3. Mesajul ICMP este încapsulat în vederea transmisiei cu antetul IP.

4. Operația PING se realizează în două faze: prima de transmisie a cererii de ecou ICMP, a doua de recepționare a răspunsului la ecou prin intermediul ICMP. Un răspuns afirmativ, de găsire a destinației, include durata de transfer dus-întors a pachetului între sursă și destinație, exprimată în milisecunde, rata de erori etc.

5. Mesajele ICMP de interogare a routerelor sunt utilizate pentru actualizarea dinamică a tabelelor de rutare.

II.1.11 Protocoale de management a rețelei

Gestionarea rețelelor de calculatoare se realizează pe baza protocoalelor de management de rețea.

Suita TCP/IP include protocolul de management SNMP (*Simple Network Management Protocol*) definit în RFC 1155 - 1157, care implementează un mecanism de gestionare a resurselor rețelei, folosind baze de date MIB (*Management Information Base*), cu informații referitoare la toate componentele rețelei (RFC 1514 - *Host Resources MIB;* RFC 1398 - *Ethernet-like Interface Types MIB;* RFC 1493 - *Bridge MIB* și altele). RFC 1213 definește MIB-II care include obiectele gestionate pentru rețelele bazate pe suita TCP/IP.

SNMP poate folosi oricare din protocoalele de transport din suita TCP/IP dar în cele mai multe cazuri utilizează UDP, pe porturile de aplicații 161 și 162.

Un sistem de management a rețelelor de calculatoare include trei categorii de componente (Fig. II.15):

1. **componente gestionate** (*managed device*);

2. **stații de gestionare** sau **de management** (*network management station*);

3. **protocolul de management** (*management protocol*) utilizat pentru comunicația dintre celelalte componente ale sistemului de management.

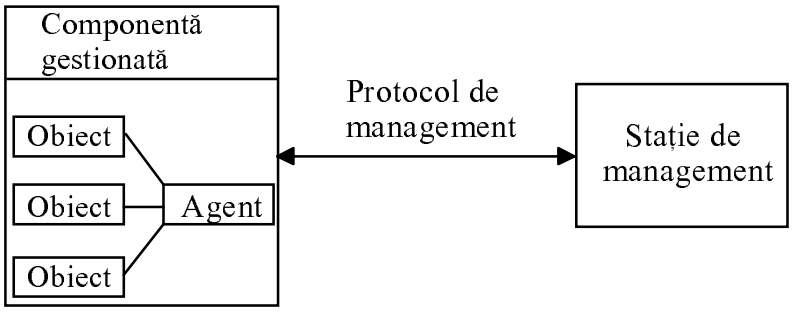

Fig.II.15 Structura de bază a sistemului de management al rețelei

RFC 1155 descrie un mecanism de identificare și descriere a obiectelor din MIB, denumit SMI (*Structure of Management Information*), care definește schema de organizare a colecției de obiecte gestionate din MIB, pe baza unei diagrame 'arbore', cu mai multe nivele (Fig.II.16).

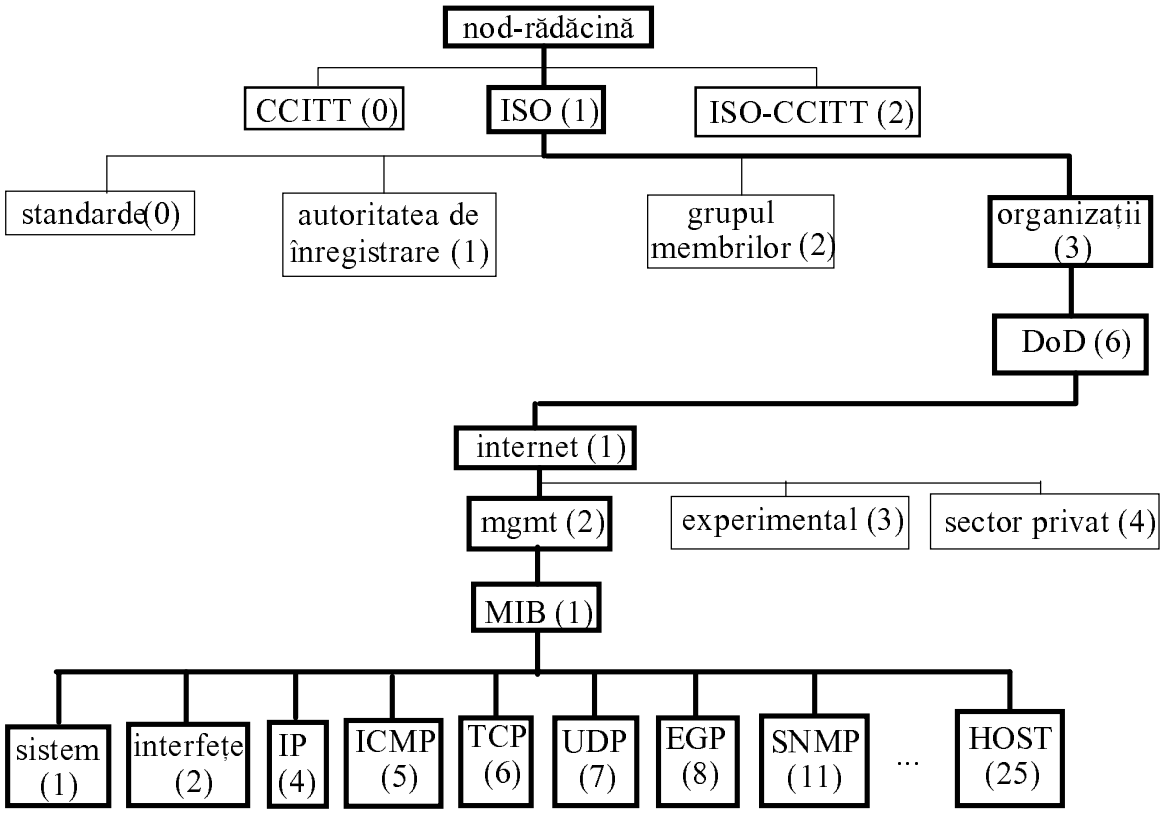

Fig. II.16 Diagrama-arbore de organizare a MIB în Internet

Fiecare nod din această diagramă este numerotat și, eventual, i se asociază și un scurt text descriptiv.

Observăm că în MIB I sunt incluse ca obiecte protocoalele din suita TCP/IP (în figură au fost reprezentate doar câteva dintre acestea).

Referitor la fiecare obiect, în MIB sunt incluse informații de natură administrativă și operațională.

Fiecare obiect se specifică numele, sintaxa, modul de acces, starea și o descriere a acestuia.

Numele reprezintă un identificator global, unic al obiectului, care rezultă urmărind calea care leagă nodul-rădăcină și obiectul gestionat din MIB. Acesta poate fi exprimat în trei formate diferite, echivalente:

1. **numeric cu puncte**;
2. **text** cu separare prin puncte, încadrat de paranteze pătrate;
3. **combinat** (text și numere de noduri).

De exemplu, pentru protocolul IP se specifică numele sau identificatorul:

1.3.6.1.2.1.4

echivalent cu:

[iso org dod internet mgmt mib 4]

echivalent cu

[iso(1) org(3) dod(6) internet(1) mgmt(2) mib(1) 4].

Se poate utiliza și un nume relativ, de exemplu [mib 4], care specifică al 4-lea nod din sub-arborele "MIB".

Nu se impun limite referitor la lungimea șirului de caractere care identifică un obiect din MIB.

Fiecărui obiect din MIB i se asociază un șir de caractere pentru descrierea sa, un așa-numit **mnemonic**, mai comod pentru utilizatorul uman decât un nume exprimat numeric (de exemplu, *sysDescr* pentru nodul "sistem" sau *ifTable* pentru nodul "interfețe" etc).

De fapt, obiectele din MIB sunt manipulate pe baza unor valori memorate la diverse momente (*instances*), ca date de tipuri diferite în funcție de natura obiectului.

Stațiile de management a rețelelor (NMS - *Network Management Station*) lucrează cu aceste valori instantanee ale obiectelor care sunt identificate prin așa-numitul **identificator de valoare** (*instance-identifier*), atașat identificatorului de obiect.

Dacă obiectul nu este o coloană dintr-un tabel, se folosește identificatorul de valoare 'nul' (0).

Exemplu: Se utilizează *sysDescr*.0 echivalent cu 1.3.6.1.2.1.1.0 pentru obiectul 'sistem'.

Dacă obiectul gestionat din MIB este structurat ca o coloană dintr-un tabel, atunci se anexează la identificatorul de obiect, indicii corespunzători coloanei din acel tabel, mai precis celulei în care este înregistrată o anumită valoare. În caz general, se anexează indicii tuturor coloanelor care descriu obiectul analizat.

Exemplu: Pentru starea unei conexiuni TCP (*tcpConnState*) specificată prin identificatorul relativ la TCP, 13.1.1, se combină în identificatorul de valoare adresa IP a sursei (192.168.34.81), portul de aplicație sursă (23), adresa IP a destinației (194.210.225.14), portul de aplicație de la destinație (2002) și se anexează identificatorului de obiect, rezultând:

1.3.6.1.2.1.6.13.1.1.192.168.34.81.23.194.210.225.14.2002

Sintaxa unui obiect constă în tipul datelor referitoare la acesta (INTEGER, OCTET STRING ș.a.).

Accesul la un obiect din MIB poate fi restricționat (*not-accessible; read-only; write-only*) sau liber (*read-write*).

Prin **starea** unui obiect se exprimă condițiile de implementare ale acestuia:

1. **mandatar**: componenta gestionată de NMS implementează în mod obligatoriu acel obiect;

2. **opțional**: componenta gestionată de NMS implementează opțional acel obiect;

3. **depășit:** componenta gestionată de NMS nu mai implementează acel obiect;

4. **depreciat**: componenta gestionată de NMS poate implementa acel obiect, dar există un nou obiect în MIB superior acestuia.

Descrierea obiectului se poate face printr-un scurt text descriptiv asociat acestuia.

Protocolul SNMP este utilizat de stația de management (NMS) pentru a transmite mesaje componentei gestionate, mai precis agentului de management din cadrul acesteia.

În general, SNMP acționează în mod recursiv, prin interogarea periodică (*polling*) a agenților de management ai componentelor gestionate de NMS.

Numai în situații critice, un agent poate iniția schimbul de informații cu NMS, pentru a o înștiința de modificările apărute, transmițând mesaje-capcană (*trap*) care întrerup procesul de *polling*. Un agent nu poate transmite oricât de multe mesaje-capcană spre NMS, pentru a evita pierderea controlului asupra întregii rețele.

Un mesaj SNMP (figura II.17) include un câmp de versiune a protocolului, un câmp referitor la grupul de utilizatori cărora li se adresează mesajul și un câmp de date.

Versiune	Grup adresabil	Date

Fig. II.17 Formatul mesajului SNMP

Prin stabilirea adresabilității protocolului, se realizează o procedură simplă de autentificare a mesajelor.

Unitatea de date sau mesajul SNMP (PDU - *Protocol Data Unit*) poate fi denumită în cinci moduri distincte, în funcție de natura informației transmise:

1. **cerere simplă** (*get-request*) - NMS cere unui agent de management informații despre un obiect;

2. **cerere recursivă** (*get-next-request*) - NMS cere unui agent de management informații despre obiectul următor din MIB;

3. **cerere de impunere** (*set-request*) - NMS impune o anumită valoare pentru un obiect din MIB-ul agentului;

4. **răspuns** (*get-response*) - un agent trimite informații spre NMS, despre un obiect, ca răspuns la cererea acesteia;

5. **"capcană"** (*trap*) - un agent transmite spre MIB informații referitoare la un eveniment extraordinar care a afectat componenta gestionată prin intermediul său (reinițializarea agentului de management, schimbarea stării unei interfețe, nerespectarea unor condiții de autentificare etc). Există șapte tipuri de mesaje-capcană SNMP.

Primele patru tipuri de mesaje SNMP se transmit prin UDP, pe portul 161. Numai mesajele-capcană se transmit pe portul de aplicație 162.

SNMP este considerat a fi un protocol simplu deoarece nu are decât cinci operații, corespunzătoare celor cinci tipuri de mesaje SNMP (*get, get-next, set, get-response* și *trap*).

În funcție de modul de acces, se poate folosi un număr mai mic de mesaje SNMP.

Obiectele din MIB pot fi grupate în subseturi (SNMP MIB *View*), în funcție de accesibilitatea acestora: parțială (*read-only*) sau totală (*read-write*).

Pentru agenții de management, se definesc **profile** prin care se stabilesc drepturile de acces la diferitele subseturi de obiecte din MIB, total sau parțial accesibile (Tabel II.9):

1. cu drept de citire (*read-only*);
2. cu drept de scriere (*write-only*);
3. cu drepturi de citire și de scriere (*read-write*);
4. fără drepturi de acces la MIB (*not-accessible*).

Tabel II.9

Operații SNMP admise profilelor de agenți

în funcție de accesibilitatea obiectelor din MIB

Accesibilitatea obiectului SNMP	Profilele agenților de management			
	cu drept de citire	cu drept de scriere	cu drepturi de citire și de scriere	fără drepturi de acces
parțială	cerere simplă cerere recursivă cerere-capcană	-	cerere simplă cerere recursivă cerere-capcană	-
totală	cerere simplă cerere recursivă cerere-capcană	cerere simplă cerere recursivă cerere de impunere cerere-capcană	cerere simplă cerere recursivă cerere de impunere cerere-capcană	-

Observații

1. Se impun măsuri stricte de securitate referitor la mesajele SNMP, întrucât prin definirea unui profil de agenți cu drept de scriere pe un grup de obiecte cu accesibilitate totală se pot produce daune majore rețelei de către persoane neautorizate care cunosc numele profilului.

2. SNMP este un protocol rutabil întrucât folosește protocolul IP pentru încapsularea datelor și, implicit, adresarea IP.

3. Există și protocoale de management al rețelelor locale de calculatoare, nerutabile. Un astfel de protocol este NetBeui (*Network BIOS extended user interface*), dezvoltat de firma Microsoft pentru rețele Netware (de PC-uri), cu sistem de operare NT, pe baza modelului client-server. Pe lângă operațiile de management de rețea, NetBeui include și funcțiile de transport, de corecție a erorilor de transmisie, de confirmare a recepției corecte a datelor (ACK), fiind echivalent unei stive de protocoale cu funcții distincte. Toate acestea determină o creștere considerabilă a timpului de transmisie a pachetelor și apariția blocajelor în rețea cauzate de așteptarea unor mesaje de confirmare pierdute. O altă limitare a NetBeui este aceea dată de numărul maxim admis de sesiuni simultan deschise în rețea (254). Aceste dezavantaje ale NetBeui sunt eliminate în cadrul protocolului NBF (*NetBeui Frame*), cu 'fereastră glisantă' (*sliding window*) de transmisie.