Network Management & Monitoring

Introduction to SNMP

Overview

- What is SNMP?
- Polling and querying
- OIDs and MIBs
- Notifications
- SNMPv3

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**

- Monitoring generally uses GET

Object Identifiers (OIDs)

- Keys to identify each piece of data

Concept of MIB (Management Information Base)

- Defines a collection of OIDs

What is SNMP?

Typical queries

- Bytes In/Out on an interface, errors
- CPU load
- Uptime
- Temperature or other vendor specific OIDs

For hosts (servers or workstations)

- Disk space
- Installed software
- Running processes
- ...

Windows and UNIX have SNMP agents

What is SNMP?

UDP protocol, ports 161 and 162(notifications)

SNMP versions

- V1 (1988) — Original specification
  - RFCs 1155,1157,1213
- v2 — Security+new data types+new operators
  - RFCs 1901,1909,1910,2011,2576,2578,2579,2580,3416,3417,3418
  - 64-bit counters, get-bulk, v2 notifications
  - Failed standard!
- v2c — Defacto standard, basically RFC 1901
  - v2 with v1 security (community string) (simple security model)
- v3 — Robust security: USM/VACM
  - RFCs 3411…3415,3417…3418,3826,5343,5345,5590

Typically we use SNMPv2c in this class

SNMP roles

Terminology:

- Manager (the monitoring station)
- Agent (running on the equipment/server)

How does it work?

Basic commands

- GET (manager -> agent)
  - Query for a value
- GET-NEXT (manager -> agent)
  - Get next value (e.g. 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, ...)

OIDs and MIBs

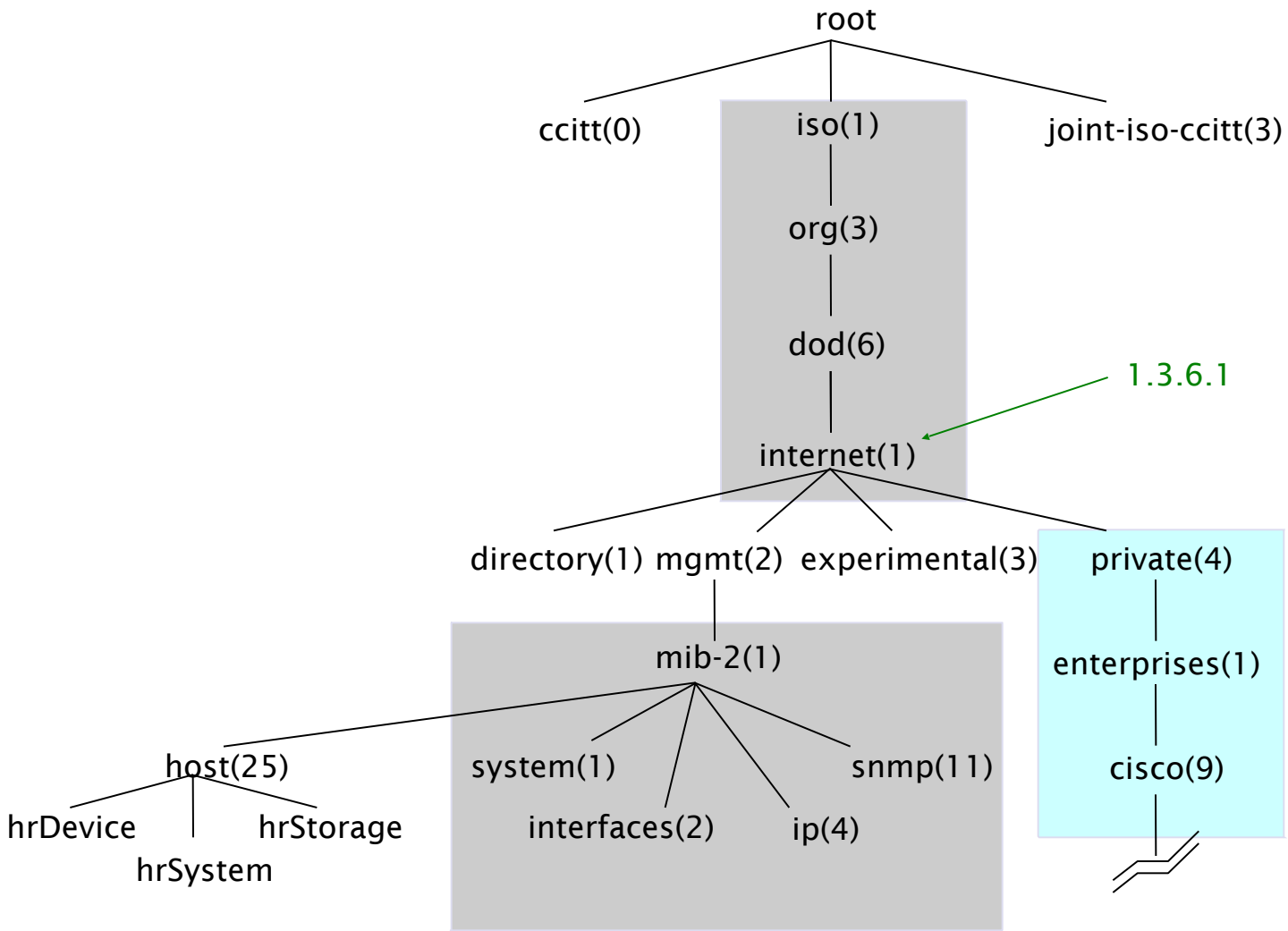
OID: Object Identifier

- A unique key to select a particular item of data in the device
- The same piece of information is always found at the same OID. That's simple!
- An OID is a variable-length string of numbers, e.g. 1.3.6.1.2.1.1.3
- Allocated hierarchically in a tree to ensure uniqueness *(similar to DNS)*

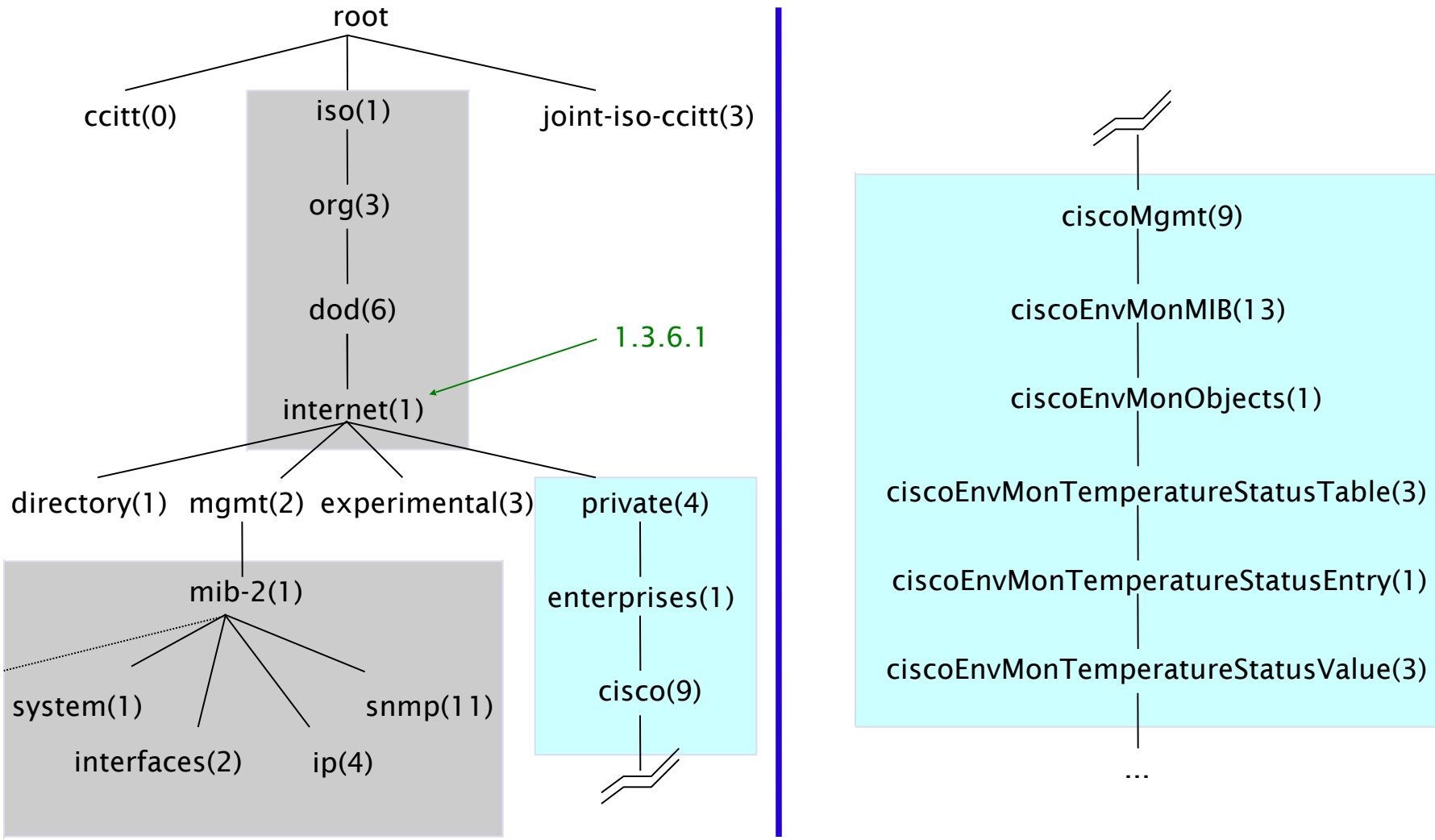
MIB: Management Information Base

- A collection of related OIDs
- A mapping of numeric OIDs to human-readable names

The MIB Tree


root
ccitt(0)
iso(1)
joint-iso-ccitt(3)
org(3)
dod(6)
1.3.6.1
internet(1)
directory(1)
mgmt(2)
experimental(3)
private(4)
mib-2(1)
enterprises(1)
host(25)
system(1)
snmp(11)
cisco(9)
hrDevice
hrStorage
interfaces(2)
ip(4)
hrSystem

The MIB Tree


root
ccitt(0)
iso(1)
joint-iso-ccitt(3)
org(3)
dod(6)
1.3.6.1
internet(1)
directory(1)
mgmt(2)
experimental(3)
private(4)
mib-2(1)
enterprises(1)
system(1)
snmp(11)
cisco(9)
interfaces(2)
ip(4)
ciscoMgmt(9)
ciscoEnvMonMIB(13)
ciscoEnvMonObjects(1)
ciscoEnvMonTemperatureStatusTable(3)
ciscoEnvMonTemperatureStatusEntry(1)
ciscoEnvMonTemperatureStatusValue(3)
...

If Email Addresses were OIDs

user@nsrc.org

would have been something like:

user@nsrc.enterprises.private.internet.dod.org.iso

user@99999.1.4.1.6.3.1

except that we write the top-most part at the left:

1.3.6.1.4.1.99999.117.115.101.114

Don't worry about the deeply branched tree. What matters is that OIDs are unique.

Ensures vendors don't have conflicting OIDs

The numeric OID is what gets sent on the wire

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

* Really only two branches of any interest:

1.3.6.1.2.1 = Standard MIBs

1.3.6.1.4.1 = Vendor-specific (proprietary) MIBs

OIDs and MIBs

- Read from left to right
- OID components separated by '.'
  - `1.3.6.1.4.1.9. ...`
- Each 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!

MIB files

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

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 }`
The `sysUpTime` object is the third branch off of the `system` object group tree.

MIB files - 2

MIB files 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 ?
- Look for the Textual Convention (tc) in the MIB

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.
```

Cisco SNMPv2c configuration

snmp-server community NetManage RO

snmp-server enable traps

snmp-server host 10.10.0.1 traps version 2c NetManage

Net-SNMP SNMP config&example

Configuration

apt-get install snmp

net-snmp-config —default-mibdirs

edit /etc/snmp/snmp.conf and comment out the line:

mibs :

Example

snmpwalk -v2c -c NetManage 10.10.0.252 sysUptime

DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (1707174) 4:44:31.74

#

Net-SNMP SNMPD config&example

Configuration

apt-get install snmpd

add the following line to /etc/snmp/snmpd.conf:

rocommunity NetManage

/etc/init.d/snmpd restart

Example

snmpwalk -v2c -c NetManage localhost sysUptime

DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (1552) 0:00:15.52

#

Querying SNMP agent

Some typical commands for querying:

- `snmpget`
- `snmpwalk`
- `snmpstatus`
- `snmptable`

Syntax:

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

Querying SNMP agent

Let's take an example

- `snmpstatus -c NetManage -v2c 10.10.0.254`
- `snmpget -c NetManage -v2c 10.10.0.254 ifNumber.0`
- `snmpwalk -c NetManage -v2c 10.10.0.254 ifDescr`

Querying SNMP agent

Community:

- A ”security” string (password) to define whether the querying manager will have RO (read only) or RW (read write) access
- This is the simplest form of authentication in SNMP

OID

- A value, for example, .1.3.6.1.2.1.1.5.0
- or its name equivalent: sysName.0

Let's ask for the system's name (using the OID above)

- Why the .0? What do you notice?

SNMP failure: no response?

The device might be offline or unreachable

The device might not be running an SNMP agent

The device might be configured with a different community string

The device might be configured to refuse SNMP queries from your IP address

In all of these cases you will get no response

Optional Materials

SNMP Version 3

SNMP and Security

- SNMP versions 1 and 2c are insecure
- SNMP version 3 created to fix this

- Components
  - Dispatcher
  - Message processing subsystem
  - Security subsystem
  - Access control subsystem

SNMP version 3 (SNMPv3)

The most common module is based in user, or a “User-based Security Model”

- **Authenticity and integrity:** Keys are used for users and messages have digital signatures generated with a hash function (MD5 or SHA)
- **Privacy:** Messages can be encrypted with secret-key (private) algorithms (DES or AES)
- **Temporary validity:** Utilizes a synchronized clock with a 150 second window with sequence checking.

Security Levels

noAuthNoPriv

- No authentication, no privacy

authNoPriv

- Authentication with no privacy

authPriv

- Authentication with privacy

Cisco SNMPv3 configuration

Read-only

```
snmp-server group ReadGroup v3 auth
snmp-server user admin ReadGroup v3 auth sha NetManage
```

Read-write

```
snmp-server group WriteGroup v3 auth write v1default
snmp-server user admin-rw WriteGroup v3 auth sha NetManage
    priv des56 NetWrite
```

Net-SNMP SNMPv3 config&example

```
# net-snmp-config --create-snmpv3-user -a "NetManage" admin
  /usr/sbin/snmpd


# snmpwalk -v3 -u admin -l authNoPriv -a MD5 -A "NetManage"
    localhost sysUpTime
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (4800)
    0:00:48.00
#
```

Net-SNMP snmp.conf

/etc/snmp/snmp.conf

- system-wide config

~/.snmp/snmp.conf

- user config

defVersion 2c

defCommunity NetManage

defSecurityName admin

defSecurityLevel authNoPriv

defAuthPassphrase NetManage

defAuthType SHA

Net-SNMP snmp.conf

```
# snmpwalk 10.10.0.252 sysUpTime
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (1946738)
    5:24:27.38
# snmpwalk -v 3 10.10.0.252 sysUpTime
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (1953429)
    5:25:34.29
#
```

Coming up in our exercises...

- Using snmpwalk, snmpget
  - Config file: `/etc/snmp/`**`snmp`**`.conf`
- Running Linux SNMP agent *(daemon)*
  - Config file: `/etc/snmp/`**`snmpd`**`.conf`
- Loading MIBs
- Configuring SNMPv3 (optional)

References

- *Essential SNMP* (O'Reilly Books) Douglas Mauro, Kevin Schmi
- *Basic SNMP at Cisco*
  http://www.cisco.com/warp/public/535/3.html
  http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.htm
- Wikipedia:
  http://en.wikipedia.org/wiki/Simple_Network_Management_Protocol
- IP Monitor MIB Browser
  http://support.ipmonitor.com/mibs_byoidtree.aspx
  Cisco MIB browser: http://tools.cisco.com/Support/SNMP/do/BrowseOID.do
- Open Source Java MIB Browser
  http://www.kill-9.org/mbrowse
  http://www.dwipal.com/mibbrowser.htm (Java)
- SNMP Link – collection of SNMP resources
  http://www.snmplink.org/
- Net-SNMP Open Source SNMP tools
  http://net-snmp.sourceforge.net/
- Integration with Nagios http://www.cisl.ucar.edu/nets/tools/nagios/SNMP-traps.html