CompTIA Network+ (N10-009) Day 6

Interpreting Complex Prefixes

Classless Inter-Domain Routing Example (CIDR) –

215.99.44.22 is a Class C address, which normally has a /24 mask. CIDR is used on the Internet's BGP routing table to group many networks into larger networks. CIDR is a form of **route summarization**.

215.99.44.0/24

215.99.45.0/24

215.99.46.0/24

215.99.47.0/24

They can be summarized and advertised as:

215.99.44.0/22

VLSM and FLSM

VLSM –VLSM allows a network to be subnetted into subnets of different sizes, using different subnet masks within the same address space. This helps avoid wasting IP addresses.

Example:
You have `192.168.1.0/24`.

- Subnet 1: Needs 50 hosts → Use `/26` (62 usable addresses) → `192.168.1.0/26`
- Subnet 2: Needs 10 hosts → Use `/28` (14 usable addresses) → `192.168.1.64/28`
- Subnet 3: Needs 2 hosts → Use `/30` (2 usable addresses) → `192.168.1.80/30`

- *Example:* Assigning a /28 mask to a small subnet with few hosts and a /24 mask to a larger subnet within the same network.

FLSM –FLSM uses the same subnet mask for all subnets in the network, meaning each subnet has the same number of usable host addresses.
Example:
If `192.168.1.0/24` is divided into `/26` subnets, every subnet has exactly 62 usable host addres

IPv6 Address Structure

- **128 bits long**
- **32 hexadecimal digits** required
- Groups of 4 hex digits are separated by colons (`:`)
  These are called **quartets**.
- Up to **three leading zeros** in any quartet can be dropped.
- One or more quartets containing all zeros may be represented by two colons `::` — **can only be used once in an address**.
- Read from left to right.

Examples:

- `::1` is the IPv6 loopback address.

IPv6 Global Unicast and Anycast Addressing

- **Global Unicast** = Public / Internet / Routable
- Starts with `2000::/3` and assigned by IANA
- Range: `2000::/3` – `3FFF::/3`

Note: Global Unicast addresses can also be used as IPv6 **Anycast** addresses.
Anycast communication is "one-to-nearest" communication.

IPv6 Address Breakdown Example:
(Each quartet may represent site prefix, subnet prefix, and interface ID depending on prefix length and allocation)

IPv6 Unique Local Addressing

- Private / Routable inside your network (IPv6 version of IPv4 RFC 1918 addresses)
- Usable by many organizations at the same time
- Prefix: `FC00::/7`
  - `FC00::/8` (rarely used)
  - `FD00::/8` (commonly used)

IPv6 Link-Local Addressing

- Private / Non-Routable
- Prefix: `FE80::/10`
- Self-assigned or manually assigned
- Every IPv6 interface **must** have one
- Only **one** can exist on an interface
- Used for many low-level protocols
- Used as the **next-hop address** for IPv6 routing

IPv6 Multicast Addresses

- Begin with `FF`
- Always a **destination address**
- Used to send traffic to multiple systems on a LAN simultaneously

---

EUI-64 Addresses

- Uses the MAC address to create a unique host ID
- Inserts `FFFE` in the middle of the 48-bit MAC address
- **Flip the 7th bit from the left**
- Produces the **64-bit interface identifier** in an IPv6 address

---

IPv6 Router Discovery

Router Solicitation:

- Src = Link-Local Address (`FE80::/10`)
- Dst = All-routers multicast (`FF02::2`)

Router Advertisement:

- Src = Link-Local Address (`FE80::/10`)
- Dst = All-nodes multicast (`FF02::1`)
- Includes options such as subnet prefix, lifetime, and autoconfig settings

---

IPv6 Neighbor Discovery Protocol (NDP)

Neighbor Solicitation:

- Src = A
- Dst = Solicited-node multicast of B
- Data = Link address of A
- Query: "What is your link-layer address?"

Neighbor Advertisement:

- Src = A
- Dst = B
- Data = Link address of B

Stateless Address Autoconfiguration (SLAAC)

- Allows IPv6 hosts to configure themselves automatically without DHCPv6

Router advertisements tell clients whether to use SLAAC, DHCPv6, or both

Definition:
An IPv6 method where hosts automatically configure their own IP addresses and default gateway using information from router advertisements (RAs), without needing a DHCPv6 server.
Example:

- Router sends RA with prefix `2001:db8:abcd:1::/64`
- Host uses EUI-64 or random interface ID to create `2001:db8:abcd:1:abcd:ef12:3456:789a`
- Host sets default gateway to the router's link-local address.

DHCPv6 (SARR)

1. **Solicit** (multicast)
2. **Advertise** (unicast)
3. **Request** (multicast)
4. **Reply** (unicast)

AAAA Records

- DNS records that map a hostname to an IPv6 address

IPv6 Tunneling Mechanisms

6to4:

- Starts with `2002::`
- Encodes the IPv4 address in the second quartet

Teredo:

- Encapsulates IPv6 packets in IPv4 UDP headers
- Allows IPv4 hosts to communicate with IPv6 systems

NAT64:

- Allows IPv6-only hosts to communicate with IPv4 servers
- **DNS64 role:** Synthesizes IPv6 AAAA records from IPv4 A records when necessary
- NAT64 gateway translates IPv6 packets to IPv4 packets and vice versa

Chapter 10: Security Services

Security Infrastructure Systems

Firewall Types

- **Network Firewalls** – Guard against unwanted traffic between network boundaries.
- **Host Firewalls** – Provide additional protection on an individual host by limiting inbound/outbound traffic.

Firewall Generations

- **Stateless Firewalls**
  - Filter based on IP addresses and TCP/UDP ports (e.g., ACLs).
- **Stateful Firewalls**
  - Track and filter traffic based on connection state.
- **Next-Generation Firewalls (NGFW)**
  - Combine stateful filtering with application-layer inspection, IPS/IDS, and anti-malware features.

Firewall Zones – Screened Subnets / DMZ

- Internet = **Untrusted Zone**
- Internal network = **Trusted Zone**
- **DMZ (Demilitarized Zone)** – Isolated subnet for public-facing services.
    - Should not initiate traffic to the internal network.
    - Common DMZ services: web servers, FTP servers.

Firewall Pairs

- Deployed as **High Availability (HA) pairs**:
    - **Active-Standby** – One firewall active, the other on standby.
    - **Active-Active** – Both firewalls process traffic simultaneously.
- Can increase throughput and decrease latency.

Working with Firewall Filters

Packet Filters – Access Control Lists (ACLs)

- Filter by: Source IP, Destination IP, TCP/UDP ports.

URL Filters

- Block access to specific URLs (e.g., `www.facebook.com`).

Content Filters

- Block based on content categories (e.g., gambling, social media).

ACL Logic:

- **Top-down processing** – First match is applied immediately.
- **Implicit deny any** – Any unmatched traffic is denied.

Traffic Mirroring and Packet Capture

- **Traffic Mirroring** – Duplicating network traffic for inspection.
- **Port Mirroring / SPAN** – Copies traffic from one/more ports to a monitoring port.
- **Protocol Analyzers:**
  - Wireshark (GUI)
  - tcpdump (CLI)
- **TAP** – Physical device that passes all network traffic through while duplicating it for monitoring (adds latency vs SPAN).

Promiscuous Mode:

- NIC captures **all traffic** it sees, not just frames addressed to it.

Intrusion Detection & Prevention Systems (IDS/IPS)

- **Signature-Based Detection** – Looks for known attack patterns.
  - *False positives* – Benign traffic triggers an alert.
  - *False negatives* – Malicious traffic not detected.

Intrusion Prevention System (IPS)

- **Inline** with network traffic.
- Can block or allow traffic based on detected threats.

Intrusion Detection System (IDS)

- Can be **inline or out-of-band** (SPAN/TAP).
- Alerts/logs suspicious activity but does not block traffic.
- Does not add latency when out-of-band.

Security Technologies

Honeypot – Single decoy system to attract attackers.
Honeynet – Network of honeypots to collect more extensive attack data.

Network Access Control (NAC) and BYOD

- Validates devices before allowing network access (OS version, AV status, patches).
- **Guest network** – Internet-only access.
- **Quarantine network** – Isolated network for non-compliant systems.

Jump Boxes

- Hardened systems used as controlled access points to secure environments.
- Accessed before reaching internal servers.

Proxy Server

- Forwards requests on behalf of clients.
- Can filter, cache, and log activity.
- Adds a layer of security for web traffic.

Load Balancers & Virtual IP (VIP)

- Clients connect to a VIP instead of a real server IP.
- Balances load across multiple servers.

Network Address Translation (NAT)

PAT (Port Address Translation)

- Many-to-one mapping.
- Used for inside-to-outside internet access.

Static NAT

- One-to-one mapping.
- Used when a private server needs a fixed public IP.

Site-to-Site Connectivity

GRE Tunnels

- Encapsulate various network protocols inside IP tunnels.
- No encryption by default.

DMVPN – Dynamic Multipoint Virtual Private Network

DMVPN

- Dynamic multipoint VPN that allows on-demand direct tunnels between sites.

Definition:
A Cisco technology that allows secure, dynamic, on-demand VPN tunnels between remote sites without needing a permanent point-to-point configuration for each site.
Example:
In a hub-and-spoke network, Spoke A can communicate directly with Spoke B after initial setup through the hub, creating a dynamic spoke-to-spoke tunnel when needed.

Virtual Private Networks (VPNs)

IPsec

- **ESP (Encapsulating Security Payload)** – Encryption + integrity + authentication.
- **AH (Authentication Header)** – Integrity + authentication only.
- **IKE (Internet Key Exchange)** – Negotiates security associations.

Clientless SSL/TLS VPN

- Web-based, limited to HTTPS-accessible resources.

Client-to-Site VPN

- Requires VPN client software, full network access possible.

IPsec Framework

- **Transport protocols:** ESP, AH, ESP+AH
- **Encryption:** AES-128, AES-192, AES-256
- **Integrity:** SHA-384, SHA-512
- **Authentication:** Pre-shared keys, certificates
- **Key Negotiation:** DH-16, DH-20

Split Tunneling vs Full Tunneling

- **Full Tunnel:** All traffic routes through VPN concentrator.
- **Split Tunnel:** Only organizational traffic goes through VPN; internet traffic goes direct.