

SNMP (Simple Network Management Protocol) - CCNA Summary

SNMP (Simple Network Management Protocol) - Summary for CCNA

What is SNMP?

SNMP is a protocol used for network management. It allows network devices like routers and switches to be monitored.

SNMP Key Components:

1. Managed Device:

- A network device being monitored (e.g., router, switch).
- Runs an SNMP Agent to respond to NMS requests.

2. SNMP Agent:

- Software on a managed device that stores and retrieves management data as defined in the MIB (Management Information Base).

3. Network Management Station (NMS):

- The server or tool that queries and receives data from SNMP Agents.
- Initiates Get, Set operations and receives Traps or Informs.

4. Management Information Base (MIB):

- A hierarchical database of all manageable variables on a device.
- Each variable has an Object Identifier (OID).

Object Identifiers (OIDs):

- Uniquely identify MIB variables.
- Example: .1.3.6.1.2.1.1.5 corresponds to the system name.

SNMP Message Types:

1. Get: Request to read a variable.

2. GetNext: Retrieves the next variable in the MIB tree.
3. GetBulk (v2+): Efficient retrieval of large data blocks.
4. Set: Used to modify a variable.
5. Trap: Asynchronous alert from agent to NMS (no ACK).
6. Inform: Alert with acknowledgment (reliable).
7. Response: Reply to Get, Set, etc.

SNMP Versions:

- SNMPv1: Basic operations, insecure (plaintext).
- SNMPv2c: Adds GetBulk, uses community strings.
- SNMPv3: Secure (supports encryption and authentication).

Ports:

- SNMP Agents use UDP port 161.
- SNMP Managers receive Traps/Informs on UDP port 162.

Community Strings (v1/v2c):

- Function like passwords to control access.
- "public" = read-only; "private" = read-write.

SNMPv2c Basic Configuration (Example):

snmp-server contact admin@example.com

snmp-server location HQ

snmp-server community public RO

snmp-server community private RW

snmp-server host 192.168.1.1 version 2c public

snmp-server enable traps snmp linkdown linkup config

Security Notes:

- SNMPv1 and SNMPv2c send data in plaintext; vulnerable to sniffing.
- Use SNMPv3 in production for secure communication.

Use Cases in Real Networks:

- Monitoring interface status (up/down).
- Measuring CPU/memory usage.
- Getting link utilization metrics.
- Detecting failures via trap alerts.