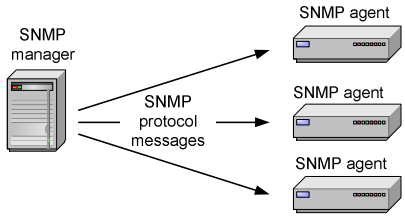
Protocoale de nivel aplicaţie:

SNMP

SNMP



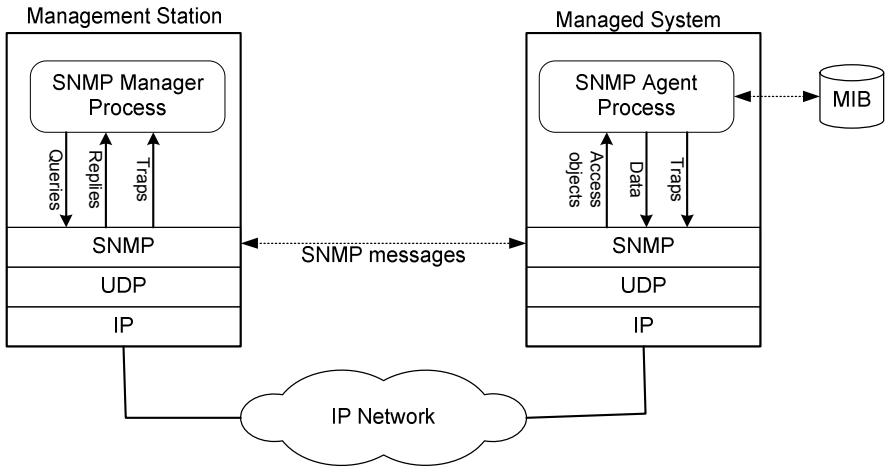
Protocol de nivelul 7: *Simple Network Management Protocol*
compus din 3 entităţi:

- *SNMP manager*
  - poate fi un ruter sau alte echipament de monitorizare (PC cu soft specific)
  - managerul interacţionează cu agenţii prin mesaje SNMP
- *SNMP agent*
  - echipamentele de reţea monitorizate sînt agenţi: rutere, switchuri etc
- *Management Information Base (MIB)*
  - agenţii conţin variabile MIB
  - managerul poate interoga valorile variabilelor, sau le poate schimba

Istoric

- *1983* - TCP/IP, apariţia internetului
- *1987* - ISO OSI propune **CMIP** - Common Management Information Protocol, şi **CMOT** (CMIP over TCP) ca protocoale de network management
- *Nov. 1987* - **SGMP** - Simple Gateway Monitoring protocol (*RFC 1028*)
- *1989* - Marshall T. Rose conduce **SNMP** working group pentru a crea un cadru comun de network management care să fie folosit de **SGMP** şi **CMOT** şi în perspectivă să permită tranziţia către **CMOT**
- *Aug. 1989* - "**Internet-standard Network Management Framework**" definit (*RFCs 1065, 1066, 1067*)
- *Apr. 1989* - **SNMP** avansat la ***recommended*** status, devenind cadru de management de facto în network management TCP/IP (*RFC 1098*)
- *June 1989* - commitetul IAB decide ca **SNMP** şi **CMOT** să fie dezvoltate separat
- *May 1990* - IAB avansează SNMP la statutul de **standard protocol with a recommended status** (*RFC 1157*)
- *Mar. 1991* - formatul MIBs şi traps definit (*RFCs 1212, 1215*)
- formatul TCP/IP MIB actualizat pentru a crea **SNMPv1** (RFC 1213)
- **SNMPv2**: 1996
- **SNMPv3**: 2002 (2004: RFC3411-3418)

Interacţiuni în SNMP



MIB

- O structură de date cu scopul de a stoca variabilele accesibile prin SNMP, numite obiecte
- Un MIB specifică “obiectele” cu care managerul interacţionează
- MIB este un fişier text, care descrie obiectele folosind sintaxa ASN.1 (Abstract Syntax Notation nr. 1)
- Este structurat arborescent, asemenea unui sistem de fişiere
- ASN.1 este un limbaj de descriere formală

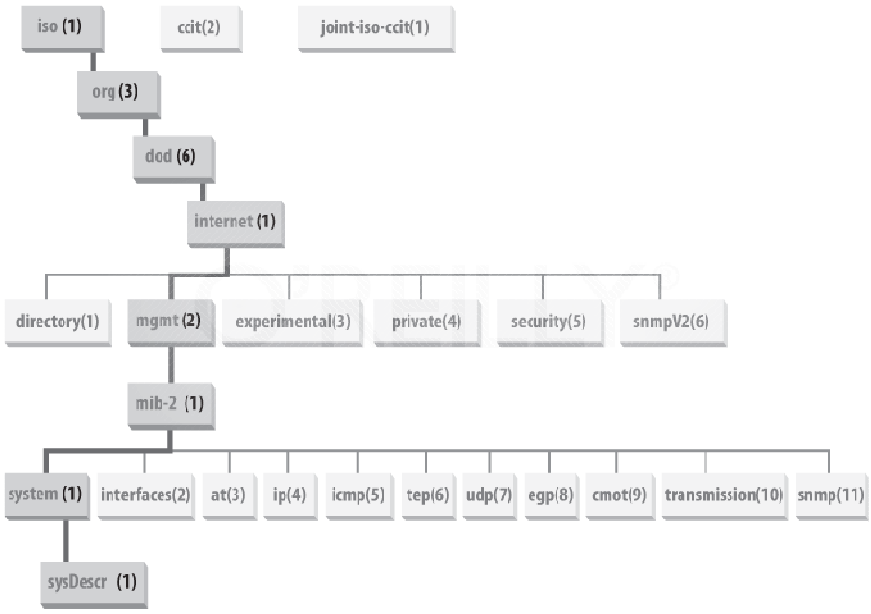
Obiecte

- Un obiect este reprezentat de un *object identifier (OID)*
- Un OID este specificatr într-un fişier text de tip MIB.
- Un OID e reprezentat de o serie de etichete (prescurtate prin numere), despărţite prin puncte:

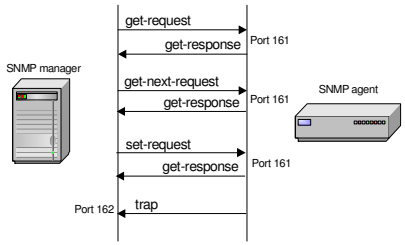
  Exemple echivalente:
  - *1.3.6.1.2.1.4.6.*
  - *iso.org.dod.internet.mgmt.mib-2.ip.ipForwDatagrams*

- Cînd un manager cere un obiect de la un agent, îi specifică OID-ul acestuia.

Ierarhia OID



Protocolul SNMP



- UDP/161
- UDP/162 pentru *trap*

- Model: *request-response*
- Mesajele *trap* sînt singurele fără confirmare

Mesaje (primitive de protocol) SNMP

- **Get-request.** Cere valoarea unuia sau mai multor OID
- **Get-next-request.** Cere valoarea următorului OID, conform ordonării OID în MIB.
- **Set-request.** Cere modificarea valorii unui OID

- **Get-response.** Răspuns de la agent către manager pentru cele 3 pachete de mai sus.

- **Trap.** Notificare trimisă de un agent în urma apariţiei unui eveniment.
- **Inform request.** *(doar începînd cu SNMPv2)* Notificare gen trap, fiabilă (confirmată)

Mesajele *Inform request* solicită mai multe resurse: trebuie memorate pînă la confirmare, confirmările generează trafic suplimentar, etc

Mesaje TRAP

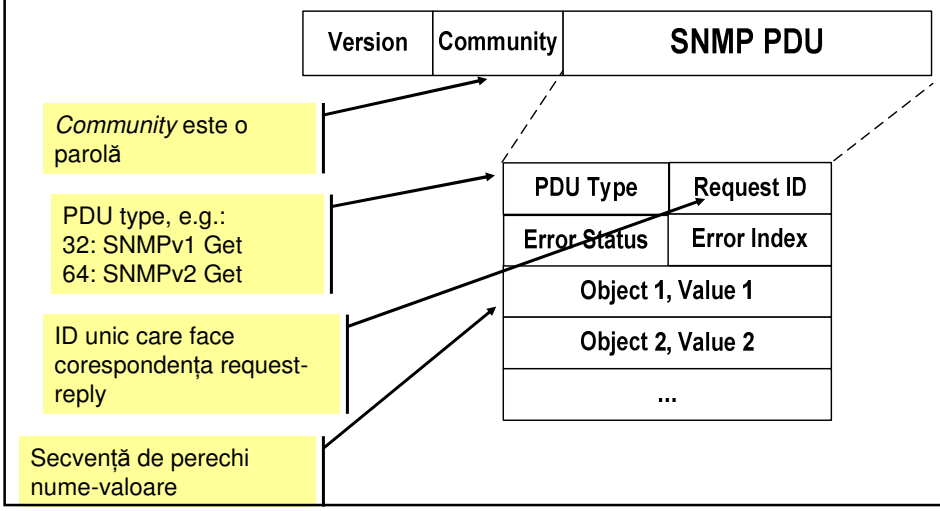
- Sînt mesaje asincrone, de la agent la manager
- Exemple de TRAP:
  - linkDown: interfaţa este “down”
  - coldStart – restartare neaşteptată (poate fi un “system crash”)
  - warmStart - soft reboot
  - linkUp - opusul linkDown
  - (SNMP) AuthenticationFailure
  - …

Versiuni SNMP

- 3 versiuni:
  - SNMPv1 (1990)
  - SNMPv2c (1996)
    - *Adaugă funcţia "GetBulk" function şi cîteva tipuri noi*
    - *Adaugă capabilitatea RMON (remote monitoring)*
  - SNMPv3 (2002)
    - *SNMPv3 bazat pe SNMPv1 (nu SNMPv2c)*
    - *Introduce aspecte de securitate şi autentificare*
- Toate versiunile sînt în folosinţă şi azi
- Versiunea 2c este varianta dintre multiplele versiuni 2 propuse, care a fost acceptată
- Mulţi agenţi şi manageri suportă toate cele 3 versiuni.

Formatul mesajelor SNMP

- SNMPv1 Get/Set:



Securitatea SNMP

- SNMPv1 foloseşte parole de tip *plain-text* numite *communities*
  parolele sînt transmise în clar în mesajele SNMP
  securitate f. redusă: *Security Not My Problem*

- SNMPv2 : s-a intenţionat adăugarea de elemente de securitate, dar efortul de standardizare a eşuat ("c" vine de la "*community*")

- SNMPv3 are numeroase elemente de securitate:
  - Asigurarea că un pachet nu a fost alterat (**integritate**),
  - Asigurarea că sursa pachetului este cea care pretinde că este (**autentificare**)
  - Asigurarea că un mesaj nu poate fi citit decît de destinatar (***privacy***).

Comunităţi

- RO (read-only)
  admite doar interogări

- RW (read-write)
  admite şi operaţii SET

setarea aceluiaşi *nume* de comunitate în agent şi în manager echivalează cu cunoaşterea parolei

Exemplu:
community *public* ro
community *private* rw

Modelul de securitate SNMP v3

- 2 componente:
  1. SNMP v3 dă acces userilor şi nu comunităţii.
  2. Accesul poate fi limitat la porţiuni din MIB (V*ersion-based Access Control Module* (VACM). Drepturile de acces pot fi limitate prin:
     - Specificarea unui domeniu de adrese IP valid pentru un user sau o comunitate
     - Specifiarea părţii din "arborele" MIB care poate fi accesată

Nivele de securitate în SNMP v2/v3

SNMP v1, v2c:

- *SNMPv1, SNMPv2*: autentificare pe baza potrivirii numelui comunităţii

SNMP v3 are 3 nivele de securitate:

- *noAuthNoPriv*: autentificare pe baza potrivirii numelui comunităţii.
- *authNoPriv*: Autentificare cu MD5 sau SHA.
- *authPriv:* Authenticare cu MD5 sau SHA şi criptare cu DES

MIB

- Există un sg. MIB = 1 arbore
- MIB conţine obiecte
- Unele obiecte sînt standard (RFC), ex: *sysUpTime*; altele depind de producător
- Orice producător poate insera obiecte în MIB (tipic în categoria "private") şi publică secţiunea respectivă de MIB (numită "modul MIB"); formează categoria *Enterprise*

Obiect MIB:

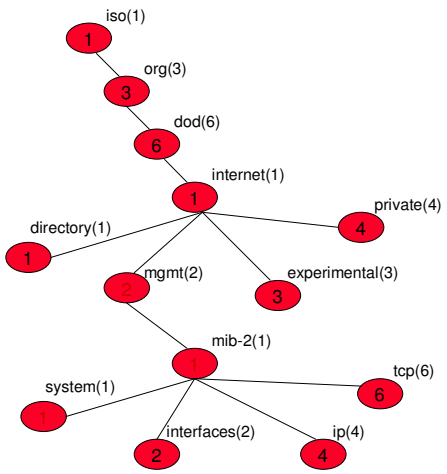
sysUpTime **OBJECT-TYPE**
SYNTAX Time-Ticks
ACCESS read-only
STATUS mandatory
DESCRIPTION
"Time since the network management portion of the system was last re-initialised.
::= {system 3}

- Conţinut MIB …

- 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.
- ::= {system 3}
  - Is the third branch off of the system object group tree

MIB

- Object IDentifier (OID)
- - Exemplu .1.3.6.1.2.1.1
- - iso(1) org(3) dod(6) internet(1)
- mgmt(2)
- mib-2(1)
- system(1)

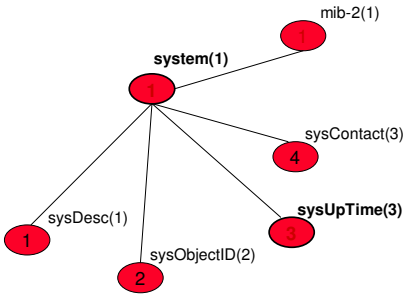


OBS :

- - .1.3.6.1 există 100%.
- - mgmt şi private: cele mai întîlnite.

MIB

MIB - arbore

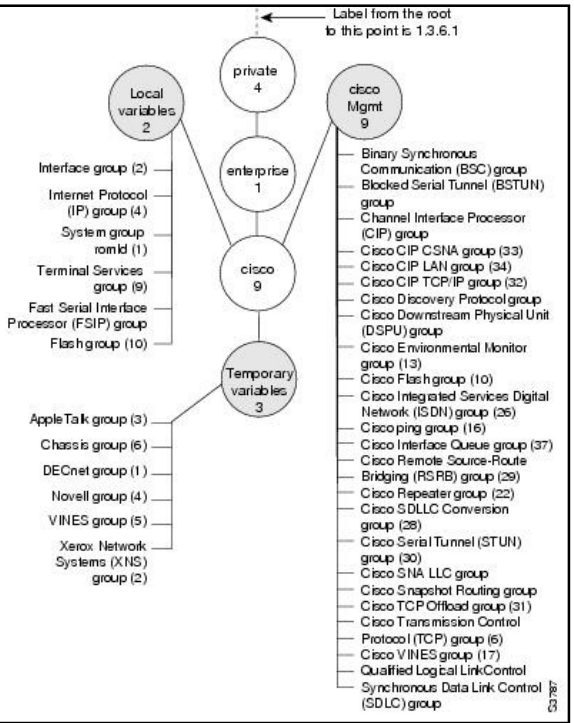


MIB - sintaxa

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

- Exemplu: Enterprise/**Cisco** (1.3.6.1.4.1.**9**)
- Conţine 3 ramuri (sub-arbori)



MIB

iso.org.dod.internet.private.IOS.cisco.
ciscoMgmt variables.ping.group
1.3.6.1.4.1.9.9.16.1.1.1 [*MIB Variable*]

ciscoPingTable

Detaliere din grupul *management*

ciscoPingSerialNumber [**1**]
ciscoPingProtocol [**2**]
ciscoPingAddress[**3**]
ciscoPingPacketCount [**4**]
ciscoPingPacketSize[**5**]
ciscoPingPacketTimeout[**6**]
ciscoPingDelay[**7**]
ciscoPingTrapOnCompletion[**8**]
ciscoPingSentPackets[**9**]
ciscoPingReceivedPackets[**10**]
ciscoPingMinRtt[**11**]
ciscoPingAvgRtt[**12**]
ciscoPingMaxRtt[**13**]
ciscoPingCompleted[**14**]
ciscoPingEntryOwner[**15**]
ciscoPingEntryStatus[**16**]

S2978

MIB

- Instanţe SNMP
- Fiecare obiect MIB poate avea o instanţă
  - un MIB pentru o interfaţă a unui ruter…
- iso(1) org(3) dod(6) internet(1) mgmt(2) mib-2(1) interfaces(2) **ifTable(2) ifEntry(1)** ifType(3)
  - necesară o valoare *ifType* per interfaţă (de ex. 3)
  - O definiţie a unui obiect MIB poate reprezenta multiple instanţe prin *Tables, Entries, Indexes* (Tabele, Intrări, Indexuri)

MIB

- *Tables, Entries, Indexes.*
- *tables* echivalează cu *spreadsheets*…
  - 3 tipuri de interfeţe echivalează cu 3 rînduri = 3 *index*-uri
  - fiecare coloană reprezintă un obiect MIB, definit de *entry* (intrare)

ENTRY + INDEX = INSTANCE

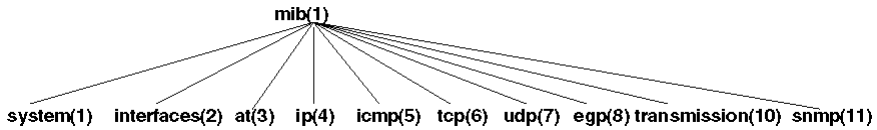
	ifType(3)	**ifMtu(4)**	**Etc…**
Index #1	ifType.1[**6**]	ifMtu.1	
Index #2	ifType.2:[**9**]	ifMtu.2	
Index #3	ifType.3:[**15**]	ifMtu.3	

MIB

- Exemplu MIB *Query*…
- Un *query* pe MIB pentru *ifType* ne întoarce:
  - ifType.1 : 6
  - ifType.2 : 9
  - ifType.3 : 15
  - corespondenţa:
  - ifType.1 : ethernet
  - ifType.2 : tokenRing
  - ifType.3 : fddi

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

Obiecte în 1.3.6.1.2.1 (MIB-2)



system	*1.3.6.1.2.1.1*	Defines a list of objects of system operation: sys uptime, sys contact, and sys name
interfaces	*1.3.6.1.2.1.2*	It monitors interfaces are up/down and # octets sent/received, errors and discards…
at	*1.3.6.1.2.1.3*	The address translation
ip	*1.3.6.1.2.1.4*	Keeps track of many aspects of IP, including IP routing.
icmp	*1.3.6.1.2.1.5*	Tracks things such as ICMP errors, discards, etc.
tcp	*1.3.6.1.2.1.6*	Tracks, sockets, the state of the TCP connection (e.g., *closed*, *listen*, *synSent*, etc.).
udp	*1.3.6.1.2.1.7*	Tracks UDP statistics, datagrams in and out, etc.
egp	*1.3.6.1.2.1.8*	Tracks various statistics about EGP and keeps an EGP neighbor table.
host	*1.3.6.1.2.1.25*	Host: filesystems, media, memory, CPU, disks, Installed Software, all process etc.

MIB-2

Interface (1.3.6.1.2.1.2):

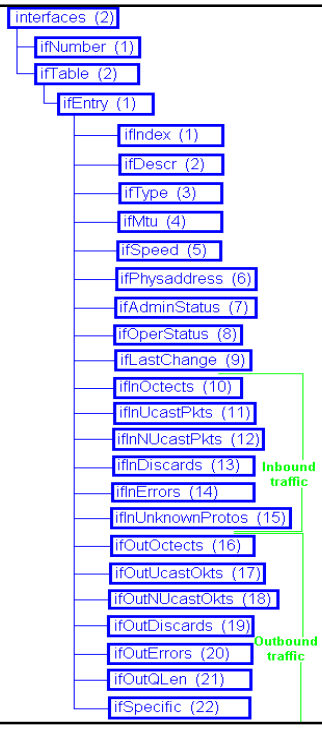
Trafic TCP/IP în cadrul ifMIB:

- **•ifInOctets –**număr de octeţi recepţionaţi de interfaţă.
- **•ifOutOctets –** Număr de octeţi transmişi de interfaţă
- **•ifInNUcastPkts –**numărul de pachete non-unicast trimise spre o entitate de protocol superioară

Exemplu:

$ snmpget kryklinuxm iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifInOctets

Counter32: 578697860



ASN.1

ASN.1 (Abstract Syntax Notation 1) este un limbaj care prezintă similarităţi cu C.

Exemple:

```
-- 2 liniuţe reprezintă un comentariu– Echivalentul C este scris după --
MostSevereAlarm ::= INTEGER          -- typedef MostSevereAlarm int;
circuitAlarms MostSevereAlarm ::= 3  -- MostSevereAlarm circuitAlarms = 3;
MostSevereAlarm ::= INTEGER (1..5)   -- specifică domeniul de valori
ErrorCounts ::= SEQUENCE {
   circuitID              OCTET STRING,
   erroredSeconds         INTEGER,
   unavailableSeconds     INTEGER
}   -- structurile de date se definesc cu cuvîntul cheie SEQUENCE
```

Tipuri de date în SNMP

- INTEGER -- signed 32-bit integer
- OCTET STRING
- OBJECT IDENTIFIER (OID)
- NULL -- valoare, nu tip de date

Culoare pentru termeni definiţi în ASN.1

Culoare pentru termeni definiţi în RFC 1155

- IpAddress -- OCTET STRING de 4B, network byte order (B.E.)
- Counter -- unsigned 32-bit integer (*rolls over*)
- Counter64 -- idem, 64 biţi, începînd cu SNMPv2
- Gauge -- unsigned 32-bit integer (*tops out*)
- TimeTicks -- unsigned 32-bit integer (*rolls over* după 497 zile)
- Opaque -- utilizat pt a crea tipuri de date care nu-s în SNMPv1
- DateAndTime, DisplayString, MacAddress, PhysAddress, TimeInterval, TimeStamp, TruthValue, VariablePointer – convenţii textuale utilizate ca tipuri

OIDs & MIBs

Exemplu de definiţie obiect în MIB:

```
sysContact OBJECT-TYPE          -- OBJECT-TYPE este un macro
    SYNTAX      DisplayString (SIZE (0..255))
    ACCESS      read-only       -- sau: read-write, write-only, not-accessible
    STATUS      mandatory       -- sau: optional, deprecated, obsolete
    DESCRIPTION
        "Ruter etaj 3 corp A"
    ::= { system 4 }
```

RFC relevante pentru SNMP

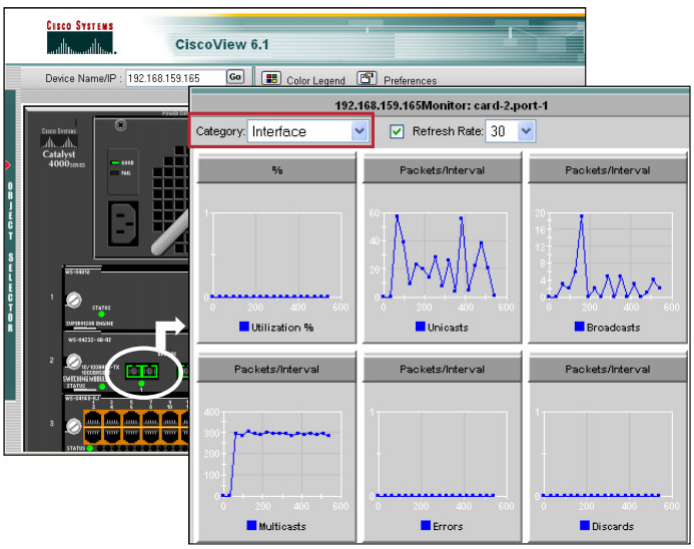
RFC	Description	Published	Current Status
1065	SMIv1	Aug-88	Obsoleted by 1155
1066	SNMPv1 MIB	Aug-88	Obsoleted by 1156
1067	SNMPv1	Aug-88	Obsoleted by 1098
1098	SNMPv1	Apr-89	Obsoleted by 1157
1155	SMIv1	May-90	Standard
1156	SNMPv1 MIB	May-90	Historic
1157	SNMPv1	May-90	Standard
1158	SNMPv1 MIB-II	May-90	Obsoleted by 1213
1212	SNMPv1 MIB definitions	Mar-91	Standard
1213	SNMPv1 MIB-II	Mar-91	Standard
1215	SNMPv1 traps	Mar-91	Informational
1351	Secure SNMP administrative model	Jul-92	Proposed Standard
1352	Secure SNMP managed objects	Jul-92	Proposed Standard
1353	Secure SNMP security protocols	Jul-92	Proposed Standard
1441	Introduction to SNMPv2	Apr-93	Proposed Standard
1442	SMIv2	Apr-93	Obsoleted by 1902
1443	Textual conventions for SNMPv2	Apr-93	Obsoleted by 1903
1444	Conformance statements for SNMPv2	Apr-93	Obsoleted by 1904
1445	SNMPv2 administrative model	Apr-93	Historic
1446	SNMPv2 security protocols	Apr-93	Historic
1447	SNMPv2 party MIB	Apr-93	Historic
1448	SNMPv2 protocol operations	Apr-93	Obsoleted by 1905
1449	SNMPv2 transport mapping	Apr-93	Obsoleted by 1906
1450	SNMPv2 MIB	Apr-93	Obsoleted by 1907
1451	Manger-to-manger MIB	Apr-93	Historic
1452	Coexistence of SNMPv1 and SNMPv2	Apr-93	Obsoleted by 1908
1901	Community-Based SNMPv2	Jan-96	Experimental
1902	SMIv2	Jan-96	Draft Standard
1903	Textual conventions for SNMPv2	Jan-96	Draft Standard
1904	Conformance statements for SNMPv2	Jan-96	Draft Standard
1905	Protocol operations for SNMPv2	Jan-96	Draft Standard
1906	Transport mapping for SNMPv2	Jan-96	Draft Standard
1907	SNMPv2 MIB	Jan-96	Draft Standard
1908	Coexistence of SNMPv1 and SNMPv2	Jan-96	Draft Standard
1909	Administrative infrastructure for SNMPv2	Feb-96	Experimental
1910	User-based security for SNMPv2	Feb-96	Experimental

NMS comerciale

NMS = Network Monitoring System (sau Management System)

•http://www.hp.com/go/openview/	HP OpenView
•http://www.tivoli.com/	IBM NetView
•http://www.novell.com/products/managewise/	Novell ManageWise
•http://www.sun.com/solstice/	Sun MicroSystems Solstice
•http://www.microsoft.com/smsmgmt/	Microsoft SMS Server
•http://www.compaq.com/products/servers/management/	Compaq Insight Manger
•http://www.redpt.com/	SnmpQL - ODBC Compliant
•http://www.empiretech.com/	Empire Technologies
•ftp://ftp.cinco.com/users/cinco/demo/	Cinco Networks NetXray
•http://www.netinst.com/html/snmp.html	SNMP Collector (Win9X/NT)
•http://www.netinst.com/html/Observer.html	Observer
•http://www.gordian.com/products_technologies/snmp.html	Gordian's SNMP Agent
•http://www.castlerock.com/	Castle Rock Computing
•http://www.adventnet.com/	Advent Network Management
•http://www.smplsft.com/	SimpleAgent, SimpleTester

NMS comerciale



Exemplu NMS: CiscoWorks CiscoView

Exemple de sintaxă: Cisco

1) activarea SNMP

```
R0(config)#snmp-server host 192.168.1.2 public tty config
  snmp
R0(config)#snmp-server contact gigel
R0(config)#snmp-server chassis-id Cisco2500-1234
R0(config)#snmp-server community public ro
R0(config)#snmp-server community private rw
```

2) enable traps

```
R0(config)# snmp-server host 192.168.1.2 traps public tty
  config snmp
R0(config)# snmp-server enable traps
```

3) activarea accesului RW

```
R0(config)#snmp-server host 192.168.1.2 private
R0(config)#snmp-server system-shutdown
```

Exemple de sintaxă: Linux

pachete instalate: snmpd, snmp, mrtg

- afişarea OID (acces RO)

pt un grup de variabile:

```
snmpwalk -v1 -c public 192.168.1.1 1.3.6.1.4.1.9.2.1
```

pt numele imaginii:

```
snmpwalk -v1 -c public 192.168.1.1 1.3.6.1.4.1.9.2.1.
```

pt free RAM:

```
snmpwalk -v1 -c public 192.168.1.1 1.3.6.1.4.1.9.2.1.
```

pt CPU use:

```
snmpwalk -v1 -c public 192.168.1.1 1.3.6.1.4.1.9.2.1.57
```

- efectuarea unui remote shutdown (acces RW)

```
snmpset -v 2c -c private 192.168.1.1
  .1.3.6.1.4.1.9.2.9.9.0 i 2
```

Bibliografie

- Monitoring the router and the network (document online Cisco)
- Karl Quinn, NDS M.Sc., *SNMP Tutorial*
- Chris Francois, CS 417d Fall 1998, *SNMP*
- Albert Kagarmanov, Matthias Clausen (DESY), *SNMP Diagnostics*
- David N. Blank-Edelman, *The 20-Minute SNMP Tutorial - Automating System Administration with Perl*