Final Exam 2025 - Networking Topics

Introduction to NAT

NAT (Network Address Translation) allows multiple devices on a local network to share a single public IP address, improving security and conserving IPv4 addresses.

Types of NAT

- Static NAT: One-to-one mapping between private and public IPs.
- Dynamic NAT: Assigns a public IP dynamically from a pool.
- Overloading (PAT): Maps multiple private IPs to a single public IP using different port numbers.

Dynamic vs Static PAT

- Static PAT is used when a specific internal service (e.g., web server) needs to be accessible from outside.
- Dynamic PAT is used when multiple devices need to share a single public IP with different port numbers.

Concept of PAT vs NAT

PAT (Port Address Translation) is a type of NAT that uses different port numbers to allow multiple private IPs to share a single public IP.

Purpose of ACLs

ACLs (Access Control Lists) filter and control network traffic to enhance security by permitting or denying specific traffic.

Types of ACLs

- Standard ACL: Filters based on source IP.
- Extended ACL: Filters based on source, destination IP, and protocols.
- Named ACL: Uses names instead of numbers for better management.
- Numbered ACL: Uses numeric identifiers (1-99 standard, 100-199 extended).

Wildcard Masking in ACLs

Wildcard masks define a range of IPs in ACLs, allowing flexible filtering (e.g., 0.0.0.255 matches all IPs in a /24 subnet).

ACLs and Security

ACLs enhance security by controlling traffic flow, acting as firewall rules, and supporting IDS/IPS to detect and block threats.

Introduction to WAN

A Wide Area Network (WAN) connects multiple LANs over large geographic areas using leased or public networks.

Differences: LAN vs MAN vs WAN

- LAN: Small, localized network (e.g., office, home).
- MAN: City-wide network (e.g., metropolitan services).
- WAN: Large-scale, global interconnection of LANs.

Importance of WAN

Essential for enterprise networks, enabling secure, long-distance communication and remote access.

WAN Technologies and Protocols

- Frame Relay: Packet-switched technology for leased lines.
- MPLS: Directs data using labels instead of IP headers.
- Metro Ethernet: Ethernet-based WAN service for businesses.
- ISDN: Digital transmission over traditional phone lines.
- DSL: Broadband over telephone lines.
- Broadband & Fiber: High-speed internet connectivity.

WAN Devices

- Routers: Direct traffic between networks.
- CSU/DSU: Converts signals between network and provider.
- Modems: Convert digital to analog signals.
- Core & Edge Routers: Handle high-speed WAN traffic.

WAN Connection Methods

- Point-to-Point: Dedicated link between two sites.
- VPN: Encrypted private network over public internet.
- Site-to-Site VPN vs Remote Access VPN:
  - Site-to-Site: Connects entire networks securely.
  - Remote Access: Allows users to connect individually.
- SD-WAN: Uses software to manage WAN traffic.

WAN Protocols

- PPP: Encapsulates data for transmission over serial links.
- HDLC: Default protocol for Cisco routers.
- ATM: High-speed, packet-switching technology.

WAN Security

- Common Threats: Eavesdropping, MITM attacks, DDoS.
- Encryption Methods: AES, 3DES for secure data transmission.
- IPSec & SSL VPNs: Encrypt data for secure remote access.
- Role of Firewalls & IDS/IPS: Monitor and block threats.

Neighbor Discovery

Discovers and manages neighbors in IPv6 networks, replacing ARP in IPv4.

Differences: ARP vs NDP

- ARP (IPv4): Maps IP to MAC address.
- NDP (IPv6): Uses ICMPv6 messages for address resolution.

Key NDP Messages

- Router Solicitation (RS): Clients request router info.
- Router Advertisement (RA): Routers announce presence.
- Neighbor Solicitation (NS): Requests MAC for an IP.
- Neighbor Advertisement (NA): Responds to NS queries.
- Redirect Message: Suggests a better route.