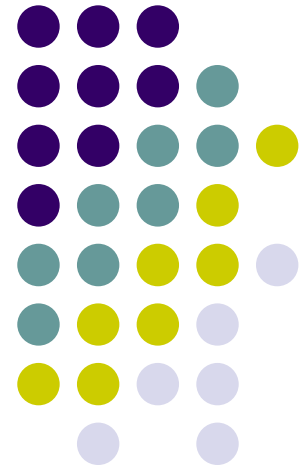


SNMP Tutorial

Karl Quinn

23rd November 2004

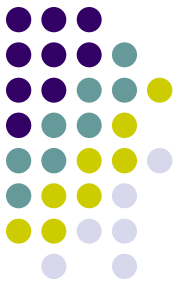
NDS M.Sc.





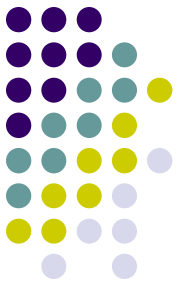
Tutorial Overview

- Introduction
- Management Information Base (MIB)
- Simple Network Management Protocol (SNMP)
- SNMP Commands
- Tools
 - 'SNMPwalk' (CLI)
 - 'MIB Browser' (GUI)



Introduction

- (1) **SNMP**
 - Application-layer protocol for managing TCP/IP based networks.
 - Runs over UDP, which runs over IP
- (2) NMS (Network Management Station)
 - Device that pools SNMP agent for info.
- (3) **SNMP Agent**
 - Device (e.g. Router) running software that understands SNMP language
- (4) **MIB**
 - Database of info conforming to SMI.
- (5) SMI Structure of Management Information
 - Standard that defines how to create a MIB.



MIB – Management Information Base

● MIB Breakdown...

- **OBJECT-TYPE**
 - String that describes the MIB object.
 - Object Identifier (OID).
- **SYNTAX**
 - Defines what kind of info is stored in the MIB object.
- **ACCESS**
 - READ-ONLY, READ-WRITE.
- **STATUS**
 - State of object in regards the SNMP community.
- **DESCRIPTION**
 - Reason why the MIB object exists.

Standard MIB Object:

sysUpTime **OBJECT-TYPE**

SYNTAX Time-Ticks

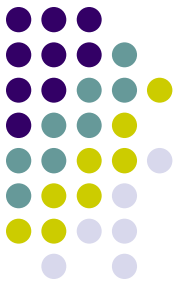
ACCESS read-only

STATUS mandatory

DESCRIPTION

“Time since the network management portion of the system was last re-initialised.

::= {system 3}



MIB – Management Information Base

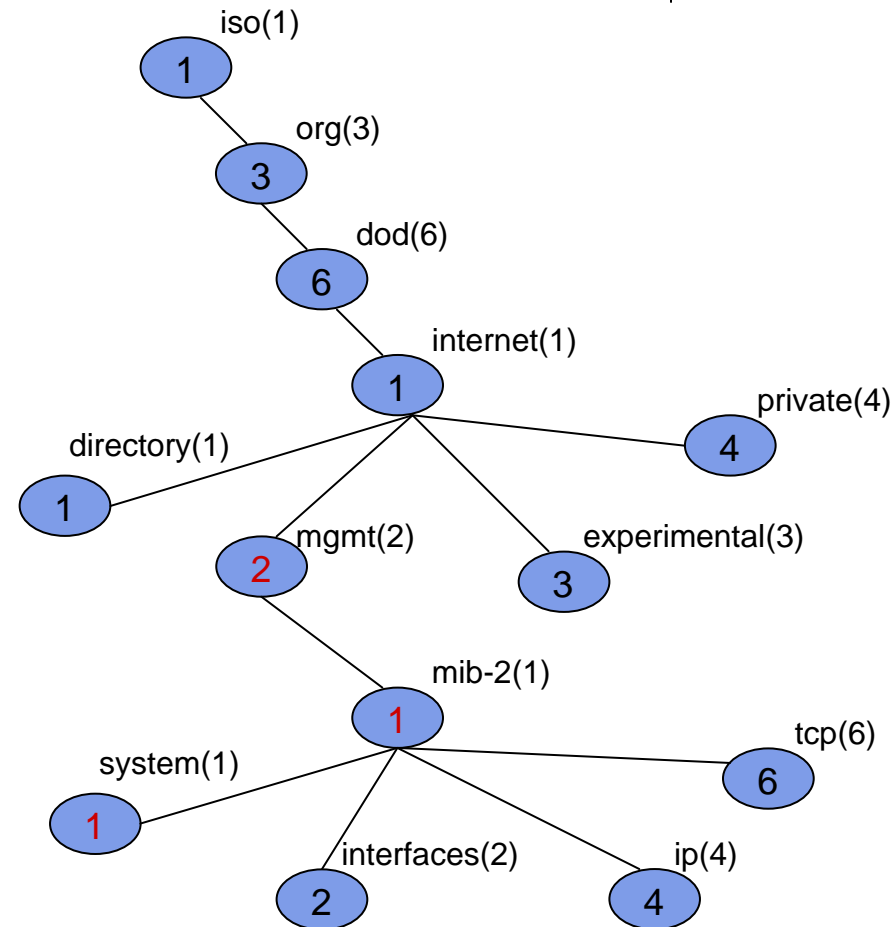
- Object Identifier (OID)

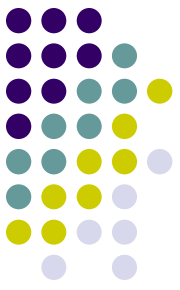
- Example .1.3.6.1.2.1.1

- iso(1) org(3) dod(6) internet(1)
 mgmt(2)
 mib-2(1)
 system(1)

Note:

- .1.3.6.1 ~100% present.
- mgmt and private most common.
- MIB-2 successor to original MIB.
- STATUS 'mandatory', All or nothing in group

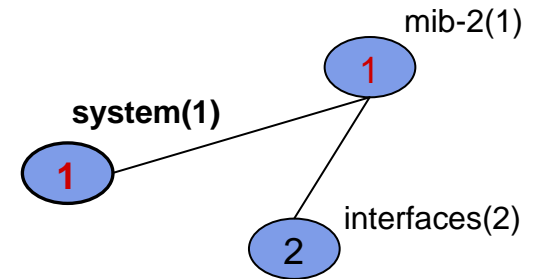




MIB – Management Information Base

- **system(1) group**

- Contains objects that describe some basic information on an entity.
- An entity can be the agent itself or the network object that the agent is on.



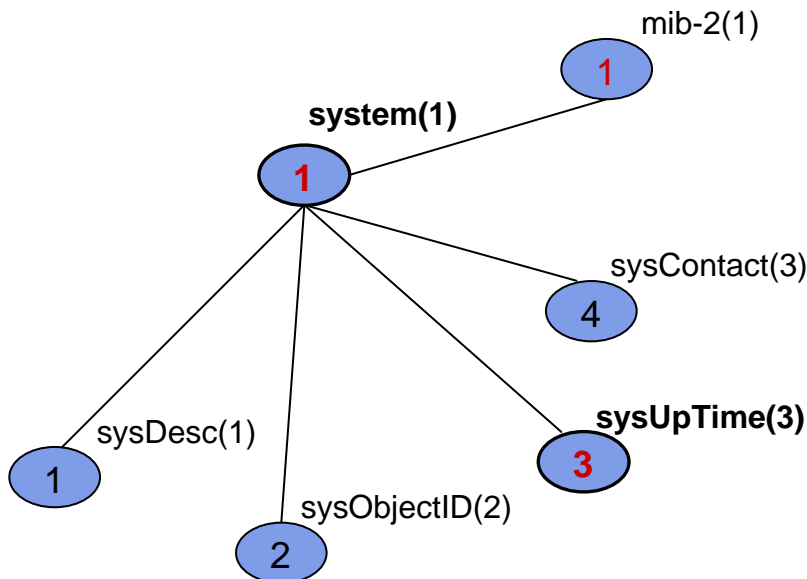
- **system(1) group objects**

- **sysDescr(1)** → Description of the entity.
- **sysObjectID(2)** → Vendor defined OID string.
- **sysUpTime(3)** → Time since net-mgt was last re-initialised.
- **sysContact(4)** → Name of person responsible for the entity.

MIB – Management Information Base



MIB - tree view



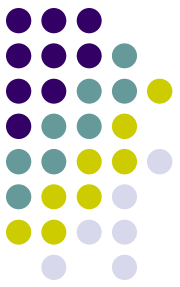
MIB - syntax view

sysUpTime **OBJECT-TYPE**
SYNTAX INTEGER
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 }

MIB – Management Information Base

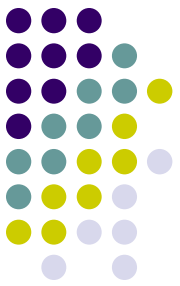


- SNMP Instances

- Each MIB object can have an instance.
 - A MIB for a router's (entity) interface information...

iso(1) org(3) dod(6) internet(1) mgmt(2) mib-2(1) interfaces(2) **ifTable(2)** **ifEntry(1)** ifType(3)

- Require one ifType value per interface (e.g. 3)
- One MIB object definition can represent multiple instances through Tables, Entries, and Indexes.

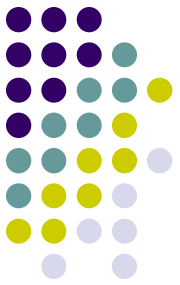


MIB – Management Information Base

- Tables, Entries, and Indexes.
 - Imagine tables as spreadsheets...
 - Three interface types require 3 rows (index no.s)
 - Each column represents a MIB object, as defined by the entry node.

ENTRY + INDEX = INSTANCE

	ifType(3)	ifMtu(4)	Etc...
Index #1	ifType.1[6]	ifMtu.1	
Index #2	ifType.2:[9]	ifMtu.2	
Index #3	ifType.3:[15]	ifMtu.3	



MIB – Management Information Base

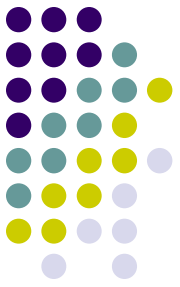
- Example MIB Query...
- If we queried the MIB on ifType we could get:
 - ifType.1 : 6
 - ifType.2 : 9
 - ifType.3 : 15

Which corresponds to...

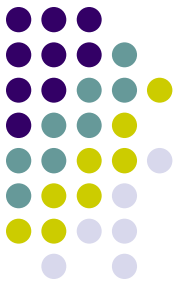
- ifType.1 : ethernet
- ifType.2 : tokenRing
- ifType.3 : fddi

```
ifType OBJECT-TYPE
      SYNTAX INTEGER {
        other(1),
        ethernet(6),
        tokenRing(9)
        fddi(15),
        ... }
      etc...
```

Simple Network Management Protocol

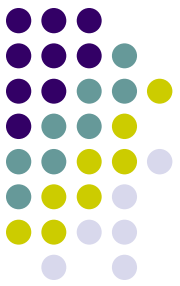


- Retrieval protocol for MIB.
- Can retrieve by
 - CLI (snmpwalk),
 - GUI (MIB Browser), or
 - Larger applications (Sun Net Manager) called Network Management Software (NMS).
- NMS collection of smaller applications to manage network with illustrations, graphs, etc.
- NMS run on Network Management Stations (also NMS), which can run several different NMS software applications.



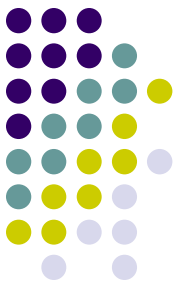
SNMP Commands

- SNMP has 5 different functions referred to as Protocol Data Units (PDU's), which are:
 - (1) GetRequest, aka Get
 - (2) GetNextRequest, aka GetNext
 - (3) GetResponse, aka Response
 - (4) SetRequest, aka Set
 - (5) Trap



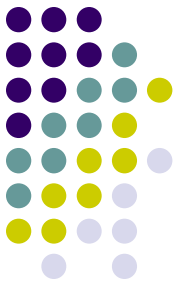
SNMP Commands [Get]

- GetRequest [Get]
 - Most common PDU.
 - Used to ask SNMP agent for value of a particular MIB agent.
 - NMS sends out 1 Get PDU for each instance, which is a unique OID string.
 - What happens if you don't know how many instances of a MIB object exist?



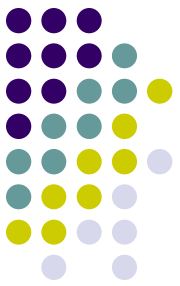
SNMP Commands [GetNext]

- **GetNextRequest [GetNext]**
 - NMS application uses GetNext to ‘walk’ down a table within a MIB.
 - Designed to ask for the OID and value of the MIB instance that comes after the one asked for.
 - Once the agent responds the NMS application can increment its count and generate a GetNext.
 - This can continue until the NMS application detects that the OID has changed, i.e. it has reached the end of the table.



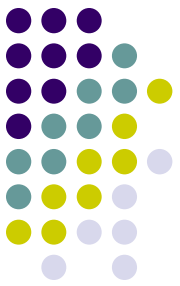
SNMP Commands [GetResponse]

- GetResponse [Response]
 - Simply a response to a Get, GetNext or Set.
 - SNMP agent responds to all requests or commands via this PDU.



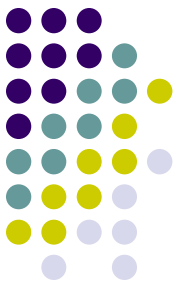
SNMP Commands [SetRequest]

- SetRequest [Set]
 - Issued by an NMS application to change a MIB instance to the variable within the Set PDU.
 - For example, you could issue a
 - GetRequest against a KDEG server asking for sysLocation.0 and may get 'ORI' as the response.
 - Then, if the server was moved, you could issue a Set against that KDEG server to change its location to 'INS'.
 - You must have the correct permissions when using the set PDU.



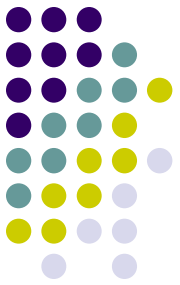
SNMP Commands [Trap]

- Trap
 - Asynchronous notification.
 - SNMP agents can be programmed to send a trap when a certain set of circumstances arise.
 - Circumstances can be view as thresholds, i.e. a trap may be sent when the temperature of the core breaches a predefined level.



SNMP Security

- SNMP Community Strings (like passwords)
 - 3 kinds:
 - READ-ONLY: You can send out a Get & GetNext to the SNMP agent, and if the agent is using the same read-only string it will process the request.
 - READ-WRITE: Get, GetNext, and Set. If a MIB object has an ACCESS value of read-write, then a Set PDU can change the value of that object with the correct read-write community string.
 - TRAP: Allows administrators to cluster network entities into communities. Fairly redundant.



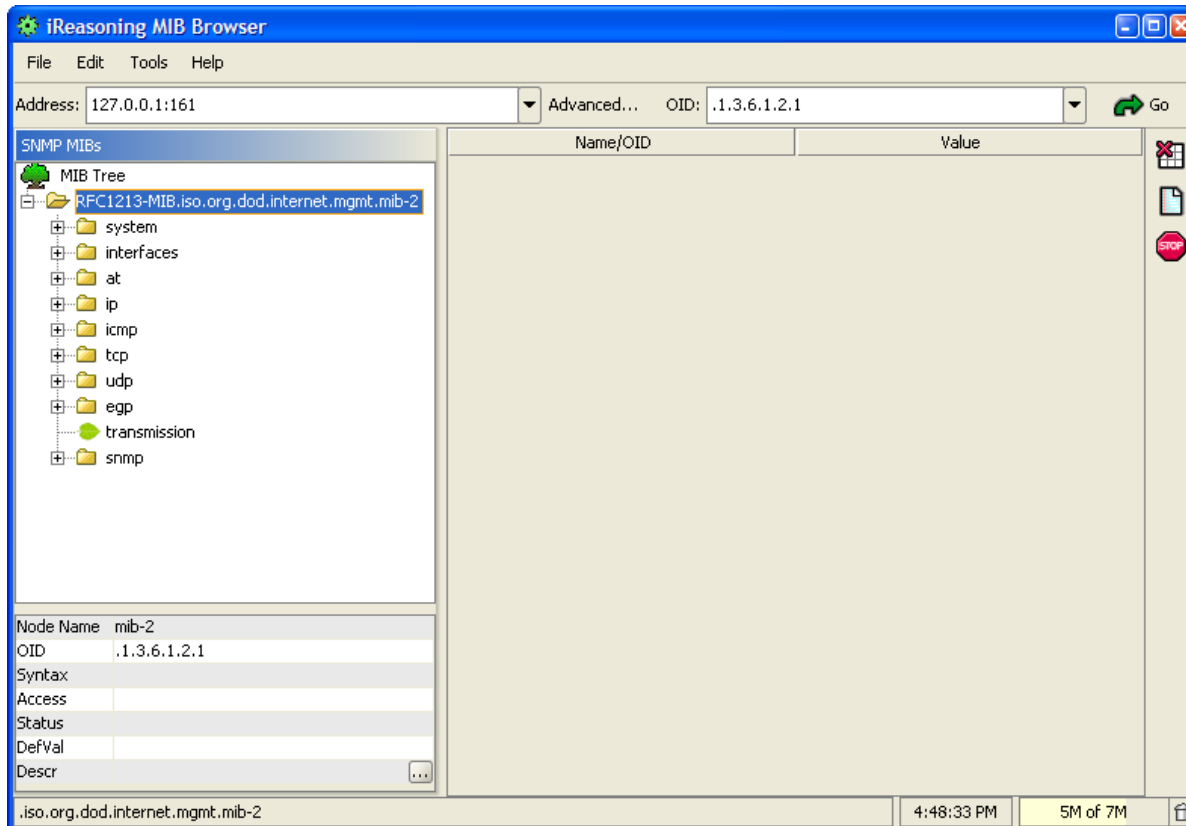
SNMP Tools

- Command Line Interface
 - e.g. 'snmpwalk'
- Graphical User Interface
 - e.g. iReasoning's MIB Browser
 - <http://209.59.152.192/download/mibpro/mibbrowser.zip>
 - Or via www.ireasoning.com



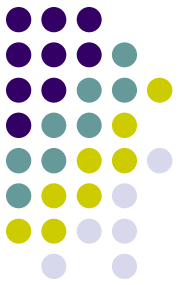
SNMP – MIB Browser (1)

- Initial set-up... `java -Xmx384m -jar "XYZ\lib\browser.jar"` (where XYZ = your specific path)



Breakdown...

- LHS is the SNMP MIB structure.
- Lower LHS has details of MIB structure.
- RHS will present MIB values.



SNMP – MIB Browser (2)

IP address	sysDescr	sysObjectID	sysUpTime	sysContact	sysName	sysLocation
134.XXX.XXX.XXX	HP ETHERNET...	.1.3.6.1.4.1....	106434260		laserjet8	DSG, O'Reilly I...
134.XXX.XXX.XXX						
134.XXX.XXX.XXX						
134.XXX.XXX.XXX						
134.XXX.XXX.XXX						
134.XXX.XXX.XXX	Lexmark T630...	.1.3.6.1.4.1....	86441184		LXKE8183D	
134.XXX.XXX.XXX						
134.XXX.XXX.XXX						

Checking 134.226.36.3...

Discovery...

- Subnet: 134.XXX.XXX.*

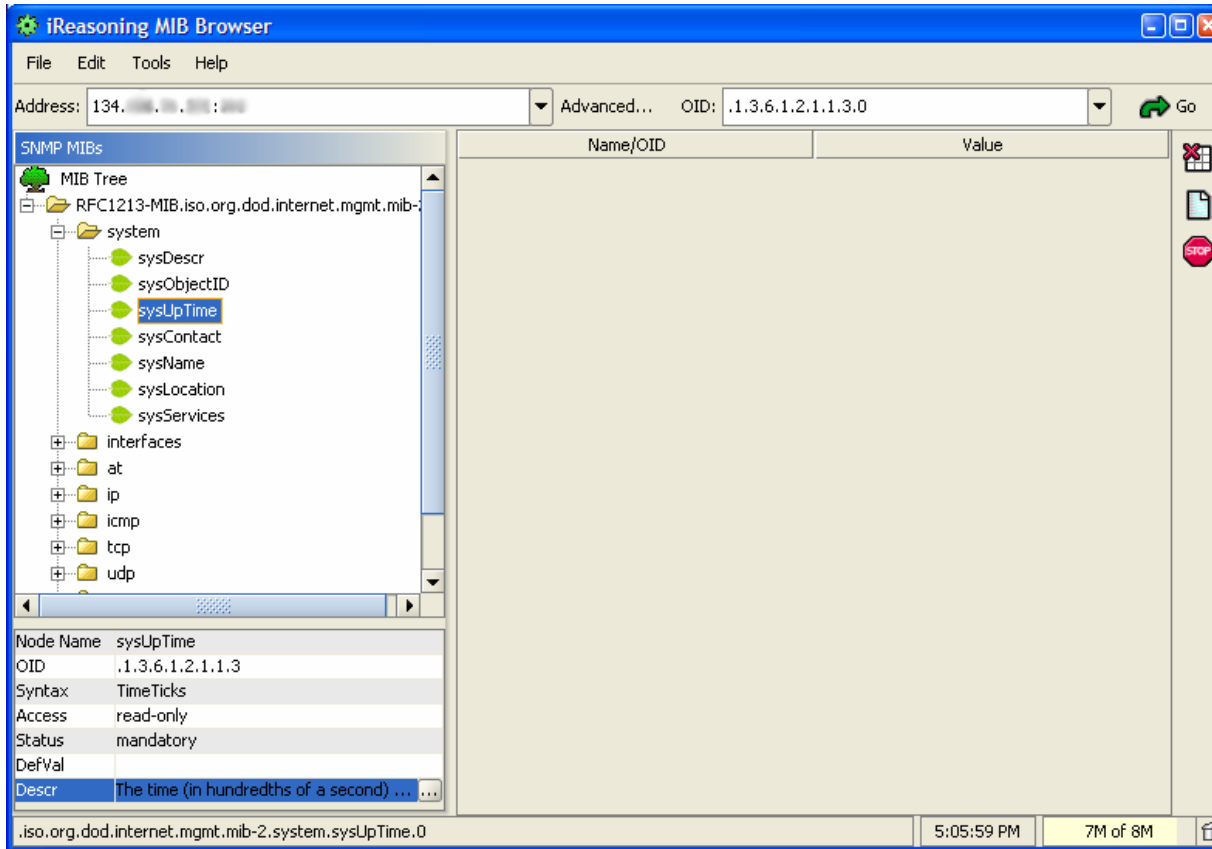
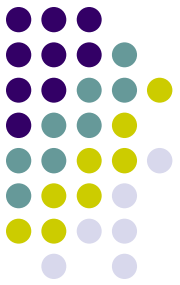
- Read Community: public

→ Start

Note IP Address.

← Stop

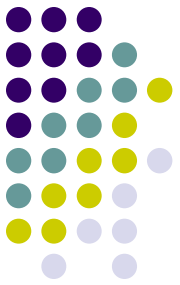
SNMP – MIB Browser (3)



Navigation...

- MIB Tree
 - System
 - sysUpTime
- Notice Lower LHS
- Notice OID

SNMP – MIB Browser (4)



Name/OID	Value
sysUpTime.0	106494930

Node Name	sysUpTime
OID	.1.3.6.1.2.1.1.3
Syntax	TimeTicks
Access	read-only
Status	mandatory
DefVal	
Descr	The time (in hundredths of a second) ...

SNMP PDU's...

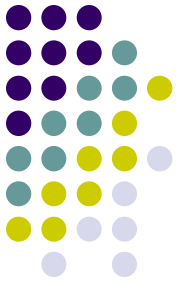
(1) Get

- Select 'Go'
→ 'Get'

- RHS has values.

- OID – Value

SNMP – MIB Browser (5)



Address: 134... Advanced... OID: .1.3.6.1.2.1.1.5.0 Go

SNMP MIBs

MIB Tree

- RFC1213-MIB.iso.org.dod.internet.mgmt.mib-2
 - system
 - sysDescr
 - sysObjectID
 - sysUpTime
 - sysContact
 - sysName
 - sysLocation
 - sysServices
 - interfaces
 - at
 - ip
 - icmp
 - tcp
 - udp

Name/OID	Value
sysLocation.0	DSG, O'Reilly Institute, F.35

Node Name sysName
OID .1.3.6.1.2.1.1.5
Syntax DisplayString (SIZE (0,255))
Access read-write
Status mandatory
DefVal
Descr An administratively-assigned name for...

.iso.org.dod.internet.mgmt.mib-2.system.sysName.0 5:14:37 PM 7M of 8M

SNMP PDU's...

(2) GetNext

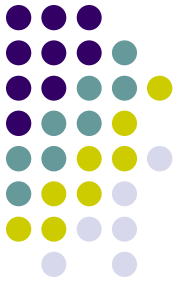
-Selected OID is:
.1.3.6.1.2.1.1.5

-Returned value:
(.1.3.6.1.2.1.1.6)

or

“DSG, O'Reilly Institute,
F.35”

SNMP – MIB Browser (6)



Name/OID	Value
sysDescr.0	HP ETHERNET MULTI-ENVIRONMENT,RC
sysObjectID.0	.1.3.6.1.4.1.11.2.3.9.1
sysUpTime.0	106543680
sysContact.0	
sysName.0	laserjet8
sysLocation.0	DSG, O'Reilly Institute, F.35
sysServices.0	79

SNMP...

(3) Get SubTree

-Position of MIB:

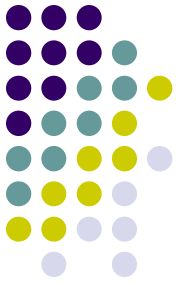
.1.3.6.1.2.1.1

(a.k.a. system)

-RHS values:

Returns all values
below system.

SNMP – MIB Browser (7)



The screenshot shows the iReasoning MIB Browser interface. The address bar is set to 134.100.100.100 and the OID is .1.3.6.1.2.1. The MIB tree on the left shows the path: RFC1213-MIB.iso.org.dod.internet.mgmt.mib-2 > system > sysServices. The table on the right lists various MIB objects and their values. A context menu is open over the table, with the 'Walk' option highlighted.

Name/OID	Value
sysDescr.0	HP ETHERNET MULTI-ENVIRONMENT,ROM
sysObjectID.0	.1.3.6.1.4.1.11.2.3.9.1
sysUpTime.0	106564230
sysContact.0	
sysName.0	laserjet8
sysLocation.0	DSG, O'Reilly Institute, F.35
sysServices.0	79
ifNumber.0	2
ifIndex.1	1
ifIndex.2	2
ifDescr.1	HP ETHERNET MULTI-ENVIRONMENT,ROM ...
ifDescr.2	HP ETHERNET MULTI-ENVIRONMENT,ROM ...
ifType.1	ethernet-csmacd
ifType.2	softwareLoopback
ifMtu.1	1500
ifMtu.2	32768
ifSpeed.1	10000000
ifSpeed.2	0
ifPhysAddress.1	0x00 0x30 0xC1 0xCC 0x1B 0x85
ifPhysAddress.2	
ifAdminStatus.1	up
ifAdminStatus.2	up
ifOperStatus.1	up
ifOperStatus.2	up
ifLastChange.1	0
ifLastChange.2	0
ifToOctets.1	741500316

SNMP...

(4) Walk

-MIB Location:

.1.3.6.1.2.1

(a.k.a. mib-2)

- Returns ***ALL***
values under mib-
2

SNMP – MIB Browser (8)



The screenshot shows the iReasoning MIB Browser interface. The address bar is set to 134.1.1.1. The MIB tree on the left shows the path: RFC1213-MIB.iso.org.dod.internet.mgmt. > system > interfaces > ifTable. A context menu is open over the ifTable node, with options: Get, Get Next, Set, Get Subtree, Walk, Table View (highlighted), and Graph. The main pane shows a table with columns 'Name/OID' and 'Value'. The status bar at the bottom indicates the path: .iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable and the time: 6:25:35 PM.

Tables...

- MIB Location:
.1.3.6.1.2.1.2.2
(or interfaces)

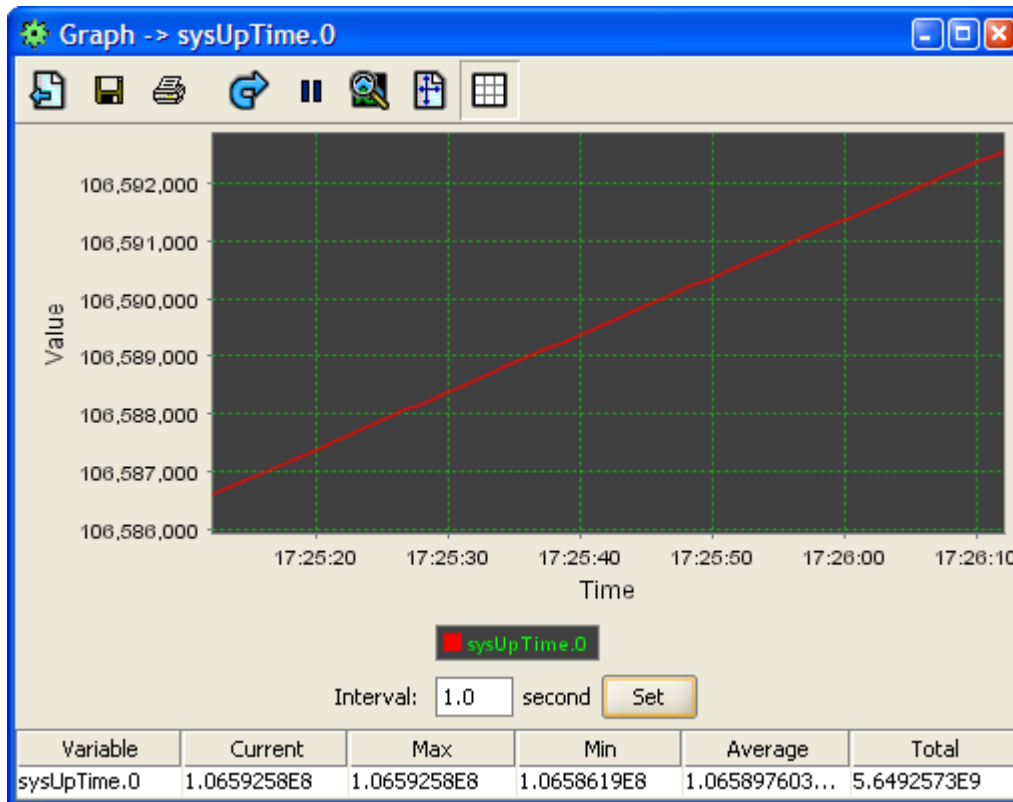
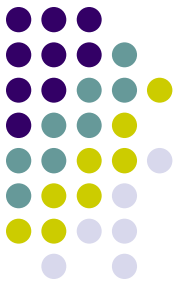
- Select ifTable,
→ Go, then Table
View.

- Refresh/Poll

The screenshot shows the ifTable window with a table of interface data. The table has columns: ifDescr, ifType, ifMtu, ifSpeed, ifPhysAddress, ifAdminStatus, ifOperStatus, ifLastChange, ifInOctets, ifInUcastPkts, ifInNUcastPkts, ifInDiscards, ifInErrors, ifOutOctets, ifOutUcastPkts, ifOutNUcastPkts, and ifSpecific. The data is as follows:

...	ifDescr	ifType	ifMtu	ifSpeed	ifPhysAddress	ifAdminStatus	ifOperStatus	ifLastChange	ifInOctets	ifInUcastPkts	ifInNUcastPkts	ifInDiscards	ifInErrors	if...	ifOutOctets	ifOutUcastPkts	ifOutNUcastPkts	...	if...	...	ifSpecific
1	HP ETHERNET ...	ethernet-c...	1500	10000000	0x00 0x30 0x...	up	up	0	745482794	296035	4721623	92005	0	0	14196063	125605	27265	0	0	0	.0.0
2	HP ETHERNET ...	software...	32768	0		up	up	0	4294967295	572	0	0	0	0	4294967295	572	0	0	0	0	.0.0

SNMP – MIB Browser (9)



SNMP...

- Graph
- Select a value from the RHS, say sysUpTime
- Highlight and select 'Go', then 'Graph'.
- Interval = 1s
→ set.