| configure terminal | | | ↓↑ | exit | | |
| Global configuration | | | | | | |
| line + type + number | ↓↑ | exit |  | interface + type + number | ↓↑ | exit |
| Line configuration | | |  | Interface configuration | | |
| (use end or ctrl + z to return from subconfig modes to privileged EXEC) | | | | | | |

## Command structure

Prompt + command + space + keywords or arguments (if any)

Keywords are predefined words in the system, meant to be typed in exactly. Arguments are user-provided values.

When unsure what to type next, typing ‘?’ will provide context-sensitive help.

## Basic device configuration

Configuring device names:

* Useful for device identification when connecting via SSH.
* Performed in global configuration mode.
* Syntax: hostname <name>
* Remove name with: no hostname

Configuring passwords:

* Set a password for user EXEC through the console:

configure terminal

line console 0

password <password>

login

* Set a password for privileged EXEC:

configure terminal

enable secret <password>

* Set a password for remote access (SSH/Telnet) through virtual terminal lines:

configure terminal

line vty 0 15 (all 16 vty lines)

password <password>

login

Encrypting passwords:

* Most passwords in startup-config and running-config files are in plaintext, meaning that they are visible once someone accesses said files.
* Encrypt passwords in config files with “service password-encryption” in global config mode. This encryption applies to config files only.

Setting banner messages:

* Banner messages inform users that only authorized personnel can access the device.
* Set a banner message in global config mode with: banner motd #<message>#. The # can be replaced with any character that does not appear in the message.

## Configuration files

Device configuration is stored in 2 files:

* startup-config: Saved in NVRAM, configuration used by device on startup or reboot. Remains unaffected when the power is cut off.
* running-config: Saved in RAM, contains current running configuration. Loses content when power is cut off or when device is restarted.

View configuration files with: show running-config and show startup-config in privileged EXEC mode.

Save changes in running configuration file to startup configuration file with: copy running-config startup-config in privileged EXEC mode.

Reverse the effects of modified and unsaved running configuration with “reload” (incurs brief network downtime) or remove the changed commands individually.

If undesired changes were saved to startup config, clearing all configurations may be needed. Use “erase startup-config” in privileged EXEC mode. Afterwards, the device will use factory-default configuration.

## Ports and addresses

Each end device must be assigned an IP address. IP addresses help end devices locate one another.

IPv4 addresses follow dotted decimal notation and are represented by four decimal numbers between 0 and 255 separated by periods. IPv4 addresses also come with a subnet mask, which can be used to get the network portion of the address. A host may also know of a default gateway, which is the IP address of the router that connects the host to remote networks.

IPv6 addresses are 128 bits long and written as a string of 32 hexadecimals. Groups of 4 digits are separated by a colon.

Network communications depend on end user device interfaces, networking device interfaces and cables. Each link of a network requires a specific network media type and a particular network technology.

The ports on Cisco switches do not support IP addresses. Switches have one or more switch virtual interfaces (SVIs), which are not associated with any hardware. These interfaces let users remotely manage a switch using IP addresses.

## Configure IP addressing

IP addresses can be assigned to end devices manually or automatically with Dynamic Host Configuration Protocol (DHCP)

SVI configuration to allow remote access:

configure terminal

interface vlan 1 (open the interface for configuration)

ip address <ip-address> <subnet-mask> (assign an IP address)

no shutdown (enable the interface)

# Module 3 - Protocols and Models

## Communication rules

The transmission of data across a network is governed by protocols. Some common protocol requirements include:

* Message encoding: Messages are converted into an appropriate form for transmission depending on the type of network media. On arrival, the messages are decoded to obtain the data.
* Message formatting and encapsulation: Messages follow a specific format based on the type and channel.
* Message size: Messages are broken down into frames which contain addressing information. The frames will be reconstructed into the original message by the recipient.
* Message timing: Consists of (1) flow control - controlling the rate of transmission, (2) response timeout - determining what to do when a response does not come after a specified amount of time, and (3) access method - determining when the medium is free so as to avoid collisions.
* Message delivery options: Messages can be delivered in three ways - unicast (one device), multicast (more than one device), and broadcast (all devices).

## Protocols

Networking protocols are implemented in software, hardware, or both. Network communications often involve a combination of different protocols, each serving a specific function.

Some protocol types include:

* Communication protocols: Protocols that allow communication between devices across one or more networks. Examples: Internet Protocol (IP), Transmission Control Protocol (TCP), HyperText Transfer Protocol (HTTP).
* Security protocols: Protocols that provide authentication, data integrity and encryption. Examples: Secure Shell (SSH), Secure Sockets Layer (SSL), Transport Layer Security (TLS)
* Routing protocols: Protocols that enable routers to exchange route information, compare path information and select the best path. Examples: Open Shortest Path First (OSPF), Border Gateway Protocol (BGP).
* Service discovery protocols: Protocols that automatically detect devices or services. Examples: Dynamic Host Configuration Protocol (DHCP) for automatic IP assignment, Domain Name System (DNS) for name-to-IP translation.

Network communication protocols perform one or more of the following functions:

* Addressing: Identifies the sender and intended receiver using an addressing scheme. Examples: Ethernet, IPv4, IPv6.
* Reliability: Guarantees message delivery in the case of data loss or corruption during transit. Example: TCP.
* Flow control: Ensures an efficient rate of data flow. Example: TCP.
* Sequencing: Labels data segments appropriately for correct reassembly. Example: TCP.
* Error detection: Determines data corruption. Examples: Ethernet, IPv4, IPv6, TCP.
* Application interface: Includes information for process-to-process communications between network applications. Examples: HTTP, HTTPS.

## Protocol suites

Since a protocol cannot perform all functions needed for network communication, multiple protocols need to work in conjunction. Protocol suites are sets of protocols designed to seamlessly work together for network communication.

Some protocol suites include:

* Internet Protocol Suite or TCP/IP: Most popular, open standard, maintained by the Internet Engineering Task Force (IETF).
* Open Systems Interconnection (OSI): Most commonly known for OSI reference model. Largely replaced by TCP/IP.
* AppleTalk: Developed by Apple. Replaced by TCP/IP.
* Novell NetWare: Developed by Novell Inc. Replaced by TCP/IP.

TCP/IP is the most widely adopted protocol suite today. It is open standard (freely available to the public) and standards-based (endorsed by the industry and approved by a standards organization). TCP/IP include protocols for the application, transport and internet layers. There are no protocols for the network access layer.

TCP/IP application layer protocols:

* DNS (Domain Name System): Translates domain names into IP addresses.
* DHCPv4: Assigns IPv4 addressing information to DHCPv4 clients at start-up.
* DHCPv6: Similar to v4.
* SLAAC (Stateless Address Autoconfiguration): Allows a device to obtain IPv6 addressing information without a DHCPv6 server.
* SMTP (Simple Mail Transfer Protocol): Allows client-to-server and server-to-server mail sending.
* POP3 (Post Office Protocol v3): Allows clients to retrieve emails from a server and download them.
* IMAP (Internet Message Access Protocol): Permits client access to emails stored on a server and maintenance of emails on the server.
* FTP (File Transfer Protocol): Allows hosts to access and transfer files. Reliable, connection-oriented, acknowledged.
* SFTP (SSH File Transfer Protocol): Establishes a secure file transfer session where the file is encrypted.
* TFTP (Trivial File Transfer Protocol): Connectionless protocol with best-effort, unacknowledged file delivery. Less overhead than FTP.
* HTTP (Hypertext Transfer Protocol): Governs text and multimedia file exchange on the World Wide Web.
* HTTPS (HTTP Secure): HTTP with data encryption.
* REST (Representational State Transfer): Constitutes a set of rules for creating web services that involve the use of application programming interfaces (APIs) and HTTP requests.

TCP/IP transport layer protocols:

* TCP (Transmission Control Protocol): Enables reliable communication between processes on different hosts. Provides reliable, acknowledged transmissions that confirm successful delivery.
* UDP (User Datagram Protocol): Enables a process on one host to send packets to a process on another host. Does not confirm successful transmission.

TCP/IP Internet layer protocols:

* IPv4 (Internet Protocol v4): Receives message segments from transport layer. Packages messages into packets and addresses them for end-to-end delivery.
* IPv6 (Internet Protocol v6): Similar to IPv4 but uses a 128bit address.
* NAT (Network Address Translation): Translates private network IPv4 addresses into globally unique public addresses.
* ICMPv4 (Internet Control Message Protocol for IPv4): Provides feedback to the source about errors during delivery.
* ICMPv6 (ICMP for IPv6): Similar to ICMPv4 but used for IPv6 packets.
* ICMPv6 ND (ICMPv6 Neighbor Discovery): Includes 4 protocol messages for address resolution and duplicate address detection.
* OSPF (Open Shortest Path First): Link-state routing protocol that uses a hierarchical design based on areas. Open standard interior routing protocol.
* EIGRP (Enhanced Interior Gateway Routing Protocol): Cisco proprietary protocol that uses a composite metric based on bandwidth, delay, load and reliability.
* BGP (Border Gateway Protocol): Open standard exterior gateway routing protocol used between ISPs or between ISPs and private clients.

Network Access Layer protocols:

* ARP (Address Resolution Protocol): Dynamically maps an IPv4 address to a hardware address.
* Ethernet: Defines the rules for wiring and signaling standards of the network access layer.
* WLAN (Wireless LAN): Defines the rules for wireless signaling across the 2.4 GHz and 5 GHz radio frequencies.

## Standards Organizations

Open standards allow networking devices from different manufacturers to work together. These standards are set by international standards organizations, which are typically vendor-neutral and non-profit.

Involved in the development of standards for the Internet and the TCP/IP protocol suite are:

* Internet Society (ISOC): Promotes the open development and evolution of the Internet worldwide.
* Internet Architecture Board (IAB): Manages and develops internet standards.
* Internet Engineering Task Force (IETF): Develops, updates and maintains internet and TCP/IP technologies. Issues Request for Comments (RFC) documents to develop new protocols and update existing ones.
* Internet Research Task Force (IRTF): Conducts long-term research concerning Internet and TCP/IP technologies.

Some organizations provide further support to TCP/IP:

* Internet Corporation for Assigned Names and Numbers (ICANN): US-based organization which coordinates IP address allocation, domain name management and assignment of other information used in TCP/IP protocols.
* Internet Assigned Numbers Authority (IANA): Oversees and manages IP address allocation, domain name management, and protocol identifiers for ICANN.

Other organizations develop the electronic and communications standards to deliver data over a wired or wireless medium:

* Institute of Electrical and Electronics Engineers (IEEE): Develops the 802.3 Ethernet and 802.11 WLAN standards among others.
* Electronic Industries Alliance (EIA): Sets standards relating to electrical wiring, connectors and mounting racks.
* Telecommunications Industry Association (TIA): Develops communication standards in areas such as radio equipment, cellular towers, Voice over IP devices, satellite communications, etc.
* International Telecommunications Union-Telecommunications Standardization Sector (ITU-T): Defines standards for video compression, Internet Protocol Television, and broadband communications.

## Reference models

Reference models are used to separate the operation of a network into easy-to-understand layers. Each layer describes one step in the networking process. They provide the following benefits:

* Assist in protocol design (protocols that work at a specific layer have information to act on and an interface to above and below layers)
* Foster competition (products can interoperate)
* Prevent technology or capability changes in one layer from affecting other layers.
* Provide a common language to describe networking functions and capabilities.

Two models are used to describe networks: The OSI (Open System Interconnection) model and TCP/IP model.

The OSI model lists the functions and services that can occur at each layer. It stipulates what things must be done but not how they should be achieved. The OSI model consists of 7 layers:

* Application (layer 7): Contains protocols for process-to-process communications.
* Presentation (layer 6): Provides for common representation of the data transferred between application layer services.
* Session (layer 5): Provides services to the presentation layer to organize dialogue and manage data exchange.
* Transport (layer 4): Defines services to segment, transfer and reassemble data.
* Network (layer 3): Provides services to exchange individual pieces of data between end devices.
* Data link (layer 2): Describes methods for exchanging data frames over a common media.
* Physical (layer 1): Describes the means to activate, maintain and de-activate physical connections for a bit transmission.

The TCP/IP model corresponds with the protocol layers in the TCP/IP protocol suite. It consists of 4 layers:

* Application (layer 4): Represents data to the user, including encoding and dialog control.
* Transport (layer 3): Supports communication between devices.
* Internet (layer 2): Picks the best path through the network.
* Network Access (layer 1): Controls the hardware devices and media.

OSI and TCP/IP comparison:

* Layer 4 of the OSI (Transport) maps to Layer 3 of the TCP/IP model (Transport).
* Layer 3 of the OSI (Network) maps to Layer 2 of the TCP/IP model (Internet).
* Layer 4 of the TCP/IP model (Application) maps to Layers 7, 6, 5 (Application, Presentation, Session) of the OSI model.
* Layer 1 of the TCP/IP model (Network Access) maps to Layers 2, 1 (Data link, Physical) of the OSI model.

## Data encapsulation

Before transmission, a message needs to be broken down into packets (segmenting). This prevents large files from clogging up a link, allows packets to travel along different paths, and enables partial retransmission during a network failure.

Segmented packets need to be sequenced so that the complete message can be correctly reassembled by the receiver. This is handled by TCP.

As the chopped up data moves down the protocol stack before being transmitted, various protocol information is added at each level. Each level takes the data from the previous layer and attach some of its own related information in a process called encapsulation. The form that a piece of data takes at any layer is called a protocol data unit (PDU). A PDU has a different name at each layer to reflect its new functions. The names are as follows:

* Data: PDU at application layer.
* Segment (for TCP transport header) / Datagram (for UDP header): PDU at transport layer.
* Packet: PDU at network layer.
* Frame: PDU at data link layer.
* Bits: PDU at physical layer.

Encapsulation starts from top to bottom, and everything in one layer is considered data in the next. Deencapsulation reverses the process, removing one or more protocol headers at each layer then moving the data up.

## Network layer and data link layer addresses

Both the IP packet (network layer) and the frame (data link layer) contain their own addressing information about the sender and receiver. For the data link layer, destination address comes before source address. For the network layer, source address comes before destination address.

Network layer and data link layer addresses serve different purposes:

* Network layer source and destination addresses (layer 3 addresses - logical): Used to deliver the IP packet from the original source to final destination, which may be on the same network or on different networks. An IP address consists of 2 parts: Network portion and host portion (IPv4) or prefix and interface ID (IPv6). The subnet mask (IPv4) or prefix-length (IPv6) is used to get the network portion of an IP address.
* Data link layer source and destination addresses (layer 2 addresses - physical): Used to deliver the frame from one NIC to another on the same network. As an IP packet hops from host to router, router to router, and router to host, at each point it will be encapsulated in a new data link frame reflecting the layer 2 addresses of the sending router and receiving router/host.

When the sender and receiver of the message are on the same network (as determined by the network portion of the source and destination IP addresses in the packet), the frame is sent directly to the receiver. On an Ethernet network, the data link addresses are called media access control addresses (MACs), which are physically embedded on the NIC.

When the sender and receiver of the message are on different networks, the frame is sent to the router or default gateway, which lies on the same network as the sender. The router/default gateway will forward the packet directly to the destination if it is on another network connected to the router/default gateway. Otherwise, the frame is forwarded to another router.

# Module 4 - The physical layer

## Purpose

A physical connection to the network is the first step to network communication. This connection can be either wired (cables) or wireless (radio waves), depending on the network setup.

For wireless connections, a device must be connected to a wireless access point or a wireless router. An access point includes an antenna, several Ethernet switchports, and an internet port.

Network Interface Cards (NICs) connect a device to the network. Ethernet NICs are used for wired connections, and wireless local area network (WLAN) NICs are used for wireless connections.

The OSI physical layer provides the mechanisms to transport the bits that make up a data link frame. It encodes a data link frame into a series of electrical, optical, or radio signals to be transmitted across the media. These signals are sent one by one over the media, received by an end or intermediary device, then decoded back to a frame.

## Standards and characteristics

The standards governing the physical layer mainly concern themselves with physical circuitry. Therefore, they are defined by electrical and communications engineering organizations. These organizations range from international to regional and from governmental to private.

The physical layer standards concern themselves with three areas:

* Physical components: These are the hardware devices, media and connectors that engage in bit transmission.
* Encoding: This is the method or pattern used to represent digital information.
* Signaling: This is the way bits (0s or 1s) are represented physically.

Bandwidth is the data capacity of a medium. It measures the amount of data that CAN flow in a given amount of time. Typical units of measurement are kilobits per second (kbps), megabits per second (Mbps), or gigabits per second (Gbps). Factors that influence bandwidth are the properties of the media and the technologies chosen for signaling and detecting signals.

Latency refers to the time needed for data to travel from one point to another, including delays.

Throughput is the actual transfer of bits across the media over a given period of time. Throughput is typically lower than bandwidth due to the amount of traffic, type of traffic, and latency.

Goodput is the measure of usable data transferred over a period of time. Goodput is throughput minus traffic overhead.

Goodput < Throughput < Bandwidth

## Copper cabling

Converts data into electrical pulses for transmission. Most common type of cabling today.

Advantages:

* Inexpensive.
* Easy to install.
* Low resistance to electrical current.

Disadvantages:

* Limited by distance (signal attenuation)
* Vulnerable to signal interference.

Signal interference can come from two sources:

* Electromagnetic interference (EMI) or radio frequency interference (RFI): radio waves, electromagnetic devices like fluorescent lights and electric motors.
* Crosstalk: Signal on one wire disturbs that of an adjacent wire.

Solutions to interference:

* EMI/RFI: Metallic shielding, proper grounding connections.
* Crosstalk: Twisting opposite circuit wire pairs together to cancel crosstalk.

Unshielded twisted-pair (UTP) cabling

* Terminated by RJ-45 connectors.
* Interconnects hosts with intermediary devices.
* Features 4 color-coded pairs of twisted wires.
* Protected by a plastic jacket.

Shielded twisted-pair (STP)

* Better noise protection than UTP but more expensive and difficult to install.
* Uses RJ-45 connector. Terminated with shielded STP connectors.
* Pairs of twisted wires are wrapped in protective foil. The four pairs are then wrapped in a metallic braid or foil. Protected by an outer plastic jacket.

Coaxial cable

* Used in wireless installations and cable internet installations.
* Consists of a copper conductor to carry electric signals at its core, protected by a layer of plastic insulation. This plastic is then wrapped in a copper braid or foil which shields the core from outside interference. The entire cable is protected by a plastic jacket.
* Types of connectors: Bayonet Neill-Concelman (BNC), N type, F type.

## UTP Cabling

In a UTP cable, interference is limited solely by:

* Cancellation: Wires are paired together to cancel one another’s magnetic field and outside interference.
* Varied numbers of twists per pair: The number of twists per meter is precisely governed.

The standards for UTP cabling are set jointly by the TIA/EIA. They cover the following elements: cable types, cable lengths, connectors, cable termination, and methods of testing. Cables are categorized in terms of bandwidth by the IEEE.

A UTP cable is usually terminated with an RJ-45 connector.

UTP cable wiring may change depending on the situation. This means the wires in the cable may have to be connected in different orders to the sets of pins in the RJ-45 connectors. Main cable types include:

* Ethernet straight-through (both ends T568A or T568B): connects a host to a network device (switch/hub)
* Ethernet crossover (one end T568A, other T658B): connects two hosts or two intermediary devices.
* Rollover (Cisco proprietary): connects a workstation to a router using an adapter.

## Fiber-optic cabling

Converts data into light pulses. Not as commonly used as copper cabling.

Advantages:

* Supports longer distances and higher bandwidths than other media.
* Less signal attenuation. Completely immune to EMI and RFI.

Disadvantages:

* Expensive.
* Requires more expertise to install.

Two main types:

* Single-mode fiber (SMF): Contains a small optical fiber core meant for a single ray of light. Powered by expensive laser technology. Suitable for long-distance situations up to hundreds of kms. Fiber is wrapped in glass cladding and finally polymetric coating.
* Multi-mode fiber (MMF): Contains a larger core for multiple rays. Powered by low-cost LEDs. Supports up to 10 Gbps of bandwidth and approx. 500 meters of link length.

Usage:

* Enterprise networks.
* Fiber-to-the-Home (FTTH).
* Long-haul networks.
* Submarine cable networks.

Connectors:

* Straight-tip (ST): Uses twist-on/off mechanism.
* Subscriber connector (SC): Widely adopted. Uses push-pull mechanism. Used with single mode and multimode fiber.
* Lucent Connector (LC) Simplex: Smaller version of SC.
* Duplex multimode LC: Similar to LC simplex but uses a duplex connector.

Cords (yellow jacket for single-mode, orange/aqua jacket for multimode):

* SC-SC multimode
* LC-LC single-mode
* ST-SC multimode
* SC-ST single-mode

Comparisons with copper:

* Bandwidth: Up to 10Gbs vs. Up to 100Gb/s
* Distance: Up to 100m vs. Up to 100,000m.
* Immunity to interference and electrical hazards: Low vs. Completely immune.
* Costs, expertise required, and safety precautions: Lowest vs. Highest.

## Wireless media

Converts data into radio waves or microwaves. Most common type of connection for end users.

Advantages:

* Allows the most mobility.
* Saves wiring costs.
* Offers ease of use.

Disadvantages:

* Works well in open areas but terrain features and construction materials can limit coverage.
* Vulnerable to interference from common household devices like cordless phones, fluorescent lights or microwaves.
* Presents security risks since any device can access the network.
* Compromises bandwidth per user when many users access the network at the same time.

Wireless standards (all set by IEEE):

* Wi-Fi: Wireless LAN (WLAN) technology. Uses the CSMA/CA protocol (carrier sense multiple access/collision avoidance). The wireless NIC listens to determine if the radio channel is clear before transmitting data.
* Bluetooth: Wireless personal area network (WPAN) standard. It pairs devices for communication up to 100 meters.
* WiMAX: Worldwide Interoperability for Microwave Access. Uses a point-to-point topology to provide wireless broadband access.
* Zigbee: For low-data rate, low-power communications. Typically used for industrial or IoT applications.

A wireless LAN wirelessly connects devices together. A WLAN setup requires the following devices:

* Wireless Access Point (AP): Concentrates the wireless signals from users and connects to the existing copper-based network infrastructure, such as Ethernet.
* Wireless NIC: Allows hosts to wirelessly connect to the network.

## Module 5 - Number systems

## Binary number system

IPv4 addresses are represented in networking devices as 32-bit strings of 0s and 1s. An address is divided into 4 sections called octets, each with 8 bits. When working with IPv4 addresses, it is easier to translate them into decimals in dotted decimal notation.

## Hexadecimal number system

IPv6 and Ethernet MAC addresses are represented in hexadecimal. IPv6 addresses are 128 bits in length, which allows for 32 hexadecimal values. The preferred format for writing an IPv6 address is X:X:X:X:X:X:X:X where each X represents four hexadecimal values.

For information on how to convert between the different number systems, check Computer Systems Week 1 notes. :)

# Module 6 - Data link layer

# Module 14 - Transport layer

Roles:

* Tracking individual conversations, which are sets of data flowing between source and destination.
* Segmenting data into blocks and reassembling them.
* Adding header fields to perform different communication management functions.
* Identifying the target applications with port number.
* Segmenting and multiplexing multiple conversations on the same network.

Protocols: TCP (Transmission Control Protocol), and UDP (User Datagram Protocol)

TCP:

* Connection-oriented protocol which establishes a connection between sender and receiver to maintain state of conversation and track information.
* Provides reliability and flow control by:
  + Number and track data segments.
  + Acknowledge received data.
  + Retransmit unacknowledged data after a period of time.
  + Sequence out-of-order data.
  + Send data efficiently at a manageable rate to the receiver.
* Divides data into segments.
* Suitable for applications that require reliability.
* Roles: establish session, ensure reliable delivery, provide same-order delivery, support flow control.
* TCP Header: 10 fields, 20 bytes.

UDP:

* Connectionless, does not provide reliability and flow control so fewer header fields.
* Best-effort, successful delivery is not acknowledged by the sender. Lost datagrams are not resent.
* Sender and receiver cannot negotiate resource availability.
* Datagrams may not be in order.
* Faster than TCP.
* Divides data into datagrams.
* Suitable for applications that require speed over reliability: live video and multimedia, simple request and reply, applications that handle reliability themselves.

Port number:

* Used by the transport layer to distinguish between different conversations running on the same host or client.
* Source/dest IP address + sort/dest port = socket.
* Assignment of port numbers is managed by the IANA (Internet Assigned Number Authority). Three categories (Well-known from 0 to 1023, registered from 1024 to 49151, private or dynamic ports from 49152 to 65535)

TCP three way handshake:

* A mechanism to establish a connection between the local host and the remote server.
* The initiating host first sends a SYN segment to request client-to-server communication. After receiving this, the remote server sends an ACK segment to acknowledge the host’s message and sends its own SYN to request server-to-client communication. The host finally sends an ACK segment.
* Functions: Confirms to the host that the destination device is present and has an active application accepting requests on the requested port number. Informs the destination that the host wants to establish a connection to that port number.
* SYN and ACK are indicated by the control bits in the segment header.

TCP termination two way handshake:

* Each two-way handshake ends a one-way connection between client and server. Either device can initiate the request.
* First device sends a FIN segment, the other device acknowledges it with an ACK segment. Second device will do the same.
* A total of 4 exchanges needed to close a session.