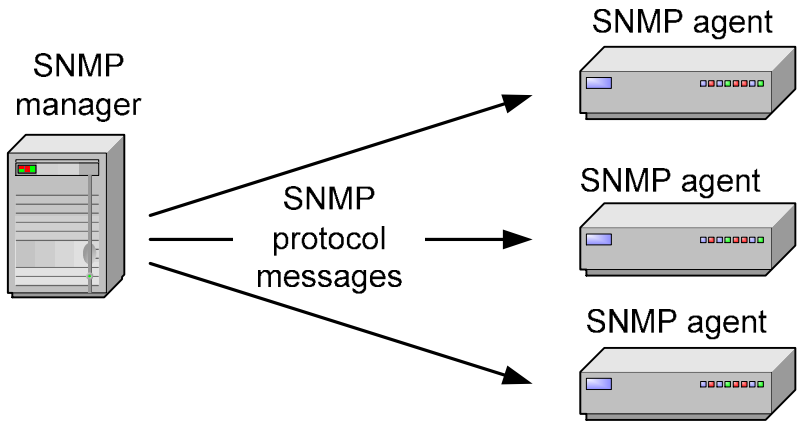
SNMP
Simple Network Management Protocol

Simple Network Management Protocol

- SNMP este un cadru care asigură facilități pentru managementul şi monitorizarea resurselor de rețea în Internet.
- Componente ale SNMP:
  - **Agenti** SNMP
  - **Manageri** SNMP (NMS)
  - **Management Information Bases** (MIBs)
  - **Protocolul SNMP**



Simple Network Management Protocol

- Într-un **mediu SNMP** tipic există:
  - Un număr de sisteme care trebuie administrate - ***managed systems***
  - Unul sau mai multe sisteme care le administrează - ***managing systems***
- O componentă soft numită ***agent:***
  - Rulează pe fiecare sistem administrat
  - raportează informații via SNMP sistemului de administrare

Simple Network Management Protocol

- **SNMP agent** este un software care rulează pe un equipment (host, router, printer, etc.) si care menține informație despre configurarea şi starea sa curentă într-o bază de date
- **Management Information Bases (MIBs)** defineşte informația de management
- Un **manager SNMP (NMS)** este un program (aplicatie) care contactează un agent SNMP pentru al întreba valoarea unui obiect din MIB sau modifica valoarea acestuia din baza de date ținută de agent.
- **Protocolul SNMP** este un protocol de nivel aplicatie ce descrie regulile de comunicare dintre agent si stația de management.

Simple Network Management Protocol

- Agentul SNMP relevă date de interes din sistemul administrat
  - Variabile ca:
    - "**free memory**“
    - "**system name**“
    - "**number of running processes**“
    - "**default route**“.....

sunt **obiecte administrate** (variabile din sistemul administrat care iau valori concrete în funcție de starea curentă a rețelei) Ele sunt memorate în **MIB**

Fiecare OID **identifică o variabilă** ce poate fi **citită** sau **setată** via SNMP

Simple Network Management Protocol

Există două tipuri de obiecte:

Objecte scalare

Definesc o singură instanță a obiectului

Objecte tabulare (grupuri de obiecte)

Definesc instanțe de obiecte multiple legate

Grupate în tabele MIB

De exemplu obiectul ***.interfaces*** al unui ruter are în subarborele său două obiecte:
.ifNumber ca *obiect scalar* şi
.ifTable ca *obiect tabelar,* cu mai multe intrări

.ifIndex
.ifDescr
.ifType
.ifSpeed
.ifPhysAddress
.....

Simple Network Management Protocol

Exemple de obiecte MIB:

ifMtu	OBJECT-TYPE
SYNTAX:	INTEGER
ACESS:	read-only
STATUS:	mandatory
DESCRIPTION:	"The size of the largest IP datagram through the interface, in octets"
::=	{ifEntry 4}

sysUpTime	OBJECT-TYPE
SYNTAX:	TimeTicks
ACESS:	read-only
STATUS:	mandatory
DESCRIPTION:	"The time in hundredth of sec. since reinitialization of net-management"
::=	{system 3}

Simple Network Management Protocol

Exemple de grupuri de obiecte în MIB-II

- Grupul **sistem**
- Grupul **interfata**
- Grupul **de translatare a adreselor**
- Grupul **IP**
- Grupul **ICMP**
- Grupul **TCP**
- Grupul **UDP**
- Grupul **EGP**
- **Transmisia**
- **SNMP**

Simple Network Management Protocol

Grupul IP - defineşte parametrii de configurare pentru protocolul IP

Scalari IP

ip 1 - ipForwarding - arata daca echipamentul are rol de gazda sau gateway
ip 2 - ipDefaultTTL - valoarea implicita pusa in cimpul TTL - durata de viata
ip 3 - ipInReceives - numarul total de datagrame primite de la interfete
ip 4 - ipInHdrErrs -datagrame ignorate datorita unor erori in header
ip 5 - ipInAddrErrors - ignorate datorita adresei destinatie IP invalide
ip 6 - ipForwDatagrams - Datagrame transmise mai departe la protocoale de nivel mai inalt
ip 7 - ipInUnknownProtos - Datagrams desinate unor protocoale necunoscute
ip 8 - ipInDiscards - Datagrame ignorate din lipsa de spatiu in buffer
ip 9 - ipInDelivers - Datagrame transmise la protocoale utilizator IP
ip 10- ipOutRequests - datagrame de la protocoale utilizator IP
ip 11- ipOutDiscards - datagrame ignorate din lipsa de spatiu in buffer
ip 13- ipReasmTimeout - Fragmentele mentinute pentru reasamblare
ip 14- ipReasmReqds - Fragmente primite care trebuie reasamblate
ip 15- ipReasmOKs - datagrame reasmablate cu succes
ip 16- ipReasmFails - erori la reasamblare
ip 17- ipFragOKs - datagrame fragmentate cu succes
ip 18- ipFragFails -erori de fragmentare
ip 19- ipFragCreates - fragmente generate in urma fragmentarii
ip 23- ipRoutingDiscards - intrari valide de routare ignorate

Simple Network Management Protocol

Grupul IP - continuare

Tabela de adrese IP

ip 20 ipAddrTable - tabele de informatii de adrese pentru nodul administrat
ipAddrTable 1 ipAddrTableEntry - un rind din tabela de adrese
ipAddrTableEntry 1 ipAdEntAddr - adresa IP pentru rindul de intrare
ipAddrTableEntry 2 ipAdEntIndx - index de identificare a interfetei rindului
ipAddrTableEntry 3 ipAdEntNetMask - masca de subretea asociata adresei IP
ipAddrTableEntry 4 ipAdEntBcastAddr - bitul cel mai putin semnificativ al adresei broadcast IP
ipAddrTableEntry 5 ipAdEntReasmMaxSize - dimensiunea celei mai mari datagrame de reasamblat din fragmentel sosite

Simple Network Management Protocol

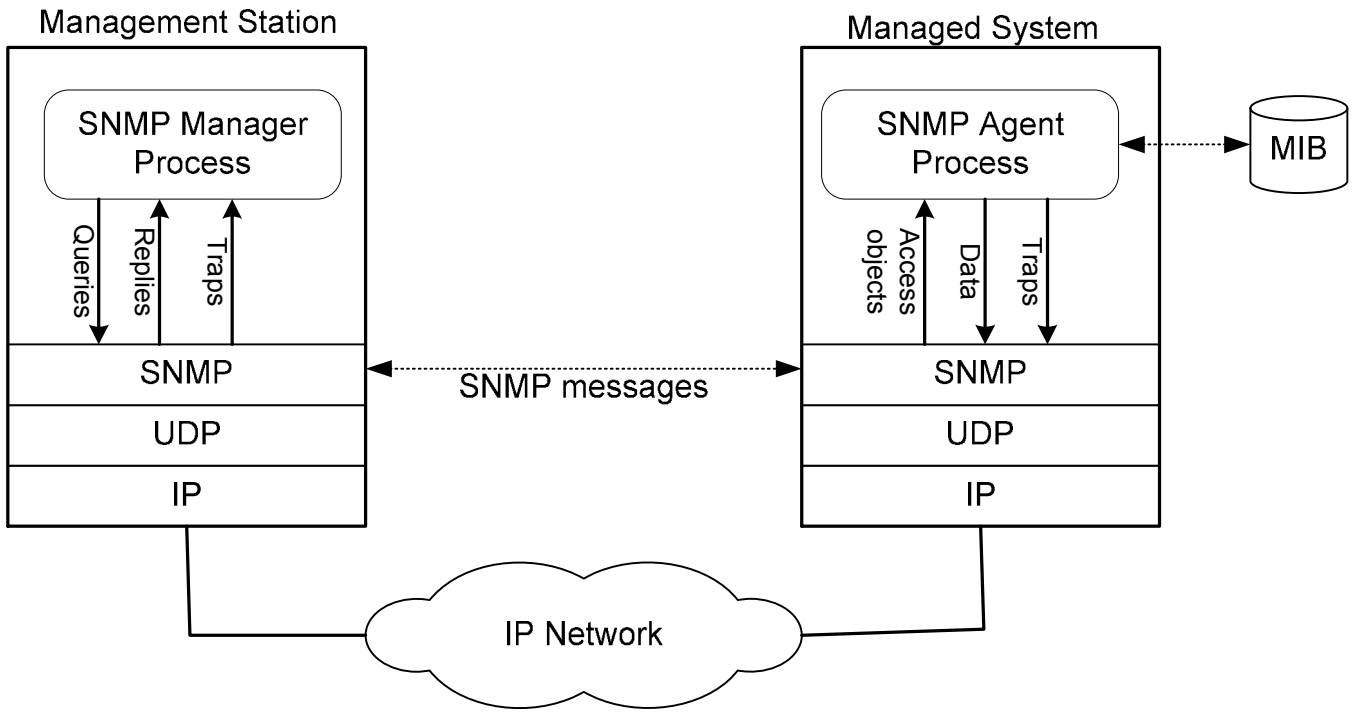
Grupul IP - continuare

Tabela de rutare IP

ip 21 ipRouteTable - tabela de rutare IP a achipamentului
ipRouteTable 1 ipRouteEntry - un rind din tabela de rutasre IP
ipRouteEntry 1 ipRouteDest - adresa IP a destinatiei
ipRouteEntry 2 ipRouteIfIndex - interfata prin care se ajunge la urmatorul hop
ipRouteEntry 3 ipRouteMetric1 - metrica primara de rutare pentru ruta
ipRouteEntry 4 ipRouteMetric2 - metrica alternativa
ipRouteEntry 5 ipRouteMetric3
ipRouteEntry 6 ipRouteMetric4
ipRouteEntry 7 ipRouteNextHop - adresa IP pentru urmatorul hop de pe aceasta ruta
ipRouteEntry 8 ipRouteType - tipul rutei (invalid, direct, remote, other)
ipRouteEntry 9 ipRouteProto - mecanismul prin care s-a aflat ruta
ipRouteEntry 10 ipRouteAge - numar de secunde de la actualizarea rutei
ipRouteEntry 11 ipRouteMask - masca de subretea pentru adresa IP destinatie
ipRouteEntry 12 ipRouteMetric5
ipRouteEntry 13 ipRouteRouteInfo - referinta la definitie MIB specifica pentru protocolul de rutare responsabil de ruta, dat de valoarea ipRouteProto

SNMP

- Schimbul de mesaje în SNMP



MIB

- Un **MIB** specifică objectele administrate
- MIB este un fişier text care descrie objectele administrate folosind ASN.1 (Abstract Syntax Notation 1)
- ASN.1 este un limbaj formal ce descrie datele şi proprietățile lor
- In Linux, fişierele MIB sunt în directorul */usr/share/snmp/mibs*
  - *Există mai multe MIB-uri*
  - ***MIB-II** (definit in RFC 1213) conține **obiectele administrate din rețelele TCP/IP***

Objecte administrate

- Fiecare obiect administrat are un ***object identifier*** *(OID)*
- OID este specificat într-un fişier MIB.
- Un OID este reprezentat ca o secvență de numere întregi separate prin puncte, sau cu un şir text:

  Exemplu:

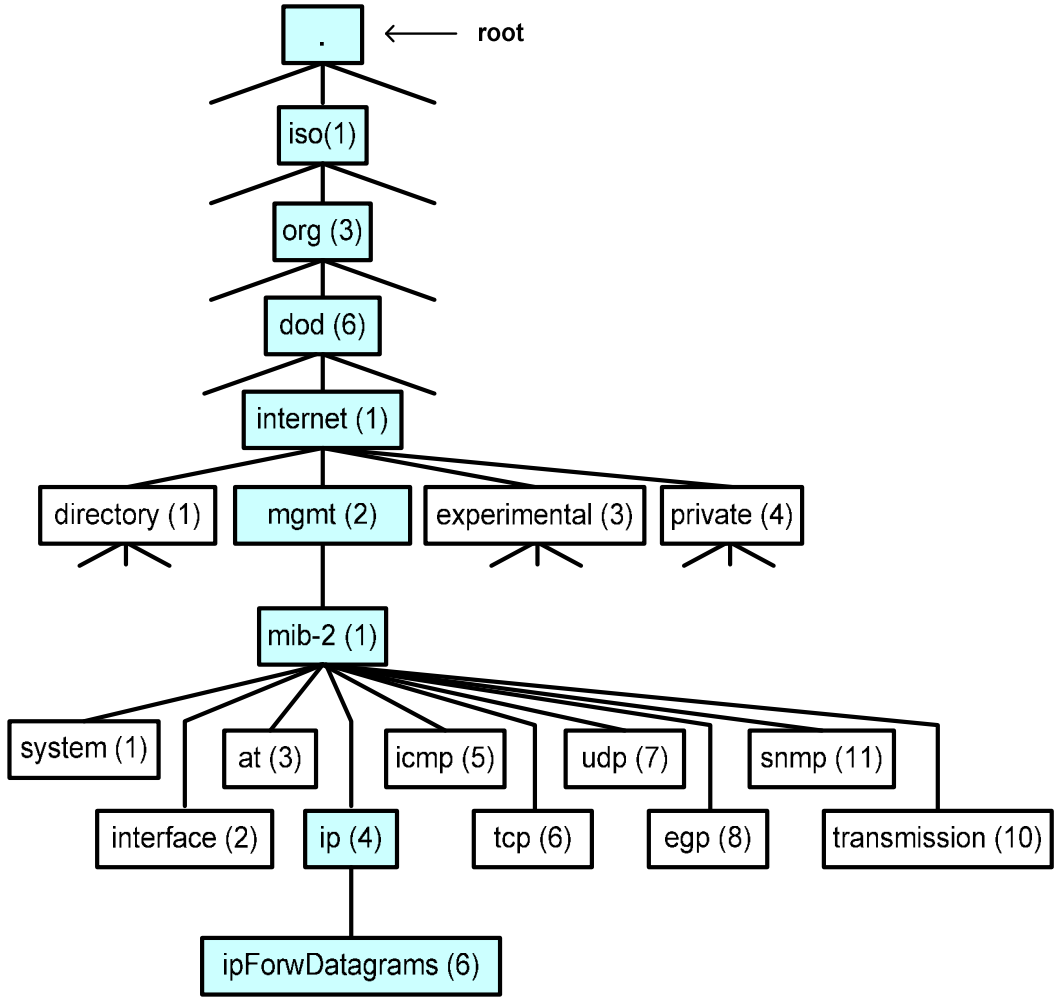
  – *1. 3. 6. 1. 2. 1. 4. 6.*

  – i*so.org.dod.internet.mgmt.mib-2.ip.ipForwDatagrams*

- Când un manager SNMP interoghează un obiect, el trimite OID la agentul SNMP.

Organizarea obiectelor administrate

- Obiectele administrate sunt organizate într-un arbore, iar OID reflectă ierarhia structurală
- Fiecare **OID** reprezintă un **nod** în arbore.
- Obiectul cu OID 1.3.6.1.2.1 (*iso.org.dod.internet.mgmt.mib-2)* este în topul ierarhiei pentru toate obiectele administrate de **MIB-II**.
- Producătorii de echipamente de rețea pot adăuga obiecte specifice produselor lor în această ierarhie (ramura ***private*** *(4)*).



Organizarea obiectelor administrate

- Subarborele MIB-II conține obiecte administrate din Internet

```
system OBJECT IDENTIFIER :: { mib-2 1 }
interface OBJECT IDENTIFIER :: { mib-2 2 }
at OBJECT IDENTIFIER :: { mib-2 3 }
ip OBJECT IDENTIFIER :: { mib-2 4 }
icmp OBJECT IDENTIFIER :: { mib-2 5 }
tcp OBJECT IDENTIFIER :: { mib-2 6 }
udp OBJECT IDENTIFIER :: { mib-2 7 }
egp OBJECT IDENTIFIER :: { mib-2 8 }
transmission OBJECT IDENTIFIER :: { mib-2 10 }
snmp OBJECT IDENTIFIER :: { mib-2 11 }
```

Definiția obiectelor administrate în MIB

Descrierea unui obiect MIB (***ipForwDatagrams*** - numărul de datagrame IP transmise)

```
ipForwDatagrams OBJECT-TYPE
    SYNTAX  Counter
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
            "The number of input datagrams for which this
            entity was not their final IP destination, as a
            result of which an attempt was made to find a
            route to forward them to that final destination.
            In entities which do not act as IP Gateways, this
            counter will include only those packets which were
            Source-Routed via this entity, and the Source-
            Route option processing was successful."
    ::= { ip 6 }
```

Definiția obiectelor administrate in MIB

- Foloseşte **Abstract Syntax Notation One** (ASN.1)
  - Notatie Standard, flexibilă
  - Descrie structuri de date pentru:
    - Reprezentare
    - Codare
    - Transmitere
    - Decodare date
- Produce un set de reguli formale
  - Descrie structura objectelor
    - Independent de tehnicile de codare specifice unei maşini
    - Este precisă, notația formală minimizează ambiguitățile

Abstract Syntax Notation One

- Standard reunit ISO şi ITU-T
  - Defined inițial in 1984
    - Parte a CCITT X.409:1984
  - Devenit standard de sine, X.208 (1988)
    - Foarte largă aplicabilitate
  - Revizuit substantial în 1995
    - Acoperit de seriile X.680
- **Structure of Management Information (SMI)**
  - Un subset adaptat al ASN.1
  - Folosit în SNMP pentru a defini un set de obiecte MIB

Tipuri de date specifice SNMPv1 and SMI

SNMPv1 SMI

SMI specifică tipurile de date folosite în SNMP

Împărțite în două categorii:

Simple data types

Application-wide data types

Date de tip simplu

În the SNMPv1 SMI sunt definite trei tipuri de date simple:

Integer data type:

Întreg cu semn în gama 2^0 to 2^{31}-1.

Octet strings:

Secvențe ordonate de octeți, de la 0 la 65 535

Object IDs:

Fromează setul de identificatoare de obiecte alocate conform regulilor specificate in ASN.1

Toate valorile sunt unice

Tipuri de date specifice SNMPv1 and SMI

Application-wide data types

Există şapte tipuri de date pentru application-wide in SNMPv1 SMI:

- **Network addresses**
- **Counters**
- **Gauges**
- **Time ticks**
- **Opaques**
- **Integers**
- **Unsigned integers**

Tipuri de date specifice SNMPv1 and SMI

Application-wide data types

Network addresses

Reprezintă o adresă a unei familii particulare de protocole.

SNMPv1 suportă doar adrese IP pe 32-bit.

Counters

Integi ne-negativi care cresc

- Până ating valoarea maximă
- Apoi revin la zero

In SNMPv1, un counter este pe 32-biti

Tipuri de date specifice SNMPv1 and SMI

Application-wide data types

Gauges

Întregi ne negativi

Pot creşte sau descreşte între valorile minimă şi maximă specificate

A system property going outside the specified range:

The value of the gauge itself will not go beyond the respective maximum or minimum

Specified in RFC 2578.

Tipuri de date specifice SNMPv1 and SMI

Application-wide data types

Time tick

Reprezintă a sutimi de secundă de la un anumit eveniment

Opaque

Reprezintă o codare arbitrară folosită pentru a transfera un şir de informaţii care nu sunt conforme cu tipurile de date utilizate uzual de SNMP, în baza regulilor SMI

Tipuri de date specifice SNMPv1 and SMI

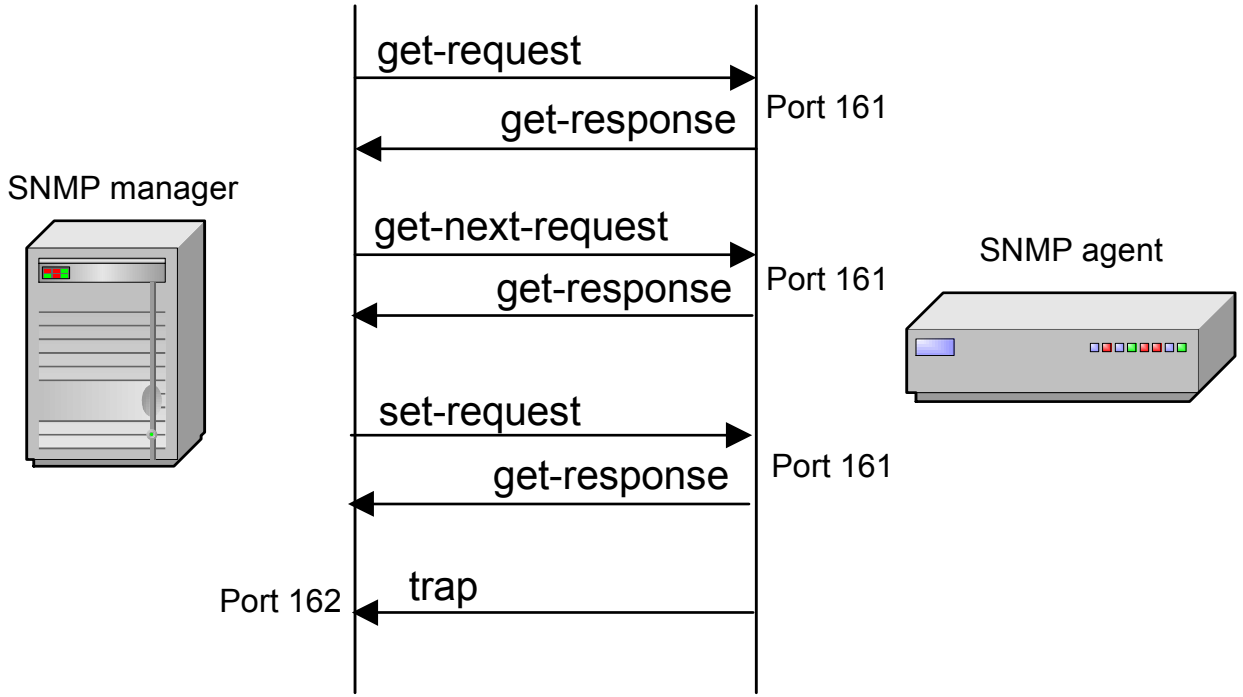
Application-wide data types

- **Integer**
  - Reprezintă un număr întreg cu semn
  - Redefineste tipul de date întreg
    - Precizie în ASN.1
    - Precizie limitată în SMI

- **Unsigned integer**
  - Reprezintă un număr întreg fără semn
  - Utile când valorile sunt întotdeauna non-negative

Protocolul SNMP

- SNMP manager şi SNMP agent comunică folosind protocolul SNMP (managerul este pe rol de **client**, agentul este pe rol de **server**)
  - Cazul general: Managerul trimite cereri (interogări) si agentul răspunde
  - Exceptie: Trap-urile sunt inițiate de agent.



SNMP Protocol

Tipuri de pachete SNMP

- **Get-request.** Cere valori ale unui sau mai multor obiecte
- **Get-next-request.** Cere valoarea următorului obiect, conform ordinii din OIDs.
- **Set-request.** Cere modificarea valorii unuia sau mai multor obiecte
- **Get-response.** Trimis de agentul SNMP ca răspuns la mesaje *get-request, get-next-request, or set-request* .
- **Trap.** Un trap SNMP este o notificare trimisă de către un agent SNMP la un manager SNMP, declanşat de către un eveniment stabilit anterior.

Trap-urile

- Trap-urile sunt mesaje transmise asincron de un agent spre un manager
- Sunt declanşate de un eveniment
- Trap-urile definite includ:
  - l**inkDown**: cînd cade o interfață
  - **coldStart** – restart neaşteptat (i.e., system crash)
  - **warmStar**t - soft reboot
  - **linkUp** – o linie trece din starea down în starea up
  - (SNMP) **AuthenticationFailure**
  - …

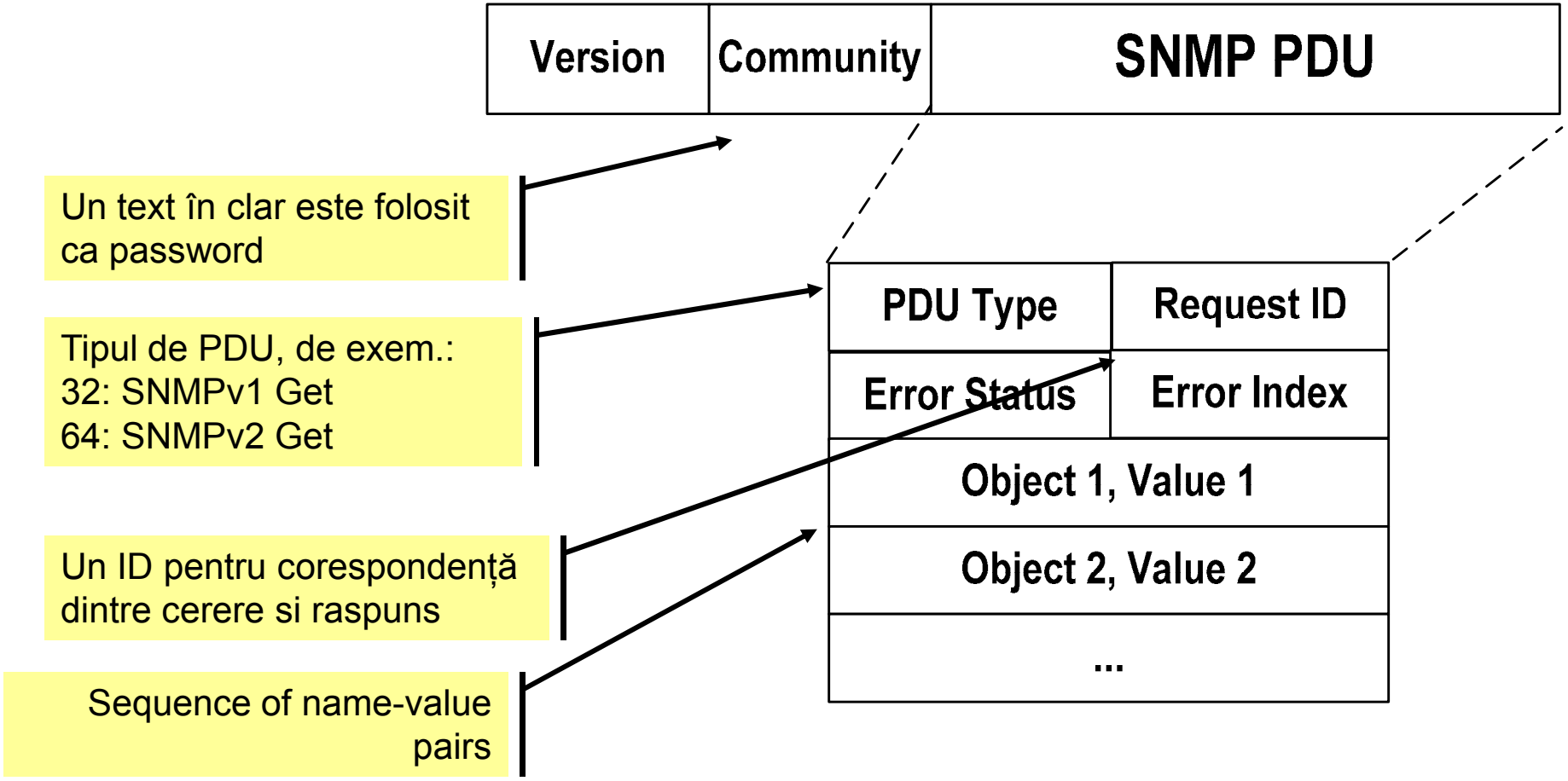
SNMP Versions

- Trei versiuni sunt cunoscute:
  - SNMPv1 (1990)
  - SNMPv2c (1996)
    - *A adăugat functia “GetBulk” şi alte câteva tipuri*
    - *A adăugat facilități RMON (remote monitoring)*
  - SNMPv3 (2002)
    - *SNMPv3 a pornit de la SNMPv1 (nu de la SNMPv2c)*
    - *Are facilități de securitate*

- Toate versiunile sunt utilizate în prezent
- Majoritatea agentilor SNMP şi a managerilor suportă toate cele trei versiuni de protocol.

Formatul Pachetelor SNMP

- Mesaje SNMPv1 Get/Set :



Securitate SNMP

- SNMPv1 foloseşte un text în clar pentru a autentifica entitățile care schimbă mesaje (fără criptare)

- SNMPv2 a făcut unele eforturi pe linia recunoaşterii comunităților (sufixul “c” in SNMPv2c vine de la “community”).
-
- SNMPv3 are mai multe facilități de securitate:
  - Asigură **integritatea datelor**,
  - Asigură **autenticitatea** entităților care comunică
  - Asigură **confidențialitatea**.

SNMP Security

- Modelul de securitate la SNMPv3 are două componente:
  1. In loc să dea drepturi de acces la nivel de comunitate, SNMPv3 acordă acces utilizatorilor.
  2. Accesul poate fi restrîns la sectiuni din MIB (V*ersion-based Access Control Module* (VACM). Drepturile de acces pot fi limitate:
     - Specificând o gamă adreseIP valide pentru un user sau o comunitate,
     - sau specificând că doar o parte din arborele MIB poate fi accesat.

Nivele de securitate în SNMPv2

SNMPv3 are trei nivele de securitate:

- *noAuthNoPriv*: Autentificare pe baza potrivirii numelui userului.
- *authNoPriv*: Autentificare pe baza rezumatelor mesajelor MD5 sau SHA.
- *authPriv:* Autentificare pe baza rezumatelor mesajelor MD5 sau SHA şi criptare cu DES

Aceste facilități de securitate sunt superioare SNMPv1 and SNMPv2c:

- *SNMPv1, SNMPv2*: autentificarea persupune doar potrivirea şirului *community*.