SNMP

Simple Network Management Protocol

Outline

- **Overview**
- Protocol
- MIB
- Net-SNMP

Network Management

- How to monitor your servers?
  - Trying to use the service frequently?
  - Wait the users to complain? (CSCC: #54747)
  - Writing scripts to send email when service fails?
  - ICMP tools: ping, traceroute..etc
- Not only servers need to be monitored
  - Switches
  - Routers
  - UPS
  - Embedded Devices

Requirements of Network Management

- **F**ault Management
  - Detect, isolate, reconfigurate and repair the abnormal network environment
  - Problem tracking and control
- **C**onfiguration and Name Management
  - Startup, shutdown, reconfigure network component when
    - Upgrade, fault recovery or security checks
- **A**ccounting Management
  - Track the use of network resources by end-user to provide
    - Impropriate usage tracing, charging, statistics
- **P**erformance Management
  - Capacity utilization, throughput, response time, bottleneck
    - Collect information and assess current situation
- **S**ecurity Management
  - Information protection and access control

Simple Network Management Protocol

- What does it do?
  - How information look like
  - How they're organized.
  - How to transmit the information you want?
- Cross Platform
- Lightweight
- Simple (!= Easy)
- Best-known implementation: Net-SNMP (BSD Licensed)
- Lots of network management tools are based on snmp. (e.g. Cacti)
- SNMPv3 is defined in RFC 3411 – RFC 3418

History

- In 1989
  - SNMP was adopted as TCP/IP-based Internet standards
- In 1991
  - RMON – Remote network MONitoring
    - Supplement to SNMP to include management of LAN and WAN packet flow
- In 1995
  - SNMPv2 (2c)
    - Functional enhancements to SNMP
    - SNMP on OSI-based networks
  - RMON2
    - Network layer and application layer
- In 1998
  - **SNMPv3**
    - Precise definition, but the content is the same as SNMPv2
    - **Security capability** for SNMP

Components

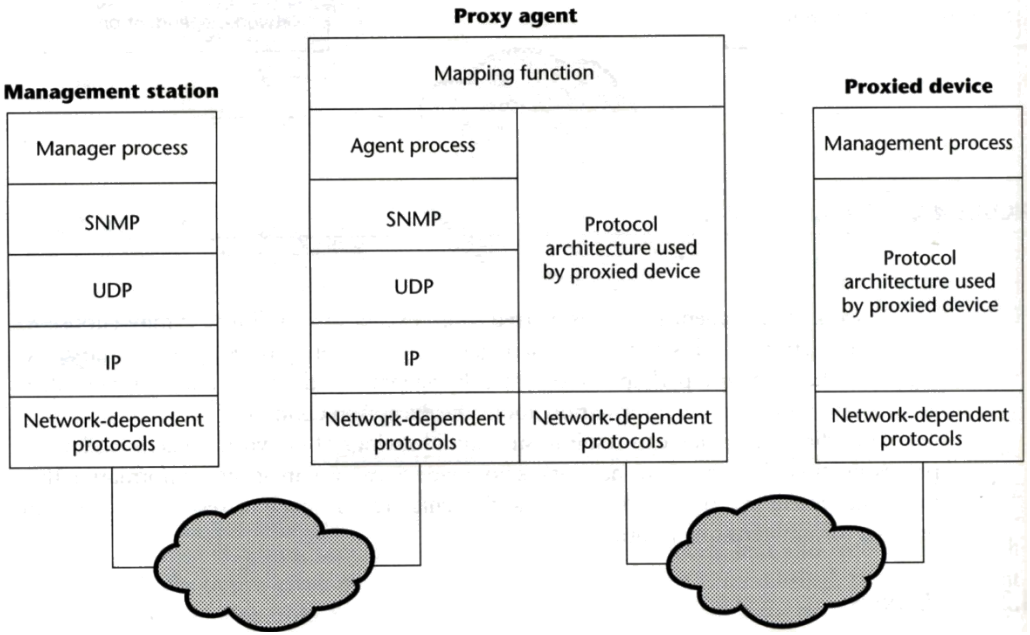
- Protocol
  - Commands: GET, SET, GET-NEXT, GET-BULK, GET-RESPONSE, TRAP.
- SMI: Structure of Management Information
  - Defines how the data in MIB should be defined.
  - Defines data types.
  - A subset of ASN.1 (Abstract Syntax Notation One)
- MIB: Management Information Base
  - What information does an agent has?
  - Tree structure.
  - Standard MIB and Private MIB.

Roles

- Agent
  - Devices to be monitored or managed.
  - Listens port 161 (snmpd) to get the query requests from NMS.
- NMS: Network Management Station
  - Usually the machine in your control (workstation, PC..etc)
  - Querying information from agents.
  - Listens port 162 (snmptrapd) to catch TRAPs.
- Proxy agents
  - See next page

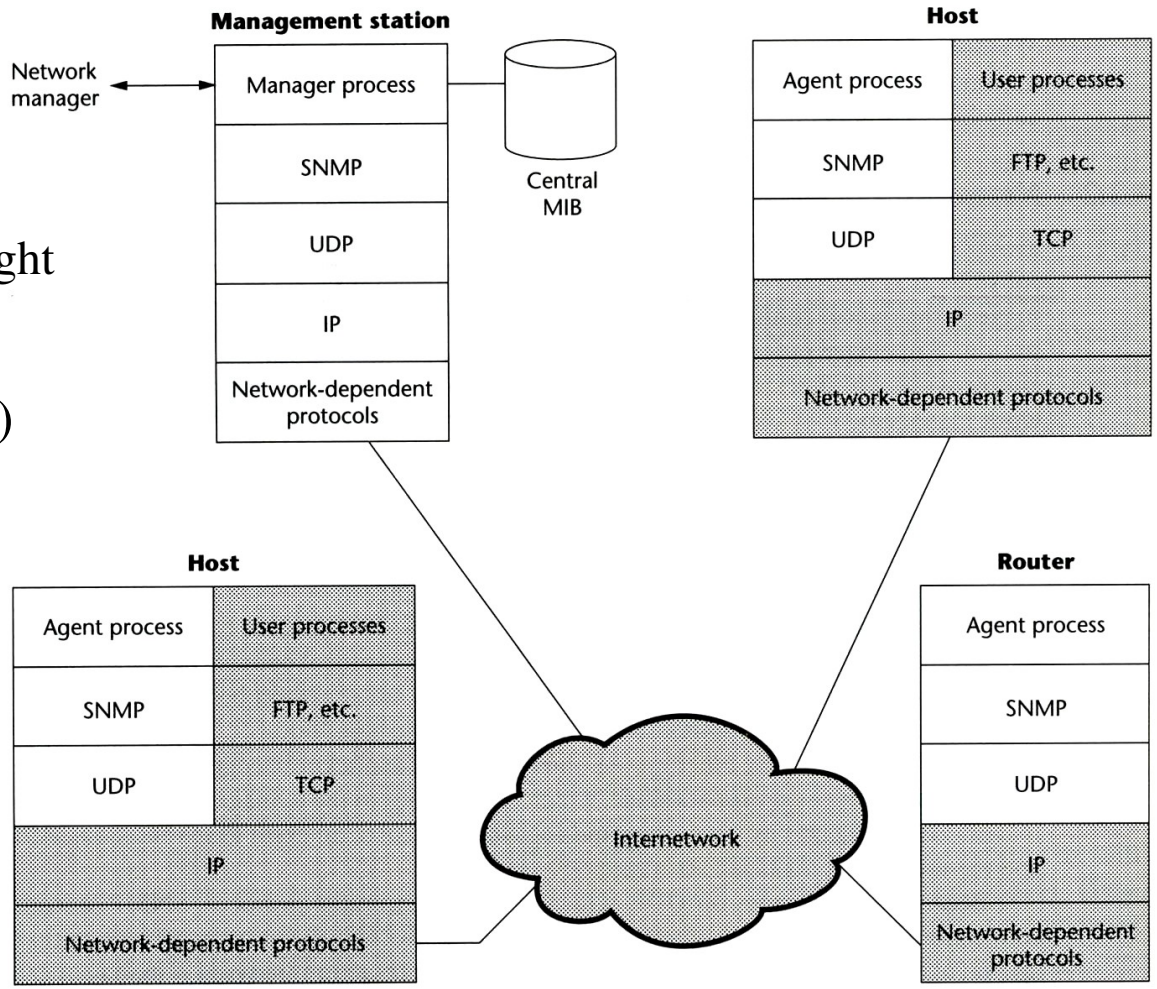
Proxy Agents

- Devices that do not support UDP/IP
  - ex: Bridge, Modem
- Devices that do not want to add burden of SNMP agent
  - ex: PC, programmable controller
- An NMS can be a proxy agent of upper level.



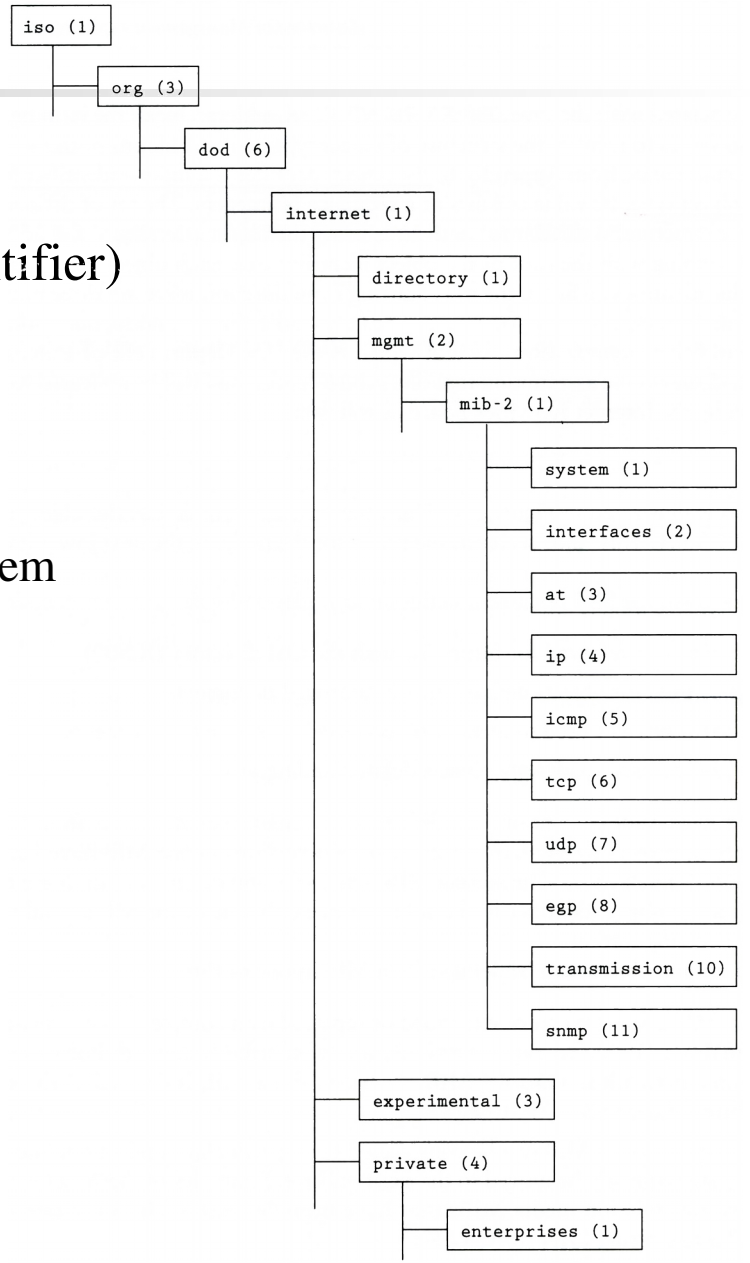
Architecture

- UDP
  - No SYN, ACKs
  - Reduce traffic
  - Fast and lightweight
- Port 161(snmp)
- Port 162(snmp-trap)



MIB Tree

- Tree structure
- An object is called OID (Object IDentifier)
- Numbered like IP address format
  - Non-negative integer (can be large)
  - 1.3.6.1.2.1.1
  - iso.org.dod.internet.mgmt.mib-2.system



Outline

- Overview
- **Protocol**
- MIB
- Net-SNMP

SNMP Versions and Security

- SNMPv1, SNMPv2c: Plain-text community string
  - Private, Public, CSCC, NCTU
- SNMPv3
  - USM (User-based security model), most used.
  - Authentication and encryption
  - Also supports SSH, TLS, Kerberos…

SNMP Operations

- GET-like Operations: Query the information of the agent.
  - GET: Get a specific OID.
  - GET-Next: Get next OID available, used for traversing.
  - GET-Bulk: Optimized version of GET-Next. We can provide a list of OIDs to query.
- SET: Write the OIDs that we have write permission
- TRAP: Send information to NMS.

SNMP Protocol – communities

- Authentication
  - The community name
- Access policy
  - Community profile
    - SNMP MIB view
      - A subset of MIB objects
      - What data is accessible for certain community
    - SNMP access mode
      - read-only, read-write, write-only, non-accessible

SNMP Protocol – Where is the security

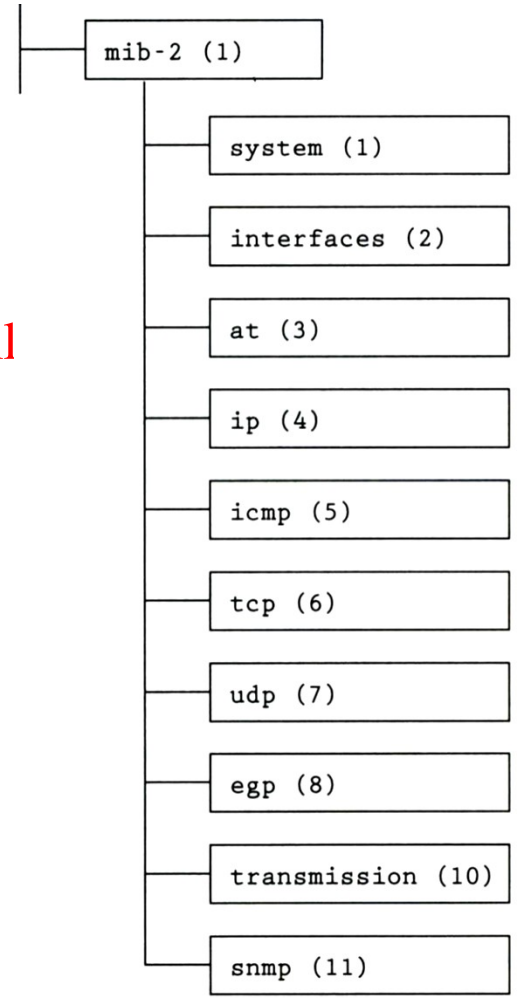
- SNMPv3
  - User-based Security Model (USM)
    - Message Authentication
      - HMAC
        - » MD5, SHA-1
        - » Authentication passphrase, secret key
    - Encryption
      - CBC-DES
  - View-based Access Control Model (VACM)
    - Context table
    - Security to group table
    - Access table
    - View tree family table

Outline

- Overview
- Protocol
- **MIB**
- Net-SNMP

MIB-II

- MIB-I (RFC 1156)
- MIB-II is a superset of MIB-I with some additional objects and groups (RFC1213)
- Reference: http://www.alvestrand.no/objectid/1.3.6.1.2.1.html

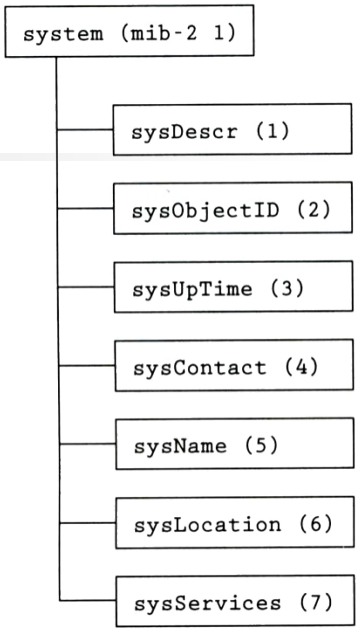


MIB-II (cont'd)

- First layer under mib-2
  - 1.3.6.1.2.1 (iso.org.dod.internet.mgmt.mib-2)
  - system
    - Overall information about the system
  - interfaces
    - Information about each interface
  - at
    - Address translation (obsolete)
  - ip, icmp, tcp, udp, egp
  - transmission
    - Transmission schemes and access protocol at each system interface
  - snmp

MIB-II

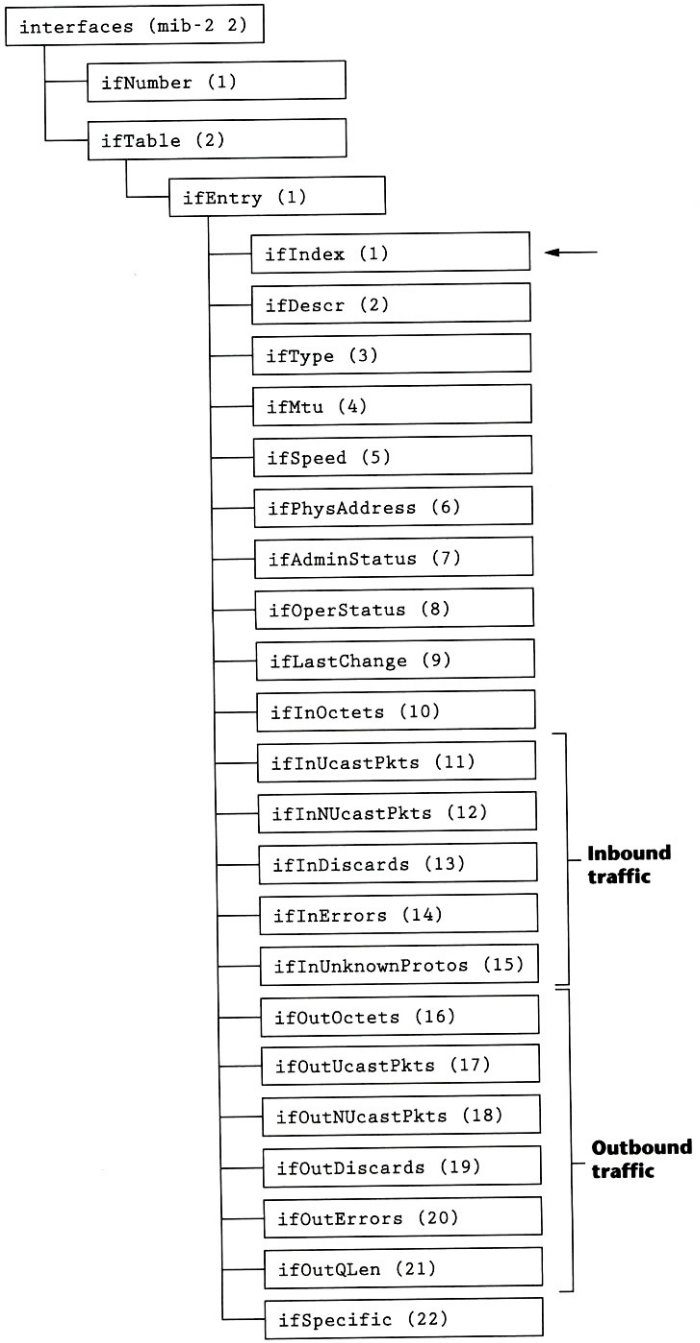
system group



- sysServices
  - 1 physical (ex: repeater)
  - 2 datalink/subnetwork (ex: bridge)
  - 3 internet (ex: router)
  - 4 end-to-end (ex: IP hosts)
  - 7 applications (ex: mail relays)

Object	Syntax	Access	Description
sysDescr	DisplayString (SIZE (0 . . . 255))	RO	A description of the entity, such as hardware, operating system, etc.
sysObjectID	OBJECT IDENTIFIER	RO	The vendor's authoritative identification of the network management subsystem contained in the entity
sysUpTime	TimeTicks	RO	The time since the network management portion of the system was last reinitialized
sysContact	DisplayString (SIZE (0 . . . 255))	RW	The identification and contact information of the contact person for this managed node
sysName	DisplayString (SIZE (0 . . . 255))	RW	An administratively assigned name for this managed node
sysLocation	DisplayString (SIZE (0 . . . 255))	RW	The physical location of this node
sysServices	INTEGER (0 . . . 127)	RO	A value that indicates the set of services this entity primarily offers

MIB-II
interface group



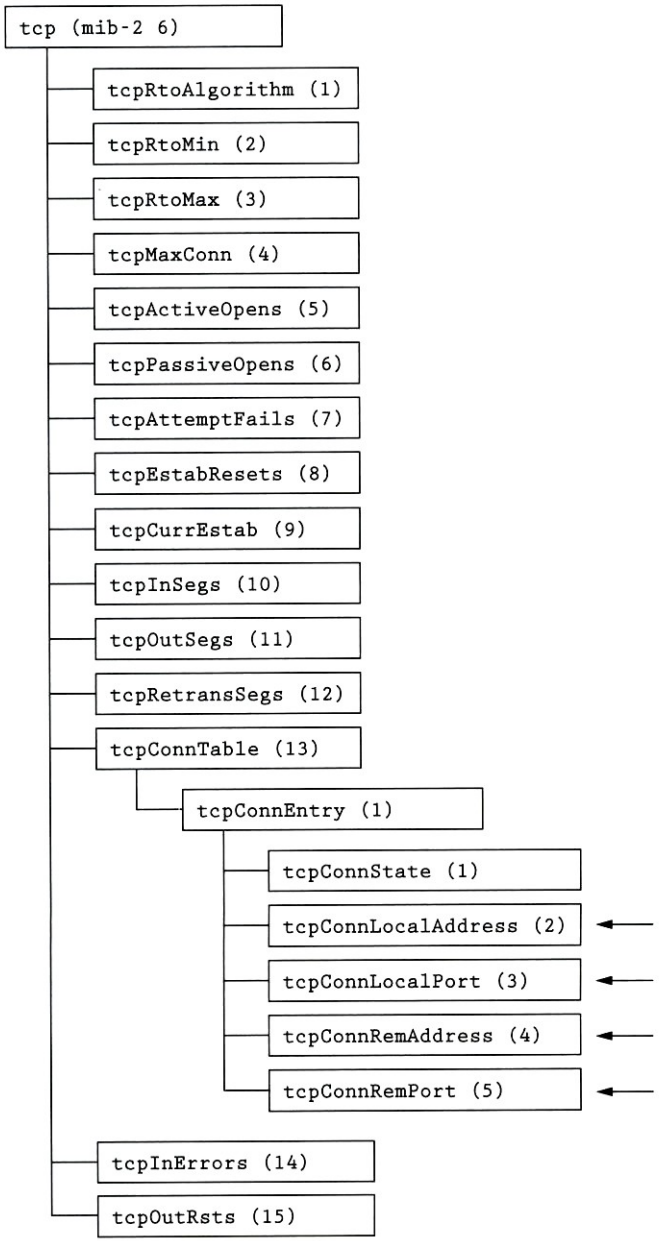
MIB-II
interface group (cont'd)

TABLE 6.2 interfaces Group Objects

Object	Syntax	Access	Description
ifNumber	INTEGER	RO	The number of network interfaces
ifTable	SEQUENCE OF ifEntry	NA	A list of interface entries
ifEntry	SEQUENCE	NA	An interface entry containing objects at the subnetwork layer and below for a particular interface
ifIndex	INTEGER	RO	A unique value for each interface
ifDescr	DisplayString (SIZE (0 . . . 255))	RO	Information about the interface, including name of manufacturer, product name, and version of the hardware interface
ifType	INTEGER	RO	Type of interface, distinguished according to the physical/link protocol(s)
ifMtu	INTEGER	RO	The size of the largest protocol data unit, in octets, that can be sent/received on the interface
ifSpeed	Gauge	RO	An estimate of the interface's current data rate capacity
ifPhysAddress	PhysAddress	RO	The interface's address at the protocol layer immediately below the network layer
ifAdminStatus	INTEGER	RW	Desired interface state (up(1), down(2), testing(3))
ifOperStatus	INTEGER	RO	Current operational interface state (up(1), down(2), testing(3))
ifLastChange	TimeTicks	RO	Value of sysUpTime at the time the interface entered its current operational state
ifInOctets	Counter	RO	Total number of octets received on the interface, including framing characters
ifInUcastPkts	Counter	RO	Number of subnetwork-unicast packets delivered to a higher-layer protocol
ifInNUcastPkts	Counter	RO	Number of nonunicast packets delivered to a higher-layer protocol
ifInDiscards	Counter	RO	Number of inbound packets discarded, even though no errors had been detected, to prevent their being deliverable to a higher-layer protocol (e.g., buffer overflow)
ifInErrors	Counter	RO	Number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol
ifInUnknownProtos	Counter	RO	Number of inbound packets that were discarded because of an unknown or unsupported protocol
ifOutOctets	Counter	RO	Total number of octets transmitted on the interface, including framing characters
ifOutUcastPkts	Counter	RO	Total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or otherwise not sent
ifOutNUcastPkts	Counter	RO	Total number of packets that higher-level protocols requested be transmitted to a nonunicast address, including those that were discarded or otherwise not sent
ifOutDiscards	Counter	RO	Number of outbound packets discarded even though no errors had been detected to prevent their being transmitted (e.g., buffer overflow)
ifOutErrors	Counter	RO	Number of outbound packets that could not be transmitted because of errors
ifOutQLen	Gauge	RO	Length of the output packet queue
ifSpecific	OBJECT IDENTIFIER	RO	Reference to MIB definitions specific to the particular media being used to realize the interface

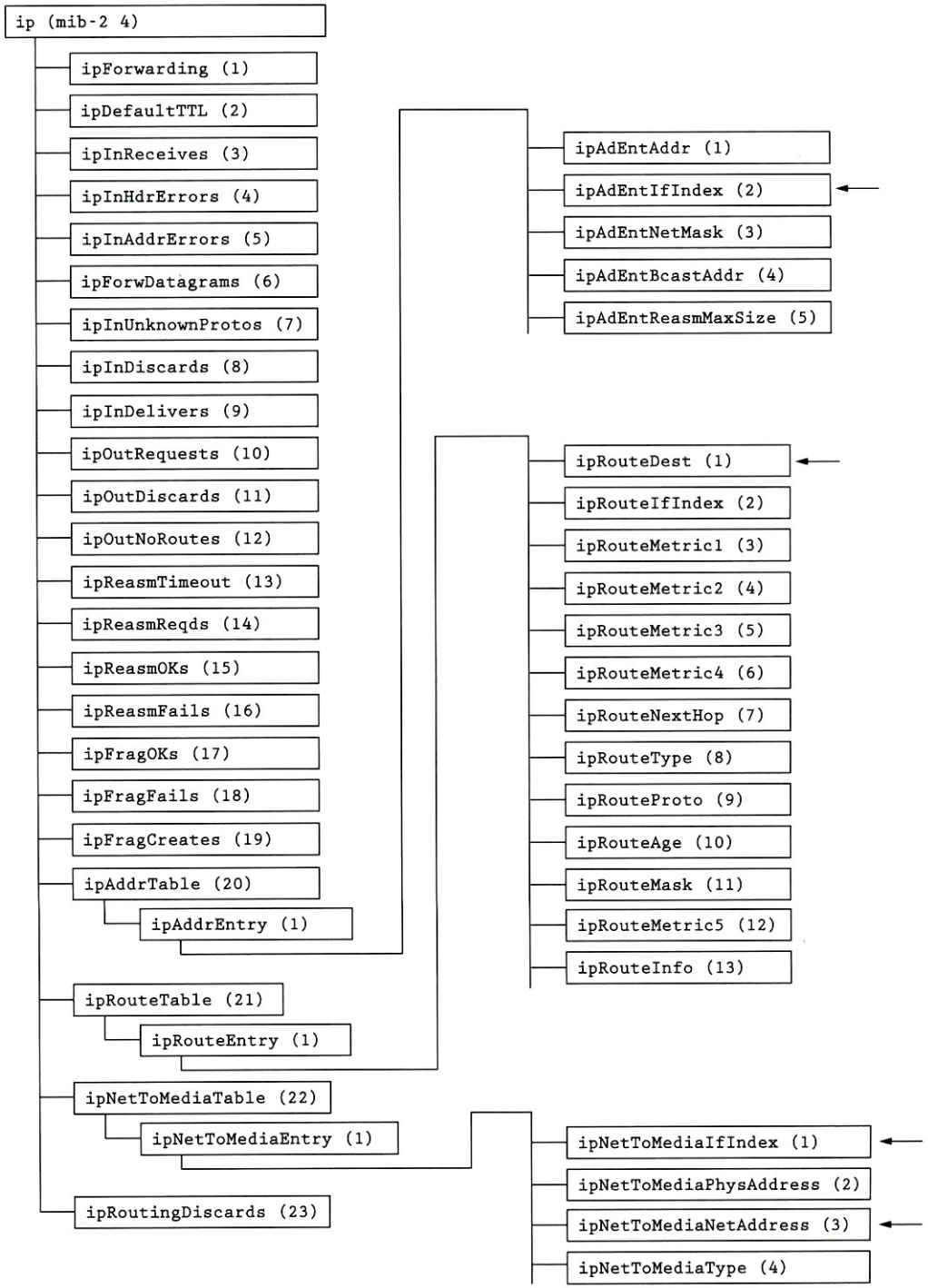
MIB-II

tcp group



MIB-II

ip group



Host Resource MIB

- RFC2790
  - host OBJECT IDENTIFIER ::= { mib-2 25 }
  - hrSystem OBJECT IDENTIFIER ::= { host 1 }
  - hrStorage OBJECT IDENTIFIER ::= { host 2 }
  - hrDevice OBJECT IDENTIFIER ::= { host 3 }
  - hrSWRun OBJECT IDENTIFIER ::= { host 4 }
  - hrSWRunPerf OBJECT IDENTIFIER ::= { host 5 }
  - hrSWInstalled OBJECT IDENTIFIER ::= { host 6 }
  - hrMIBAdminInfo OBJECT IDENTIFIER ::= { host 7 }

Where to Add Your Own MIB?

- For internal use only
  - 1.3.6.1.3 (iso.org.dod.internet.experimental)
- If your are enterprise who want to sell network devices or something
  - 1.3.6.1.4.1 (iso.org.dod.internet.private.enterprises)
  - http://www.alvestrand.no/objectid/1.3.6.1.4.1.html
  - 1.3.6.1.4.1.2: IBM
  - 1.3.6.1.4.1.9: Cisco
  - 1.3.6.1.4.1.11: Hawlett-Packard Company
  - 1.3.6.1.4.1.63: Apple
  - 1.3.6.1.4.1.311: Microsoft
  - 1.3.6.1.4.1.11129: Google
  - 1.3.6.1.4.1.937: D-link

How MIBs being Organized

- First layer:
  - CCITT (0): ITU-T assigned (ITU Telecommunication Standardization Sector)
  - ISO (1): ISO assigned OIDs.
  - Joint-iso-ccitt
- Second layer:
  - Iso.org (1.3): Organizations acknowledged by ISO
- Third layer:
  - Iso.org.dod (1.3.6): US Department of Defense
  - This **international (?)** organization is significant because it is the parent of the Internet OID. (Description here)
- 1.3.6.1 – Internet

Outline

- Overview
- Protocol
- MIB
- **Net-SNMP**

Configuration Files

- Server configuration files
  - /etc/snmp/snmpd.conf
  - /etc/snmp/snmptrapd.conf
  - /var/net-snmp/snmpd.conf
    - for *createUser*, will be rewritten by daemon
- Client configuration files
  - Setting default values when using snmp commands / applications
  - /etc/snmp/snmp.conf
- Search path: /etc/snmp, /usr/share/snmp, /usr/lib/snmp, $HOME/.snmp
- See *man snmp_config(5)* for more info.
- If your’re using FreeBSD, maybe you can also find them in /usr/local

Config tool: snmpconf

- snmpconf -g basic_setup
- Generate snmpd.conf interactively in your current directory by default.
- You can modify the result later.
- In the following example, we're not going to configure trap and advanced agent options.
  - Do you want to configure where and if the agent will send traps? (default = y): n
  - Do you want to configure the agent's ability to monitor various aspects of your system? (default = y): n
- See man pages for more info.

snmpconf: System MIB Group (1.3.6.1.2.1)

- Information returned in the system MIB group (1.3.6.1.2.1):
- The location of the system: NCTU, Hsinchu, Taiwan
- The contact information: mongokim@nasa.cs.nctu.edu.tw
- sysServices.0 (1.3.6.1.2.1.1.7)
  - physical services (eg, like a repeater): 0
  - datalink/subnetwork services (eg, like a bridge): 0
  - internet services (eg, supports IP): 1
  - end-to-end services (eg, supports TCP): 1
  - application services (eg, supports SMTP): 1
  - Finished Output: sysservices 76 (1001100)

snmpconf: Access control setup (v3)

- SNMPv3 read-write user based access
  - user that should have read-write access: rwuser
  - The minimum security level required for that user: auth
  - The OID that this community should be restricted to: [enter]
- SNMPv3 read-only user based access
  - user that should have read-only access to the system: rouser
  - The minimum security level required for that user: auth
  - The OID that this community should be restricted to: 1.3.6.1.2.1

snmpconf: Access control setup (v1, v2c)

- SNMPv1/v2c read-write community access
  - community name to add read-write access for: private
  - hstname or network address to accept from: 192.168.0.0/24
- SNMPv1/v2c read-only community access
  - community name to add read-only access for: public
  - hostname or network address to accept from:
    - type default if you want to allow all hosts, if you leave it empty, it will result in strange behavior when you query.
  - The OID that this community should be restricted to [RETURN for no-restriction]: 1.3.6.1.2.1

Test snmpd with Basic Configurations

- Copy the file generated by *snmpconf* to /etc/snmp or other places you want.
- Start the service
  - systemctl start snmpd
- Test the SNMP communities we just set:
  - snmpwalk -v 2c -c public localhost
  - snmpwalk -v 2c -c private localhost
  - You shall see lots of MIB outputs on screen.

SNMPv3 User Configuration

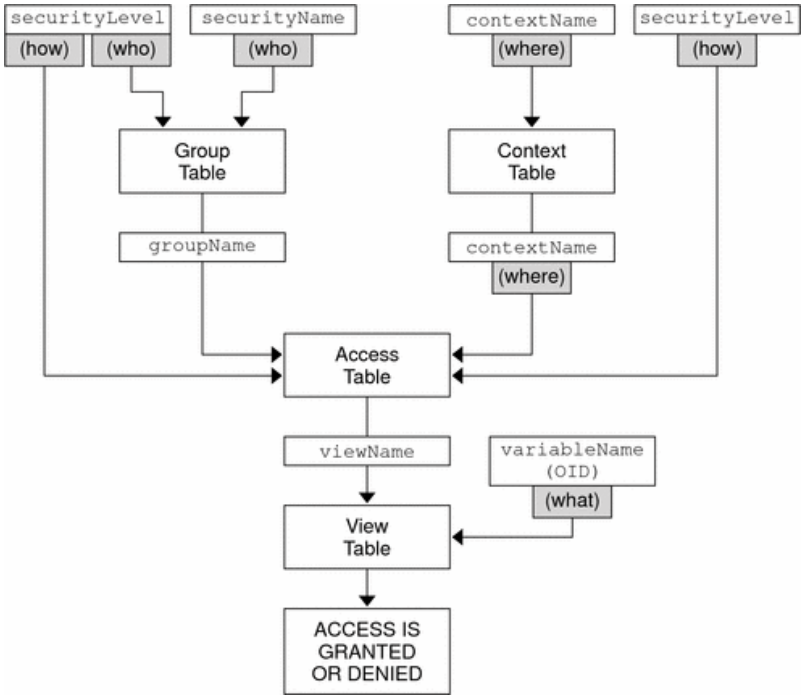
- We haven't set the password to our SNMPv3 user.
- Append the following line to /var/net-snmp/snmpd.conf
  - createUser rwuser SHA "snmp5566" AES "gogo5566"
- Restart daemon and test your configuration
  - snmpwalk -v3 -u rwuser -a SHA -A "snmp5566" -x AES -X "gogo5566" -l authPriv localhost
- /var/net-snmp/snmpd.conf
  - When you restart the daemon, snmpd will read your *createUser* directives and encrypt your plain-text passwords.

Review of Our Basic Configuration

- /etc/snmp/snmpd.conf
  - System information
  - Configure *rwuser, rouser, rwcommunity, rocommunity*
- /var/net-snmp/snmpd.conf
  - createUser directives

View-Based Access Control Model

- Advanced access control feature.
- Integrate SNMP[v1, v2c]'s community and SNMPv3's USM.
- I think it's a little bit complicated (not so "Simple")



http://docs.oracle.com/cd/E19253-01/817-3000/images/VACMflowChart.gif

VACM Keywords: com2sec, group, view

- VACM keywords in *snmpd.conf*
- *com2sec*: map *community string* and a *source IP* to a *security name*.
  - com2sec <security name> <source> <community>
- *group*: map a *security model* and *security name* to a *group name*.
  - group <group name> <security model> <security name>
  - *security model* can be like *v1, v2c, usm* or other security models.
  - For SNMPv3, the security name is simply SNMPv3 username.
  - A *security name* (a.k.a. user in SNMPv3) cannot belongs to more than one group.
- *view*: Defines a subtree in MIB.
  - view <view name> <included / excluded> <OID> [mask]

VACM Keywords: access

- *access*: Define the permissions for all security components we've discussed.
  - access <context> <sec. model> <sec. level> <match> <read> <write> <notify>
  - *security level* can be *noauth*, *auth*, *priv*.

VACM Example Configuration

```
#         sec. name  source          community
com2sec localSec  10.0.0.0/16     private
com2sec pubSec       default       public
com2sec nctuSec   140.113.0.0/16  public

#      group name sec. model sec. name
group rwGroup    v2c          localSec
group rwGroup    usm           rwUser
group rwGroup    usm           admin
group pubGroup   v2c          pubSec
group pubGroup   usm           pubUser
group roGroup    v2c          nctuSec
group roGroup    usm           roUser
```

VACM Example Configuration

```
#      view name   incl/excl   subtree
view      all      included     .1
view    sysInfo    included   .1.3.6.1.2.1

#      grp. name context sec. model sec. level match read  write notify
access rwGroup    “”         any       auth    exact  all    all   none
access roGroup    “”         any     noauth    exact  all    none  none
access pubGroup   “”         any     noauth    exact sysInfo none  none
```

Net-SNMP Command Line Tools

- SNMP-CMD [options] agent [parameter]
- Common options:
  - -c <community string>
  - -v <version: 1,2c,3>
  - -a <authentication protocol: MD5, SHA>
  - -A <passphrase>
  - -u <user name>
  - -x <privacy protocol>
  - -X <privacy passphrase>
  - see *man snmpcmd(1)*

Net-SNMP Command Line Tools (cont'd)

- Basic operations:
  - snmp[get,getnext,set] [options] hostname OIDs
    - OID can be either number format or text format.

```
snmpget  -v 2c -On -c public_v2c localhost
```

Net-SNMP Command Line Tools (cont'd)

- Basic operations:
  - snmpgetbulk [options] **[-CnX -CrY]** hostname <OID list>
    - Both X and Y are integers.
    - *-Cn* for *non-repeater*, *-Cr* for *max-repetition*.
    - Let **N** be min(*Non-repeater*, number of OIDs specified) .
    - Let **M** be the *Max-repetition* here.
    - It will perform a GET-NEXT for first **N** OIDs , then perform **M** GET-NEXTs for reamaining OIDs.

```
[tsn@snmp ~]$ snmpbulkget -Cn1 -Cr2 -v 2c -c public_v2c localhost .1.3.6.1.2.1.1.1  .
1.3.6.1.2.1.25.3.2.1.3

.SNMPv2-MIB::sysDescr.0 = STRING: Linux yui 4.5.4-1-ARCH #1 SMP PREEMPT Wed May 11
22:21:28 CEST 2016 x86_64

HOST-RESOURCES-MIB::hrDeviceDescr.196608 = STRING: GenuineIntel: Intel(R) Core(TM)
i5-4460  CPU @ 3.20GHz

HOST-RESOURCES-MIB::hrDeviceDescr.196609 = STRING: GenuineIntel: Intel(R) Core(TM)
i5-4460  CPU @ 3.20GHz
```

Net-SNMP Command Line Tools (cont'd)

- Basic operations:
  - snmpwalk, snmpbulkwalk
    - Traversal the subtree(s) you specified.

```
[joshua5201@yui ~]$ snmpwalk  -v 2c  -c public_v2c localhost .1.3.6.1.2.1.25.3.2.1.3
HOST-RESOURCES-MIB::hrDeviceDescr.196608 = STRING: GenuineIntel: Intel(R) Core(TM)
i5-4460  CPU @ 3.20GHz
...
HOST-RESOURCES-MIB::hrDeviceDescr.262145 = STRING: network interface lo
HOST-RESOURCES-MIB::hrDeviceDescr.262146 = STRING: network interface eno1
...
HOST-RESOURCES-MIB::hrDeviceDescr.393232 = STRING: SCSI disk (/dev/sda)
HOST-RESOURCES-MIB::hrDeviceDescr.393233 = STRING: SCSI disk (/dev/sdb)
HOST-RESOURCES-MIB::hrDeviceDescr.393234 = STRING: SCSI disk (/dev/sdc)
HOST-RESOURCES-MIB::hrDeviceDescr.786432 = STRING: Guessing that there's a floating
point co-processor
```

  - snmptrap, snmptable

Net-SNMP Command Line Tools (cont'd)

- Information collecting tools
  - snmpdf

```
[tsn@snmp ~]$ snmpdf -c public_v2c -v 2c localhost
Description               Size (kB)           Used       Available Used%
Physical memory            16378768        13697696         2681072   83%
. . .
/                          51475068        38212120        13262948   74%
```

  - snmpnetstat

```
[tsn@snmp ~]$ snmpnetstat -c public_v2c -v 2c localhost
Active Internet (tcp) Connections
Proto Local Address               Remote Address                    State   PID
tcp4  localhost.localdom.37322    localhost.localdom.53382    ESTABLISHED 23842
```

  - snmpstatus

```
[tsn@snmp ~]$ snmpstatus -c public_v2c -v 2c localhost
[UDP: [127.0.0.1]:161->[0.0.0.0]:37205]=>[Linux yui 4.5.4-1-ARCH #1 SMP PREEMPT Wed May
11 22:21:28 CEST 2016 x86_64] Up: 11:17:45.79
Interfaces: 4, Recv/Trans packets: 3192997/1527997 | IP: 2127420/1089732
1 interface is down!
```

Net-SNMP Command Line Tools (cont'd)

- Configuration tools
  - snmpconf
    - snmpconf
    - snmpconf -g basic_setup
  - snmpusm
    - User management tool
    - snmpusm [options] passwd OLD-PASSWD NEW-PASSWD <USER>
  - snmpvacm
    - snmpvacm [options] createSec2group MODEL SEC_NAME GRP_NAME

References

- (中國書）深入理解 Net-SNMP 張春強 機械工業出版社
- man pages
- http://nicku.org/snm/lectures/snmp-v3/snmp-v3-8up.pdf