

# Introduction to SNMP

---

Network Management Workshop

November 2009  
Nadi, Fiji



# Overview

---

- What is SNMP ?
- OIDs
- MIBs
- Polling and querying
- Traps

# What is SNMP ?

---

- SNMP – Simple Network Management Protocol
  - Industry standard, hundreds of tools exist to exploit it
  - Present on any decent network equipment
- Query – response based
  - GET / SET
    - Mostly GET is used for monitoring
- Tree hierarchy
  - Query for "Object Identifiers" (OIDs)
- Concept of MIBs (Management Information Base)
  - Standard and vendor-specific (Enterprise)

# What is SNMP ?

---

- UDP protocol, port 161
- Different versions
  - Originally, 1988
  - v1 – RFC1155, RFC1156, RFC1157
    - Original specification
  - v2 – RFC1901 ... RFC1908 + RFC2578
    - Extends v1, new data types, better retrieval methods (GETBULK)
    - Really is version v2c (without security model)
  - v3 – RFC3411 ... RFC3418
- Typically we use SNMPv2
- Terminology:
  - Manager (the monitoring "client")
  - Agent (running on the equipment/server)

# What is SNMP ?

---

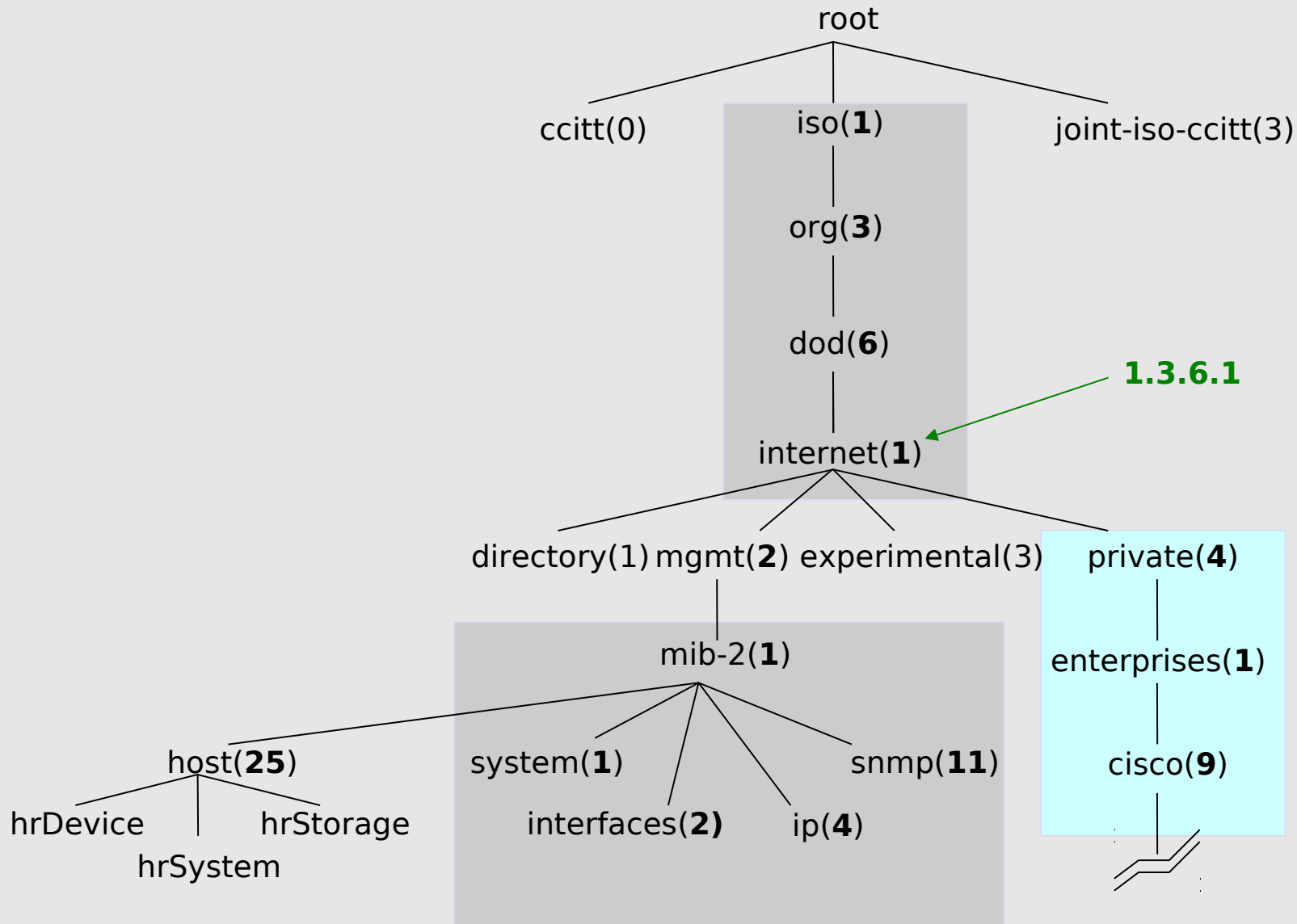
- Typical queries
  - Bytes In/Out on an interface, errors
  - CPU load
  - Uptime
  - Temperature
  - ...
- For hosts (servers or workstations)
  - Diskspace
  - Installed software
  - Running processes
  - ...
- Windows and UNIX have SNMP

# How does it work ?

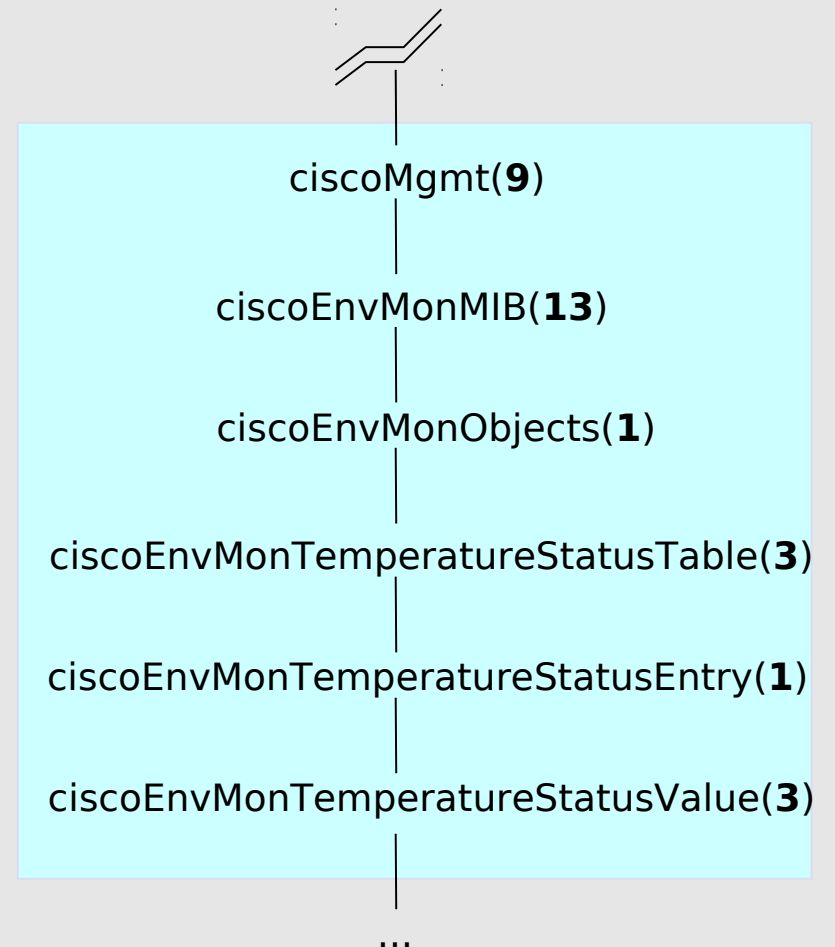
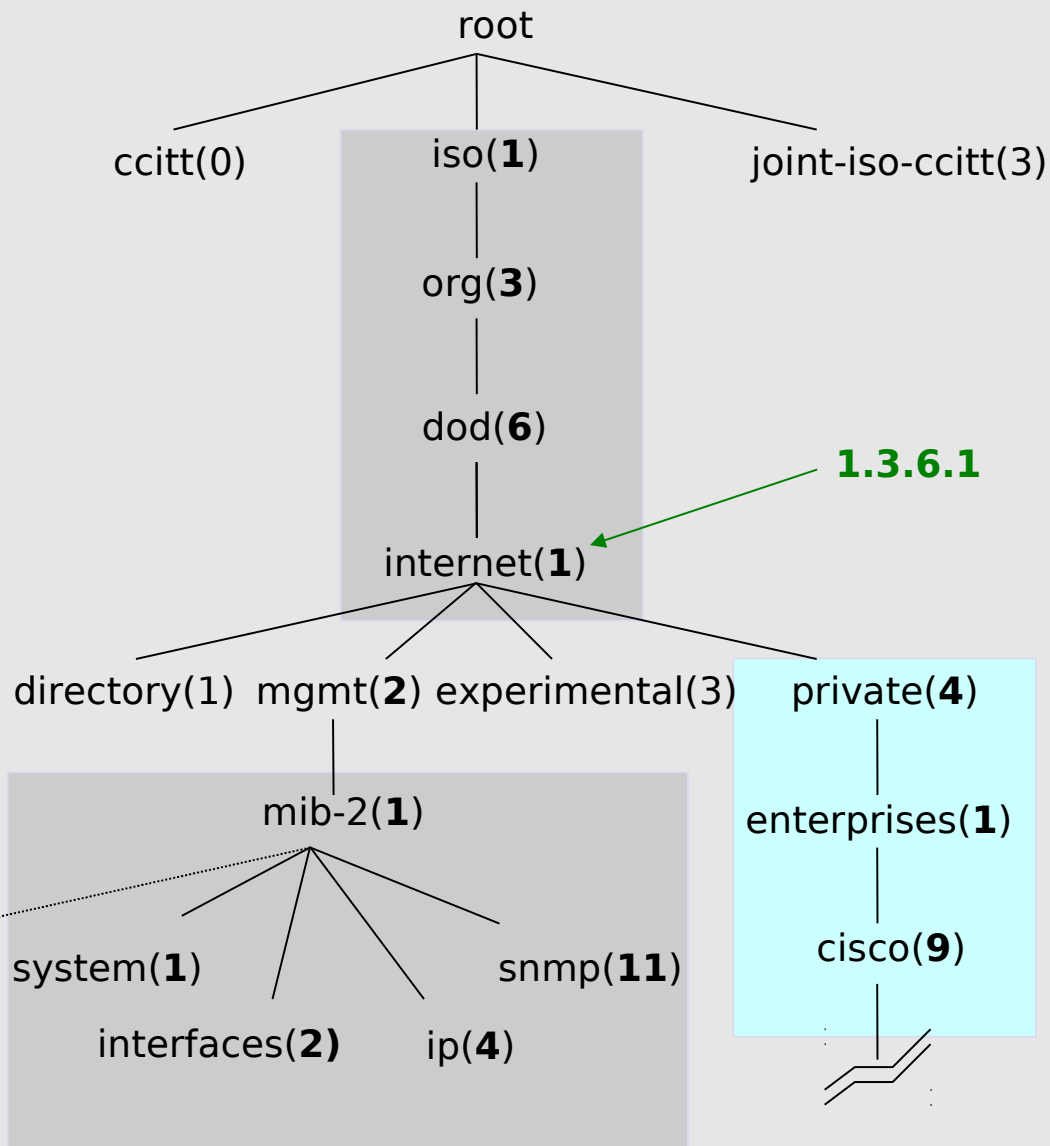
---

- Basic commands
  - GET (manager -> agent)
    - Query for a value
  - GET-NEXT (manager -> agent)
    - Get next value (list of values for a table)
  - GET-RESPONSE (agent -> manager)
    - Response to GET/SET, or error
  - SET (manager -> agent)
    - Set a value, or perform action
  - TRAP (agent -> manager)
    - Spontaneous notification from equipment (line down, temperature above threshold, ...)

# The MIB tree



# The MIB tree





# The Internet MIB

---

- `directory(1)`      OSI directory
- `mgmt(2)`            RFC standard objects
- `experimental(3)`    Internet experiments
- `private(4)`          Vendor-specific
- `security(5)`         Security
- `snmpV2(6)`          SNMP internal

# OIDs and MIBs

---

- Navigate tree downwards
- OIDs separated by '.'
  - 1.3.6.1.4.1.9. ....
- OID corresponds to a label
  - .1.3.6.1.2.1.1.5 => sysName
- The complete path:
  - .iso.org.dod.internet.mgmt.mib-2.system.sysName
- How do we convert from OIDs to Labels (and vice versa ?)
  - Use of MIBs files!
- Internet Standard MIB = 1.3.6.1.2.1
- Cisco MIB = 1.3.6.1.4.1.9

# MIBs

---

- MIBs are files defining the objects that can be queried, including:
  - Object name
  - Object description
  - Data type (integer, text, list)
- MIBS are structured text, using ASN.1
- Standard MIBs include:
  - MIB-II – (RFC1213) – a group of sub-MIBs
  - HOST-RESOURCES-MIB (RFC2790)

# MIBs - 2

---

- MIBs also make it possible to interpret a returned value from an agent
  - For example, the status for a fan could be 1,2,3,4,5,6 – what does it mean ?

# MIBs - SAMPLE

---

sysUpTime OBJECT-TYPE

SYNTAX TimeTicks

ACCESS read-only

STATUS mandatory

DESCRIPTION

"The time (in hundredths of a second) since the network management portion of the system was last re-initialized."

::= { system 3 }

**sysUpTime OBJECT-TYPE**

This defines the object called sysUpTime.

**SYNTAX TimeTicks**

This object is of the type TimeTicks. Object types are specified in the SMI we mentioned a moment ago.

**ACCESS read-only**

This object can only be read via SNMP (i.e., get-request); it cannot be changed (i.e., set-request).

**STATUS mandatory**

This object must be implemented in any SNMP agent.

**DESCRIPTION**

A description of the object

::= { system 3 }

# MIBs - SAMPLE

---

CiscoEnvMonState ::= TEXTUAL-CONVENTION

STATUS current

DESCRIPTION

"Represents the state of a device being monitored.  
Valid values are:

- normal(1): the environment is good, such as low temperature.
- warning(2): the environment is bad, such as temperature above normal operation range but not too high.
- critical(3): the environment is very bad, such as temperature much higher than normal operation limit.
- shutdown(4): the environment is the worst, the system should be shutdown immediately.
- notPresent(5): the environmental monitor is not present, such as temperature sensors do not exist.
- notFunctioning(6): the environmental monitor does not function properly, such as a temperature sensor generates a abnormal data like 1000 C

# Querying SNMP agent

---

- Some typical commands for querying:

- snmpget
- snmpwalk
- snmpstatus

- Syntax:

```
snmpXXX -c community -v1 host [oid]  
snmpXXX -c community -v2c host [oid]
```

- Let's take an example

- snmpstatus -c pacn0g2k9 -v1 192.168.1.221
- snmpget -c pacn0g2k9 -v1 192.168.1.223  
.iso.org.dod.internet.mgmt.mib-  
2.interfaces.ifNumber.0
- snmpwalk -c pacn0g2k9 -v1 192.168.1.222  
ifDescr

# Querying SNMP agent

---

- Community:
  - A "security" string (password) to define whether the querying manager will have R0 (read only) or RW (read write) access
  - This is the simplest form of authentication in SNMP
- OID
  - A value, for example, or it's name equivalent
  - `.iso.org.dod.internet.mgmt.mib-2.system.sysName.0`
- Let's ask for the system's name (using the OID above)

Why the `.0` ? `.1.3.6.1.2.1.1.5.0`, What do you notice ?



# Coming up...

---

- Using `snmpwalk`, `snmpget`
- Configuring SNMPD
- Loading MIBs

# References

---

Basic SNMP at Cisco

<http://www.cisco.com/en/US/docs/internetworking/technology/handbook/SNMP.html>

Wikipedia:

[http://en.wikipedia.org/wiki/Simple\\_Network\\_Management\\_Protocol](http://en.wikipedia.org/wiki/Simple_Network_Management_Protocol)

IP Monitor MIB Browser

<http://www.solarwinds.com/products/ipmonitor/>

Cisco MIB browser:

<http://tools.cisco.com/Support/SNMP/do/BrowseOID.do>

Open Source Java MIB Browser

<http://www.dwipal.com/mibbrowser.htm> (Java)

SNMP Link – collection of SNMP resources

<http://www.snmlink.org/>

Net-SNMP Open Source SNMP tools

<http://net-snmp.sourceforge.net>