

Lanka Education And Research Network

Simple Network Management Protocol



What is SNMP?

- **“Is an Internet Standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior”.**
- Used for monitoring and management of network devices(managed devices).
- Can query (Polling) devices and retrieve information
- Can receive notifications (Traps) from devices
- Can change device states/information
- Industry standard protocol
- Supported by almost every network device(vendor)
- Supported by many of available network monitoring and management tools/applications.

What is SNMP?

- Application Layer Protocol
- Uses UDP and ports 161, 162
 - Agent receives Polling requests on port 161
 - Manager receives Traps and Informs on port 162
- History and Versions
 - V1 (1988)
 - V2 (1996)
 - Currently used version v2c
 - V3 (1998)
 - With security (Authentication + Privacy)
- Widely used version is v2
- Newest version V3
 - Its management framework features primarily involve enhanced security. The SNMPv3 architecture introduces the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control.

What it can do?

- Monitor and manage network routers and switches
 - Device status
 - Interface bandwidth
 - CPU usage
 - Temperature
- Servers, PCs/Workstations
 - Disk utility
 - Installed applications/processes
 - CPU load average
- Network printer ink level and paper tray status
- UPS remaining backup power

SNMP Network Components

- An SNMP-managed network consists of three key components:
 - Manager
 - Run on Network management station (NMS) Tools like SNMP tools, Cacti, Zabbix, MRGT
 - Agent
 - Software which runs on Managed Devices like Routers, Switches, Printers, UPS etc.
- MIBs (Management Information Base)
 - Specification containing definitions of management information of a particular device
 - A formatted text file

How it works

SIMPLE NETWORK MANAGEMENT PROTOCOL



Basic Operations (PDU types)

- 1) GetRequest (Manager → Agent)
 - Query for a value
- 2) GetNextRequest (Manager → Agent)
 - Get next value (from a list of values of table)
- 3) GetBulkRequest (Manager → Agent)
 - Multiple iterations of GetNextRequest
- 4) Response (Agent → Manager)
 - Response to GetRequest/GetNextRequest/GetBulkRequest/SetRequest
- 5) SetRequest (Manager → Agent)
 - Modify a value
- 6) Trap (Agent → Manager)
 - Notification from equipment like link down, temperature warning
- 7) InformRequest (Agent → Manager)
 - UDP, yet reliable

Management Information Base (MIB)

- A Specification that defines management information of managed devices.
- Is a Text file which defines information in a hierarchical (tree-structured) way using ASN.1 notation.
- Each Entry(Information) is called a variable or object.
- Each variable/object is identified by a unique identifier which is called Object Identifier (OID).
- OID is a series of numbers separated by periods/dots.

Ex: .1.3.6.1.2.1.1.5

- Read from left to right
- Has a corresponding textual representation

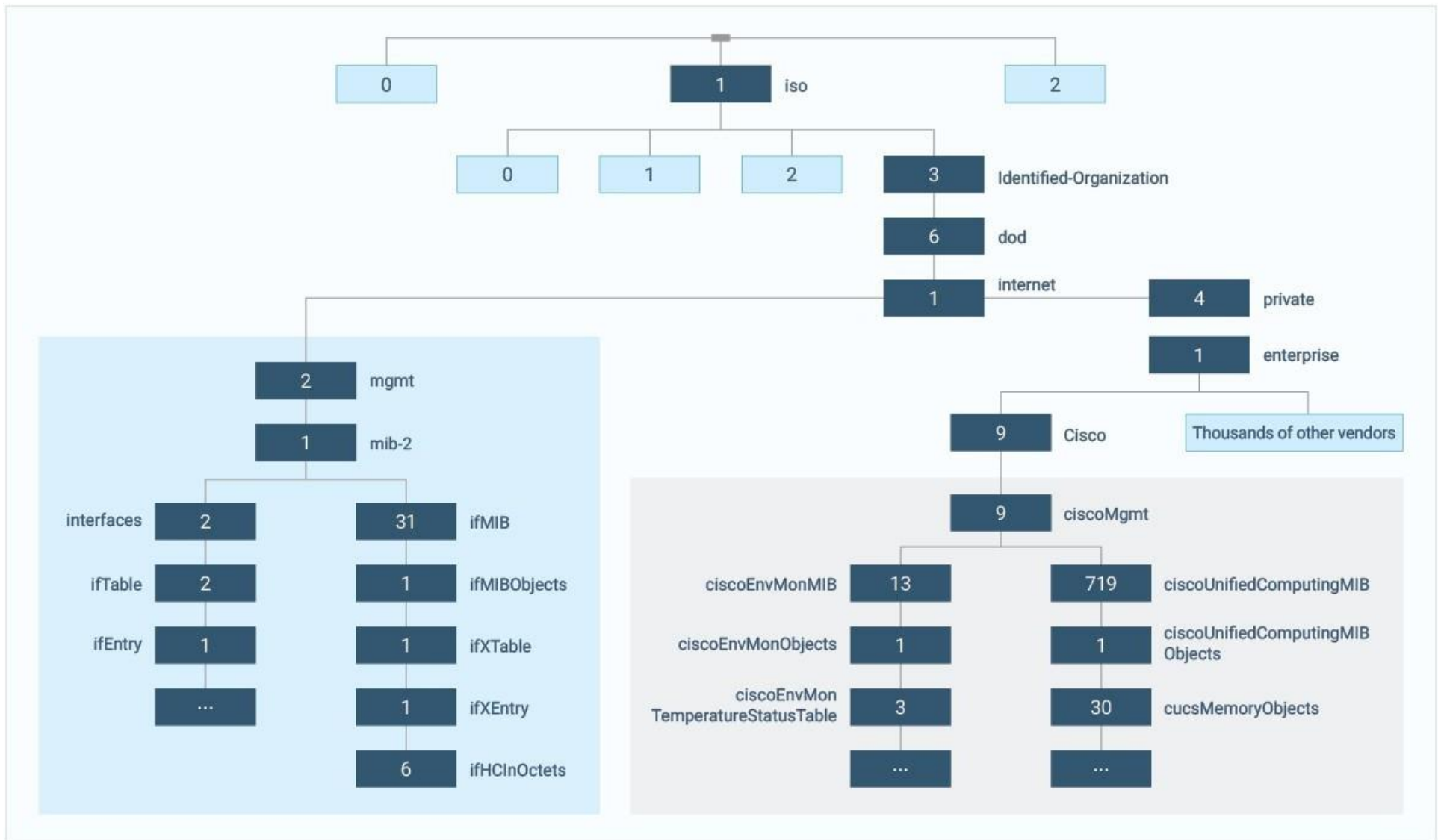
iso.org.dod.internet.mgmt.mib-2.system.sysName = .1.3.6.1.2.1.1.5

Last word of the OID is called (here sysName) the LabelName.

Management Information Base (MIB)

- MIB Object Types (Two Types)
 - Scalar objects
 - Has single instance
EX: sysName (.1.3.6.1.2.1.1.5)
 - Always accessed with Index .0
Ex: snmpget [options] <target-IP> sysName.0
snmpget [options] <target-IP> .1.3.6.1.2.1.1.5.0
 - Tabular objects
 - Has Multiple instances like table or list
EX: ifOperStatus (.1.3.6.1.2.1.2.2.1.8)
snmpwalk [options] <target-IP> ifOperStatus
snmpwalk [options] <target-IP>.1.3.6.1.2.1.2.2.1.8

Management Information Base (MIB)



Querying information through SNMP

- SNMP Client(Manager) Tools has utilities
 - snmpget, snmpgetnext, snmpwalk, snmpbulkget, snmpbulkwalk, snmpstatus, snmpset etc.
- Syntax:
 - snmpxxx -v <1|2c|3> -c community target-host [OID]
- Examples
 - snmpget -v 1 -c NetCommunity 192.168.10.2 .1.3.6.1.2.1.2.2.1.8.1
 - snmpwalk -v 2c -c NetCommunity 192.168.10.2 ifOperStatus
 - snmpgetnext -v 3 -a SHA -A NetAdmin@1 192.168.10.2 IF-MIB::ifOperStatus
 - snmpstatus -v 2c -c NetCommunity 192.168.10.2

SNMP Versions

- SNMP v1
 - Manager(or Request) authenticated through Community String
- SNMP v2c
 - SNMP v1 +
 - Inform request
 - New Data types
 - New retrieval methods (getbulk)
 - Improved error handling
 - Improved SET commands
 - Widely used

SNMP Versions

- SNMP v3 security
 - Authentication
 - User based
 - Uses SHA, MD5 hash functions
- Privacy
 - Encrypted messages using AES, DES
- Message Integrity
 - Ensure the message has not been tampered while in transit

SNMP Views and Groups

- Views
 - Used for controlling access to MIBs
- Groups
 - Combine users into groups of different authorization and access privileges

SNMP V3 Security Levels

- NoAuthNoPriv – No authentication and No privacy
 - Similar to community string level security (Just like v1 v2c)
- AuthNoPriv – Authentication but no Privacy
 - Messages are not encrypted
- AuthPriv – Both authentication and privacy
 - Access authenticated while messages are encrypted
 - High resource consumption

SNMP Agent Configuration on a Network Device (Generic)

- SNMPv1-v2c configuration
 - snmp-server community <COMMUNITY-STRING> view <VIEW-NAME> <read-only|read-write> acl <ACL-NUMBER>
- SNMPv3 configuration
 - snmp-server group v3 <GROUP-NAME> <noAuthNoPriv|authNoPriv|authPrivacy> <read-view|write-view> <VIEW-NAME> acl <ACL-NUMBER>
 - snmp-server user v3 <USER-NAME> <GROUP-NAME> authentication-mode <md5|sha> <AUTHENTICATION-PASSPHRASE> privacy-mode <des|aes> <PRIVACY-PASSPHRASE>

Thank You



National Research and Education Network of Sri Lanka