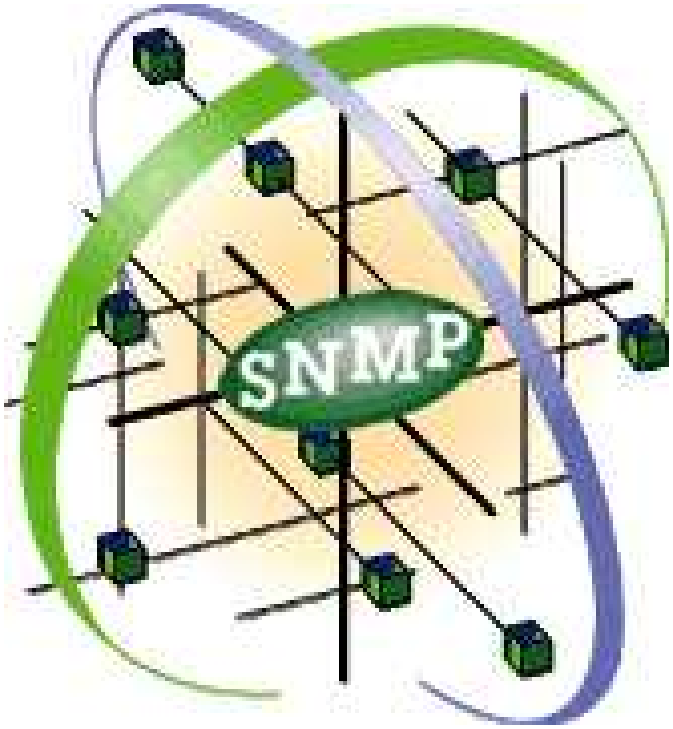
# SNMP and OpenNMS




## Part –1 SNMP

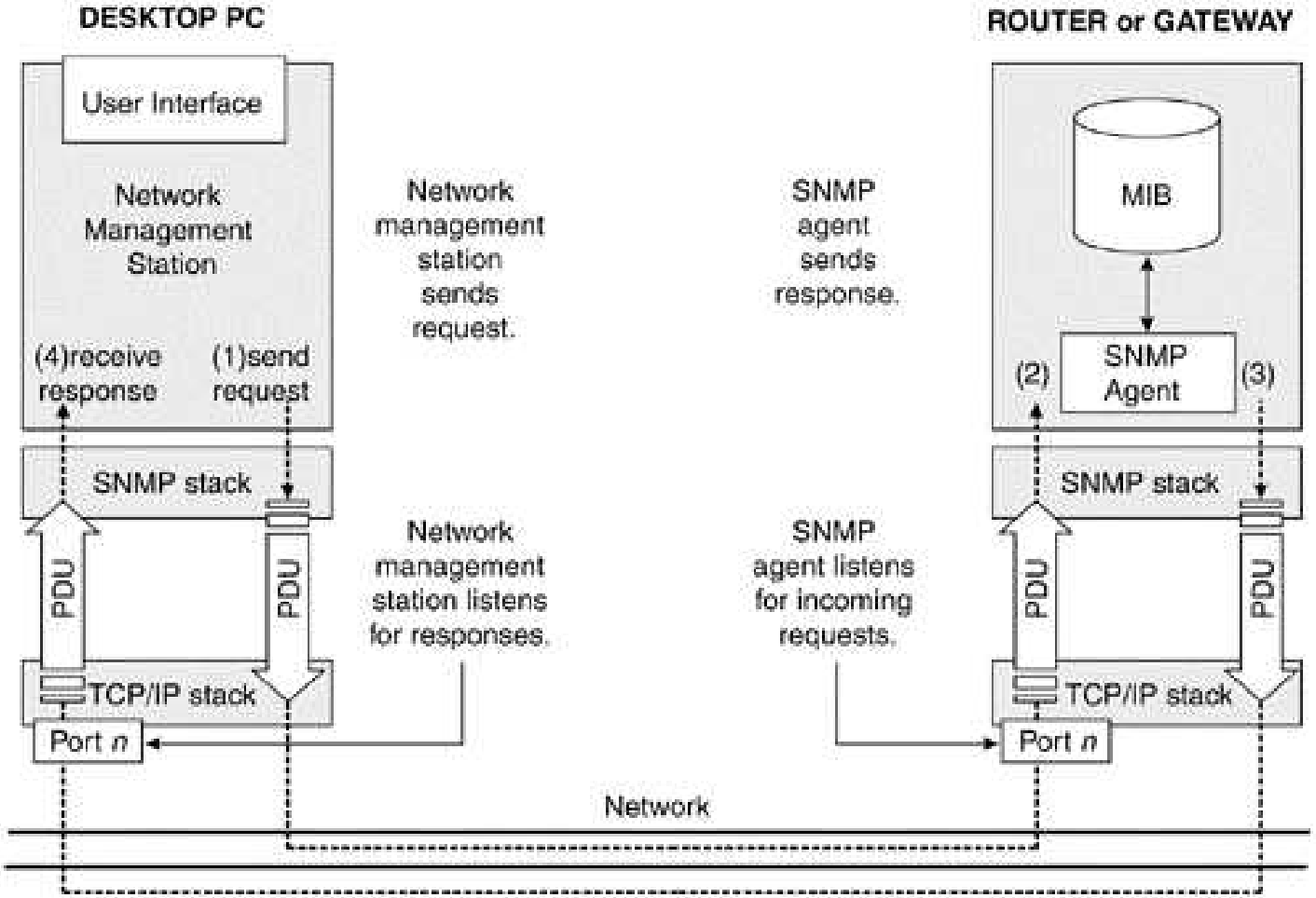
Zeev Halevi

# Introduction

- Designed in 1987 by Internet Engineering Task Force (IETF) to send and receive management and status information across networks
- Most widely used network management protocol on IP networks
- Designed to be simple, easy to implement and consume minimal processor and network resources.

# Overview

- Request/response protocol, management information moves between "SNMP managers"  and "SNMP agents"
- Information defined by a set of managed objects: "Management Information Base" (MIB).
- Network Management Station (NMS) applicatiob collects status, configuration, and performance information from "Network Elements" with "SNMP agents"
- Example: HP openView on a server (NMS) collects performance information from a Crisco router (agent)
- SNMP Versions 1 , 2c , 3




| | |
|---|---|
| PDU: | Protocol Data Unit, used by SNMP when transferring data between two protocol stacks. |
| Port *n,m*: | Where n or m is typically port 161: However this is a user definable value. Note that port 162 is the default port for a network management station to receive traps. |

# Use UDP

- Faster than TCP, no need to initiate connection before sending data.
- Minimal use of network bandwidth: no re-send, no polling of destination address
- Less reliable

# SNMP Commands

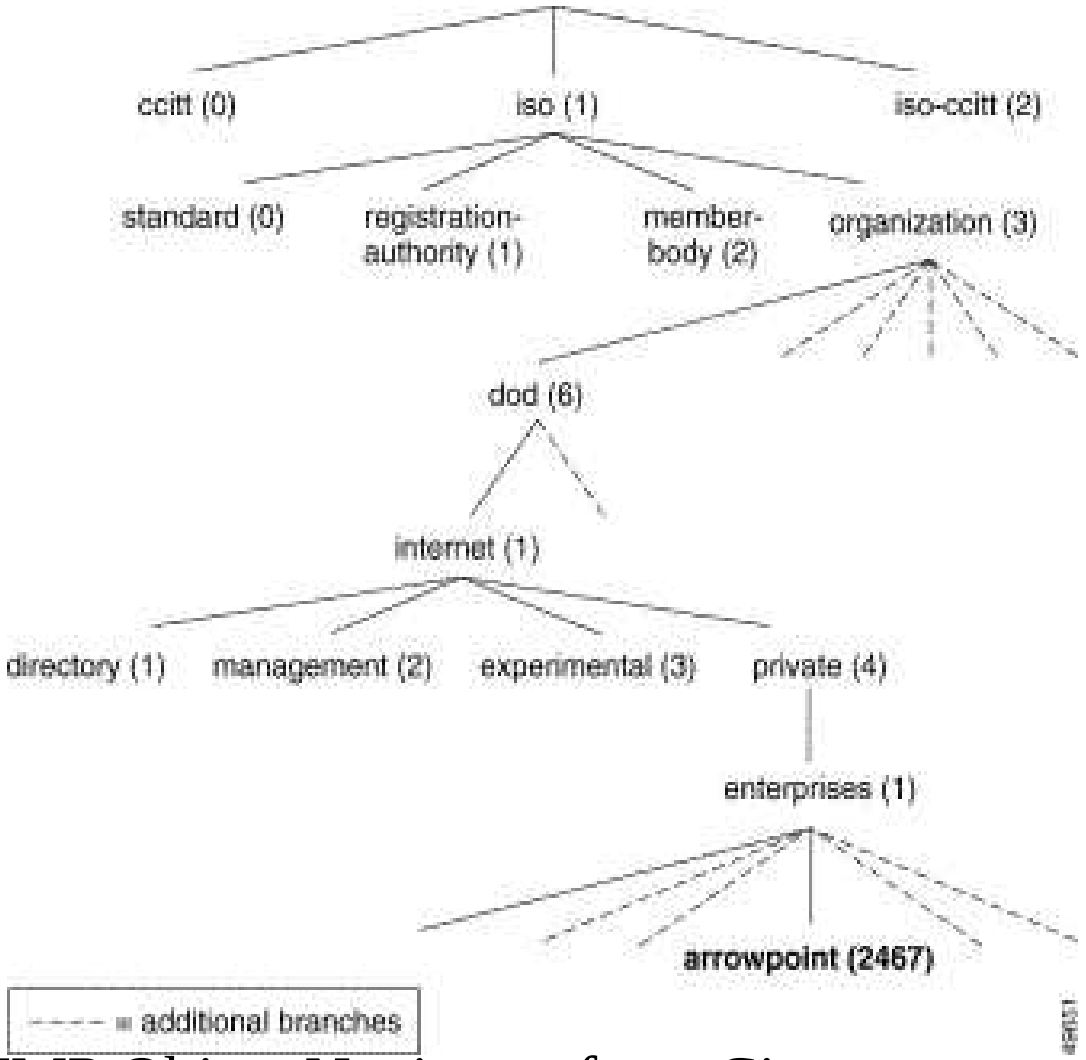
| Operation | PDU | Comment | Flow |
|---|---|---|---|
| Get | GetRequest | Contains the values of the requested object instances. | M->A |
| | GetResponse | Retrieves a variable on an SNMP agent. | A->M |
| Set | SetRequest | Sets a variable on an SNMP agent. | M->A |
| | GetResponse | Contains the error status of SetRequest. | A->M |
| Trap | Trap | Signals the occurrence of an unexpected event. | A->M |
| Getnext | GetNextRequest | Retrieves object instances. | M->A |
| | GetResponse | Contains the values of object instances. | M->A |

get-bulk (SNMPv2 and SNMPv3)

# "Structure of Management Information" SMI

- The name - object identifier(OID), uniquely defines a managed object.
- The type - defined using Abstract Syntax Notation One(ASN.1) : INTEGER, "OCTET STRING" , TimeTicks etc.

# The MIB tree




Online SNMP Object Navigator from Cisco

http://tools.cisco.com/Support/SNMP/do/BrowseOID.do?local=en&substep=2&translate=Translate&tree=NO

# MIB Variables

- Scalar - an object with a single representation
- Tabular - an object with multiple representations depending on "index"

# A closer look on one variable

**Name**: wmtsChassisDescr

**Object IDentifier / OID**: **1.3.6.1.4.1.3066.2.2.2.1.1.1.1.1**

**Full path:**

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).vyyo(3066).vyyoProduct(2).bwaWmtsDocsis(2).wmts21(2).wmtsMIB(1).wmtsMibObjects(1).wmtsComponents(1).wmtsChassis(1).wmtsChassisDescr(1)

**Base syntax:** OCTET STRING

**Max access:** read-only

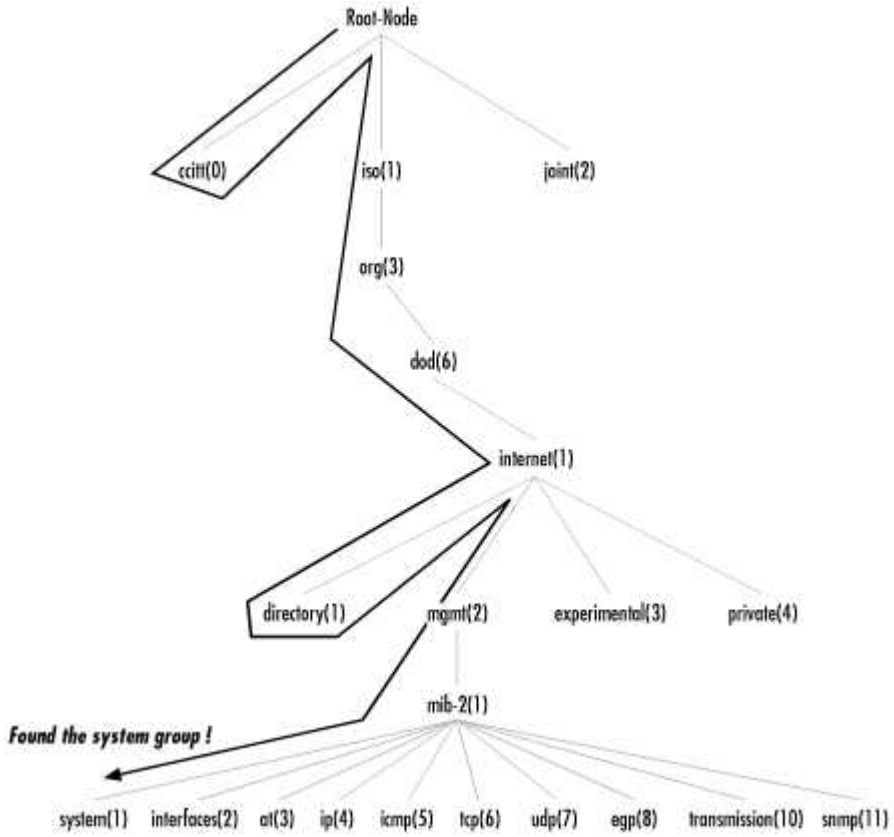
**Description:** A textual description of the chassis.

# MIB-II (RFC 1213)

| Subtree Name | OID | Description |
|---|---|---|
| *system* | *1.3.6.1.2.1.1* | Defines a list of objects that pertain to system operation, such as the system uptime, system contact, and system name. |
| *interfaces* | *1.3.6.1.2.1.2* | Keeps track of the status of each interface on a managed entity. The *interfaces* group monitors which interfaces are up or down and tracks such things as octets sent and received, errors and discards, etc. |
| ..... | | |

See example: RFC1213-MIB.txt

# SNMP Walk




Start at the root  and walk down walk_example.txt

# SNMP Set

- Change the value of one or more variables
- Requires “Set Community”
- Configuring devices using SNMP is hard
- Complex device configuration is typically done using CLI or configuration files
- Emerging IETF standard for configuration uses “Web-Services” NETCONF

  http://www.ops.ietf.org/netconf/

# Traps / Notifications

- Initiated by the agent (Network Element)
- Unusually to port 162
- Example:

Name: wmtsWmuRegistrationComplete

Type: NOTIFICATION-TYPE

OID: 1.3.6.1.4.1.3066.2.2.2.1.2.0.31

Module: VYYO-WMTS21-30-MIB

Objects: 1: trapText

2: docsIfCmtsCmStatusIndex

3: docsIfCmtsCmStatusMacAddress

4: docsIfCmtsCmStatusIpAddress

Description: WMU registration successfully completed.

# NET-SNMP

- Used to be UCD SNMP
- Included in most Linux distributions
- snmpget
- snmpwalk
- snmpset
- More: http://www.net-snmp.org/

# NET-SNMP snmpget, snmpset

```
[root@nmsLinux zeev]# snmpget -v 1 -c zzzzzzzzz 10.200.1.100  system.sysContact.0
SNMPv2-MIB::sysContact.0 = STRING: Sys Admin
[root@nmsLinux zeev]# snmpset -v 1 -c zzzzzzzzz 10.200.1.100  system.sysContact.0 s "Zeev Home"
SNMPv2-MIB::sysContact.0 = STRING: Zeev Home
[root@nmsLinux zeev]# snmpget -v 1 -c zzzzzzzzz 10.200.1.100  system.sysContact.0
SNMPv2-MIB::sysContact.0 = STRING: Zeev Home
```

# NET-SNMP snmpwalk

```
[root@nmsLinux zeev]# snmpwalk  -v 1 -c zzzzzzzzz   10.200.1.100 1.3.6.1.2.1.10.127.1.3.3.1
SNMPv2-SMI::transmission.127.1.3.3.1.2.1 = Hex-STRING: 00 10 3D 12 7D FA
SNMPv2-SMI::transmission.127.1.3.3.1.3.1 = IpAddress: 0.0.0.0
SNMPv2-SMI::transmission.127.1.3.3.1.4.1 = INTEGER: 2
SNMPv2-SMI::transmission.127.1.3.3.1.5.1 = INTEGER: 34
SNMPv2-SMI::transmission.127.1.3.3.1.6.1 = INTEGER: 0
SNMPv2-SMI::transmission.127.1.3.3.1.7.1 = Gauge32: 0
SNMPv2-SMI::transmission.127.1.3.3.1.8.1 = ""
SNMPv2-SMI::transmission.127.1.3.3.1.9.1 = INTEGER: 4
```

# snmpd

## Steps (RedHat)

1. Create /etc/snmp/snmpd.conf using snmpconf

    rwuser  zeev

    rwcommunity  zeev

    disk  / 1000

    agentaddress  161

    syscontact  Zeev Halevi

2. service snmpd restart

# Example: Monitor disk usage

```
[root@nmsLinux snmp]# snmptable -v 1 -c zeev localhost  hrStorageTable
SNMP table: HOST-RESOURCES-MIB::hrStorageTable

 hrStorageIndex                              hrStorageType hrStorageDescr  hrStorageSize hrStorageUsed
              1     HOST-RESOURCES-TYPES::hrStorageFixedDisk              /        4747707 1497931
              2     HOST-RESOURCES-TYPES::hrStorageFixedDisk  /proc/bus/usb             0       0
              3     HOST-RESOURCES-TYPES::hrStorageFixedDisk          /boot         101089    9380
              4     HOST-RESOURCES-TYPES::hrStorageFixedDisk       /dev/pts              0       0
              5     HOST-RESOURCES-TYPES::hrStorageFixedDisk       /dev/shm          64241       0
            101           HOST-RESOURCES-TYPES::hrStorageRam    Real Memory         513932  396632
            102 HOST-RESOURCES-TYPES::hrStorageVirtualMemory     Swap Space         522104       0
            103         HOST-RESOURCES-TYPES::hrStorageOther Memory Buffers              ?       ?
```

# MRTG

- "Multi Router Traffic Grapher" (MRTG) - monitor traffic load on network-links.
- MRTG generates trend-analysis HTML pages with live visual representation of this traffic.
- Using Perl, GNU license.
- http://people.ee.ethz.ch/~oetiker/webtools/mrtg/
- Example: mrtg_example.htm
- Interface types are defined in MIB-II (RFV 1213)

# RRDTool

- From MRTG a new project was born: RRDTool , a tool that maintains "round robin databases" (RRDs) for time-series data.
- example 1 wheather monitoring
- Example 2 laptop monitoring
- http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/

# Other tools

- MIB Browser: tkmib from NET-SNMP
- libsmi, an open source MIB parser library:
  http://www.ibr.cs.tu-bs.de/projects/libsmi/

# Security considerations

- SNMPv1 and SNMPv2 use "communities“
- SNMPv3 added cryptographic security
- Vulnerabilities in Many Implementations of SNMP:

  http://www.cert.org/advisories/CA-2002-03.html

# Other Service Monitoring tools

- Nagios: host, service and network monitoring http://www.nagios.org/
- Sysmon - service monitoring http://www.sysmon.org/

# Measurement/Monitoring tools lists

- CAIDA Measurement and Analysis Tools
- http://www.caida.org/tools/measurement/
- Network Monitoring Tools
- http://www.slac.stanford.edu/xorg/nmtf/nmtf-tools.html
- Historical review: “Evolution of Open Source SNMP Tools” sane-2002.pdf

# Standards

- Apparently SNMP is not so simple – see the list of related RFCs snmp_rfc.txt