CCNA Wireless

Wireless LAN Topologies

- **Basic Service Set (BSS) aka Cell / BS Area**
  - 802.11 frame is encapsulated into an 802.3 frame for transmission over wired networks
- **Extended Service Set (ESS)**
  - Multiple BSSs connected via a distribution system (DS), allowing broader coverage and seamless roaming
- **Independent Basic Service Set (IBSS)**
  - Also called an ad-hoc network, where wireless devices communicate directly without an access point
- **SSID (Service Set Identifier)**
  - The name of a wireless network used by clients to identify and connect to it
- **Access Points (APs)**
  - Devices that connect wireless clients to the wired network and facilitate communication between BSSs
- **Wireless Channels and Frequency Bands**
  - 2.4 GHz and 5 GHz are common frequency bands; channels must be selected to minimize interference

Types of APs

- **Standalone APs**
  - Operate independently without a central controller; all configuration and management are done locally on the AP (autonomous)
- **Lightweight AP (LWAP)**
  - Managed by a Wireless LAN Controller (WLC); configuration and policies are pushed from the WLC, simplifying management in large deployments
    - **Local Mode (Default):** The AP forwards data through the CAPWAP tunnel to the WLC for centralized management.
    - **FlexConnect Mode:** The AP can locally switch client data at the branch site while still maintaining control communication with the WLC, useful for remote deployments with limited bandwidth.
    - **Converged Mode:** AP handles both wired and wireless bridging locally, providing simplified deployment and improved efficiency in integrated networks.

- **Wireless LAN Controller (WLC)**
    - Centralized device that manages multiple lightweight APs, handles authentication, roaming, and policy enforcement
    - **Control Traffic**
        - Management and signaling messages between APs and WLC, including AP join, configuration updates, and heartbeats
    - **Data Traffic**
        - User-generated traffic (data frames) that may be tunneled to the WLC or switched locally depending on configuration
    - **CAPWAP Tunnel (Control And Provisioning of Wireless Access Points)**
        - A standardized protocol that carries both control and data traffic between the WLC and lightweight APs, enabling centralized management and configuration.

Wi-Fi

- Radio technologies based on IEEE 802.11 standards
- Provides secure, reliable, and fast wireless connectivity
- Wi-Fi networks operate in unlicensed radio bands:
    - 2.4 GHz
    - 5 GHz

802.11 Specifications

- **802.11a:** 5 GHz, up to 54 Mbps
- **802.11b:** 2.4 GHz, up to 11 Mbps
- **802.11g:** 2.4 GHz, up to 54 Mbps
- **802.11n:** 2.4/5 GHz, up to 600 Mbps
- **802.11ac:** 5 GHz, up to 1.3 Gbps
- **802.11ax (Wi-Fi 6):** 2.4/5 GHz, up to 9.6 Gbps

Signal Measurement

- **mW (milliwatts):** Unit of power used to measure the transmit power of a wireless signal.
    - Most accurate
    - Many leading zeros
    - Ex: -60 dBm ≈ 0.000001 W
- **dBm:** Decibels relative to 1 milliwatt; logarithmic measurement of signal strength.
    - Commonly measured from -30 dBm (excellent) to -100 dBm (unusable)
    - +3 dB equals a doubling of signal strength
    - -3 dB equals a halving of signal strength
    - Signal strength ranges and quality description:
        - **-30 dBm:** Very strong, close to AP
        - **-50 dBm:** Excellent signal for most applications
        - **-60 dBm:** Good, reliable for standard usage
        - **-70 dBm:** Fair, some applications may experience latency
        - **-80 dBm:** Weak, not reliable for high-bandwidth applications
        - **-90 dBm:** Very weak, likely unusable
- **RSSI (Received Signal Strength Indicator):** Value reported by the device representing the power level of the received signal, used to assess link quality.
    - Typically 0-60 or 0-255 depending on vendor implementation
    - Indicates quality of the wireless connection

Band Choosing vs Band Steering

- **Band Choosing**
    - Performed by the client device.
    - The device independently selects which frequency band (2.4 GHz or 5 GHz) to connect to based on signal strength, interference, and network conditions.
    - The AP does not force the selection; the client makes the decision.
- **Band Steering**
    - Performed by the access point (AP).
    - The AP actively influences or directs dual-band capable clients to connect to the higher-performance or less congested band (usually 5 GHz) instead of 2.4 GHz.
    - Improves overall network efficiency by balancing client distribution across bands.

Key Difference:

- Band Choosing = client-driven decision.
- Band Steering = AP-driven guidance.

Wireless Security Protocols

- **WPA (Wi-Fi Protected Access):** Introduced as an improvement over WEP, it uses TKIP (Temporal Key Integrity Protocol) for stronger encryption and dynamic key generation. Considered insecure today.
    - Uses a **four-way handshake** to establish keys.
- **WPA2:** Successor to WPA, it introduced AES (Advanced Encryption Standard) with CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) for stronger security. Widely used but vulnerable to brute-force attacks when using weak passwords.
    - Uses a **four-way handshake** to establish keys.
- **WPA3:** Latest version, uses SAE (Simultaneous Authentication of Equals) to provide stronger protection against password-guessing attacks and individualized encryption for open networks.
    - Supports 128-bit and 192-bit encryption keys.
    - Uses **ECDH (Elliptic Curve Diffie-Hellman)** and **ECDSA (Elliptic Curve Digital Signature Algorithm)** for secure key exchange and authentication.
    - Relies on **Perfect Forward Secrecy (PFS)** so session keys cannot be reused if long-term keys are compromised.
    - **OWE (Opportunistic Wireless Encryption):** Provides encryption for open Wi-Fi networks by automatically establishing encrypted sessions without requiring a pre-shared key or password.

Authentication Methods

- **Enterprise:** Uses a RADIUS or TACACS+ server with 802.1X for centralized authentication and policy enforcement.
    - Can integrate with LDAP or Active Directory.
- **Personal:** Uses a Pre-Shared Key (PSK) for WPA and WPA2; WPA3-Personal uses SAE instead of PSK for more secure authentication.

Protected Management Frame (PMF)

- Management frames in 802.11 were originally unauthenticated and unencrypted, making them vulnerable to attacks like deauthentication or disassociation floods.
- **802.11w (Management Frame Protection):** Introduced to protect certain management frames (e.g., deauthentication, disassociation, action frames) by encrypting them, preventing spoofing and denial-of-service attacks.
- Required in WPA3, optional in WPA2.

Fast Transition (802.11r)

- A roaming standard that reduces latency when a wireless client moves between access points.
- Allows clients to perform part of the authentication process **before** moving to the new AP.
- Uses **Fast BSS Transition (FT)** where keys are derived and shared in advance, enabling faster handoffs.
- Essential for real-time applications like VoIP and video conferencing where seamless roaming is critical.

AP and WLC Management Access Connections

- **Console:** Terminal connection for direct local management.
- **Telnet (Do not use):** Terminal connection, insecure (unencrypted).
- **SSH:** Terminal connection, secure (encrypted).
- **HTTP/HTTPS:** GUI-based management (HTTPS recommended).
- **TACACS+/RADIUS:** Centralized authentication servers that can integrate with LDAP/Active Directory.

Wireless "Interfaces" on WLC

- **Management Interface:** Used for in-band management, system communication, and to terminate CAPWAP tunnels with lightweight APs.
- **AP-Manager Interface:** Handles Layer 3 communications and management traffic between the WLC and APs (used primarily in older WLC platforms, often consolidated with management in modern systems).
- **Virtual Interface:** Provides a consistent IP address for mobility management, DHCP relay, guest web authentication, and other WLC services. It is not tied to a physical port.
- **Service Port:** A dedicated physical port on the WLC used for out-of-band management, system recovery, and initial setup. It does not support CAPWAP.
- **Dynamic Interface:** Maps WLANs (SSIDs) to VLANs on the wired network. Each WLAN can be assigned to a specific dynamic interface for traffic segmentation.

Wireless ACLs

- **CPU ACL:** Controls traffic destined to or from the WLC's CPU. Used to restrict management access (e.g., SSH, SNMP, HTTPS) or limit control plane traffic.
- **Interface ACL:** Applied to specific dynamic interfaces, controlling data traffic between wireless clients and the wired network (similar to traditional router ACLs).

Automation and Programmability

What is network automation and programmability

- Feature to make your network more:
    - Flexible
    - Agile

Automation

- Permits you to embrace new technology quickly
- Permits you to make updates, upgrades, and changes quickly
- Reduces operational expenses/costs
- Reduces errors and builds resiliency

Programmability

- **CRUD** – The four basic functions of persistent storage or APIs:
    - **Create** – Adds new data or resources into the system.
    - **Read** – Retrieves or views existing data.
    - **Update** – Modifies or changes existing data.
    - **Delete** – Removes existing data.

REST-based APIs

- Application Programming Interfaces that follow REST (Representational State Transfer) principles.
- They use standard HTTP methods for communication between systems.
- Stateless: Each request from client to server must contain all the information needed.
- Widely used in network automation for interoperability and integration.
- Using HTTP verbs such as:
    - **GET** – Retrieves data from a resource (read-only).
    - **POST** – Submits new data to a resource (create).
    - **PUT** – Updates or replaces an existing resource.
    - **DELETE** – Removes an existing resource.

HTTP(s) Messages

- **Start-Line:** The first line of an HTTP request or response. In a request, it includes the method (GET, POST, etc.), the target resource (path/URL), and the HTTP version. In a response, it contains the HTTP version, status code, and status message.

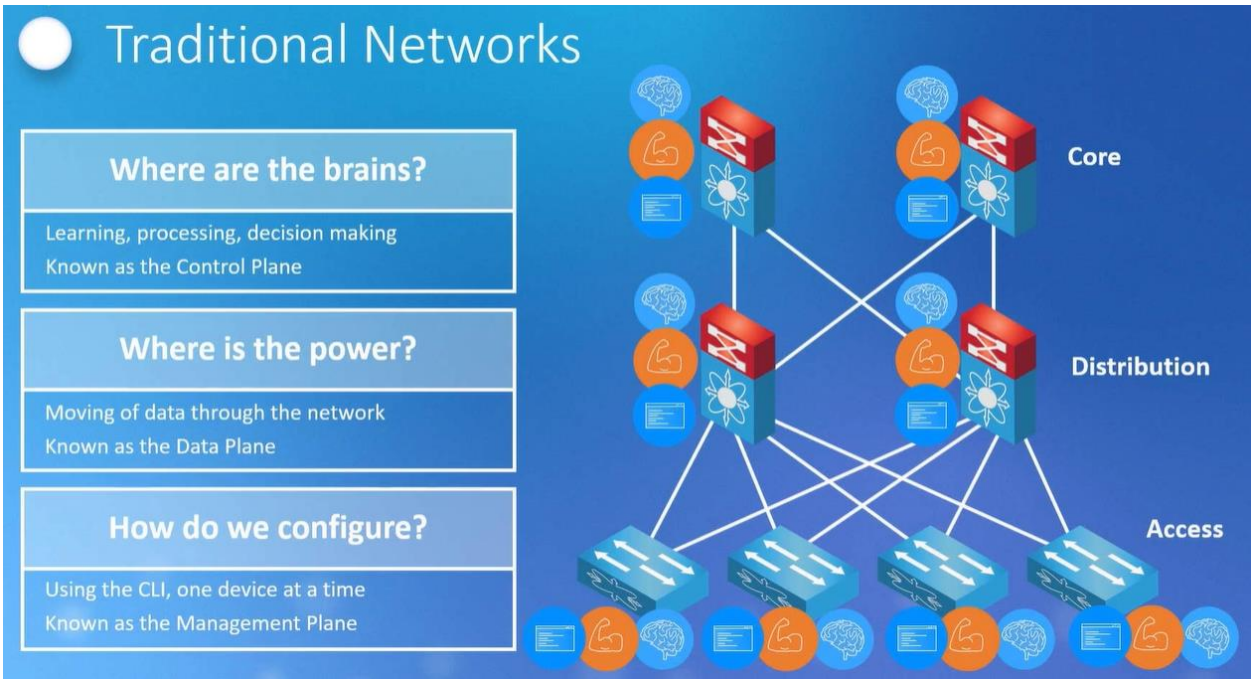
- **Headers:** Key-value pairs that provide additional information about the request or response, such as content type, content length, host, and authentication details.
    - **Content-Type:** Tells the server or client the format of the data being sent (e.g., `application/json`, `text/html`).
    - **Accept:** Informs the server what content types the client can process (e.g., `application/json`).
    - **Authorization:** Carries credentials (such as tokens, API keys, or Basic Auth) for authenticating the client to the server.
    - **Date:** Shows the date and time at which the message was sent, useful for logging and caching.
- **Empty-Line:** A blank line that separates the headers from the body. It indicates the end of the header section.
- **Body:** The payload of the message. In requests, it may include data being sent to the server (e.g., JSON). In responses, it often contains the resource or data being returned.

REST API Security

- **None:** No security applied; communications are unencrypted and unauthenticated. Not recommended.
- **HTTPS:** Uses SSL/TLS to encrypt communications between client and server, preventing eavesdropping and tampering.
- **Token:** The client provides a unique token (often in the Authorization header) to authenticate API requests. Tokens are more secure than static credentials.
- **OAuth:** An open standard for access delegation, often used for granting applications limited access to user resources without exposing credentials. Considered the best option for modern APIs.

Data Encoding

- **JSON (JavaScript Object Notation):** A lightweight data-interchange format that is easy for humans to read and write and easy for machines to parse. Commonly used in REST APIs.
    - **Key-Value Pair:** A data representation format where each field (key) is associated with a specific value (e.g., `"username": "admin"`).
- **XML (eXtensible Markup Language):** A markup language that defines rules for encoding documents in a format both human-readable and machine-readable. Older than JSON but still used in some systems.



Control Plane vs Data Plane

- **Control Plane:**
  - Responsible for making decisions about where traffic is sent.
  - Handles routing protocols, building routing tables, and maintaining neighbor relationships.
  - Examples: OSPF calculating best paths, BGP exchanging routes.
- **Data Plane (Forwarding Plane):**
  - Responsible for the actual movement of packets through the device.
  - Uses the information from the control plane (routing table, forwarding table) to forward packets.
  - Operates at high speed in hardware/ASICs for efficiency.

Key Difference:

- Control Plane = decision-making (brains).
- Data Plane = forwarding (muscle).

Centralized Control Plane - Cisco DNA Center

- **Centralized Control Plane:**
  - Instead of each device running its own control plane independently, decision-making is centralized.

    - Provides a single point for policy, automation, and assurance.
    - Simplifies management, reduces configuration errors, and enables advanced analytics.
- **Cisco DNA Center:**
    - Cisco's intent-based networking solution that provides centralized automation and assurance.
    - Offers a GUI-based management platform for provisioning, monitoring, and troubleshooting.
    - Uses APIs for programmability and integration with other systems.
    - Supports features like software-defined access (SD-Access), segmentation, and policy-based automation.
        - Principles of DNA: Policy, Security, Automation, Analytics, Open Platform, Cloud, Physical and Virtual Infrastructure
        - Benefits of DNA: IT agility and scale, Reduced risk, Improved user experience, investment protection.

Key Benefits:

- Simplified management.
- Faster deployment and updates.
- Enhanced visibility and assurance.
- Integration with automation and programmability tools.

Southbound API

- **Southbound API:**
    - Interface between the controller and the underlying network devices (switches, routers, firewalls).
    - Used by the controller to communicate instructions and policies to devices.
    - Common protocols: **OpenFlow, NETCONF, RESTCONF, gNMI**.
    - Provides detailed device-level control, including configuration, state monitoring, and enforcement of network policies.
    - Ensures consistency between the network's intended design and actual operational state.
        - Southbound = controller ↔ devices: Focused on actual device configuration, enforcement of control plane decisions, and direct interaction with network hardware.

Types of Southbound APIs:

- **NETCONF:** Network configuration protocol using XML to manage device configuration and state.
- **RESTCONF:** RESTful API for managing network devices, supporting JSON or XML payloads for configuration and monitoring.

Programmable Networks

- Adjust the network based on application needs.
- Deploy applications in days instead of months.

Northbound API

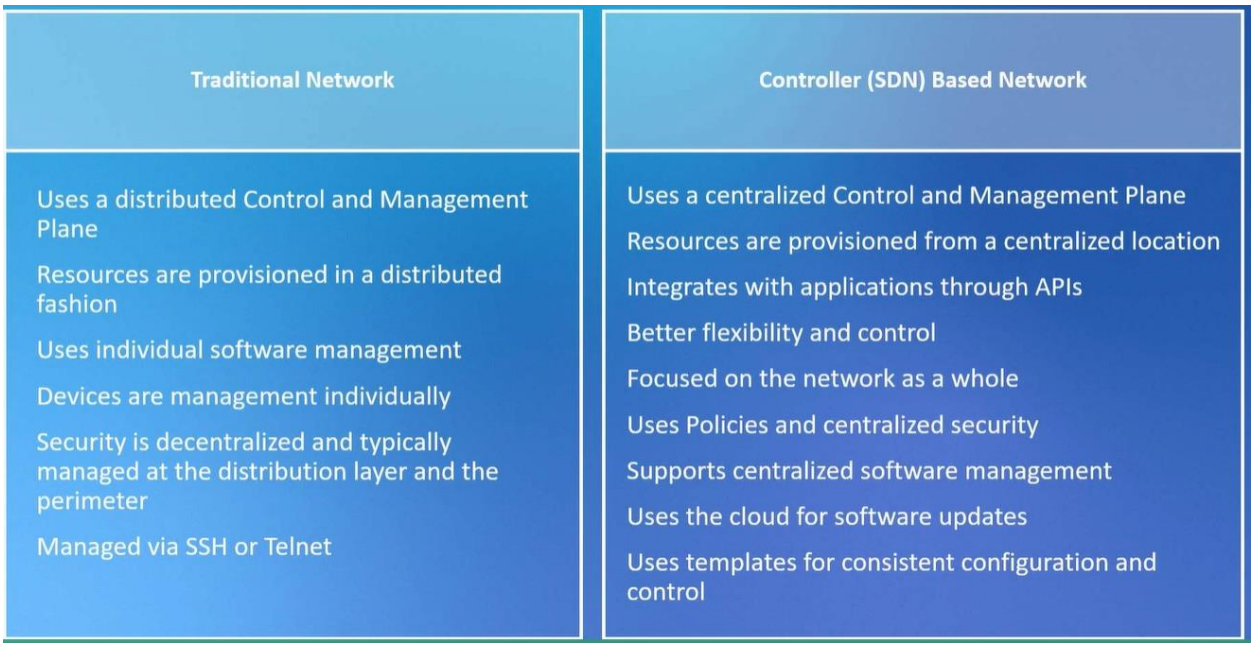
- **Northbound API:**
    - Interface between the controller (such as Cisco DNA Center or SDN controller) and higher-level applications.
    - Used by applications, orchestration platforms, or business systems to request network services and data from the controller.
    - Example: An orchestration system requesting the controller to deploy a new VLAN, QoS policy, or security rule.
    - Provides a simplified, abstracted view of the network for applications, hiding underlying device complexity.
    - Enables automation, integration with IT service management (ITSM) tools, analytics, and business policy enforcement.
        - Northbound = controller ↔ applications: Focused on abstraction, orchestration, and enabling higher-level automation for IT and business processes.

Types of Northbound APIs:

- REST API
- XML
- JSON
- Others

Intent-Based Networking (IBN):

- An approach to networking where the desired business outcomes (intent) are defined and the network automatically implements, monitors, and adapts to achieve those outcomes.
- Uses automation, AI/ML analytics, and policy-based management to align network behavior with business intent.
- Reduces manual configuration, improves consistency, and enables faster response to business needs.



Configuration Management Tools

- **Ansible:**
  - An open-source automation tool that allows you to configure and manage network devices, servers, and cloud infrastructure.
  - Uses YAML-based playbooks to define configurations, making it agentless and simple to deploy.
  - Supports idempotent operations, ensuring changes are applied consistently without causing duplication or errors.
- **Terraform:**
  - An open-source infrastructure-as-code (IaC) tool that allows you to provision and manage cloud and on-premises resources declaratively.
  - Uses configuration files to define the desired state of infrastructure and automatically creates, updates, or deletes resources to match that state.
  - Supports multiple providers (AWS, Azure, GCP, VMware, etc.) for consistent multi-cloud management.
- Automate Network and Cloud Environments
- Increase Efficiency and Reduce Manual Errors

Artificial Intelligence for Network Operations (AIOps)

- Uses algorithms and models that mimic human intelligence to perform tasks such as:
    - Analyzing network data
    - Identifying patterns
    - Predicting issues
    - Automating decision-making

Generative AI

- AI that can create new content or solutions based on existing data and patterns.
- Examples include generating configuration templates, scripts, network diagrams, or documentation automatically.
- Useful for speeding up routine network tasks and providing recommendations.

Predictive AI

- AI that forecasts future network events or issues based on historical data and trends.
- Examples include predicting device failures, bandwidth congestion, or security threats before they occur.
- Enables proactive maintenance and reduces downtime by allowing operators to take preventive action.

Machine Learning (ML)

- A subset of AI that enables systems to learn from data, identify patterns, and make decisions with minimal human intervention.
- Used for network traffic analysis, anomaly detection, predictive maintenance, and optimizing network performance.

Types of ML

- **Supervised Learning:**
  - ML model is trained on labeled data, where the correct output is provided.
  - The model learns to map inputs to outputs and can predict outcomes for new, unseen data.
  - Example: Classifying emails as spam or not spam based on previous labeled examples.
- **Unsupervised Learning:**
  - ML model is trained on unlabeled data, and it identifies hidden patterns or structures within the data.
  - Often used for clustering, anomaly detection, and data segmentation.
  - Example: Grouping similar network devices based on usage patterns without predefined categories.
- **Reinforcement Learning:**
  - ML model learns by interacting with an environment and receiving feedback in the form of rewards or penalties.
  - Useful for optimizing decision-making processes over time.
  - Example: Dynamically adjusting network routing policies to maximize throughput and minimize congestion.