Noutati si tendinte în domeniul retelelor de calculatoare

Asist.dr. Razvan ZOTA
Catedra de Informatica Economica, A.S.E. Bucuresti

Progresele tehnologice impresionante înregistrate în ultimele doua decenii în domeniul calculatoarelor si, în special, în domeniul comunicatiilor dintre acestea, au condus la o crestere spectaculoasa a dezvoltarii retelelor de calculatoare. Pornind de la retele locale (LAN), retele de arie întinsa (WAN) sau metropolitane (MAN) si pâna la retele de sateliti, aceasta crestere s-a datorat nevoii de comunicare si a folosirii unor metode pentru aceasta mai performante din punct de vedere al timpilor de asteptare, al fiabilitatii legaturilor si al securitatii datelor.
O importanta deosebita în dezvoltarea retelelor a avut-o, desigur, Internet-ul, aceasta "retea a retelelor", care a oferit oricui posibilitatea accesului la o baza de date mondiala prin intermediul careia se pot accesa documente, informatii de diverse tipuri, se poate comunica cu orice persoana de pe planeta daca si aceasta are acces la Internet. Tendintele din domeniul retelelor de calculatoare cuprind diverse aspecte, cum ar fi: aparitia si dezvoltarea de noi protocoale si medii de comunicatie ce permit viteze de transport de ordinul Gigabitilor/sec, dezvoltarea fara precedent a comunicatiilor fara fir deosebit de necesare utilizatorii mobili, dezvoltarea retelelor de sateliti, a accesului la distanta în scopul unor operatiuni de comert electronic sau pentru diverse tranzactii electronice on-line.
Cuvinte cheie: *retele de calculatoare, trafic IP, Internet, retele private virtuale, IP-mobil, QoS (calitatea serviciilor), Gigabit Ethernet.*

Noutati în domeniul traficului IP, tehnologiei ATM si cresterii calitatii serviciilor Internet

Dezvoltarea continua a pachetelor de servicii oferite pe Internet duce totodata la sporirea calitatii acestora prin intermediul celor care le ofera. Astfel, furnizorii de servicii Internet pretind faptul ca începând din acest an retelele vor îngloba o serie de clase de servicii de date împreuna cu o crestere substantiala a calitatii acestor servicii.
În plus fata de cele doua optiuni disponibile în prezent, si anume:

- Perfectionarea dirijarii IP pe baza îmbunatatirii continue a capacitatii retelelor de a asigura calitatea serviciilor din fiecare clasa si
- Tehnologia ATM, ce constituie un mediu creat special pentru asigurarea latimii de banda si a calitatii serviciilor (QoS – Quality Of Service) pentru retelele Internet,

pretentiile anilor urmatori constau în suprapunerea pachetelor IP peste retelele de comutatie ATM si SONET, fapt ce elimina toate trecerile prin ruterele existente pentru fiecare pachet transmis, precum si timpul necesar conversiei pachetelor în celule ATM.
Cele doua standarde competitive existente pentru transportul IP peste retele ATM sunt **MPOA** (**M**ulti**P**rotocol **O**ver **A**TM) si **MPLS** (**M**ulti**P**rotocol **L**abel **S**witching). Primul standard foloseste conceptul de server pentru dirijare descentralizata iar cel de-al doilea standard utilizeaza inteligenta distribuita, având drept sustinatori pe CISCO, colosul ce detine 80% din piata mondiala de rutere, precum si firma Alcatel. Un avantaj al utilizarii celor doua standarde este acela ca pachetele care traverseaza retelele ATM sunt capabile sa foloseasca avantajele calitatii serviciilor, ce sunt integrate în ATM.
Odata cu aparitia spectrului QoS s-a modificat fundamental ideea latimii de banda în Internet, astfel încât nu mai exista, practic, posibilitatea producerii congestiilor. La nivel fizic apare noua tehnologie **DWDM**

(**D**ense **W**avelegth **D**ivision **M**ultiplexing) ce multiplica capacitatea de transport a fibrei optice. Operatorii folosesc în comunicatii atât modelul ATM cât si DWDM, dar se observa o renuntare a unora dintre acestia la ATM si SONET si adoptarea insertiei directe a protocolului IP în multiplexoare compatibile DWDM, ceea ce duce la o crestere semnificativa a latimii de banda.

În general, QoS are nevoie de doua componente greu de implementat: semnalizarea si firele de asteptare. Semnalizarea permite unui flux sa semnaleze propriile cerinte; în acest sens exista pentru IP protocolul **RSVP** (**R**e**S**ource reser**V**ation **P**rotocol), însa acesta rezolva doar jumatate din problema deoarece gestioneaza doar cererile de la receptor, fara a oferi ajutor pentru determinarea traseului si a sirului utilizat pentru un flux. Pentru a putea oferi nivele de calitate a serviciilor, fiecare ruter sau comutator ce prelucreaza un flux trebuie sa mentina viteza si întârzierea garantata.

Pentru a garanta viteza trebuie sa existe atât un sir prioritar cât si o cale pentru a se asigura ca nu este supraîncarcat cu clienti. Acest lucru trebuie facut însa prin intermediul stocarii de catre comutatoare a informatiilor de stare pentru fiecare flux, ceea ce este total necunoscut protocolului IP. Daca un comutator nu stie când a trimis ultimul pachet pentru fiecare flux, rezulta ca nu poate sa-l planifice pe urmatorul. Lipsa unei informatii de stare la nivel de flux individual face sa nu existe garantii pentru întârzieri, deci nu poate exista nici calitate audio sau video.

Toate propunerile pentru IP QoS au evitat stocarea informatiei de stare peste IP, asigurându-ne ca adevarata calitate a serviciilor nu poate fi realizata, cel putin deocamdata. Firma AT&T a lansat anul acesta un nou serviciu IP de tip FRS ce îmbina calitatea deosebita QoS a tehnologiei FRS cu flexibilitatea arhitecturala a protocoalelor de retea Internet si Internet2. Acest serviciu este dezvoltat împreuna cu CISCO pe baza tehnologiei MPLS, despre care am discutat anterior, care este proiectat astfel încât sa permita retelelor IP sa atinga aproape acelasi nivel de QoS la fel ca si retelele traditionale bazate pe FRS. În momentul trecerii unui pachet prin retea, fiecare ruter trebuie sa ia doua decizii: una de dirijare si una de îndrumare. Protocolul MPLS efectueaza decizia de dirijare si apoi creeaza o eticheta ce defineste traseul pe care pachetul îl va urma prin reteaua bazata pe IP. Apar astfel câstiguri de timpi pe care fiecare ruter i-ar fi necesitat pentru a efectua decizia de dirijare pe tot parcursul traseului.

În acest sens, singura diferenta între calitatea serviciilor oferita de o retea bazata pe IP si una FRS este aceea data de timpul pe care îl necesita primul tip de retea pentru a efectua cercetarea initiala a traseului IP. Se rezolva, de asemenea, o problema a FRS-ului, aceea ca pentru a dezvolta o retea FRS complet întretesuta clientul trebuie sa defineasca un circuit virtual permanent (PVC – Permanent Virtual Circuit) între oricare doua noduri ale retelei.

Noi protocoale IP

Comertul electronic reprezinta în ziua de astazi o realitate din ce în ce mai pregnanta, cu toate ca lipsa unei infrastructuri adecvate face ca în România acesta sa fie practic inexistent. În ciuda acestor inconveniente, exista deja pionieri în domeniu si la noi în tara. Implementarea comertului electronic a dus la aparitia unor protocoale IP ce vin sa-l consolideze. Aceste protocoale se împart în doua mari categorii:

- Protocoale pentru securizare în scopul oferirii sigurantei comertului electronic prin intermediul Internetului;
- Protocoale pentru confidentialitate care gestioneaza modul de folosire a masivelor de date colectate despre clienti.

Protocoale pentru securizare

- Protocolul **TLS** (Transport Layer Security) reprezinta baza pentru taskuri simple ce permit codificarea informatiilor de pe cartile de credit pentru a fi transmise prin WWW si asigurarea ca tranzactiile prin Internet nu pot fi interceptate de diversi terti.

Acest protocol este de fapt versiunea IETF (Internet Engineering Task Force), neutra fata de orice vânzator, a protocolului **SSL**[1] (Secure Sockets Layer) de la Netscape, la care s-a adaugat un sistem de management pentru certificare digitala si integritate a datelor. Acesta este un protocol tip deschis (open-ended) de nivel înalt, ce permite o mare scalabilitate prin adaugarea de noi tehnologii pentru autentificare si codificare/decodificare în versiunile ulterioare.

- Protocolul **SET** (**S**ecure **E**lectronic **T**ransaction) reprezinta un protocol standardizat ce ofera un canal securizat pentru comunicatii între consumatori si furnizorii de bunuri si servicii prin Internet, incluzând si semnatura digitala a consumatorului pentru certificarea achizitiei.

Acest protocol include în plus fata de TLS semnatura digitala certificata, ceea ce conduce implicit la scaderea ratei de frauda. Consumatorii sunt protejati deoarece numerele cartilor de credit nu mai sunt cunoscute de catre vânzatori, deci baza de date cu numerele cartilor de credit de la comerciant dispare si, în consecinta, dispare si riscul ca aceasta sa fie desconspirata de catre hackeri.

Protocoale IP pentru confidentialitate

- Protocolul **P3P** (Platform for Privacy Preferences) este rezultatul partial al unui efort al consortiului W3C si ofera o platforma pentru tranzactii on-line credibile, ce permit preferinte foarte diverse, pornind de la norme culturale pâna la medii legislative foarte diferite.
- Protocolul **OPS** (Open Profile Standard) completeaza P3P si ofera mediul pentru stocarea sigura a informatiilor profilului utilizatorului, în scopul permiterii schimbului de informatii dintre un utilizator si un serviciu on-line, împreuna cu protejarea datelor individuale confidentiale.

Dezvoltari în domeniul retelelor de calculatoare fara fir

Odata cu evolutia tehnologiei de productie, domeniul retelelor fara fir se extinde continuu. Exista actualmente sisteme în productie ce ofera 100 Mb/s Fast Ethernet la distante pâna la 2 Km folosind tehnologia microundelor. Ultimile dezvoltari în domeniul interconectarilor între cladiri includ viteze de ordinul gigabitilor prin legaturi fara fir cu tehnologie optica, precum si legaturi multimedia de distanta lunga de tip microunde ce includ un sistem cu 2 porturi autosenzoriale de 10-100 Mb/s Ethernet, un port de 2 Mb/s G703 si un canal de 64 Kb/s pentru date, voce si transmisii video în cadrul aceleiasi legaturi.

Dezvoltarile sistemelor de 2,4 GHz au aratat posibilitatea conexiunilor între cladiri la costuri reduse. Folosind tehnologia bridge într-o retea interna fara fir LAN cu antene montate extern, poate fi stabilita o conexiune de 2 Mb/s. Avându-se în vedere gama larga de antene existente actual, pot fi atinse distante de pâna la 8 km punct-la-punct. Exista, de asemenea, o serie de dezvoltari în tehnologia fara fir PCMCIA ce permit transmisii la 2,4 GHz în acelasi mod clasic al placilor de retea pentru PC, acest lucru permitând o conectivitate mobila pentru utilizatori în roaming.

Aplicatiile mobile de viteza înalta din zilele noastre includ: microbrowsere (trafic Internet, e-mail, ftp, news, alte servicii); aplicatii mobile video si multimedia; sisteme si servicii GPS; recunoasterea vocii si aplicatii "hands-free" pentru utilizatorii aflati în miscare; acces la reteaua privata virtuala a companiei.

[1] SSL este un protocol dezvoltat de Netscape pentru transmiterea documentelor private via Internet. El foloseste o cheie privata pentru codificarea datelor transmise prin conexiunea SSL. Atât Netscape Navigator cât si Internet Explorer suporta acest protocol, în timp ce multe situri Web folosesc acest protocol pentru a obtine informatii confidentiale despre utilizatori, cum ar fi numerele cartilor de credit. Prin conventie, paginile Web ce necesita o conexiune SSL încep cu https: în loc de http:.
Un alt protocol folosit pentru transferul protejat al datelor pe WWW este Secure HTTP(S-HTTP). În timp ce SSL creaza o conexiune sigura de tipul client-server, S-HTTP este conceput sa transmita mesaje individuale sigure. Aceste doua protocoale (ce se completeaza reciproc) pot fi privite ca si complementare, folosind tehnologii diferite; ambele au fost aprobate de IETF ca standarde.

"Fara fir" *(wireless)* nu înseamna doar interfata radio sau latimea de banda disponibila pentru un abonat, incluzând o serie de alte caracteristici importante, precum: fiabilitate, flexibilitate, calitatea serviciilor; micsorarea investitiilor deja facute sau planificate; posibilitatea oferirii unor servicii si aplicatii ce duc la cresterea utilizarii echipamentelor si a beneficiilor; reducerea costurilor.

Retelele de date fara fir nu mai reprezinta de mult doar domeniul filmelor stiintifico-fantastice; odata cu popularitatea pe care au capatat-o telefoanele celulare, explozia Internetului si alte descoperiri înregistrate în tehnologiile de comunicatie fara fir digitale, retelele fara fir au devenit aproape peste noapte o solutie viabila pentru o serie larga de aplicatii din lumea reala.

Noile retele fara fir vor fi construite pe o baza ATM/SONET/Optica cu solutii multi-servicii pentru trunchiuri de retele IP si ATM ce folosesc sisteme de acces fara fir 3G. Serviciile de baza oferite sunt:

– Acces pentru date pâna la 2 Mbps (comert electronic, acces Internet); folosirea IP-mobil[2] pentru utilizatorii ficsi sau mobili din cadrul diferitelor retele;

– Multimedia – Voice over IP (VOIP), H.323.

– Retele private virtuale – abonati din zone fixe sau nu.

Centrul retelei este folosit pentru conectarea statiilor de baza în cadrul retelei cu serverele de acces localizate în apropierea punctelor de iesire sau a nodurilor de servicii pe care le deservesc. Serverele de acces asigura interfata radio specifica protocoalelor folosite si distribuie traficul prin intermediul retelei ATM. Aceste servere pot fi configurate într-o maniera flexibila cu functii de inter-retea pentru voce (incluzând "vocoder-e" sau proxy-uri H.323) si/sau functii de inter-retea pentru date (interfata IP-mobil).

Toate serviciile pentru pachete de date sunt suportate prin intermediul serverelor IP-mobil, care reprezinta rutere IP standard ce ofera suport pentru proceduri de management pentru IP-mobil sau standarde IETF evoluate din acesta. Aceste proceduri vor asigura înregistrarea, autentificarea, autorizarea accesului si transmiterea mesajelor sau apelurilor catre/de la utilizatorul mobil. Ele vor conlucra cu servere de taxare si contabilizare ce vor folosi, de asemenea, proceduri IP evoluate pentru negocierea de servicii si efectuarea platilor.

Furnizorii de servicii mobile încearca sa optimizeze arhitectura retelei prin intermediul unor solutii inter-retea foarte flexibile.

– VOIP (Voice Over IP) wireless ofera posibilitatea înlocuirii PSTN cu retea IP si reducerea costurilor de operare;

– VOA (Voice Over ATM) wireless ofera aceeasi posibilitate a înlocuirii PSTN cu o retea ATM si reducerea costurilor de operare.

Retelele cu sau fara fir bazate pe IP-Mobil vor permite furnizorilor de servicii de telecomunicatii sa ofere tuturor clientilor acces integrat la distanta împreuna cu solutia mobila indiferent de mediul retelelor (wireless, PSTN, ISDN, DSL, etc.).

Ofertele vor fi prezentate sub forma unor servicii variate, începând de la servicii de baza Internet, servicii IP VPN, acces la distanta si roaming între furnizori de servicii Internet. Infrastructurile fara fir de

[2] IP-mobil (Mobile-IP) este un standard în versiune draft pentru utilizatorii mobili la nivel retea. Functionalitatea acestuia este prezentata în RFC 2002-2006 iar alte caracteristici de securitate si suport VPN sunt abordate de RFC 2290, 2344 precum si alte versiuni draft IETF sau TIA. Standardul permite unui nod mobil (laptop, PDA, smart phone) sa-si schimbe locatia fara a fi necesara repornirea aplicatiilor sau terminarea si restabilirea conexiunii, oferind utilizatorilor facilitati de roaming fara a fi nevoie sa-si schimbe adresa IP personala (home IP address) de fiecare data atunci când calatoresc într-un alt loc din aria de acoperire a furnizorului de servicii. În acest mod, IP-mobil ofera mobilitate oriunde si oricând, limitarea fiind doar cea impusa de aria aplicatiei sau de punctele de conexiune disponibile. IP-mobil este folosit pe scara larga în sistemele CDMA 3G (de la firma Lucent Technologies) si se asteapta a fi folosit în comunicatiile prin satelit, LAN sau alte modalitati de transmisiuni ce folosesc pachete de date.

generatia 3 precum CDMA 3G, infrastructurile cablate de acces la distanta si retelele LAN vor fi toate componente integrate ale solutiei. Diversilor utilizatori (profesionisti IT, studenti, diversi angajati, etc.) li se va oferi posibilitatea mobilitatii în cadrul corporatiei, campusului universitar sau al firmei pentru accesul la reteaua privata virtuala prin reteaua LAN, conexiunii dial-up sau sistemelor celulare.

Folosirea standardului IP-Mobil pentru a îmbunatati tehnologia din domeniul retelelor IP mobile va oferi avantajele aduse de evitarea costurilor ridicate, eventuale limitari si nivele de dezvoltare si implementare ale solutiilor bazate pe GPRS.

Solutia se va baza pe IP-Mobil asa cum este el definit în RFC-uri si pentru partea wireless în TIA TR45.6. Arhitectura de baza va cuprinde o infrastructura CDMA 3G, platforme RAS de acces dial-up la retea folosind reteaua telefonica clasica dar care ofera suport pentru functionalitati IP-Mobil, retea LAN cu implementare IP-Mobil pe comutatoarele si ruterele IP din reteaua LAN. Suportul pentru retele prvate virtuale va fi oferit de catre toate tehnologiile de acces.

Lumea comunicatiilor fara fir este o lume aflata în prezent într-o permanenta dinamica, determinata de utilizatorii mobili ce folosesc laptop-uri, PC-uri hand-held, Palm PC-uri sau telefoane mobile ca mijloace de comunicare. În multe cazuri, solutiile oferite de catre comunicatiile fara fir sunt avantajoase (din punct de vedere al serviciilor, calitatii dar si al preturilor) pentru solutii home sau small office-home office (SoHo).

Viitorul cu privire la conexiunile la retea apartine retelelor integrate în fiecare casa (Home Networks) ce dispunde de cel putin doua calculatoare personale. În acest mod, pot fi interconectate, sub controlul unui "Home Management System" (sistem de administrare de casa), pe lânga calculatoare si telefoane celulare sau obisnuite, sisteme audio/video, aparate TV, diverse aparate electronice ce pot comunica cu lumea de afara prin intermediul liniilor telefonice, cablurilor Cat 5 UTP sau a tehnologiilor fara fir.

În domeniul fara fir, standardele existente acum sunt pe cât de frumoase pe atât de confuze, datorita multitudinii lor; în acest sens trebuie sa se ajunga la un consens în viitorul apropiat înainte ca tehnologiile *home networking* fara fir sa ia cu adevarat amploare. Astfel, conform unor estimari ale firmei The Yankee Group, în anul 2003 în Statele Unite ale Americii, retele *home* – de casa – destinate comunicatiilor si divertismentului vor exista în aproximativ 6 milioane de familii. Mediul predominant de legatura va fi linia telefonica în timp ce tehnologia fara fir va detine circa 25% din piata.

Unul dintre standardele tehnologiei fara fir este suita de specificatii IEEE 802.11, care foloseste tehnologia spectrului împrastiat (spread spectrum) DS (direct-sequence) cât si FH (frequency-hopping). Rata maxima de transmisie si într-un caz si în celalalt este de 2 Mb/s, dar exista si o versiune tehnologica IEEE 802.11 ce ofera o viteza de 11 Mb/s. Aceasta tehnologie, dezvoltata inital pentru telefonia celulara, are sanse sa se impuna în domeniul *home-network*.

În acest sens, produse ce opereaza la viteze de 11 Mb/s sub specificatia IEEE 802.11 sunt testate în faza beta de Home Wireless Networks Inc. Produsele se bazeaza pe o tehnica speciala folosita si de compania Lucent Technologies si Apple Computer. De asemenea, compania ShareWave Inc., sustinuta de Cisco Systems, Kyushu Matsushita Electric Co. si Netgear (subsidiara Nortel) doreste sa ofere echipamente cu acelasi caracteristici. Pentru a putea oferi fluxuri video si televiziune de definitie înalta (HDTV), Home Wireless Networks lucreaza la dezvoltarea unei noi tehnologii denumita LST (Layered Space-Time processing) ce va oferi o rata de transfer între 50-100 Mb/s la aceeasi latime de banda ca si sistemele actuale la 11 Mb/s.

Tot în viitor se prevede ca specificatia IEEE 802.11 sa permita transferuri de date în intervalul 6-54 Mbps folosind DMT (Discrete MultiTone) precum si OFDM

(Orthogonal Frequency-Division Multiplexing). Un alt set de specificatii a fost initiat de consortiul HomeRF Working Group si suportat de mai multe companii de comunicatii, majoritatea din America de Nord. Acest consortiu a dezvoltat specificatia de numita SWAP (Shared Wireless Access Protocol), ce foloseste tehnologia de spectru împrastiat FH în banda de 2,4 GHz la o rata de ransfer de 1 Mbps. Produsele ce folosesc aceasta tehnologie se gasesc sub numele de Symphony, existând posibilitatea dezvoltarii unei tehnologii Swap de viteza mai mare (11 Mbps).

Institutul European de Standarde în Telecomunicatii (ETSI) ofera suport pentru doua protocoale wireless – HiperLAN pentru trafic de mare viteza si DECT *(Digital European Cordless Telecommunications)* ce opereaza la viteze mai mici. HiperLAN va fi folosita în viitor ca BRAN *(Broadband Radio Access Networks)* este un set de specificatii pentru retea ce operaza la 5GHz si o rata de transfer de 24 Mbps, suficienta pentru HDTV.

Cel de-al doilea protocol, DECT, opereaza la 1,152 Mbps utilizând frecvente între 1880 si 1990 de Mhz. Echipamentele construite conform acestor specificatii ofera numai comunicatii de voce, existând însa cercetari ale firmei Home Wireless Networks pentru a integra atât voce cât si date în echipamentele compatibile DECT. Cel mai mare transportator de date din Marea Britanie, British Telecommunications, a semnat contracte cu Home Wireless Networks pentru echipamente ce vor fi instalate în casele clientilor.

O alta tehnologie relativ ieftina de implementat este Bluetooth, un set de specificatii destinate domeniului restrâns pentru casa sau birou. Se poate comunica prin intermediul echipamentelor Bluetooth fara ca acestea sa fie dependente de o retea. Primele companii ce au sprijinit acest protocol sunt Ericsson, Nokia si Intel (numele a fost preluat de la un rege scandinav din secolul 10 care a unificat mai multe regate daneze).

Retele private virtuale

O problema permanenta legata de conceptia retelelor este aceea a securitatii datelor, mai ales în contextul actual al conexiunilor uzuale la Internet unde se manipuleaza o cantitate impresionanta de informatii de interes mai mult sau mai putin general. Pentru a folosi Internetul ca "schelet" de comunicatie pentru companie, trebuie sa se asigure aceasta securitate a datelor, având în vedere ca acesta ofera o posibilitate relativ ieftina de conectare în retea a diverselor filiale ale companiei. Prin conexiunea la Internet se asigura conectarea separata a fiecarei filiale a companiei la retea (prin intermediul unui furnizor de servicii Internet) si se minimizeaza astfel costurile implicate de linii dedicate la mare distanta.

Apare astfel notiunea noua de *retea privata virtuala (VPN – Virtual Private Network)* ce reprezinta o solutie prin care se asigura securitatea datelor vehiculate într-un mediu public cum este Internetul. Aceasta securitate poate fi asigurata prin mai multe modalitati, determinând gradul de securitate al VPN. Dupa cum am mai subliniat, motivatia de baza pentru construirea unei astfel de retele este legata de reducerea costurilor legate de comunicatii, deoarece este mult mai ieftin sa se foloseasca o singura legatura fizica comuna pentru servirea mai multor clienti din retea decât sa se utilizeze legaturi separate pentru fiecare client din reteaua privata. Se estimeaza ca se reduc în acest caz costurile cu aproximativ 80% fata de variantele clasice ce foloseau linii închiriate la mare distanta. Un alt avantaj al folosirii retelelor VPN este legat de necesitatea confidentialitatii datelor, nivelul de securitate din retea fiind dat de nivelul de securitate necesar organizatiei ce implementeaza VPN. O alta caracteristica a unei retele VPN este crearea unei retele comune ce uneste toate subretele companiei sau organizatiei respective, subretele aflate la distante mari între ele.

O retea privata virtuala este de fapt o retea în care statiile de calcul comunica prin intermediul unei infrastructuri publice, ilu-

zia fiind aceea ca aceasta comunicatie este dedicata exclusiv acesteia; retelele private virtuale existente ofera o solutie (partiala) atractiva problemelor de retea, însa majoritatea acestora nu suporta înca diferentieri de calitate a serviciilor sau alte tipuri speciale de servicii.

Limitari ale retelelor private virtuale

Cu toate avantajele pe care le ofera, retelele private virtuale au o serie de limitari care se încearca a fi depasite în momentul de fata prin intermediul unei noi abordari, aceea a retelelor private virtuale dinamice, subiect tratat în subcapitolul urmator. Principalele limitari ale retelelor private virtuale sunt urmatoarele:

- Toleranta la erori nu este abordata foarte bine, în sensul ca serverele constituie puncte singulare de cadere. Aceasta înseamna ca daca serverul respectiv cade, întreg sistemul se prabuseste. De exemplu, zidul de protectie nativ NT 4.0 se bazeaza pe un singur server Kerberos pentru autentificarea clientilor. Daca acest server cade, clientii nu vor mai putea avea acces la resurse;
- Zidurile de protectie si subretelele IP nu pot fi adaugate dinamic la o retea privata virtuala;
- Conexiunile punct-la-punct sunt folosite pentru conectarea zidurilor de protectie, acest lucru fiind problematic daca multimea de ziduri de protectie ar fi dinamica. Daca presupunem ca doua multimi de ziduri de protectie F_1 cu n elemente si F_2 cu m elemente, trebuie sa existe $O(n^2)$ conexiuni pentru F_1 si $O(m^2)$ conexiuni pentru F_2. Pentru a realiza conexiunea totala a acestor doua multimi, trebuie stabilite n*m conexiuni. În cazul invers, al îndepartarii din retea a unui numar de m ziduri de protectie atunci trebuie distruse (n-m)*m conexiuni;
- Retelele private virtuale ofera protectie prin intermediul unor tehnici speciale, dintre care: filtrare IP, criptare, proxy-uri software, verificare antivirus, etc, acest lucru adunând o mare functionalitate într-un singur pachet. De regula, ideal ar fi ca utilizatorul sa poata sa discearna mai precis între functionalitatile de care într-adevar nevoie.

Vom prezenta în continuare solutia (de extindere) data de retelele private virtuale dinamice si modalitatile prin care aceasta solutie îsi propune sa îmbunatateasca sistemul de functionare al retelelor private virtuale.

Retele private virtuale dinamice

Motivatie

Utilizarea din ce în ce mai crescânda a Internet-ului a impus cerinte de securitate stricte. Solutiile de securitate ale retelelor de azi sunt, de regula, o combinatie de ziduri de protectie (firewalls) cu retele private virtuale (VPN). Retelele VPN contin în mod tipic subretele private IP securizate fata de lumea exterioara prin intermediul zidurilor de protectie, care sunt conectate printr-o retea completa de legaturi punct-la-punct.

Având în vedere ca legaturile sunt cu acces Internet, acestea trebuie securizate prin criptare pentru a ramâne private. În multe implementari VPN însa, cheile de criptare sunt statice (ramân nemodificate) mult timp, ceea ce face ca cei care intra în posesia acestora sa aiba acces nelimitat la reteaua VPN. Alte chei sunt dinamice, schimbându-se periodic, dar în moduri ce depind de servere centrale a caror cadere sau deconectare poate duce la caderea retelei VPN. Apare astfel nevoia unei retele autoadministrate ce împrospateaza cheile ce pot fi compromise si tine evidenta unei multimi dinamice de masini carora trebuie asigurata protectie. O astfel de implementare de numeste retea privata virtuala dinamica *(Dynamic Virtual Private Network - DVPN)*, ce extinde retelele VPN traditionale cu aceste proprietati. Abordarea retelei DVPN foloseste comunicarea dintre grupuri pentru mentinerea unui context partajat securizat între calculatoarele din reteaua DVPN.

Toate masinile din retea vor avea o cheie de securitate prin intermediul careia toata comunicatia este criptata si semnata, aceasta cheie fiind schimbata de administrator

ori de câte ori este necesar. Accesul la reteaua DVPN este limitat de un mecanism de autorizare si autentificare. Astfel, toate masinile din interior sunt sigure, iar cele din exterior trebuie validate din interior pentru a putea avea acces la reteaua interioara. Comunicarea dintre interior si exterior este securizata de un filtru de pachete; folosirea comunicatiilor de grup permite retelei DVPN sa previna partitionarile sau eventualele fuziuni de retea precum si caderile de legaturi sau de masini. Reteaua DVPN utilizeaza o noua retea IP neutilizata, în care toate masinile au atribuite adrese IP; comunicarea protejata DVPN este facuta prin intermediul acestor adrese. O masina din cadrul retelei DVPN poate "vedea" doar adresele IP din interiorul acestei retele, neputând "vedea", în mod normal, alte adrese.

Filtrul de pachete refuza preluarea pachetelor ce provin de la adrese externe; în acest mod oferindu-se transparenta; aplicatiile pot folosi comunicatii obisnuite IP (socket-uri) si functii fara modificare dar cu o protectie sporita. Ca prim pas în implementarea unei retele DVPN este acela de a restrictiona comunicatia aplicatiilor doar cu cele din interiorul retelei, prin implementarea unei astfel de politici în interiorul filtrului de pachete. Spre exemplu, o aproximare (relativa) a unei arhitecturi de securitate multinivel poate fi construita folosind o multime concentrica de retele DVPN ce folosesc politici ce permit aplicatiilor sa primeasca informatie de la retelele DVPN mai putin sigure si sa poata transmite informatii catre retele DVPN cu un nivel mai înalt de securitate. Aceasta idee ofera o arhitectura DVPN care poate fi mult mai flexibila decât sistemele traditionale VPN.

Spre deosebire de abordari standard VPN, aceasta solutie reface cheile de protectie rapid si dinamic (ori de câte ori este necesar) si creeaza o retea DVPN auto-administrata ce poate supravietui caderilor de sistem si erorilor de retea. O implementare initiala a unui astfel de sistem demonstreaza fezabilitatea acestei abordari, putând fi executata cu modificari minime ale sistemului de operare. În viitor se poate extinde functionalitatea acestei solutii prin oferirea de suport pentru retele DVPN ce au politici de securitate definite si scalare la nivel de retele de arie larga.

Caracteristicile retelelor private virtuale dinamice

- *Management descentralizat.* O retea privata virtuala dinamica nu are un centru unic de management. Daca reteaua privata virtuala dinamica este împartita în subcomponente ca urmare a întreruperii unei legaturi de retea, atunci fiecare componenta este capabila sa se administreze singura, pastrându-si disponibilitatea de a fuziona din nou cu celelalte componente atunci când se restabileste legatura de retea.
- *Participare dinamica în cadrul retelei:* statiile de calcul pot adera (respectiv pot parasi) în mod dinamic la retea. În momentul în care o statie de calcul (ce are o anumita relatie de încredere cu reteaua) adera la reteaua privata virtuala dinamica, ea primeste automat cheia (cheile) de securitate actualizata precum si alte informatii relevante.
- *Necesita putine resurse de sistem:* o retea privata virtuala dinamica nu consuma o cantitate mare de resurse sistem, ceea ce permite chiar sa fie rulate mai multe retele private virtuale dinamice pe aceeasi statie de calcul, implementându-se astfel o securitate multinivel.
- *Tehnologie de criptare a comunicatiei* prin intermediul unei chei secrete partajate. În acest scop se foloseste un mecanism riguros pentru securizarea "prospetimii" cheii de protectie astfel încât doar membrii corespunzatori si autorizati sa o primeasca. Avantajul fata de conexiunile securizate punct-la-punct este acela ca este mai usor sa se lucreze cu adaugari sau înlaturari dinamice de ziduri de protectie. Atunci când statiile de calcul sunt atasate retelei, doar cheia de securitate trebuie transmisa, iar atunci când o statie înceteaza sa mai fie "de încredere", cheia este pur si simplu schimbata, având drept efect înlaturarea statiei respective din retea.

Un model simplu de securitate

Pentru implementarea unei securitati în detaliu, se poate elabora o politica de securitate care sa prevada existenta unor grupuri de utilizatori carora le sunt asociate anumite nivele de securitate. Spre exemplu, în figura 1 este prezentata o companie în care C reprezinta centrul (conducerea bancii), grupul de manageri include centrul (C), M_F si M_I, angajatii sunt A_F, A_{I1}, A_{I2}, A_{I3} – figura 1. Managerii formeaza grupul managerilor M în cadrul caruia poarta propriile discutii. Exista, de asemenea, grupul Financiar si grupul Informatic ce folosesc, de asemenea, propriile retele private virtuale dinamice pentru discutii. Centrul C este un membru al tuturor acestor grupuri, exsitând si un grup ce reprezinta întreaga companie. Retelele private virtuale dinamice sunt folosite pentru a oferi informatii statiilor de calcul autorizate. Fluxul informational trebuie sa curga de la manageri spre angajati; pentru a impune asemenea restrictii se propune un filtru IP pentru a impune o politica pentru comunicatia intra-retea. Un astfel de filtru instalat pe toate statiile de lucru din cadrul companiei va impune o politica de securitate conform tabelului 1.

O asemenea filtrare poate fi eficienta si va preveni scurgerile de informatii de la statiile din M catre statiile mai putin sigure. Apare întrebarea când o statie de lucru ***s*** poate apartine retelei DVPN $\mathbf{R_1}$ si $\mathbf{R_2}$? Raspunsul este: atunci când acest lucru este sigur pentru ambele retele DVPN. Se ataseaza în acest sens un nivel de securitate fiecarei retele DVPN si fiecarei sattii de calcul. Nivelele de securitate sunt elemente ale unei grile unde sunt definite operatiile maxime cât si cele minime. Astfel, ***s*** poate fi membru atât în $\mathbf{R_1}$ cât si în $\mathbf{R_2}$ doar daca nivelul sau de securitate este mai mare sau egal cu $\max(\mathbf{R_1},\mathbf{R_2})$.

Servicii de date gigabit

Managementul retelelor de calculatoare din sistemele informatice de companie sunt puse în fata unor noi confruntari pentru a oferi cele mai bune servicii legate de cele mai recente aplicatii:

– Aplicatiile actuale sunt critice din punct de vedere al influentei pe care o au asupra dezvoltarii afacerilor decât cele care odinioara au dus la necesitatea partajarii fisierelor si aplicatiilor în cadrul unei retele de calculatoare;

– Datorita naturii critice a aplicatiilor, retelele bancare trebuie sa fie mult mai fiabile; timpii de cadere trebuie redusi la zero; oferta de servicii mai bune si mai fiabile trebuie facuta cu o eficienta crescuta, astfel încât managerilor de retea li se cere sa faca mai mult fara cresteri semnificative în bugetul de operatii, a numarului de personal sau a instruirii acestora.

În plus fata de necesitatile cunoscute pentru aplicatiile curente, noile aplicatii aduc noi probleme pentru care se face cu atât mai greu planificarea:

– Noi aplicatii, spre exemplu cele legate de tehnologiile Web, necesita noi abordari prin prisma serviciilor pe care reteaua trebuie sa le asigure.

– Aceste noi aplicatii vor creste convergenta functiilor si datelor de retea spre voce/video/date.

– Totodata, regulile de planificare a traficului ce au guvernat vechea infrastructura de retea sunt fundamental schimbate în cazul noilor tehnologii.

În ultimii ani, au aparut o serie de noi thenologii ce permit crearea unor noi modalitati de construire a retelelor de calculatoare. Astfel:

– Dezvoltarea tehnologica în domeniul Gigabit Ethernet si conectivitatea desktop la 100 Mbps a facut ca latimea de banda desktop sa creasca de ordinul a câteva ori. Costul unui Megabit/secunda s-a micsorat de la aproximativ 25 USD/Mbps la mijlocul anului 1996 la sub 1,25 USD/Mbps în 1998.

– Odata cu cresterea capacitatilor s-au dezvoltat si noi tehnologii de control, în special privind comutarea la nivelul retea si sporirea inteligentei în cazul comutarii la nivelul legatura de date, odata cu cresterea performantelor si scaderea costurilor.

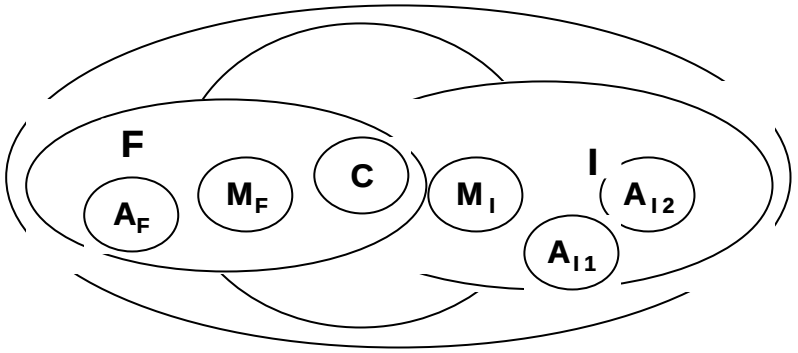

Fig. 1. Un model ierarhic de retea privata virtuala dinamica într-o companie

Reteaua DVPN	M	F	I
M	T	F	F
F	T	T	F
I	T	F	T

Tabelul 1. Un exemplu de politica DVPN (informatiile pot ajunge de la M la M, de la S la M si S si de la P la P si M)

Capacitatile imense disponibile acum (la un pret rezonabil) ofera oportunitatea simplificarii modalitatii de proiectare, constructie si management a unei retele LAN. Aceasta oportunitate în cazul latimii de banda de retea este acum în avans fata de necesitatile aplicatiilor curente; prin aceasta metoda de supra-dimensionare a latimii de banda putem elimina timpul si costurile implicate prin continua slabire a performantelor retelei.

Bibliografie

1. Cisco Seminar Series - Network Solutions for Mid Sized Business, Cisco Systems, San Jose, CA, USA, 1998
2. Mir Rizwan Mustafa - Satellite Data Networks, www.ohio-state.edu, 2000
3. Semeria Chuck - Multiprotocol Label Switching: Enhancing Routing in the New Public Network, Juniper Networks, 1999
4. Theis T.N. - The future of interconnection technology, IBM Journal of Research and Development, 1999
5. George Brendan - Gigabit Ethernet in the LAN and MAN, presentation at Broadband Networking Symposium, Barcelona, 1999
6. Parham Patty - Building IP VPNs, prezentare Cisco Seminar Series, 1998
7. Rodeh Ohad, Birman Ken, Hayden Mark, Dolev Danny - Dynamic Virtual Private Networks, 1998, Cornell University, USA