## NAT Configuration and Verification

**NAT (Network Address Translation)** - A method used on routers to translate private IP addresses inside a network to a public IP address (or addresses) when accessing external networks, such as the Internet. This conserves public IP addresses and adds a layer of privacy by hiding internal IP structures.

- **Static NAT** - Maps a single private IP address to a single public IP address. One-to-one mapping.
- **Dynamic NAT** - Maps a private IP address to any available public IP address from a pool. Many-to-many mapping.
- **PAT (Port Address Translation / NAT Overload)** - Maps multiple private IP addresses to a single public IP address by using different port numbers. Many-to-one mapping.

**Examples:**

- **Static NAT Example:**

```
ip nat inside source static 192.168.1.10 203.0.113.10
interface FastEthernet0/0
 ip nat inside
interface Serial0/0
 ip nat outside
```

This configuration maps the internal host `192.168.1.10` to the public IP `203.0.113.10`.

- **Dynamic NAT Example:**

```
ip nat pool DYN_POOL 203.0.113.20 203.0.113.30 netmask 255.255.255.0
access-list 1 permit 192.168.1.0 0.0.0.255
ip nat inside source list 1 pool DYN_POOL
interface FastEthernet0/0
 ip nat inside
interface Serial0/0
 ip nat outside
```

This configuration allows internal hosts in the `192.168.1.0/24` network to use any available public IP from `203.0.113.20–203.0.113.30`.

- **PAT (NAT Overload) Example:**

```
access-list 1 permit 192.168.1.0 0.0.0.255
ip nat inside source list 1 interface Serial0/0 overload
interface FastEthernet0/0
 ip nat inside
interface Serial0/0
 ip nat outside
```

This configuration allows all hosts in the `192.168.1.0/24` network to share the single public IP assigned to `Serial0/0` using port numbers.

**Common NAT Commands:**

```
ip nat inside source static <private-ip> <public-ip>
ip nat pool <name> <start-ip> <end-ip> netmask <subnet-mask>
ip nat inside source list <ACL> pool <name>
ip nat inside source list <ACL> interface <interface> overload

interface <interface>
 ip nat inside

interface <interface>
 ip nat outside

show ip nat translations
show ip nat statistics
```

- `ip nat inside` and `ip nat outside` are applied to interfaces to designate where NAT will occur.
- ACLs are often used to define which internal traffic should be translated.
- `overload` is used with PAT to allow multiple hosts to share one public IP.

## CDP and LLDP Configuration and Verification

**CDP (Cisco Discovery Protocol)** - A Cisco proprietary Layer 2 protocol used to share information about directly connected Cisco devices. It allows devices to advertise information such as device ID, IP address, platform, capabilities, and the interfaces they are connected to. Useful for troubleshooting and network topology discovery.

**LLDP (Link Layer Discovery Protocol)** - An IEEE standard (802.1AB) Layer 2 protocol similar to CDP, but vendor-neutral. It allows devices from different vendors to advertise and discover information about directly connected devices.

**Common Commands:**

```
! Enable CDP globally (enabled by default on Cisco devices)
cdp run

! Disable CDP globally
no cdp run

! Enable CDP on an interface
interface <interface>
 cdp enable

! Disable CDP on an interface
interface <interface>
 no cdp enable

! Verify CDP
show cdp neighbors
show cdp neighbors detail

! Enable LLDP globally
lldp run

! Disable LLDP globally
no lldp run
```

```
! Enable LLDP on an interface
interface <interface>
 lldp transmit
 lldp receive

! Disable LLDP on an interface
interface <interface>
 no lldp transmit
 no lldp receive

! Verify LLDP
show lldp neighbors
show lldp neighbors detail
```

**Exam Note:** CDP and LLDP are primarily used for device discovery, not directly for providing Power over Ethernet (PoE). However, LLDP has an extension called **LLDP-MED (Media Endpoint Discovery)**, which can be used by IP phones and other devices to negotiate power requirements, VLAN information, and QoS settings with the switch. CDP can also advertise similar information in Cisco environments, such as the voice VLAN for Cisco IP phones. This is useful in PoE-enabled networks for properly configuring phones and endpoints.

## NTP Configuration and Verification

Network Time Protocol Configuration and Verification

**Synchronized Time** - A consistent and accurate time reference across all devices in a network. It ensures that logs, authentication, security protocols, and scheduled tasks operate correctly by aligning all devices to the same clock source.

**NTP (Network Time Protocol)** - A protocol used to synchronize the clocks of devices over a network. NTP allows routers, switches, servers, and other devices to obtain the correct time from an authoritative source (such as an NTP server) and maintain time consistency across the network. It uses **UDP port 123**.

- NTP uses a Client / Server Model
  - **Stratum Level** - Defines the distance from the reference clock source. Ranges from **0–15** (where 0 = atomic clock/GPS, 1 = directly connected to stratum 0, and higher numbers = further away). Stratum 16 means unsynchronized.
- NTP can use internal or external time sources such as:
  - Global NTP Server
  - GPS or Atomic Clock
  - Master clock (e.g., Domain Controller)
  - Router loopback interface (best practice for internal NTP source and redundancy)

**What does the `ntp server` command do?**

- It configures the device to synchronize its time with a specified external or internal NTP server.
- This makes the device act as an **NTP client**, requesting accurate time from that server.
- Example (using a loopback for redundancy):

```
ntp server 10.1.1.1 source Loopback0
```

**What does the `ntp master` command do?**

- It configures the device to act as an **authoritative NTP time source** for other devices in the network.
- The device assigns itself a stratum level and provides time to NTP clients when no external NTP server is available.
- Common in lab environments or isolated networks without access to public NTP servers.
- Example:

```
ntp master 5
```

**Common NTP Commands:**

```
! Configure a device to use an NTP server
ntp server <ip-address> [source Loopback0]

! Configure a device as an NTP master (stratum level)
ntp master <stratum-level>

! Verify NTP status
show ntp status

! Verify NTP associations (peers/servers)
show ntp associations
```

**Note:** Time synchronization is crucial for security features (such as Kerberos authentication, certificates, and logging) and accurate troubleshooting across devices.

**Time Commands:**

```
! Display the current system clock
show clock

! Set the time zone (example: Central Standard Time)
clock timezone CST -6

! Configure daylight saving time adjustment
clock summer-time CDT recurring

! Manually set the clock (not recommended if using NTP)
clock set HH:MM:SS DAY MONTH YEAR
```

**NTP Logging and Debugging:**

```
! Enable NTP debug messages (real-time monitoring)
debug ntp events
debug ntp packets
```

```
! Disable debugging
undebug all

! View system log messages (NTP and management)
show logging
```

- Use **`debug ntp events`** to monitor synchronization changes.
- Use **`debug ntp packets`** to view NTP communication messages.
- Always disable debugging with **`undebug all`** after troubleshooting to avoid performance issues.

**Best Practice:** Use a loopback interface as the NTP source where possible. This ensures the router remains reachable as an NTP server even if a physical interface goes down, providing redundancy and stability for your network time synchronization.

## Syslog Configuration and Verification

**Syslog** - A protocol used to send system log or event messages from network devices to a centralized server for monitoring, analysis, and troubleshooting. It provides a standardized way to capture logs and system events across multiple devices.

- On Cisco IOS devices, Syslog messages are sent to the **console**, **VTY lines**, and **RAM** by default.
  - If you are not seeing Syslog messages on a terminal session, enable them with:

```
terminal monitor
```

- Optimally, Syslog messages should be sent to a centralized repository such as a **Syslog server**.

- Syslog defines **severity levels 0–7**. The lower the number, the more severe the issue (Every Awesome Cisco Engineer Will Need Icecream Daily):
  - 0: Emergency - System is unusable; immediate action required.
  - 1: Alert - Critical condition that should be corrected immediately.
  - 2: Critical - Critical conditions, typically hardware or major software failures.
  - 3: Error - Error conditions, usually software or configuration issues.
  - 4: Warning - Warning conditions indicating potential problems.
  - 5: Notification - Normal but significant conditions, informational messages.
  - 6: Informational - General informational messages about system operation.
  - 7: Debug - Debugging messages for troubleshooting and detailed analysis.

## SNMP Configuration and Verification

**SNMP (Simple Network Management Protocol)** - A protocol used to monitor and manage network devices such as routers, switches, servers, and firewalls. SNMP allows network administrators to collect information about device performance, configuration, and status, and can also be used to modify device settings remotely. SNMP operates over UDP and uses ports 161 (for requests) and 162 (for traps/notifications(informs)).

- **Versions:**
  - **SNMPv1:** Original version, basic features, community strings for authentication.
  - **SNMPv2c:** Improved performance and features over v1, still uses community strings.
    - **RO (Read-Only):** Allows read access to MIB objects but no changes.
    - **RW (Read-Write):** Allows both read access and modification of MIB objects.
  - **SNMPv3:** Adds authentication and encryption for secure management.
    - **noAuth:** No authentication, only basic identification.
    - **Auth:** Authentication using username and password (MD5 or SHA).
    - **Priv:** Authentication plus encryption of SNMP messages for confidentiality (AES or DES).
- **Common SNMP Terms:**
  - **Agent:** The software on a managed device that collects and reports information.
  - **Manager:** The system used to monitor and control SNMP-enabled devices.
  - **MIB (Management Information Base):** Database of device information accessible via SNMP.

- **Trap:** Asynchronous notification sent from an agent to the manager about an event. **Inform** messages are similar to traps but require acknowledgment from the manager.
- **Community String:** A password-like string used for authentication in SNMPv1/v2c.
- **SNMP NMS (Network Management System):** The platform or software used by administrators to manage, monitor, and analyze SNMP-enabled devices on the network. It acts as the SNMP manager collecting information from agents.

**Common SNMP Commands:**

```
! Configure SNMP community string (v2c)
snmp-server community <community-string> RO
snmp-server community <community-string> RW

! Configure SNMPv3 user with authentication and encryption
snmp-server user <username> <group> v3 auth md5 <password> priv aes
128 <password>

! Enable SNMP traps to a management server
snmp-server host <ip-address> version 2c <community-string>
snmp-server enable traps

! Verify SNMP configuration
show snmp
show snmp user
show snmp group
```

## Quality of Service (QoS) Overview

**What is QoS?** - QoS (Quality of Service) refers to a set of techniques used to manage network resources by prioritizing certain types of traffic. It ensures that critical applications, such as voice and video, receive the necessary bandwidth and low delay, especially during times of network congestion. QoS only takes effect when congestion occurs; if there is no congestion, all traffic flows normally.

**QoS Terminology**

- **Bandwidth** - The maximum rate at which data can be transmitted across a network link, usually measured in bits per second (bps). QoS can allocate or guarantee bandwidth for specific traffic types.
- **Delay** - The time it takes for a packet to travel from the source to the destination. For real-time traffic like VoIP, minimizing delay is critical.
- **Jitter** - The variation in packet arrival times. High jitter can cause poor voice and video quality, so QoS mechanisms work to smooth out these variations.
- **Loss** - The percentage of packets that are dropped during transmission. Packet loss negatively impacts applications such as VoIP and video conferencing. QoS aims to reduce or eliminate loss for critical traffic.
- **Recommendations for VoIP**
  - Bandwidth: Allocate at least 30–50 kbps per VoIP call (depending on codec).
  - Delay: Should be less than 150 ms one-way.
  - Jitter: Should be less than 30 ms.
  - Loss: Should be less than 1%.

**QoS Mechanics**

- **Classification** - The process of identifying and categorizing traffic into different classes based on parameters such as source/destination IP address, protocol, or application type. This step ensures that traffic can be treated differently according to its importance.
- **Marking** - The process of assigning a value (such as DSCP or CoS) to packets once they are classified. This marking is used by other devices in the network to apply QoS policies consistently.
- **Congestion Management** - Techniques such as queuing that determine how packets are stored and transmitted when there is congestion. Examples include FIFO, Priority Queuing (PQ) - 4 queues, QC - 16 user queues (round robin), and Class-Based Weighted Fair Queuing (CBWFQ) - 256 queues, by default.
- **Traffic Policing** - Monitors traffic rates against a defined policy and enforces limits by either dropping excess traffic or remarking it. This is used to ensure traffic does not exceed contracted bandwidth.
- **Traffic Shaping** - Similar to policing, but instead of dropping excess traffic, it buffers and delays packets to smooth traffic flow to match the allowed rate.
- **WRED (Weighted Random Early Detection)** - A congestion **avoidance** mechanism that drops lower-priority packets probabilistically before queues are full, reducing the chance of global TCP synchronization and maintaining fairness.

## IPv6 Addressing

**IPv6** - A 128-bit hexadecimal address format used to replace IPv4 and provide a vastly larger address space.

- Groups of 4 hex digits are separated by colons ":"
  - These groups are called **quartets**
- Up to three leading zeroes in any quartet can be dropped
- One or more consecutive quartets containing all zeroes may be represented by a double colon "::" (but this can only be used once in an address)
- IPv6 does not use broadcast; instead, it uses multicast for one-to-many communication.

**Types of IPv6 Addresses:**

- **Unicast:** Identifies a single interface.
- **Multicast:** Identifies a group of interfaces; packets are delivered to all in the group.
- **Anycast:** Assigned to multiple interfaces, but packets are delivered to the nearest one (based on routing distance).

**Common IPv6 Address Ranges:**

- **Unspecified Address:** ::/128 – Equivalent of 0.0.0.0 in IPv4; used when a device does not yet have an address.
- **Loopback:** ::1/128 – Used by a host to send traffic to itself.
- **Link-local:** FE80::/10 – Range spans FE80:: to FEBF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF. Used for communication on a single link, automatically assigned. Every interface will always have a link-local address.
- **Unique Local:** FC00::/7 – Range spans FC00:: to FDFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF. Private IPv6 addressing, equivalent to IPv4 private ranges.
- **Global Unicast:** 2000::/3 – Range spans 2000:: to 3FFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF. Globally routable IPv6 addresses (similar to public IPv4 addresses).
- **Multicast:** FF00::/8 – Range spans FF00:: to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF. Reserved for multicast groups.

- **Documentation Range:** 2001:DB8::/32 – Reserved for documentation and examples.

**Best Practice:** Always assign loopback addresses (::1) to routers for stability and management. Loopbacks remain up even if physical interfaces go down, ensuring more reliable reachability.

**Configure IPv6 Host:**

- **Static:** The IPv6 address, prefix length, and default gateway are manually configured on the host. Example:

```
ipv6 address 2001:db8:abcd:1::100/64
ipv6 default-gateway 2001:db8:abcd:1::1
```

- **Dynamic EUI-64:** The host automatically generates the interface ID portion (last 64 bits) of the IPv6 address using its MAC address. The router provides the network prefix via Router Advertisement. Example:

```
ipv6 address 2001:db8:abcd:1::/64 eui-64
```

This ensures uniqueness while reducing manual configuration.

**How IPv6 EUI-64 Works:**

1. The host takes its 48-bit MAC address (for example: 00-1A-2B-3C-4D-5E).
2. It splits the MAC into two 24-bit halves: 00-1A-2B and 3C-4D-5E.
3. The value FFFE (16 bits) is inserted in the middle, making it 64 bits: 00-1A-2B-FF-FE-3C-4D-5E.
4. The 7th bit of the first byte (called the Universal/Local (U/L) bit) is flipped:
   a. Original first byte: 00 = 00000000
   b. Flip the 7th bit → 00000010 = 02
   c. New first byte: 02
5. The final EUI-64 Interface ID becomes: 021A:2BFF:FE3C:4D5E.

**Final IPv6 Address Example:** If the router advertises the prefix 2001:db8:abcd:1::/64, the full address becomes:

2001:db8:abcd:1:021A:2BFF:FE3C:4D5E

- **Dynamic (Random):** The operating system can generate a random 64-bit interface ID for privacy, instead of using the MAC address (used by SLAAC with privacy extensions).

## IPv6 Static Routing

Before configuring static routes, enable IPv6 routing on the device:

```
configure terminal
ipv6 unicast-routing
```

- On some layer 3 switches, you may need to verify or change the DSM template:

```
show dsm prefer
```

  - The DSM should prefer a routing template that supports IPv6.
- **Static Route Command Syntax:**

```
ipv6 route <network> <prefix-length> <next-hop-address>
```