Network Fundamentals

Devices, Architectures, and the Cloud

- **Layer 2 Switch** – A switch that operates at the Data Link Layer (Layer 2) of the OSI model. It forwards frames based on MAC addresses and builds a MAC address table.
- **Multilayer Switch / Layer 3 Switch** – A switch that can operate at both Layer 2 (switching) and Layer 3 (routing). It can make forwarding decisions based on MAC addresses and IP addresses.
- **Router** – A device that operates at Layer 3 (Network Layer) of the OSI model. It forwards packets between networks using IP addressing and maintains a routing table.
- **Firewall** – A security device (hardware or software) that monitors and controls traffic based on defined security rules, typically operating at Layers 3–7.
- **IDS/IPS** – Intrusion Detection System (IDS) monitors network traffic for malicious activity. Intrusion Prevention System (IPS) actively blocks or prevents detected threats.
- **Access Point (AP)** – A device that allows wireless devices to connect to a wired LAN using Wi-Fi.
- **Wireless LAN Controller (WLC)** – A centralized device that manages multiple APs, providing functions like authentication, configuration, and channel assignment.
- **SDN Controller** – A central control platform for Software-Defined Networking, separating the control plane from the data plane and enabling programmable network management.
- **Virtual Server** – A logical server created through virtualization on a physical machine, providing services such as DHCP, DNS, or applications in a virtualized environment.

Planes:

- **Management Plane** – Used for device configuration, monitoring, and management (e.g., Telnet, SSH, FTP, HTTP, TFTP). This is how administrators interact with network devices.
- **Control Plane** – Responsible for building and maintaining the network topology and routing information (e.g., routing protocols, MAC address table, ARP cache, Routing Information Base [RIB]).

- **Data Plane** – Handles the actual forwarding of packets and frames based on existing tables (e.g., CAM table, Adjacency Information Base [AIB], Forwarding Information Base [FIB]).

Hierarchical Models

LAN Three-tier Hierarchical Model

- **Core** – Provides high-speed backbone connectivity and fast transport between distribution layers.
- **Building Distribution (Aggregation Layer)** – Enforces policies, applies filtering, and aggregates access layer connections.
- **Access** – Connects end devices (PCs, printers, IP phones) to the network and provides initial entry point.

LAN Collapsed Core Hierarchical Model (2-Tier) – Combines core and distribution into a single layer, commonly used in smaller networks.

Data Center Spine and Leaf Topology

- **Spine (Core and Distribution)** – Provides fast, non-blocking interconnection between leaf switches.
- **Leaf (Access)** – Connects servers, storage, and endpoints, and forwards traffic to the spine.

WAN Connections

- **Point-to-Point** – A direct connection between two devices or sites, providing dedicated bandwidth.
- **Point-to-Multipoint** – A single central site connected to multiple remote sites, often using technologies like Frame Relay or MPLS.
- **Mesh Point-to-Point** – Multiple sites connected directly to each other, providing redundancy and multiple paths.
- **Mesh Point-to-Multipoint** – A hybrid topology where some sites have direct connections while others connect through central points.

LAN Small Office/Home Office (SOHO)

Broadband – High-speed internet access delivered via cable, DSL, fiber, or satellite. In CCNA, commonly refers to WAN connectivity for small networks.

On-Prem vs Cloud Network

Considerations: (On-prem means you are responsible for deployment, cost, security, control, and compliance.)

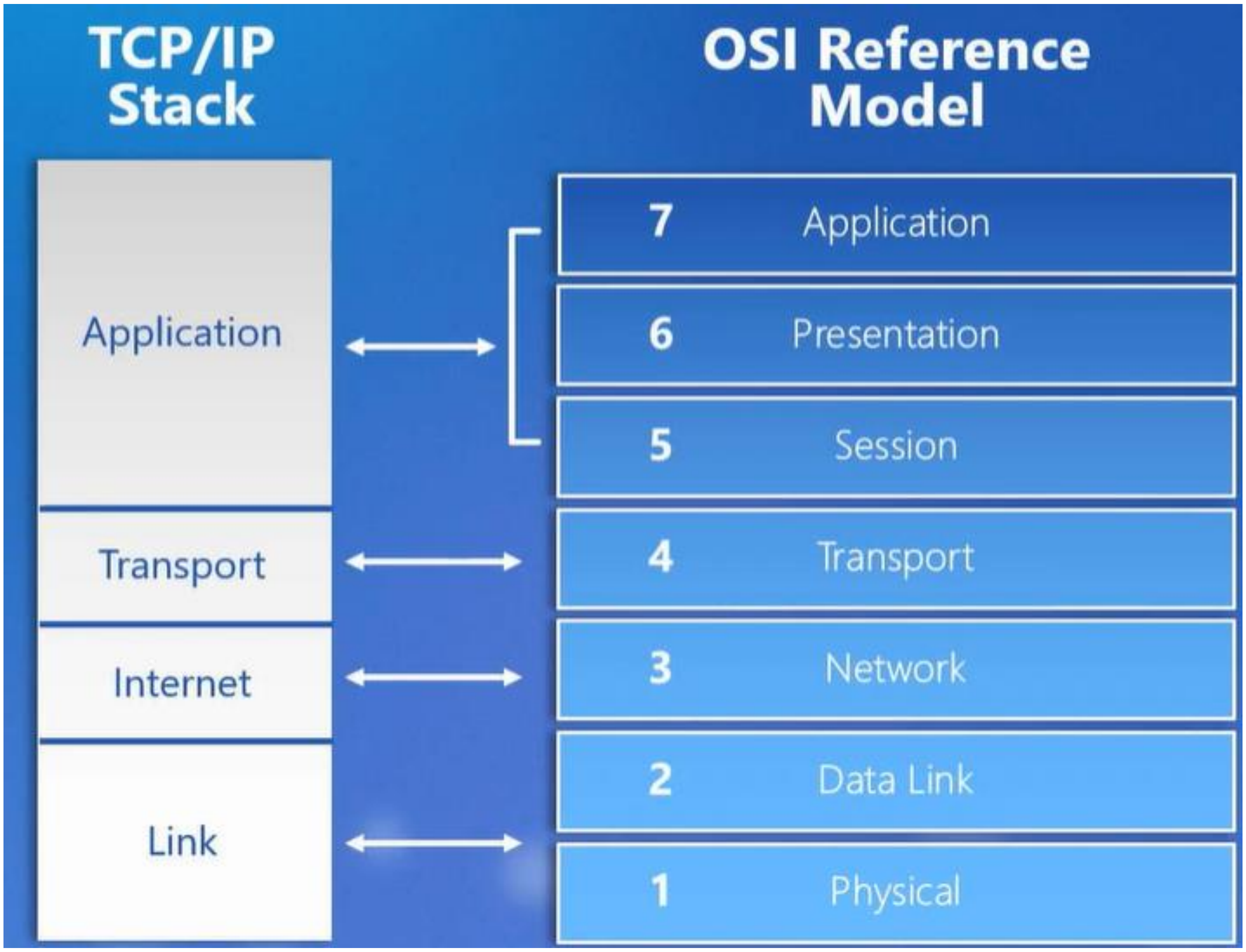
Cloud Network Models:

- **IaaS (Infrastructure as a Service)** – Provides virtualized computing resources over the internet (e.g., virtual machines, storage, networking). You manage OS, apps, and data.
- **PaaS (Platform as a Service)** – Provides a development and deployment environment in the cloud. You manage apps and data, while the provider manages infrastructure and OS.
- **SaaS (Software as a Service)** – Provides ready-to-use software applications over the internet (e.g., Office 365, WebEx). The provider manages everything, and you just use the application.

OSI and TCP/IP Models: Introduction, Application, and Transport Layers

Blueprint for Network Communications

- **Proprietary Model** – Each application uses its own proprietary infrastructure, services, and protocols. This can cause vendor lock-in and interoperability issues.
- **Standards-Based Model** – Built on industry standards (IEEE, IETF, ISO) to ensure interoperability.
  - Multivendor Network Hardware: Cisco, Juniper, Arista, HP
  - Multivendor End-User Devices: Dell, Apple (Mac), Asus, Lenovo
  - Multivendor Software: Applications and services that conform to open standards



OSI Model (Open Systems Interconnection)

- Layer 7 – Application – Interfaces with the user and provides network services (e.g., HTTP, FTP, SMTP).
- Layer 6 – Presentation – Handles data translation, encryption, and compression.
- Layer 5 – Session – Establishes, manages, and terminates sessions between applications.
- Layer 4 – Transport – Provides reliable or unreliable delivery (e.g., TCP, UDP).
- Layer 3 – Network – Provides logical addressing and routing (e.g., IP).
- Layer 2 – Data Link – Provides physical addressing and error detection (e.g., Ethernet, MAC addresses).
- Layer 1 – Physical – Transmits raw bits over the physical medium (e.g., cables, NICs, hubs).

TCP/IP Model

- **Application Layer** – Combines OSI's Application, Presentation, and Session layers (e.g., HTTP, DNS, SMTP).
- **Transport Layer** – Provides host-to-host communication and reliability (TCP, UDP).
- **Internet Layer** – Responsible for logical addressing and routing (IP, ICMP).
- **Network Access Layer** – Encompasses OSI's Data Link and Physical layers, handling physical delivery of data.

Protocol Data Unit (PDU)

- **Layers 5–7 (Data)** – Contains the application data. Common protocols include: FTP (21), SSH (22), Telnet (23), SMTP (25), HTTP (80), HTTPS (443), DNS (53), TFTP (69), SNMP (161, 162)
- **Layer 4 (Segment/TCP or Datagram/UDP)** – Adds the transport layer header to the data (L4 Header)
- **Layer 3 (Packet)** – Adds the network layer header (L3 Header)
- **Layer 2 (Frame)** – Adds the data link layer header (L2 Header)
- **Layer 1 (Bits)** – Transmits the frame as electrical or optical signals over the physical medium

Encapsulation/Decapsulation Steps:

- **Encapsulation**: Layer 7 → Layer 1 (Data is wrapped with headers as it moves down)
- **Decapsulation**: Layer 1 → Layer 7 (Headers are removed as data moves up)

Port Ranges

- **Well-Known Ports:** 0–1023
- **Registered Ports:** 1024–49151
- **Dynamic/Private/Ephemeral Ports:** 49152–65535

TCP vs UDP

- **TCP (Transmission Control Protocol)** – Connection-oriented; ensures reliable, ordered delivery using acknowledgments and retransmissions. Typical applications: HTTP, HTTPS, FTP, SSH
- **UDP (User Datagram Protocol)** – Connectionless; no guarantee of delivery or order, but faster with lower overhead. Typical applications: DNS, DHCP, SNMP, streaming

Key CCNA Tip: Use TCP when reliability is essential, UDP when speed is more important than reliability.

OSI and TCP/IP Models: Internet and Link Layer (Frames)

Layer 3: Network Layer

- **Fragmentation** – Managed in the Layer 3 header with the Identification, Flags, and Fragment Offset fields. Happens when a packet is larger than the Maximum Transmission Unit (MTU) and must be divided into smaller fragments.
- **PMTUD (Path MTU Discovery)** – Identifies the smallest MTU along the communication path between source and destination. Prevents fragmentation by ensuring packets are sent at the correct size for the entire path.

Types of IPv4 Addressing

- **Unicast (1 to 1)** – One device communicates directly with another device. *Example: PC (192.168.1.1) sending traffic to its default gateway (192.168.1.254)*.
- **Broadcast (1 to Everyone)** – One device sends traffic to all devices in the broadcast domain. *Example: ARP request to 255.255.255.255*.
- **Multicast (1 to Group)** – One device sends traffic to a group of subscribed devices. *Example: Streaming video to multicast address 239.1.1.1*.

IPv4 Address Classes

- **Class A** – 0.0.0.0 to 127.255.255.255
  - Private Range: 10.0.0.0/8
  - Public: Anything outside private range

- **Class B** – 128.0.0.0 to 191.255.255.255
  - Private Range: 172.16.0.0/12
  - Public: Anything outside private range
- **Class C** – 192.0.0.0 to 223.255.255.255
  - Private Range: 192.168.0.0/16
  - Public: Anything outside private range
- **Class D** – 224.0.0.0 to 239.255.255.255 (Multicast only)
- **Class E** – 240.0.0.0 to 255.255.255.255 (Experimental use)

Layer 2: Data-Link Layer

- **Frame Check Sequence (FCS)** – A 4-byte error-detection field in the Ethernet trailer. Uses a Cyclic Redundancy Check (CRC) value to confirm data integrity.
- **Ethernet Frame Format** – Includes: Preamble, Destination MAC Address, Source MAC Address, Type/Length, Data, and FCS.
- **Jumbo Frames** – Frames larger than the standard 1500-byte MTU (up to 9000 bytes). Improves efficiency in high-performance networks.

MAC Address Formats

- **Cisco:** 0000.0c43.2e08
- **Linux:** 00:00:0c:43:2e:08
- **Windows:** 00-00-0C-43-2E-08
  - **OUI** - Represents the manufacturer. The first six hexadecimal values of the MAC.
  - **Vendor Assigned** - The last six hexadecimal values.

Types of Frame Based on MAC Address

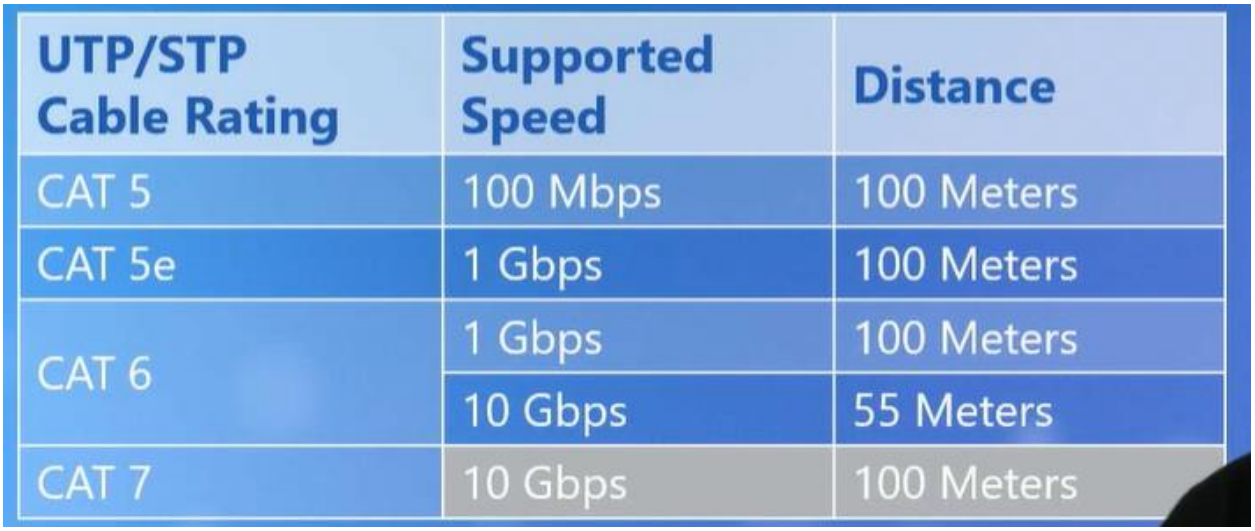
- **Unicast (1 to 1)** - Any MAC to any MAC.
- **Broadcast (1 to Everyone)** - Destination = FF-FF-FF-FF-FF-FF
- **Multicast (1 to a Group)** - Destination = 01-00-5E-XX-XX-XX

Address Resolution Protocol (ARP)

- ARP is for Layer 3 to Layer 2 mapping.

  - ARP requests are sent only within a Broadcast Domain / VLAN / Subnet because ARP is a broadcast.
- Local devices store their mappings in a cache.
  - **ARP Cache** - A table stored on a device that maps IP addresses to their corresponding MAC addresses, used to avoid repeated ARP requests.

OSI and TCP/IP Models: Link Layer (Bits) and PoE



UTP/STP Cable Rating	Supported Speed	Distance
CAT 5	100 Mbps	100 Meters
CAT 5e	1 Gbps	100 Meters
CAT 6	1 Gbps	100 Meters
	10 Gbps	55 Meters
CAT 7	10 Gbps	100 Meters

Wiring Standards

- **T-568A** - Pinout: 1. White/Green, 2. Green, 3. White/Orange, 4. Blue, 5. White/Blue, 6. Orange, 7. White/Brown, 8. Brown
- **T-568B** - Pinout: 1. White/Orange, 2. Orange, 3. White/Green, 4. Blue, 5. White/Blue, 6. Green, 7. White/Brown, 8. Brown

Types of Cables

- **Straight Through Cable** - Connects devices of different types (e.g., PC to Switch). Both ends use the same wiring standard.
- **Crossover Cable** - Connects devices of the same type (e.g., Switch to Switch). One end T-568A, other end T-568B.
- **Rollover Cable** - Connects a PC to a console port on a router or switch. The pinout is reversed (1↔8, 2↔7, etc.).

    - **Auto-MDI-X** - Automatically detects the cable type and configures the interface accordingly.
        - Speed and duplex must be set to AUTO.
            - Manual configuration is not required.

Concepts of PoE

- Delivers power over the same copper cable as Ethernet if the switch is POE-enabled.
    - Detects POE-connected devices using **CDP/LLDP**
        - Negotiates power requirements automatically
- **Standards**
    - **Type 1 - 802.3af (PoE)** - Max 15.4W
    - **Type 2 - 802.3at (PoE+)** - Max 30W
    - **Type 3 - 802.3bt (4PPoE)** - Max 55W
    - **Type 4 - 802.3bt (4PPoE)** - Max 100W

Types of Fiber

- **LC (Lucent Connector)** - Small form factor connector, commonly used in data centers.
- **ST (Straight Tip)** - Bayonet-style connector, used in legacy networks.
- **SC (Subscriber Connector)** - Push-pull connector, widely used in telecom.
- The transceiver type must match on both ends (e.g., short-range to short-range). Mismatched types (short to long range) will not work.