MINISTERUL EDUCAȚIEI, CERCETĂRII ŞI INOVĂRII

UNIVERSITATEA TEHNICĂ
DIN CLUJ-NAPOCA

Facultatea de Electronică, Telecomunicații şi Tehnologia Informației

Ing. Cristian Mihai Vancea

REZUMATUL TEZEI DE DOCTORAT

CONTRIBUȚII LA MANAGEMENTUL REȚELELOR LOCALE ŞI PERSONALE DE TELECOMUNICAȚII

Conducător ştiințific,
Prof.dr.ing.Virgil DOBROTĂ

2009

Comisia de evaluare a tezei:

PREŞEDINTE:

Prof.dr.ing. **Marina Dana Ţopa** - decan,
Facultatea de Electronică,Telecomunicaţii şi Tehnologia Informaţiei,
Universitatea Tehnică din Cluj-Napoca

MEMBRI:

Prof.dr.ing. **Virgil Mircea Dobrotă** - conducător ştiinţific,
Universitatea Tehnică din Cluj-Napoca

Prof.dr.mat. **Florian Mircea Boian -** referent,
Universitatea „Babeş-Bolyai" din Cluj Napoca

Prof.dr.ing. **Miranda Monica Naforniţă** - referent,
Universitatea „Politehnica" din Timişoara

Prof.dr.ing. **Aurel Vlaicu** - referent,
Universitatea Tehnică din Cluj-Napoca

Susţinerea publică a tezei de doctorat : 23 octombrie 2009, ora 10:00
Aula „Alexandru Domşa"
Universitatea Tehnică Cluj Napoca
Str. C. Daicoviciu nr.15

Cuprins

Capitolul 1. Introducere 4
1.1 Introducere în managementul rețelelor 4
1.2 Scop teză 6
1.3 Organizare teză 7
Capitolul 2. Arhitecturi pentru managementul rețelelor de telecomunicații 7
2.1 Arhitectura SNMP 7
2.2 Arhitectura TMN 14
2.3 Arhitecturi CMIP şi CMOT 15
Capitolul 3. Agent hardware pentru managementul rețelelor locale IEEE 802.3, 802.3u 16
3.1 Standarde IEEE 802.3, IEEE 802.3u 16
3.2 Implementare hardware bazată pe microcontrolerul MC9S12NE64 17
3.3 MIB pentru Internet (MIB II) 17
3.4 Implementare agent SNMP hardware pentru IEEE 802.3, 802.3u 18
Capitolul 4. Agent hardware pentru managementul rețelelor personale IEEE 802.15.4 20
4.1 Standard IEEE 802.15.4 20
4.2 Arhitectura hardware bazată pe microcontrolerul MC9S12NE64 şi CC2420 21
4.3 Realizare MIB pentru IEEE 802.15.4 24
4.4 Implementare agent SNMP hardware pentru IEEE 802.15.4 25
Capitolul 5. Agent software pentru managementul rețelelor locale fără fir IEEE 802.11 26
5.1 Standard IEEE 802.11 pentru WLAN 26
5.2 Implementari software existente pentru agenți SNMP în Windows şi Linux 27
5.3 Arhitectura bazată pe interfața AirPcap şi analizorul software Wireshark 28
5.4 Realizare MIB pentru IEEE 802.11 29
5.5 Implementare agent SNMP software pentru IEEE 802.11 30
Capitolul 6. Agent software pentru managementul aplicațiilor VoIP în rețelele locale cu şi fără fir 32
6.1 Arhitectura Asterisk 32
6.2 Extindere MIB pentru Asterisk 33
6.3 Extindere agent SNMP software pentru Asterisk 34
Capitolul 7. Manageri software pentru rețele locale şi personale 36
7.1 Soluții software existente 36
7.2 Soluție propusă pentru manager software: SNMP Manager 37
7.3 Propunere de tranziție spre managementul integrat al rețelelor de telecomunicații 38
Capitolul 8. Contribuții la managementul rețelelor locale şi personale de telecomunicații 41
8.1 Contribuții originale în această teză 41
8.1.1 Implementare agent SNMP hardware pentru IEEE 802.3 41
8.1.2 Implementare agent SNMP hardware pentru IEEE 802.15.4 41
8.1.3 Realizare MIB pentru IEEE 802.15.4 41
8.1.4 Implementare agent SNMP software pentru IEEE 802.11 42
8.1.5 Realizare MIB pentru IEEE 802.11 42
8.1.6 Extindere agent SNMP software pentru Asterisk 42
8.1.7 Extindere MIB pentru Asterisk 42
8.1.8 Propunere tranziție spre managementul integrat 43
8.2 Remarci finale 43
Bibliografie selectivă 43

Capitolul 1. Introducere

1.1 Introducere în managementul rețelelor

Prin gestiunea (managementul) rețelelor de telecomunicații se înțelege coordonarea tuturor resurselor care sunt necesare pentru proiectarea, planificarea, controlul, simularea, generarea, implementarea, analiza, supravegherea, măsurarea şi testarea rețelelor de telecomunicații, cu scopul de a garanta utilizatorului final un grad de servicii cu costuri adecvate, printr-o distribuție optimală a capacității.

Managementul rețelelor poate fi văzut ca un proces de monitorizare (supraveghere) şi control a unor sisteme distribuite de dimensiuni mari, medii sau mici în care erorile sau defectele apar în mod normal. Putem spune că managementul rețelelor poate avea următoarele componente:

- controlul rețelelor
- monitorizarea rețelelor
- întreținerea rețelelor
- operare

Din punct de vedere al modelului de referință OSI, managementul rețelelor oferă o modalitate de a menține rețele în funcțiune şi de a funcționa la parametrii stabiliți, conform [Mau01]. De asemenea oferă facilități de comandă şi control. Managementul rețelelor poate fi împartit în următoarele componente:

- *Managementul defectelor* - toate echipamentele se pot defecta la un moment dat, iar conexiunile şi interfețele se pot opri. Toate acestea împreuna pot cauza apariția unor informații greşite în rețea. Evenimentele pot fi considerate defecte, cu precizarea că ele nu înseamnă neaparat că ceva s-a defectat în rețea. Evenimentele există ca să informeze sistemul de management despre apariția unor lucruri în sistem.
- *Managementul configurațiilor* – toate echipamentele încearcă să obțină anumite configurații sau reglaje. Setările de configurație pot fi citite sau înscrise în echipamente.
- *Managementul financiar* – facturarea pentru servicile oferite este o componentă importantă în cadrul sistemului de management. Această funcție va fi folosită pentru taxarea utilizării resurselor de către fiecare departament, utilizator, etc şi de asemenea verificarea corectitudinii taxării trimise de furnizorul de servicii.
- *Managementul performanțelor* – pe masură ce numărul de utilizatori şi nevoia de bandă creşte, este esential să poata fi măsurate performanțele, mai ales pentru îndeplinirea unui anumit SLA (Service Level Agreement). Verificarea performanțelor poate fi folosită şi pentru prediciția posibilelor congestii.
- *Managementul securității* – atacurile împotriva rețelelor pot include accesul neautorizat, modificarea datelor sau furtul acestora,etc. Securitatea este dorită pentru a asigura că atât datele cât şi rețeaua în sine sunt protejate.

Toate aceste categorii descriu de fapt ceea ce se consideră din punct de vedere al modelului OSI ca fiind zonele funcționale ale managementului rețelelor. Un acronim care identifică aceste componente ale unui sistem de management, conform [Mau01] este *FCAPS (Fault, Configuration, Accountig, Performance, Security).*

Arhitecturi de management

Arhitectura de management reprezintă o colecție de echipamente gestionate, echipamente care monitorizează şi modalități de transfer a informațiilor între ele [Sta98]. Când se vorbeste

despre o arhitectură de management este important de înteles că aceasta este legată de tehnologia de management aleasă.

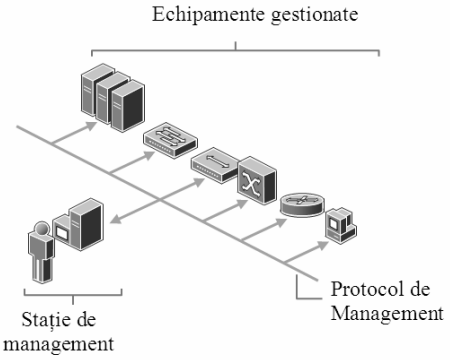

Figura 1.1 Arhitectura generală a unui sistem de management

Manageri

Managerii (sau NMS – Network Management Station) reprezintă probabil cel mai important element din infrastructura de management care colectează datele despre starea rețelei şi trimit mesaje de configurare a elementelor de rețea. Funcțiile principale ale unui manager sunt acelea de a recepționa alarmele trimise de echipamentele gestionate, de a cere informații de la aceste echipamente şi de a trimite parametrii de configurare. Un manager ar trebui să ofere posibilitatea configurării anumitor parametrii, de exemplu numărul de reîncercari pentru obținea informațiilor, durata de aşteptare a răspunsului (timeout) sau intervalul de interogare, parametrii care pot fi utilizați pentru a determina dacă un echipament nu răspunde comenzilor. Managerii trebuie să cunoască structura şi formatul informației de management folosite de echipamentele gestionate, indiferent de protocolul sau tehnologia folosită.

Agentul

Agenții sunt părți de software sau hardware care implementează diverse funcții şi care rulează în interiorul echipamentelor monitorizate. Prima sarcină şi cea mai importantă a unui agent este aceea de a răspunde cererilor trimise de manageri. Agenții necesită de obicei o configurație minimală înainte de folosire (de exemplu informații despre sistem, pozitionarea, administratorul sistemului, drepturile de acces). Astfel de informații (drepturile de access) pot ajuta sistemul de management să răspundă doar mesajelor de management venite de la o stație de management de încredere.

Topologii de management

În momentul actual tendința este de a merge spre un sistem centralizat, care poate fi realizat într-un fel relativ simplu prin folosirea unui singur sistem de management care supervizează întreaga activitate. Dezavantajul este că acest mod de lucru consumă din resursele rețelei prin nevoia de a adăuga de exemplu rețelele suplimentare de semnalizare. Dezavantajul major rămane faptul că dacă infrastructura rețelei creşte foarte mult un sistem simplu de management nu mai poate face față. Arhitectura de management descentralizată a fost prima abordare existentă în implementarea funcțiilor de management. Are avantajul că oferă flexibilitate, fiind proiectată să față tuturor tipurilor de trafic din zona pe care o acoperă. Problemele legate de faptul că practic fiecare astfel de zonă este izolată, se datorează faptului că efortul depus pentru configurare şi suport este mai mare şi dacă reteaua este foarte mare este dificil de avut o viziune de ansamblu asupra comportamentului acesteia.

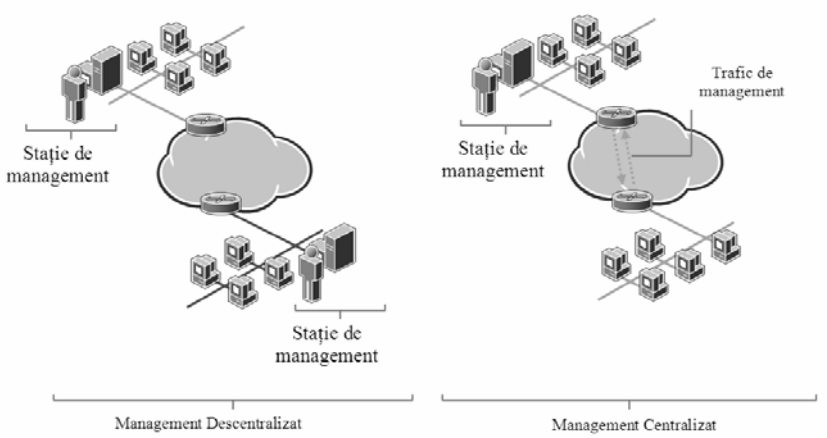

Figura 1.2 Management Centralizat sau Descentralizat

Comunicarea Manager – Agent

Un lucru important care trebuie adăugat la cele de mai sus este legată de procesul de comunicare dintre manager şi agent. Folosind acest proces agentul trimite informaţiile către manager. Comunicarea se bazează de obicei pe suportul de transport oferit de un anume protocol de management care este specific în general tehnologiei folosite. Din punctul de vedere al modului de transmitere a informaţiilor exista două mari categorii:

- Comunicare bazată pe interogare
- Comunicare bazată pe evenimente

Cea mai folosita metodă este de fapt o combinaţie între cele două prezentate mai sus. În acest caz mesaje bazate pe evenimente vor fi transmise în cazuri excepţionale, în timp ce mecanismul de interogare va fi folosit cu intervale de interogare mai mari. Uneori este posibil ca un mesaj generat de agent în cazul unui eveniment să conduca la generarea unor mesaje de interogare pentru a obţine mai multe informaţii.

1.2 Scop teză

La data începerii cercetărilor pentru această teză, reţelele locale de calculatoare utilizau un management centralizat bazat pe protocolul SNMP. Evoluţia reţelelor de telecomunicaţii a adus în prim plan şi alte arhitecturi cum ar fi TMN şi CMIP, dar care se pare că au pierdut „bătălia" pentru supremaţie cu SNMP. În plus au apărut şi alte tipuri de reţele cum ar fi : WPAN, WLAN, WAN, MAN, WMAN la care s-a pus problema dacă SNMP poate fi generalizat. Teza îşi propune să investigheze posibilităţile de implementare SNMP în orice tip de reţea locală şi personală indiferent de tipul de tehnologie de strat 1 şi 2.
Pe durata desfăşurării cercetărilor au apărut concepte noi, cum ar fi managementul distribuit, managementul integrat şi managementul intrinsec. De aceea teza şi-a propus în plus să demonstreze că odată ce SNMP a fost generalizat se poate trece la următoarea fază şi anume la managementul integrat. S-au abordat atât soluţii hardware cât şi software inclusiv pentru tehnologii care nu au avut suport implicit pentru SNMP (ex. IEEE 802.15.4).

S-a dorit să se demonstreze că pentru tehnologiile IEEE 802.3 (LAN), IEEE 801.22 (WLAN) şi IEEE 802.15.4 (WPAN) protocolul propus de IETF poate fi generalizat. În ultima parte teza şi-a propus să demonstreze care sunt paşii necesari integrării managementului în echipamentele hardware existente, precum şi în aplicaţiile software. Ca un studiu de caz s-a ales platforma Asterisk, adică un PBX IP la care s-au conectat toate tipurile de interfeţe studiate. De menţionat că teza nu şi-a propus să studieze tehnologiile WAN, MAN şi WMAN.

1.3 Organizare teză

În continuare, acest document este organizat în modul următor :
Capitolul 2 „Arhitecturi pentru managementul rețelelor de telecomunicații” descrie principalele arhitecturi de management existente (SNMP, TMN, CMIP, CMOT). Accentul a fost pus pe arhitectura SNMP, fiind prezentate versiunile, structura informației de management, baza de date cu informații de management, regulile de încapsulare şi formatul mesajelor. Celelalte arhitecturi concurente (TMN, CMIP şi CMOT) au fost abordate sintetic, prezentându-se cadrul de lucru, obiectivele şi modelul funcțional.
Capitolul 3 “Agent hardware pentru managementul rețelelor locale IEEE 802.3, 802.3u” este dedicat modalităților de implementare hardware a agenților SNMP care obțin informații despre rețele de tip Ethernet, FastEthernet, folosind MIB-II. În ideea unui agent generic s-a optat pentru o soluție bazată pe microcontrolerul MC9S12NE64 de la Freescale.
Capitolul 4 „Agent hardware pentru managementul rețelelor personale IEEE 802.15.4” prezintă mecanismele care pot face posibilă integrarea într-un sistem de management a echipamentelor care folosesc la nivelul stratului fizic şi MAC standardul IEEE 802.15.4. Pe platforma hardware propusă în capitolul 3 se înlocuieşte MIB-II cu un nou MIB şi se adaugă partea de coordonator PAN. În plus apare şi interfața radio bazată pe CC2420 de la Texas Instruments.
Capitolul 5 „Agent software pentru managementul rețelelor locale fără fir IEEE 802.11” este dedicat monitorizării rețelelor WLAN folosind SNMP. Ideea a fost să se înlocuiască MIB existent cu un nou MIB care să fie orientat pe rețea şi nu pe echipament. Soluția se bazează pe interfața AirPcap şi analizorul de protocoale Wireshark şi pe un nou agent software.
Capitolul 6 “Agent software pentru managementul aplicațiilor VoIP în rețelele locale cu şi fără fir” prezintă modalitatea de extindere a unui MIB deja definit pentru aplicații. S-a ales ca studiu de caz centrala telefonica PBX-IP Asterisk iar aplicațiile sunt bazate pe VoIP.
Capitolul 7 “Manageri software pentru rețele locale şi personale” prezintă aplicații existente (HP OpenView, Net-SNMP, PRTG Network Monitor, Open NMS). S-a implementat o aplicație numită SNMP Manager necesară pentru demonstrarea propunerii de tranziție spre un management integrat. În acest scop, pe platforma Asterisk sub Linux pot fi integrați toți agenții propuşi anterior şi se poate utiliza soluția AgentX pentru o arhitectură multi-agent.
Capitolul 8 “Contribuții la managementul rețelelor locale şi personale de telecomunicații” sintetizează cele 8 contribuții aduse la managementul rețelelor locale şi personale de telecomunicații. Sunt incluse şi concluziile finale ale tezei, iar publicațiile sunt grupate astfel: publicații personale citate în teză, referate de doctorat, publicații în afara scopului tezei.

Capitolul 2. Arhitecturi pentru managementul rețelelor de telecomunicații

2.1 Arhitectura SNMP

În acest capitol vor fi descrise cele mai cunoscute sisteme de management existente în acest moment. Primul paragraf va descrie sistemul de management bazat pe protocolul SNMP (Simple Network Management Protocol), cel de al doilea descrie sistemul bazat pe TMN, iar în ultima secțiune o descriere a sistemului bazat pe CMIP (dezvoltat ca un înlocuitor pentru SNMP).

Versiuni SNMP

Scopul SNMP este de a oferi un set simplu de operații (şi informații pe care aceste operații le obțin) care dau administratorului posibilitatea de a afla şi schimba starea unor echipamente, cu condiția să aibă implementat acest protocol. A existat un predecesor numit SGMP (Simple Gateway Management Protocol) care a fost gândit doar pentru a controla routere din Internet. Spre deosebire de acesta, SNMP poate controla diverse sisteme de operare şi echipamente. El este elementul central al Internet Standard Management Framework (ISMF) care conține două tipuri de entități SNMP (manageri şi agenți), un protocolul de transfer a informației şi informația propriu zisă de management. Proiectanții IETF au dezvoltat până acum trei versiuni majore de protocol. Acestea sunt prezentate în Tabelul 2.1.

Versiune	Descriere
SNMPv1	A fost gândit ca un protocol simplu şi robust pentru managementul rețelelor IP, mai ales pentru partea de configurare şi defecte. Rezultatul a fost un protocol acceptat de marea majoritate a producătorilor, şi astfel aproape toate echipamentele au suport pentru SNMP. Dezavantajul este că nu are suport decât pentru rețele IP, este ineficient la transferul unor cantități mari de informație, şi practic este fără nici un mecanism de securitate.
SNMPv2	Această versiune a încercat să elimine dezavantajele primei versiuni, însă a fost dificil să se găsească o soluție agreată de toată lumea şi de aceea au apărut mai multe versiuni ale acestui standard. Din păcate în industrie a existat reticentă la implementarea acestui protocol.
SNMPv2p	SNMPv2p a adus îmbunătățiri protocolului de comunicare, la partea de operații, tipuri de date şi unele îmbunătățiri la mecanismul de securitate.
SNMPv2c	Această versiune este numită "community string-based SNMPv2". Foloseşte acelaşi mecanism de securitate ca şi SNMPv1 bazat pe nume de comunitate.
SNMPv2u	La fel ca şi SNMPv2c, dar a îmbunatatit sistemul de securitate, prin introducerea unui mecanism de autentificare criptat.
SNMPv3	Versiunea 3 a adus schimbări mari nu numai la protocol în sine dar şi la conceptele din sistemul de management. Permite securitate bazată pe criptografie, permițând protecție prin autentificare.

Tabelul 2.1 Versiuni de SNMP

Un manager este un echipament (un server) denumit NMS (Network Management Station) pe care rulează un sistem de operare capabil să ofere servicii de management pentru rețea. El este responsabil pentru interogarea şi primirea de notificări din partea agenților din rețea. Al doilea tip de entitate, agentul, este un program care rulează în echipamentele din rețea care sunt gestionate. Poate fi un program independent (un daemon) sau poate fi integrat în sistemul de operare al echipamentelor.

Structura informației de management (SMI)

Informația de management este informația despre nodurile şi echipamentele gestionate. Ea poate fi organizată în variabile, fiecare mentinând anumite aspecte sau proprietăți ale elementului de rețea, conform [Ros90] şi [McC99]. Fiecare element de informație este conceput ca o abstractizare folosind notiunea de obiect gestionat. Ele reprezintă resurse fizice sau logice care sunt gestionate, iar proprietățile acelor obiecte reprezintă informația efectivă.

Întrucât acestea nu sunt decât convenții utilizate între manager şi agent, s-a impus introducerea unor reguli. Pentru început, există un număr redus de tipuri de date posibile. Dacă sunt puține tipuri posibile de date, implementările pot fi simplificate. În al doilea rând fiecare obiect trebuie să fie identificat.

În general o colecție de obiecte gestionate se numeşte bază de informații de management MIB (Management Information Base). Regulile de definire a acestor obiecte, comportarea lor, regulile de definire a MIB-lui poartă numele de structură de informații de management SMI (Structure of Management Information). Au apărut până în momentul de față, două versiuni pentru SMI. SMI se ocupă cu reguli şi convenții pentru datele de management care sunt definite în MIB şi sunt transportate de protocol. Prima versiune de SMI avea următoarele obiective:

- Specificarea structurii şi căilor dintr-un arbore MIB, cu reguli precise despre localizarea obiectelor şi unde pot fi adaugate noi obiecte. Arhitectura MIB a fost creată utilizând convențiile ASN.1
- Specificarea modului de definire a obiectelor gestionate. Aceasta înseamnă sintaxa, semantica, tipuri de date, atribute, codare, etc.. Definirea textuală a fiecarei definiții a unui obiect care se găseşte în MIB se numeşte *macro*.

SMIv2 a adus numeroase îmbunătățiri. A crescut numărul de tipuri de date pentru a veni în întâmpinarea cererilor dezvoltatorilor (mai multe tipuri pe 32 şi 64 biți) şi un număr de tipuri de obiecte.

Baza de date cu informații de management (MIB)

Management Information Base (MIB) este o bază de date virtuală, care conține informațiile de management de la echipamentele gestionate. MIB defineşte obiectele gestionate pe care un manager le monitorizează la un agent SNMP, conform [Sta98]. Fiecare sistem din rețea menține un MIB care reflectă starea resurselor din sistem. MIB nu conține date statice, dar în schimb este o bază de date orientată pe obiect, care conține o colecție logică de definiții ale obiectelor monitorizate. MIB defineşte tipul datelor şi descrie fiecare obiect. MIB este organizat în formă de arbore unde nodurile arborelui reprezintă obiectele monitorizate. Obiectele care au legătură directă cu SNMP se găsesc pe ramura *internet* care conține două mari ramuri :

- *mgmt=2*, care este definită de către RFC-urile de la Internet Engineering Task Force (IETF) şi este aceeaşi pentru toate obiectele SNMP
- *private=4*, care este menținută de către Internet Assigned Numbers Authority (IANA), şi este definită de către companii şi organizații la care fiecare ramură este atribuită

Management *(mgmt)*, este ramura publică cea mai folosită, defineşte parametri de management a rețelelor care sunt comuni la toate echipamentele de la toti producătorii. În continuarea acestei ramuri se găseşte MIB-II (*mib-2*) – un MIB special care trebuie implementat de către orice echipament care suportă SNMP.

Obiecte monitorizate

Definirea fiecărui obiect din MIB, din punct de vedere al programării, include următoarele elemente:

- un nume de obiect şi un identificator (cunoscut ca şi OID).
- descrierea textuală a obiectului
- definiția tipului de date a obiectului
- nivelul de acces permis asupra obiectului
- restricții legate de dimensiuni

SNMP accesează fiecare variabilă din MIB folosindu-se de OID (Object Identifier), care identifică localizarea unui obiect dat în MIB. OID reflectă poziția obiectului în ierarhia arborescentă a MIB, continând o secvență de identificatori care încep cu rădăcina arborelui şi până la obiect. Identificatorii sunt separați cu ".". În Figura 2.1 se prezintă o modalitate de a identifica obiectul fie prin denumire textuală a identificatorilor fie prin reprezentarea zecimală.

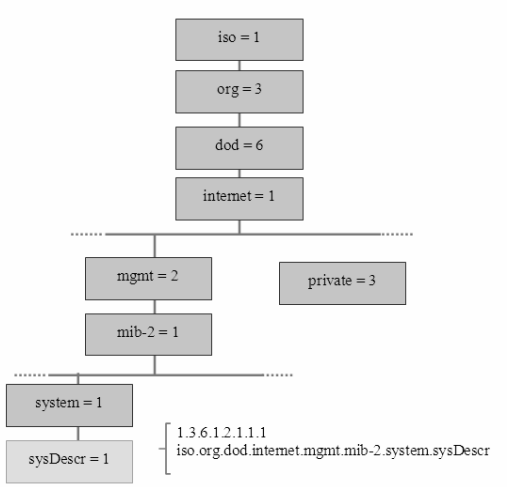

Figura 2.1 Identificarea obiecteler (OID)

Corespunzător fiecărui identificator de obiect vom găsi valoarea acelui identificator care identifică starea actuală a acelui obiect. SNMP se foloseşte de identificatorul în format zecimal cu punct pentru a accesa valoarea curentă a acelui obiect.

Exemple de MIB

În continuare urmează scurte prezentări a MIB-urilor existente şi opțiunile de creare a unora noi. În mod normal un manager trebuie să cunoască toate MIB-urile care sunt folosite în rețea. Cel mai cunoscut MIB este Internet Standard MIB sau MIB-II [McC91]. Acest lucru se datorează faptului că trebuie implementat în orice echipament cu SNMP activat. Acest MIB este o versiune îmbunatățită a lui MIB-1[McC90] şi contine obiecte generale. MIB-I conține un număr relativ mic de obiecte (114). Aceste obiecte inițial definite sunt esențiale pentru managementul configurărilor şi a defectelor. MIB-II a crescut numărul de obiecte la 117, acestea fiind grupate în 11 grupuri (cu 2 mai mult decat MIB-I).

În plus, față de Internet Standard MIB, există multe alte MIB-uri standardizate de către IETF în scopul folosirii altor tehnologii în Internet, de exemplu Frame-Relay-DTE-MIB, ISDN-MIB, RMON-MIB şi RMON2-MIB. Pe lângă aceste MIB-uri există alte MIB-uri standardizate de IETF, şi care sunt specifice fiecărui tip de echipament. Acestea sunt înregistrate sub ramura *enterprise* şi sunt folosite pentru a îmbunătăîi şi extinde functionalitatea şi suportul pentru aceste echipamente. Informații suplimentare despre aceste MIB-uri se găsesc în anexa 2.

Nume grup	**OID**	**Descriere**
system	1.3.6.1.2.1.1	Conține informații generice despre echipament, persoana de contact.
interfaces	1.3.6.1.2.1.2	Conține obiecte care reprezintă parametri ai interfețelor din nodului respectiv.
address translation	1.3.6.1.2.1.3	Conține informații de mapare adrese IP la adrese fizice (similar cu tabela ARP).
ip	1.3.6.1.2.1.4	Conține informații despre protocolul IP.

icmp	1.3.6.1.2.1.5	Conține informații despre protocolul ICMP
tcp	1.3.6.1.2.1.6	Conține informații despre protocolul TCP
udp	1.3.6.1.2.1.7	Conține informații despre protocolul UDP
egp	1.3.6.1.2.1.8	Conține informații despre protocolul EGP
cmot	1.3.6.1.2.1.9	Conține informații despre protocolul CMOT
transmission	1.3.6.1.2.1.10	Conține informații despre tipuri specifice de interfețe (IEEE 802.3 sau IEEE 802.5).
snmp	1.3.6.1.2.1.11	Conține informații despre protocolul SNMP.

Tabelul 2.2 Primele nivele din MIB-2.

În momentul de față există foarte multe MIB-uri definite fie de IETF, fie de producătorii de echipamente sau diverse instituții. Un sistem de management ar trebui să fie capabil să obțină informații din toate aceste MIB-uri. Acest lucru poate pune probleme referitoare la cantitatea de informații care ar trebui procesate de stațiile de management. Pentru a ușura sarcina stațiilor de management, a fost propusă o arhitectură de distribuție a acestor MIB-uri pe mai multe stații [Bor01].

Reguli de încapsulare

BER (Basic Encoding Rules) stabileşte regulile de încapsulare a fluxurilor de date fiind parte din standardul ASN.1. Schema de încapsulare se mai numeşte TLV (type-length-value). Aceste reguli de încapsulare precizează că fiecare secvență de date este încapsulată prin identificatorul de tip, lungime, şi valoarea propriu-zisă, un întreg PDU fiind de fapt o înşiruire de unități de încapsulare de tip TLV. Câmpul *tip* are lungimea de un octet, iar câmpul lungime specifică lungimea următoarelor secvențe, iar după lungime urmează valoarea domeniului, care la rândul ei se poate încapsula TLV [Sim97].

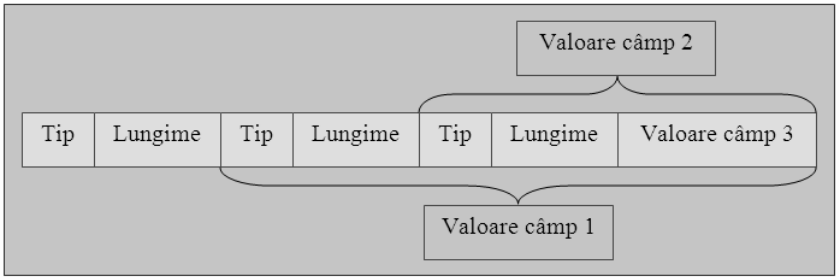

Figura 2.2 Încapsularea BER a unei secvențe de date

În structura câmpului *tip* primii doi biți definesc clasa din care face parte fiecare tip de date. SNMP utilizează primele trei tipuri de clase: *universal , aplicație şi context special*.

Următorul câmp este cel pentru *lungime*, acesta determină numărul de octeți din câmpul valoare. Acest câmp poate folosi două moduri diferite pentru a preciza valoarea. Primul mod se aplică când numărul de octeți din câmpul *valoare* este cuprins între 0 şi 127. În acest caz primul bit (MSB) este întotdeauna 0. Cel de al doilea mod se foloseşte pentru lungimi mai mari de 128 octeți. În acest caz bitul 8 va avea valoarea 1, ceilalți şapte biți precizând numarul de octeți care urmează în câmpul lungime. Acest număr trebuie să fie între 1 şi 126, 127 fiind rezervat pentru extinderi ulterioare.

Format mesaje SNMP v1, v2, v3

SNMP foloseşte UDP (User Datagram Protocol) ca şi protocol de strat transport pentru a transfera date între manager şi agent. El a fost ales în defavoarea protocolului TCP pentru că este neorientat pe conexiune, însemnând că nu trebuie stabilită o legatură prealabilă între

agent şi manager. Acest lucru poate introduce probleme suplimentare, din cauză că nu există confirmări pentru pachetele transmise şi pierdute. Rămâne în sarcina aplicației SNMP să determine dacă pachetul a fost pierdut şi să încerce retransmisia dacă se doreşte.
Protocolul de comunicație în SNMP se bazează pe operații de cerere de informații şi primirea răspunsului. Un mesaj SNMP conține o unitate de împachetare a datelor (PDU) la care se adaugă un antet (conținutul acestuia diferă de la o versiune de SNMP la alta). Un agent SNMP va trimite informații în două cazuri :

1. ca răspuns la o cerere formulată de manager
2. când are loc un eveniment şi se generează o notificare

În versiunea 1 a protocolului au fost definite următoarele tipuri de operații care pot fi folosite de către manager şi agent.

Nume operație	**Direcție**	**Descriere**
Get	Manager → Agent	Accesarea valoarea unui obiect din agentul SNMP
Get-Next	Manager → Agent	Accesarea tuturor obiectelor din MIB, prin citirea acestor în mod secvențial
Set	Manager → Agent	Schimbarea valorii curente a unui obiect din MIB
Get-Response	Agent → Manager	Răspuns la *Get, Get-Next şi Set*
Trap	Agent → Manager	Notificarea unui SNMP manager de apariția unor evenimente

Tabelul 2.3 Operații definite în SNMPv1.

În versiunea 2 a standardului au fost adăugate următoarele tipuri de operații:

Nume operație	**Direcție**	**Descriere**
Get-Bulk	Manager → Agent	Accesarea unor informații în cantități mari, minimizând numarul de mesaje schimbate
Notification	Agent → Manager	Acelaşi tip ca şi Set şi Get, inițial gândit pentru notificări
Inform	Manager → Manager	Folosit la comunicarea între manageri
Report	--	Nu a fost implementat

Tabelul 2.4 Operații adăugate în SNMPv2.

Securitatea în SNMPv1 şi SNMPv2

În ambele versiuni de protocol varianta cea mai implementată de securitate este cea bazată pe comunități. În SNMPv2 au fost prevăzute modalități de autentificare a utilizatorului, ele nu prea sunt implementate. Practic SNMPv1 şi SNMPv2 nu implementează nici o metodă de autentificare sau criptare, fiind vulnerabile la o multitudine de atacuri de securitate.

Din aceste motive, cei mai mulți producători de echipamente oferă suport doar pentru monitorizarea echipamentelor, partea de control (echivalentul operației *set*) fiind disponibilă doar prin conectare directă la echipament. Partea de securitate a fost rezolvată prin introducerea versiunii 3 a acestui standard (SNMPv3).

SNMPv3

Specificațiile pentru SNMPv3 au fost aprobate de către IESG (Internet Engineering Steering Group) ca standard în anul 2002. Prima variantă de standard (draft) fusese aprobată de acelaşi comitet în 1999. Principalele modificări aduse se referă la securitate şi la posibilitatea de configurare de la distanță a echipamentelor. Prin modalitatea de elaborare, prima impresie este că lucrurile diferă foarte mult față de versiunile precedente, prin introducerea de noi convenții, concepte şi terminologii. În standard este descrisă arhitectura globală de

management şi se prezintă mult mai detailat modalitatea de implementare a echipamentelor care vor oferi suport pentru SNMP.

În noua arhitectura, conceptul de agent şi manager nu mai există. A fost introdus conceptul de entitate SNMP, care poate fi manager, agent sau ambele. Mai multe detalii se găsesc în paragrafele care urmează. Prin acest mod de prezentare practic se defineşte o arhitectură, în loc de un simplu set de mesaje şi operaţii. Specificaţiile pentru această arhitectură au fost definite în [Har02].

Entităţi SNMPv3

Structura unei entităţi SNMPv3 este prezentată în Figura 2.3 [Cas99a].

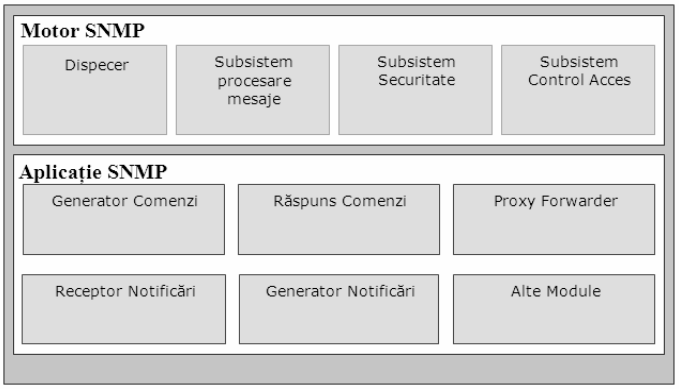

Figura 2.3 Structura unei entităţi în SNMPv3

În SNMPv3 motorul SNMP are rolul de a recepţiona şi trimite mesaje SNMP, ca la manager sau agent din vechile versiuni [Cas99b]. Pe lângă aceste funcţii mai oferă servicii de autentificare, criptare şi control acces. Principalele componente sunt descrise în Tabelul 2.5.

Componentă	**Descriere**
Dispecer	Are rolul de a trimite şi recepţiona mesaje SNMP. Determină versiunea de protocol folosită şi dacă versiunea este suportată transferă mesajul spre subsistemul de procesare mesaje
Subsistem procesare mesaje	Pregăteşte mesajul care va fi transmis sau extrage datele din mesajele recepţionate. Conţine câte un submodul separat pentru fiecare versiune de SNMP suportată
Subsistem securitate	Se ocupă de autentificare şi criptarea datelor
Subsistem control acces	Controlează accesul la obiectele din MIB.

Tabelul 2.5 Componentele principale ale motorului SNMP

Aplicaţia SNMP se foloseşte de serviciile motorului SNMP şi oferă partea de funcţionalitate deja cunoscută în SNMP. Componentele principale sunt :

Componentă	**Descriere**
Generator comenzi	Generează cererile *get*, *get-next*, *get-bulk*, şi *set* şi procesează răspunsurile. Funcţiile oferite sunt specifice managerilor.
Răspuns comenzi	Răspunde la cererile *get*, *get-next*, *get-bulk*, şi *set*. Funcţiile oferite sunt specifice agenţilor.
Generator notificări	Generează notificări. Funcţiile oferite sunt specifice agenţilor.
Receptor notificări	Recepţionează notificări. Funcţiile oferite sunt specifice managerilor.
Proxy Forwarder	Implementează mecanismul de transfer de mesaje între diverse entităţi SNMP

Tabelul 2.6 Componentele principale ale aplicaţiei SNMP

Ca şi la precedentele versiuni, mesajul SNMP are două părți : un antet şi o unitate de date protocol (PDU). Nu există modificări la partea de unitate de date protocol, fiind la fel ca la SNMPv2 doar că poate fi criptat dacă este cazul [Zel99]. În schimb, antetul SNMPv3 conține 13 câmpuri importante pentru partea de identificare şi autentificare.

Securitatea în SNMPv3

Principalele obiective fixate pentru securitate în SNMPv3 se referă la:

- determinarea dacă un mesaj a ajuns la destinație fără erori şi în timp util
- să determine dacă operația cerută poate fi efectuată, ținând cont de drepturile utilizatorului
- determinarea permisiunilor pentru un mesaj recepționat în funcție de cine l-a generat

Aceste obiective sunt îndeplinite de modulele de securitate şi control acces [Wij98]. SNMPv3 suportă mai multe modele de securitate (definite deja sau care vor fi definite). Pentru a menține compatibilitate între echipamente, fiecare echipament trebuie să implementeze modelul USM (User-based Security Model) [Blu98]. Acest model implementează următoarele :

- autentificare – autentificarea utilizatorului (poate folosi algoritmii MD5 şi SHA)
- Oportunitate în timp – protejare împotriva modificării fluxului de mesaje prin trimiterea timpului în fiecare mesaj
- Criptare – foloseşte algoritmul DES pentru criptarea şi decriptarea mesajelor.

2.2 Arhitectura TMN

Obiective TMN

Telecommunication Management Network, prescurtat TMN, a fost pentru mulți ani una dintre cele mai complexe platforme de management, proiectată să facă față cerințelor din rețelele de telecomunicații de astăzi.
TMN este un cadru de lucru conceptual, dezvoltat de ITU pentru a interconecta diverse sisteme de operare şi rețele de telecomunicații. El definește infrastructura necesară pentru a putea implementa managementul serviciilor de telecomunicații [M.3000].

Cadru de lucru

TMN ca model operational este gândit pentru a atinge două obiective importante: interoperabilitatea între diverse platforme şi optimizarea funcționalității rețelelor, vezi [M.3010]. Standardul a fost publicat de către ITU-T în seria recomandărilor M.3000, care se bazează pe standardele OSI deja existente [Div99]. TMN utilizează conceptele din sistemul de management al OSI şi le aplică în managementul telecomunicațiilor. Aceasta înseamna că TMN se bazează pe modelul de referință OSI, CMIP şi CMISE pentru management, GDMO ca şi reguli pentru descrierea informatiei de management (similar cu SMI de la IETF), ASN.1.

El oferă o arhitectură centralizată pentru managementul sistemelor de tip multi-vendor, prin următoarele:

- Concepte şi definiții
- Principii de rețea, unele fiind deja existente în standardele OSI
- Zone funcționale de management
- Model informațional
- Arhitectura fizică

Arhitectura TMN

Chiar dacă TMN este din punct de vedere conceptual o entitate separată, conectată la rețeaua de telecomunicații prin intermediul interfețelor, poate folosi o parte din rețea pentru comunicarea proprie, conform [M.3010]. Aşa cum s-a arătat mai devreme conceptul TMN include calculatoare, baze de date, terminale, rețele de comunicații. TMN are o arhitectură organizată în aşa fel încât să poată interconecta diverse elemente de rețea şi OSS. TMN precizează interfețele standard şi protocoalele folosite pentru a schimba informații între OSS şi elemente de rețea şi de asemenea tot ce este nevoie pentru o rețea de management [Shr95].

TMN poate fi folosit pentru o simplă conexiune între OSS şi NE, cât şi pentru rețele compuse din mai multe OSS şi un număr mare de elemente de rețea. Figura următoare arată relația de legatură dintre TMN şi rețeaua de telecomunicații. Aceasta constă dintr-un număr de sisteme de management (OSS) şi multe elemente de retea (NE) conectate prin intermediul interfeței Q3.

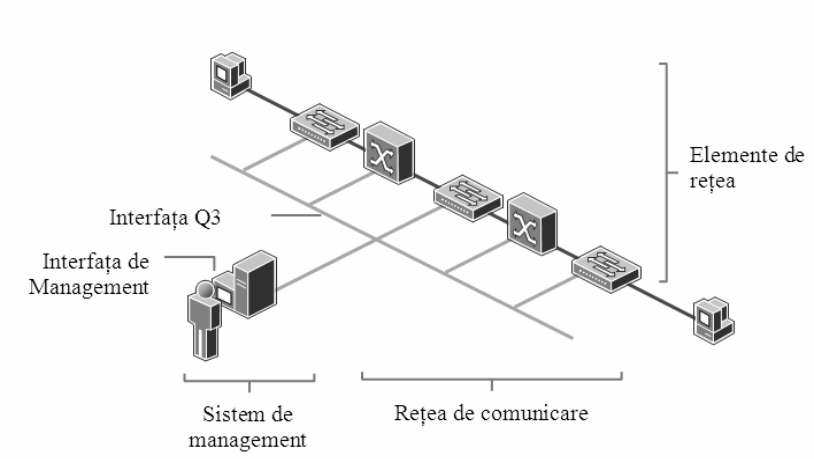

Figura 2.4 Arhitectura TMN

Pentru a putea descrie un sistem de management în mod schematic, recomandările TMN au definit o interfață şi un număr de modele:

- Un model logic care defineşte sau sugerează diverse nivele de management care pot fi implementate începand cu cel mai înalt nivel folosit pentru managementul corporațiilor până la cel mai de jos nivel folosit pentru managementul resurselor de rețea.
- Un model funcțional care împarte atât rețeaua cât şi procesul de management în zone cu funcționalități specifice. Pentru fiecare din acestea TMN precizează interfețele şi modul de interconectare
- Un model fizic, care se ocupă cu diverse tipuri de echipamente şi interconectarea lor folosind mediul de transmisie. De exemplu modelul fizic specifică tipul tehnologiei care este cea mai potrivită pentru TMN (în cazul legăturii între OSS şi NE folosind interfața Q_3 soluția recomandată este comutația de pachete de tip X.25 sau Frame Relay)

2.3 Arhitecturi CMIP şi CMOT

CMIP (Common Management Information Protocol) este un protocol pentru managementul rețelelor, oferind implementări pentru servicii definite cu ajutorul CMISE (Common Management Information Services), permițând comunicarea dintre aplicații de management al rețelei şi agenți. Combinația CMISE/CMIP se bazează pe modelul de referință OSI (elaborat de ISO) şi a fost definit în seria de standarde ITU-T X.700. Acest paragraf va prezenta sintetic aceste arhitecturi, pentru mai multe detalii se pot consulta [X.701], [X.710-711] şi [X.720-722].

Modele de management

Managementul rețelelor poate fi modelat în mai multe feluri. Din punctul de vedere al OSI există trei modele. Primul model (model organizațional) descrie modurile în care partea de management poate fi distribuită din punct de vedere administrativ. Modelul funcțional descrie funcțiile de management şi legăturile între ele, iar modelul informațional oferă indicații despre cum se descriu obiectele monitorizate şi informațiile asociate cu aceste obiecte.
Pentru funcționarea CMIP a fost elaborată o suită de protocoloale pentru nivelurile din modelul de referința OSI. Legăturile între protocoalele din suita CMIP este descrisă în Figura 2.5 [War89].

Modelul OSI
Aplicație
Prezentare
Sesiune
Transport
Rețea
Legături date
Fizic

Stiva CMIS/CMIP	
CMIS ISO 9595	CMIP ISO 9596
ACSE ISO 8649/8650	ROSE ISO DIS 9072-1/2
Protocol ISO Prezentare	
Protocol ISO Sesiune	
Protocol ISO Transport	
Protocol ISO Rețea	
Protocol ISO Legături date	
Protocol ISO Fizic	

Figura 2.5 Suita de protocoale CMISE/CMIP

Arhitectura de management CMOT

Managementul rețelelor care folosesc stiva TCP/IP folosind CMIP este cunoscut sub denumirea de CMOT. Un echipament compatibil cu acest protocol trebuie să implementeze următoarele protocoale : ACSE, ROSE, CMIP, LPP, UDP, TCP şi IP. Poziționarea acestor protocoale referitor la modelul de referință OSI poate fi observată în Figura 2.6.

Modelul OSI
Aplicație
Prezentare
Sesiune
Transport
Rețea
Legături date
Fizic

Stiva CMOT	
CMIS ISO 9595	CMIP ISO 9596
ACSE ISO 8649/8650	ROSE ISO DIS 9072-1/2
Lightweight Presentation Protocol (LPP) RFC 1085	
TCP RFC 793	UDP RFC 768
IP RFC 791	
Protocol Legături date	
Protocol Fizic	

Figura 2.6 Suita de protocoale CMOT

Capitolul 3. Agent hardware pentru managementul rețelelor locale IEEE 802.3, 802.3u

3.1 Standarde IEEE 802.3, IEEE 802.3u

IEEE 802.3 a fost prima dată publicat în 1985. De atunci au apărut diverse proiecte care au încercat să țină pasul cu dezvoltarea tehnologică. Specificațiile acestui standard acoperă funcțiile stratului fizic şi a substratului MAC, conform modelului de referință OSI [Tan03].
Pentru stratul fizic prima versiune specifică un debit binar de 10 Mbps. De atunci s-au tot adăugat alte opțiuni de strat fizic ajungându-se până la 40 Gbps şi 100 Gbps. Variantele cele mai folosite în ziua de azi sunt IEEE 802.3u cu debit binar de 100 Mbps (cunoscut sub numele de Fast Ethernet) şi IEEE 802.3z cu debit binar de 1000 Mbps (Gigabit Ethernet).

Pentru substratul MAC standardul defineşte mecanismul de control al accesului la mediul de comunicație, care este *Carrier Sense Multiple Access with Collision Detection* (CSMA/CD). Pe lânga acest mecanism în standard se descrie şi formatul cadrelor folosite. Structura unui cadru se poate observa în Figura 3.1. Detalii suplimentare se găsesc în [802.3], [Spu00] şi [Zin06].

7 octeți	1 octet	6 octeți	6 octeți	2 octeți	0..1500 octeți	0..46 octeți	4 octeți
Preambul	Delimitator început cadru	Adresa destinație	Adresa sursă	Tip/ Lungime	Date	PAD	Suma Control

Figura 3.1 Structura cadrului IEEE 802.3 / Ethernet

Lungimea cadrului este de minimum 64 octeți, iar lungimea maximă de 1518 octeți, fără a lua în calcul câmpul preambul şi delimitator de început de cadru.

3.2 Implementare hardware bazată pe microcontrolerul MC9S12NE64

MC9S12NE64 este un microcontroler fabricat de Freescale (fost Motorola) destinat aplicațiilor care necesită costuri reduse de producție [Fre06]. El este compus dintr-un set standard de periferice, incluzând o unitate de calcul pe 16 biți (HCS12 CPU), 64 Kocteți de memorie FLASH EEPROM, 8 Kocteți de memorie RAM, un controler de acces la mediu de tip Ethernet (EMAC) care include şi un transceiver Ethernet de 10/100 Mbps, două porturi de comunicație asincronă (SCI), un port de comunicație serială sincronă (SPI), un port de comunicație I2C (Inter-Integrated Circuit), un modul timer cu 4 canale, fiecare canal având 16 biți, un modul de conversie analog-digital cu 8 canale de 10 biți fiecare. De asemenea include un modul PLL care permite ajustarea performanțelor şi a consumului de putere în funcție de aplicație.Dintre interfețele acestui microcontroler au fost folosite:

- Interfața serială SCI
- Interfața serială SPI
- Controlerul de acces la mediu Ethernet (EMAC)
- Tranceiver Ethernet 10/100 Mbps (EPHY)
- CRG (clock and reset generator module)

3.3 MIB pentru Internet (MIB II)

Internet Standard MIB sau MIB-II este o îmbunătățire a primei versiuni a MIB-ului dezvoltat pentru rețelele care folosesc stiva TCP/IP. Este situat sub ramura *mgmt* din arborele cu obiecte. Un echipament care se doreşte să fie compatibil cu SNMP trebuie să implementeze acest MIB [McC91]. Localizarea în arborele cu obiecte a grupurilor definite în MIB se prezintă în Figura 3.3. Acest MIB conține 171 obiecte monitorizate organizate în 11 grupuri după cum se observă în Tabelul precedent. Din cele 11 grupuri inițial definite, grupul cu informații legate de CMOT este păstrat doar din motive istorice. Pe lângă aceste grupuri mai există definite cinci obiecte care sunt folosite pentru notificări. Acest MIB a fost implementat în agentul hardware descris în acest capitol.

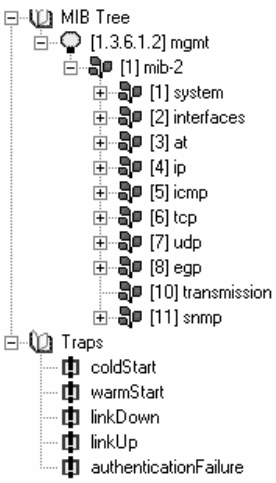

Figura 3.2 Grupurile definite în MIB-II

3.4 Implementare agent SNMP hardware pentru IEEE 802.3, 802.3u

Pentru relizarea unui agent SNMP de tip hardware avem nevoie de o interfață de tip Ethernet (care este oferită de microcontrolerul MC9S12NE64) plus scrierea în microcontroler a stivei de protocoale necesare pentru SNMP [Van05c]. În Figura 3.3 sunt prezentate protocoalele care au fost implementate pentru a activa standardul SNMP pe acel echipament şi localizarea lor conform modelului de referință OSI.

Modelul OSI	Protocoale implementate		
Aplicație	SNMP		
Prezentare			
Sesiune			
Transport	UDP		
Rețea	IP	ICMP	ARP
Legături date	IEEE 802.3		
Fizic	IEEE 802.3		

Figura 3.3 Protocoalele implementate în agentul SNMP

Pe lânga realizare stivei de protocoale, în agent trebuie implementat şi un MIB. Pentru a putea fi compatibil cu SNMP echipamentul trebuie să aibă cel puțin MIB-II [McC91]. În agentul SNMP există 3 module diferite: unul este pentru stiva SNMP, al doilea menține datele din MIB (MIB-II), iar cel de al treilea se ocupă cu colectarea datelor definite. În cazul în care se dorește conectarea acestui agent la un alt tip de echipament sau rețea, partea care trebuie modificată este cea care se ocupă cu colectarea datelor. Modulele existente în agent sunt prezentate în Figura 3.4.

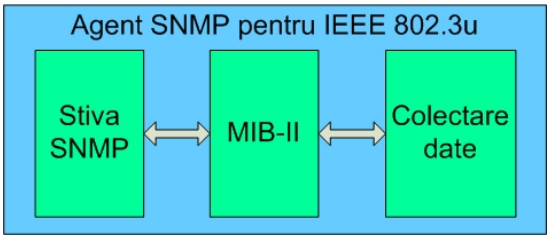

Figura 3.4 Modulele existente în agentul SNMP

Programul care va rula în microcontroler s-a dorit a fi modular, rezultând o structură relativ simplă a buclei principale. Softwareul a fost structurat astfel încât codul sursă care implementează fiecare protocol în parte se găseşte în fişiere sursă diferite, având astfel posibilitatea de a porta codul pe alte platforme fără mare efort. Sistemul de operare

implementat în microcontroler este un sistem de operare bazat pe întreruperi. Fiecare eveniment are asociată o întrerupere hardware, care la generarea ei va activa un „flag", care va fi tratat în bucla principală a sistemului de operare. O îmbunătățire care se poate aduce în această parte este legată de implementarea unui sistem de operare în timp real de tip RTOS (Real Time Operating System). În versiunea actuală au fost implementate protocoalele ARP, ICMP, IP,UDP, SNMP. În momentul în care se primeşte o cerere din partea managerului pentru a obține un anume OID, dacă pachetul a îndeplinit criteriile de securitate, următoarea verificare care se face este aceea de a verifica dacă obiectul cerut de manager este implementat de către agent. Acest lucru se realizează prin căutarea OID-ului receptionat, în tabelul menținut intern în memoria μC şi care conține OID-urile implementate. Singurele comenzi implementate sunt *get* şi *set*. Nu s-au implementat toate obiectele definite de MIB-II, ci doar grupurile *System, Interfaces, IP, ICMP, UDP* şi *SNMP*

Rezultate experimentale

Pentru a verifica corectitudinea implementării SNMP folosind microcontrolerul MC9S12NE64 au fost realizate câteva experimente în care a fost nevoie de un program manager Net-SNMP cu scopul de a genera şi recepționa comenzi SNMP. În paralel s-a utilizat utilitarul Ethereal (versiunea inițială a lui Wireshark) pentru verificarea corectitudinii pachetelor trimise şi recepționate.

Experimentele realizate au constat în generarea unor comenzi de către manager şi trimiterea acestora către agent. Acesta în cazul recepției pachetului îl va decoda, va interpreta cererea managerului şi va trimite un mesaj corespunzător. Astfel s-a încercat obținerea valorilor corezpunzătoare fiecărui OID implementat de către agent. În continuare vor fi prezentate rezultatele, prezentând atât răspunsul cât şi pachetul decodat cu ajutorul analizorului de protocoale.

Pentru aflarea numelui acelui sistem *sysName*, adică OID 1.3.6.1.2.1.1.1.5, s-a generat şi transmis din linia de comandă un mesaj SNMPv3 GET, aşa cum se observă în Figura 3.5.

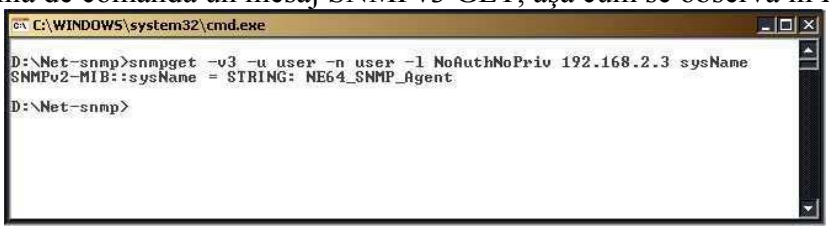

Figura 3.5 Comanda Net-SNMP pentru numele sistemului

Concluzii

S-a dorit realizarea unui agent SNMP hardware care să poată fi folosit independent, dar şi ca un punct de pornire pentru realizarea altor agenți. Echipamentul hardware folosind microcontrolerul MC9S12NE64 împreună cu protocoalele implementate în software au fost realizate şi testate cu succes folosind aplicații cunoscute în domeniu.
Bineînțeles că există şi părți care nu s-au putut realiza, cele mai multe din ele fiind din cauza resurselor limitate disponibile în μC (mai ales memoria). De exemplu implementarea mecanismele de securitate oferite de versiunea 3 a standardului SNMP lipseşte. Iar numărul de obiecte care pot gestionate de agent este mic.
Pentru eliminarea acestor neajunsuri şi pentru îmbunătățirea ulterioară a acestui agent se recomandă în viitor :

- adăugarea unui supliment de memorie (RAM+Flash) care să permită implementarea facilităților lipsă în acest moment
- implementarea mecanismelor de securitate oferite de versiunea 3 de SNMP

- folosirea altor tipuri de microcontrolere (în ultima perioadă au apărut circuite de la alți producatori, cum ar fi MicroChip sau Atmel) şi realizarea unui studiu comparativ. O primă diferență ar putea să o constituie faptul că MC9S12NE64 este un procesor CISC, iar celelalte sunt de tip RISC.

Capitolul 4. Agent hardware pentru managementul rețelelor personale IEEE 802.15.4

4.1 Standard IEEE 802.15.4

Această recomandare IEEE defineşte modalitățile de interconectare şi comunicare între echipamente, folosind comunicație radio, în domeniul PAN (Personal Area network). Se utilizează un control al accesului la mediu de tip CSMA-CA, şi sunt suportate atât topologii de tip stea cât şi de tip punct-la-punct. Accesul la mediu este de tip concurențial, dar folosind structuri de tip supercadru pot fi alocate cuante de timp de către coordonatorul de PAN pentru echipamentele care au de transferat date critice în timp. Standardul specifică în stratul fizic două posibilități: banda ISM 868/915 MHz folosind tehnici cu spectru distribuit (Direct Sequence Spread Spectrum - DSSS) şi banda ISM 2450 MHz tot cu tehnici cu spectru distribuit (DSSS). Pentru 2450 MHz debitul binar este de 250 kbps, iar pentru 868/915 MHz este 20 kbps şi 40 kbps.

Au fost definite următoarele tipuri de dispozitive [802.15.4]:

- **coordonator:** Este un echipament FFD care este configurat să ofere servicii de sincronizare prin transmiterea de cadre beacon.
- **full-function device (FFD):** Un echipament capabil să opereze ca şi coordonator sau echipament final şi care implementează întreg protocolul IEEE 802.15.4.
- **coordonator de PAN:** Un coordonator care este principalul coordonator din *PAN*. O rețea IEEE 802.15.4 are un singur astfel de dispozitiv.
- **reduced-function device (RFD):** Un dispozitiv funcționând cu o implementare minimă a protocolului IEEE 802.15.4.

Aceste echipamente acoperă un spațiu denumit spațiu de acoperire personală *POS (Personal Operating Space)* din jurul unei persoane sau obiect staționar sau mobil, având o valoare tipică de 10 m în toate direcțiile.

Topologii de rețea

În funcție de aplicație, echipamentele WPAN pot fi configurate să lucreze în:

- topologie stea
- topologie punct la punct (peer-to-peer)

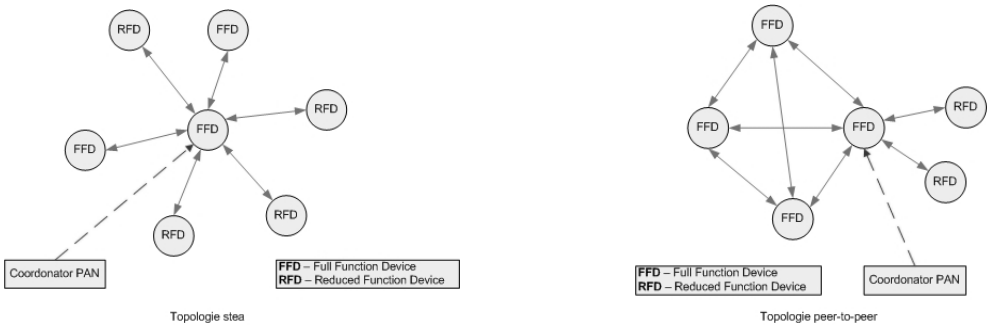

Figura 4.1 Topologii definite de IEEE 802.15.4

Stiva de protocoale WPAN

Arhitectura LR-WPAN este definită sub formă de straturi, cu scopul simplificării standardului, structură care se bazează pe modelul de referinta OSI. Interfețele dintre straturi servesc pentru a defini legăturile logice descrise în standard. Un echipament LR-WPAN cuprinde stratul fizic, care definește transmisia în radio frecvență, împreună cu mecanismele atașate, şi substratul MAC care oferă accesul la canalul fizic pentru toate tipurile de transfer definite. Legătura cu straturilor superioare poate fi făcută prin intermediul protocolului IEEE 802.2 LLC. Nivelele superioare (rețea până la aplicație) nu sunt definite în acest standard (ele fiind incluse în seria de standarde cunoscute sub denumirea „ZigBee").

Stratul fizic

Printre caracteristicile stratului fizic se numără activarea şi dezactivarea tranceiverului radio, detecția de energie, LQI (Link Quality Indication) pentru pachetele receptionate, CCA (Clear Channel Assessment) pentru tehnica CSMA/CA, selecția canalului, transmisia şi recepția pachetelor în şi din mediul fizic de transmisie.

Substratul MAC

Substratul MAC oferă două tipuri de servicii : servicii de date şi servicii de management, interfațându-se cu punctul de acces la servicii al unității de management MLME (cunoscută ca MLME-SAP). Serviciul de date permite transmisia şi recepția unităților de date MAC (MPDU) prin intermediul serviciului de date al stratului fizic. Facilitățile oferite de substratul MAC sunt: managementul cadrelor *beacon*, managementul GTS, accesul la canal, validarea cadrelor, transmiterea cadrelor de confirmare, asocierea şi disasocierea. De asemenea se oferă servicii pentru implementarea de mecanisme de securitate.

Structura cadrului IEEE 802.15.4

Structura cadrului a fost proiectată în aşa fel încât să mențină complexitatea la minim, dar şi suficient de robustă pentru a fi folosită la transmisii pe canale cu erori [Cal02]. LR-WPAN definește patru tipuri de structuri de cadru :

- Cadru beacon folosit de coordonator
- Cadru de date folosit pentru transferul datelor
- Cadru de confirmare folosit pentru confirmarea recepției cu succes a cadrelor
- Cadru de comandă MAC folosit pentru controlul transferului intre entitatile MAC

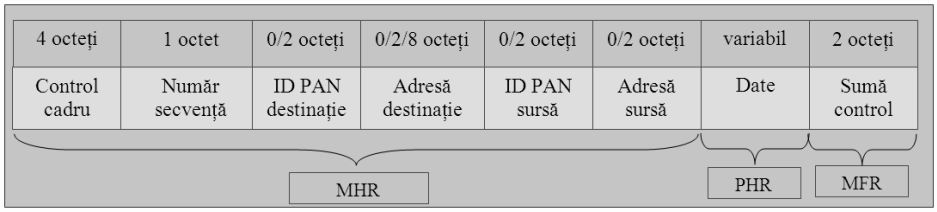

Figura 4.2 Formatul cadrelor pentru IEEE 802.15.4

4.2 Arhitectura hardware bazată pe microcontrolerul MC9S12NE64 şi CC2420

Circuitul CC2420

Circuitul integrat CC2420 este produs de către Texas Instruments şi este un circuit dezvoltat pentru a oferi comunicații fără fir, în banda de frecvență de 2.4 GHz, implementând funcțiile

stratului fizic şi ale substratului MAC pentru standardul IEEE 802.15.4. A fost proiectat să respecte prevederile ETSI EN 300 328 şi EN 300 440 clasa 2 (Europa), FCC CFR47 Part 15 (USA) şi ARIB STD-T66 (Japonia) [Tex07].
Acest circuit oferă suport hardware pentru criptarea şi decriptarea datelor, manipularea pachetelor, informaţii pentru calitatea legăturii. Aceste facilităţi implementate în circuit reduc cantitatea de informaţii care trebuie procesate de microcontrolerul ataşat, ceea ce conduce la posibilitatea de a folosi microcontrolere mai puţin performante. Comunicarea cu microcontrolerul se face prin intermediul interfeţei seriale SPI.

Printre facilităţile oferite de circuit se pot aminti :

- Putere de emisie programabilă
- Poate fi folosit pentru echipamente FFD şi RFD
- Suport pentru criptare implementat în hardware (AES-128)
- Debitul binar de 250kbps, debitul de simbol 2 Mchip/s
- Buffer de transmisie de tip FIFO de 128 octeţi
- Buffer de recepţie de tip FIFO de 128 octeţi
- Suport hardware pentru substratul MAC definit de IEEE 802.15.5
- Interfaţa SPI pe 4 fire pentru comunicarea cu microcontrolerul
- Generarea automată a preambulului
- Adăugarea automată a sumei de control CRC-16 şi verificarea la recepţie a corectitudinii sumei de control recepţionată

Acest circuit a fost folosit atât pentru coordonatorul de PAN cât şi pentru senzorii de temperatură descrişi în continuare.

Arhitectura sistemului propus

IEEE 802.15.4 a fost dezvoltat pentru a fi implementat de echipamente cu o complexitate redusă, care să consume foarte puţină energie. SNMP a fost dezvoltat pentru echipamente care implementeaza stiva de protocoale TCP/IP la care complexitatea nu era o problemă foarte mare. Din aceste motive integrarea echipamentelor care implementeaza IEEE 802.15.4 în sisteme de management care folosesc SNMP (dar şi în alte sisteme de management) pare irealizabilă. În ceea ce urmează voi prezenta un sistem care va permite integrarea echipamentelor IEEE 802.15.4 în sistemele de management existente. Soluţia propusă cuprinde un echipament hardware care implementează un MIB adaptat sistemului propus, conform [Van07a],[Van07b]. Abordări similare se găsesc în [Cho06]. Arhitectura sistemului propus poate fi observată în Figura 4.3.

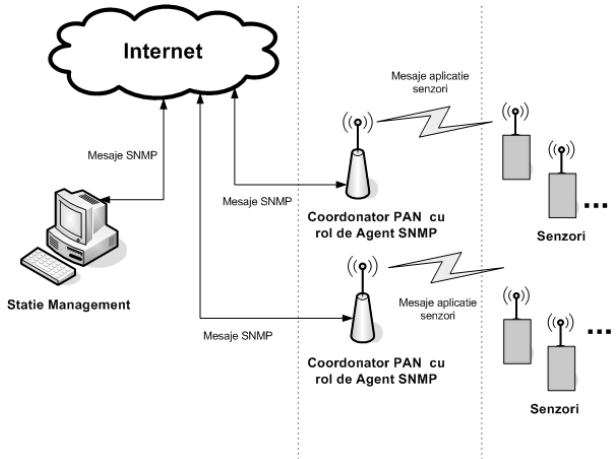

Figura 4.3 Arhitectura sistemul de test pentru agent

Din punct de vedere al IEEE 802.15.4 avem două categorii de echipamente: FFD şi RFD. Soluția care a fost adoptată a fost aceea de a implementa un agent SNMP în cadrul unui echipament FFD, care este de asemenea şi un coordonator de PAN. Agentul care a fost dezvoltat implementeaza un MIB, denumit ieee802dot15dot4, descris în paragraful următor. Pentru realizarea agentului ca şi platformă hardware de bază a fost aleasă cea folosită pentru implementarea agentului SNMP de tip hardware pentru MIB-II.

Soluția aleasă a fost aceea de a avea un microcontroler cu interfață Fast Ethernet la care printr-o interfață serială sincronă se conecteaza un modul care implementeaza funcțiile standardului IEEE 802.15.4. Ca şi microcontroler a fost ales M9S12NE64 fabricat de Freescale (fosta Motorola), iar pentru modulul radio a fost ales CC2420 de la Texas Instrument (fost Chipcon). Blocurile componente şi legatura dintre ele pentru arhitectura hardware a agentului este descrisă în Figura 4.4. Topologia folosită este topologia de tip stea.

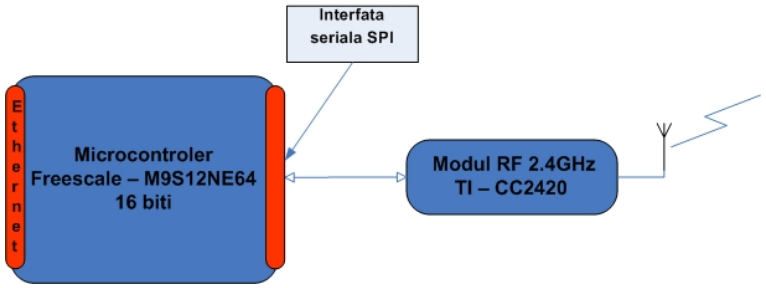

Figura 4.4 Blocuri componente ale agentului SNMP (hardware)

După ce agentul a fost realizat fizic, au trebuit implementate stivele de protocoale (pentru SNMP şi IEEE 802.15.4). Pentru SNMP protocoalele necesare sunt: IEEE 802.3 PHY, IEEE 802.3 MAC, IP, ICMP, ARP, UDP şi SNMP. Dintre protocoalele enumerate IEEE 802.3 PHY şi IEEE 802.3 MAC sunt realizate de către modulul Fast Ehernet din microcontroler, celelalte fiind obținute prin programul dezvoltat pentru microcontroler. Pentru IEEE 802.15.4 protocoalele necesare sunt: IEEE 802.15.4 PHY, IEEE 802.15.4. MAC. Din acestea IEEE 802.15.4 PHY şi o parte din funcțiile pentru IEEE 802.15.4 MAC sunt implementate de circuitul CC2420, restul funcțiilor fiind realizate în program. Cele două stive de protocoale comunică între ele prin intermediul zonei de memorie în care este stocat MIB.

Astfel din punct de vedere al implementării software, există două zone distincte. Una se numeşte HAL (Hardware Abstraction Layer) şi cea de a doua OSAL (Operating System Abstraction Layer). În cadrul HAL a fost introdus codul care depinde direct de circuitele hardware folosite, iar în cadrul OSAL a fost introdus codul care nu depinde de circuitele hardware folosite. Prin acest mod de implementare, trecerea la alte circuite va însemna ca modificări necesare de cod sursă, doar schimbarea codului localizat în HAL.

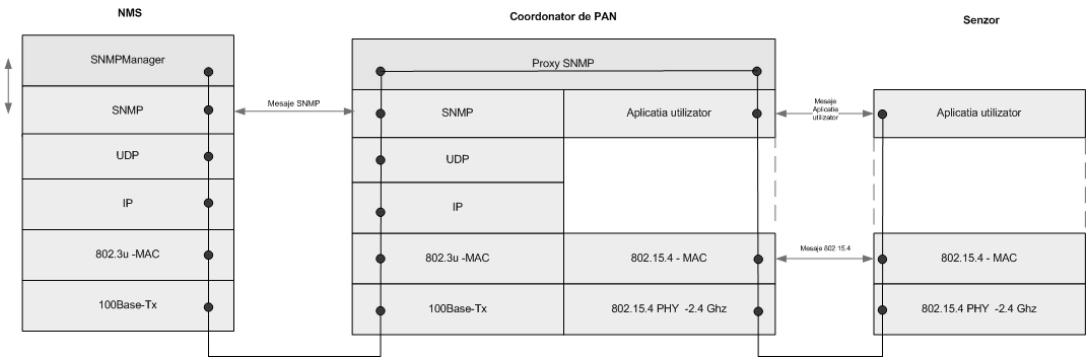

Figura 4.5 Legăturile între diversele protocoale implementate în sistem

În Figura 4.5 este prezentată modalitatea de comunicare între diversele protocoale implementate în agentul SNMP şi celelalte entităţi prezente în sistem.

Astfel pentru aplicaţia de management folosită (SNMP Manager) acesta se foloseşte de o legătură Fast Ethernet, stiva TCP/IP şi în stratul aplicaţie de suportul SNMP. Se transferă mesaje SNMP cu partea din agent care implementează stiva TCP/IP şi SNMP. În urma unui mesaj SNMP recepţionat, valoarea cerută se va citi din zona de memorie unde este salvat MIB implementat de agent. Ea este scrisă de către coordonatorul de PAN, care în acelaşi timp va controla reţeaua WPAN, prin schimb de mesaje specifice IEEE 802.15.4 (şi mesaje ale aplicaţiei implementate în coordonator şi senzor). În funcţie de cadrele recepţionate va face „update" la zona de memorie în care este stocat MIB-ul.

4.3 Realizare MIB pentru IEEE 802.15.4

Pentru dezvoltarea acestui MIB, am început prin a captura traficul real dintr-o reţea IEEE 802.15.4 cu scopul de a determina care sunt informaţiile relevante care se găsesc cel mai des. Capturarea cadrelor a fost făcută cu ajutorul unui pachet software specializat, denumit Zena (dezvoltat de către firma Microchip), şi a unei plăci de captură hardware, dezvoltată tot de Microchip. În urma utilizării acestui software au rezultat o serie de fişiere de captură care au fost analizate, rezultatele obţinute fiind apoi folosite pentru conceperea şi dezvoltarea MIB-ului pentru reţelele IEEE 802.15.4. Mai multe informaţii despre acest utilitar şi placă de captură pot fi găsite în [Mic09]. Pentru alegerea obiectelor care vor apărea în MIB s-a ţinut cont şi de recomandările care apar în [Bie02].

MIB-ul implementat de către acest agent SNMP conţine cinci secţiuni diferite: dot15dot4system, dot15dot4phy, dot15dot4mac, dot15dot4AsociatedDevices şi dot15dot4Notifications. Am decis ca acest MIB să fie salvat în ramura *experimental* din arborele cu obiecte, folosind 26840 ca punct de pornire, acesta fiind selectat aleatoriu din cele nealocate de către IANA. Ramura *experimental* este rezervată pentru testare şi experimentare.

Secţiune	**Descriere**
dot15dot4system	Conţine patru obiecte care oferă informaţii de identificare şi localizare a sistemului
dot15dot4phy	Conţine un tabel cu un număr de linii egal cu numărul interfeţelor radio prezente în agent (de cele mai multe ori va doar o singură interfaţă), fiecare linie având trei coloane. datele din această secţiune oferă informaţii despre stratul fizic
dot15dot4mac	Conţine un tabel cu un număr de linii egal cu numărul interfeţelor radio prezente în agent (de cele mai multe ori va doar o singură interfaţă), fiecare linie având 16 coloane. Datele din această secţiune oferă informaţii despre stratul MAC
dot15dot4AsociatedDevices	Conţine un tabel cu un număr de linii egal cu numărul de echipamente asociate acestui coordonator de PAN, numărul de coloane fiind 7, datele menţinute oferind informaţii despre echipamentele asociate
dot15dot4Notifications	Conţine doua obiecte, care specifică valori la depăşirea cărora se vor genera notificări către manager

Tabelul 4.1 Descrierea secţiunilor definite în MIB

Obiectele definite de către MIB au fost transpuse sub forma unor variabile care sunt manipulate de către microcontroler. În Figura 4.6 se poate observa poziționarea MIB-ului în arborele cu obiecte.

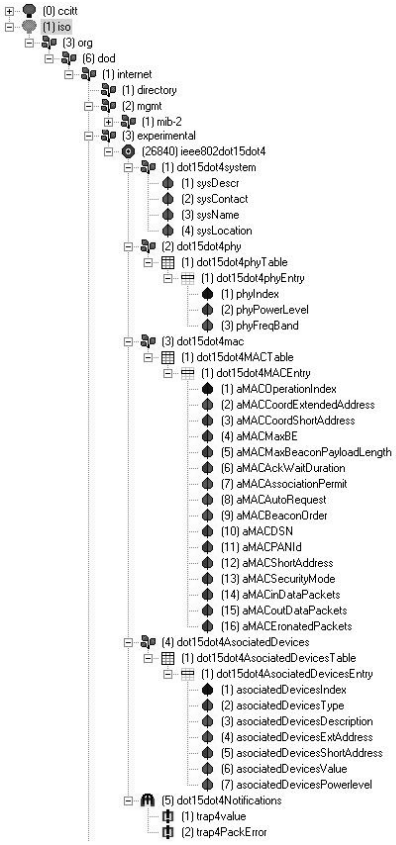

Figura 4.6 Poziționarea MIB-ului în arborele cu obiecte

4.4 Implementare agent SNMP hardware pentru IEEE 802.15.4

Pentru demonstrarea funcționalității agentului creat şi pentru validarea MIB-ului dezvoltat, am creat o arhitectură de test. Arhitectura folosită poate fi văzută în Figura 4.7. Pentru testarea completă este nevoie de un calculator pe care va rula aplicația de management, un număr de echipamente cu rol de coordonator de PAN (proxy SNMP) şi un număr de senzori care se vor asocia coordonatorilor.

În experimentele efectuate am folosit un număr de doi coordonatori de PAN (primul având alocată adresa IP 192.168.2.101 şi identificatorul de PAN 1, iar cel de al doilea adresa IP 192.168.2.102 şi identificatorul de PAN 2), şase senzori de temperatură, câte 3 asociați fiecărui coordonator de PAN şi o stație de management (care rulează aplicația SNMP Manager) care are alocată adresa IP 192.168.2.100. Stația de management şi cei doi coordonatori de PAN sunt conectați într-un comutator pentru a forma o rețea locală. Senzorii de temperatură au fost amplasați în două camere diferite (S1-1, S1-2, S1-3 în camera 1 formând o rețea WPAN şi S2-1, S2-2, S2-3 în camera 2, formând o altă rețea WPAN).

În primul tip de experimente am monitorizat cu ajutorul aplicației de management temperaturile raportate de fiecare senzor. SNMP Manager interoghează periodic fiecare coordonator de PAN şi obține valorile de temperatură a fiecărui senzor. Cel de al doilea experiment a fost identic cu primul, din punct de vedere al configurației, doar că s-a dorit generarea de notificări legate de depăşirea unui prag a numărului de cadre eronate. Pentru acesta în camerele cu senzori s-au amplasat (sau reactivat) echipamente care folosesc acceaşi

bandă de frecventă ISM (plăci de rețea IEEE 802.11, cuptoare cu microunde şi dispozitive Bluetooth).

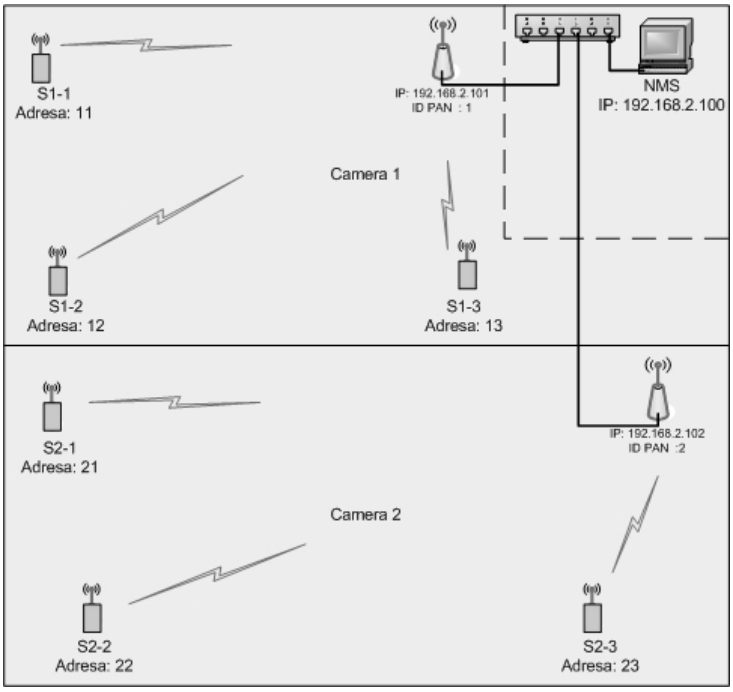

Figura 4.7 Arhitectura de test pentru agentul SNMP

Concluzii

Scopul elaborării acestui sistem a fost acela de a oferi o soluție administratorilor de rețea posibilitatea de monitorizare a parametrilor de mediu (temperatură, umiditate) folosind acelaşi mecanism de management ca şi pentru rețelele de calculatoare. Prin amplasarea acestor echipamente în zone sensibile (camera echipamentelor) ei vor putea obține informații în timp real. Experimentele efectuate au demonstrat că este fezabilă crearea de astfel de echipamente şi că integrarea lor în sistemele de management nu este un proces complicat.
Ca dezvoltări ulterioare, am în vedere extinderea MIB-ului în aşa fel încât să fie introduse şi informații despre straturile superioare (rețea până la aplicație), întrucât în acest moment informațiile acoperă doar straturile Fizic şi Legături de date.
O altă abordare se referă la implementarea SNMP direct în senzori. Acest lucru deocamdată nu este fezabil conform [Nan07a]. Acest lucru presupune implementarea IP şi UDP, dar acestea necesită resurse care de obicei nu sunt diponibile în senzori. Alte probleme care trebuie depăşite sunt prezentate în [Nan07b]. În final soluția pare să fie implementarea protocolului IPv6 peste IEEE 802.15.4, dar aceasta necesită multe adaptări. La momentul redactării tezei, există deja specificații şi echipamente care permit integrarea protocolului SNMP direct în senzori, dar specificațiile nu sunt încă în forma finală [Bor09].

Un ultim aspect care va îmbunătăți performanțele este acela de a implementa (sau folosi) un sistem de operare în timp real, lucru care ar oferi o întârziere minimă la tratarea întreruperilor şi la schimbarea proceselor active în microcontroler.

Capitolul 5. Agent software pentru managementul rețelelor locale fără fir IEEE 802.11

5.1 Standard IEEE 802.11 pentru WLAN

Pentru rețelele locale de calculatoare, unul dintre standardele care este implementat din ce în ce mai mult este cel elaborat de IEEE sub denumirea de IEEE 802.11.

Standardul IEEE 802.11 a fost lansat pe piață în anul 1997. Versiunea inițială de standard preciza opțiuni pentru stratul fizic care să permită conectarea fără fir a echipamentelor fixe, portabile şi a terminalelor mobile într-o rețea locală. Pe langă opțiunile de strat fizic au fost descrise şi modalitatea de implementare a substratului MAC [802.11].

Transmisia se poate face în spectrul infraroşu sau în unde radio (folosind banda de frecvențe ISM de 2.4 GHz) [Zin06]. În aceste benzi de frecvență sunt folosite tehnici cu spectru distribuit (*spread spectrum*). Variantele de transmisie cu spectru distribuit definite sunt:

- FHSS (*Frequency Hopping Spread Spectrum*)
- DSSS (*Direct Sequence Spread Spectrum*)

Toate variantele de standarde definesc două moduri de lucru posibile în rețelele WLAN şi anume:

1. modul bazat pe infrastructura existentă (*Infrastructure mode*)
2. modul ad-hoc (*Ad-hoc mode*)

Specificațiile pentru substratul MAC definesc tehnica de control al accesului la mediul de comunicație, tipuri de cadre folosite, structura acestor cadre.

Tehnica de control a accesului la mediul de comunicație pentru IEEE 802.11 este codificată CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*). Împreună cu această tehnică s-a definit şi un mecanism de confirmare a cadrelor transmise de tipul PAR (Positive Acknowledgement with Retransmission). Există trei tipuri de cadre definite de IEEE 802.11. Acestea sunt: cadre de date, cadre de control şi cadre de management. Structura cadrului MAC definită de IEEE 802.11 este prezentată în Figura 5.1.

2 octeți	2 octeți	6 octeți	6 octeți	6 octeți	2 octeți	6 octeți	0-2312 octeți	4 octeți
Control cadru	Durata/ Identificator	Adresă 1	Adresă 2	Adresă 3	Control secvență	Adresă 4	Date utile	CRC

Figura 5.1 Structura cadrului MAC IEEE 802.11

5.2 Implementari software existente pentru agenți SNMP în Windows şi Linux

Agent software pentru sistemul de operare Windows

În sistemul de operare Windows versiunile de agent SNMP depind de tipul de sistem de operare instalat. În Windows 2000, suportul pentru SNMP vine sub forma a două fişiere executabile: SNMP.exe care joacă rolul clientului SNMP, şi SNMPTRAP.exe care este folosit pentru a genera notificări în cazul unor evenimente. Pe lângă aceste două utilitare, Microsoft oferă şi o bibliotecă DLL cu scopul de a extinde facilitățile agentului principal.
Începând cu Microsoft Windows Server 2003 şi apoi la Windows XP, clientul SNMP este oferit sub forma unui serviciu, care dă posibilitate de management a calculatorului respectiv. El are următoarele facilități :

- răspunde la cererile legate de starea sistemului, acceptând cereri de la mai mulți manageri.
- raportează evenimentele semnificative spre managerii configurați
- identifică echipamentele care fac cereri şi la care se vor trimite informații pe baza adresei IPv4

Pentru crearea unor agenți SNMP personalizați sunt disponibile următoarele biblioteci (API) :

- SNMP Management API, care este un set de funcții care pot fi folosite pentru dezvoltarea sistemului de management
- WinSNMP API, care este un set de funcții pentru codare, decodare, trimitere şi recepționare a mesajelor SNMP
- SNMP Extension Agent API, care este un set de interfețe dintre serviciul SNMP şi agentul dezvoltat

Toate aceste biblioteci au fost dezvoltate în special pentru programare în limbajele C sau C++, dar pot fi folosite şi cu alte limbaje de programare (de exemplu Delphi, Java).

Agent software pentru sistemul de operare Linux

În sistemul de operare Linux agentul SNMP prezent implicit este cel din pachetul Net-SNMP. Acest pachet include pe lângă agent şi aplicații cu rol de manager. Mai există şi alți agenți, dar prezența lor depinde de distribuția de Linux folosită.

Aplicații SNMP de bază disponibile

snmpget – este o aplicație care comunică cu agenții SNMP folosind cereri de tip SNMP GET.
snmpgetnext – este o aplicație care comunică cu agenții SNMP folosind cereri de tip SNMP GETNEXT.
snmpbulkget – este o aplicație care comunică cu agenții SNMP folosind cereri de tip SNMP GETBULK.
snmpwalk – este o aplicație care comunică cu agenții SNMP folosind cereri de tip SNMP GETNEXT.
snmpset – este o aplicație care comunică cu agenții SNMP folosind cereri de tip SNMP SET.
snmpd – este aplicația care joacă rolul agentului SNMP. Rulează ca daemon şi recepționează şi răspunde la cererile SNMP venite de la manageri.

5.3 Arhitectura bazată pe interfața AirPcap şi analizorul software Wireshark

Analizorul de protocoale Wireshark

În anul 1998 Gerald Combs a lansat prima versiune a unui utilitar pentru analiza şi decodarea cadrelor care circulă în rețelele de calculatoare, numit Ethereal. În anul 2006 acest proiect a fost redenumit Wireshark, datorită unor probleme legate de drepturi de autor. În momentul de față, el este cel mai cunoscut analizor de protocoale şi este un standard „de facto”(deseori chiar „de jure”) în multe sectoare de activitate şi medii educaționale [Wir09a] .

Wireshark se foloseşte de biblioteca LibPcap (pentru Windows se numeşte WinPcap) pentru captura efectivă a cadrului din rețea. Pentru partea de decodare a cadrelor se folosesc module (denumite de autori - *dissectors*) care interpretează cadrul captat, în concordanță cu informațiile din câmpuri. Aceste module pot fi incluse direct în Wireshark sau pot fi încărcate dinamic (acest lucru oferă posibilitatea de interpretare a unui protocol nou apărut fără schimbarea aplicației). Interfața cu utilizatorul poate fi în mod grafic sau în mod text, ultima dând posibilitatea de a utiliza Wireshark împreună cu alte aplicații pentru obținerea de

informații. Acest mecanism a fost utilizat pentru obținerea de informații de către agentul SNMP descris în acest paragraf.

Structura fişierelor PCAP

Wireshark poate fi configurat să salveze cadrele capturate în fişiere, în format binar de către modulul WireTap sau în formate text predefinite. Formatul fişierelor binare este definit de către modulul Libpcap. Există mai multe versiuni ale formatului binar, cea folosită şi descrisă fiind 2.4. Ultima modificare a formatului a avut loc în 1998, şi nu se aşteaptă să se schimbe prea curând [Wir09b]. Fişierele conţin un antet global care conţine informaţii generale şi apoi un număr de înregistrări pentru fiecare cadru capturat.

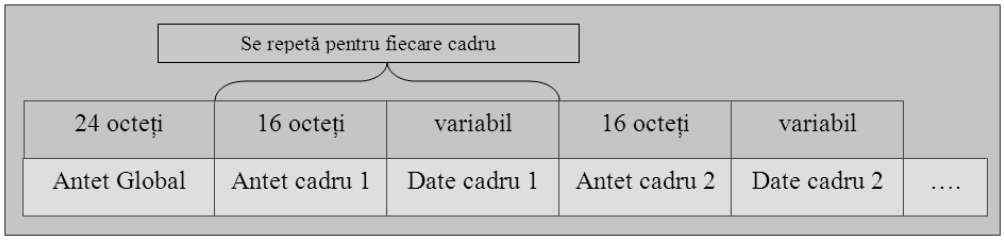

Figura 5.2 Structura fişierelor PCAP

Acesta nu va conține întotdeauna toți octeții așa cum au fost preluați, uneori doar primii „n" octeți din cadru. De fapt acest număr depinde un parametru numit „snapshot length" care este definit de utilizator. Valoare implicită este de 65535, care este mai mare decât lungimea uzuală a cadrelor. După acest antet urmează cadrul capturat.

Interfața AirPcap

Capturarea cadrelor IEEE 802.11 în sistemul Windows, folosind Wireshark (sau alte aplicații similare) este aproape imposibilă. Acest lucru se datorează implementării bibliotecii WinPcap şi a driverelor folosite pentru plăcile de rețea. De cele mai multe ori se vor captura cadrele de date, fără a avea acces la cadrele de control sau management, iar antetul acestora va fi convertit de driverul plăcii de rețea în antet de cadru Ethernet. Interfața AirPcap a fost special proiectată să captureze toate cadrele IEEE 802.11 şi să le ofere utilitarului Wireshark în sistemul Windows.

Antetul RadioTap

Acest antet RadioTap [Ber09] a fost introdus cu scopul de a oferi informații suplimentare despre cadrul recepționat, inițial fiind implementat doar în sistemul de operare NetBSD. El are o parte fixă de 8 octeți, urmată de un număr de octeți cu lungime variabilă.

5.4 Realizare MIB pentru IEEE 802.11

Structura MIB propusă conține informații despre staturile Fizic şi Legături de date pentru rețelele WLAN. Descrierea MIB s-a făcut ținând cont de regulile specificate de SMIv2. A fost definită o singură secțiune denumită wLANStatistics, cu 20 obiecte diferite. Am luat decizia de a introduce acest MIB sub ramura *experimental*, alegând aleatoriu valoarea de 7330, dintre valorile nealocate de IANA. Informațiile de trafic real care sunt descrise în acest MIB pot fi utilizate de către administratorii rețelelor pentru o mai bună alocare a resurselor şi pot fi coroborate cu cele obținute în mod teoretic prin aplicarea unor algoritmi de predicție a traficului în rețelele WLAN [Fen06]. Descrierea în detaliu a fiecărui obiect este prezentată în continuare.

- 1.3.6.1.3.7330.1 – este numărul total de cadre capturate şi se obţine prin numărarea tuturor cadrelor din fişierul de captură
- 1.3.6.1.3.7330.2 – este numărul total de cadre eronate şi se obţine prin numărarea tuturor cadrelor eronate din fişierul de captură
- 1.3.6.1.3.7330.3 – este numărul total de cadre de tip beacon şi se obţine prin numărarea tuturor cadrelor de tip beacon din fişierul de captură
- 1.3.6.1.3.7330.4 – este numărul total de cadre de tip acknowledge şi se obţine prin numărarea tuturor cadrelor de tip acknowledge din fişierul de captură
- 1.3.6.1.3.7330.5 – este numărul total de cadre de tip Probe Request şi se obţine prin numărarea tuturor cadrelor de tip Probe Request din fişierul de captură
- 1.3.6.1.3.7330.6 – este numărul total de cadre de date şi se obţine prin numărarea tuturor cadrelor de date utile din fişierul de captură
- 1.3.6.1.3.7330.7 – reprezintă numărul de cadre de alt tip neincluse în celelalte categorii
- 1.3.6.1.3.7330.8 – este momentul de timp al captării primului cadru şi se obţine prin citirea din fişierul de captură a momentului de timp salvat pentru primul cadru
- 1.3.6.1.3.7330.9 – este lungimea în secunde a intervalului monitorizat
- 1.3.6.1.3.7330.10 – este numărul de cadre beacon raportate la secundă şi se obţine prin împărţirea numărului de cadre de tip beacon la numărul de secunde din intervalul de monitorizare
- 1.3.6.1.3.7330.11 – este numărul de cadre acknoledge raportate la secundă şi se obţine prin împărţirea numărului de cadre de tip acknoledge la numărul de secunde din intervalul de monitorizare
- 1.3.6.1.3.7330.12 – este numărul de cadre Probe Request raportate la secundă şi se obţine prin împărţirea numărului de cadre de tip Probe Request la numărul de secunde din intervalul de monitorizare
- 1.3.6.1.3.7330.13 – este numărul de cadre de date raportate la secundă şi se obţine prin împărţirea numărului de cadre de date utile la numărul de secunde din intervalul de monitorizare
- 1.3.6.1.3.7330.14 – reprezintă numărul de adrese destinaţie diferite întâlnite în fişierul de captură
- 1.3.6.1.3.7330.15 – reprezintă numărul de adrese sursă diferite întâlnite în fişierul de captură
- 1.3.6.1.3.7330.16 – reprezintă numărul de AP diferite
- 1.3.6.1.3.7330.17 – valoarea medie a valorii SSI pentru semnalul util
- 1.3.6.1.3.7330.18 – valoarea medie a valorii SSI a zgomotului
- 1.3.6.1.3.7330.19 – valoarea medie a calităţii semnalului
- 1.3.6.1.3.7330.20 – numărul de cadre de pe fiecare canal

5.5 Implementare agent SNMP software pentru IEEE 802.11

Agentul software dezvoltat pentru reţelele WLAN este constituit din 2 aplicaţii sofware fiecare având un rol bine definit şi anume: *NetAnalyzer* pentru colectarea datelor şi *WLAN_Agent* pentru comunicarea cu managerul SNMP [Van09b]. Alte abordări privind folosirea SNMP pentru reţele WLAN pot fi găsite în [Ker03]. Programele au fost dezvoltate pentru a fi utilizate în sistemul de operare Windows, iar pentru funcţionarea corectă ele trebuie să fie instalate în acelaşi director. Este vorba de *NetAnalyzer.exe*, care se ocupă de extragerea informaţiilor din fişierele generate de Wireshark, *WLAN_Agent.exe*, care este responsabil de partea de comunicare cu managerii, şi fişierul *MIB_Data.xml*, care are rolul de

fişier de legătură între cele două aplicații. Pe lângă aceste trei fişiere este nevoie ca pe acel calculator să fie instalată şi aplicația Wireshark.

Aplicația *NetAnalyzer* a fost creată cu scopul prelucrării fişierelor de captură generate de către aplicația *Wireshark*. Această aplicație va porni automat *Wireshark* la lansarea capturii, *Wireshark* fiind configurat cu parametrii introduşi în *NetAnalyzer*. Printre opțiunile de configurare se află intervalul de timp la care Wireshark salvează cadrele capturate în fişierul de captură şi numele fişierului de captură. La momentul specificat NetAnalyzer va citi fişierul de captură şi va scrie valorile obținute în fişierul *MIB_Data.xml*. Prelucrarea unui fişier conținând aproximativ 55000 cadre a durat aproximativ 500 milisecunde.

Arhitectura de test

Pentru demonstrarea funcționalității agentului creat, şi pentru validarea MIB-ului dezvoltat, am creat o arhitectură de test, conform cu Figura 5.3. Pentru testarea completă este nevoie de un calculator pe care va rula aplicația de management şi un al doilea calculator pe care s-au instalat toate aplicațiile necesare pentru funcționarea agentului WLAN. Pentru validare s-au efectuat mai multe experimente, toate având aceeaşi configurație, diferența între ele constând în traficul WLAN. Astfel s-au efectuat experimente în care numărul de AP disponibile era mai mare de 10, experimente în care numărul de AP disponibile era între 5 şi 10 şi experimente în care numarul de AP era mai mic de 5.

Un alt parametru care s-a shimbat pe parcursul diferitelor teste a fost intervalul de salvare de către aplicația *Wireshark* şi de prelucrare a fişierelor de către *NetAnalyzer*. Acesta a fost variat între 5 minute şi 30 minute. Aplicația *NetAnalyzer* poate fi configurată să prelucreze fişiere până la 24 ore, dar la intervale mai mari este mai dificil de rulat testele (durata unui test poate ajunge la câteva zile). Pentru partea de aplicație de management s-a utilizat SNMPManager.

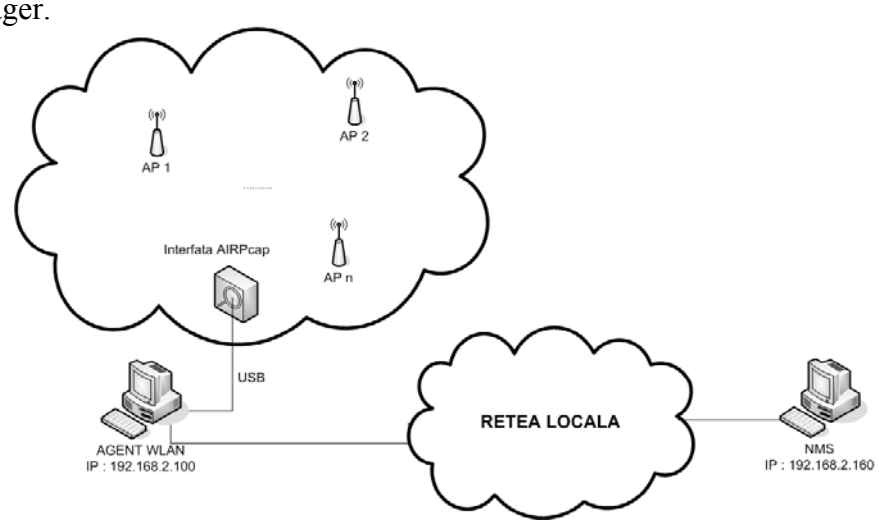

Figura 5.3 Arhitectura de test folosită pentru agentul software WLAN

Un prim set de experimente a fost efectuat într-o zonă în care numărul de AP era relativ mic (sub 5 AP disponibile). Au fost monitorizați toți parametrii definiți în MIB. Intervalul de monitorizare a fost de câteva ore. Folosind modul de reprezentări grafice disponibile în *SNMP Manager*, s-au reprezentat grafic datele obținute în urma experimentelor.

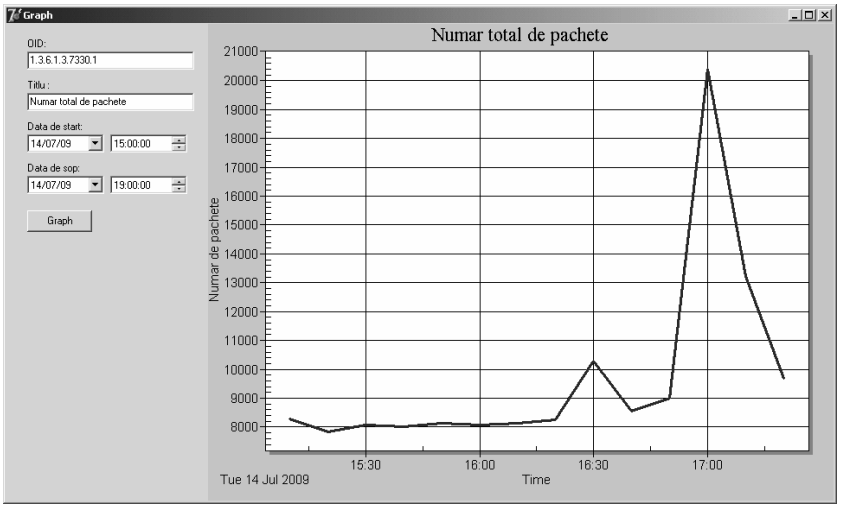

Figura 5.4 Variația numărului total de pachete în setul 1 de experimente

Un al doilea set de experimente a fost efectuat într-o zonă în care numărul de AP era mediu (între 5 şi 10 AP disponibile). Au fost monitorizați toți parametrii definiți în MIB, iar intervalul de monitorizare a fost de câteva ore. Cel de al treilea set de experimente a fost efectuat într-o zonă în care numarul de AP era relativ mare (peste 10 AP disponibile), fiind monitorizați toți parametrii definiți în MIB, pe un interval de monitorizare de câteva ore. Rezultatele obținute în setul 2 şi setul 3 de experimente sunt similare cu cele obținute în setul 1, variația numărului de cadre fiind similară.

Capitolul 6. Agent software pentru managementul aplicațiilor VoIP în rețelele locale cu şi fără fir

În PBX Asterisk există suport pentru SNMP dar acesta este relativ simplu. Scopul acestui capitol este de a oferi o modalitate de extindere a informațiilor oferite de agentul SNMP existent. Informațiile suplimentare care vor fi oferite se referă la numărul apelurilor inițiate şi primite în Asterisk, durata acestor apeluri (informații de la nivelul stratului aplicație conform modelului de referință OSI). S-au studiat inițial şi alte aspecte ale managementului resurselor în VoIP, după cum rezultă din [Dob02a],[Zin02a] şi [Zin02c]. Ideea a fost să se monitorizeze în timp real parametrii specifici comunicațiilor VoIP, sintetizați prin R-Factor. Rezervarea resurselor a fost abordată în [Zin02b], dar s-a considerat că este mai relevant să se studieze în continuare o platformă care să integreze toate aceste realizări punctuale.

6.1 Arhitectura Asterisk

Asterisk este o centrală telefonică de instituție implementată software, instalându-se pe orice distribuție de Linux/Unix (inclusiv pe CentOS). Mark Spencer, principalul autor, a ținut să facă public codul acesteia, astfel că o comunitate largă de programatori au fost atraşi de acest concept. Neoficial Asterisk poate fi considerat probabil cel mai puternic, flexibil şi extensibil software de telecomunicații OpenSource disponibil pe piață. Ideea de la care s-a pornit este că multe dintre facilitățile incluse într-un PBX sunt rar sau chiar deloc folosite, fiind însă plătite de cumpărător. De aceea, Asterisk nu implementează toate funcțiile unei centrale, dar fiind distribuit sub licență GPL *(General Public License)* se pot adăuga oricând module software cerute de clienți. Pentru instalarea suportului SNMP în Asterisk, este nevoie să fie instalat pachetul Net-SNMP. Pentru activarea suportului pentru SNMP, Asterisk trebuie recompilat [Cha09].

AgentX

AgentX reprezintă un cadru generic de lucru care permite extinderea agenților SNMP existenți pe calculatoare. Acest cadru de lucru defineşte noțiunea de agent master, subagent şi prezintă un protocol folosit pentru comunicarea între agentul master şi subagenți [Dan00]. Necesitatea introducerii acestui protocol se datorează apariției a noi agenți, cei vechi trebuind extinşi iar acest lucru devinind din ce în ce mai greu de administrat. Modalitatea de interconectare a acestor module este descrisă în Figura 6.1.

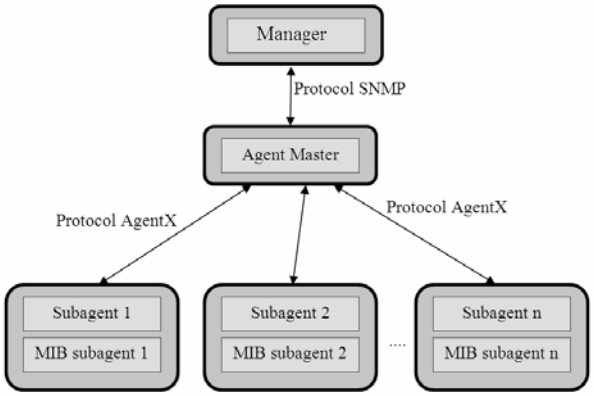

Figura 6.1 Modulele şi legăturile dintre ele definite de AgentX

Din punct de vedere al AgentX, un agent SNMP va fi compus din :

- Agent master, care va recepționa şi trimite mesajele SNMP ca şi până acum, dar care nu mai are (sau are acces limitat) la informațiile de management
- Unul sau mai multe entități, denumite subagenți care nu implementează mecanismul de comunicare SNMP, dar care au acces la informațiile de management
- Comunicația între agentul master şi subagenți se va face prin intermediul protocolului AgentX. Comunicarea între agent master şi subagent se face prin intermediul unor cadre care includ un antet fix de 20 octeți şi o parte variabilă care conține de obicei informația de management. Stabilirea conexiunii între agentul master şi subagent se face la inițiativa subagentului, el fiind responsabil de inițierea sesiunii de lucru.

6.2 Extindere MIB pentru Asterisk

Pentru colectarea informațiilor despre apelurile efectuate folosind Asterisk, a fost extins MIB-ul original. Varianta inițială de MIB are cinci secțiuni diferite, informațiile din fiecare secțiune fiind descrise în Tabelul 6.1. După cum se observă nu există nici o informație statistică legată de apeluri (singurele informații legate de apeluri referindu-se la parametrii legăturilor care pot sau sunt folosite) [Van09a].

Secțiune	**Descriere**
asteriskVersion	Informații despre versiunea de Asterisk
asteriskConfiguration	Informații despre procesele care rulează în Asterisk
asteriskModules	Numărul de module încărcate de Asterisk
asteriskIndications	Indicatori de zonă folosiți de Asterisk
asteriskChannels	Detalii despre canalele active în Asterisk

Tabelul 6.1 Secțiunile inițiale definite în MIB-ul pentru Asterisk

În urma analizei MIB-ului original şi a necesității de a avea informații despre apeluri am luat decizia de a adauga o nouă secțiune în MIB şi în aceea secțiune să avem 7 obiecte Informațiile oferite de MIB se referă la numărul de apeluri şi la durata totală a acestora. Ramura unde este definit MIB-ul original se află sub ramura *enterprises*, având numărul

ramurii 22736. Această ramură a fost alocată către Digium, cei care sunt dezvoltatorii pentru Asterisk. În MIB extins propus au fost introduse 7 obiecte, grupate într-un singur grup denumit *asteriskCallStatistics* identificat cu OID-ul 1.3.6.1.4.1.22736.6.

Parametru/OID	Descriere	Tip
asteriskAnsweredCalls 1.3.6.1.4.1.22736.6.1	Numărul de apeluri la care s-a răspuns. Pentru determinarea acestor tipuri de apeluri s-a căutat valoarea *ANSWERED* de pe fiecare linie înregistrată în Master.csv în poziția corespunzătoare parametrului CDR (disposition) care reprezintă statusul apelului	Counter32
asteriskNotAnsweredCalls 1.3.6.1.4.1.22736.6.2	Numărul de apeluri la care nu s-a răspuns. Pentru determinarea acestor tipuri de apeluri s-a căutat valoarea *NO ANSWER* de pe fiecare linie înregistrată în Master.csv în poziția corespunzătoare parametrului CDR (disposition) care reprezintă statusul apelului.	Counter32
asteriskBusyCalls 1.3.6.1.4.1.22736.6.3	Numarul de apeluri care nu s-au efectuat din cauza apelatul ocupat. Pentru determinarea acestor tipuri de apeluri s-a căutat valoarea *BUSY* de pe fiecare linie înregistrată în *Master.csv* în poziția corespunzătoare parametrului CDR (disposition) care reprezintă statusul apelului.	Counter32
asteriskTotalCalls 1.3.6.1.4.1.22736.6.4	Numărul total de apeluri. Valoarea din acest OID reprezintă suma numerelor din câmpurile precedente.	Counter32
asteriskTotalCallers 1.3.6.1.4.1.22736.6.5	Numărul de apelanți diferiți	Counter32
asteriskBillingInterval 1.3.6.1.4.1.22736.6.6	Numărul total de secunde taxabile. Această valoare s-a obținut prin însumarea valorilor aflate în câmpul CDR(billsec) aflat pe fiecare linie înregistrată în fișierul *Master.csv*.	Counter32
asteriskMonitoringInterval 1.3.6.1.4.1.22736.6.7	Intervalul de monitorizare. Este prezentat sub formă unei perechi de două numere primul fiind momentul de start al monitorizării iar cel de al doilea este numărul de secunde trecute de la momentul de start.	OCTET STRING

Tabelul 6.2 Obiectele adăugate în MIB-ul extins

Toate valorile corespunzătoare obiectelor din MIB sunt valabile pe o perioadă de monitorizare (care depinde de valoarea intervalului stabilit la aplicația *parserd*). Din acest motiv se recomandă ca aceste valori sa fie citite de către manager la un interval egal cu perioada de monitorizare. Dacă nu se respectă acest lucru, există posibilitatea de a pierde informații. Pentru eliminarea acestei posibile surse de erori, la următoarea extindere a MIB-ului se vor introduce noi obiecte care să păstreze valorile cumulate a valorilor instantanee, de la inițializarea sistemului. O altă posibilă extindere se referă la accesul la Asterisk (în sensul că apelul folosește ca modalitate de transport rețeaua Internet sau rețeaua PSTN). Prin acest mecanism se va putea vedea care este raportul dintre numărul de apeluri de tip VoIP şi apeluri de tip PSTN, putându-se lua o decizie de reconfigurare a accesului la Asterisk.

6.3 Extindere agent SNMP software pentru Asterisk

Toate experimentele legate de obținerea de informații despre apeluri de la Asterisk au fost executate folosind PC-uri rulând Linux Fedora Core 8 şi Asterisk 1.4.7. Informațiile despre apeluri au fost obținute din fişierele de log generate de către Asterisk. Aceste fişiere sunt actualizate după fiecare apel. Fişierele de log vor conține informații despre fiecare apel în

parte, tipul informației fiind specificat într-un fișier de configurare Asterisk. Acest fișier se numește `cdr_custom.conf` și este situat în directorul `/etc/asterisk`. Implicit fișierul de log are formatul CSV (Comma Separated Value) și este salvat în directorul `/var/log/asterisk/cdr-csv`. Fișierul implicit în care se stochează informațiile se numește Master.csv. Aceste informații se mai pot salva și în baze de date. În acest moment sistemele de baze de date suportate de către Asterisk sunt SQLite, PostgreSQL, MySQL, și unixODBC. Informațiile necesare sunt obținute prin prelucrarea periodică a fișierului *Master.csv*. Pentru prelucrarea acestui fișier a fost dezvoltată o aplicație numită *parserd*. Această aplicație va citi informațiile din fișier la intervale regulate, intervalul fiind configurabil. Valoarea implicită a intervalului de citire este de 30 minute și poate fi configurat între 5 secunde și 24 ore. Această aplicație va citi fișierul *Master.csv*, va obține informațiile și apoi le salvează într-un fișier care este oferit ca și parametru de intrare la aplicație.

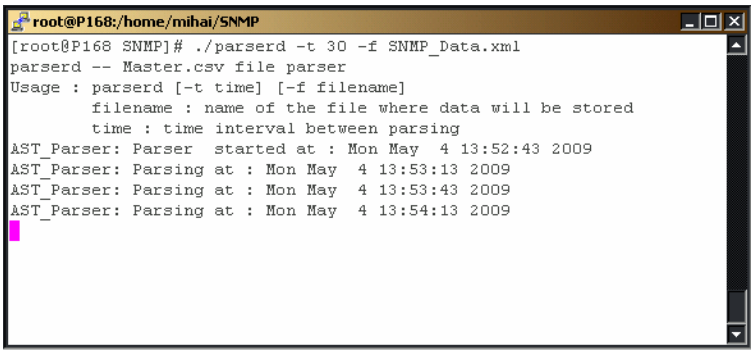

Figura 6.2 Utilizarea aplicației *parserd*

Informațiile obținute de aplicația *parserd* sunt stocate în fișierul de tip .xml, fișier care va fi citit de către agentul SNMP în momentul în care sunt cerute informațiile stocate în acesta.

Pentru experimente s-a folosit o rețea locală de calculatoare, pe fiecare calculator fiind instalată o aplicație capabilă să genereze și să recepționeze apeluri de tip VoIP sub Windows XP. În aceeași rețea pe un alt calculator a rulat *Asterisk*, iar pe un altul managerul (aplicația *SNMP Manager*).

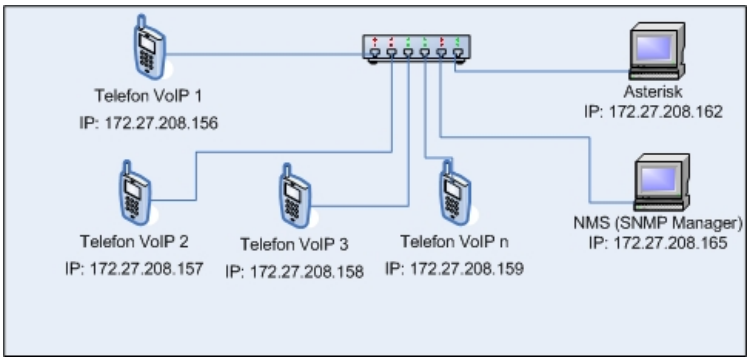

Figura 6.3 Echipamente folosite pentru realizarea experimentelor

După pornirea tuturor aplicațiilor s-au generat apeluri între clienții centralei telefonice *Asterisk*, toate informațiile rezultate în urma apelurilor fiind înregistrate de către Asterisk în fișierul *Master.csv*. Apoi, s-a verificat corectitudinea rezultatelor obținute de către aplicația *parserd*, prin verificarea informațiilor înregistrate în fișierul *SNMP_Data.xml* cu cele înregistrate în fișierul *Master.csv*. Mecanisme de programare legate de sistemul de operare Linux se găsesc în [Ste05]. Aplicația *parserd* rulează pe același PC ca și Asterisk și a fost configurat să citească informațiile din Master.csv la fiecare 10 minute. Prelucrarea unui fișier *Master.csv* conținând aproximativ 5500 înregistrări a durat mai puțin de 1 secundă. Deoarece

informațiile au fost corect înregistrate, am trecut la verificarea transferului de informații de la agentul SNMP spre manager. Astfel s-au comparat informațiile obținute cu cele din fișierul *SNMP_Data.xml*. De asemenea pentru verificare am folosit şi aplicația *snmpget.exe* disponibilă în pachetul NetSNMP.

Concluzii şi dezvoltări ulterioare

Prin extinderea MIB-ului inițial dezvoltat pentru Asterisk s-a dorit îmbunătățirea informațiilor pe care administratorii de sistem le au la dispoziție prin intermediul sistemelor de management. Prin acest mecanism administratorii pot avea informații legate de apelurile de tip VoIP şi chiar de tip PSTN care au fost inițiate prin intermediul centralei telefonice software Asterisk. Varianta prezentată în această teză obține informațiile dintr-un fişier de tip *.csv*. Acest lucru nu prezintă mari probleme la citirea informațiilor, deoarece cantitatea de informații este relativ mică. În cazul în care numărul de apeluri din centrala telefonică vor crește, se impune trecerea la un sistem de salvare a „log-urilor" în baze de date. Variantele actuale oferite de Asterisk includ SQLite, PostgreSQL şi MySQL. Prin folosirea bazelor de date se va uşura modalitatea de obținere a valorilor pentru OID-uri, deoarece se pot crea interogări mai complexe cu care să se obțină şi alte tipuri de informații.

Capitolul 7. Manageri software pentru rețele locale şi personale

În acest capitol vor fi trecute în revistă diverse aplicații care pot fi folosite pentru managementul rețelelor. Toate aceste aplicații pentru management oferă suport pentru SNMP, motivul fiind generalizarea acestui protocol.Ele oferă posibilitatea de a obține informațiile de la agenții configurați, opțiuni de detecție automată a agenților din rețeaua monitorizată, modalități de reprezentări grafice a valorilor obținute, precum şi module de analiză a datelor. Există şi funcționalitatea de control al rețelei, care să conducă la îmbunătățirea performanțelor acesteia.

7.1 Soluții software existente

a) HP Open View

HP Open View înglobată sub denumirea de HP Software & Solutions este probabil cel mai folosită aplicație comercială de management în momentul de față elaborată de Hewlett Packard. Scopul acestei suite de aplicații a fost de a asigura managementul unor rețele de dimensiuni mari. Oferă posibilitatea de extindere, încărcarea de module care să permită comunicarea cu alte sisteme de management. Elementul important în această suită o constituie "HP Network Node Manager". Printre facilitățile oferite de această aplicație sunt următoarele :

- Automatizarea managementului pentru erori, disponibilitate şi configurări în rețea
- Accesul rapid la informații prin intermediul unei interfețe grafice şi elemente predefinite pentru condiții de bază
- Detecția continuă şi automată a echipamentelor de pe straturile 2 şi 3 ale modelui OSI
- Scalabilitate, putând fi folosit pentru rețele de dimensiuni mici cât şi pentru rețele foarte mari

Această aplicație de management a fost folosită în [Dob04] pentru compararea a două sisteme diferite de management (SNMP şi CMIP). Printre facilitățile verificate au fost cele referitoare la descoperirea agenților SNMP din rețea şi mecanismul de prezentare a alarmelor. Mai multe informații despre această suită de aplicații se pot găsi în [Hp09].

b) Net-SNMP

Net-SNMP este o suită de aplicații care implementează SNMPv1,v2 şi v3. Pot fi folosite cu protocolul IPv4 şi IPv6. Toate aplicațiile din această suită sunt aplicații care sunt rulate din linia de comanda (nu au o interfață grafică, cu o excepție tkmib). Această suită de aplicații este disponibilă gratuit, fiind elaborată sub licență GPL, oferind şi codurile sursă şi rulând sub diverse sisteme de operare (Linux, Windows, FreeBSD,etc..). Detalii de folosire au fost prezentate deja în paragraful 5.2, alte informații fiind disponibile în [Net09b].

c) PRTG Network Monitor

PRTG Network Monitor poate fi folosit pentru monitorizarea rețelelor de tip LAN, WAN cu un număr maxim de echipamente de 30000. Conform producătorului, mecanismul de instalare va permite instalarea şi configurarea scenariilor de management în câteva minute. Printre facilitățile oferite amintim :

- detecția automată a echipamentelor din rețea
- şabloane predefinite pentru echipamente comune
- interfața grafică intuitivă
- posibilitatea de monitorizare a rețelelor de dimensiuni mici, medii şi mari
- aplicații ajutătoare de monitorizare
- diverse modalități de alertare şi notificare (e-mail, SMS,…)

Mai multe detalii şi informații sunt disponibile în [Pae09].

d) OpenNMS

OpenNMS este o aplicație dezvoltată atât după modelul open-source cât şi în format comercial, principala țintă finnd scalabilitatea pentru a acoperi toate aspectele precizate de modelul de management FCAPS. Principalele zone acoperite sunt:

- determinarea disponibilității serviciilor
- colectarea datelor
- managementul evenimentelor şi notificărilor

Se oferă multe posibilități de configurare a echipamentelor, de urmărire a alarmelor, rapoarte, etc... Pentru mai multe informații se poate consulta [Ope09].

7.2 Soluție propusă pentru manager software: SNMP Manager

În prima fază s-a conceput o aplicație de management [Bik06], având la bază informațiile din [Van05a] şi [Van05b]. După o perioadă de timp am renunțat la această soluție din următoarele motive :

- nu era portabilă pe toate platformele existente
- nu era optimizată pentru folosirea resurselor locale existente
- introduce trafic suplimentar care în unele cazuri poate afecta funcționarea rețelei

Din aceste motive şi datorită faptului că s-a dorit dezvoltarea unei platforme de management generale (nu dedicată masurătorilor de parametri QoS), am luat decizia de creare a unei noi aplicații cu rol de manager care va fi descrisă în continuare.
SNMP Manager este o aplicație care a fost dezvoltată cu scopul de a fi o platformă care să permită integrarea în sistemele de management a noilor agenți dezvoltați pe parcursul stagiului de doctorat. De asemenea s-a dorit analizarea mecanismelor care ar putea conduce spre realizarea unui management integrat (descris în subcapitolul următor). Aplicația SNMP Manager a fost proiectată să facă fața traficului din rețele de dimensiuni mici (LAN). Au fost incluse facilități de descoperire de agenți SNMP din rețeaua locală, de interogare periodică a unui set de OID, de creeare, editare şi export a fişierelor de tip MIB, implementează versiunile 1, 2c şi 3 ale standardului SNMP.

7.3 Propunere de tranziție spre managementul integrat al rețelelor de telecomunicații

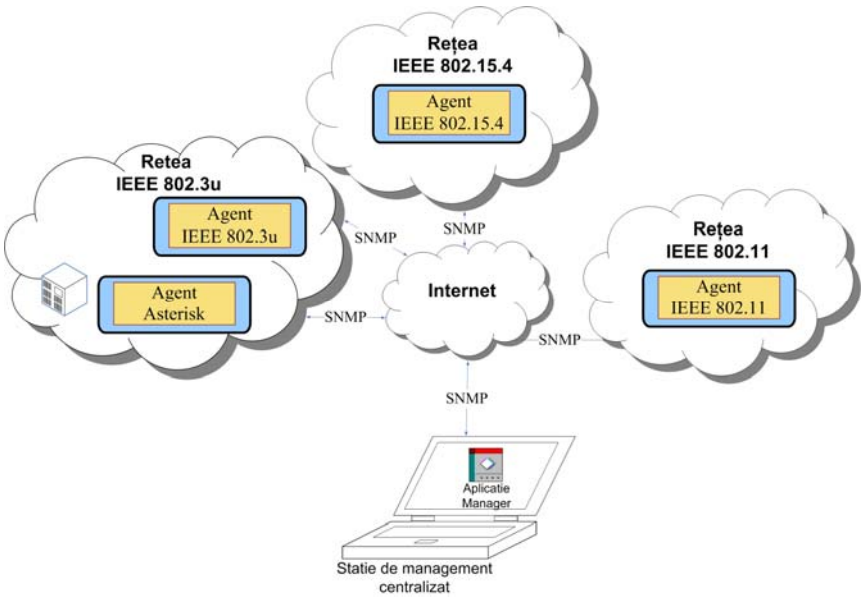

Figura 7.1 Sistemul de management centralizat bazat pe SNMP

În Figura 7.1 s-au sintetizat toate contribuțiile aduse în paragrafele precedente referitoare la generalizarea SNMP pentru rețele locale şi personale. Soluțiile în sine sunt compatibile cu conceptul de **management centralizat**, în care protocolul propus de IETF lucrează în stratul aplicație într-o arhitectură client-server, serviciile fiind oferite la portul UDP 161. Această viziune centralizată are meritul că include toate tipurile de rețele locale cu fir. Chiar dacă au fost exemplificate numai IEEE 802.3 şi IEEE 802.3u, managementul pentru Gigabit Ethernet (IEEE 802.3ab) nu diferă din punct de vedere al informațiilor gestionate. Diferențele între standarde sunt în stratul fizic şi substratul MAC, iar ideea tezei a fost ca managementul să fie plasat deasupra stivei menționate.

De asemenea, referitor la rețele locale fără fir, s-au realizat agenți software pentru IEEE 802.11a,b şi g. Pentru noile standarde IEEE 802.11n, IEEE 802.11e, soluțiile propuse sunt perfect compatibile, chiar dacă este adevărat că pot fi definite şi alte tipuri de informații de management specifice (de exemplu legate de QoS). Acestea constituie însa doar detalii care nu modifică ideea principală a tezei menționată în capitolul 1.

Soluția IEEE 802.15.4b aleasă este reprezentativă pentru întregul grup de standarde întrucât se bazează pe cele mai nefavorabile condiții (hardware minimal cu mare autonomie de funcționare din punct de vedere al consumului). Întrucât SNMP nu a fost proiectat pentru

acest tip de rețele, faptul că s-a putut generaliza managementul cu acest protocol pentru 802.15.4, demonstrează că soluții similare se pot propune şi în condiții mai puțin restrictive (de exemplu Bluetooth).
Cu toate acestea, următorul scop al tezei a fost să demonstreze că se poate face tranziția spre conceptul de management integrat, în care rolul administratorului de rețea, cu solide cunoştințe tehnice în domeniu, să fie simplificat. Eliminarea completă a intervenției umane (pe partea de management) din punct de vedere tehnic va deveni posibilă în viitor când se va trece la managementul intrinsec [Nun09].

Pentru aceasta pe platforma Asterisk sub Linux au fost integrați toți agenții propuşi anterior şi s-a ales soluția AgentX pentru o arhitectură multi-agent. Pornind de la această integrare, tranziția spre managementul integrat cerut de viitorul Internet devine posibilă dacă se respectă următorii paşi:
a) Implementarea software-ului de manager împreună cu cel de agent.

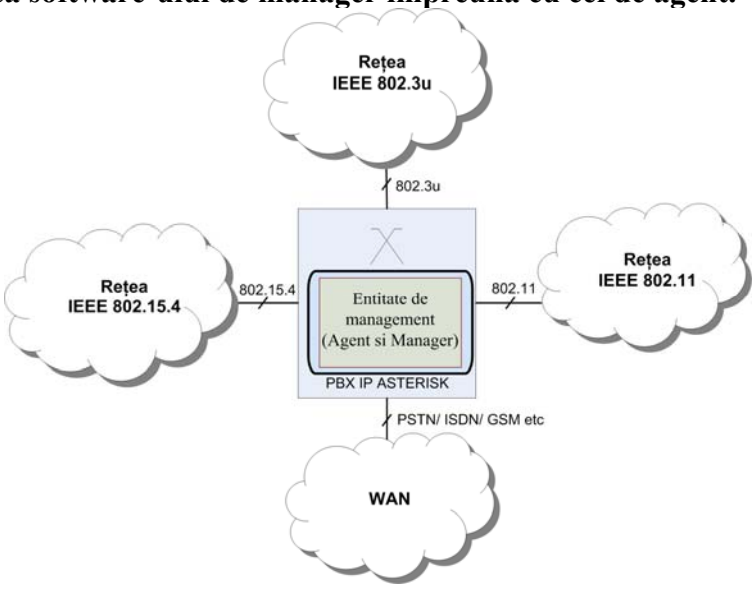

Figura 7.2 Entitate de management care integrează agentul şi managerul

Entitatea de management conține toate componente hardware/software dezvoltate în capitolele precedente.

b) Renunțarea la managementul centralizat bazat pe arhitectura client-server. Fiecare entitate de management descoperă vecinii şi are capabilități atât de manager cât şi de agent. Mai multe entități care se pot auto-gestiona şi au caracteristicile menționate anterior formează un domeniu de management.

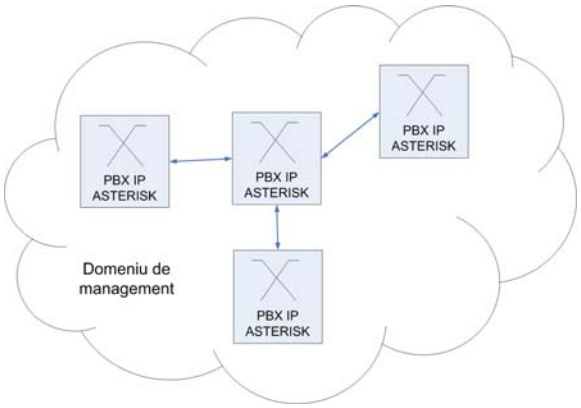

Figura 7.3 Mai multe entități de management într-un domeniu

c) Eliminarea protocoalelor de transport TCP, UDP şi chiar a protocolului de strat rețea IP.
d) Mutarea managementului direct peste substratul MAC la orice tehnologie de acces.

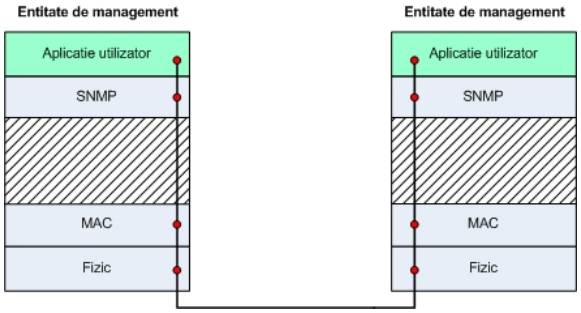

Figura 7.4 Entități de management fără stiva TCP/IP

e) În perspectivă înlocuirea SNMP cu un protocol de management integrat, de exemplu INMP propus în [Nun09]. De menționat că INMP nu a fost încă definit şi nici implementat întrucât proiectul FP7-4WARD este în curs de desfăşurare. De alftel încă se mai lucrează la extensii ale SNMP.

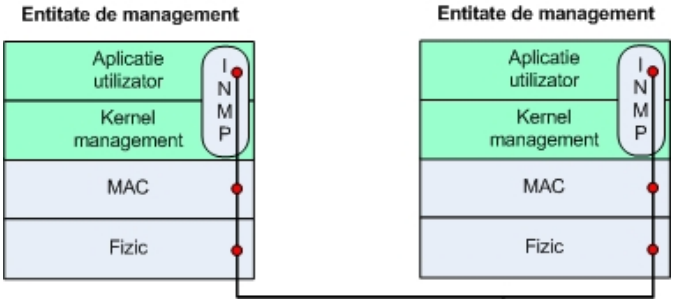

Figura 7.5 Entități de management cu INMP

Problema auto-gestionării se complică în cazul comunicațiilor inter-domeniu. Entitățile de management vor avea implementate tehnici de transmisie multi-cale, cu sau fără codarea rețelei, iar problema adresării rămâne de rezolvat. Aceste aspecte nu a fost însă abordate în teză, ele constituind propuneri pentru dezvoltări viitoare.

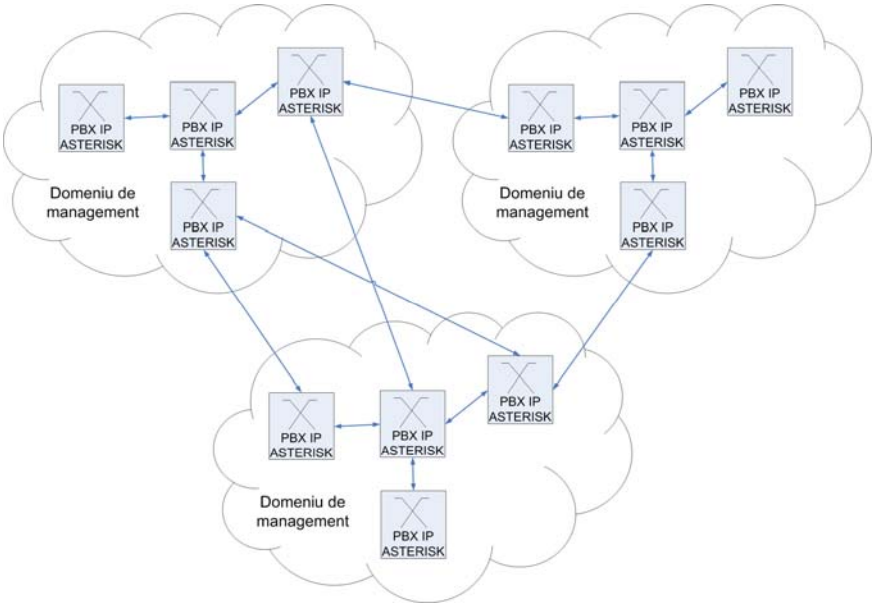

Figura 7.6 Management integrat inter-domeniu

Capitolul 8. Contribuții la managementul rețelelor locale şi personale de telecomunicații

8.1 Contribuții originale în această teză

8.1.1 Implementare agent SNMP hardware pentru IEEE 802.3

Analizând implementările de agenți SNMP existente pentru IEEE 802.3, s-a constatat că ele sunt dependente de tipul de producător (Allied Telesyn, Cisco, 3COM, etc). Sunt şi cazuri când nu există suport pentru implementări SNMP. S-a dorit implementarea unui agent hardware generic care să poată fi integrat pe orice tip de echipament, indiferent de fabricant. Conectarea spre acesta se face prin interfețe seriale asincrone (SCI), sincrone (SPI) sau paralele (GPIO pe 8 biți), iar spre rețea prin interfața EPHY de tip MII (Medium-Independent Interface) conformă cu IEEE 802.3, IEEE 802.3u. Soluția se bazează pe microcontrolerul MC9S12NE64 (Freescale), care va fi utilizat şi pentru alte contribuții, şi MIB-II. Singura parte dependentă de echipament este reprezentată de modulele software care colectează datele şi le stochează în MIB-II.

Contribuția se găseşte în: capitolul 3
Publicații: [Van05b], [Van05c]

8.1.2 Implementare agent SNMP hardware pentru IEEE 802.15.4

Din faza de standardizare s-a constatat că implementarea SNMP în rețele personale, conforme cu IEEE 802.15.4, nu este justificată, astfel că nu a existat o soluție pentru dispozitivele FFD (Full-Function Device) şi RFD (Reduced-Function Device) existente. De aceea s-a conceput un mecanism de introducere a comunicării între FFD (cu rol de coordonator de PAN) şi managerul SNMP. Comunicarea între FFD şi RFD (care poate fi un senzor, un actuator sau element de securitate) rămâne neschimbată. Față de contribuția 8.1.1, în plus la soluția hardware s-a utilizat modulul tranceiver CC2420 de la Texas Instruments, conectat la microcontroler pe interfața serială sincronă SPI. În acest fel s-a reuşit generalizarea SNMP şi în rețele personale, ca un pas spre integrarea lor într-un sistem de management complet.

Contribuția se găseşte în: capitolul 4
Publicații: [Van07a], [Van07b]

8.1.3 Realizare MIB pentru IEEE 802.15.4

Contribuția 8.1.2 este condiționată de implementarea originală a unui MIB (inexistent în faza de cercetare la doctorat) dedicat IEEE 802.15.4. Pe baza analizei traficului, s-au definit 32 de obiecte (caracterizate prin tip şi valoare) care să ofere informații relevante, cum ar fi: a) la stratul fizic : puterea de emisie şi banda de frecvență folosită; b) la substratul MAC: identificatorul de PAN, numărul de pachete transmise, numărul de pachete recepționate; c) informații despre echipamentele asociate: tip, denumire, adresă scurtă/extinsă, valoare, nivel de putere de emisie; d) în plus se pot defini praguri pentru notificări (în funcție de valoare şi/sau pachete eronate).

Contribuția se găseşte în: capitolul 4
Publicații: [Van07a], [Van07b]

8.1.4 Implementare agent SNMP software pentru IEEE 802.11

Gestionarea unei rețele WLAN cu implementarea SNMP existentă nu permite o viziune globală asupra situației tuturor stațiilor şi punctelor de acces. S-a conceput un agent software generic care să fie independent de versiunea de standard (IEEE 802.11 a,b,g,n,e) şi care să ofere informații statistice despre traficul capturat din rețeaua wireless. Soluția se bazează pe colectarea cu ajutorul unei interfețe specializate AirPcap (CACE Technologies) şi interpretarea cu analizorul de protocoale Wireshark, rulând sub sistemul de operare Windows. Rezultatele sunt stocate în fişiere .xml şi sunt accesate de agent care implementează comunicarea cu managerul prin mesaje SNMP (versiunea 1 şi 3). De menționat că versiunea de agent SNMP implementat de Windows nu a putut fi utilizată întrucât s-a bazat pe MIB-II.

Contribuția se găseşte în: capitolul 5
Publicații: [Van09b]

8.1.5 Realizare MIB pentru IEEE 802.11

Cu toate că în standarde s-a prevăzut utilizarea SNMP în rețele wireless, soluția de MIB utilizată (MIB-II) nu oferă informații specifice WLAN. În acest sens s-a conceput un MIB bazat pe 20 de obiecte (caracterizate prin tip şi valoare) care să ofere informații relevante despre: numărul de cadre (total, beacon, ACK, data, ProbeRequest, eronate, alte tipuri), valori instantanee (număr de cadre beacon/s, Ack/s, ProbeRequest/s, data/s), numărul de adrese destinație diferite, număr de adrese sursă diferite, număr de puncte de acces. Aceste informații de management pot fi utilizate în îmbunătățirea proiectării rețelei, în justificarea extinderii/ reducerii ei şi pentru îmbunătățirea securității rețelei.

Contribuția se găseşte în: capitolul 5
Publicații: [Van09b]

8.1.6 Extindere agent SNMP software pentru Asterisk

Ideea integrării mai multor agenți SNMP a fost concretizată prin crearea de către IETF a protocolului AgentX, care separă comunicarea cu managerul SNMP în 2 părți: protocolul AgentX este activat între sub-agenți şi agentul master, iar protocolul SNMP rămâne pentru comunicația între agentul master şi manager. Un exemplu de utilizare a acestei idei se referă la contribuția adusă la extinderea agentului SNMP software dintr-o centrală PBX IP de tip Asterisk. Astfel, informații de management legate de stratul aplicație (apeluri şi taxare) pot fi colectate dintr-un fişier de tip .log, trecute printr-un program de analiză şi interpretare (parsare) şi stocate într-un fişier .xml. Acesta va fi utilizat de sub-agentul SNMP implementat, care va comunica cu agentul master. Soluția aleasă este în conjuncție cu contribuția 8.1.8.

Contribuția se găseşte în: capitolul 6
Publicații: [Van09a]

8.1.7 Extindere MIB pentru Asterisk

Contribuția nu se referă la noi tehnologii de acces în rețele, ea fiind de data aceasta focalizată pe extinderea MIB pentru aplicații VoIP (Asterisk), deci pentru stratul aplicație. S-au definit 7 obiecte (caracterizate prin tip şi valoare) care să ofere informații relevante despre: numărul

total de apeluri, numărul de apeluri la care s-a răspuns, numărul de apeluri la care nu s-a răspuns, număr de apeluri pentru abonați ocupați, intervalul de taxare, intervalul de monitorizare. Chiar dacă informațiile de management obținute servesc la o situație concretă (apelurile în Asterisk), de fapt s-a dorit să se demonstreze fezabilitatea integrării managementului aplicațiilor cu managementul accesului la rețea.

Contribuția se găseşte în: capitolul 6
Publicații: [Van09a]

8.1.8 Propunere tranziție spre managementul integrat

Accentul în teză a căzut pe cercetarea comportamentului agenților de management, fără a se insista pe partea de NMS (Network Management Station) pe care rulează de regulă o aplicație cu rol de manager. S-au analizat soluțiile existente (HP Open View, NetSNMP, PRTG Network Monitor, Open NMS), dar s-a ajuns la concluzia că este nevoie de o soluție flexibilă care să permită extensii, conform noilor agenți definiți. S-a implementat o aplicație numită SNMP Manager, necesară pentru demonstrarea propunerii de tranziție spre un management integrat. În acest scop, pe platforma Asterisk sub Linux pot fi integrați toți agenții propuşi în contribuțiile 8.1.1–8.1.7 şi se poate utiliza soluția AgentX pentru o arhitectură multi-agent. Pornind de la această integrare, tranziția spre managementul integrat cerut de viitorul Internet devine posibilă dacă se respectă următorii paşi: a) implementarea software-ului de manager împreună cu cel de agent; b) renunțarea la managementul centralizat bazat pe arhitectura client-server; c) eliminarea protocoalelor de transport (TCP, UDP) şi chiar a protocolului de strat rețea (IP); d) mutarea managementului direct peste substratul MAC la orice tehnologie de acces; e) în perspectivă înlocuirea SNMP cu un protocol de management integrat.

Contribuția se găseşte în: capitolul 7
Publicații: [Bik06], [Dob04], [Van05a], [Van05b]

8.2 Remarci finale

Faza îndelungată de cercetare (circa 10 ani) a impus evident reorientarea tezei spre noile concepte (management distribuit, management integrat) alături de noile tehnologii apărute în ultimii ani (atât în rețele locale cât şi în rețele personale). Interesul deosebit pentru acest subiect este dovedit şi prin includerea tematicii ca prioritate în proiecte de cercetare internaționale de tip FP7. Proiectul FP7-4WARD (pronunțat ca şi cuvântul "Forward") este intitulat „Arhitecture and Design for the Future Internet", fiind un răspuns la provocările Internetului de mâine. Actualele arhitecturi de rețele nu mai permit inovații decât la partea de aplicații, când de fapt este nevoie de schimbări radicale în structura şi principiile folosite. 4WARD nu îşi propune să creeze soluții evolutive ci pur şi simplu **să regândească complet filosofia Internetului,** pornind de la cerințele tot mai mari de mobilitate şi acces wireless. Mai multe tipuri de rețele vor coexista pe platforme comune, la care virtualizarea să joace un rol esential. Rețelele trebuie să se auto-gestioneze (vezi conceptul INM, adică In-Network Management) iar aplicațiile trebuie să fie centrate pe obiecte de informație în loc să fie centrate pe noduri de rețea. Soluțiile vor include toate tipurile de rețele, de la cele bazate pe fibre optice, până la rețele wireless sau de senzori.

Bibliografie selectivă

[802.3] ***, IEEE Std 802.3™-2008 – Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications, *IEEE*, September 2008

[802.11] ***, IEEE Std 802.11™-2007 - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, *IEEE*, 2007

[802.15.4] ***, IEEE Std 802.15.4™-2006 - Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs), *IEEE*, 2007

[ASN87] ***, „Information Processing Systems - Open Systems Interconnection – Specification of Abstract Syntax Notation One (ASN.1)", *International Standard 8824,* ISO 1987.

[Ber09] J.Berg, „Radiotap Header Description", 2009, http://www.radiotap.org/

[Bej06] Y.Bejerano, „Taking the skeletons out of the closets: A simple and efficient topology discovery scheme for large ethernet LANs", Proc. IEEE INFOCOM, 2006, pp. 1797 - 1809, April 2006.

[Bik06] A.Bikfalvi, P.Patras, **C.M.Vancea** & V.Dobrota, „The Management Infrastructure of a Network Measurement System for QoS Parameters", *14th International Conference on Software, Telecommunications & Computer Networks SOFTCOM 2006*, Split-Dubrovnik, Croatia, September 29–October 1, 2006, S6-6128-2909, ISBN 953-6114-87-9, pp.242-246

[Blu98] U.Blumenthal, B.Wijnen, „User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3).", *RFC2274*, IETF, January 1998.

[Bor01] S.Boros, B. Helthuis, A. Pras, „Distributed MIB Object Information Service", Proceedings of the High Speed Networking, May 2001

[Bor09] C.Bormann, G.Mulligan, „6lowpan Status Pages", *IETF*, 2009, http://tools.ietf.org/wg/6lowpan/

[Cac09] ***, AirPcap Family, *CACE Technologies,* 2009, http://www.cacetech.com/products/airpcap.html

[Cal02] E.Callaway, P.Gorday, L.Hester, J.A.Gutierrez, M.Naeve, B.Heile, V.Bahl, „Home Networking with IEEE 802.15.4: A Developing Standard for Low-Rate Wireless Personal Area Networks, *IEEE Communications Magazine,* Vol.40, No.8, August 2002, pp.70-77

[Cas90] J.D.Case, M.Fedor, M.L.Schoffstall, J.Davin, „Simple Network Management Protocol (SNMP)", *RFC1157*, IETF, May 1990.

[Cas93] J.Case, K.McCloghrie, M.Rose, S.Waldbusser, „Structure of Management Information for version 2 of the Simple Network Management Protocol (SNMPv2).", *RFC1442*, IETF, April 1993.

[Cas96a] J.Case, K.McCloghrie, M.Rose, S.Waldbusser, „Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2).", *RFC1902*, IETF, January 1996.

[Cas96b] J.Case, K.McCloghrie, M.Rose, S.Waldbusser, „Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2).", *RFC1905*, IETF, January 1996.

[Cas99a] J.Case, D.Harrington, R.Presuhn, B.Wijnen, „Message Processing and Dispatching for the Simple Network Management Protocol (SNMP).", *RFC2572*, IETF, April 1999.

[Cas99b] J.Case, R.Frye, J.Saperia, *SNMPv3 Survival Guide,* John Wiley & Sons 1999

[Cha09] E.Chamberlain, „HowTo: Monitor Asterisk with SNMP", 2009, http://voxilla.com/2009/02/03/configuring-asterisk-snmp-support-1131

[Cho06] D.Choi, H.Jang, K.Jeong, P.Kim, S.Kim, „Delivery and Storage Architecture for Sensed Information Using SNMP", „*Management of Convergence Networks and Services",* Springer Berlin / Heidelberg, September 2006

[Dan00] M.Daniele, B.Wijnen, M.Ellison, D.Francisco, „Agent Extensibility (AgentX) Protocol Version 1", *RFC 2741*, IETF, January 2000

[Div99] K.U.Divakara, „TMN: Telecommunications Management Network (TMN)", McGraw-Hill, 1999

[Dob02] V.Dobrota, D.Zinca, **C.M.Vancea** & G.Lazar, "Voice over IP Solutions for CAMAN: H.323 versus SIP", *First RoEduNet International Conference "Networking in Education and Research"* , Cluj-Napoca, 18-19 April 2002

[Dob04] V.Dobrota, D.Zinca, **C.M.Vancea**, B.Moraru, T.Blaga, F.Copaciu & G.Lazar, "PSTN/ ISDN/ VoIP-Based Solution for Voice Communications within Cluj-Napoca Academic MAN", 3rd RoEduNet International Conference "Networking in Education and Research", Timisoara, 27-29 May 2004, *Scientific Bulletin of the "POLITEHNICA" University of Timisoara, Romania, Transactions on AUTOMATIC CONTROL and COMPUTER SCIENCE,* Vol. 49(63) 2004 No. 5, pp. 107-112, ISSN 1224-600X

[Fre06] ***, MC9S12NE64 Data Sheet, *Freescale Semiconductor*, June 2006, http://www.freescale.com/files/microcontrollers/doc/data_sheet/MC9S12NE64V1.pdf

[Fen06] H.Feng, Y.Shu, S.Wang, M.Ma, „SVM-based models for predicting WLAN traffic", *Proc. IEEE ICC*, 2006, pp. 591 - 596, June 2006.

[Gut01] J.A.Gutierrez, M.Naeve, E.Callaway, M.Bourgeois, V.Mitter, B. Heile, „IEEE 802.15.4: A Developing Standard for Low-Power Low-Cost Wireless Personal Area Networks", *IEEE Network*, Vol.15, No.5, 2001, pp.12-19, ISSN: 0890-8044

[Har02] D.Harrington, R.Presuhn, B.Wijnen, „An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks.", *RFC3411*, IETF, December 2002.

[How03] I.Howitt, J.A.Gutierrez, „IEEE 802.15.4 Low-Rate Wireless Personal Area Network Coexistence Issues", *IEEE Wireless Communications and Networking*, Vol.3, 2003, pp.1481-1486

[Hp09] ***, HP Network Node Manager (NNM) Advanced Edition software, *HP*, 2009, http://www.openview.hp.com/products/nnm/index.html

[Ian09] ***, Network Management Parameters, *IANA,* 2009, http://www.iana.org/assignments/smi-numbers

[Iet09] ***, „IETF Overview", IETF, 2009, http://www.ietf.org/overview.html

[Iso09] ***, ISO Description, 2009, http://www.iso.org/iso/about.htm

[Ker03] J.Kerdsri, „*SNMP Over Wi-Fi Wireless Networks"*, Storming Media, 2003

[M.3000] ***, „Overview of TMN Recommendations", *ITU-T M.3000*, 1994

[M.3010] ***, „Principles for a Telecommunications management network", *ITU-T M.3010*, 1996

[M.3020] ***, „TMN Interface Specification Methodology", *ITU-T M.3020*, 1995

[M.3320] ***, „Management requirements framework for the TMN X-Interface", *ITU-T M.3320*, 1997

[M.3400] ***, „TMN Management Functions", *ITU-T M.3400*, 1997

[Mau01] D.Mauro, „*Essential SNMP"*, O'Reilly , 2001

[McC90] K.McCloghrie, M.T.Rose, „Management Information Base for network management of TCP/IP-based internets.", *RFC1156*, IETF, May 1990.

[McC91] K.McCloghrie, M.Rose, „Management Information Base for Network Management of TCP/IP-based internets:MIB-II", *RFC1213*, IETF, March 1991.

[McC99] K.McCloghrie, D.Perkins, J.Schoenwaelder, „Structure of Management Information Version 2 (SMIv2).", *RFC2578*, IETF, April 1999.

[Meg05] J. VanMeggelen, J.Smith & L.Madsen, "*Asterisk™ The Future of Telephony",* O'Reilly Media Inc, 2005

[Mic09] ***, ZENA Network Analyzer, *Microchip,* 2009,

http://www.microchip.com/stellent/idcplg?IdcService=SS_GET_PAGE&nodeId=1406&dDocName=en520682
[Mil97] M.A.Miller, „*Managing Internetworks with SNMP”*, IDG Books Worldwide, 1997
[Nan07a] K.Nandakishore, „6LoWPAN: Overview, Assumptions, Problem Statement and Goals 7”, February 2007, http://tools.ietf.org/html/draft-ietf-6lowpan-problem-07
[Nan07b] K.Nandakishore, „6LoWPAN: Overview, Assumptions, Problem Statement and Goals 8, February 2007, http://tools.ietf.org/html/draft-ietf-6lowpan-problem-08
[Net09a] ***, Net-SNMP Man pages, 2009, http://www.net-snmp.org/docs/man/
[Net09b] ***, Net-SNMP Tutorials, 2009, http://www.net-snmp.org/wiki/index.php/Tutorials
[Nun09] G.Nunzi, D.Dudkowski (editors), V.Dobrota, A.B.Rus (included in list of contributors) et al., “Example of INM Framework Instantiation”, *D-4.2 In -Network Management Concept”, FP7-ICT-2007-1-216041-4WARD– “Architecture and Design for the Future Internet”,* 31 March 2009, Revision 2.0, pp.39-42, 115-122.
[Ope09] ***, OpenNMS Main Page, 2009, http://www.opennms.org
[Pae09] ***, PRTG Network Monitor, *Paessler AG,* 2009, http://www.paessler.com/prtg/
[Per96] D.Perkins, E.McGinnis, ”*Understanding SNMP MIBs”,* PrenticeHall,1996
[Ros90] M.T.Rose, K.McCloghrie, „Structure and Identification of Management Information for TCP/IP-Based Internets”, *RFC1155*, IETF, May 1990.
[Shr95] J.K. Shrewsbury, „An Introduction to TMN”, Journal of Network and Systems Management, Vol. 3, No. 1, March 1995
[Sim97] P.Simoneau, „*Hands-On SNMP*, McGraw-Hill, 1997
[Spe03] M.Spencer, M.Allison, C.Rhodes, *The Asterisk Handbook Version 2*, http://www.digium.com, 2003
[Spe09] M.Spencer et al., „IAX: Inter-Asterisk eXchange Version 2, draft-guy-iax-05”, *Internet Draft,* IETF 2009, http://tools.ietf.org/html/draft-guy-iax-05
[Spu00] C.E. Spurgeon, *Ethernet : The Definitive Guide*, O'Reilly, 2000
[Sta93] W.Stallings, *SNMP, SNMPv2, and CMIP: The Practical Guide to Network Management Standards,* Addison-Wesley, Reading, MA, USA, 1993.
[Sta98] W.Stallings, *SNMP, SNMPv2, SNMPv3, RMON 1 and 2*, Addison-Wesley Pub Co ,1998
[Ste05] W.R.Stevens, S.A.Rago, *Advanced Programming in the UNIX(R) Environment (2nd Edition)*, Addison-Wesley Professional, 2005
[Tan03] A.S.Tanenbaum, *Computer Networks, Fourth Edition*, Prentice-Hall, 2003
[Tex07] ****, CC2420 Data Sheet, *Texas Instruments,* March 2007, http://focus.ti.com/lit/ds/symlink/cc2420.pdf
[Van05a] **C.M.Vancea**, Referat de doctorat I: „Analiza rețelelor de telecomuncații în vederea gestionării”, *Universitatea Tehnică din Cluj-Napoca,* 2005.
[Van05b] **C.M.Vancea**, Referat de doctorat II: „Algoritmi de gestionare a calității”, *Universitatea Tehnică din Cluj-Napoca,* 2005.
[Van05c] **C.M.Vancea,** Referat de doctorat III: „Rezultate experimentale în gestionarea calității serviciilor”, *Universitatea Tehnică din Cluj-Napoca,* 2005.
[Van07a] **C.M.Vancea** & V.Dobrota, “Monitoring Low-Rate Wireless Personal Area Networks Using SNMP”, *ACTA TECHNICA NAPOCENSIS, Electronics and Telecommunications,* ISSN 1221-6542, Vol.48, No.3, 2007, pp.5-8
[Van07b] **C.M.Vancea** & V.Dobrota, “Enabling SNMP for IEEE 802.15.4: A Practical Architecture”, *6th RoEduNet International Conference “Networking in*

Education and Research", Craiova, Romania, November 23-24, 2007, pp.49 -53, ISBN 978-973-746-581-8

[Van09a] **C.M.Vancea** & V.Dobrota, "Retrieving Call Detail Records from Asterisk using SNMP", *ACTA TECHNICA NAPOCENSIS, Electronics and Telecommunications,* ISSN 1221-6542, Vol.50, No.3, 2009 (spre publicare)

[Van09b] **C.M.Vancea** & V.Dobrota, "SNMP Agent for WLAN networks", *8th RoEduNet International Conference"Networking in Education and Research",* Galati, Romania, 2009 (spre publicare)

[War89] U.Warrier, L.Besaw, „The Common Management Information Services and Protocol over TCP/IP (CMOT)", *RFC1095,* IETF, April 1989

[Wir09a] ***, About Wireshark, 2009, http://www.wireshark.org/about.html

[Wir09b] ***, Libpcap File Format, 2009, http://wiki.wireshark.org/Development/LibpcapFileFormat

[Wij98] B.Wijnen, R.Presuhn, K.McCloghrie, „View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP).", *RFC2275,* IETF, January 1998.

[Zel99] David Zeltserman, Dave Zeltserman, *Practical Guide to SNMPv3 and Network Management,* Prentice Hall, 1999

[Zhe04] J.Zheng, M.J. Lee, „Will IEEE 802.15.4 make Ubiquitous networking a reality?: A discussion on a potential low power, low bit rate standard.", *IEEE Communications Magazine*, vol. 42, pp. 140 - 146, June 2004

[Zin02a] D.Zinca, V.Dobrota, **C.M.Vancea** & G.Lazar, "A Practical Evaluation of QoS for Voice over IP", *Proceedings of the 12th IEEE Workshop on Local and Metropolitan Area Networks, LANMAN 2002*, 11-14 August 2002, Stockholm-Kista, Sweden, pp.65-69

[Zin02b] D.Zinca, V.Dobrota, **C.M.Vancea** & G.Lazar, "Protocols for Communication Between QoS Agents: COPS and SDP", *Proceedings of the 3rd COST #276 Workshop on Information and Knowledge Management for Integrated Media Communication,* Budapest, Hungary, 11-12 October 2002, pp.53-58

[Zin02c] D.Zinca, V.Dobrota, **C.M.Vancea** & G.Lazar, "A Practical Quality of Service Evaluation for Voice over IP: IntServ Approach versus DiffServ Approach", *Proceedings of the IEEE International Conference "Communications 2002",* Bucharest, 5-7 December 2002, ISBN 973-8290-67-8, pp. 73-78

[Zin06] D.Zinca, *Rețele de calculatoare*, Editura Risoprint, Cluj-Napoca, 2006

[X.701] ***, „Information Technology - Open Systems Interconnection - Systems Management Overview", *ITU-T X.701*, Geneva 1997

[X.710] ***, „Information technology - Open Systems Interconnection - Common Management Information service", *ITU-T X.710*, Geneva 1997

[X.711] ***, „Information technology - Open Systems Interconnection - Common Management Information Protocol: Specification", *ITU-T X.711*, Geneva 1997

[X.720] ***, „Information technology - Open Systems Interconnection - Structure of management information: Management information model ", *ITU-T X.720*, Geneva 1992

[X.721] ***, „Information technology - Open Systems Interconnection - Structure of management information: Definition of management information", *ITU-T X.721*, Geneva 1992

[X.722] ***, „Information technology - Open Systems Interconnection - Structure of management information: Guidelines for the definition of managed objects", *ITU-T X.722*, Geneva 1992

UNIVERSITATEA TEHNICA CLUJ-NAPOCA FACULTATEA ELECTRONICA, TELECOMUNICATII SI TEHNOLOGIA INFORMATIEI

INFORMATII PERSONALE

Numele si prenumele	**VANCEA, CRISTIAN MIHAI**
Telefon/Fax	0264-401264; 0264-597083
E-mail	**Mihai.Vancea@com.utcluj.ro**

PROFESIA/OCUPATIA ACTUALA

• Data	1999
• Loc de munca	Catedra Comunicatii; Facultatea Electronica, Telecomunicatii si Tehnologia Informatiei
• Profesia	Inginer, Specializarea Electronica si Telecomunicatii
• Ocupatia	Asistent
• Activitatea principala	Activitati didactice si de cercetare
• Conducator de doctorat	Nu
• Domeniul	

EDUCATIE SI STUDII DE CALIFICARE

• Anul	1998
• Numele si tipul organizatiei	Universitatea Tehnica Cluj-Napoca, Facultatea de Electronica si Telecomunicatii
• Titlul obtinut	Inginer electronica si telecomunicatii
• Specializarea	Comunicatii
• Anul	1999
• Numele si tipul organizatiei	Universitatea Tehnica din Cluj-Napoca, Facultatea Electronica si Telecomunicatii
• Titlul obtinut	Master
• Specializarea	Inginer electronica si telecomunicatii

CURSURI DE PERFECȚIONARE SAU SPECIALIZARE

• Anul	Iulie 2001
• *Certificare obținută*	Academia locala Cisco Facultatea de Electronica, Telecomunicatii si Tehnologia Informatiei, 4 module CCNA – Certified Cisco Network Associate
• Anul	Septembrie 2001
• *Certificare obținută*	Curs specializare „ISP Network Management”, Ericsson, Dublin
• *Anul*	Septembrie 2001
• *Certificare obținută*	Curs specializare „Voice over IP”, Ericsson, Dublin

ACTIVITATE DIDACTICA

EXPERIENTA PROFESIONALA

COLABORATOR AL CURSURILOR	PROGRAMUL DE STUDII	ANUL
Protocoale pentru Internet	Telecomunicații	IV
Sisteme de comutație şi rutare	Telecomunicații	III
Rețele de calculatoare	Telecomunicații	III

ACTIVITATE STIINTIFICA

TEME DE CERCETARE

- Managementul retelelor de telecomunicatii
- Sisteme cu microcontrolere

PUBLICATII

(TOTAL DIN CARE 5 LUCRARI REPREZENTATIVE PUBLICATE DIN 2002)

17 lucrari din care:

1. D.Zinca, V.Dobrota & **C.M.Vancea** - "Estimating the Optimal Model for Layer 4 Switching in IPv6 and IPv4", *11th IEEE Workshop on Local and Metropolitan Area Networks LANMAN'2001*, Boulder, Colorado, USA, pp.68-71.

2. D.Zinca, V.Dobrota, **C.M.Vancea** & G.Lazar, "A Practical Evaluation of QoS for Voice over IP", *Proceedings of the 12th IEEE Workshop on Local and Metropolitan Area Networks, LANMAN 2002*, 11-14 August 2002, Stockholm-Kista, Sweden, pp.65-69.

3. A.Bikfalvi, P.Patras, **C.M.Vancea** & V.Dobrota, "The Management Infrastructure of a Network Measurement System for QoS Parameters", *14th International Conference on Software, Telecommunications & Computer Networks SOFTCOM 2006,* Split-Dubrovnik, Croatia, September 29 – October 1, 2006, S6-6128-2909, ISBN 953-6114-87-9

4**. C.M.Vancea** & V.Dobrota - "Monitoring Low-Rate Wireless Personal Area SNMP", *ACTA TECHNICA NAPOCENSIS, Electronics and Telecommunications,* ISSN 1221-6542, Vol.48, No.3, 2007, pp.5-8

5. **C.M.Vancea** & V.Dobrota, "Retrieving Call Detail Records from Asterisk" *ACTA TECHNICA NAPOCENSIS, Electronics and Telecommunications,* ISSN 1221-6542, Vol.50, No.3, 2009

Cluj-Napoca
10/09/2009

As. ing. Cristian Mihai VANCEA