UNIVERSITATEA "POLITEHNICA" BUCUREŞTI

-Facultatea de Electronică, Telecomunicații şi Tehnologia Informației –

TEHNOLOGII DEDICATE COMUNICAȚIILOR INTERNET

CUPRINS:

1. INTRODUCERE

2. TEHNOLOGIA WI-FI – *autor, Trancă Ioan-Alexandru, 454A*
   - 2.1. INTRODUCERE
   - 2.2. ECHIPAMENTE STANDARD
     - 2.2.1.ACCES POINT
     - 2.2.2.ADAPTOR WIRELESS
     - 2.2.3.ROUTER WIRELESS
     - 2.2.4.NETWORK BRIDGE
     - 2.2.5.ANTENE ŞI CONECTORI
   - 2.3. STANDARDELE DE COMUNICAŢIE WI-FI IEEE 802.11
     - 2.3.1.802.11a
     - 2.3.2.802.11b
     - 2.3.3.802.11g
     - 2.3.4.802.11n
   - 2.4. SECURITATE ŞI METODE DE CRIPTARE
     - 2.4.1.WIRED EQUIVALENT PRIVACY – WEP
       - 2.4.1.1.METODE DE AUTENTIFICARE
     - 2.4.2.WI-FI PROTECTED ACCESS
   - 2.5. CONCLUZII
   - 2.6. REFERINŢE BIBLIOGRAFICE

3. TEHNOLOGIA ISDN – *autor, Dicu Mario-Lucian, 453A* .
   - 3.1. INTRODUCERE
   - 3.2. CONFIGURAŢII
   - 3.3. PUNCTE DE REFERINŢĂ
   - 3.4. TIPURI DE COMUNICAŢII SUPORTATE
   - 3.5. SPECIFICAŢII ISDN
     - 3.5.1.LAYER 1
     - 3.5.2.LAYER 2
     - 3.5.3.LAYER 3
   - 3.6. CONCLUZII
     - 3.6.1.APLICAŢII
     - 3.6.2.LUMEA REALĂ
   - 3.7. REFERINŢE BIBLIOGRAFICE

4. TEHNOLOGIA DSL – *autor, Enache Elena, 455A*
   - 4.1. INTRODUCERE
   - 4.2. VOCE ŞI DATE
   - 4.3. FUNCŢIONARE
   - 4.4. ECHIPAMENTE
   - 4.5. SETĂRI STANDARD ŞI PROCEDURI DE CONECTARE
   - 4.6. PROTOCOALE ŞI CONFICURAŢII

4.7. Tehnologii DSL
4.8. Metode de Transmisie
4.9. Concluzii
4.10. Referințe bibliografice

5. **Tehnologia ATM** – ***autor, Niculescu Bogdan, 454A*** .
5.1. Introducere
5.2. Structura celulei ATM
5.3. Transferul trunchiurilor PBX în ATM
5.4. Parametri de calitate ATM
5.5. Aplicațiile modului de transfer
5.6. Maparea Protocolului
5.7. Concluzii
5.8. Referințe Bibiliografice

6. **Tehnologia MPLS** – ***autor, Ghiță Ana-Maria, 455A***
6.1. Introducere
6.2. Concepte de rutare și comutare
6.3. Concepte MPLS și terminologie
6.3.1.Forwarding-ul bazat pe IP
6.3.2.Forwarding-ul bazat pe FEC
6.3.3.Forwarding-ul bazat pe MPLS
6.3.4.Routere cu comutare de etichetă – LSR
6.3.5.MPLS peste IP standard
6.3.6.Distribuția de etichete LDP
6.3.7.Label Switch Path – LSP
6.4. Quality of Service
6.5. Concluzii
6.6. Referințe Bibliografice

7. **Tehnologia VoIP** – ***autor, Dochie Oana-Andreea, 454A*** .
7.1. Introducere
7.2. VoIP vs. Rețeaua de Telefonie Publică
7.2.1.Dezavantajele rețelei de telefonie
7.2.2.Diferența între comutarea de circuit și comutarea de pachete
7.2.3.Avantaje VoIP
7.3. Descrierea tehnologiei VoIP
7.3.1.Protocolul IP
7.3.2.Carcteristici VoIP
7.3.2.1.Intârzierea/Latența
7.3.2.2.Jitterul
7.3.2.3.Compresia vocii
7.3.2.4.Ecoul
7.3.2.5.Pierderea de Pachete
7.3.2.6.Detecția Activității vocii

7.4. Protocoale de transport
7.4.1. Protocolul de transport în timp real
7.4.2. Protocolul de control RTP (RTCP)
7.5. Semnalizarea VoIP
7.5.1. Semnalizarea între rutere şi PBX-uri
7.5.2. Protocoale şi standarde
7.5.3. Protocolul H.323
7.5.4. Session Initiation Protocol (SIP)
7.5.5. Servere SIP
7.6. Securitatea reţelelor VoIP
7.6.1. Protocoale de telefonie vulnerabile
7.6.2. Cerinţe de securitate în reţelele bazate pe telefonie IP
7.7. Concluzii
7.8. Referinţe Bibliografice

8. Concluzii

9. Referinţe Bibliografice

1. INTRODUCERE

„La început a fost cablul...”

Se întâmpla în anul 1858 când omenirea era pe punctul de a face un pas istoric. Se simțea nevoia de o comunicare mult mai simplă, foarte rapidă, lucru ce părea imposibil de realizat între Europa şi America cu sistemele de comunicații existente la acea vreme.

Având în vedere raportarea la timpul istoric a acestei manifestări, în vecinătatea revoluției industriale, era totuşi evidentă găsirea unei soluții, umanitatea deja având la dispoziție resursele atât logistice cât şi stiințifice ce stăteau la baza realizării unui sistem de comunicații între cele două continente puternic dezvoltate.

Astfel, la data de 28 Iulie 1866 a fost inaugurat primul sistem de comunicații de anvergură ce lega cele două continente. Existaseră şi în anii precedenți câteva încercări similare dar toate fuseseră catalogate drept eşecuri, cablul cedând fizic de mai multe ori.

Acest sistem de comunicații a rămas în istorie, sub numele de „Cablul Atlantic”, ca stând la baza genezei erei informatice ce avea să influențeze defintiv societatea începând cu secolul XX.

Sistemul inaugurat in 1866 lega Insula Valentia din vestul Irlandei cu provincia Newfoundland din Canada. Dispunea de un cablu cu o lungime de 4260km ce era alcătuit din şapte fire de cupru învelite fiecare în câte trei învelişuri de gutta-percha, greutatea finală a cablului fiind de circa 550kg/km.

Cablul inaugurat în 1866 putea transmite opt cuvinte/minut şi era de 50 de ori mai rapid decât cel pe care se bazase sistemul încercat în 1858. Cu timpul, performanțele sale au crescut, ajungând la începutul secolului al XX-lea la o viteză de 120 cuvinte/minut.

Acesta a fost doar începutul a ceea ce astăzi se numeşte sistem de comunicații „world wide” sau World Wide Web.

In prezent, vitezele de comunicație sunt amețitoare în comparație cu cele de la începutul secolului. Evoluția tehnologică şi mai ales explozia erei informatice au dus la progrese uimitoare în ultima decadă. Dacă în 1858 viteze precum 0.2 cuvinte/minut şi Cablul Transatlantic păreau realizări incredibile ale vremii, prezentul ne oferă o gamă largă de sisteme de comunicații.

Noile tehnologii utilizate în comunicațiile Internet oferă atât viteze foarte mari cât şi o serie de caracteristici şi funcționalități ce le fac foarte uşor de folosit şi la îndemâna oricui.

(www.atlantic-cable.com, http://en.wikipedia.org/wiki/Atlantic_cable;)

Fig. 1: Secțiune transversală a cablului utilizat în 1866
(http://www.electricedge.com/greymatter/images4/cable_atlantic.jpg)

2. TEHNOLOGIA WI-FI

2.1. INTRODUCERE

In ultimii zece ani, întregul mapamond a devenit mult mai mobil. Ca urmare a acestei tendințe, nici metodele clasice de rețelistica nu puteau rămâne aceleaşi, trebuiau să se conformeze noului stil de viață pe care omenirea începuse să-l adopte. Dacă toți utilizatorii de aplicații internet şi nu numai ar trebui să fie conectați fizic la rețelele din care fac parte, gradul de mobilitate ar scădea dramatic. S-a căutat o soluție care să confere utilizatorilor mobilitate cât se poate de mare dar care să şi păstreze performanțe asemănătoare tehnologiilor de conectare cu fir folosite până la momentul respectiv. Astfel au apărut mai multe soluții fără fir, una dintre cele mai importante fiind tehnologia Wi-Fi cunoscută şi sub numele de tehnologia 802.11.
Cu ajutorul acestei tehnologii se urmăreşte apropierea mobilității rețelelor de calculatoare cu acces la Internet de gradul la care a ajuns în prezent mobilitatea telefoniei fără fir.
(***802.11® Wireless Networks: The Definitive Guide, published by O`REILLY, 2002 by Matthew Gast, pag. 14***)

Wi-Fi reprezintă o marcă înregistrată a consorțiului Wi-Fi Alliance menită a îmbunătăți interoperabilitatea rețelelor locale de calculatoare fără fir construite pe baza standardelor IEEE 802.11. Aplicațiile comune ale Wi-Fi înglobează Internet şi acces la telefonie Voice over IP, posibilitatea de conectare altor echipamente cum ar fi DVD player-e, camere digitale sau console dedicate jocurilor.Wi-Fi foloseşte atât tehnologia radio de propagare cu o singură purtătoare şi spectru propagat în seuccesiune directă, DSSS (direct sequence spread spectrum) cât şi cea cu purtătoare multiplă şi multipelxare cu divizare ortogonală a frecvenței, OFDM (Orthogonal Frequency Division Multiplexing). Aceste tehnologii au stat şi la baza dezvoltării celorlalte tehnolgii fără fir cum ar fi HomeRF şi Bluetooth. In anul 1985, Comisia Federală de Comunicații (FCC) a făcut posibilă folosirea tehnolgiei wireless făra brevet în SUA, urmând ca mai târziu şi alte țări să adopte această directivă.

Tehnolgia precursoare Wi-Fi a fost inventată în anul 1991 de către o echipă de ingineri de la NCR Corporation/AT&T în Nieuwgwin, Olanda. Purta numele WaveLAN şi oferea viteze aflate între 1Mbit/s şi 2Mbit/s.

Tehnolgia Wi-Fi a apărut în anul 1997 ca brand al Wi-Fi Alliance, un consorțiu alcătuit din mai multe companii ce şi-au dedicat o parte din activitate cercetării şi găsirii unei posibilități de asigurare a interoperabilității produselor wireless bazate pe familia de standarde IEEE 802.11.Wi-Fi Alliance certifică produsele după un set de reguli şi proceduri de testare bine stabilite urmând ca producătorii de echipamente wireless care au primit certificarea lor să poată marca pe ambalajele produselor logoul Wi-Fi.In momentul de față, toate sistemele de operare de largă utilizare (Windows, Mac OS, Solaris, Linux) sunt cofigurate să suporte tehnolgia de conectare wireless la Internet sau alte echipamente.Conexiunea este realizată prin intermediul unei antene care trebuie să se afle în raza de acțiune a unui access-point sau a mai multor access-point-uri interconectate-hotspot.

Hotspot-urile pot acoperi o suprafață variabilă, în funcție de mediul înconjurător. Pot acoperi suprafața unei singure camere dacă aceasta are pereții opaci pentru undele elctromagnetice sau pot ajunge până la câțiva kilometri pătrați. Wi-Fi poate asigura şi conexiuni în mod peer-to-peer (rețele fără fir ad-hoc) ceea ce conferă echipamentelor posibilitatea coenxiunii directe între ele. De-a lungul timpului tehnolgia Wi-Fi a evoluat foarte mult, ajungând în prezent să poată oferi un gateway securizat pentru rețelele de calculatoare, firewall, server DHCP, sisteme de protecție şi multe alte funcții. (***http://en.wikipedia.org/wiki/Wi-fi***)

2.2. ECHIPAMENTE STANDARD

2.2.1.ACCES POINT

Aceste echipamente permit conectarea unuia sau mai multor dispozitive cu funcționalități wireless să fie conectate la o rețea locala adiacentă cu fir.

Un acces point este un echipament asemănător cu un hub având funcția de a realiza schimbul de date dintre dispozitivele wireless conectate la access point şi rețeaua cu fir la care acesta este conectat. Astfel se asigură posibilitatea comunicării între echipamentele fără fir şi echipamentele cu fir conectate la rețeaua locală.Acest tip de echipament s-a bucurat de o popularitate foarte mare la începutul anilor 2000 fiind prima soluție ce putea oferi mobilitate şi un acces simplu şi uşor, fără fir, utilizatorilor de calculatoare din întreaga lume.

Cu toate acestea, odată cu progresul tehnologic şi tendința prezentului de a adopta soluții cât mai mobile, access point-urile s-au dovedit a fi limitate. Suportă maxim 30 de conexiuni şi acoperă o arie cu o rază de circa 100m, aceasta putând fi totuşi extinsă folosind repetoare si reflectoare care pot duce semnalul pana la câțiva kilometri.(http://en.wikipedia.org/wiki/Wireless_access_point)

Apropae toate access-point-urile dispun de o interfață TCP/IP putându-se face astfel configurări de bază cum ar fi setarea IP-ului, gateway sau netmask.In funcție de nivelul de complexitate hardware si software se pot face şi alte configurări la nivel de bază.

Depinzând de piața țintă pentru care au fost construite, unele acces point-uri pot oferi si server DHCP sau NAT (network address translation).

(***802.11® Wireless Networks: The Definitive Guide, published by O`REILLY, 2002 by Matthew Gast, cap. 14***)

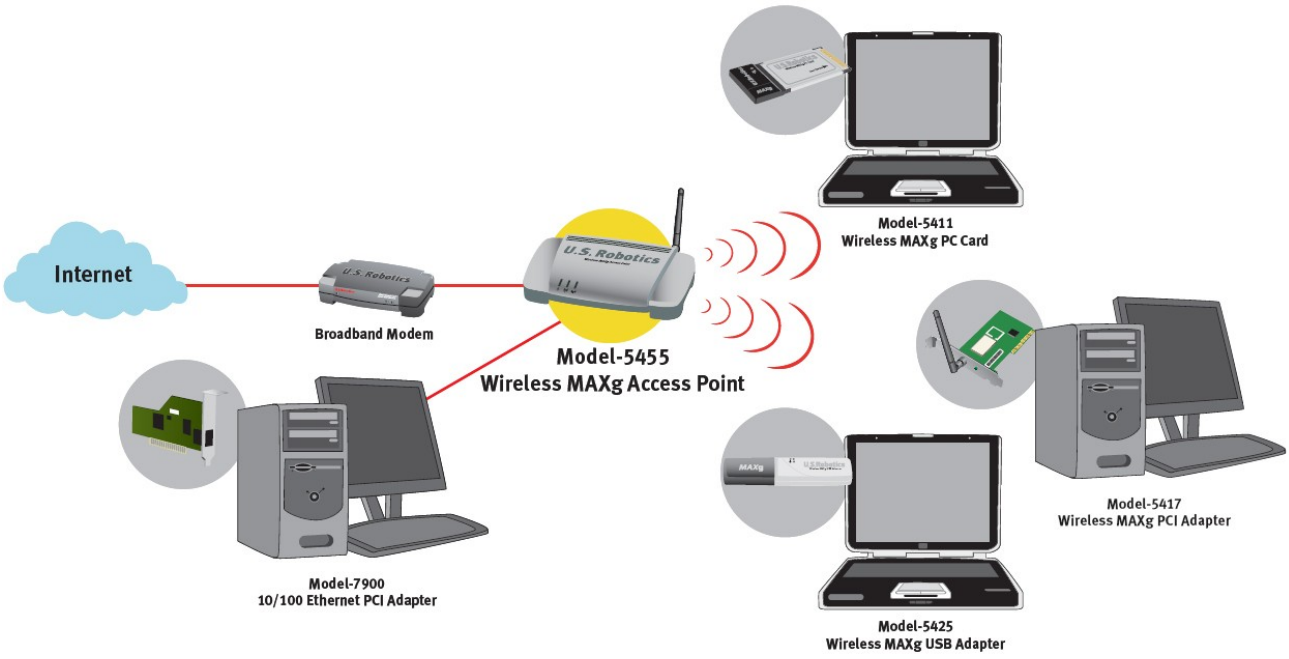


Fig. 2: Diagrama de conexiune la internet via Access Point
(http://www.usr.com/images/products/5455/5455-diagram.jpg)

2.2.2.ADAPTOR WIRELESS

Adaptoarele wireless permit echipamentelor ce nu au fost concepute cu posibilitatea de conectare la o rețea wireless să poată fi conectate la un access point sau router wireless în raza căruia se află. Aceste adaptoare se pot coencta al dispozitive prin porturi de coenctare interiaore cum ar fi PCI, miniPCI sau exterioare, USB.Majoritatea laptop-urilor actuale sunt echipate cu adaptoare interne.

2.2.3.ROUTER WIRELESS

Routerele wireless înglobează intr-un singur echipament un access point, un switch ethernet si un firmware intern pentru aplicații de tip router ce oferă servicii precum routare IP, NAT şi DNS, printr-o interfață WAN. Un router wireless permite conectarea echipamentelor cu fir sau fără fir să se conecteze la o rețea metropolitană prin intermediul unui modem prin cablu sau DSL. Toate cele trei echipamente înglobate de către router pot fi configurate printr-o singură aplicație. Această aplicație este de obicei un server web integrat sau în unele cazuri, Apple`s AirPort, paote fi o aplicație ce rulează pe un calcualtor de tip desktop.

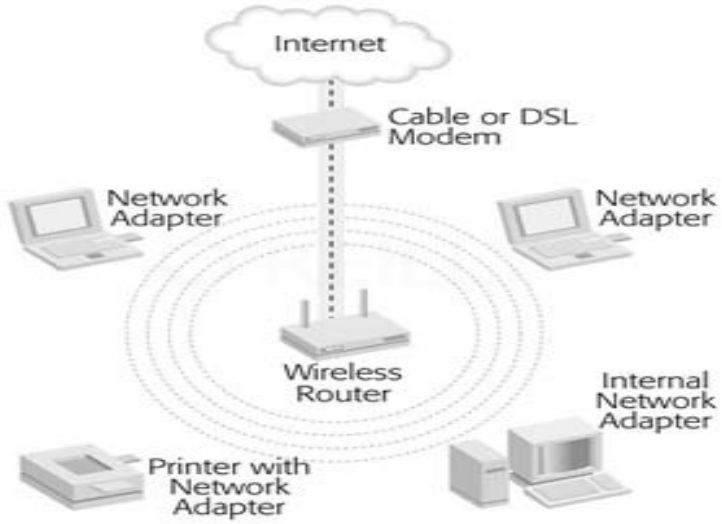


Fig. 3: Diagrama de conexiune la Internet via Router wireless
(http://www.oreilly.com/catalog/homenettmm/figs/I_1_tt12.png)

2.2.4.NETWORK BRIDGE

Network bridge-ul wireless, asemnea Access Point-ului conectează o rețea cu fir la o rețea fără fir dar spre deosebire de AP care conectează cele două rețele la nivel de date, network bridge-ul poate aisgura şi legătura dintre două rețele cu fir aflate la distanță.

Majoritatea access-point-urilor 802.11 aflate pe piață oferă posibilitatea configurării unui network bridge iar pentru cele care nu suportă network bridge, problema se rezolvă printr-un upgrade de firmware. ***(802.11® Wireless Networks: The Definitive Guide, published by O`REILLY, 2002 by Matthew Gast, cap. 2.2.2)***

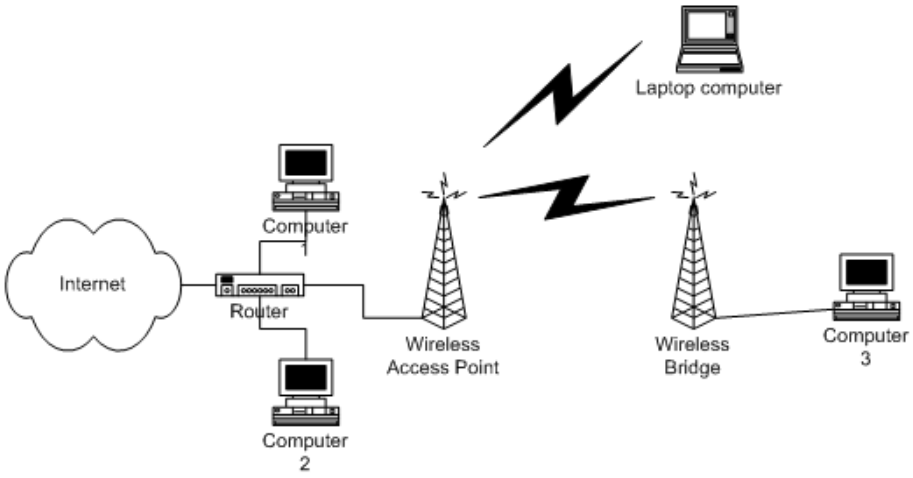


Fig. 4: Diagrama de conexiune prin Network Bridge
(http://ask-leo.com/images/wireless-remotelaptop.png)

Pe lângă toate aceste echipamente descrise mai sus, există şi o serie dispoztive dedicate extinderii razei de acţiune a reţelelor wireless. Aceste repetoare permit semnalului să acopere o arie mai mare cu precizarea ca toate echipamentele care vor fi conectate la reţeaua Wi-Fi prin intermediul repetoarelor de semnal vor suferi latenţe directe proportionale cu numărul de hopuri. ***(http://en.wikipedia.org/wiki/Wi-fi)***

2.2.5.ANTENE ŞI CONECTORI

Majoritatea echipamentelor tehnologiei Wi-Fi aflate în comerţ, indiferent de compelxitatea lor, folosesc conectori de anten de tipul RP-SMA (coenctori RF coaxiali) sau RP-TNC(versiune a conectorilor BNC dedicată deomeniului microundelor). Adaptoarele wireless PCI folosesc de obicei tot coenctori SMA. Majoritatea plăcilor sau echipamentelor de recepţie wireless prin USB dispun de o antenă internă, proiectată direct pe circuitul imprimat. Există şi câteva dispozitive USB care dispun de conector SMA. ***(http://en.wikipedia.org/wiki/Wi-fi)***

Fig. 5: Conector RP-SMA

Fig. 6: Conector RP-TNC

(***http://elara.ie/elara/graphics/I251210.jpg***)

2.3. STANDARDELE IEEE 802.11

IEEE 802.11 reprezintă un set de standarde dedicate cumunicațiilor de tip wireless între calculatoare. Acest set de standarde a fost dezvoltat de comitetul de standarde **IEEE LAN/MAN (IEEE 802)** şi a fost proiectat să funcționeze pe orice bandă publica de frecevență cuprinsă între 2.5GHz si 5GHz.

Cu toate că în prezent termenii "802.11" si "Wi-Fi" reprezintă acelaşi lucru, în trecut Wi-Fi Alliance a folosit termenul "Wi-Fi" pentru un set de standarde diferite față de cele actuale putând astfel certifica produsele înainte de defintivarea amendamentelor IEEE 802.11.

Familia 802.11 include tehnici de modulație ce au la bază acelaşi protocol, cele mai populare standarde din această familie fiind **802.11b** şi **802.11g**. Aceste două standarde reprezintă amendamente la cel original, 802.11a fiind acceptate şi recunoscute în întreaga lume.

La început, rețelele ce aveau la bază cele două standarde, **802.11b** şi **802.11g**, prezentau un grad de securitate ingrijorător de scăzut în special pentru instituțiile guvernamentale.

Astfel a apărut standardul **802.11i** menit să îmbunătățească securitatea datelor.

802.11n este ultimul alăturat familiei 802.11,este conceput pe baza unor tehnici de modulație încă foarte noi şi care încă mai sunt in faza de testare cu toate că deja au fost realizate şi comercializate în serii limitate produse construite conform primelor rezultate ale acestei noi tehnici de modulație.

Celelate standarde ale familiei **802.11, c-f, h şi j** nu reprezintă decât nişte amendamente la standardele originale cu rolul de a aduce, unele modificări sau corecții pe lângă specificațiile clasice ale acestora.

Standardele 802.11b şi 802.11g folosesc Banda ISM (Indsutrial, Sceintific and Medical Band) de 2.4GHz dar datorită acestei alegeri, în unele cazuri s-au înregistrat interferențe cu telefoanele fără fir sau cu cuptoarele cu microunde. Cu toate ca şi dispozitivele **Bluetooth** operează în aceeaşi bandă de frecvență, acestea nu interferează cu echipamentele 802.11b/g deoarece folosesc tehnici de propagare diferite. In timp ce 802.11b/g folosesc DSSS(Direct Sequence Spread Spectrum), dispozitivele **Bluetooth** folosesc metoda FHSS (Frequency Hopping Spread Spectrum).

2.3.1.802.11a

802.11a a fost primul standrad dedicat comunicațiilor wireless între calculatoare. Foloseşte banda U-NII de 5GHz, bandă ce oferă 8 canale disponibile, față de cele 3 oferite de banda ISM. A fost lansat în octombrie 1999 şi are o rată de transfer nominală de 23Mbit/s şi o rată de transfer maximă de 54Mbit/s.

Folosind o purtătoare de înaltă frecvență, distanța maximă de emisie este mică în comparație cu distanța maximă de emisie în cazul standardelor b/g, aceasta fiind de apoximativ 120m în mediu deschis. In cazul în care sunt prezente şi alte obstacole, cum ar fi pereții unei camere, raza de acțiune a echipamentelor bazate pe acest standard este drastic diminuată, ajungând la maxim 35m.

Această tehnologie foloseşte patru tipuri de modulație OFDM, în funcție de rata de transfer asigurată: 6-9Mbit/s-BPSK, 12-18Mbit/s-QPSK, 24-36Mbit/s-16QAM şi 48-54Mbit/s – 64QAM.

2.3.2.802.11b

802.11b a fost lansat în octombrie 1999 ca un amendament la predecesorului său, 802.11a. Funcționează pe o frecvență centrală de 2.4GHz având rata de transfer nominală de 4.5Mbit/s iar rata de transfer maximă de 11Mbit/s. Cu toate că nu este la fel de performantă ca tehnolgia ei predecesoare, tehnologia 802.11b a fost prima tehnologie standard recunsocută şi acceptată pentru rețelele de calculatoare de tip wireless.

Dezavantajul acestei tehnologii a fost acela că echipamentele dezvoltate pe baza ei au suferit interferențe cu celelate dispozitive ce funcționează în aceeaşi banda de frecvență.

Foloseşte ca tehnică de modulare metoda DSSS şi prezintă o rază maximă de emisie în mediu deschis este de cca. 140m iar în mediu închis ajunge la maxim 38m.

2.3.3.802.11g

In iunie 2003 a apărut al treilea standard de modulare a transmisiilor wireles de date.
La fel ca şi 802.11b, această tehnologie a fost dezvoltată tot pentru banda de 2.4Ghz dar spre deosebire de predecesoarea ei, rata de transfer a fost mult îmbunătățită, având o rată de transfer nominală de 19Mbit/s iar cea maximă ajungând până la 54Mbit/s.

Cu toate ca a fost acceptată şi recunoscută ca fiind tehnologia standard a momentului în ianuarie 2003, 802.11g a oferit şi compatibilitate hardware cu tehnologia precedentă 802.11b. Astfel, echipamentele mai vechi, concepute pe baza tehnologiei 802.11b puteau totuşi să se conecteze la noile Access Point-urile sau alte echipamente ce emiteau folosind standardul 802.11g.

Din vara anului 2003 toate produsele de tip wireless dual-band aud evenit dual-band/tri-mode înglobând toate cele trei standarde, a,b şi g într-un singur adaptor sau acces point.Asemenea produselor conforme standardelor 802.11b, şi echipamentele 802.11g suferă interferențe cu celelate dispozitive ce funcționează în aceeaşi bandă de frecvență.

802.11g foloseşte ca tehnică de modulare metoda OFDM şi prezintă o rază maximă de emisie în mediu deschis este de cca. 140m iar în mediu închis ajunge la maxim 38m.

In 2003 a fost creat documentul oficial ce atestă existența comună a celor opt standarde de comunicație wireless, **802.11a,b,d,e,g,h,i,j** sub acronimul **802.11REVma.** Pe 8 martie 2007, **802.11REVma** a fost redenumit în **IEEE 802.11-2007** acesta fiind singurul document oficial ce conține toate datele şi caracteristicile standardelor analizate.

2.3.4.802.11n

802.11n reprezintă ultimul amendament propus pentru a îmbunătăți performanțele şi caractersiticile tehnologiilor ce folosesc standardele anterioare. Acest standard este încă în stadiul de dezvoltare/testare, una dintre cele mai importante funcționalități care se doresc a fi introduse odată cu acesta fiind MIMO (Multiple Input Multiple Output).

Lansarea lui oficială este estimată undeva în 2009, va funcționa în ambele bande de frecvență, atât în 2.4GHz cât şi în banda de 5GHz şi va avea o rată de transfer nominală de 74Mbit/s iar cea maximă de 248Mbit/s. Raza de acțiune în mediu deschis va fi de circa 250m iar în mediu închis de maxim 70m.

(***® Wireless Networks: The Definitive Guide, published by O`REILLY, 2002 by Matthew Gast, cap.3, cap.15, http://standards.ieee.org/announcements/80211gfinal.html , http://en.wikipedia.org/wiki/802.11***)

2.4.SECURITATE ŞI METODE DE CRIPTARE

La începuturile tehnologiei Wi-Fi/802.11 s-a dorit oferirea accesului liber la acces point-uri pentru oricine care se afla în raza acestora în ideea popularizării rețelelor wireless.

Odată cu popularizarea rețelelor wireless şi datorită creşterii numărului de utilizatori de laptopuri rețelele aud evenit supraîncărcate şi astfel s-a luat decizia dezvoltării unor metode de a acorda accesul la acces point numai unei liste de utilizatori, "white-list". In acest sens, s-a dezvoltat un sistem de securitate şi criptare a rețelelor astfel încât utilizatorii se puteau conecta numai pe baza unei adrese MAC valide şi conform anumitor standarde de criptare.

Aceste metode au fost destul de ineficiente, criptanalistului fiindu-i relativ uşor să afle SSID-ul (Service Set IDentifier) şi adresa MAC a utilizatorilor deja conectați. (***http://en.wikipedia.org/wiki/Wi-fi***)

2.4.1.WIRED EQUIVALENT PRIVACY (WEP)

WEP este un algoritm de securitate dedicat rețelelor wireless IEEE 802.11/Wi-Fi. Datorită faptului că rețelele wireless transmit datele prin intermediul undelor electromagnetice, acestea sunt expuse mult mai mult atacurilor informatice în comparație cu rețelele clasice, prin cablu.

WEP a fost introdus ca standard în 1999 şi asigură atât confidențialitatea datelor, cu ajutorul cifrului RC4 cât şi verificarea integralității datelor transmise cu ajutorul unui cod CRC-32. Acest standard este din ce in ce mai rar folosit din 2004 până in prezent dar totuşi va fi prezentat şi va rămâne ca referință pentru celelate mecanisme de criptare apărute ulterior.

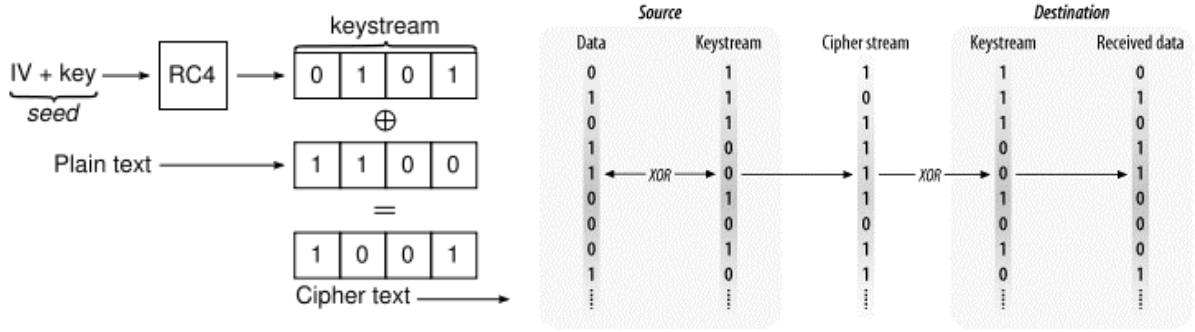


Fig. 7: Algoritmul de criptare WEP

(http://upload.wikimedia.org/wikipedia/commons/thumb/4/44/Wep-crypt-alt.svg/305px-Wep-crypt-alt.svg.png; 802.11 ® Wireless Networks: The Definitive Guide, published by O`REILLY, 2002 by Matthew Gast, pag. 97)

Metoda standard de criptare WEP pe 64 de biți foloseşte o cheie pe 40 de biți concatenată cu un vector de inițializare de 24 de biți (IV-intialization vector) petru a forma cheia de trafic RC4. Odată cu lansarea WEP-64, Guvernul SUA a impus restricții în tehnologia criptografiei limitând lungimea maximă a cheilor publice la 64 de biți. După anularea acestor directive s-a putut dezvolta şi un algortim WEP extins, pe 128 de biți cu o cheie publică pe 104 biți.

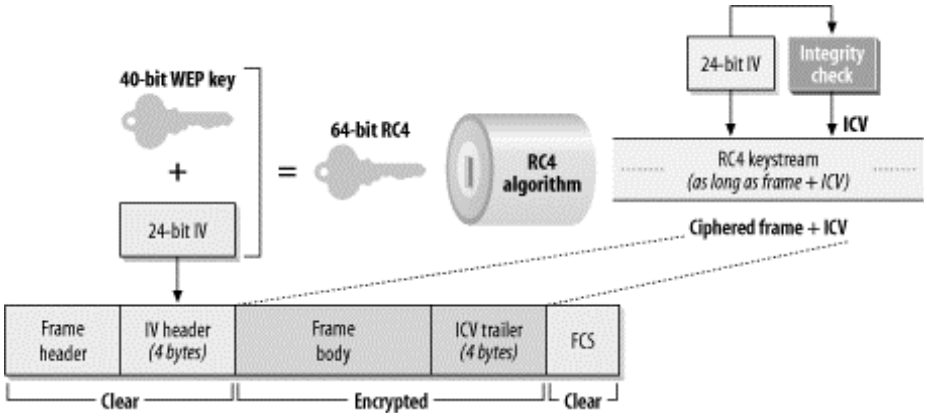


Fig. 8: Mecansimul de criptare WEP-64

(***802.11 ® Wireless Networks: The Definitive Guide, published by O`REILLY, 2002 by Matthew Gast, pag. 99***)

Cheia algoritmului de criptare WEP-128 este întotdeauna introdusă de utilizator ca un şir de 26 de caractere Hexazecimale. Fiecare caracter reprezintă 4 biți ai cheii de unde rezultă lungimea maximă a cheii de 104 biți. Adăugând cei 24 de biți ai vectorului de inițializare se obține aşa-zisul cifru WEP-128.

Este disponibil şi un algoritm de criptare WEP pe 256 de biți care dispune de o cheie pe 232 de biți la care se adaugă vectorul de inițializare pe 24 de biți. In acest caz cheia este introdusă ca 58 de caractere Hexazecimale.

Lungimea cheii nu este singura limitare majoră a securității WEP. Spargerea unui cifru lung necesită interceptarea foarte multor pachete. Acest lucru era foarte greu posibil realizat cu metodele mai vechi folosite în tehnologia transmisiunii informației dar, odată cu progresul tehnologic, au apărut diverse metode active de simulare a traficului necesar pentru spargerea chiar şi a unui cifru pe 256 de biți, astfel metodele de criptare WEP fiind depăşite.

Pe lângă cele amintite mai sus, WEP mai prezintă unele puncte slabe, cum ar fi coliziunea pachetelor cu vectorul de inițializare. Probabilitatea de a se întâmpla acest lucru este direct proporțională cu lungimea cheii.

2.4.1.1.Metode de autentificare

WEP poate folosi două metode de autentificare, **OSA (Open System Authentification)** şi **SKA (Shared Key Authentification).**

In cazul autentificării **OSA**, utilizatorul nu trebuie să se identifice cu user şi parolă față de access point, astfel orice utilizator, indiferent de cheia WEP asociata se poate autentifica pe Acces Point după care urmând faza de asociere cu acesta. După autentificare şi asociere, cifrul WEP poate fi utilizat pentru criptarea cadrelor de date, din acest moment, utilizatorul trebuie să dețină cheia pentru a se putea conecta.

In cazul autentificării **SKA,** WEP este utilizat pentru autentificare după care urmează patru etape de negociere între client şi Acces Point:

- Stația-client trimite o cerere de autentificare către Acces Point;

- Acces Point-ul trimite înapoi un mesaj text pentru a verifica dacă clientul deține cheia WEP corespunzătoare;
- Clientul primeşte mesajul şi va trebui să-l cripteze cu cheia WEP corespunzătoare după care îl va trimite înapoi Acces Point-ului.

- Acces Point-ul decriptează mesajul primit de la clientşi îl compară cu textul inițial pe care el i l-a trimis clientului. In funcție de rezultat, Acces Point-ul va trimite inapoi un mesaj de acordare sau neacrodare a accesului la rețea al stației-client.

După autentificare şi asociere, cifrul WEP poate fi folosit pentru criptarea cadrelor de date.

Cifrul WEP reprezintă o metodă de criptare ce asigură un grad de protecție de o complexitate medie fiind foarte uşor de descifrat cu unele tool-uri software cum ar fi AirSnort (necesită accesul la 5-10 milioane de pachete criptate pentru a descifra cheia WEP în mai puțin de o secundă) sau Air Crack (are o rată de succes de 50% la 40.000 de pachete văzute).

(***http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy; 802.11 ® Wireless Networks: The Definitive Guide, published by O`REILLY, 2002 by Matthew Gast, cap 5; Metode Criptografice – note de curs prof.dr. ing. Adriana Vlad-UPB***)

2.4.2.Wi-Fi Protected Access (WPA)

Wi-Fi Protected Access (**WPA şi WPA2-IEEE 802.11i**) reprezintă un ansamblu de sisteme dedicat asigurării unei mai bune securități a rețelelor wireless.

WPA a fost creat ca răspuns la problemele serioase întâmpinate de cheia WEP şi implementează majoritatea standardelor 802.11i. Această metodă a fost concepută să funcționeze chiar şi în cazul plăcilor de interfață ale rețelelor construite înainte de apariția metodelor de criptare WPA printr-un simplu upgrade de firmware. **WPA2** implementează ultima generație de standarde dar nu funcționează pe unele sitemele mai invechite.

Există două tipuri de metode WPA, un set dedicat uzului personal şi un altul dedicat companiilor. Metodele WPA dedicate companiilor necesită folosirea unui server de autentificare prin standardul IEEE 802.1X ce distribuie o cheie diferită fiecărui client.

Setul de metode WPA pentru uz personal foloseşte o cheie prestabilită, PSK(Pre-Shared Key), fiecare client primind aceeaşi parolă.

Modul PSK a fost proiectat pentru rețelele care nu necesită un grad de securitate comparabil cu cel oferit de serverele de autentificare 802.1X. Fiecare utilizator va trebui sa introducă o simplă parolă pentru a avea acces la rețeaua wireless. Această parolă poate fi în format ASCII sau Hexazecimal.

Securitatea poate fi îmbunătățită prin adăugarea unei funcții de derivare a cheii, PBKDF2. De obicei, parolele cele mai întâlnite fiind foarte uşor de spart, se recomandă parole de cel puțin 20 de caractere aleatoare iar cele iar pentru o securitate foarte bună, parole de cel puțin 33 de caractere.
(***http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access, http://en.wikipedia.org/wiki/Pre-shared_key***)

2.5.CONCLUZII

2.5.1.AVANTAJE

Tehnologia **WI-FI** permite realizarea de rețele locale foarte comode, la un preț mai mic decât cel al rețelelor locale prin cablu.
Avantajul major al acestor rețele îl reprezintă lipsa cablurilor, astfel, rețeaua putând fi extinsă chiar şi acolo unde în mod normal cablurile nu pot ajunge.
In prezent rețelele locale de tip Wi-Fi sunt într-o continuă expansiune, acest lucru datorându-se în special noilor chipset-uri Wi-Fi dedicate calculatoarelor portabile, la un preț ce se află într-o continuă scădere.
Un alt avantaj al acestei tehnologii îl reprezintă interoperabilitatea dintre diferitele branduri de echipamente wireless dedicate Wi-Fi aflate pe piață. Toate echipamentele dedicate acestei tehnologii necesită certificarea Wi-Fi Alliance, astfel, spre deosebire de echipamentele din telefonia mobilă, echipamentele Wi-Fi vor funcționa şi vor putea opera între ele, oriunde în lume, indiferent de ce firmă au fost produse.
In prezent, rețelele de tip Wi-Fi sunt foarte răspândite, de la hotspot-uri publice până la rețele wireless de uz personal sau organizațional.
Standardul de securitate WPA este unul foarte sigur în prezent, în special dacă parolele utilizate sunt foarte lungi iar extensia sa, WPA2 încă nu a prezentat nicio slăbiciune.
S-au dezvoltat şi o serie de protocoale dedicate îmbunătățirii serviciilor oferite prin intermediul acestei tehnologii wireless cum ar fi aplicații pentru eliminarea latențelor nedorite în cazul transmisiilor video sau audio sau mecanisme pentru controlul consumului de energie electrică.

2.5.2.DEZAVANTAJE

Un prim dezavantaj al acestei tehnologii îl reprezintă inconsistența canalelor de transmisiune utilizate pe suprafața Globului.Transmisiunile Wi-Fi ocupă 5 canale în banda de frecvență de 2.4 GHz dar de fapt doar o parte din acestea nu se suprapun, trei in SUA, canalele 1, 6, 11 şi patru în Europa, canalele 1, 5, 9, 13.
Un alt aspect ingrijorător al acestei tehnologii îl reprezintă puterea consumată de echipamentele aferente, durata de viață a bateriilor fiind destul de scăzută.
Rețelele wireless necriptate nu oferă securitatea datelor cu excepția celor care sunt proiectate să folosească metode de securitate specializate, cum ar fi VPN sau HTTPSecure.
In cazul rețelelor necriptate şi fără măsuri de securizare a datelor, toate informațiile transmise sau primite pot fi citite sau copiate.

Un alt dezvanataj al acestor rețele îl reprezintă raza de acțiune limitată. Odată cu viitorul standard 802.11n, acest dezavantaj va fi eradicat, raza de acțiune extinzându-se foarte mult atât în mediu inchis cât şi în mediu deschis.

(***http://en.wikipedia.org/wiki/Wi-fi***; ***802.11 ® Wireless Networks: The Definitive Guide, published by O`REILLY, 2002 by Matthew Gast***)

2.6.Referințe Bibliografice

- *802.11 ® Wireless Networks: The Definitive Guide,* published by O`REILLY, 2002 by Matthew Gast
- www.wikipedia.org
- www.ieee.org
- www.oreilly.com
- Note de curs Metode Criptografice – prof. dr. ing. Adriana Vlad – U.P.B.
- www.wi-fi.org

3. TEHNOLOGIA ISDN

3.1.INTRODUCERE

Rețea cu servicii digitale integrate (ISDN) este un model specific rețelei telefonice cu comutație de circuite, proiectat să permită transmisia de voce şi de date printr-un banal cablu de cupru, rezultând o îmbunatățire dramatică a calității şi a vitezei, față de cele oferite în sistemele analogice. Într-un mod şi mai larg, ISDN este un set de protocoale folosite pentru stabilirea şi întreruprea conexiunilor telefonice, cât şi pentru funcționalități complexe pentru utilizatorul serviciului telefonic. Originea termenului vine din limba germană, "Integriertes Sprach- und Datennetz" ("rețea integrată de voce şi date").

Într-o videoconferință, ISDN se ocupă simultan de voce, de video şi de transmisia text între un terminal individual şi grupul de sisteme aflat în conferință.

Sunt doua puncte de vedere in lumea ISDN. Cel mai comun punct de vedere este cel al utilizatorului final, care vrea o conexiune digitala in reteaua telefonica/date de acasa, ale carei performante ar fi mai bune decat o conexiune analigica prin modem conventional. Conexiunea tipica pt end-user la internet este din acest punct de vedere, si discutia asupra performantelor difetelor modemuri ISDN, tarife, sunt dun aceasta perspectiva.

Al doilea punct de vedere: cel al industriei de telefonie, unde ISDN este o tehnologie de core. Cele mai comune specificatii electrice pentru semnalele electrice in fire este T1 sau E1. Pe o linie normala T1, semnalizarea este facuta cu bitii A&B pentru a indica „on-hook" sau „off-hook" si tonuri MF si DTMF pentru a coda numarul destinatie. ISDN este mult mai bun deoarece mesajele pot fi trimise mult mai repede decat incercand sa codzi numerele in secvente de ton(pana la 100ms pe digit).

Este de asemenea folosit ca o tehnologie rețea-inteligentă intenționată sa adauge noi servicii pentru reteaua de telefonie publica (PSTN) acordand userilor acces direct serviciilor digitale circuit-switched end-to-end.

ISDN BRI (Basic Rate Interface) nu a reusit sa castige popularitatea ca o tehnologie de acces telefonica in america de nord si ramane un produs de nisa. Cu toate acestea, majoritatea modemurilor non-VoIP PBX folosesc linii T1 PRI (Primary Rate Interface) pentru a comunica cu un switch central Telco de clasa 5, inlocuind mai vechi linii bidirectionale Direct Inward Dialing (DID). PRI este capabil Automatic Number Identification (ANI) in ambele directii ca numarul de telefon a unei extensii, decat un numar principal de telefon al unei companii, poate fi trimis. Este inca foarte folosit in studiouri de inregistrare, cand un actor de voce este intrun studio, dar regizorul si producatorul intrun studio in alta locatie. ISDN este folosit pentru garantia sa de „real time", si nu prin internet al serviciului, si calitatea audio superioara comparata cu POTS.

(http://en.wikipedia.org/wiki/ISDN; Cartea: CCNA Exam Prep 2 Exam 640-801)

3.2.CONFIGURAȚII

În ISDN există două tipuri de canale: B (de la "Bearer") şi D (de la "Delta"). Canalele B sunt folosite pentru transmisiile de date (pot include şi voce). Canalele D sunt folosite pentru semnalizare şi control (dar nu este exclus să fie folosite şi pentru date).

Există două tipuri de interfețe ISDN:

- Basic rate interface (BRI) — numit şi Basic rate access (BRA) — constă în două canale de tip B, fiecare cu o bandă de 64 kbit/s, şi un canal D cu o bandă de 16 kbit/s. Împreună aceste trei canale pot fi descrise de notația 2B+D.

- Primary rate interface (PRI) — numită şi Primary rate access (PRA) — au un număr mai mare de canale de tip B precum şi de un canal D cu o lățime a benzii de 64 kbit/s. Numărul de canale B dintr-un PRI variază de la țară la țară: în America de Nord şi Japonia este de 23B+1D, cu o bandă însumată de 1.544 Mbit/s (T1); în Europa şi Australia numărul de canale este de 30B+1D, având o bandă totală de 2.048 Mbit/s (E1).

Folosind tehnica codării cu marcarea inversărilor, datele apelului telefonic se transmit pe canale de tip (B), iar canalele de tip (D) sunt folosite pentru stabilirea apelului şi administrarea legăturii create. Dupa ce apelul a fost stabilit, între cele două parți ale apelului există o simplă legătură sincronă bidirecțională de 64 kbit/s care este menținută până la terminarea apelului. Pot coexista un număr maxim de apeluri câte canale de date sunt. Canalele Bearer pot fi şi ele multiplexate într-un canal unic de capacitate mare printr-un proces numit "bonding" (grupare).

Canalul D poate să fie de asemenea folosit pentru a trasmite şi recepționa pachete X.25 precum şi pentru conexiuni la rețeaua cu comutare de pachete X.25, după cum este specificat în standardul X.31. În lumea reală, X.31 a fost implementat ca serviciu comercial numai în Franța şi Japonia. (***http://en.wikipedia.org/wiki/ISDN)***

3.3.PUNCTE DE REFERINȚĂ

Un set de puncte de referință sunt definite în standardul ISDN pentru a descrie anumite puncte dintre telco şi echipamentul terminal ISDN al utilizatorului.

- R - defineşte punctul dintre un echipament ne-ISDN şi terminal adaptator (TA) care are rolul de translator dinspre şi înspre un astfel de dispozitiv
- S - defineşte punctul dintre un echipament ISDN (sau TA) şi o terminație de rețea de tip 2 (NT-2)
- T - defineşte punctul dintre un echipament NT-2 şi unul NT-1
- U - defineşte punctul dintre un echipament NT-1 şi switch-ul telco.

Majoritatea dispozitivelor NT-1 înglobează şi funcții NT-2, astfel punctele de referință S şi T sunt în general înglobate într-un singur punct de referință numit S/T. În America de nord, dispozitivul NT-1 este considerat echipament al clientului final şi întreținerea sa îi revine acestuia. Prin urmare, serviciu oferit clientului este interfața U. În alte locuri, dispozitivul NT-1 este întreținut de către operatorul telefonic, şi serviciul oferit este interfața S/T.

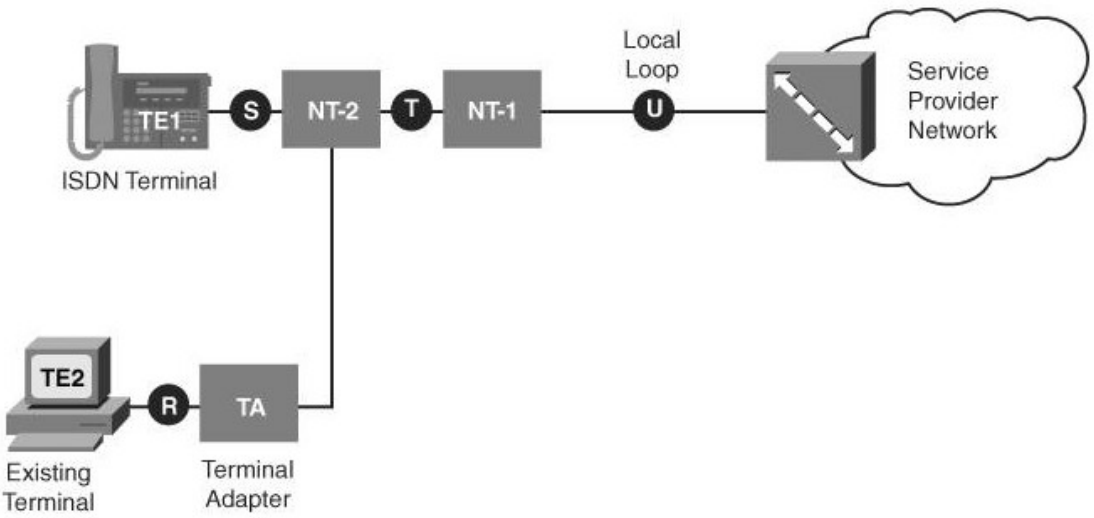


Fig. 9: Puncte de referință intr-o rețea ISDN

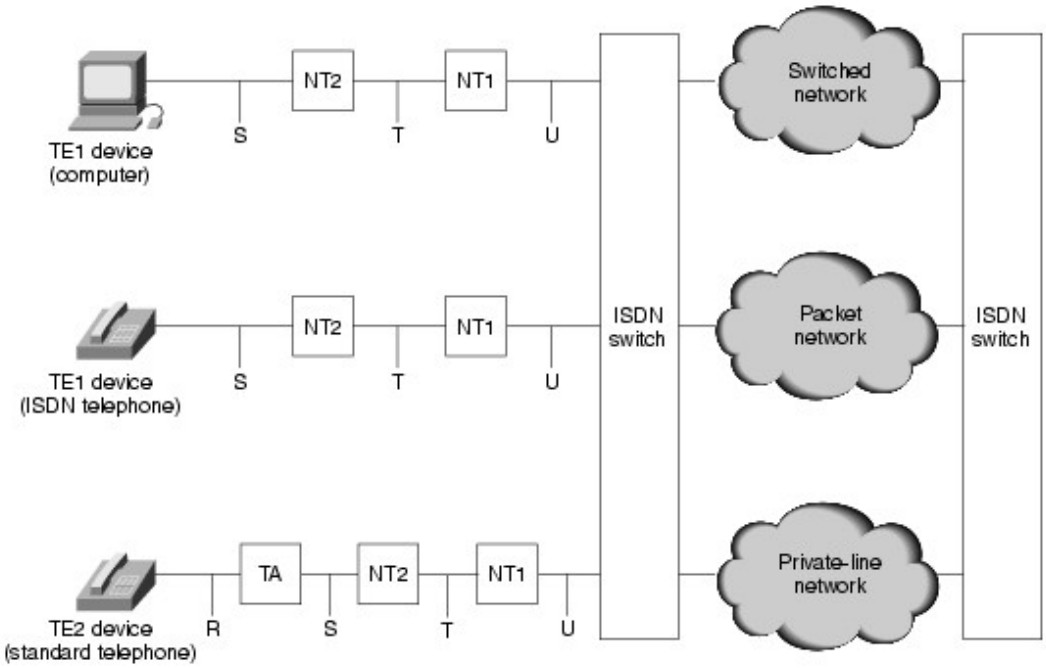


Figura 10: Exemplu de configurație ISDN ce ilustrează relația dintre Device-uri şi Puncte de referință

(http://en.wikipedia.org/wiki/ISDN; Cartea: CCNA Exam Prep 2 Exam 640-801)

3.4.Tipuri de Comunicație suportate

Printre tipurile de date care pot fi transmise prin aceste canale de 64 kbit/s sunt şi apelurile telefonice cu modulație în puls (PCM), asigurând astfel acces la serviciile tradiționale de voce PSTN. Aceste informații pot fi schimbate între rețea şi utilizator în momentul stabilirii apelului telefonic. În America de nord, ISDN este folosit în acest moment ca o alternativă la conexiunile analogice, utilizarea cea mai fecventa fiind cea de acces la internet. Totuşi, câteva servicii care au fost proiectate să lucreze pe ISDN sunt acum transportate prin intermediul Internetului. În Europa, şi mai ales în Germania, ISDN-ul a fost vândut cu succes ca un telefon cu capabilități extinse față de telefonul analog POTS (Plain Old Telephone Service), care nu are, sau are puține astel de capabilități. Între timp, capabilități care erau la început disponibile numai folosind un terminal ISDN (precum apel conferință, Call forwarding, Caller ID, etc.) sunt acum disponibile în mod curent şi pentru telefoanele analogice, elimiându-se astfel avantajele ISDN-ului.

Alt avantaj al telefonului ISDN este posibilitatea unor convorbiri simultane (un apel per canal B), util în cazul unor familii numeroase. Totuşi şi acest avantaj începe să dispară odată cu reducerea costurilor telefoniei mobile, făcând ISDN-ul o tehnologie neatractivă pentru utilizatorul casnic.

Pentru o conexiune de date, în cazul unei linii analogice este nevoie de un modem, iar în cazul unei conexiuni ISDN este necesar un adaptor terminal (TA).

(http://en.wikipedia.org/wiki/ISDN)

3.5.Specificații ISDN

Aceasta secțiune descrie specificatiile ISDN pentru Layer 1, Layer 2, and Layer 3.

3.5.1.Layer 1

ISDN nivelul fizic (Layer 1) formatele frame-urilor difera depinzând de ce frame este outbound (de la terminal la retea) sau inbound (de la retea la terminal). Ambele interfețe la nivelul fizic sunt in figura 3. Frame-urile sunt de lungime de 48 biti, din care 36 biti reprezintă data. Bitii unui frame ISDN la nivel fizic sunt folositi dupa cum urmează:

- **F**—Ofera sincronizare
- **L**—Ajusteaza valoare medie de bit
- **E—**Asigura rezolutia cand mai multe terminale pe o magistrala pasiva cer un canal
- **A—**Activeaza echipamentele
- **S—**Nu este folosit
- **B1**, **B2**, si **D**—Au grija de datele utilizatorului

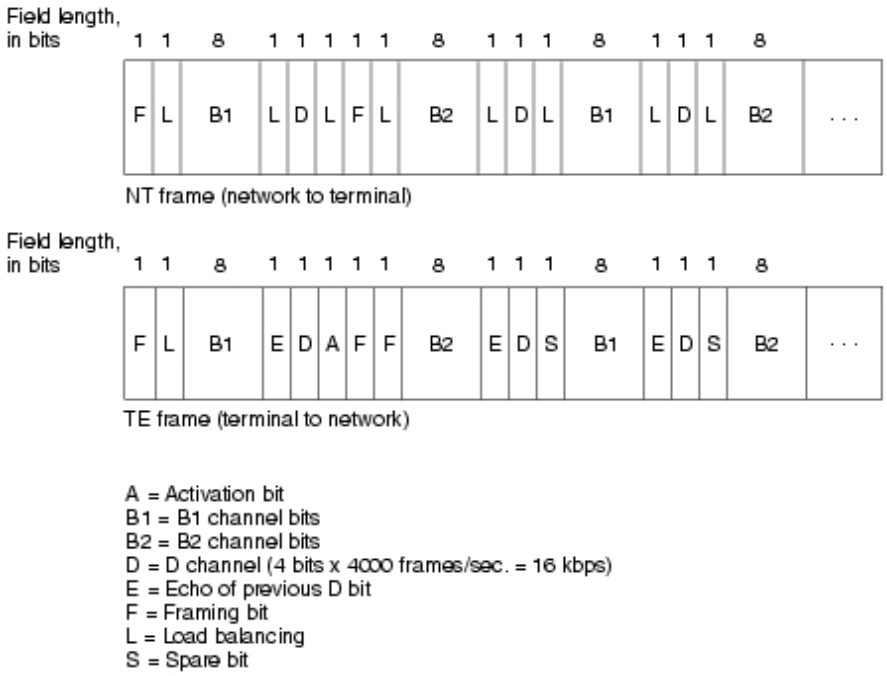


Figura 11: Frame ISDN Nivel Fizic difera in fucntie de directia lor

Mai multe echipamente ISDN pot fi fizic conectate la un circuit. In aceasta configurare, coliziuni pot rezulta daca doua terminale transmit simultan. De aceea ISDN are implementat metode de determinarea starii legaturii. Cand un NT primeste un bit D de la TE, el trimite inapoi bitul in urmatoarea pozitie a bitului E. TE se asteapta ca urmatorul bit E sa fie acelasi ca bitul D trimis
Terminalele nu pot transmite in canalul D decat daca intai detecteaza un numar specific de 1 (care indica “no signal”) corespunzator unei prioritati prestabilite. Daca TE detecteaza un bit in canalul E (echo) care este diferit de biti sai D, el opreste transmisia imediat. Aceasta tehnica simpla asicara ca numai un singur terminal poate transmite mesajul D la un moment dat.

Dupa o transmisie cu success a unui mesaj D, terminalul are prioritatea scazuta fiind nevoie sa detecteze un numar mai mare de 1 la rand inainte de a transmite. Terminalele nu pot sa-si mareasca prioritatea pana cand toate terminalele de pe aceeasi linie nu au avut oportunitatea de a trimite un mesaj D. Conexiunile telefonice au prioritate mai mare decat toate celelalte servicii, si informatia de semnalizare are o prioritate mai mare decat informatia de nonsemnalizare.

3.5.2.LAYER 2

Layer 2 al protocolului de semnalizare ISDN este Link Access Procedure, canalul D (LAPD). LAPD este similar cu High-Level Data Link Control (HDLC) şi Link Access Procedure, Balaced (LAPB). După cum indică şi acronimul LAPD, acest layer este folosit prin canalul D pentru a asigura că informația de control şi semnalizare curge şi este primită corect.

Formatul frame-ului LAPD (figura 4) este foarte asemnător cu cel al HDLC; ca şi HDLC, LAPD foloseste frame-uri de supervizare, informare, si nenumerotate. Protocolul LAPD este specificat in ITU-T Q.920 si ITU-T Q.921.

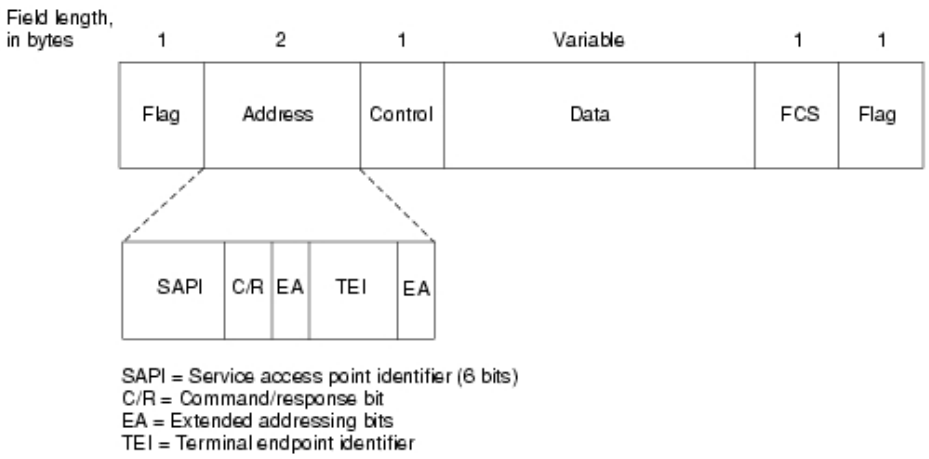


Figura 12: Frame Formatul LAPD este similar cu cel al HDLC si LAPB

Câmpurile Flag-ul şi de control LAPD sunt identice cu cele ale HDLC. Campul de adresă. LAPD poate fi de 1 sau 2 octeti lungime. Dacă bitul de adresă extinsă a primului octet este setat, atunci lungimea este de 1 octet, dacă nu este setat atunci adresa este de 2 octeti. Primul octet al câmpului adresă conține identificatorul de acces la service (SAPI), care identifică portalul la care servicii LAPD sunt furnizate Layer-ului 3. Bitul de C/R indică daca frame-ul conține o comanda sau un raspuns. Câmpul pentru Terminal Endpoint Identifier (TEI) identifică unul sau mai multe terminale. Un camp TEI plin de 1 indetifică un broadcast.

3.5.3.LAYER 3

Doua specificații de Layer 3 sunt folosite pentru semnalizarea ISDN: ITU-T (fost CCITT) I.450 (de asemenea cunoscut ca ITU-T Q.930) şi ITU-T I.451 (cunoscut şi ca ITU-T Q.931). Împreună, aceste protocoale suportă conexiuni user-user, circuit-switched, şi packet-swiched. O varietate de call--establishment, call-termination, informații, şi alte mesaje sunt specificate inclusiv SETUP, CONNECT, RELEASE, USER INFORMATION, CANCEL, STATUS şi DISCONECT. Aceste mesaje sunt functional similare cu cele furnizate de catre protocolul X.25.

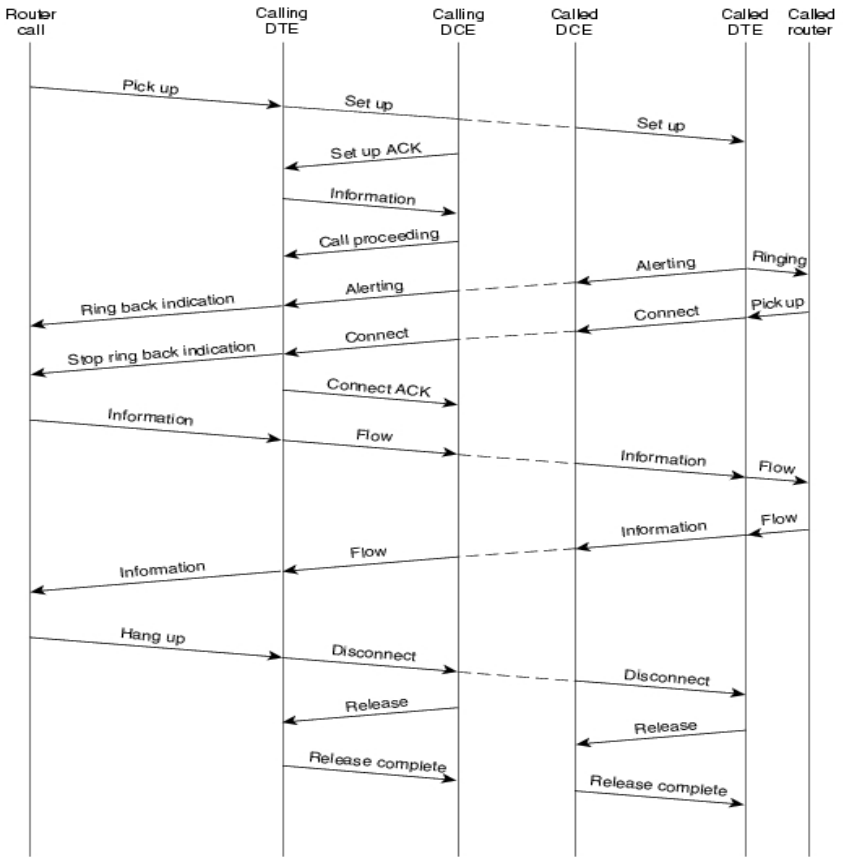


Figura 13: Un Apel Circuit-Switched ISDN se propagă prin diferite stagii până la destinație.

(http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/isdn.htm)

3.6. CONCLUZII

3.6.1. APLICATII

Standardizarea aplicatiilor este seoarata de standardele ISDN, dar aceste aplicatii vor fi importante pentru succesul pe viitor al ISDN-ului. In momentul de fata se fac cercetari pentru video-telefonie, voce low-res, sunet high-res.

3.6.2. LUMEA REALA

Pe masura ce ISDN este folosit, putini oameni isi inlocuiesc conexiunea telefonica clasica, cu una ISDN. Trend-ul pentru moment este de a promova intreaga retea ISDN intr-un singur pachet, cu echipamentele NT1, TA si TE1. Un exemplu ar fi Pipeline 25, de la Ascend, care furnizeaza solutii ISDN pentru conexiuni ethernet, folosind IP. Are un NT1 integrat si are prize pentru telefon pentru telefoanele POTS clasic.

4. TEHNOLOGIA DSL

4.6. INTRODUCERE

DSL sau **xDSL** este o familie de tehnologii care asigură transmisii digitale prin intermediul cablurilor rețelei de telefonie fixă. DSL a fost inițial definit de la Digital Subscriber Loop, dar recent s-a adoptat Digital Subscriber Line ca un termen mai marketing-friendly pentru cea mai popular versiune a DSL, ADSL.

În mod normal, viteza de download a serviciilor DSL pentru consumatori variază de la 512kbps pana la 24000kbit/s, depinzând de tehnologia DSL, condițiile liniilor si nivel implementat. In mod normal, viteza de upload este mai mică decat viteza de download pentru Asymmetric Digital Subscriber Line (ADSL) si egală cu viteza de download pentru Symmetric Digital Subscriber Line (SDSL).

(http://en.wikipedia.org/wiki/Digital_subscriber_line)

4.7. VOCE ŞI DATE

Unele viariante ale conexiunilor DSL, cum ar fi ADSL şi very high speed DSL (VDSL), functionează in mod normal divizând frecvențele utilizate intr-o singură linie telefonică în două benzi primare. Datele ISP sunt purtate pe banda de inaltă frecventă (25kHz sau mai mare) unde vocea este purtată pe banda de frecvențe mici (4kHz sau mai jos). Utilizatorul de obicei instalează un filtru la fiecare telefon. Acestea filtrează frecvențele inalte de la telefon, in aşa fel incât telefonul trimite si primeşte numai frecvenşe joase. (vocea umana). Modemul DSL şi echipamentul telephonic normal pot fi folosite simultan fară nici o interferență intre ele.

(http://en.wikipedia.org/wiki/Digital_subscriber_line)

4.8.FUNCȚIONAREA

Linia locala a rețelei publice de telefonie lâocala (POTS) a fost inițial proiectată să transmită comunicații prin voce si semnalizare, din moment ce conceptul de comuncații de date pe care il ştim astăzi nu exista. Din motive economice, sistemul telephonic in mod normal lasă să treacă datele audio intre 300 si 3400 Hz care se crede ca este intervalul necesar pentru ca vocea sa fie inteligibilă corect.

În centrala telefonică vocea este in general digitizată într-un stream de 64kbit/s în forma unui semnal de 8 biti folosind o rată de sample 8000Hz, conform th lui Nyquist – orice semnal mai sus de 4000Hz nu este lăsat sa treacă de catre reteaua de telefonie(şi trebuie să fie blocat de filtru pentru a provoca efectele de aliere).

Legile fizicii – in special limita Shannon – limitează viteza de transmisie. Pentru o perioadă lungă de timp s-a crezut ca o linie telefonică conventională nu poate fi impinsă mai sus de limita de 9600bit/s.

Legatura locală care conectează centrala teleflonică de abonaţi este capabilă să poarte frecvenţe mult mai mari de 3.4kHz limita superioară a POTS. Depinzând de lungimea si de caliteatea legaturii, limita superioară poate fi de zeci de MHz. DSL preia avantajul acestei latimi de banda nefolosite a legaturii locale si creeaza canale de 4312.5Hz lăţime intre 10 si 100kHz, depinzând de cum este configurat sistemul. Alocarea canaleler continuă la frecvenţe din ce in ce mai mari (pana la 1.2MHz pentru ADSL) pâna când noile canale nu sunt utilizabile. Fiecare canal este evaluat pentru folosintă in acelaşi fel ca şi un modem analog ar fi pe o conexiune POTS. Cu cât mai multe canale utilizabile cu atât mai mare lătimea de banda, de aceea distanta şi calitatea liniei este un factor (cu cât distanţa este mai mică cu atat mai mare viteza DSL). Canalele utilizabile sunt imparţite in doua benzi de frecventa pentru trafic upstream si downstream, bazat pe o ratie preconfigurata. Aceasta segregare reduce interferentele. Odata ce un grupurile de canale au fost impartite in doua benzi de frecvente diferite, canalele sunt legate intr-o pereche de circuite virtuale, una pentru fiecare directie. Ca si la modemurile analogice, tranceiverele DSL monitorizează constant calitatea fiecarui canal şi îl vor adăuga sau scoate din serviciu depinzand daca sunt utilizabile sau nu.

Deoarece DSL operează la mai mult de 3.4kHz (limita vocii), nu poate fi trecut printr-o bobină de incărcare, care sunt in esentă filtre care blochează frecvenţele non-voce. Şi sunt plasate la distante regulate in linii doar pentru servicii POTS. Un semnal DSL nu poate trece printr-o bobina de incarcare instalata corect si functionala, cum nici un serviciu de voce sa fie metinut dupa o oarecare distanta fara asemenea bobine. Unele zone care sunt in zona pentru servicii DSL nu sunt alese pentru plasamnetul bobinelor de sarcina. Din aceasta cauza companiile de telefonie incearca sa inlature bobinele de sarcina pe circuitele de cupru care pot lucra fara ele. Si conditionand liniile sa nu mai fie nevoie de ele prin folosirea fibrei in zona sau nod FTTN.

Mai multi factori au contribuit la popularizarea tehnologiei DSL:

- Până la sfârşitul anului 1990. Costul procesoarelor de semnal era prohibitiv. Toate formele de DSL folosesc procesoare de semnal complexe, şi algoritmi care să inlature limitarile existente in perechile de fire torsadate.
- Linie DSL poate fi desfasurată peste un cablu existent, incluzând chiar şi costul echipamentului tot este mai ieftin decât instalarea de fibra optică pe aceeaşi rută şi distantă.

Cele mai multe implementări rezidenţiale şi firme mici de DSL primesc frecvenţe mici pentru serviciul POTS, pentru că cu ajutorul filtrelor si spliterelor serviciile existente de voce sa fie in continuare utilizabile şi să functioneze independent de serviciul DSL. Chiar dacă şi comunicaţiile POTS, incluzând fax-ul si modemurile analogice, pot folosi cablurile cu DSL. Doar un modem DSL poate folosi linia in acelasi timp. Pentru a folosi mai multe calculatoare in acelasi timp legatura este nevoie de un router care sa stabileasca conexiuni intre modemul DSL si reteaua din care fac parte computerele.

Odată ce canalalele de upload şi donwload sunt stabilite, sunt folosite pentru a conecta linia abonatului la un serviciu cum ar fi un ISP.

(http://en.wikipedia.org/wiki/Digital_subscriber_line)

4.9. ECHIPAMENTE

Echipamentul din partea clientului a conexiunii constă intr-un modem DSL. Care converteşte informaţia din semnale digitale folosite de calculatoare intr-un semnal de voltaj pentru gama de frecvenţa care este folosită de linia telefonică.

Pentru unele variante de DSL (de exemplu HDSL), modemul este conectat direct la calculator printr-o interfaţă serială, folosind protocoale ca RS-232 sau V.35. În alte cazuri (in special ADSL), este comun ca echipamentul clientului să integreze un nivel mai mare de funcţionalitate, cum ar fi rutarea, firewall, sau alte aplicaţii specifice hardware şi software. In acest caz tot echipamentul este numit DSL router sau DSL gateway.

Unele forme de tehnologie DSL necesită instalarea de filtre speciale pentru a separa sau imparţi semnalul DSL de frecventa joasă pentru voce. Separarea se poate face fie la punctul de demarcaţie, fie cu filtre instalate la prizele telefonice in perimetrul clientului.

În schimb, un multiplexor digital de acces la linie (DSLAM) finalizeaza circuitul DSL şi le agreghează, unde sunt trimise către reţeaua de transport. In cazul ADSL, componenta vocală este de asemenea separată la acest pas, ori de un filtru integrat in DSLAM ori de un echipament specializat instalat inaintea lui. DSLAM termină toate conexiunile şi recuperează informaţia digitală initială.

(http://en.wikipedia.org/wiki/Digital_subscriber_line)

4.10. SETĂRI TIPICE ŞI PROCEDURI DE CONECTARE

Primul pas este conexiunea fizică. În partea clientului, modemul DSL este conectat la o linie telefonică. Compania telefonică se conectează la celalalt capăt printr-un DSLAM, care concentrează un numar mare de conexiuni individuale DSL intr-o singură cutie. Locaţia DSLAM este in funcţie de compania de telecomunicaţii, dar nu poate fi plasată prea departe de utilizator datorită atenuării, pierderea datelor datorita rezistentei electrice mari intalnite intre DSLAM şi modemul utilizatorului. Este normal ca si câteva strazi sa fie conectate la acelasi DSLAM. Când modemul DSL este pornit, trece printr-o procedură de sincronizare. Procesul actual variază de la modem la modem dar poate fi descrisa in general ca:

- Modemul face un self-test

- Modemul verifică şi conexiunea dintre el si computer. Pentru variantele rezidenţiale aceasta este de obicei protul Ethernet sau USB; in modele mai rare se foloseste si portul FireWire. De asemenea unele variante folosesc conexiuni seriale sincrone.

- Modemul incearcă să se sincronizeze cu DSLAM-ul. Datele pot fi primite de catre computer numai dupa ce modemul si DSLAM-ul s-au sincronizat. Procedura de sincronizare este relativ rapidă dar foarte complexa, include teste pentru ca ambele părti sa optimizeze performanţa potrivit liniei folosite.

(http://en.wikipedia.org/wiki/Digital_subscriber_line)

4.11.PROTOCOALE ŞI CONFIGURAȚII

Multe tehnologii DSL implementează un mod de transfer asincron ATM peste stream-ul de biti low-level pentru a permite adaptarea unui număr de tehnologii diferite in acelasi link.

Implementarile DSL pot creea retele bridged sau rutate. In configurația bridge, grupul de abonați se pot conecta efectiv intr-un singur subnet. Cele mai vechi implementari ale DHCP pentru a furniza detalii ca adresa de IP spre echipamentul abonaților, cu autentificare folosind adresa de MAC sau un hostname stabilit. Mai târziu implementarile folosesc mai des PPPoE sau PPPoA, in timp ce autentificarea se face cu un userid si o parola folosind mecanisme PPP pentru a furniza setarile de retea.

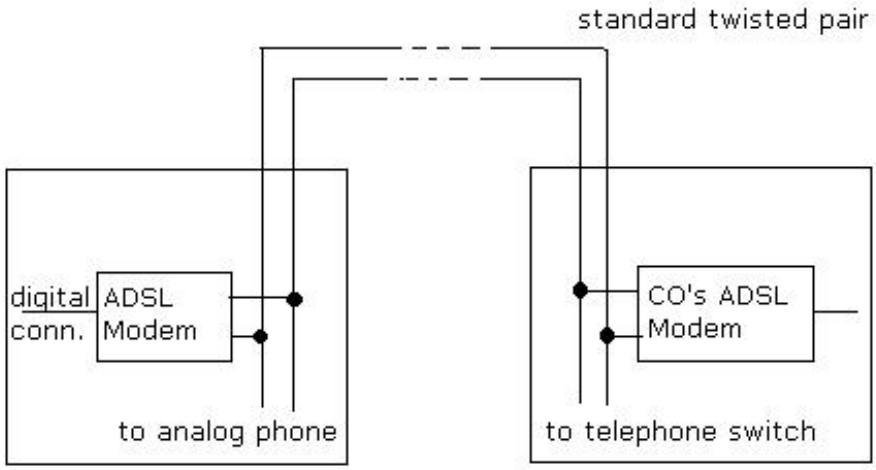


Fig. 14: Modem ADSL conectat la bucla locală

4.12.TEHNOLOGII DSL

Limitarile legate de lungimea liniilor intre telefoane si subscriberi sunt mai restrictive la rate de transmisie mai mari.Tehnologii ca de exemplu VDSL ofera o viteza foarte ridicata, putand oferi servicii „triple play" (internet de mare viteza, televiziune, si telefonie).Tehnologii ca GDSL pot creste in continuare viteza de transmisie a DSL.

Exemple de tehnologii DSL:

- High Data Rate Digital Subscriber Line (**HDSL**)
- Symmetric Digital Subscriber Line (SDSL),versiunea standardizata a lui HDSL
- Asymmetric Digital Subscriber Line (ADSL), o versiune a DSL cu o viteza mai mica de upload
- ISDN Digital Subscriber Line (IDSL)
- Rate-Adaptive Digital Subscriber Line (RADSL)
- Very High Speed Digital Subscriber Line (VDSL)
- Very High Speed Digital Subscriber Line 2 (VDSL2), o versiune inbunattita a lui VDSL
- Symmetric High-speed Digital Subscriber Line (G.SHDSL), o inlocuire standardizata pentru SDSL de catre International Telecommunication Union Telecommunication Standardization Sector

- Powerline Digital Subscriber Line (PDSL), o soluie de comunicatii de inalta viteza, care moduleaza datele de mare viteza pe distributia existent de electricitate
- UDSL
- Etherloop Ethernet Local Loop
- GDSL Gigabit DSL, bazata pe tehnologia MIMO (***http://en.wikipedia.org/wiki/Digital_subscriber_line***)

4.13.METODE DE TRANSMISIE

Metodele de transmisie difera in functie de piata, regiune, cariera si echipament.

- 2B1Q: Two-binary, one-quaternary, folosita pentru IDSL si HDSL
- CAP: Carrierless Amplitude Phase Modulation -dezaprobata in 1996 for ADSL, folosita pentru HDSL
- DMT: Discrete Multitone Modulation, cea mai folosita, cunoscuta si ca OFDM
- OFDM: Orthogonal Frequency-Division Multiplexing

(*http://en.wikipedia.org/wiki/Digital_subscriber_line*)

4.14.CONCLUZII

O arie largă de servicii rezidente sau din clasa business se pregătesc să treacă la tehnologia DSL, care va fi suportata de următoarea generație DSLAM pentru a oferi o suită de capabilități de servicii de calitate (QoS) . ***(http://en.wikipedia.org/wiki/Digital_subscriber_line)***

4.10. REFERINȚE BIBLIOGRAFICE

- *http://en.wikipedia.org/wiki/Digital_subscriber_line*
- *Burstein, Dave (2002). DSL. John Wiley and Sons, New York. ISBN 0-471-08390-9. pp 53-86*
- *Lechleider, Joseph, High Bit Rate Digital Subscriber Lines: A Review of HDSL Progress, IEEE Journal 9:6 (August 1991) pp 769-84*
- *B. Lee, J.Cioffi, et al, Gigabit DSL, IEEE Transaction on Communication, Sep, 2007, pp 1689-1692*

5. TEHNOLOGIA ATM

5.6. INTRODUCERE

Este cea mai răspândită tehnologie de telecomunicații, bazată pe standarde bine definite, pentru transportul de date, video şi voce la viteze foarte înalte şi se utilizează de obicei în arterele principale ale rețelelor (backbone). ATM a căpătat o răspândire largă din cauza flexibilității înalte de susținere a unei game largi de tehnologii, cum ar fi Frame Relay, IP, DSL şi altele. Tehnologia ATM se poate folosi pentru interconectarea nodurilor, iar în anumite cazuri şi pentru conectarea clienților.

Structura unei retele ATM:

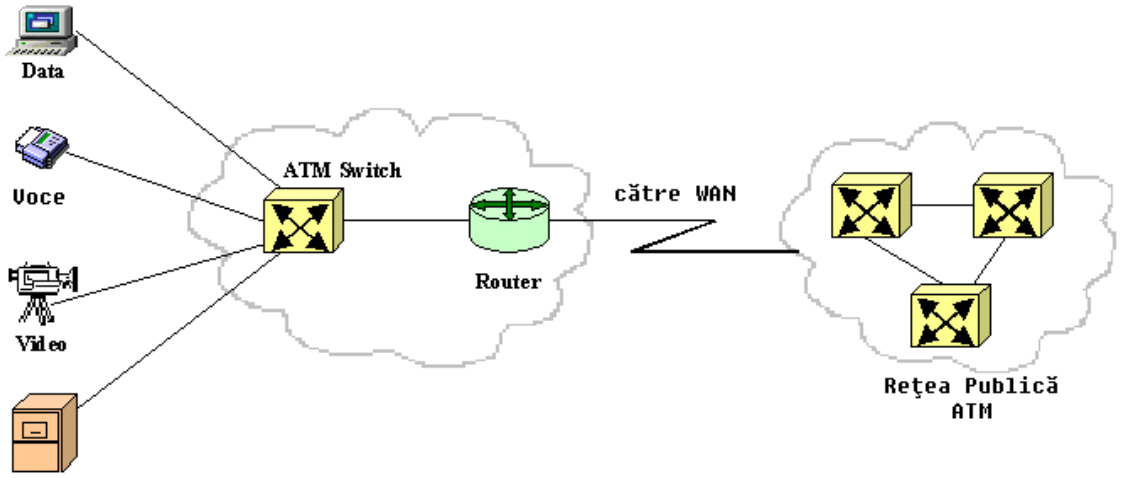


***Fig 15** (http://www2.rad.com/networks/2004/atm/intro/devices_files/image001.gif)*

ATM este o tehnologie de comutare a celulelor (de aceea ea se mai numeşte uneori (Cell Relay) şi de multiplexare, ceea ce combină avantajele comutării de circuite (viteză garantată şi întârziere constantă) şi pe cele ale comutării de pachete (flexibilitate şi eficiență în caz de trafic discontinuu). La intrarea în comutatoarele din rețeaua ATM toate datele se despart în porțiuni de 48 octeți, cărora li se adaugă 5 octeți de antet care conține date de serviciu. Astfel se formează celule ATM de 53 octeți, care se transmit prin rețea. La ieşire din rețea antetele se aruncă şi datele ajung la destinație sub forma inițială. Tehnologia ATM permite utilizarea unei lărgimi de bandă de la câțiva megabiți pe secundă până la zeci de gigabiți pe secundă.

ATM se defineşte un mod de transfer asincron, pentru a-l deosebi de alte tehnologii sincrone, cum ar fi TDM (Time Division Multiplexing). În cazul TDM fiecărui utilizator i se atribuie un anumit interval de timp, care îi aparține şi în care nu poate transmite nimeni altul. Dacă o stație are de transmis mai multe date, ea poate transmite doar în intervalul de timp rezervat ei, chiar dacă altă stație nu are nimic de transmis în acelaşi interval de timp, şi ale cărei intervale rămân neutilizate. În cazul ATM, intervalele de timp sunt disponibile la cerere în dependență de trafic, iar selectarea destinației se efectuează prin descifrarea adreselor cuprinse în fiecare celulă de informație ATM.

Câmpul de 4 biți corespunzător identificatorului fluxului generic (GFI) este folosit pentru reglarea fluxului de informații într-o rețea ATM. Câmpul de 8 biți corespunzător dentificatorului căii virtuale (VPI Virtual Path Identifier) reprezintă jumătate dintr-un identificator de conexiune care cuprinde două părți. Acest câmp identifică o cale virtuală care poate reprezenta un grup de cuvinte virtuale existente pe acelaşi traseu.

GFC = Generic Flow Control CLP = Cell Loss Priority
VPI = Virtual Path Identifier HEC = Header Error Control
VCI = Virtual Circuit Identifier NMI = Network Node Interface
PTI = Playload Type Identifier UNI = User Network

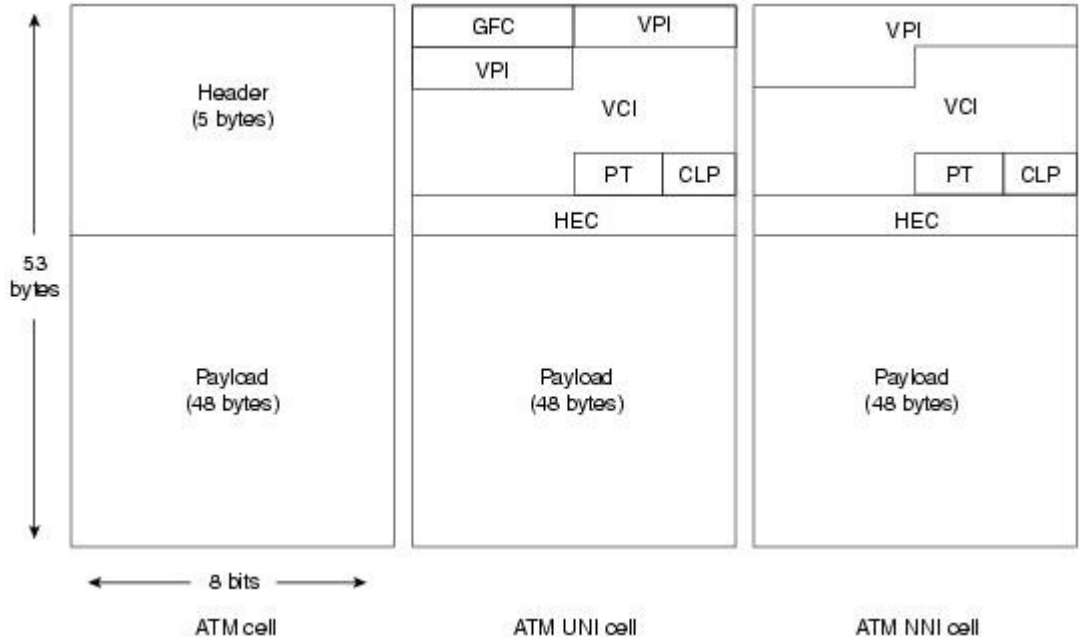


***Fig. 16** (http://www2.rad.com/networks/2004/atm/intro/cellbase_files/image001.gif)*

Câmpul identificatorului canalului virtual (VCI) este a doua jumătate a identificatorului de conexiune (ce cuprinde două părți) transmis în antetul ATM. Câmpul VCI de 8 biți identifică o conexiune între două terminale (stații) ATM între care se realizează o aplicație. Canalele virtuale multiple pot fi transportate în cadrul unei căi virtuale unice.

***Fig. 17** (http://www.cisco.com/univercd/illus/c/06/ct842706.jpg)*

Câmpul tipul informației utile (PTI) specifică tipul informației transportate în zona de 48 octeți informaționali ai celulei ATM. Câmpul de 3 biți specifică tipul informațiilor utile adică sunt informații de gestiune sau date utilizator. Celelalte câmpuri suplimentare vor primi utilizări viitoare.

Câmpul Prioritatea Celulelor Pierdute de 1 bit indică importanța celulelor. Dacă bitul este 1 celula poate fi eliminată de un comutator în caz de congestionare a traficului. Dacă celula poate fi eliminată, bitul corespunzător câmpului primeşte valoarea zero.
Câmpul Controlului Erorilor de Antet (HEC) are 8 biți şi reprezintă rezultatul unui cod redundant ciclic (CRC) calculat pentru antetul celulei ATM. Câmpul asigură capacitatea de detectare a erorilor de un bit şi a unor anumite erori de biți multipli ce pot aparea în antetul celulei ATM de 40 de biți.
Modul de transfer asincron (ATM) se foloseşte pentru a expedia şi semnal pe lângă alte tipuri de trafic WAN, dar nu uşor, tehnica nu este flexibilă şi nici ieftină.

Celulele sunt pregatite de transmisie astfel incat sa se pastreze ordinea lor:

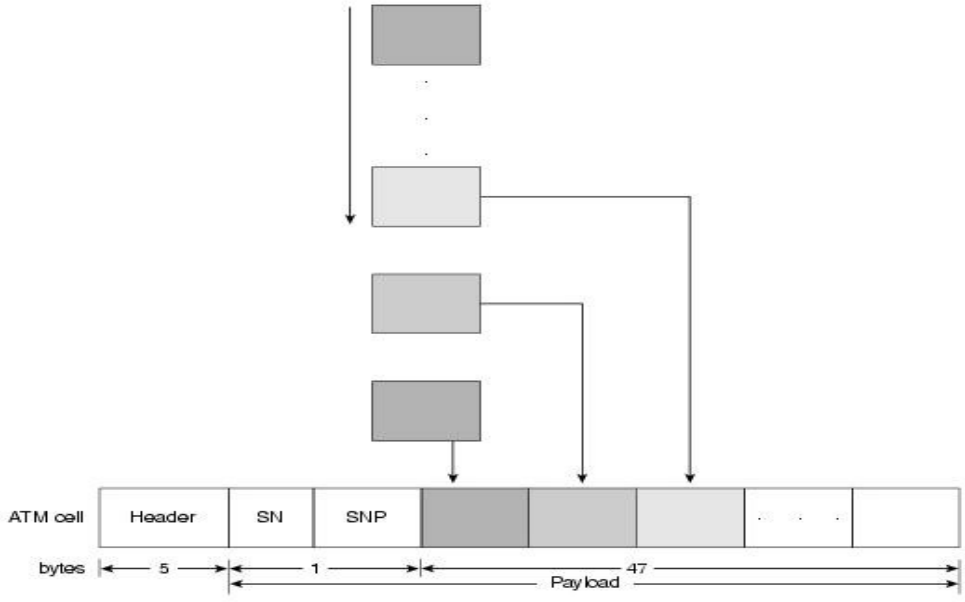


***Fig. 18** (http://www.cisco.com/univercd/illus/c/08/ct842708.jpg; http://www2.rad.com/networks/2004/atm/main.htm)*

5.8. TRASFERUL TRUNCHIURILOR PBX IN ATM

PBX(Private Branch Exchange)

Sunt cunoscute două principale metode de abordare a operării tradiționale în rețelele PBX: prima metodă constă în utilizarea liniilor particulare pentru a conecta centrale de corporații (PBX); a doua metodă înseamnă conectarea fiecărei centrale PBX la rețeaua publică vocală si abonarea la un serviciu de rețea privată virtuală (VPN). Rețelele vocale private cer întretinerea tabelelor de rutare prin rețea, în fiecare PBX. Cu rețelele private virtuale (VPN), tabelele de rutare din PBX sunt gestionate de serviciul cerut.

În fiecare caz, trunchiurile PBX vocale pot fi transferate în ATM. Totusi, furnizarea suportului optim pentru trunchiuri are nevoie de interpretarea semnalelor inter-PBX, cum este cazul semnalizărilor prin SS7 "Siganlign System 7" din America de Nord.

Interpretarea acestor semnalizări aduce şi avantaje. Apelurile tip semnale de date sau fax pot fi îndrumate diferit față de apelul vocal. Rutarea apelului poate fi optimizată pentru a îmbunătăti disponibilitățile rețelei şi costurile. Planul de apelare poate fi întreținut central. Apelurile sigure, apelurile internaționale pot fi comprimate pentru a oferi o eficiență mai bună în rețea.

Sunt însă şi două probleme majore. Există destul de multe sisteme de semnalizare vocale tip SS7, utilizate în întreaga lume. În plus, nu sunt încă mecanisme care să permită rețelelor ATM să traducă aceste sisteme de semnalizare foarte diverse şi nici nu este clar când vor apărea.

O altă problemă tehnică este întârzierea adresării pe durata procesului de transmitere a semnalului vocal de la un capăt la altul. Întârzierea poate apărea când se adaptează semnalul vocal în fluxul de celule ATM şi la ieşirea din rețeaua ATM, acolo unde celulele trebuie memorate temporar în buffer-e, pentru a minimiza efectele jitter-ului de rețea. Dacă un apel este dirijat prin centrale PBX intermediare, aceste întârzieri componente se adună, deoarece la fiecare joncțiune traficul trebuie convertit de la formatul celulă ATM în semnal vocal si apoi invers, în celule.

5.4. PARAMETRII DE CALITATE ATM

Tehnica ATM are un aşa-numit parametru de calitate (QOS) - toleranță la variația întârzierii unei celule (CDVT) - proiectat să mențină variația în întârziere dintre celule la minimum. Parametrul "întârzierea celulei în tranzit" (CTD) este o combinație între întârzierea de propagare şi cea de procesare în nodul unei rețele. Întârzierea la nivelul unui nod este determinată de procesarea cozilor de aşteptare de comutare şi de routare.

Testarea semnalului vocal prin ATM nu este încă edificatoare, pentru a înțelege setările optime ale acestor parametri şi ceea ce se întâmplă într-un mediu fizic real. Cu alte cuvinte, nu s-a demonstrat că "merge".

Ecoul este un aspect controversat, o altă problemă tehnică, care poate fi uşor depistat de utilizatorii "orientați" pe semnalul de date, implicați probabil cu implementarea rețelelor ATM. Toate telefoanele analogice produc ecou, care devine semnificativ (supărător) dacă întârzierea cap-la-cap sare de 32 de milisecunde. Pentru a evita această problemă în rețelele vocale, operatorii plasează compensatoare de ecou cât mai aproape posibil de fiecare abonat. Compensatoarele de ecou sunt necesare şi în rețelele ATM, deci trebuie să căutăm un echipament dotat cu caracteristici de compensare integrală a ecoului.

Pentru a fi eficient, semnalul vocal pus în seama ATM-ului are nevoie de clasa de serviciu cu rata binară variabilă (VBR) în timp real. Un echipament local de abonat (CPE) trebuie să îndeplinească minimum trei funcții: detecția pauzei în dialog, compensarea/anularea ecoului,

compresia (optional), şi acesta ar fi doar începutul. Pentru că saltul calitativ s-ar vedea doar când s-ar susține caracteristicile rețelelor private virtuale (VPN) sau când s-ar rezolva problemele de semnalizare.

Problema este în principal cauzată de pierderea, ignorarea standardelor CPE. Soluțiile de azi care facilitează transportul vocii prin rețeaua ATM sunt în general particulare. Forumul ATM mai are pe cap multe standarde de elaborat, chiar şi în ceea ce priveşte conversia în celule ATM. Cât timp standardele nu sunt finalizate, nu prea este de ales altceva decât varianta CBR - rata binară constantă - sau decât emularea de circuite.

5.5. APLICAȚIILE MODULUI DE TRANSFER

Maparea protocoalelor LAN în rețelele ATM, ca şi dezvoltarea API-ATM (Application Program Interface - Asyncronous Transfer Mode) sunt două dintre cele mai importante aplicații .

Dar ATM-ul este o tehnologie universală - se simte ca la ea acasă şi în rețele LAN şi în rețele WAN - deci orice aplicație poate fi în cele din urmă o aplicație ATM. Orice aplicație, mai nouă sau mai puțin nouă, trebuie să exploateze caracteristicile ATM-ului.

În realitate, peste 95 de procente din aplicațiile ATM care vor rula în anii următori sunt scrise deja. Mai mult, este vorba despre aplicațiile critice de business din LAN-urile care deja operează si care vor trebui să ruleze sub emblema ATM, pentru a-i certifica succesul.

Se cunosc două căi de strămutare a unei aplicații de LAN într-o rețea ATM. Unu: aplicația poate fi mapată în ATM la nivelul de protocol, cu un driver special software de LAN special, care controlează adaptorul ATM în sistemul clientului. Vânzătorii de adaptoare oferă clienților un software de emulare LAN. Doi: aplicațiile pot fi legate direct la ATM, mai bine decât printr-un protocol LAN, via middleware (driverul WinSock/Windows - Microsoft). Cum va arăta un astfel de software matur este încă o enigmă.

5.6. MAPAREA PROTOCOLULUI

Maparea de protocol pentru aplicațiile LAN este tocmai ceea ce a aprobat Forumul ATM în standardul numit Versiunea 1 - Emularea LAN-ATM (LANE). LANE operează la nivelul 2 - MAC/OSI (controlul accesului la mediu) şi va fi folosită, în prima fază, pentru operarea în rețea ATM la nivel de workgroup.

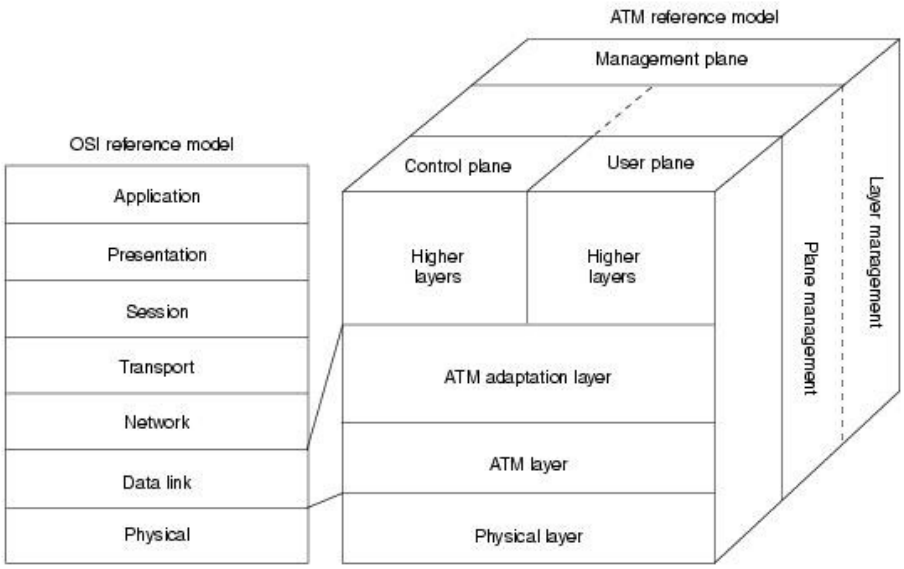


***Fig. 19** (http://www.cisco.com/univercd/illus/c/07/ct842707.jpg http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/atm.htm#wp1020715)*

Pentru operarea în rețeaua de întreprindere, exista două activități care folosesc emularea la nivelul 3 - OSI (REȚEA). Deoarece aici intră în discuție procesul de rutare, aceste două standarde proiect ne vor schimba cunoştinţele despre routerele din rețelele noastre.

Prima opțiune este standardul Multiprotocol - ATM (MPOA - Multiprotocol over ATM), deja conturat de Forum. Cisco Systems, Newbridge Networks sunt cei mai decişi suporteri ai standardului MPOA.

Folosind MPOA, protocoalele LAN actuale sunt mapate în adrese ATM de către un server de dirijare. Serverul este un fel de server de directoare, care "ştie" adresele ATM ale statiilor ATM care rulează aplicații LAN sau care "vede" punctele de contact ATM cele mai oportune în preluarea stațiilor LAN.

A doua opțiune pentru protocoalele de nivel 3 este interfața privată integrată, pentru accesul rețea-la-rețea (Integrated Private Network-to-Network Interface, I - PNNI), mai adecvată vederilor IBM sau BayNetworks.

Cu I-PNNI, propriul protocol de routare ATM este pus să transporte informații de adresare şi topologie despre LAN-urile tradiționale sau despre statiile LAN emulate ATM din rețelele ATM. La limita rețelei ATM, această informație este utilizată pentru a transpune informații de dirijare în protocoalele tradiționale de nivel 3, cum sunt RIP (Routing Information Protocol) sau Open Shortest Path First.

Maparea unui protocol în ATM înseamnă interceptarea conexiunii pe care curge o aplicație LAN, după ce a fost creat un număr oarecare de niveluri pentru protocoale LAN, de către un software de client sau de server.

De exemplu, LANE operează la nivelul MAC şi emulează servicii pentru oricare aplicație LAN. Protocolul MPDA, care furnizează servicii şi la nivelul 2 şi la 3, ar putea emula caracteristicile unor protocoale ca IP.

Valoarea mapării de protocoale este dată de faptul că, de multe ori, poate fi utilizată pe aplicațiile existente. Se înlocuieşte pur şi simplu un driver de cartelă-interfață de rețea cu un SW bazat pe ATM si

care susține standardul de mapare a protocoalelor utilizate. Nu este nevoie de o recompilare a codului sursă şi nici nu se impun schimbări ale aplicațiilor.

Maparea unui protocol protejează întreaga stivă de protocoale de aplicații, inclusiv antetul acesteia; astfel, legarea stațiilor ATM cu cele tradiționale LAN se poate face usor: pur şi simplu se extrage antetul ATM adăugat mesajului "LAN" şi ceea ce rămâne poate fi remis rețelei locale.

5.7. Concluzii

Tehnologia ATM este ideala pentru conexiunile la retele de dimensiuni mari de tip WAN ,unde este nevoie de suportpentru aplicatii de timp real si servicii integrate(voce,imagine,date ,text).

Utilizarea tehnologiei de comutare a celulelor într-un mediu LAN asigură avantaje deosebite față de tehnologia de partajare a mediului utilizată de rețelele FDDI, inel, Ethernet. Un prim avantaj este obținerea unui acces complex de banda de transfer la comutatoarele ATM pentru stațiile ATM; alt important avantaj este ca dispozitivele accesate pot opera la viteze de transfer diferite.

Se prezintă un comutator ATM ce este utilizat pentru trei viteze separate de operare. Stațiile de lucru (ST) se pot conecta la comutator la viteze de transfer de 25 Mb/s pentru realizarea conexiunii într-o rețea de comunicații sau pentru a forma o rețea locală mai mare. Tehnologia ATM este caracterizată prin mod de operare asincron si funcționare bazată pe conexiuni.

Celulele ATM sunt multiplexate şi transmise prin linkuri la comutatoarele ATM printr-un flux unic de celule. Multiplexarea celulelor ATM se realizează prin transfer asincron, fiind transmise numai atunci când există date de transmis spre deosebire de cazul multiplexarii tradiționale cu diviziune în timp când se transmit octeți de sincronizare sau supraviețuire când nu sunt date de transferat.

Privitor la tehnologia orientată pe conexiuni se poate spune ca între stațiile (terminalele) ATM se realizează o conexiune. Se specifică o cale de transmisie între comutatoarele ATM şi stațiile (terminalele) ATM, permițându-se folosirea antetului corespunzător celulelor ATM în procesul de rutare pe calea specificăta în cadrul unei rețele ATM. Modelul arhitectural de referință al protocolului ATM are trei niveluri: nivelul fizic,nivelul ATM si nivelul de adaptare ATM.

Rutarea celulelor ATM între comutatoarele ATM se bazează pe intrările tabelului de rutare pentru fiecare comutator, care cuprind Identificatorul Caii Virtuale (VPI) şi numărul de port.

Rutarea curentă a celulelor ATM depinde de modul de stabilire a unei conexiuni configurată la cerere sau prestabilită. Tipul prestabilit de conexiune este cunoscut sub numele de conexiune virtuală permanentă (PVC Permanent Virtual Connection), iar cel de-al doilea tip este cunoscut ca fiind conexiune comutată virtuală (SVC Swiched Virtual Connection).

Prin prezentarea structurii antetului celulei ATM rezultă că există două câmpuri VCI (Identificatorul canalului virtual) şi VPI (Identaficatorul căii virtuale) ce asigură 256 căi virtuale, fiecare cale permițând 216 (65536) conexiuni virtuale.

5.8. Referințe Bibliografice:

- *http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/atm.htm#wp1020715*
- *http://www.rad.com/Home/0,6583,5847,00.html*
- *traducere Cisco CCNA 4*

6. TEHNOLOGIA MPLS

6.1. INTRODUCERE

Comutarea Multiprotocol cu Etichete (Multi Protocol Label Switching) reprezintă o nouă arhitectură în care nodurile terminale adaugă o etichetă unui pachet IP ce identifică drumul spre destinatie, iar pachetele sunt directionate pe baza etichetei, fără inspectarea header-ului initial.
MPLS reprezintă ultimul pas făcut în evolutia tehnologiilor de comutare/rutare pentru Internet, folosind o solutie ce integrează atât controlul rutării IP, cât si comutarea de la nivelul legăturii de date (nivelul 2 din modelul OSI). Mai mult, MPLS oferă bazele unor servicii de rutare avansate, rezolvând o serie de probleme:

- se adresează problemelor privind scalabilitatea, legate de modelul IP-over-ATM;
- reduce complexitatea operatiilor din retea;
- facilitează aparitia de noi posibilităti de rutare, ce îmbunătătesc tehnicile de rutare IP existente;
- oferă o solutie standardizată, ce are avantajul interoperabilităţii între diversi furnizori de produse si servicii.

Esenta MPLS-ului este generarea unei etichete „label" scurte, de dimensiune fixa, care se comporta ca o reprezentare simplificata a header-ului pachetului IP. Este la fel cum codul poştal este o forma simplificata pentru adresa unei case, a unei strazi şi a unui oraş în adresa poştala, folosind aceasta eticheta pentru a lua o decizie în procesul de forward. Pachetele IP au un câmp în header-ul lor care contine adresa spre care pachetul este rutat. Procesul traditional de rutare într-o retea proceseaza aceasta informatie la fiecare router, într-o cale a pachetului prin retea (rutare pas cu pas).

În MPLS, pachetele IP sunt încapsulate cu aceste etichete de catre primul dispozitiv MPLS pe care-l întâlnesc de cum intra în retea. Router-ul MPLS din margine (egde-router) analizeaza continutul header-ului IP şi selecteaza o eticheta potrivita cu care sa încapsuleze pachetul.

Cel mai mare avantaj al MPLS-ului vine tocmai din faptul ca în contrast cu rutarea IP conventionala, aceasta analiza poate sa nu se bazeze numai pe adresa destinatie care este purtata de header-ul IP, ci şi pe alte elemente. La fiecare dintre nodurile ulterioare din retea, eticheta MPLS (şi nu header-ul IP) se foloseşte pentru a lua decizia de forwarding pentru un pachet. În final, pe parcurs ce pachetele MPLS etichetate parasesc reteaua, un alt edge router elimina etichetele

În terminologia MPLS, nodurile sau router-ele care manipuleaza pachetele se numesc *Label Switched Routers (LSR)* – routere cu comutare de etichete. Derivarea acestor termeni este evidenta: router-ele MPLS forward-eaza pachetele, luând decizii de comutare bazate pe eticheta MPLS. Aceasta ilustreaza un alt concept cheie în MPLS. Router-ele IP conventionale contin „tabele de rutare" care sunt interogate folosind un header IP dintr-un pachet pentru a decide cun sa forward-eze acest pachet. Aceste tabele sunt construite de catre protocoale de rutare IP (cum ar fi RIP, OSPF), care poarta informatia IP destinatie sub forma de adrese IP. În practica observam ca acest forwarding (inspectarea header-ului IP)

şi planurile de control (generarea tabelelor de rutare) sunt strâns cuplate. Întrucât forwarding-ul MPLS este bazat pe etichete, este posibila separarea clara a planului de forward-are (bazat pe eticheta) de planul de control pentru protocolul de rutare. Prin separarea acestora doua, fiecare poate sa fie modificat independent. Cu o astfel de separare, nu mai avem nevoie sa schimbam maşina care face forwarding-ul, de exemplu, pentru a migra spre o noua strategie de rutare în retea.

Suita de protocoale TCP/IP (şi în special protocolul IP) este acum fundamentul pentru multe retele publice (Internet-ul) şi private (Intranet-uri) de date. Viitoarea convergenta a vocii, datelor şi retelelor multimedia se aşteapta sa fie în mare bazata pe protocoale IP, ducând la necesitatea de îmbunatatiri din punct de vedere tehnic şi operational.

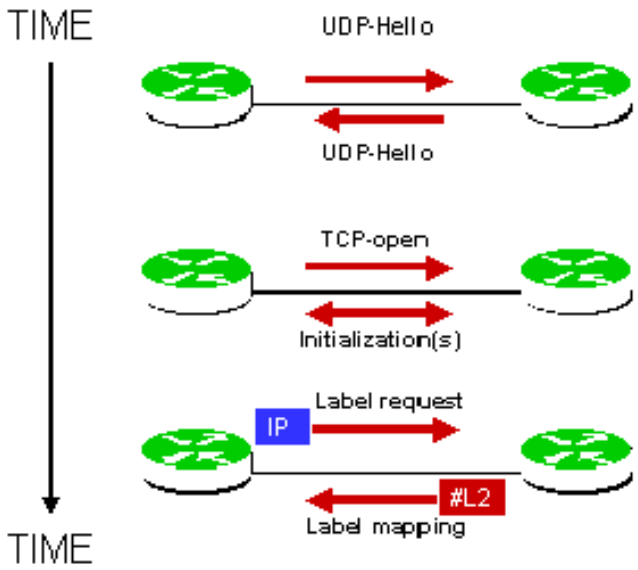


Fig. 20: Modul de lucru MPLS

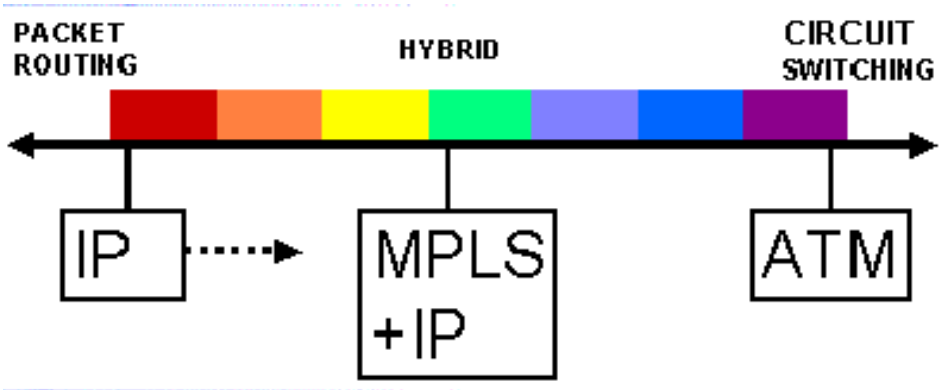


Fig. 21: Cel mai bun din cele doua lumi

6.2. CONCEPTE DE RUTARE ŞI COMUTARE

Conceptele de baza care se aplica în orice tehnologie de comutare:

- ***Rutarea*** este un termen folosit pentru a descrie actiunile care trebuiesc luate într-o retea pentru a muta pachetele prin ea. Vorbim astfel de pachete care vor fi „rutate" de la „a" la „b", sau despre ele ca fiind rutate printr-o retea sau între retele. Pot fi multe routere într-o retea conectate într-o oarecare maniera arbitrara. Pachetele înainteaza prin retea fiind trimise de la o maşina la alta pâna la destinatia lor. Protocoalele de rutare (de exemplu RIP, OSPF) permit fiecarei maşini sa înteleaga care alta maşina este „urmatorul hop" pe care un pachet îl va urma spre destinatia sa. Router-ele folosesc protocoalele de rutare pentru a construi tabele de rutare. Când ele primesc un pachet şi trebuie sa ia o decizie de forwarding, router-ele „inspecteaza" tabela de rutare, folosind adresa IP destinatie a pachetului ca un index, şi astfel obtin identitatea maşinii din „urmatorul hop". Constructia tabelelor şi folosirea lor pentru inspectarea în momentul forwarding-ului sunt operatii separate logic. Figura de mai jos ilustreaza aceste functii care pot aparea într-un router.

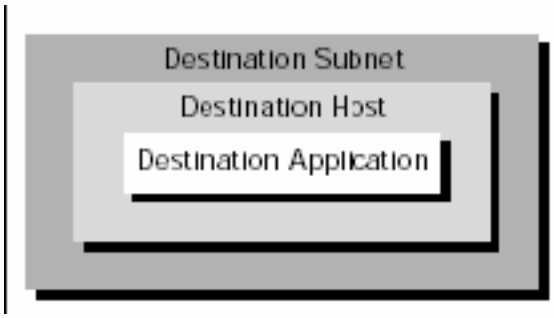
- ***Comutarea*** este folosita în general pentru a descrie transferul de date de la un port de intrare la un port de ieşire al unei maşini, în care selectia portului de ieşire este bazata pe informatia de nivel 2 (de exemplu ATM VPI/VCI).

- ***Componenta de control*** construieşte şi mentine o tabela de forwarding pentru nodul folosit. Ea functioneaza cu componentele de control de la alte noduri pentru a distribui informatia de rutare cu acuratete, asigurându-se de asemenea ca procedurile locale consistente sunt folosite pentru crearea tabelelor de forwarding. Protocoalele de rutare standard (de exemplu OSPF, BGP şi RIP) sunt folosite pentru schimbul informatiei de rutare între componentele de control. Componentele de control trebuie sa reactioneze atunci când apar schimbari în retea (cum ar fi o cadere de legatura), dar nu sunt implicate în procesarea pachetelor individuale.

- ***Componenta de forwarding*** realizeaza forwarding-ul pachetului. Foloseşte informatia din tabela de forwarding (cea care este mentinuta de router), informatie care este transportata de pachet şi împreuna cu un set de proceduri locale iau decizia de forwarding. Într-un router conventional, un algoritm de comparatie bazat pe potrivirea cea mai lunga, compara adresa destinatie din pachet cu intrarile din tabela de forwarding, pâna când obtine cea mai buna potrivire. Mai important, procesul total de decizie trebuie sa fie repetat la fiecare nod de-a lungul caii de la sursa la destinaaie. Într-un LSR, un algoritm de swapping al etichetelor (cu potrivire exacta), foloseşte eticheta din pachet şi o tabela de forwarding bazata pe etichete, pentru a obtine o „noua" eticheta şi interfata de ieşire pentru pachet.

- ***O tabela de forwarding*** este setul de intrari într-o tabela care ofera informatii pentru a ajuta componenta de forwarding sa-şi efectueze functia de switching (comutare). Tabela de forwarding trebuie sa asocieze fiecare pachet cu o intrare (în mod traditional adresa destinatie), care ofera instructiuni înspre ce şi unde se întreapta în continuare pachetul.

- ***O clasa de echivalenta pentru forwarding*** *(Forwarding Equivalence Class- FEC)* care este definita ca orice grup de pachete care poate fi tratat într-o maniera echivalenta pentru scopuri de forwarding. Un exemplu de FEC este setul de pachete de unicast a caror adrese destinatie se potrivesc prefixului unei adrese IP particulare. Un alt FEC este setul de pachete a caror adrese sursa şi destinatie este la fel. FEC-urile pot fi definite la diferite nivele. Figura de mai jos ilustreaza acest lucru:



O eticheta este un identificator relativ scurt, de lungime fixa, nestructurat, care poate fi folosit în asistarea procesului de forwarding. Etichetele sunt asociate cu un FEC în timpul procesului de unire. Etichetele sunt în mod normal locale unei singure legaturi de date şi nu au semnificatie globala (aşa cum are adresa). Etichetele sunt analog cu DLCI-urile folosite în retele Frame Relay, sau cu VPI/VCI-urile din mediile ATM. Întrucât ATM este o tehnologie care deja foloseşte câmpuri scurte de dimensiune fixa pentru realizarea deciziilor de switching, comutarea de etichete este considerata o modalitate eficienta de implementare a IP-ului „peste" ATM. Etichetele sunt legate cu un FEC (şi astfel capata semnificatie), ca rezultat a unor evenimente care indica necesitatea unei legaturi.

Aceste evenimente pot fi divizate în doua categorii:

•***legaturi determinatede date*** care apar atunci când începe transferul de trafic, este trimis la LSR şi este recunoscut ca un candidat pentru comutarea de etichete. Legarile etichetelor sunt stabilite doar atunci când este nevoie, rezultând astfel mai putine intrari în tabela de forwarding. Etichetele sunt asignate fluxurilor de trafic IP individuale şi nu pachetelor singulare. Într-o retea ATM, aceasta poate duce la folosirea unui numar substantial de circuite virtuale, ceea ce poate limita scalabilitatea retelei;

•***legaturi determinate de control*** care sunt stabilite ca rezultat al activitatii planului de control şi sunt independente de date. Legaturile etichetei pot fi stabilite ca raspuns la actualizarea rutelor sau receptia mesajelor RSVP. Legatura etichetei determinata de control este mai scalabila decât cele determinate de date, şi din acest motiv se foloseşte în MPLS.

6.3. Concepte MPLS si Terminologie

Conform tehnologiei MPLS, trecerea pachetelor dintr-o retea in alta (forwarding) este bazata pe etichete(*label*), care sunt atribuite pachetelor atunci cand acestea din urma intra in retea, si sunt extrase, atunci cand pachetele parasesc reteaua. Etichetele se pun in fata pachetului, iar nodurile din reteaua MPLS, forwardeaza pachetele /celulele bazandu-se pe valoarea etichetei (nu pe informatia IP). MPLS permite sa avem decizii de forwarding bazate pe: Traffic Engineering, multicast, VPN, QoS, etc.

6.3.1. Forwarding-ul bazat pe IP

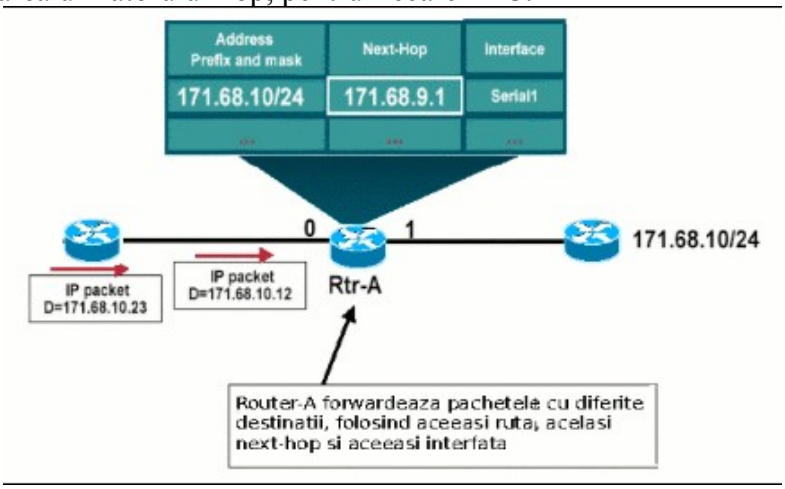
Caracteristici:

- Forwarding-ul este facut in mod independent la fiecare hop;
- Decizia de rutare este bazata pe header-ul pachetului si pe algoritmul de rutare (tabela de rutare);
- Fiecare ruter (hop) IP foloseste propria instanta a algoritmului de rutare;
- Fiecare hop IP isi face propriile decizii de rutare.

6.3.2.Forwarding-ul bazat pe FEC (Forwarding Equivalence Class)

Caracteristici:

- Pachetele sunt organizate pe grupuri de pachete care sunt forward-ate in aceeasi maiera (spre aceeasi cale, aplicanule acelasi “tratament”);
- Forwardarea propriuzisa a unui pachet consta in: asignarea pachetului catre un FEC, determinarea urmatorului hop, pentru fiecare FEC.



6.3.3. Forwarding-ul bazat pe MPLS

Caracteristici:

- MPLS utilizeaza FEC;
- Nodurile MPLS asigneaza eticheta (label) fiecarui FEC;
- Forwarding-ul MPLS este facut in mod asemanator atat in switchurile ATM, cat si in rutare. Cu toate acestea, in cazul switchurilor ATM, numarul de ordine din cozile de asteptare sunt date de valoarea etichetei VCI (Virtual Circuit Identifier), pe cand la routere, acest numar de ordine este dat bitii "Exp" din headerul etichetei;
- Switchurile ATM nu au capabilitatea de a analiza headerele de nivel 3 retea;
- Etichetele pot fi distribuite cu ajutorul mai multor protocoale printre care: LDP (Label Distribution Protocol), RSVP (Resource Reservation Protocol), PIM (Protocol Independent Multicast), BGP (Border Gateway Protocol).

6.3.4. Routerele cu comutare de eticheta (Label Switch Routers) LSR

Exista doua categorii de LSR. La marginea retelei, este nevoie de clasificatori de pachete foarte performanti, care pot sa aplice sau sa elimine etichetele respective. Acestea sunt router-ele MPLS de edge – de margine. Cealalta categorie de LSRuri sunt cele de core. LSR-ul de core trebuie sa fie capabile sa proceseze la latimi de banda extrem de mari pachetele etichetate.

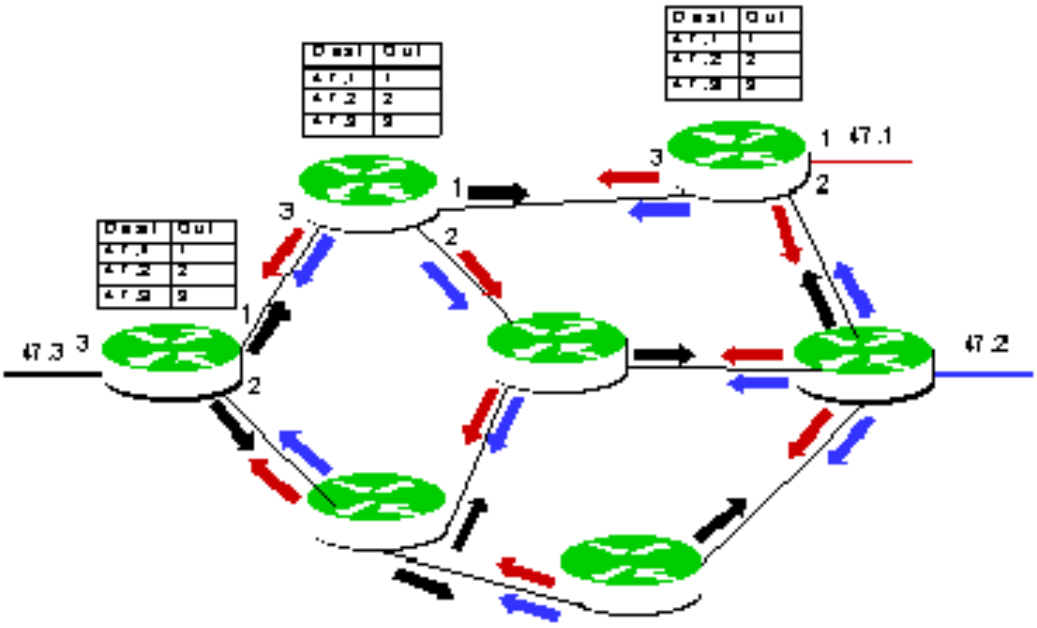
Pot fi realizate din switchuri ATM sau din routere. Routerele LSR "de margine" (Edge-LSR) realizeaza introducerea si extragerea etichetei, atunci cand pachetele patrund, respectiv parasesc reteaua MPLS. Pentru schimbul informatiei de rutare, toate LSR-urile folosesc protocoalele existente de rutare IP. De asemenea toate LSR-urile folosesc LDP.

Formatul etichetei si lungimea acesteia depind de incapsulare, acest lucu va fi negociat de perechile de routere prin interfetele ATM ale acestora.

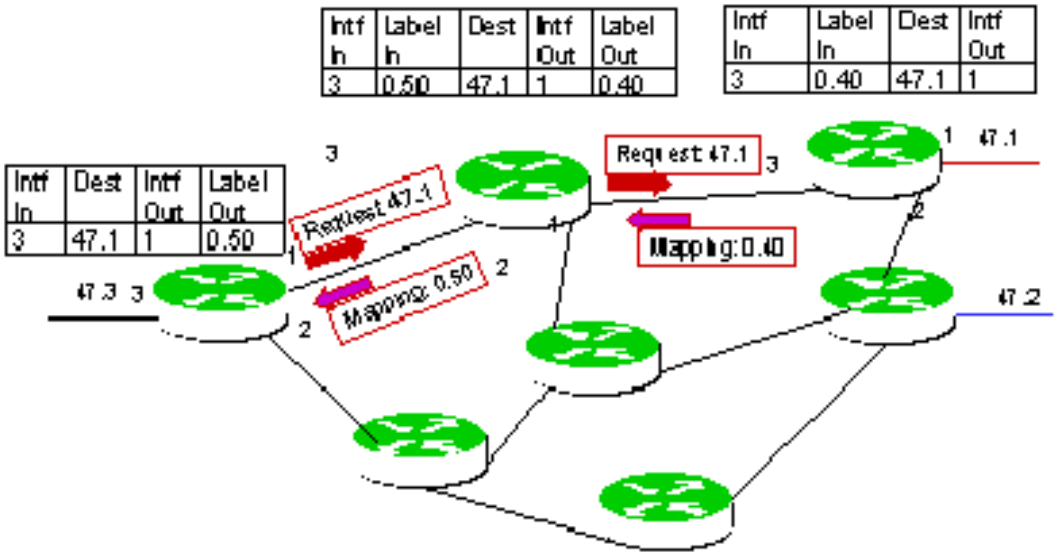
Deasemenea este permisa existenta simultana a mai multor etichete. In acest caz, etichetele sunt ordonate intr-o stiva de etichete (Label Stack).

LSR-urile MPLS executa forwarding-ul pachetelor pe baza valorii etichetei aflata pe prima pozitie din stiva de etichete.

6.3.5. MPLS peste IP standard



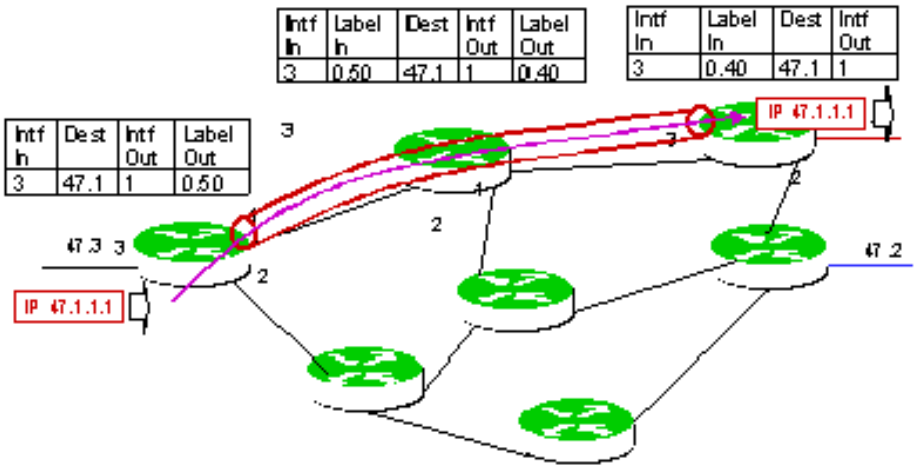
6.3.6. Distributia de etichete LDP



Caracteristicile de baza ale LDP:

- furnizeaza un mecanism de “descoperire” a LSR, pentru a permite LSR-urilor sa se descopere unul pe altul si sa se stabileaca o comunicare intre ele
- Se definesc 4 tipuri de mesaje:
    1. Discovery
    2. Adjacency
    3. Label Advertisement
    4. Notification
- Ruleaza pe protocolul TCP (cu exceptia Discovery)

6.3.7. Label switched path, LSP



(http://hermes.etc.upt.ro/teaching/tart/; ftp.utcluj.ro/pub/users/tarc/t; www.wikipedia.com)

6.4. Quality of Service

- Multi cred ca QoS este puterea principala a MPLS
- Este o neintelegere
- Comparat cu alti factori (VPN, Traffic Engineering), QoS nu este partea cea mai puternica a MPLS
- MPLS QoS intro retea MPLS este bazat in realitate pe IP QoS
- Acesta se poate motiva prin faptul ca MPLS -ul nu este un end-to-end protocol
- ISP -urile vand servicii IP si nu MPLS.
- Acest lucru insa nu inseamna ca MPLS -ul nu are un rol major in QoS.
- Dinpotriva el poate oferi QoS pe o varietate mare de echipamente (ATM)
- Doua modele de QoS suportate se MPLS
- Integrated Serviced
- Diferentiated Services

6.5. Concluzii

Retelele de tip MPLS satisfac cerintele unei infrastructurei de retea puternice prin oferirea unei solutii standard care satisface urmatoarele

- Creste performantele de dirijare ale pachetelor prin retea:MPLS imbunatateste si simplifica dirijarea pachetelor prin rutere folosind comutarea la nivelul 2.Modelul MPLS este simplu,ceea ce permite o implementare usoara.MPLS creste performantele deoarece inlocuieste rutarea traditionala cu comutare la viteze mult mai mari.

- MPLS asigura scalablitatea retelei:MPLS poate fii folosita pentru a ocoli problemele de congestie care apar in retele tip mesh IP –ATM.

- Asigura integrarea IP-ATM intr-o retea,ofera legatura dintre IP si reteaua ATM,MPLS poate refolosi infrastructura ruter/comutator ATM existenta,realizand interconactarea eficienta a celor doua componenta.

- MPLS permite construirea de retele interoperabile,faciliteaza integrarea IP- over-SONET si trecerea la comutarea optica

- MPLS ajuta la construirea de VPN scalabile cu garantarea calitatii traficului Qos

6.6. Referințe Bibliografice:

- *http://hermes.etc.upt.ro/teaching/tart/*

- *ftp.utcluj.ro/pub/users/tarc/t*

- *www.wikipedia.com*

- *http://www.ietf.org/html.charters/mpls-charter.html*

- *http://www.mpls-experts.com/default.asp?page=pages/howmplsworks.asp&v=*

7. TEHNOLOGIA VoIP

7.1. INTRODUCERE

VoIP (Voice Over IP) reprezintă un protocol optimizat pentru prin care se pot purta convorbiri telefonice, se pot trimite faxuri, se pot organiza conferințe audio/video peste o rețea bazată pe protocolul IP ce reuşeşete să asigure o anumită calitate a serviciului şi cu un raport cost/beneficii superior.

(http://en.wikipedia.org/wiki/VoIP)

Multe dintre companiile actuale folosesc o rețea de telefonie tradițională, proiectată în jurul PBX-urilor. Un PBX (Private Branch Exchange) este un sistem de telefonie privată în interiorul companiei, care comută apelurile interne între utilizatori - pe linii locale. În acelaşi timp, un anumit număr de linii telefonice externe sunt distribuite între toți utilizatorii. Folosind PBX, costurile telefonice sunt mai mici, deoarece nu mai este necesar să existe o linie telefonică externă separată pentru fiecare utilizator. PBX-ul este conectat la PSTN (Public Switched Telephone Network) pentru apeluri externe către utilizatorii de telefoane fixe sau mobile, sau către utilizatorii dintr-un birou aflat la distanță, care este echipat, de asemenea, cu un PBX. Când compania are foarte mult trafic telefonic între birourile aflate la distanță, o linie închiriată poate reduce semnificativ costurile.

Toate companiile din deține astăzi, de asemenea, o rețea de computere. Calculatoarele din birourile locale sunt conectate într-un LAN, folosind switch-uri LAN. Ruterele conectează acest LAN la Internet sau, printr-o linie închiriată, la birourile aflate la distanță. Folosind tehnologii de securitate ca IPSec sau VPN, utilizatorii aflați în birourile din teritoriu, în birourile de acasă sau cei care călătoresc se pot conecta la Intranetul companiei. În acest mod, ei sunt capabili să folosească aplicații, instrumente şi informații ca şi cum ar fi utilizatori locali. Folosirea a două rețele separate pentru comunicațiile telefonice pe de o parte şi comunicațiile de date pe de altă parte este scumpă şi redundantă.

Folosind telefonia IP, apelurile telefonice interne sunt menținute local şi au loc prin LAN-ul companiei, necesitând numai o infrastructură de rețea pentru apeluri locale. În acelaşi mod, apelurile între filiale diferite pot avea loc prin infrastructura existentă de rețea IP folosită pentru comunicațiile de date. În fine, apelurile către utilizatorii externi cu telefoane tradiționale sunt rutate pe rețeaua telefonică publică (PSTN) tradițională. Această arhitectură de rețea este bazată pe modelul Cisco AVVID Arhitecture for Voice, Video and Integrated Data.

("A Systematic Approach to Understanding the Basics of Voice Over IP – Voice over IP Fundamantals" – Cisco Press, 2000 - editia pdf - paginile 34-35, 38-39
http://www.cisco.com/global/RO/media/smbcube/techsols_eseminars/VoIP.swf

O soluție de telefonie IP necesită de obicei trei tipuri de componente de rețea: un **Voice Gateway**, **software-ul Call Manager** şi **telefoane IP**. Voice Gateway conectează rețeaua locală la rețeaua tradițională PSTN, astfel încât comunicarea telefonică sa fie posibilă între telefoanele IP şi telefoanele externe tradiționale. Acest rol poate fi îndeplinit, de asemenea, de un ruter special. Switch-urile LAN care pot comuta atât traficul de voce cât şi pe cel de date, folosesc tehnologia Quality-of-Service, pentru a asigura transmisia de voce clară şi de înaltă calitate prin rețea. Software-ul Call Manager oferă servicii specializate, centralizate pentru procesarea vocii către telefoane,

gateway-uri şi servicii adiţionale. El acţionează ca un nucleu inteligent al reţelei şi îndeplineşte funcţii ca: administrarea utilizatorilor, servicii de agendă telefonică şi translatarea numărului de telefon într-o adresă IP. În final, telefoanele specializate IP sunt aparatele pe care utilizatorii finali le au pe birouri. Acestea transformă datele în voce şi invers. Există diverse tipuri de telefoane în funcţie de serviciile disponibile. Unele telefoane includ caracteristici suplimentare cum ar fi acces la agenda telefonică, sistem de conferinţă şi chiar acces la informaţii pe web.

http://www.cisco.com/global/RO/media/smbcube/techsols_eseminars/VoIP.swf

7.2. VoIP VERSUS REŢEAUA DE TELEFONIE PUBLICA

7.2.1. DEZAVANTAJELE RETELEI DE TELEFONIE

Cu toate că reţeaua publică de telefonie funcţionează satisfăcător pentru scopul ei iniţial, apare totuşi un nou tip de reţea, unde **vocea este o aplicaţie peste reţeaua de date**. Acest fenomen s-a întâmplat din mai multe motive:

- **Cantitatea de date a depăşit cantitatea de voce, ca trafic primar, în multe reţele concepute pentru voce**. În momentul de faţă, datele se află peste reţeaua care a fost concepută pentru traficul de voce. Ele însă au diferite caracteristici, cum ar fi lărgimea de bandă variabilă şi o nevoie de lărgime de bandă mai mare. În curând, reţelele de voce vor rula peste reţelele de date. Traficul va fi diferenţiat în acel moment prin aplicaţii şi nu prin circuite fizice.
- **Reţeaua publică de telefonie nu poate crea şi lansa servicii destul de rapid**. PSTN-ul este construit pe o infrastructură, unde doar producătorii de echipamente PSTN dezvoltă aplicaţii pentru acel echipament. Este foarte dificil pentru o companie să satisfacă toate nevoile unui client şi de aceea este nevoie de o infrastructură deschisă, unde mai mulţi producători pot pune la dispoziţie diverse aplicaţii. Deci, în reţelele tradiţionale de telefonie serviciile noi nu pot fi introduse sau sunt greu de implementat datorită constrângerilor din felul în care reţelele tradiţionale de telefonie sunt construite.
- **Aplicaţiile D/V/V (Date/Voce/Video) nu se pot executa pe această infrastructură în modul în care este creată acum**. Cu o singură linie analogica (56kb) nu putem avea acces la date (Internet, de exemplu), acces la telefonie şi acces la video. Este nevoie de un acces de bandă largă, cum ar fi DSL-ul (Digital Subscriber Line), cablul sau wireless-ul (reţelele fără fir).
- **Arhitectura reţelei de voce nu este destul de flexibilă pentru a transporta datele**.

("A Systematic Approach to Understanding the Basics of Voice Over IP – Voice over IP Fundamantals" – Cisco Press, 2000 - editia pdf - paginile 24-26)
http://www.cisco.com/global/RO/media/smbcube/techsols_eseminars/VoIP.swf

Este de asemenea important de remarcat că apelurile comutate în circuit necesită un **circuit permanent** de 64Kbps între cele două echipamente telefonice. În momentul convorbirii între două persoane, conexiunea de 64kbps nu poate fi folosită în alte scopuri. Când se vorbeşte, toţi cei 64Kbps a lărgimii de bandă sunt folosiţi, iar când este linişte şi nu se vorbeşte, se consumă în continuare tot 64Kbps. Orice ar face cele două persoane, atât timp cât linia este ocupată, se ţin ocupaţi şi cei 64Kbps. Dacă un comutator pică sau cineva taie fibra, apelul ia sfârşit.

Companiile de telefonie au mers drum lung pana au putut oferi servicii de tipul apel în aşteptare, căsuţă vocală sau robot telefonic. Dar aceste servicii nu se pot integra în reţeaua locală de

acasă sau de la locul de muncă. Aceste servicii sunt „blocate” pe comutatorul companiei de telefonie. Aici intervine VoIP, care este un standard deschis noilor implementări. Pentru VoIP, oricine poate crea propria aplicație, pentru a manevra apelurile de voce într-un mod particular. Acest lucru nu ar fi posibil pe telefonul de acasă sau pe PBX-ul de la locul de muncă. Sistemele de telefonie tradițională sunt sisteme închise, care nu permit (cel puțin nu uşor) sa fie create aplicații terțe.

(“A Systematic Approach to Understanding the Basics of Voice Over IP – Voice over IP Fundamantals” – Cisco Press, 2000 - editia pdf - paginile 14,16,18-19)

7.2.2. Diferența între comutarea de circuit şi comutarea de pachete

Modelul de comutare în circuit se „sparge” într-un nou model în care sunt interfețe open-standard. Un nivel va purta vocea (cel fizic), nivelul de control al apelului va fi separat de cel fizic, iar nivelul aplicație va permite crearea unor servicii noi.

Nivelul de infrastructură - Infrastructura comutației de pachete înlocuieşte infrastructura comutației de circuit în acest nou model. Această infrastructură va fi cel mai probabil de tip IP, deşi acest model funcționează chiar şi peste ATM. IP-ul este de dorit, deoarece el transportă pur şi simplu datele cap-la-cap, fără să intereseze conținutul.

Protocolul de transmisiune a datelor în timp real (**RTP-Real-Time Transport Protocol**) a fost proiectat pentru a permite receptorului să compenseze jitter-ul şi nesecvențialitatea, introduse de rețeaua IP. RTP poate fi folosit pentru orice fel de flux de date de timp real, ca de exemplu vocea şi video-ul. RTP defineşte un mod de formare a pachetelor IP care să transporte date izocrone şi cuprinde: informații despre tipul de date transportat, mărci de timp (time stamps), numere de secvența (sequence numbers).

Alt protocol, **RTCP** (**Real-Time Control Protocol***),* este cel mai adesea folosit cu RTP, fapt ce permite transportul unor informații cu privire la calitatea transmisiunii (evoluția jitter-ului, media pachetelor pierdute etc.) şi de asemenea poate conține informații despre identitatea participanților.

RTP şi RTCP nu au nici o influența asupra comportamentului unei rețele IP; ele nu controlează calitatea serviciului în nici un fel. Rețeaua poate pierde, întârzia sau amesteca un pachet RTP la fel ca pe orice pachet IP. RTP nu trebuie confundat cu protocolul RSVP (Resource Reservation Protocol – protocol de rezervare a resurselor). RTP şi RTCP permit receptorilor să compenseze jitter-ul introdus de rețea prin memorarea şi secvențierea potrivită, şi să dea mai multe informații despre rețea, pentru ca utilizatorul să ia deciziile potrivite cu privire la metodele de corecție care trebuie aplicate (redundanța, codecurile cu rată de transfer scăzută şi altele).

RTP este utilizat peste UDP şi IP şi este notat de obicei cu: RTP/UDP/IP.

Astăzi, toate protocoalele de semnalizare VoIP folosesc RTP/UDP/IP ca mecanism de transport pentru traficul de voce.

În rețelele IP, pierderea de pachete nu este ceva anormal. De fapt, TCP/IP a fost conceput pentru a se folosi de pierderile de pachete şi în acest fel să controleze fluxul pachetelor. Daca se pierde un pachet, acesta este retransmis. ITU-T recomandă că o întârziere bidirecțională să nu fie mai lungă de 150ms. În rețelele Cisco VoIP, această întârziere este maxim 120ms.

Unul din cele mai importante avantaje ale IP-ului este ca rețelele IP pot converge bazându-se pe cea mai buna rută. Înseamnă de asemenea că există posibilitatea ca vocea (pachetizată în IP) să ia mai multe căi pentru aceeaşi destinație.

Nivelul de control – În prezent, H.323 este cel mai folosit protocolul de control al apelurilor. H.323 nu este însă văzut ca fiind foarte robust pentru rețelele PSTN. Pentru aceste rețele sunt folosite alte protocoale, cum ar fi MGCP (Media Gateway Control Protocol) şi SIP (Session Initiation Protocol).

Nivelul aplicație – Fără aplicațiile corespunzătoare, infrastructura rețelei este construită degeaba.

("A Systematic Approach to Understanding the Basics of Voice Over IP – Voice over IP Fundamantals" – Cisco Press, 2000 - editia pdf - paginile 26-30)

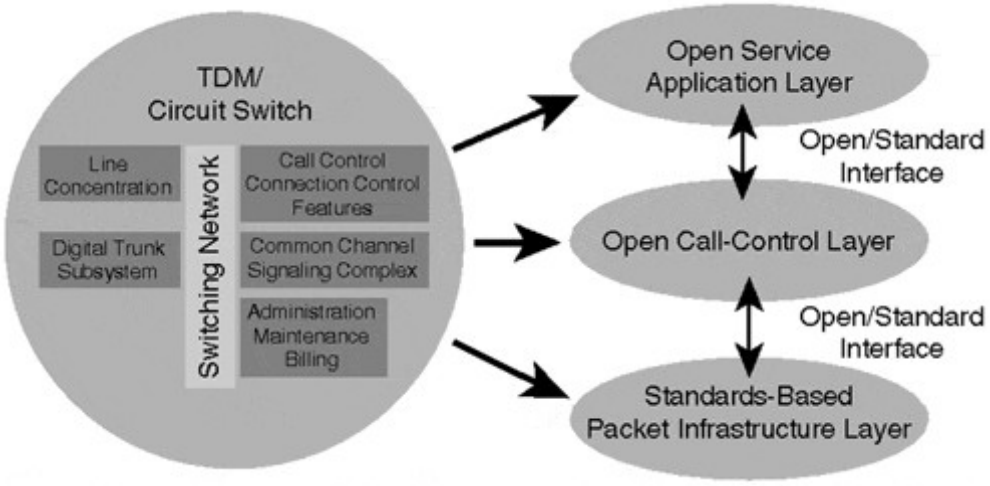


Figura 1 - ***("A Systematic Approach to Understanding the Basics of Voice Over IP – Voice over IP Fundamantals" – Cisco Press, 2000 - editia pdf - pag 27)***

Figura schematizează interacțiunea dintre cele trei nivele (layere): de control, de aplicație şi de infrastructura

7.2.3. AVANTAJE VoIP

Primul şi probabil cel mai important avantaj este o **reducere semnificativã a costurilor**, deoarece acum este nevoie ca doar o singură rețea să fie cumpărată şi administrată, iar costurile de comunicații sunt mult mai mici. În Statele Unite, unde costurile telefonice sunt deja mai mici decât în Europa, companiile care folosesc telefonia IP pot să îşi reducă factura telefonicã la 50% sau chiar 30% din suma inițiala. În rețelele tradiționale de telefonie, un producător este selectat pentru a construi întreaga rețea de telefonie, oferind ofertantului de telefonie hardware special, aplicații soft, sisteme de operare proprii, training şi dezvoltarea viitoare a serviciilor. Aceasta leagă ofertantul de telefonie de producător pentru o perioadă lungă de timp deoarece l-ar costa foarte mult pe acesta să înlocuiască echipamentele speciale sau să lase o terță parte să implementeze servicii (echipamentele producătorului sunt speciale şi astfel trebuie mai mult timp pentru o terță parte să dezvolte servicii noi decât pentru echipa de dezvoltare proprie a producătorului). Comparând cu rețelele tradiționale de telefonie, echipamentele de telefonie sunt combinații de echipamente standard de calcul produse în masa şi care sunt astfel mai ieftine decât echipamentul dedicat pe care sunt construite rețelele tradiționale de telefonie. Dar avantajul principal pentru un ofertant de servicii, care construieşte o

infrastructura de telefonie bazata pe IP, este posibilitatea de a folosi producători diverşi pentru a construi diferitele parţi ale reţelei de telefonie, precum şi facilitatea de înlocuire şi adăugare de elemente în rețea. Standardele IP sunt mai deschise şi mai flexibile decât standardele telefonice şi permit ofertantului care are telefonie IP, ca parte a infrastructurii, să implementeze noi facilitați şi noi servicii mai rapid.

Mai mult, Voice-over-IP face posibilă introducerea unor aplicații noi cum ar fi mesageria unificată, centre de comunicații bazate pe web şi a unor capabilități îmbunătățite de servire a clienților. Rețeaua de comunicații integratã devine de asemenea mai uşor administrabilă şi scalabilă, deoarece schimbările, mutările şi adăugările la rețeaua de telefonie IP sunt implementate uşor şi rapid. Caracteristicile şi funcțiile sunt programabile prin interfețe grafice standard pentru utilizatori, în timp ce PBX-urile tradiționale au adesea caracteristici - bazate pe tehnologii proprietare- care sunt dificil de programat şi necesitã contractare cu terți. În final, calitatea sunetului prin telefonia IP disponibilã astăzi s-a îmbunătățit dramatic în ultimii câțiva ani, făcând din Voice-over-IP o tehnologie foarte performanta.

("A Systematic Approach to Understanding the Basics of Voice Over IP – Voice over IP Fundamantals" – Cisco Press, 2000 - editia pdf - paginile 95-96)

Spre deosebire de telefonia tradițională care este limitată la utilizarea, la recomandarea ITU, a schemei de codec G.711 şi de a transporta astfel voce la 64kbps, rețelele de telefonie IP pot utiliza algoritmi de codare sofisticați care permit ca vocea să fie transmisă la rate mai mici precum 32kbps, 16kbps, 8kbps, etc.

Când se face designul unei rețele bazate pe telefonie IP, diferiți parametrii, alții decât cei de securitate şi confidențialitate, trebuie luați în calcul. Aceştia includ:

- **Calitatea vocii** – Fără o calitate corespunzătoare a vocii, soluțiile bazate pe telefonia IP nu pot fi adoptate. Calitatea vocii în telefonia IP este în funcție de mai mulți factori precum latența (întârzierea), jitter-ul (variația întârzierii), pierderea de pachete şi altele. În rețelele de telefonie tradiționale aceste probleme sunt rezolvate de mult sau nu există deloc.
- **Calitatea serviciilor (Quality of service QoS)** – Combinația a mai multor parametrii, calitatea serviciilor este o grijă majoră pentru rețelele bazate pe telefonia IP. Când un abonat doreşte să efectueze un apel, acesta trebuie să aibă rezervată o lărgime de bandă corespunzătoare. Daca au loc transferuri mari de date în acelaşi timp, trebuie prioritizat traficul de voce față de traficul de date pentru a evita cozile, latența sau pierderi de pachete. Chiar daca întreaga rețea este congestionată aceasta nu trebuie să afecteze traficul de voce. Pentru a prioritiza traficul şi a rezerva lărgime de bandă, rețelele bazate pe telefonia IP trebuie să utilizeze soluții bazate pe calitatea serviciilor (*quality of service - QoS*). Din nefericire nu toate soluțiile bazate pe telefonie IP pot menține o calitate a serviciilor (de exemplu telefonia pe Internet).
- **Disponibilitatea** – Situata pe locul al doilea ca importanta în telefonia IP după calitatea vocii, disponibilitatea este un parametru obligatoriu. Disponibilitatea trebuie menținută asemănător cu cea din rețelele de telefonie tradițională. De exemplu o rețea de telefonie tradițională are disponibilitatea 99,999%. Aceasta înseamnă o perioada de nefuncționare de 5 minute pe an. Operatorii de telefonie care doresc să se bazeze pe tehnologia de telefonie IP trebuie să aibă serviciul disponibil exact cum este el azi în rețelele tradiționale 99,999 % din timp.
- **Extensibilitatea** – O rețea bazata pe telefonia IP trebuie să poate fi extinsa pentru a suporta sute de mii de conexiuni/apeluri concurente pentru a păstra posibilitatea de creştere odată cu cererea.

http://en.wikipedia.org/wiki/VoIP
http://www.networkgeneral.com/uploads/files/wp_Implement_VoIP3-crpd.pdf;

("A Systematic Approach to Understanding the Basics of Voice Over IP – Voice over IP Fundamantals" – Cisco Press, 2000 - editia pdf - paginile 107-109)

7.3. DESCRIEREA TEHNOLOGIEI VOIP

7.3.1.PROTOCOLUL IP

Modelul de Referinţă OSI (engl.: Open Systems Interconnection - Reference Model), pe scurt: OSI, al organizaţiei International Organization for Standardization, numită şi ISO, este o structură de comunicare ierarhică foarte des folosită într-o reţea. Modelul OSI foloseşte 7 aşa-numite straturi pentru a transmite şi primi date eficient şi rapid. Fiecare strat are funcţii clar definite. Internetul se bazează pe acest model.

La nivelul 3, în stiva arhitecturala a tehnologiei VoIP se află evident protocolul IP, întrucât ideea elaborării tehnologiei a fost tocmai aceea de a transporta voce peste o reţea care foloseşte la nivelul 3 acest protocol.

Protocolul IP este responsabil pentru livrarea pachetelor (datagramelor) între terminalele implicate în comunicaţie. Este un protocol **fără conexiune**, ceea ce înseamnă că nu stabileşte o conexiune prin reţea înainte de începerea transmisiei. Rezulta aşadar ca acest lucru va cădea în sarcina protocoalelor de nivel superior.

De asemenea, protocolul IP **nu oferă garanţii** în ceea ce priveşte siguranţa livrării, nu efectuează control de flux şi detecţii sau corecţii de erori. Aceasta înseamnă că o datagrama poate să ajungă la destinaţie înaintea uneia trimise înaintea ei, sau după una trimisa după ea, poate ajunge la destinaţie eronata, sau poate să nu mai ajungă deloc. Totuşi, protocolul IP reuşeşte să se achite de sarcina să, aceea de a ascunde nivelelor superioare reţeaua, care pot să îşi îndeplinească atribuţiile independent de configuraţia reţelei, şi practic fără a şti de existenta ei (întrucât protocoalele de deasupra IP-ului sunt cap-la-cap, adică stabilesc comunicaţia direct între terminale).

Este important de reţinut că pentru a transmite voce peste o reţea nesigură, cel mai mult deranjează lipsa de garanţii a IP-ului în ceea ce priveşte păstrarea secvenţialitaţii, deoarece este evident ca este inacceptabil sa se redea segmentele de voce la recepţie în alta ordine decât au fost transmise, dar în schimb se acceptă o pierdere a pachetelor de voce pe un interval de timp de 100ms, sau cu atât mai uşor o eronare a lor. În schimb, faptul că protocolul nu lucrează cu confirmări este chiar un avantaj, deoarece contează foarte mult ca pachetele să ajungă la recepţie intr-un interval de timp critic, mult mai mult decât corectitudinea lor absoluta.

(Note de curs RC – Stefan Stăncescu

http://ro.wikipedia.org/wiki/Protocol_pentru_Internet

http://fpce9.fizica.unibuc.ro/telecom/internet_prot_ip.htm)

7.3.2. Termeni importanti caracteristici VoIP

7.3.2.1. Întârzierea / Latența

Întârzierea sau latența la VoIP reprezintă intervalul de timp, între primul sunet al vorbitorului şi până când ajunge la urechea ascultătorului.

Întârzierea determina apariția a două probleme majore: ecou şi suprapunerea vorbitorilor. Ecoul devine o problema importanta în momentul în care timpul de întoarcere devine mai mare de 50ms. Ecoul este perceput ca o problema semnificativa a calității transmisiei prin rețele, sistemele VoIP trebuie să implementeze echipamente specifice reducerii ecoului.

Suprapunerea vorbitorilor devine semnificativă dacă întârzierea pe o singură cale este mai mare de 250 ms. Întârzierea cap la cap este aşadar restricția majora care influențează întârzierea în rețelele cu comutare de pachete.

Sursele care influențează întârzierea apelurilor VoIP sunt:

- **întârzierea de acumulare (întârzierea algoritmică) –** este datorată necesității grupării eşantioanelor vocale într-un cadru ce va fi procesat de codorul de semnale vocale. Această întârziere este influențata de tipul codorului utilizat şi poate varia de la simpla perioada de eşantionare la (0,125ms) pana la mai multe ms.
- **întârzierea de procesare –** este determinată de procesul actual de codificare şi grupare într-un pachet a eşantioanelor codificate pentru transmiterea prin rețea. Depinde de viteza de procesare precum şi de algoritmul folosit. Frecvent, cadrele codoarelor de semnale vocale multiple sunt grupate într-un singur pachet pentru a evita supra-încărcarea rețelei. De exemplu 3 cadre din G.729, echivalente cu 30ms de convorbire, pot fi grupate şi împachetate într-un singur pachet.

("A Systematic Approach to Understanding the Basics of Voice Over IP – Voice over IP Fundamantals" – Cisco Press, 2000 - editia pdf - pag 120-121)

7.3.2.2. Jitterul

Jitterul este variația între doi timpi de sosire a pachetului. Acesta apare doar în rețelele bazate pe pachete. În aceste rețele, este de aşteptat ca transmițătorul să trimită eficient pachetele de voce în intervale regulate (de exemplu, să trimită un cadru la fiecare 20 ms). Aceste pachete de voce pot întârzia de-a lungul rețelei şi să nu ajungă chiar în acel interval de timp propus. Aceasta diferența între momentul când este aşteptat să sosească pachetul şi când soseşte cu adevărat se numeşte jitter.

Jitterul şi întârzierea totala nu sunt acelaşi lucru, cu toate ca jitterul în exces intr-o rețea de pachete poate creste întârzierea totala. Acest lucru se întâmpla, deoarece cu cat avem mai mult jitter, cu atât trebuie bufferul să fie mai mare, pentru a compensa natura nepredictibilă a rețelei de pachete.

Îndepărtarea fluctuației necesită gruparea pachetelor şi memorarea lor un timp suficient care să permită ajungerea la destinație a pachetelor cele mai lente pentru a fi rearanjate în secvența corecta. Aceasta determina o întârziere suplimentara.

Cele 2 obiective: reducerea întârzierii şi înlăturarea fluctuației au determinat apariția diferitelor scheme de adaptare a mărimii bufferului instabil, pentru a determina timpul necesar eliminării fluctuațiilor în rețea. Această adaptare are scopul explicit de a minimiza mărimea şi întârzierea bufferului instabil asigurându-se simultan un flux de date optim prin rețea.

("A Systematic Approach to Understanding the Basics of Voice Over IP – Voice over IP Fundamantals" – Cisco Press, 2000 - editia pdf - paginile 121-122)

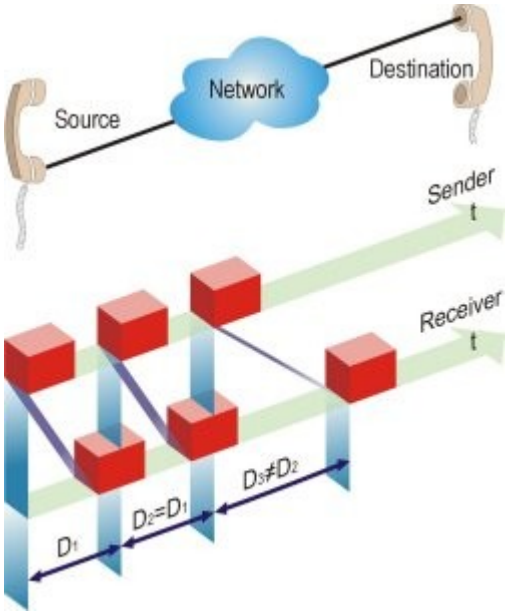


Figura 2 ***(http://archive.evaluationengineering.com/archive/articles/0503voip1.jpg)***

În figura se vede ca timpul necesar ca primele două pachete să ajungă la destinație este D1=D2. Al treilea pachet are însă o întârziere. De aceea avem nevoie de un buffer de jitter.

7.3.2.3. COMPRESIA VOCII

ITU-T a standardizat CELP (Code Excited Linear Prediction Compression), MP-MLQ PCM (Multipulse, Multilvel Quantization) şi ADPCM (Adaptive Differential Pulse Code Modulation) în recomandările sale din seriile G. Cele mai populare standarde de codare a vocii sunt G.711, G.726 / G.727, G.728 / G.729

("A Systematic Approach to Understanding the Basics of Voice Over IP – Voice over IP Fundamantals" – Cisco Press, 2000 - editia pdf - paginile 123-124)

7.3.2.4. ECOUL

Ecoul este un fenomen care poate deveni foarte deranjant în timpul unei conversații. Să ne auzim vocea proprie în receptor în timp ce vorbim este ceva obişnuit, insa să auzim vocea noastră după o întârziere mai mare de 25 ms, este supărător.

Ecoul în rețelele telefonice este datorat reflexiei semnalului transmis, reflexie generata de circuitul hibrid care converteşte semnalul între un circuit cu 4 fire (2 perechi transmițător - receptor) şi un circuit cu 2 fire (o singura pereche transmițător - receptor). Aceste fenomene determină auzirea propriei voci de către persoana care vorbeşte. Ecoul este prezent chiar şi în rețelele telefoniei convenționale cu comutare de circuite. Totuşi este acceptabil deoarece întârzierile din rețea sunt mai mici de 50 ms şi ecoul este mascat de tonul generat de fiecare telefon. Ecoul devine o problema în rețelele care transmit semnalele vocale în pachete, deoarece pentru acestea întârzierea este de cele mai multe ori mari mare de 50 ms. Deci pentru a obține rezultate satisfăcătoare se utilizează

întotdeauna metode de reducere a ecoului. Standardul ITU G165 defineşte cerinţele pe care echipamentele de reducere a ecoului trebuie să le îndeplinească prin specificaţia G.IEC. Ecoul se propaga din reţelele telefonice în reţelele cu comutare de pachete. Echipamentele de reducere a ecoului compara datele vocale recepţionate din reţea cu datele vocale ce vor fi transmise. În reţelele telefonice hibride ecoul este anulat prin intermediul unui filtru digital introdus pe calea de transmisie în reţeaua cu comutare prin pachete.

("A Systematic Approach to Understanding the Basics of Voice Over IP – Voice over IP Fundamantals" – Cisco Press, 2000 - editia pdf - paginile 125-126)

7.3.2.5. PIERDEREA DE PACHETE

Pierderea pachetelor cu informaţii poate fi o problema acuta şi este influenţata de tipul reţelelor utilizate.

Deoarece reţelele IP nu garantează întreţinerea informaţiilor, acestea sunt uzual expuse la o frecventa mult mai mare a pachetelor pierdute decât reţelele ATM. În reţelele IP actuale, toate cadrele cu semnale vocale sunt tratate ca date. În cazul apariţiei unor vârfuri de sarcina sau a aglomerării reţelelor, cadrele vocale vor fi transmise în acelaşi fel ca şi cadrele de date.

Cadrele de date sunt independente în timp deci pachetele pierdute pot fi recuperate printr-un proces de retransmitere. Pachetele vocale nu pot fi tratate în aceeaşi maniera.

Programele utilizate pentru transmiterea vocii prin reţele tratează problema cadrelor pierdute prin diverse metode:

- interpolarea pachetelor vocale pierdute prin reactivarea ultimului pachet primit în intervalul de timp în care se presupune ca s-a pierdut un pachet; aceasta schema este o metodă care umple intervalul de timp dintre cadrele vocale neînvecinate. Se poate aplica cu succes daca frecvenţa cadrelor pierdute este mică.
- Trimiterea de informaţii suplimentare daca se utilizează lăţime de banda mare. Aceasta metodă reproduce şi trimite pachetul "n" de informaţii simultan cu pachetul "n+1". Are avantajul ca este capabila să corecteze exact pachetele pierdute, dar utilizează laţime de banda mare şi determina o întârziere semnificativa în transmiterea datelor.
- Utilizarea unei metode mixte prin folosirea unui codor cu lăţime de banda mai mica pentru a furniza informaţii suplimentare transmise simultan cu pachetul "n+1".Aceasta metoda reduce lăţimea de banda necesara transmisiei, dar nu rezolva problema întârzierii.

("A Systematic Approach to Understanding the Basics of Voice Over IP – Voice over IP Fundamantals" – Cisco Press, 2000 - editia pdf - pag 126-127)

7.3.2.6. DETECŢIA ACTIVITĂŢII VOCII

Când se foloseşte VoIP, banda irosit se poate folosi în alte scopuri, insa doar atunci când detecţia activităţii vocii este activata (VAD – Voice Activity Detection). VAD detectează amplitudinea vocii în decibeli (dB) şi se decide când se va opri trimiterea vocii.

De obicei, când VAD detectează o scădere a amplitudinii vocii, mai aşteaptă un anumit interval de timp pana când opreşte amplasarea cadrelor în pachete. Acest interval de timp este de obicei 200ms. VAD întâmpina insa anumite probleme în determinarea sfârşitul sau începutul unei conversaţii şi în a distinge vocea de sunetul de pe fundal. Acest lucru înseamnă ca daca suntem intr-

o încăpere cu zgomot, VAD s-ar putea să nu poată recunoaşte diferența între sunetul de fundal şi voce. În acest caz, VAD se dezactivează singur la începutul conversației.

("A Systematic Approach to Understanding the Basics of Voice Over IP – Voice over IP Fundamantals" – Cisco Press, 2000 - editia pdf - pag 127)

7.4.PROTOCOALE DE TRANSPORT

Datorita tipului traficului, UDP/IP a fost utilizat pentru a transporta vocea, insa pentru tine pas cu cerintele actuale, s-a folosit pentru trafic în timp real protocolul RTP.

7.4.1. PROTOCOLUL DE TRANSPORT ÎN TIMP REAL (RTP)

Oferă servicii de livrare completa a datelor cu caracteristici de timp real, cum ar fi audio şi video. Aplicațiile de regulă folosesc RTP peste UDP pentru a profita de serviciile acestuia din urmă. RTP suportă transferul datelor către multiple destinații utilizând distribuția multicast oferită de rețea.

RTP nu furnizează nici un mecanism de a asigura furnizarea la timp a pachetelor sau să asigure alte garanții QoS; nivelele inferioare vor oferi toate aceste garanții. Nu garantează livrarea sau prevenirea livrărilor out-of-order (deci nu păstrează secvențialitatea) şi nici nu se bazează pe faptul că rețeaua este fiabilă şi furnizează pachetele în secvență. Numerele de secvență incluse în RTP permit receptorului să reconstruiască secvența de la transmițător. În afară de aceasta reconstituire, cu ajutorul numerelor de secvență se va putea determine locația adecvată a unui pachet (de exemplu în procesul de decodare video), fără a fi necesar să se decodeze pachetele în secvență.

("A Systematic Approach to Understanding the Basics of Voice Over IP – Voice over IP Fundamantals" – Cisco Press, 2000 - editia pdf - pag 130)

7.4.2. PROTOCOLUL DE CONTROL RTP (RTCP)

RTCP transmite periodic de pachete de control către fiecare participant la sesiune, utilizând acelaşi mecanism de distribuție ca cel al pachetelor de date.

RTCP realizează patru funcții:

- Feedback pentru calitatea distribuției datelor
- transportă un identificator de nivel transport pentru o sursă RTP numit „canonical name" sau CNAME. Pentru că pot aparea conflicte, sau restartari de programe, receptorul solicită CNAME pentru a păstra legătura cu ceilalți participanți şi pentru a realiza sincronizarea audio-video
- suportă un număr mare de participanți
- furnizează informații de control al sesiunii

("A Systematic Approach to Understanding the Basics of Voice Over IP – Voice over IP Fundamantals" – Cisco Press, 2000 - editia pdf - pag 131)

7.5. Semnalizarea VoIP

Semnalizarea VoIP este de cele mai multe ori folosită în trei arii distincte: semnalizare de la PBX la ruter, semnalizare între rutere şi semnalizare de la ruter la PBX.

7.5.1. Semnalizarea între rutere şi PBX-uri

Când se face semnalizarea de la PBX la ruter, utilizatorul ridică receptorul şi în acel moment se semnalizează începerea convorbirii. Conexiunea între PBX şi ruter apare ca o linie principala pentru PBX, care la rândul său semnalizează ruterul despre aceasta linie. În momentul în care aceasta linie este descoperită, PBX-ul transmite digiturile formate către ruter în acelaşi mod cum acestea ar fi direcţionate către un switch al unei companii de telefonie sau alt PBX. Interfaţa de semnalizare a PBX-ului spre ruter poate fi una oarecare din metodele din metodele de semnalizare folosite pentru a descoperi o linie principala, cum ar fi semnalizările FXS, FXO, E&M sau T1/E1.

PBX-ul transmite pe urma digiturile formate către ruter, descoperă linia principala către ruter şi transmite digiturile formate. Ruterul mapeaza digiturile formate către o adresa de IP şi iniţiază o cerere de stabilire a unui apel Q.931 spre ruterul la distanta. Între timp, acest canal de control este folosit pentru a iniţia un flux audio RTP, iar protocolul RSVP poate fi folosit pentru a garanta calitatea.

Când ruterul la distanţă primeşte o cerere de apel Q.931, acesta semnalizează o cerere de linie către PBX. După ce PBX-ul confirma aceasta cerere, ruterul transmite digiturile formate către PBX şi semnalizează o confirmare a apelului către ruterul iniţial.

("A Systematic Approach to Understanding the Basics of Voice Over IP – Voice over IP Fundamantals" – Cisco Press, 2000 - editia pdf - pag 172)

("QoS for Voice Over IP Solutions Guide", Cisco Press; editia pdf, pag 49-51)

7.5.2. Protocoale şi standarde

În arhitecturile de reţele fără conexiune, cum ar fi cele IP, responsabilitatea pentru stabilirea sesiunii şi semnalizarea o au staţiile de la cap. De exemplu, un agent H.323 este adăugat la ruter pentru a suporta fluxurile de audio şi de semnalizare. Protocolul Q.931 este folosit pentru stabilirea şi pentru terminarea apelului între agenţii H.323 sau staţiile de cap. H.225 este în principiu acelaşi lucru cu Q.931.

Protocolul RTCP asigura transferul fiabil al informaţiei din momentul în care s-a stabilit fluxul audio. Un protocol fiabil orientat pe sesiune cum ar fi TCP este folosit între staţiile cap pentru a transporta canalele de semnalizare. RTP, care este peste UDP, este folosit pentru transportul fluxului audio în timp real. RTP foloseşte UDP ca un mecanism de transport deoarece are o întârziere mai mica decât TCP şi pentru ca traficul de voce tolerează pierderi mici şi nu poate fi exploata în acest caz retransmisiunea.

Semnalizarea de control H.245 este folosita pentru a negocia capabilităţile şi folosirea canalului. H.245 oferă posibilitatea schimburilor capabilităţilor între staţiile cap, astfel încât să fie stabilite codecurile şi ceilalţi parametri asociaţi apelului între cele 2 capete. În H.245 va fi negociat canalul audio.

H.323 este unul din cele mai răspândite protocoale VoIP în ziua de azi. El este unul din cele mai vechi şi stabile protocoale actuale.

SIP (Session Initiation Protocol) este mult mai recent decât H.323 şi de aceea nu se bucura de o asemenea răspândire ca H.323. Totuşi, datorita scalabilității, interoperabilității şi simplității sale, acesta va deveni tot mai predominant.

("A Systematic Approach to Understanding the Basics of Voice Over IP – Voice over IP Fundamantals" – Cisco Press, 2000 - editia pdf - pag 164-166)

7.5.3. PROTOCOLUL H.323

H.323 este un set de standarde care defineşte componentele, protocoalele şi procedurile necesare pentru a se putea furniza servicii multimedia (audio, video şi date) pe rețele bazate pe IP.

Un sistem H.323 este un ansamblu de componente (hardware şi software) care implementează specificațiile H.323 referitoare la transmiterea de multimedia peste o rețea IP.

- **terminalele H.323**
- **gateway-urile (GW)**
- **gatekeeper-e (GK)**
- **unitățile de control multipunct (MCU-uri)** – controler multipunct (MC) şi procesor multipunct (MP)

Gatekeeper-ele pot lipsi dintr-un sistem H.323, ele fiind componente opționale.

Semnalele audio conțin vorbirea digitizata şi codificata, eventual comprimată. Fiecare din aceste semnale este însoțit de un semnal de control al fluxului audio.

Semnalul video conține imagini în mişcare digitizate şi codificate. Acesta este transmis cu un debit maxim posibil şi este şi el însoțit de un semnal de control al fluxului video.

Semnalele de date pot conține documente, fişiere, etc. Semnalele pentru controlul conexiunii sunt folosite pentru schimbul de capabilități, deschiderea şi închiderea canalelor logice, controlul modului de comunicație şi alte funcții care sunt parte a controlului comunicației. Semnalele pentru controlul apelului sunt folosite pentru stabilirea apelului, eliberarea lui şi alte funcții.

În cazul vocii, terminalul H.323 este în general un telefon IP. În cazul video, terminalul H.323 este un terminal de videoconferință. H.323 este răspândit şi pe calculatoarele personale. O aplicație foarte obişnuită a protocolului H.323 poate fi găsita în software-ul de la Microsoft, NetMeeting, care permite transmisiunea atât a vocii cât şi video.

Gateway-ul realizează conversia între formatele transmisiunilor şi între procedurile folosite pentru comunicație. El se va ocupa de stabilirea apelului şi de închiderea conexiunii atât în partea dinspre rețeaua IP (cu comutație de pachete), cat şi în partea de rețea cu comutație de circuite. Gateway-ul poate efectua şi conversia între formatele folosite în cele doua tipuri de rețele pentru fluxurile audio, video şi de date. În general, scopul unui gateway (atunci când nu operează ca o unitate de control multipunct) este de a ascunde caracteristicile unui terminal LAN pentru rețeaua cu comutație de circuite, şi reciproc.

Un terminal H.323 poate comunica cu un alt terminal H.323 din acelaşi LAN direct, fără participarea unui gateway. Acesta poate fi omis daca nu este necesară comunicaţia cu un terminal din reţeaua cu comutaţie de circuite. Este posibil ca un apel între doua terminale din acelaşi LAN să treacă prin gateway, daca se vrea evitarea unui ruter sau a unei porţiuni din reţeaua IP cu banda prea mică. Gateway-ul poate avea caracteristicile unui terminal H.323 sau unitate de control multipunct (MCU) spre reţeaua IP, şi ale unui terminal sau MCU cu comutaţie de circuite, către reţeaua cu comutaţie de circuite. Alegerea între rolurile de terminal şi MCU este a celui care implementează sistemul.

Este posibil ca un gateway să opereze la începutul unui apel ca un terminal, dar după aceea, prin semnalizări H.245 să devină MCU pentru acel apel care la început a fost punct-la-punct. Gatekeeper-ele ştiu care capete sunt terminale şi care sunt gateway-uri, deoarece acest lucru este specificat când un capăt se înregistrează la un gatekeeper.

La gateway se pot conecta mai multe terminale H.323, deoarece numărul acestora nu este standardizat. De asemenea, numărul de conexiuni către reţeaua cu comutaţie de circuite, numărul de conferinţe independente simultane, funcţiile de conversie în domeniul audio/ video/ date şi includerea funcţiilor pentru legături multipunct nu sunt supuse standardizării.

Un gateway poate fi conectat la un alt gateway printr-o reţea cu comutaţie de circuite, pentru a oferi suport de comunicaţie între doua terminale care nu sunt în acelaşi LAN.

(http://moicane.referate.bubble.ro/prezentare_voip/)

("A Systematic Approach to Understanding the Basics of Voice Over IP – Voice over IP Fundamantals" – Cisco Press, 2000 - editia pdf - pag 164-169)

7.5.4. Session Initiation Protocol (SIP)

SIP (Session Initiation Protocol) este un protocol de control VoIP la nivel aplicaţie, bazat pe codificarea ASCII, care poate fi utilizat la stabilirea, întreţinerea şi terminarea apelurilor între două sau mai multe noduri terminale.

Ca şi alte protocoale Voice over IP, SIP este construit să ofere funcţiile de semnalizare şi administrare a sesiunii din cadrul unei reţele de telefonie bazată pe pachete. Semnalizarea permite transportul informaţiei de apel în perimetrul reţelei. Administrarea sesiunii oferă capacitatea de control a proprietăţilor unui apel capăt-la-capăt.

Caracteristici SIP:

- Suportă rezoluţia adresei, maparea numelui şi redirectarea apelului;
- Determină capacităţile media ale punctului terminal destinaţie: prin protocolul SDP (Session Description Protocol), SIP determină nivelul cel mai scăzut al serviciilor comune între două puncte terminale
- Determină disponibilitatea punctului terminal destinaţie: dacă un apel nu poate fi încheiat din cauza indisponibilităţii punctului terminal destinaţie, SIP determină dacă partenerul apelat este angajat deja într-un apel şi nu răspunde după mai multe încercări. În acest caz, SIP întoarce un mesaj care indică motivul pentru care punctul destinaţie nu a fost disponibil;
- Stabileşte o sesiune între punctele terminale, iniţiatorul şi destinaţia: dacă un apel poate fi realizat, SIP stabileşte o sesiune între punctele terminale. De asemenea, SIP suportă modificări în timpul apelului, cum ar fi adăugarea unui alt punct terminal la o conferinţă sau modificarea caracteristicilor media sau a unui codec;

- Gestionează transferul şi încheierea apelurilor: SIP suportă transferul apelurilor de la un punct terminal la altul. În timpul transferului unui apel SIP stabileşte o sesiune între punctul terminal transferat şi un nou punct terminal (specificat de cel care face transferul) şi încheie sesiunea între punctul terminal transferat şi punctul terminal care a făcut transferul. La finalul unui apel SIP încheie sesiunile stabilite între toți participanții.

7.5.5. Servere SIP

Serverele SIP sunt formate din următoarele echipamente:

- Server proxy - recepționează mesajele SIP şi le înaintează spre următorul server SIP din rețea. Serverul proxy este un echipament intermediar ce primeşte cererile SIP de la un client şi le înaintează în numele clientului. Serverele proxy pot oferi funcții precum autentificarea, autorizarea, controlul accesului la rețea, rutarea, retransmisia în siguranță a cererii şi securitatea.
- Server de redirectare - oferă clientului informația despre următoarea sau următoarele destinații intermediare din ruta unui mesaj. Cu această informație, clientul contactează următoarea destinație server sau direct un UAS.

("A Systematic Approach to Understanding the Basics of Voice Over IP – Voice over IP Fundamantals" – Cisco Press, 2000 - editia pdf - pag 180,181)

7.6. Securitate in retelele VoIP

Securitatea şi confidențialitatea sunt cerințe obligatorii în orice rețea de telefonie. Rețelele bazate pe telefonie IP, introduc probleme de securitate cu care rețelele tradiționale de telefonie nu se confrunta. Factorii de risc asociați cu rețelele bazate pe telefonia IP sunt mult mai mari în comparație cu rețelele tradiționale de telefonie.

7.6.1. Protocoalele de telefonie IP vulnerabile

Protocoale de semnalizare - efectuează managementul sesiunii şi sunt responsabile pentru :

- Localizarea unui utilizator – Posibilitatea de a localiza abonatul apelat
- Stabilirea sesiunii – Posibilitatea de a determina disponibilitatea abonatului apelat cât şi a dorinței sale de a participa la apel. Abonatul apelat poate sa accepte, rejecteze sau sa redirijeze un apel către alta locație sau serviciu.
- Negocierea începutului sesiunii – Posibilitatea părților participante în comunicare de a negocia un set de parametrii care sa fie utilizați în timpul sesiunii, aceştia incluzând tipul codecului, mediului, rata de transfer, etc.
- Modificarea unei sesiuni – Posibilitatea de a schimba parametrii unei sesiuni în timpul unei convorbiri precum codarea audio, adăugarea şi/sau eliminarea unor participanți, etc.
- Terminarea unei sesiuni – Posibilitatea de a termina un apel (şi sesiunea)

Protocoale de transport media - responsabile pentru digitizarea, codarea (şi decodarea), împachetarea, pachetizarea, recepția şi ordonarea vocii şi a eşantioanelor de voce.

(Note de curs RC – Stefan Stăncescu

http://www.networkworld.ro/?page=node&id=2610

7.6.2. Cerințe de securitate în rețele bazate pe telefonie IP

Telefonia IP este foarte interesantă pentru hackeri şi phreakeri. Câteva din caracteristicile telefoniei IP permit unui hacker / phreaker sa încerce sa compromită şi/sau sa controleze diferite aspecte ale unei rețele bazate pe telefonie IP.

Riscurile de securitate ale unei rețele de telefonie IP sunt mult mai mari decât cele ale unei rețele telefonice obişnuite. Sunt combinații ale mai multor factori diferiți care trebuie evaluați înaintea oricăror implementări de rețele bazate pe telefonie IP. Factorii cei mai vulnerabili sunt urmtaorii:

- utilizarea protocolului IP – telefonia IP utilizează protocolul IP ca mijloc de transport pentru voce şi mosteneste toate problemele de securitate ale protocolului IP

- rețelele IP sunt uşor de accesat şi permit mai multor persoane sa exploreze probleme de securitate

- informația de semnalizare şi vocea folosesc aceeaşi rețea – in orice rețea de telefonie IP informația de semnalizare şi vocea sub forma de pachete împart acelaşi mediu de transmisie. În rețeaua clasica de telefonie, singurul loc al rețelei în care semnalizarea şi vocea împart conexiunea este partea de legătura de la abonat către centrala, iar apoi informația de semnalizare este transportata pe o alta rețea separata fizic de voce (rețeaua SS7). În telefonia IP separarea fizica intre informația de semnalizare şi vocea sub formă de pachete nu este disponibila, crescând astfel riscurile de securitate.

- vocea şi datele folosesc aceeaşi rețea – deşi mai multe tehnologii sunt utilizate pentru a separa virtual vocea de date când împart aceeaşi rețea IP, precum *virtual LAN* (*VLAN*), aceste tehnologii şi alte masuri pot fi ocolite şi eliminate, crescând astfel riscul de intruziune.

- nici o autoritate nu controlează mediul IP - în unele cazuri nu este posibila determinarea nivelului de securitate pe care o impun diferiți provideri în rețelele lor bazate pe telefonie IP, făcând aceste rețele sa fie un factor de risc potențial şi un punct de atac rauvoitori

- accesul fizic – în telefonia IP accesul fizic la fire, rețea sau componentele rețelei este considerat un risc major – de exemplu, daca o peroana neautorizata obține acces la un fir care conectează telefonul IP al unui abonat la rețea, atacatorul poate sa efectueze apeluri pe costul abonatului şi sa permită abonatului sa efectueze apeluri fără a interveni interferente.

- informația de semnalizare şi pachetele de voce pot fi capturate (cu echipamente simple în rețea, software specializat, sniffer, etc) alterate, blocate şi modificate.

Atacuri cu succes ale informației schimbate între participanții la apeluri pot duce la:

- Localizarea unui apel, găsirea sursei unui apel şi a găsirea destinației tuturor numerelor formate
- Capturarea unui apel, dirijarea unui participant sau a unor participanți la un apel către un nod care nu reprezintă destinația inițiala
- Probleme de disponibilitate (denial of service)
- Breşe de confidențialitate (posibilitatea de a înregistra o conversație, apartenența la o conversație accidentala, etc)

http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safip_wp.pdf
http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf
http://www.networkworld.com/reviews/2004/0524voipsecurity.html

7.7. CONCLUZII

Tehnologia Voice Over IP a revolutionat modul in care oamenii comunică. Dezvoltarea VoIP a insemnat in primul rand una din primele strategii complete prin care erau unificate elementele de voce, date si comunicatii video.

Adoptarea sistemului VoIP precum si a aplicatiilor corelate s-a dezvoltat rapid, numai in anul 2006 s-a reportat un trafic de peste un miliard de minute de telefonie IP, dintre care aprox. 382 milioane – convorbiri locale, 614 milioane convorbiri la distanta si aproape 83 milioane convorbiri internationale (conform iLocus, care afirma ca este singurul grup de cercetare capabil sa monitorizeze şi sa măsoare astfel de date). Prognozele pentru 2008 estimează că doar in SUA vor exista aproximativ 24 de milioane de utilizatori.

Avantajele implementarii tehnologiei VoIP sunt evidente: in ultimii doi ani, rezultatele au inceput sa apara si in cadrul aspectelor financiare, integrarea retelelor ducand la scăderea costurilor de investitii şi îmbunatățind productivitatea.

În ultima perioada, organizațiile specializate doresc să creeze strategii unificate ale comunicațiilor. Acestea stabilesc practic un sistem integrat de interfețe pentru toate serviciile de comunicație. În viitor, se doreşte ca pe baza acestui model, să se dezvolte integrarea ambelor componente: real time şi non realtime a serviciilor de comunicare.

Unele din aplicațiile integrate in cadrul strategiei comune de comunicații sunt: tehnologiile VoIP, audioconferința IP, video conferința, mesageria integrata, mesageria instant, blog-urile, chat-urile, toate acestea fiind adunate in jurul unui concept de „legare" a userilor de timp in orice moment.

Elementul intrinsec in cadrul arhitecturii tip „unified communications" il reprezinta Real Time Communications DashBoard (RTCD), ce consta in funcționalitatea a doua elemente: un desktop si software mobil folosit de client prin care se ofera diferite nivele de funcționalitate.

Astfel, folosind aplicatii Web bazate pe limbaje tip XML cum ar fi Web Service Description Language sau Simple Objects Acces Protocol se pot realiza schimburi între diferite platforme de aplicații din cadrul organizațiilor.

De asemenea, trebuie să permită integrarea cu celelalte sisteme de management din cadrul organizației iar soluțiille oferite trebuie să se bazeze pe interfețe friendly user. Suplimentar este necesar să se ia in considerare si implementarea noțiunii IPAM (IP address management) în contextul dezvoltarii tehnologiei VoIP. La ora actuală, multe, daca nu majoritatea organizațiilor gestionează manual adresele IP. in condițiile unei dezvoltari continue si tot mai complexe această formă primară de gestiune va fi tot mai greu de realizat. Protocolul IPAM reprezintă noțiuni complexe de voce si date din cadrul unei rețele, prin folosirea recent definitului mecanism ENUM care foloseşte structurile DNS şi sistemele de numerotare telefonice.

În concluzie, VoIP reprezintă un set complex de aplicații de date, voce şi multimedia în cadrul unui număr mare de organizații. Succesul implementării unor astfel de solutii trebuie privit ca o corelare între procesele de performanță, monitorizare şi management proactiv prin VoIP si pentru toate aplicatiile integrate real time din cadrul organizatiei.

http://www.networkworld.ro/?page=node&id=12193
http://www.voip-news.com/blog/20061228/voip-statistics
http://www.webwire.com/ViewPressRel.asp?aId=27988

7.8. Referințe Bibliografice

- *http://en.wikipedia.org/wiki/VoIP*
- *"A Systematic Approach to Understanding the Basics of Voice Over IP – Voice over IP Fundamantals" – Cisco Press, 2000*
- *http://www.cisco.com/global/RO/media/smbcube/techsols_eseminars/VoIP.swf*
- *Note de curs RC – Stefan Stăncescu*
- *http://ro.wikipedia.org/wiki/Protocol_pentru_Internet*
- *http://fpce9.fizica.unibuc.ro/telecom/internet_prot_ip.htm)*
- *"QoS for Voice Over IP Solutions Guide", Cisco Press*
- *http://moicane.referate.bubble.ro/prezentare_voip/*
- *http://www.networkworld.ro*
- *http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safip_wp.pdf*
- *http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf*
- *http://www.networkworld.com/reviews/2004/0524voipsecurity.html*
- *http://www.voip-news.com*
- *http://www.webwire.com/ViewPressRel.asp?aId=27988*

8. CONCLUZII

Ca o concluzie generală a celor enunțate în paginile anterioare ar fi faptul ca cele şapte tehnologii tratate in această lucrare au influențat într-un mod deosebit dezvoltarea rețelei globale de calculatoare, în ultimii ani, Internetul devenind cel mai important mijloc de informare.

La sfarşitul anului 2007 un procent de circa 19% din populația totală a Globului avea acces la Internet, conform statisticii efectuate de **http://www.internetworldstats.com/stats.htm .** Acest studiu relevă amploarea pe care a capatat-o acest mijloc media în ultimii ani.

Dacă Radioului i-au trebuit 38 de ani să ajungă la un nivel de acoperire foarte ridicat şi Televiziunii aproximativ 13 ani, Internetul a câstigat acest teren în numai 4 ani.

Statisticile arată că într-un viitor nu foarte îndepartat, acoperirea globală a Internetului va creşte foarte mult, direct proporțional cu creşterea numărului utilizatorilor de calculatoare, creştere ce poate fi asemanată cu creşterea numărului de tranzistoare din interiorul circuitelor integrate, dată de legea lui Moore.

La baza acestui succes social al comunicațiilor Internet, stau foarte multe inovații tehnologice fără de care Internetul ar fi fost şi în ziua de astăzi o poveste.

De la cablul de cupru întins de-a lungul Atlanticului în 1866 şi până în prezent, tehnologia a evoluat într-un ritm foarte alert. Ceea ce în urmă cu 20-30 de ani părea de domeniul fantasticului pentru orice om, fie el om de ştiință sau un simplu consumator, în prezent, lucrurile imaginate în trecut sunt accesibile pe piață, cu un cost rezonabil, astfel încât majoritatea populației globale poate avea acces la ultimele inovații în materie de telefonie mobilă sau automatizări şi calculatoare.

Toate aceste lucruri au fost posibile numai datorită studiilor şi cercetării amănunțite a oamenilor de ştiință ai secolului trecut, ai prezentului şi de ce nu, ai viitorului. Progresul tehnologic este inerent. Societatea actuală prezintă o serie de necesități ce nu pot fi neglijate. Astfel, se caută dezvoltarea de tehnologii care să poată satisface aceste nevoi şi mai ales de a oferi servicii de calitate, performante, fără depuneri de efort suplimentare din partea consumatorului, toate la un preț redus şi competitiv.

In materie de tehnologii dedicate comunicațiilor Internet, viitorul apropiat rezervă o serie de îmbunătățiri semnificative, nu numai în domeniul rețelelor clasice dar mai ales in domeniul rețelelor wireless.

9. Referințe Bibliografice

1. 802.11 ® Wireless Networks: The Definitive Guide, published by O`REILLY, 2002 by Matthew Gast

2. www.wikipedia.org

3. www.ieee.org

4. www.oreilly.com

5. Note de curs Metode Criptografice – prof. dr. ing. Adriana Vlad – U.P.B.

6. www.wi-fi.org

7. CCNA Exam Prep 2 Exam 640-801

8. www.cisco.com

9. Burstein, Dave (2002). DSL. John Wiley and Sons, New York. ISBN 0-471-08390-9. pp 53-86

10. Lechleider, Joseph, High Bit Rate Digital Subscriber Lines: A Review of HDSL Progress, IEEE Journal 9:6 (August 1991) pp 769-84

11. B. Lee, J.Cioffi, et al, Gigabit DSL, IEEE Transaction on Communication, Sep, 2007, pp 1689-1692

12. www.rad.com

13. Cisco CCNA 4

14. http://hermes.etc.upt.ro/teaching/tart/

15. www.mpls-experts.com

16. www.ietf.org

17. A Systematic Approach to Understanding the Basics of Voice Over IP – Voice over IP Fundamantals" – Cisco Press, 2000

18. Note de curs RC – Stefan Stăncescu

19. "QoS for Voice Over IP Solutions Guide", Cisco Press

20. www.networkworld.ro

21. http://www.voip-news.com

22. www.webwire.com

23. www.networkworld.com