SNMP overview

Network Mgmt/Sec.

Jim Binkley
Outline

◆ snmp components
  – architecture/MIBS/naming
  – protocol
  – security
◆ snmp history and versions
◆ summary
snmp elements

- client/server - architecture
- database elements (MIB)
  - ASN.1
  - naming
  - it’s the contents JIM (too)
- protocol
- security (or lack therein)
e.g., SNMP approach

manager/net console

toaster (ups/hub/switch)

router

host

web server

manager polls all nodes (send/response) with SNMP/displays data

Jim Binkley
architecture

◆ in general
◆ **manager** requests individual data items
  – in v2 tables, in v1 table elements 1 at a time
◆ from **agent**
◆ **manager** is client/client-server sense
◆ **agent** consists of MIB database + snmp code to respond to manager, server (serves database)

Jim Binkley
manager/agent

manager sends

get database item (OID)

agent sends response

Jim Binkley
proxy agent possible but rare

- proxy agent
- speaks SNMP to manager
- but “MIB” does not exist
- instead agent might speak another protocol entirely out the other side
  – level of indirection
- proxies for MIB capability
- might use RPC to talk out other end

Jim Binkley
proxy agent

Jim Binkley

manager

proxy agent

MIB simulation

agent might send messages to emulate MIB values
database elements

- agent has 1 or more sets of variables
- grouped in MIB
- MIB - management information base
- MIB is in some sense a formal specification
  - in ASCII and a parseable grammar
- basically just variables with naming mechanism plus values
- variables are typed and grouped in data structure
MIB, more

- the language for encoding MIB variables is called
- ASN.1 - Abstract Syntax Notation
- “Pascal-like” data description language
- basic and structured types
- variables consist of (name, value) and a type (e.g., `displayString`)
- types usually ints, strings, addresses, arrays
simple example of MIB values might include

- DISPLAYSTRING sysDescr ("cisco 2924")
- TIMETICKS sysUpTime ("up since yesterday")
- DISPLAYSTRING sysContact ("Charlie S.")
- INTEGER sysServices ("internet layer (router)")
MIB does not mean “Men In Black”

- can include more complex values including
- tables (2-dimensional scalars)
  - ip routing table
  - arp table
  - list of interfaces with associated ip addresses, netmasks
  - tcp connections that are open

Jim Binkley
the miracle is the naming mechanism
  – a **COMPLEX** miracle ...

borrowed from ISO/OSI protocol suite

applies both to SNMP PDU and data
  – in ISO ASN.1 was used to describe all packet elements too, e.g., CLNP

attributes include:
  – lexicographical ordering; i.e., if you know the predecessor, you can always get the next value
  – and you always know a predecessor therefore
magical MIB marvels

- any manager can always find any or all of a MIB
- without a priori knowing its elements, or table size (how big it is)
- you can walk all of it a priori
- this is due to the basic tree structure of all MIB data
a MIB data item

- is called or named by its associated
- **Object Identifier** or **OID**
- fundamental base type
- universal prefix is:
- internet OBJECT IDENTIFIER::= { iso(1), org(3), dod(6), internet(1)}
- 1.3.6.1 (iso.org.dod.internet)
- note associated string labels (but the numbers are used in the protocol)
top part of OID tree

Jim Binkley

iso(1)
org(3)
dod(6)
internet(1)
directory(1) X.500
mgmt(2)
mib-2(1)
experimental(3)
private(4)
enterprises(1)
important SNMP variables live in:

1. **MIB-2** subtree
   - prefix: **1.3.6.1.2.1**
     - 1.3.6.1.2.1.1.1 (system.sysDescr)

2. **private/enterprises** subtree
   - for proprietary MIB values
   - e.g., Cisco Mibs quite extensive
   - **1.3.6.1.4.1** (enterprises is last prefix)
so remember these two:

- **MIB-2**: 1.3.6.1.2.1
  - `{iso.org.dod.internet.mgmt.mib-2}`
- **enterprise**: 1.3.6.1.4.1
  - `{iso.org.dod.internet.private.enterprises}`
system.sysDescr

1  .3.  6.  1.  2.  1.  1.  1
iso.org.dod.internet.mgmt.mib2.system.sysDescr

sw note: depending on manager, possible that rooted OID starts with 1 or .1. read the documentation.
MIB-2(1) subtree

system (1)
interfaces(2)
at(3)
ip(4)
icmp(5)
tcp(6)
udp(7)
egp(8)
transmission(10) \{ specific link types \}
snmp(11)
and more (bridge/ethernet stats, repeaters/UPS)

Jim Binkley
some enterprise MIB values

- from Cisco-land
- environmental mib can contain temperatures!
- router may provide load average
- big switch may have traffic meter (how much is backplane utilized)
- CDP values and VLAN values in MIBS
- although not totally related, Cisco has so-called community-based VLAN indexing
  - allows per VLAN bridge/STP information

Jim Binkley
protocol

- on top of UDP
- manager “probes” agent (sends request),
  - gets back result (send/receive)
- SNMP v1 defines 5 message types
  - get, and get-next (reads)
  - set (write)
  - response (ACK if set, or value if get)
  - trap

Jim Binkley
traps

- asynchronously sent by agent to manager
- most important type is linkDown - interface crashed (e.g., router interface)
- common to have linkDown caught by some manager as part of trap/event analysis
  - HPOV can do this, or net-snmp trapd can be setup to do this
  - send page to network manager (human being)
SNMPv1 trap types include:

- coldStart(0) - unexpected restart (crash)
- warmStart(1) - soft reboot
- linkDown(2) - if down, the most imprint!
- linkUp(3) - the opposite of linkDown
- (snmp) authenticationFailure(4)
- egpNeighborLoss(5)
- enterpriseSpecific(6) - proprietary with sub-code

» Cisco has lots of these

Jim Binkley
get and get-next

- get specifies a single variable by name; e.g.,
  system.sysDescr
  - get at ip X, OID=1.3.6.1.2.1.1.1
  - response returns value “cisco 5505”

- get-next specifies OID, but value returned is next lexicographic OID and its value

- thus get-next can be used to query the entire tree, get tables, heal the sick, etc.
the amazing get-next

mib-2

system

sysDescr  sysObjectId  ...  sysServices

get-next sysDescr, and you get sysObjectId
get-next sysObjectId and get sysUpTime
get-next sysServices and get what?
security (bwaa-ha-ha)

- starting point: security is poor
- SNMPv1 relies on “passwords in the clear” like telnet/ftp/pop, etc.
- OID objects have attributes, include
  - readonly
  - read/write
  - write-only (never mind)
  - not implemented (at least be honest)
in practice,

- SNMPv1 agent has a set of community strings (passwords applied to a set of agents)
- these must be supplied with get/set requests, etc (traps too) from manager/agent
- traps are the other way of course, agent to manager
- SET of 1 or more strings for readonly/read-write request
- if PDU/packet community string matches, value returned
universal community strings

- **readonly** - *public* (common default)
- **readwrite** - *private* (default)
- usually applies to ENTIRE SET OF MIBS at agent
- authentication-only service in SNMPv1, i.e., no privacy (no encryption)
security constraints

- typically imposed by border router access-lists
- may block all but given ip address from talking to it
- assume can’t send snmp requests from WAN/Internet into site (make that so)
picture of possible SNMP security setup

1. block SNMP in here

network monitor host

2. only allow monitor to access router

border router

WAN telco link

internal LAN

average host

Jim Binkley
common-practice (v1 continued)

- by very wary of snmp “writes” - may disallow them entirely
- do not allow any snmp from outside world-in
- worry about “interior lines”, make sure manager is close to agents so that promiscuous mode sniffing cannot occur
  - with some routers/switches can start to use ssh
- you NEVER know what might be in a MIB and settable (catch fire on command)
  - could be buggy too
snmp writes may be unavoidable

- some tools may assume snmp writes ok
- cisco ciscoview, rmon probe config
- if you want to use these tools, must design network for secure access
- if hacker could break into probe, can use built-in sniffer
- hacker could manipulate vlans in switches (too awful to think about)
**network snmp write design**

- **Inet - can’t get to net 1**

  - **router uses ACL to block access to net 1**

  - **net 1, use vlans to group switches here**

  - **net 2**

  - **Inet access exists**

  - **dual-homed console**

- Jim Binkley
SNMP—short history

- late 80’s, early 90’s presumed by IETF that ISO would win out in protocol stack race
- thus SNMP was viewed as temporary compromise
- but was oddly based on ISO mechanisms (ASN.1 ...) (not necessarily a bad thing)
- ISO didn’t happen and SNMP crushed its ISO competition

Jim Binkley
SNMP versions

- v1 - widely implemented
  - many new RFCS added for mib-2 new variables sets associated with new network entities
  - RMON added for more instrumentation (especially on ethernet)
  - RMON-2 added as RMON-1 ethernet only, RMON-2 added network/transport-layer stats
v2 (aka v2c)

- v2 was supposed to add better security
- and some optimizations
- security modifications were good, and ahead of their time BUT
- IETF wg couldn’t agree, security ideas were not standardized
- all that remained of v2 practically was
  - get-bulk (get a table in one go)
  - 64 bit integers used for some counters
v3

- focus is on security (crypto wrappers)
  - and finer grain access control to MIBS
- packets may be authenticated and/or encrypted
- view as authentication wrapper on v2/v1 pkt
- simple session-key (change of key) exists
- big ticket item: **writes may be made secure**
- one may still disallow snmp across net
  - basic security policy: just say no …
remote monitoring (more real-time)
  - includes real-time promiscuous based ethernet sampling/threshold mgmt/packet sniffing/topn

rmon I (layer 2)
  - ethernet/link-layer stats only
  - e.g., top N talkers src/dest

rmon II (layer 3/4)
  - includes IP addr/tcp&udp port stats
rmon statement:

- hint to jim: say something about rmon probes/expense/functionality
- functionality:
  - layer 2 stats collected over short time snapshots
  - layer 3 stats the same
  - host 1 by host 2 traffic flow information
  - thresholds - event on too much/too little X
  - promiscuous mode sniffing
summary

» snmp consists of
  – grammar (ASN) for defining data
  – variables (MIBS) associated with device
    » standard, optional, and enterprise-specific
    » depends on the device though (hub/printer/router)
  – UDP-based L7 protocol including get-next, and trap
  – naming convention (OID/tree) that allows
    » lexicographic walk - you may but do not need to know variables names ahead of time (or number)
» security bad in v1, v3 to “fix”, v2c may be norm

Jim Binkley
more summary

- **manager** is client in client-server sense
- **agent** (or proxy) is server (where the MIBS are)
- **manager** polls (usually periodically as with HPOV, MRTG, or by hand as with ucd-snmp snmpwalk or HPOV mib browser) agents
  - displays data

Jim Binkley
some common tools

- **HPOV**
  - ip map and built-in mib browser
- **MRTG/rrdtool/Cricket and friends**
  - periodic graphing of snmp elements
- **ucd-snmp, now net-snmp (command shell utilities)**
  - snmpget, snmpset, snmpwalk
  - note HPOV supplied version similar but different in terms of command-line options