Presented by Olaniyi Babarinde

NETWORK AUTOMATION PLUS CCNA

AGENDA

1. 1.1.a Routers
2. 1.1.b Layer 2 and Layer 3 switches
3. 1.1.c Next-generation firewalls and IPS
4. 1.1.d Access points
5. 1.1.e Controllers (Cisco DNA Center and WLC)
6. 1.1.f Endpoints
7. 1.1.g Servers
8. 1.1.h PoE
9. Q & A

INTRODUCTION

Questions from Class Two.

“Where does your loyalty lie?"

– FIND THE ANSWERS IN YOU CALENDA.

ROUTERS!

A router’s primary purpose is **Path Determination**. It maintains a **Routing Table**, which is a map of the entire inter-network.

Functions of a Router.

- **Logic:** When a packet arrives, the router looks at the **Destination IP**. It searches its table for the longest prefix match to find the next "hop."
- **Encapsulation:** Routers strip away the Layer 2 header (Ethernet) of an incoming packet, examine the Layer 3 header (IP), and then re-encapsulate it with a new Layer 2 header for the next link.
- **Broadcast Control:** Routers do not forward broadcasts (Layer 2 noise). This prevents network congestion by keeping local traffic local.

ROUTERS! *CONTINUES*

- **Forwarding packets:** This is the primary function, where a router moves data packets between networks, using information found in the packet header [1].
- **Routing (Path Determination):** A router analyzes the destination IP address of incoming packets, consults its routing table to determine the best path to that destination network, and forwards the packets along that path [1]. This is different from forwarding, which is the actual movement, while routing is the decision-making process.
- **Interconnecting Networks:** Routers connect different network types, such as connecting a local area network (LAN) to a wide area network (WAN) [1].
- **Packet Filtering/Security:** Using Access Control Lists (ACLs), a router can filter packets based on source or destination IP addresses, port numbers, and other criteria. This enforces network security policies and prevents unauthorized traffic [1].
- **Providing Connectivity (Default Gateway):** Devices on a local network use the router's interface IP address as their default gateway to send traffic to devices outside of their local network [1].
- **Network Address Translation (NAT) / Port Address Translation (PAT):** Routers often perform NAT or PAT, translating private IP addresses used within a local network to a single or a pool of public IP addresses, conserving public IP address space and adding a layer of security [1].
- **Quality of Service (QoS):** Routers can prioritize certain types of traffic (like voice or video) over others to ensure reliable performance for critical applications

LAYER 2 AND LAYER 3 SWITCHES

While both provide connectivity, their "intelligence" levels differ significantly.

•**Layer 2 Switches (MAC-Based):** * **Function:** They use an **ASIC (Application-Specific Integrated Circuit)** to build a CAM (Content Addressable Memory) table. This table maps MAC addresses to physical ports.

- •**Micro-segmentation:** Each port is its own **collision domain**, meaning two devices can talk at the same time without interfering.

•**Layer 3 Switches (IP-Aware):** * **Function:** Also known as Multilayer Switches. They perform "hardware-based routing."

- •**Inter-VLAN Routing:** In a large office, you might have a "Sales" VLAN and an "HR" VLAN. A Layer 3 switch allows these two groups to communicate at lightning speed without sending the data all the way up to a main router.

NEXT-GENERATION FIREWALLS (NGFW) AND IPS

To truly understand **Next-Generation Firewalls (NGFW)** and **Intrusion Prevention Systems (IPS)**, we have to look past the "marketing" and examine the actual data processing that happens inside these appliances.

Think of a traditional firewall like a bouncer at a club who only checks IDs (IP addresses and Ports). An **NGFW/IPS combo** is more like a specialized security team that not only checks IDs but also searches bags, listens to conversations, and knows every guest's reputation.

An NGFW is defined by its ability to perform **Deep Packet Inspection (DPI)** at Layer 7 (the Application Layer).

- **Deep Packet Inspection (DPI):** The firewall reassembles data packets into their original application format to see what they are actually doing.
- **Granular Control:** You can create a policy that says: *"Allow employees to view LinkedIn, but block them from using LinkedIn Messaging."*

NEXT-GENERATION FIREWALLS (NGFW) AND IPS *CONTINUES*

1. Application Awareness (The "What")

Traditional firewalls see traffic as **Port 443 (HTTPS)**. An NGFW sees that the traffic is specifically **Facebook**, and further, it can distinguish between "Facebook Post" and "Facebook Messenger."

- **Deep Packet Inspection (DPI):** The firewall reassembles data packets into their original application format to see what they are actually doing.
- **Granular Control:** You can create a policy that says: *"Allow employees to view LinkedIn, but block them from using LinkedIn Messaging."*

NEXT-GENERATION FIREWALLS (NGFW) AND IPS
CONTINUES

2. User Identification (The "Who")

Instead of writing rules for IP address `10.1.5.50`, you write rules for "John Doe" or the "Marketing Group."

- **Directory Integration:** The NGFW links with systems like **Active Directory (AD)**.
- **Mobility:** If John Doe moves from his desk (wired) to the cafeteria (Wi-Fi), his IP address changes, but the NGFW follows his identity, ensuring his security profile remains active regardless of his location.

NEXT-GENERATION FIREWALLS (NGFW) AND IPS
CONTINUES

2. User Identification (The "Who")

- **Directory Integration:** The NGFW links with systems like **Active Directory (AD)**.
- **Mobility:** If John Doe moves from his desk (wired) to the cafeteria (Wi-Fi), his IP address changes, but the NGFW follows his identity, ensuring his security profile remains active regardless of his location.

NEXT-GENERATION FIREWALLS (NGFW) AND IPS
CONTINUES

3. SSL/TLS Decryption

Over 90% of web traffic is encrypted. Hackers hide malware inside this encrypted "tunnel."

- **The Function:** The NGFW acts as a "man-in-the-middle." It decrypts the traffic, scans it for threats, and then re-encrypts it before sending it to the user. Without this, a firewall is essentially blind to most modern threats.

INTRUSION PREVENTION SYSTEM (IPS)

While the Firewall decides *who* and *what* can enter, the IPS focuses on **malicious intent** within that allowed traffic.

1. Signature-Based Detection

This is the most common method. The IPS has a database of tens of thousands of "signatures" – digital fingerprints of known exploits.

- **Example:** If a packet contains a specific string of code known to trigger a vulnerability in a Windows Print Spooler, the IPS recognizes that pattern and drops the packet instantly.

2. Anomaly-Based Detection

This looks for "weird" behavior rather than a specific fingerprint.

- **Function:** It builds a "baseline" of what your network looks like on a normal Tuesday. If suddenly a computer starts sending 5,000 small packets per second to a database (a sign of a scanning tool or DDoS attack), the IPS flags it as an anomaly and blocks it.

INTRUSION PREVENTION SYSTEM (IPS)

3. Protocol Analysis

The IPS ensures that traffic is "well-formed."

- **Example:** If a device is sending HTTP traffic, but the data structure violates the official rules of the HTTP protocol, the IPS assumes it’s a "buffer overflow" attack attempt and stops it.

INTRUSION PREVENTION SYSTEM (IPS)

NGFW vs. IPS: The Unified Reality

In the past, these were two separate boxes. Today, the IPS is almost always a **software module** running inside the NGFW.

Feature	NGFW Role	IPS Role
Visibility	Identifies the Application (e.g., Gmail).	Identifies the Threat (e.g., Malware in the attachment).
Logic	Policy-based (Allow/Deny).	Signature/Behavior-based (Detect/Stop).
Layer	Layers 3 through 7.	Deep Layer 7 (Payload).
Action	Controls access to resources.	Prevents exploitation of vulnerabilities.

INTRUSION PREVENTION SYSTEM (IPS)

Why use both?

If you only have a firewall, a user can "legally" connect to a website that then sends a virus through the "allowed" port. If you only have an IPS, you have no way to say "Marketing can use YouTube but Finance cannot." Together, they create a **Stateful, Context-Aware** security barrier.

ACCESS POINTS (APS)

In an enterprise, APs are not "Routers." They act as a wireless-to-wired bridge.

- **Function:** They convert **802.11 (Wireless)** frames into **802.3 (Ethernet)** frames.
- **SSID Mapping:** An AP can broadcast multiple SSIDs (e.g., "Guest" and "Corporate"). It tags the traffic from these SSIDs with different **VLAN IDs** so the switch knows how to treat the data.

CONTROLLERS (WLC)

The Wireless LAN Controller (WLC) provides a centralized management plane.

- **CAPWAP Tunneling:** APs "tunnel" their traffic back to the controller using a protocol called CAPWAP. This allows a user to walk from one end of a building to the other (Roaming) without losing their Wi-Fi connection, as the controller manages the handoff between APs.
- **Radio Resource Management (RRM):** If one AP fails, the controller tells the surrounding APs to increase their signal strength to "heal" the coverage hole.

ENDPOINTS

Endpoints are any device that marks the end of a communication path.

- **Function:** Endpoints are the source and destination of the **Data Plane**.
- **Diversity:** This includes "Headless" devices like IoT sensors or security cameras, which often require specialized network segments (VLANs) because they lack the robust security software found on PCs.

SERVERS

Servers are high-performance endpoints designed for 24/7 availability.

- **Virtualization:** In modern networks, physical servers rarely run just one "role." Using hypervisors (like VMware), a single physical server might host dozens of **Virtual Machines (VMs)**, each acting as a separate server (Mail, File, Web, etc.).
- **Placement:** Servers are typically placed in a **DMZ (Demilitarized Zone)** or a dedicated Data Center segment behind a firewall to protect the sensitive data they hold.

THE NETWORK HIERARCHY

To see how these all fit together, imagine this flow:

- **Endpoint** (Laptop) connects to an **Access Point**.
- **Access Point** is managed by a **Controller** and plugged into a **Layer 2 Switch**.
- The **Layer 2 Switch** connects to a **Layer 3 Switch** for internal routing.
- Traffic destined for the internet goes through a **Next-Gen Firewall**.
- The **Router** finally sends that data out to the ISP.

THE NETWORK TOPOLOGY ARCHITECTURES

Here is a breakdown of the characteristic topologies and architectures used in modern networking.

THE NETWORK TOPOLOGY ARCHITECTURES

1.2.a Two-Tier (Collapsed Core)

The two-tier architecture is designed for small to medium-sized organizations where a full three-tier setup would be too expensive or complex.

- **Structure:** It merges the **Core** and **Distribution** layers into a single "Collapsed Core" layer.
- **Characteristics:**
  - **Cost-Effective:** Requires fewer high-end switches.
  - **Simplified Management:** Fewer layers to configure and troubleshoot.
  - **Scalability:** Limited compared to three-tier; as the network grows, the single core can become a bottleneck.
- **Ideal for:** A single building or a small campus.

THREE-TIER (HIERARCHICAL)

This is the standard "proven" model for large enterprise campus networks. It separates functions into three distinct layers to ensure predictable performance.

Layers:

- **Access Layer:** Where end-users connect (phones, PCs, APs). Focuses on port security and VLAN assignment.

- **Distribution Layer:** The "policy" layer. It aggregates access switches, performs routing between VLANs, and implements security filters.

THREE-TIER (HIERARCHICAL)

This is the standard "proven" model for large enterprise campus networks. It separates functions into three distinct layers to ensure predictable performance.

Layers:

- **Core Layer:** The "backbone." Its only job is to switch traffic as fast as possible between distribution blocks. It does not perform complex packet filtering.
- **Characteristics:** High availability, modularity (you can add a new building just by adding a new distribution block), and clear fault isolation.

SPINE-LEAF

While Three-Tier is for campuses (users), **Spine-Leaf** is the architecture for modern **Data Centers**.

Structure: A two-layer topology where every "Leaf" switch (access) is connected to every "Spine" switch (aggregation).

Characteristics:

- **East-West Traffic:** Optimized for server-to-server communication (common in cloud and virtualization).

SPINE-LEAF

Characteristics:

- **East-West Traffic:** Optimized for server-to-server communication (common in cloud and virtualization).

•**Predictable Latency:** Every device is exactly two "hops" away from any other device.

•**Scalability:** To add more bandwidth, simply add another Spine switch. To add more server ports, add another Leaf.

- **No STP:** Typically uses **ECMP (Equal-Cost Multi-Path)** routing instead of Spanning Tree, allowing all physical links to be active simultaneously.

WAN (WIDE AREA NETWORK)

A WAN connects geographically dispersed LANs (e.g., a New York office to a London office).

- **Characteristics:**
  - **High Latency/Lower Speed:** Generally slower and more expensive than local connections because it uses leased lines or public infrastructure.
  - **Technologies:** Uses MPLS, SD-WAN, or Site-to-Site VPNs.
  - **Boundary:** Usually involves a "Service Provider" (ISP) acting as the middleman.

SMALL OFFICE/HOME OFFICE (SOHO)

A SOHO network is the simplest architecture, typically found in homes or tiny businesses.

- **Characteristics:**
  - **Integrated Devices:** Usually uses a single "all-in-one" device that acts as a Router, Switch, Wireless Access Point, and Firewall.
  - **Limited Capacity:** Designed for 1–10 users.
  - **Consumer Grade:** Lacks the advanced redundancy (dual power supplies) of enterprise gear.

ON-PREMISES VS. CLOUD

This describes **where** the network resources and data reside.

Characteristic	On-Premises	Cloud
Control	Full ownership of hardware and security.	Shared responsibility with the provider (AWS/Azure).
Cost	High **CapEx** (upfront hardware costs).	Monthly **OpEx** (pay-as-you-go).
Scalability	Slow (must buy and rack new servers).	Instant (click a button to add resources).
Maintenance	You fix the hardware and cooling.	The provider handles all physical infrastructure.

SUMMARY TABLE OF TOPOLOGIES

This describes **where** the network resources and data reside.

Architecture	Primary Use Case	Key Benefit
Two-Tier	Medium Office	Cost savings / Simplicity.
Three-Tier	Large Campus	Modularity and Stability.
Spine-Leaf	Data Center	Low latency for server traffic.
SOHO	Home/Small Office	Ease of use / All-in-one.

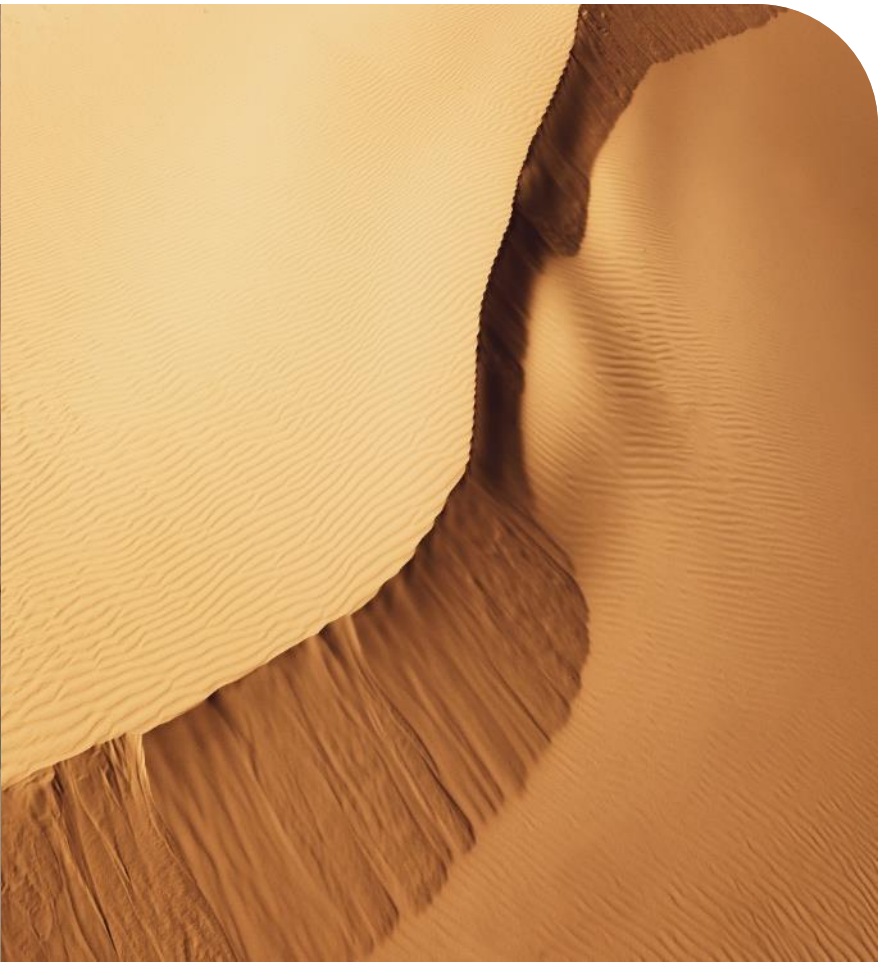
35%

OF AN AUDIENCE’S RETENTION RATE IS ATTRIBUTED TO THE VISUALS USED

DELIVERING WITH IMPACT

Keeping your audience engaged through effective techniques

EFFECTIVE DELIVERY TECHNIQUES



Your delivery can make or break your presentation. Focus on the following techniques.

Voice modulation

Vary pitch, tone, and volume to emphasize key points. Pause strategically as silence builds anticipation.

Body language

Maintain open gestures and avoid crossing your arms. Move naturally. Step forward when making a strong point.

Non-verbal cues

Look for cues (like nodding and note-taking) that show that your audience is engaged.

Additional tips

Be confident, rehearse aloud, and show enthusiasm.

Meaningful eye contact, purposeful gestures, and good posture can enhance your message and make it more memorable.

CONCLUSION

Start with a hook and a clear purpose. Engage your audience using eye contact, storytelling, and questions. Design slides that enhance your message, not distract. And deliver with confidence.

Q & A

Use this portion of your presentation to answer audience questions.