Universitatea POLITEHNICA din București
Facultatea de Electronică, Telecomunicații și Tehnologia Informației

TEMĂ DE CASĂ
REȚELE DE **C**ALCULATOARE

Quality **o**f **S**ervice

Studenți:
Ciobanu Dragoș, 443A
Mănucă Adrian, 441A
Țulucescu Alexandru, 441A

Prof. coordonator
Conf. Dr. Ing. Ștefan Stăncescu

Cuprins

1)Mecanisme si aplicatii (Ciobanu Dragoș, 443A)
- Definitie
- Calitatile de trafic
- Mecanisme
  - Over-provisioning
  - Protocoale
- Aplicatii

❖ IPTV
  - Avantaje
  - Economie
  - Interactivitate
  - Video la cerere
  - Servicii convergente bazate pe IPTV

❖ VoIP
  - Protocoale
  - Avantaje
  - Calitatea de servicii

❖ iSCSI
    - Adaptoare iSCSI
    - Aplicatii pentru retele de stocare iSCSI

2)Suportul QoS in Windows (Mănucă Adrian, 441A)
- Configurarea serviciului de livrare prioritizata
- QoS in Windows XP si Windows Server 2003
- QoS in Windows Vista si Windows Server 2008
- Crearea si editarea unei politici QoS in Windows 7 si Windows Server 2008 R2
- QoS bazat pe URL in Windows 7 si Windows Server 2008 R2
- QoS in Windows Server 2012.

3)Suportul QoS in Linux (Țulucescu Alexandru, 441A)
- Discipline de punere in coada
- Clase

Ciobanu Dragoș, 443A

Quality of Service

(QoS)

Calitatea serviciilor (QoS) se referă la mai multe aspecte legate de rețelele de telefonie și de calculator ce permite transportul de trafic cu cerințe speciale. În special,multă tehnologie a fost dezvoltat pentru a permite rețelelor de calculatoare să devină la fel de utile ca rețelele de telefonie pentru convorbiri audio, precum și sprijinirea noilor aplicații cu cerințe de servicii mai stricte .

Definiţie

În domeniul telefoniei, calitatea serviciilor a fost definită de către UIT în 1994. Calitatea serviciilor cuprinde cerințe cu privire la toate aspectele legate de o conexiune, cum ar fi timpul de răspuns al serviciilor, pierderi, raport semnal-zgomot, vorbire incrucişată, Echo, întreruperi, răspunsul în frecvență , nivelurile de intensitate, și așa mai departe. Un subgrup de telefonie QoS este gradul de cerințe al serviciu (GS), care cuprinde aspecte ale unei conexiuni cu privire la capacitatea şi acoperirea unei rețele, de exemplu, probabilitatea maximă garantată de blocare și probabilitatea întreruperii .

În domeniul retelelor de calculatoare și alte rețele de telecomunicații cu pachete comutate, termenul de inginerie de trafic se referă la mecanismele de control cu resurse rezervate, mai degrabă decât calitatea serviciilor realizate. Calitatea serviciului este capacitatea de a oferi o prioritate diferită pentru diferite aplicații, utilizatori, sau fluxuri de date, sau pentru a garanta un anumit nivel de performanță la un flux de date. De exemplu, o rată de biți necesară, întârzieri, instabilitate de scurtă durată, probabilitatea de pierdere de pachete și / sau rată de eroare a biților poate fi garantată. Calitatea de servicii garantate este importantă, dacă capacitatea rețelei este insuficientă, în special pentru aplicații în timp real de streaming multimedia, cum ar fi Voice over IP, jocuri online și IP-TV, deoarece acestea necesită de multe ori rata de biți fixă și sunt sensensibile la întârzieri, și în rețele în care capacitatea este o resursă limitată, de exemplu, în comunicarea de date pentru celular.

O rețea sau protocol care suportă QoS pot conveni asupra unui contract de trafic cu aplicația software și capacitatea de rezervă în nodurile de rețea, de exemplu, în timpul unei faze stil sesiune. În timpul sesiunii se poate monitoriza nivelul atins de performanță, de exemplu, rata de date și întârziere, precum și controlul dynamic al priorităților de programare în nodurile de rețea. Se poate elibera capacitatea rezervată în timpul unei faze de tip lacrimă în jos .

O rețea best-effort sau serviciu nu suportă calitatea serviciilor. O alternativă la mecanisme de control complexe QoS este de a oferi comunicare de înaltă calitate într-o rețea best-effort prin supra-provizionarea capacităţii , astfel incât să fie suficient pentru sarcina de trafic în vârf așteptată. Absența rezultată de congestionarea rețelei elimină necesitatea existenței unor mecanisme QoS.

QoS este uneori folosit ca o măsură de calitate, cu multe definiții alternative, mai degrabă decât referindu-se la abilitatea de a păstra resurse. Calitatea serviciilor, uneori, se referă la nivelul de calitate a serviciilor, și anume calitatea serviciu garantat. QoS maxim este adesea confundat cu un nivel ridicat de performanță sau de calitate a serviciilor realizate, de exemplu, rata de biți ridicată, latență scăzută și probabilitate de eroare scăzută a biților.

O definiție alternativă și contestată a QoS, utilizată în special în domeniul serviciilor strat de aplicații, cum ar fi telefonia și video streaming, este necesar privind o valoare care reflectă sau prezice calitatea experienţei subiective. În acest context, QoS este efectul cumulativ acceptabil asupra satisfacerea abonată a tuturor imperfecțiunilor care afectează serviciul. Alți termeni cu înțeles similar sunt calitatea experienței (QoE) conceptul de afaceri subiectiv, necesitatea "performanță percepută a utilizatorului", necesitatea "gradul de satisfacție a utilizatorului" sau vizarea "numărul de clienți fericiți". Exemple de măsuri și metode de măsurare sunt Scor de opinie medie (MOS), Măsura de calitate de vorbire perceptuală (PSQM) și Evaluarea perceptuală a calității video (PEVQ). A se vedea, de asemenea, calitatea video subiectivă.[1]

Calităţile de trafic

În rețelele cu comutare de pachete, calitatea serviciilor este afectată de diverși factori, care pot fi împărțiti în factori "umani" și "tehnici". Factorii omului includ: stabilitatea de serviciu, disponibilitatea serviciului, întârzieri, informații de utilizator. Factorii tehnici includ: fiabilitate, scalabilitate, eficiență, mentenabilitate, gradul de serviciu, etc

Multe lucruri se pot întâmpla pachetelor în timp ce călătoresc de la origine până la destinaţie, rezultând în următoarele probleme din punctul de vedere al expeditorului și receptorului:

Un randament foarte mic

Datorită variaţilor de încărcare de la alți utilizatori care împărtășesc aceleași resurse de rețea, rata de biți (transfer maxim), care poate fi furnizată la un anumit flux de date, poate fi prea mică pentru serviciile multimedia în timp real în cazul în care toate fluxurile de date obțin aceeaşi prioritate de programare .

Pachete pierdute

Routerele s-ar putea să nu livreze unele pachete de date, dacă datele lor sunt corupte sau sosesc atunci când bufferele lor sunt deja pline. Aplicaţia care primeşte poate solicita ca aceste informații să fie retransmise, cauzând eventual întârzieri drastice în transmisia generală.

Erori

Uneori pachetele sunt corupte din cauza erorilor de bit cauzate de zgomot și interferențe, în special în domeniul comunicațiilor fără fir și fire lungi de cupru. Receptorul trebuie să detecteze acest lucru și, la fel ca și în cazul în care pachetul a fost pierdut, poate solicita ca aceste informații să fie retransmise.

Latență

S-ar putea să ia o lungă perioadă de timp pentru fiecare pachet pentru a ajunge la destinație, deoarece este ţinut în cozi lungi, sau să ia o rută mai puțin directă, pentru a evita congestionarea. Acest lucru este diferit de transfer, astfel cum întârzierea poate construi de-a lungul timpului, chiar dacă tranziţia este aproape normală. În unele cazuri, latență excesivă poate face o aplicație, cum ar fi VoIP sau jocuri online inutilizabile.

Instabilitate de scurtă durată

Pachete de la sursa vor ajunge la destinație cu întârzieri diferite. Întârzierea unui pachet diferă în funcție de poziția sa în cozile de așteptare ale routerelor de-a lungul drumului dintre sursă și destinație și această poziție poate varia imprevizibil. Această variație în întârziere este cunoscută sub numele de bruiaj și poate afecta grav calitatea streaming audio și / sau video.

Transferuri de date aleatoare

Când o colecție de pachete conexe este direcționată printr-o rețea, pachete diferite pot avea trasee diferite, fiecare ducând la o întârziere diferită. Rezultatul este acela că pachetele ajung într-o ordine diferită faţă de cum au fost trimise. Această problemă necesită protocoale speciale suplimentare responsabile pentru rearanjarea aleatoare a pachetelor la o stare de izocron odata ce ajung la destinația lor. Acest lucru este important în special pentru fluxuri video și VoIP în cazul în care calitatea este dramatic afectată atât de latenta si lipsa de secvență.[1]

Mecanisme

Circuite de comutare a rețelelor, în special a celor destinate pentru transmisii de voce, cum ar fi modul de transfer asincron (ATM) sau GSM, au QoS în protocolul de bază și nu au nevoie de proceduri suplimentare pentru realizare. Unități scurte de date și conţinut QoS au fost unele din punctele de vânzare unice de ATM-uri pentru aplicații cum ar fi video la cerere.

Atunci când costurile de mecanisme pentru a oferi QoS sunt justificate, clienții de rețea și furnizorii pot intra într-un acord contractual numit Service Level Agreement (SLA), care precizează garanțiile pentru capacitatea unei rețele / protocol pentru a oferi performanțe garantate / tranzitata / limitele latenţei pe baza măsurilor stabilite de comun acord, de obicei prin prioritizarea traficului. În alte abordări, resursele sunt rezervate la fiecare pas pe rețeaua de apel, deoarece este configurat. [1]

Over-provisioning

O alternativă la mecanisme de control QoS complexe este de a oferi comunicare de înaltă calitate supra echipand generos reteaua, astfel încât capacitatea se bazează pe estimări de traffic vârf de sarcină . Această abordare este simplă pentru rețele cu sarcini previzibile de vârf. Performanța este rezonabilă pentru multe aplicații. Acest lucru ar putea include aplicații pretențioase, care pot compensa variațiile de lățime de bandă și întârzierea cu buffere largi de transmitere, care adesea este posibil, de exemplu, în streaming video. Supra aprovizionarea poate fi de utilizare limitată, cu toate acestea, în fața unor protocoale de transport (cum ar fi TCP), care în timp cresc exponential cantitatea de date introdusă pe rețea până când toată lățimea de bandă disponibilă este consumată și pachete sunt pierdute. Astfel de protocoale lacome au tendința de a crește latența și pierderea de pachete pentru toți utilizatorii.

Serviciile comerciale VoIP sunt adesea competitive cu serviciul de telefonie tradițională în ceea ce privește calitatea apelului, chiar dacă mecanisme QoS nu sunt, de obicei, în uz de conexiunea utilizatorului la ISP-ul său și conexiunea furnizorului de servicii VoIP la un alt ISP. În condiții de mare încărcare, cu toate acestea, VoIP se poate degrada la calitatea telefonului celular sau mai rău. Matematica de trafic de pachete de rețea indică faptul că reţeaua necesită doar 60% din capacitate conform unor ipoteze conservatoare.

Cantitatea de supra aprovizionare în legături interioare necesare pentru a înlocui QoS depinde de numărul de utilizatori și cererile lor de trafic. Această utilizare limitată de supra aprovizionare.Mai nou mai multe aplicații de lățime de bandă intensive și adăugarea de mai multe rezultate de utilizatori din pierderea de rețele de supra aprovizionare. Acest lucru necesită o actualizare fizică a legăturilor de rețea relevante, care este un proces costisitor. Astfel, supra aprovizionarea nu poate fi asumată orbește pe internet.

Spre deosebire de un singur administrator de rețele, Internetul este o serie de interconectare a rețelelor de schimb de puncte private. De aici miezul internet este deținut și administrat de o serie de furnizori de diferite servicii de rețea, nu o singură entitate. Comportamentul său este mult mai stohastic sau imprevizibil. De aceea, cercetarea continuă privind procedurile de QoS, care sunt dislocabile în diverse rețele de mari dimensiuni.

Servicii Integrate ("IntServ") pune în aplicare abordarea parametrizată. În acest model, aplicațiile utilizează Protocolul de rezervare de resurse (RSVP) pentru cerere și resurse de rezervă printr-o rețea. Servicii diferențiate ("DiffServ") pune în aplicare modelul de prioritate. DiffServ marchează pachete în funcție de tipul de serviciu care-l doresc. Ca răspuns la aceste marcaje, routere si switch-uri folosesc diferite strategii de așteptare pentru a adapta așteptările la performanță. Marcajele punctului de cod DiffServ (DSCP) folosesc primele 6 biți în domeniul ToS al antetului pachetului IP (v4).

Primele implementări foloseau filosofia serviciilor integrate (IntServ) de a rezerva resurse de rețea. În acest model, aplicaţiile foloseau protocolul de resurse rezervate(RSVP) pentru a cere şi a pastra resursele printr-o rețea. În timp ce mecanismele de IntServ fac munca, sa constatat că într-o rețea tipică de bandă largă al unui furnizor de mai multe servicii, routere centrale ar fi necesare să accepte, să mențină, și să dărâme mii sau, eventual, zeci de mii de camere. Se credea că această abordare nu s-ar scala cu creșterea internetului, și, în orice caz, a fost antitetic la noțiunea de proiectare a reţelelor, astfel încât routerele central să facă ceva mai mult decât să schimbe pachete pur și simplu la rate de transmisie cât mai mari.

Cea de-a doua și curentă, abordare acceptată este de servicii diferențiate (DiffServ). În modelul DiffServ, pachetele sunt marcate în conformitate cu tipul de serviciu de care au nevoie. Ca răspuns la aceste marcaje, routerele si switch-urile folosesc diferite strategii de așteptare pentru a adapta la cerințele de performanță. La nivel IP, marcajele Differentiated Services Code Point (DSCP) folosesc cei 6 biți în antetul pachetului IP. La nivelul MAC, VLAN IEEE 802.1Q și IEEE 802.1p pot fi folosite pentru a transporta în esență, aceleași informații.

Routere care susţin DiffServ folosesc cozi multiple pentru pachetele care așteaptă transmiterea de la interfețe cu constrângeri de lățime de bandă (de exemplu, zona, larga).Vânzătorii de routere oferă capacități diferite pentru configurarea acestui comportament, pentru a include numărul de cozi limită, prioritățile relative ale cozilor, si lăţime de banda rezervată pentru fiecare coadă.

În practică, atunci când un pachet trebuie să fie transmis de la o interfață cu coadă, pachetele care necesită instabilitate redusă (de exemplu, VoIP sau video-conferințe) au prioritate asupra pachetelor în alte cozi . De obicei, o parte din lățimea de bandă este alocată în mod implicit la pachete de control al rețelei (cum ar fi Internet Message Protocol și protocoale de rutare), în timp ce traficul best effort ar putea fi pur și simplu dat, indiferent de câtă lățime de bandă mai rămâne.

La nivelul Media Access Control (MAC), VLAN IEEE 802.1Q și IEEE 802.1p pot fi folosite pentru a transporta în esență, aceleași informații, ca cele folosite de către DiffServ. Teoria modelelelor de cozi de asteptare a fost dezvoltată pe analiza performanței și QoS pentru protocoale de nivel MAC .

Cisco IOS NetFlow și clasa Cisco Based QoS (CBQoS) Baza de management (MIB), sunt comercializate de către Cisco Systems.

În timp ce DiffServ este folosit în multe rețele de întreprinderi sofisticate, nu a fost desfăşurat pe larg în Internet. Aranjamente de peering pe internet sunt deja complexe, și nu pare a fi nici un entuziasm în rândul furnizorilor de sprijinire a QoS peste conexiuni peering, sau un acord cu privire la ce politici ar trebui să fie sprijinite în scopul de a face acest lucru.

Un exemplu convingător de necesitatea a QoS pe internet se referă la ruperea congestiei. Internetul se bazează pe protocoale de evitare a congestiei, astfel construite în Transmission Control Protocol (TCP), pentru a reduce traficul în condiții care altfel ar duce la "colaps". Aplicatii QoS cum ar fi VoIP și IPTV, deoarece acestea necesită rate de transfer în mare parte constante și latență scăzută nu pot folosi TCP și nu pot astfel reduce rata de trafic în alt mod pentru a ajuta la prevenirea congestiei. Limita volumului de traffic al contractelor QoS care pot fi oferite la Internet și să impună, prin urmare, prin aplicarea modelării traficului, care poate împiedica să devină supraîncărcat, și sunt, prin urmare, o parte indispensabilă a capacității Internetului să se ocupe de un amestec de trafic în timp real și traffic în timp virtual, fără colaps.

Protocoale

Protocoalele QoS(Quality of Service) au fost dezvoltate de cand rețeaua de date cere eficiența furnizării datelor. Protocoale cunoscute QoS sunt RSVP, IntServ, DiffServ, MPLS, SBM și așa mai departe. În lumea practică, de cele mai multe timp, vom folosi protocoale DiffServ și bine de ştiut despre MPLS Class of Service, de asemenea.[5]

RSVP

Protocolul de rezervari de resurse (RSVP), este un nivelul de transport destinat să rezerve resurse într-o rețea pentru un Internet de servicii integrate. "RSVP nu transporta date de aplicaţie, ci este mai degrabă un protocol de control al internetului, cum ar fi ICMP, IGMP, sau protocoale de rutare". RSVP furnizează configurarea iniţială a receptorului de rezervare de resurse pentru fluxurile de date multicast sau unicast cu scalarea și robustețea.

RSVP poate fi utilizat de către gazde sau routere fie de a solicita sau de a oferi niveluri specifice de calitate a serviciilor (QoS) pentru de date ale aplicației sau fluxuri. RSVP definește modul în care aplicațiile publică rezervări și modul în care acestea pot renunța la resursele rezervate odată ce necesitatea lor s-a încheiat. Operaţiunea RSVP va rezulta în general în resurse care sunt rezervate în fiecare nod de-a lungul unui traseu.

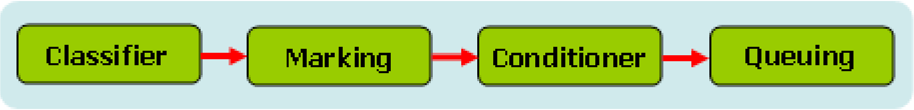
IntServ

Ideea de IntServ este aceea că fiecare router din sistem implementează IntServ, și fiecare aplicație care necesită un fel de garanții trebuie să facă o rezervare individuală. Specificatiile de debit descriu pentru ce este rezervarea, în timp ce RSVP este mecanismul de baza pentru al semnala în întreaga rețea. IntServ sau servicii integrate este o arhitectură care specifică elementele pentru a garanta calitatea serviciilor (QoS), pe rețele. IntServ poate fi, de exemplu, folosit pentru a permite video și sunet să ajungă la receptor fără întrerupere.

DiffServ

Servicii diferențiate sau DiffServ este o arhitectură a reţelei de calculator care specifică un mecanism simplu, scalabil și mecanism măzărat pentru clasificare, gestionarea traficului în rețea și asigurarea calității serviciilor (QoS) garantată în rețele IP moderne. DiffServ poate, de exemplu, să fie utilizat pentru a furniza latenţă scăzută, serviciu garantat (GS) la traficul critic de rețea , cum ar fi voce sau video cât timp se furnizează garanții de trafic simple best-effort către servicii non-critice, cum ar fi traficul de web sau transferuri de fișiere.
DiffServ a înlocuit în mare măsură mecanisme QoS pentru stratul 3 (cum ar fi IntServ) în timp ce routerele de protocol primare folosite pentru a furniza diferite niveluri de servicii.

Cum funcţionează DiffServ :

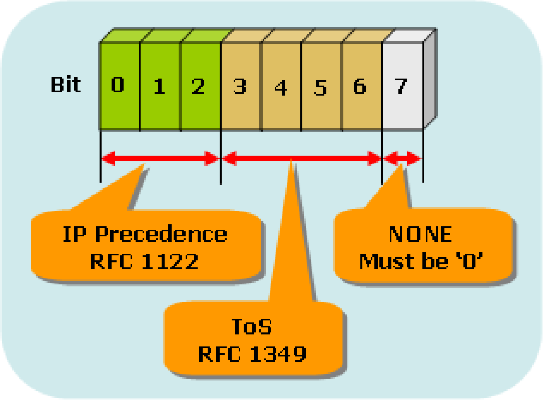


Clasificator
pachete vor fi clasificate în clase definite de ACL și harta clasei.

Marcarea
Aveți posibilitatea să aplicați altă greutate sau politică pe fiecare clasă, prin utilizarea harţii strategice
- precedenţa IP și DSCP au fost folosite pe stratul 3 ,strategii de marcare și 802.1p / Q, FR DE biți, MPLS EXP au fost folosite pe stratul 2.

Precedenţa IP

3 biti sunt folosiţi pentru a face 8 clase diferite.

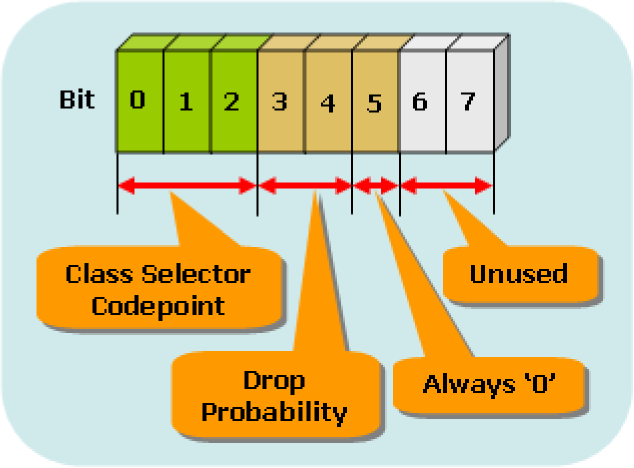


Tip de serviciu IP

precedenţa 0	000	Rutină
precedenţa 1	001	Prioritate
precedenţa 2	010	Imediat
precedenţa 3	011	Flash
precedenţa 4	100	Suprascriere Flash
precedenţa 5	101	Critic
precedenţa 6	110	Internet
precedenţa 7	111	Rețea

DSCP

6 biţi sunt folosiţi pentru a face 21 clase diferite
În cazul în care valoarea de probabilitate de cădere este de 01, probabilitatea este scăzută.
În cazul în care valoarea de probabilitate de cădere este de 10, probabilitatea este normal.
În cazul în care valoarea de probabilitate de cădere este de 11, probabilitatea este mare.



DSCP(Differentiated Services CodePrint)

Propababilitate de pierdere pachete de date	Clasa 1	Clasa 2	Clasa 3	Clasa 4
Scăzută	001010 AF 11 DSCP 10	010010 AF 21 DSCP 18	011010 AF 31 DSCP 26	100010 AF 41 DSCP 34
Medie	001100 AF12 DSCP 12	010100 AF22 DSCP 20	011100 AF32 DSCP 28	100100 AF42 DSCP 36
Mare	001110 AF13 DSCP 14	010110 AF23 DSCP 22	011110 AF33 DSCP 30	10011 AF43 DSCP 38

MPLS

Cu convergența aplicațiilor de voce, video și de date, rețele de afaceri se confruntă cu cereri tot mai mari de trafic. MPLS permite clasei de serviciu (CoS) etichetarea și prioritizarea traficului în rețea, astfel încât administratorii pot specifica ce aplicații trebuie să se deplaseze în întreaga rețea înaintea altora. Această funcție face ca o rețea MPLS deosebit de important pentru firmele care au nevoie pentru a asigura performanța aplicaţiilor de latențe mici cum ar fi VoIP și celeilalte funcţii vitale . Transportatorii MPLS diferă cu privire la numărul de clase de deservire pe care le oferă și în modul în care aceste niveluri CoS sunt taxate.

SBM

SBM vine de la Subnet Bandwidth Management (Manager), care funcționează ca protocolul RSVP. Este o abordare QoS de sus in jos și se aplică la stratul de legături de date. Tot traficul trebuie să treacă cel puțin unul dintre switch sau un router care a fost activat. [5]

Aplicații

O calitate de serviciu definită poate fi de dorită sau necesară pentru anumite tipuri de trafic de rețea, de exemplu:
În special mass-media de streaming
Internet Protocol Television (IPTV)
telefonie IP, de asemenea, cunoscută sub numele de Voice over IP (VoIP),
aplicatii de stocare, cum ar fi iSCSI și FCoE [1]

IPTV

Internet Protocol Television (IPTV) este un sistem prin care serviciile de televiziune sunt livrate folosind suita protocoalelor de internet printr-o rețea cu comutare de pachete, cum ar fi Internetul, în loc să fie livrate prin intermediul semnalului terestru tradițional, prin satelit, precum și formatele de televiziune prin cablu.

Serviciile IPTV pot fi clasificate în trei grupe principale:

- televiziune în direct, cu sau fără interactivitate referitoare la emisiunea TV curentă
- televiziune inregistrată: catch-up TV (reluare a unei emisiune TV care a fost difuzată ore sau zile în urmă), start-over TV (reluare a show-ului TV curent de la începutul său);
- video la cerere (VOD): căuta un catalog de video-uri care nu are legătură cu programele TV.

IPTV se distinge de televiziunea pe Internet prin procesul său de standardizare în curs de desfășurare (de exemplu, Institutul European de Standarde în Telecomunicații) și scenarii de implementare în rețelele preferențiale de abonat pe bază de telecomunicații, cu canale de acces de mare viteză în sediile utilizatorilor finali prin intermediul spațiilor set-top box sau alt client local de echipamente.

Din punct de vedere istoric, multe definiții diferite ale IPTV au apărut, inclusiv fluxurile elementare peste rețelele IP, fluxuri de transport peste rețele IP și o serie de sisteme proprietare.
O definiție oficială aprobată de grupul focalizat Uniunea Internațională a Telecomunicațiilor pentru IPTV (ITU-T FG IPTV) este:
"IPTV este definit ca servicii multimedia,cum ar fi televiziunea/video/audio/text/grafică/date furnizate prin rețele bazate pe IP a reușit să ofere nivelul necesar de calitate a serviciului și, de experiență, interactivitate si fiabilitate.

Avantaje

Protocolul de internet bazat pe platformă oferă avantaje semnificative, inclusiv abilitatea de a integra televiziune cu alte servicii bazate pe IP, cum ar fi accesul la Internet de mare viteză și VoIP.
O rețea IP schimbată, de asemenea, permite livrarea în mod semnificativ de mai mult conținut și funcționalitate. Într-o rețea tipică TV sau prin satelit, cu ajutorul tehnologiei de difuzare video , tot conținutul curge constant în aval la fiecare client, iar clientul selectează conținutul la set-top box. Clientul poate alege din mai multe opțiuni ca telecomunicaţiile, prin cablu sau prin satelit poate umple în "țeavă", care se scurg în casă. O rețea IP comutată funcționează diferit. Conținutul rămâne în rețea, și numai conținutul pe care clientul îl alege este trimis în casa clientului. Care eliberează lățime de bandă, precum și alegerea clientului este mai puțin restricționată de dimensiunea "ţevei" in casa. Acest lucru implică, de asemenea faptul că intimitatea clientului ar putea fi compromisă într-o măsură mai mare decât este posibilă cu TV prin satelit sau rețele tradiționale. Acesta poate oferi, de asemenea, un mijloc de a patrunde in, sau cel puțin perturba rețeaua privată.

Economie

Cheltuielile industriei de cablu de aproximativ 1 miliard de dolari pe an se bazează pe actualizări de rețea pentru a acomoda viteze mai mari de date. Cei mai mulți operatori folosesc 2-3 canale pentru a suporta viteze maxime de date de 50 Mbit/s pâna la 100 Mbit/s.. Cu toate acestea, deoarece fluxuri video necesită o rată de biți ridicată pentru perioade mai lungi de timp, cheltuielile pentru a sprijini cantități mari de trafic video vor fi mult mai mari. Acest fenomen este numit persistență. Persistența datelor este de obicei de 5% în timp ce persistența video poate ajunge cu ușurință la 50%. Deoarece traficul video continuă să crească, acest lucru înseamnă că mult mai multe canale CMTS din aval vor fi necesare pentru a transporta acest conținut video. Bazat pe piața de astăzi, este probabil ca industria cheltuielilor de extindere CMTS ar putea depăși 2 miliarde dolari pe an, aproape toate cheltuielile care să fie conduse de trafic video. Adoptarea IPTV pentru a găzduii majoritatea din acest trafic ar putea salva industria de aproximativ 75% a cheltuielilor de capital.

Interactivitate

O platformă bazată pe IP, de asemenea, permite oportunități semnificative pentru a face experiența vizionarării TV mai interactivă și personalizată.Furnizorul poate, de exemplu, să includă un ghid de program interactiv, care permite utilizatorilor să caute conținut după titlu sau numele actorului, sau o funcționalitate picture-in-picture, care le permite să "navigheze canalul", fără să părăsească programul la care se uită. Telespectatorii ar putea să vadă statistica unui jucător în timp ce vizionează un joc sportiv, sau controlează unghiul camerei. De asemenea, ei pot fi în măsură să acceseze fotografii sau muzică de pe PC-ul lor la televizor , folosesc un telefon mobil pentru a programa o înregistrare a show-ul lor preferat, sau chiar ajustarea controlului parental, astfel copilul lor poate viziona un film documentar pentru un raport la școală, în timp ce ei sunt plecaţi de acasă.

Rețineți că acest lucru este posibil, într-o anumită măsură, cu existenţa digitală terestru, satelit și rețele de cablu, în tandem cu cutii set top moderne. Pentru ca acolo să poată avea loc o interacțiune între receptor și emițător, un canal de răspuns este necesar. Datorită acestui fapt, terestru, prin satelit, precum și rețele de cablu de televiziune nu permit interactivitate. Cu toate acestea, interactivitatea acestor rețele poate fi posibil prin combinarea rețelelor de televiziune cu rețele de date, cum ar fi Internet sau la o rețea de comunicații mobile.

Video la cerere

Tehnologia IPTV este de a aduce video la cerere (VOD) la televiziune, care permite unui client să caute un program on-line sau în catalogul de film, pentru a viziona trailere și pentru a selecta, apoi o înregistrare selectată. Difuzarea a elementului selectat începe aproape instantaneu la TV-ul clientului sau PC.

Tehnic, atunci când clientul alege filmul, o conexiune punct-la-punct este configurată între decodorul clientului (set-top box sau PC) si serverul de streaming . Semnalizarea pentru funcționalitatea trick play (pauză, în slow-motion, înainte / înapoi, etc) este asigurată de RTSP (Real Time Streaming Protocol). Codec-urile cele mai comune utilizate pentru VoD sunt MPEG-2, MPEG-4 și VC-1. Într-o încercare de a evita pirateria ,conținutul VOD este, de obicei criptat,   În timp ce criptarea emisiunilor de televiziune prin satelit și prin cablu este o practică veche, cu tehnologia IPTV poate fi eficient gândită ca o formă de management a drepturilor digitale. Un film care este ales, de exemplu, poate fi redat pentru 24 de ore de la plata, după care acesta devine indisponibil.

Servicii convergente bazate pe IPTV

Un alt avantaj al unei rețele bazate pe IP este posibilitatea de integrare și convergență. Această oportunitate este amplificată atunci când se utilizează soluții bazate pe IMS .Serviciile convergente presupun interacțiunea serviciilor existente într-o manieră fără cusătură pentru a crea servicii noi cu valoare adăugată . Un exemplu este ID apelant pe ecran, obtinerea ID apelant pe un TV și capacitatea de a-l controla (trimite-l la căsuţa vocală, etc). Servicii bazate pe IP vor ajuta să permită eforturile pentru a oferi consumatorilor oricand oriunde accesul la conținut la televizorul lor. PC-uri și telefoane mobile, și să integreze servicii și conținut pentru a le lega împreună. În cadrul întreprinderilor și instituțiilor, IPTV elimină necesitatea de a conduce o infrastructură paralelă pentru a furniza servicii vii și servicii video depozitate.

IPTV este sensibil la pierderea de pachete și întârzierile în cazul în care datele de continut este nesigure. IPTV are cerințe minime stricte de viteză, în scopul de a facilita numărul corect de cadre pe secundă pentru a livra imagini în mișcare. Acest lucru înseamnă că viteza de conexiune limitată și lățimea de bandă disponibilă pentru o baza de client mare IPTV poate reduce calitatea serviciilor oferite. Deși câteva țări au bandă cu viteză mare permisă populațiilor, cum ar fi Coreea de Sud, cu 6 milioane de case care beneficiază de o viteză minimă de conectare de 100 Mbit / s, în alte țări (cum ar fi Regatul Unit) moștenirea rețelelor luptă să ofere 3 - 5 Mbit / s și astfel furnizarea simultană către casa de canale de televiziune, VOIP si acces la internet nu poate fi disponibilă. Ultima livrare pe mile pentru IPTV are, de obicei, o restricție de lățime de bandă, care permite doar un număr mic de fluxuri simultane de canale de televiziune - de obicei una la trei care urmează să fie livrate.

Streaming IPTV peste conexiunile fără fir în înteriorul casei sa dovedit a fi problematică, nu din cauza limitărilor de lățime de bandă cum mulţi își asumă, dar din cauza unor probleme cu multipath și reflecții ale semnalului RF care transportă pachete de date IP. Un flux IPTV este sensibil la pachetele care sosesc la momentul potrivit și în ordinea corectă. Îmbunătățirile în domeniul tehnologiei fără fir au început să asigure echipamente pentru a rezolva problema. Din cauza limitărilor wireless, furnizori de servicii IPTV mai folosesc azi tehnologiile cu fir de reţea acasă în loc de tehnologii fără fir, cum ar fi 802.11. Furnizorii de servicii precum AT&T (care face utilizarea extensivă a reţelei cu fir de acasa, ca parte a serviciului IPTV universal) și-au exprimat sprijinul pentru activitatea desfășurată în această direcție de către ITU-T, care a adoptat Recomandarea G.hn (de asemenea, cunoscut sub numele de G.9960), care este un urmatoarea generatie de rețea standard de acasă, care specifică un PHY / MAC comun, care poate funcționa pe orice cabluri de casă (linii electrice, linii telefonice sau cabluri coaxiale) [2]

Voice over IP

Voip over IP (VoIP, prescurtarea de la Voice over Internet Protocol), se referă de obicei la protocoalele de comunicație, tehnologii, metodologii, și tehnici de transmisie implicate sesiuni de comunicații de voce și sesiuni multimedia peste IP, cum ar fi Internetul. Alți termeni frecvent asociaţi cu VoIP sunt telefonia IP, telefonie prin Internet, Voice over Broadband (VoBB), telefonie în bandă largă, comunicații IP și telefon în bandă largă.

Telefonia prin Internet se referă la servicii de comunicatii voce-, fax, SMS-uri, și / sau aplicațiile de mesagerie vocală, care sunt transportate prin intermediul internetului, mai degrabă decât rețeaua telefonică publică comutată (PSTN). Pașii implicați în ceea ce constă apelul telefonic VoIP sunt de semnalizare și configurare a unui canal media, digitalizarea semnalului vocal analogic, codare, de împachetare, și de transmisie ca pachete IP într-o rețea cu comutare de pachete. Pe partea de primire, măsuri similare (de obicei, în ordine inversă), cum ar fi primirea de pachete IP, decodarea de pachete și conversie digital-analog reproduce fluxul vocal original. Chiar dacă telefonia IP și VoIP sunt utilizate alternativ, telefonia IP se referă la orice utilizare a protocoalelor IP pentru comunicații de voce către sistemele de telefonie digitală, în timp ce VoIP este o tehnologie utilizată de telefonie IP pentru a transporta apeluri telefonice.

Furnizorii timpurii de servicii de voce peste IP, au oferit modele de afaceri și soluții (tehnice) care oglindeau arhitectura moştenirii rețelei de telefonie . Furnizorii de generaţia a doua, cum ar fi Skype care au construit rețele închise pentru baze de utilizatori privați, oferind beneficiul de apeluri gratuite si comoditate, în timp ce neagă utilizatorii lor capacitatea de a apela în alte rețele. Acest lucru a limitat sever capacitatea utilizatorilor de a aranjare a terților de hardware și software.Furnizorii de generatia a treia, cum ar fi Google Talk au adoptat conceptul de domeniu VoIP - care este o abatere completă de la arhitectura rețelelor existente. Aceste soluții de obicei permit interconectarea arbitrară și dinamic între oricare două domenii pe Internet ori de câte ori un utilizator doreste sa facă un apel.

Sistemele VoIP utilizează protocoale de sesiune de control pentru a controla conectarea și deconectarea apelurilor, precum și codec-uri audio care codifica transmiterea vocii printr-o rețea IP audio digital prin intermediul unui flux audio. Alegerea codec-ului variază între diferite implementări de VoIP, în funcție de cerințele de aplicare și de lățime de bandă de rețea; unele implementari se bazează pe bandă îngustă și vorbire comprimată, în timp ce alții susțin codec-uri stereo de inalta fidelitate . Unele codec-uri populare includ versiuni ale unei legi universale u și a unei legi analogice a ale G.711, G.722, care este un codec de inalta fidelitate comercializat ca voce HD de către Polycom , un codec vocal popular open source cunoscut ca iLBC, un codec care utilizează doar 8 kbit / s pentru fiecare mod numit G.729, și multe altele.

VoIP este disponibil pe smartphone-uri și multe dispozitive de Internet, astfel încât utilizatorii de dispozitive portabile, care nu sunt telefoane, pot efectua apeluri sau trimite SMS mesaje text prin 3G sau Wi-Fi.

Protocoale

Voice over IP a fost pusă în aplicare în moduri diferite folosind ambele proprietaţi şi protocoale deschise și standarde. Exemple de protocoale de rețea folosite pentru a pune în aplicare VoIP includ:

- H.323
- Media Gateway Control Protocol (MGCP)
- Session Initiation Protocol (SIP)
- Real-time Transport Protocol (RTP)
- Session Description Protocol (SDP)
- Inter-Asterisk eXchange (IAX)
- Jingle XMPP VoIP extensions

Protocolul H.323 a fost unul dintre primele protocoale VoIP care a gasit aplicarea pe scară largă pentru traficul pe distanțe lungi, precum și serviciile de rețea locală. Cu toate acestea, deoarece dezvoltarea de noi protocoale, mai puțin complexe, cum ar fi MGCP și SIP, H.323 implementările sunt din ce în ce mai limitate la efectuarea traficului în rețea pe distanţe lungi . În particular, Session Initiation Protocol (SIP) a câștigat penetrare pe scară largă pe piața VoIP. O implementare notabilă de proprietate este protocolul Skype, care este, pe bazat pe principiul de reţea punct-la-punct (P2P).

Avantaje

Există mai multe avantaje la utilizarea Voice over IP. Cel mai mare avantaj unic pe care VoIP îl are peste sisteme telefonice standard este costul. În plus, apeluri internaționale folosind VoIP sunt de obicei foarte ieftine. Un alt avantaj, care va deveni mult mai pronunţat în timp ce VoIP urcă, este aceea că apelurile între utilizatorii VoIP sunt, de obicei gratuite. Utilizarea serviciilor, cum ar fi True VoIP, abonații pot suna unul pe altul, fără nici un cost pentru fiecare împarte.

Calitatea de servicii

Comunicarea de pe rețeaua IP este în mod inerent mai puțin fiabilă în contrast rețeaua de telefonie publică cu circuite comutate , deoarece nu oferă un mecanism bazat pe rețea pentru a se asigura că pachetele de date nu se pierd, și sunt livrate în ordine secvențială. Este o rețea best-effort, fără garanţia de Calitatea fundamentală a serviciilor (QoS). De aceea, implementarile VoIP se pot confrunta cu probleme de atenuare a latenței și bruiaj .

În mod implicit, routerele de rețea se ocupă de traficul pentru primul venit, primul servit. Routerele de rețea pe link-uri cu volum de trafic ridicat poate introduce latenţa, care depășește pragurile admise pentru VoIP. Întârzieri fixe nu pot fi controlate, astfel cum acestea sunt cauzate de distanța fizică parcursă de pachete, cu toate acestea, latența poate fi minimizată prin marcarea pachetelor de voce ca fiind sensibile la întârziere, cu metode, cum ar fi DiffServ .

Un pachet VoIP, de obicei, trebuie să aștepte pentru pachetul curent să termine transmisia. Deși este posibil să se anticipeze (anulat) un pachet mai puțin important în mijlocul de transmisie, acest lucru nu se face de obicei, mai ales pe legături de mare viteză unde timpii de transmitere sunt scurţi, chiar și pentru pachetele de dimensiune maximă. O alternativă la preachiziţionare a link-urilor mai lente, cum ar fi dial-up și Digital Subscriber Line (DSL), este de a reduce timpul maxim de transfer prin reducerea unitaţii de transmisie maximă. Dar fiecare pachet trebuie să conțină anteturi de protocol, astfel încât acesta creşte antetul de deasupra relativ pe fiecare link deplasat, nu doar strangulare (de obicei acces la Internet).

Modemurile DSL furnizează conexiuni Ethernet (Ethernet sau prin USB) la echipamentele locale, dar în interior sunt de fapt modemuri cu modul de transfer asincron (ATM) . Ei folosesc ATM-uri interfaţă de adaptarea 5 (AAL5) pentru a segmenta fiecare pachet Ethernet într-o serie de celule ATM de 53-bit pentru transmiterea și reasamblarea înapoi în pachete Ethernet la receptor. Un identificator de circuit virtual (VCI) este o parte a antetului de 5-biți pe fiecare celulă ATM, astfel încât emițătorul poate multiplexa circuitele virtuale active (CR), în orice ordine arbitrară. Celule de la acelaşi circuit virtual sunt întotdeauna trimise secvențial.

Cu toate acestea, marea majoritate a furnizorilor de DSL folosesc doar un singur circuit virtual pentru fiecare client, chiar si cei cu pachet de servicii VoIP. Fiecare pachet Ethernet trebuie să fie complet transmis înainte de a putea începe alt pachet. Dacă un al doilea circuit virtual a fost stabilit, având prioritate ridicată și rezervată pentru VoIP, apoi o mică prioritate de pachete de date ar putea fi suspendată în mijlocul de transmisie și un pachet de VoIP trimis imediat pe circuit virtual de înaltă prioritate. Apoi link-ul sa transporte circuit virtual cu prioritate scăzută de unde a rămas. Deoarece link-urile ATM sunt multiplexate pe baza de celulă-cu-celulă, un pachet cu prioritate mare ar trebui să aștepte cel puțin timp de 53 de biţi pentru a începe transmisia. Nu ar fi nici o nevoie de a reduce interfața MTU și să accepte creșterea rezultată în protocol de interfaţă înaltă, și nu este nevoie pentru a abandona un pachet de prioritate scăzută și retransmis mai târziu.

Voce, precum și toate celelalte date, călătoresc în pachete peste rețelele IP, cu o capacitate maximă fixă. Acest sistem poate fi mai predispus la congestionare și atacuri DoS decât sistemul de circuit tradițional pornit ; sistem de circuit comutat de capacitate insuficientă va refuza noi conexiuni în timp ce transportă restul fără depreciere, în timp ce calitatea de date în timp real cum ar fi convorbiri telefonice pe rețele cu comutare de pachete se degradează în mod dramatic.

Întârzierile fixe nu pot fi controlate în timp ce sunt cauzate de distanța fizică pe care o parcurg pachetele. Acestea sunt deosebit de problematice atunci când circuitele prin satelit sunt implicate, din cauza distanței lungi la un satelit geostaționar și înapoi; întârzieri de 400-600 ms sunt tipice.

Atunci când sarcina pe un link crește atât de repede încât comută supraincarcări a cozii, rezultate congestionării și pachetele de date sunt pierdute. Acest lucru semnalează un protocol de transport cum ar fi TCP să reducă rata de transmitere pentru a atenua congestionarea. Dar, de obicei, VoIP utilizează UDP nu TCP, deoarece recuperarea de la congestionare prin retransmisie presupune, de obicei, latenţa prea multă. Astfel mecanismele QoS pot evita pierderea nedorită a pachetelor VoIP prin transmiterea imediată a acestora înainte de orice mare parte a traficului pe acelaşi link, chiar și atunci când mare parte a traficului este în depăşire.

Receptorul trebuie să rearanjeze pachete IP care sosesc în ordine și se recuperează gratios cand pachetele ajung prea târziu sau deloc. Rezultatele bruiajului din modificările rapide și aleatorii (de exemplu, imprevizibilă), ale cozii de lungimi de-a lungul unui traseu de Internet dat, din cauza concurenței din partea altor utilizatori pentru aceleaşi legături de transmisie . Receptoare VoIP contra bruiaj prin stocarea pachetelor primite pe scurt într-o "de-bruiare" sau buffer"difuzare" , crescând în mod deliberat latenta de a îmbunătăți șansa ca fiecare pachet va fi pe o parte atunci când este timpul ca motorul de voce să-l joace. Întârzierea adăugată este, astfel, un compromis între latență excesivă și a pierderilor excesive, de exemplu, întreruperi audio momentane. [3]

iSCSI

Protocolul iSCSI (Internet Small Computer System Interface) unifică mediul de stocare în reţea cu protocolul IP, fiind o tehnologie standardizată care permite datelor să fie transportate la şi de la dispozitivele de stocare printr-o reţea IP, folosind comenzi SCSI. Folosind iSCSI, conceptul de reţea de stocare poate exista oriunde unde poate "merge IP".
iSCSI este un protocol cap-la-cap pentru transformarea blocurilor de date de I/O pentru a fi stocate de-a lungul unei reţele IP. Acest protocol este folosit pe servere, dispozitive de stocare şi dispozitive de transfer de tip poartă. iSCSI suportă la nivelul fizic interfaţa Gigabit Ethernet.

Această tehnologie oferă viteză ridicată, cost scăzut, soluţii de stocare la distanţe mari pentru site-urile Web, furnizare de servicii.
Un iSCSI HBA sau o interfaţă de stocare NIC (Network Interface Card) conectează resursele de stocare la Ethernet. Astfel nivelele de transport sunt administrate folosind aplicaţiile de administrare a reţelei. Administrarea de nivel înalt a protocolului iSCSI (cum ar fi permisiunile,informaţii despre dispozitiv şi configuraţie) poate fi cu uşurinţă construită în aceste aplicaţii.
Gigabit iSCSI poate folosi comutatoare Ethernet obişnuite în schimbul comutatoarelor canal de fibră speciale.
Reţeaua IP este globală şi nu are practic limitare de distanţă.

Adaptoare iSCSI

Combină funcţiile celorlalte 2 categorii. Aceste adaptoare acceptă blocuri de date de la aplicaţii, le segmentează şi apoi trimite pachete IP de-a lungul reţelei IP. Pentru procesarea TCP/IP solicită microprocesorul.

Avantajul acestor adaptoare este că pot lucra cu NIC-urile Ethernet existente. Principalul dezavantaj este că solicită intens utilizarea microprocesorului pentru procesarea TCP/IP.

iSCSI oferă compatibilitate cu aplicaţiile utilizatorilor precum sisteme de fişiere, baze de date, servicii Web.

Pentru a construi o reţea de stocare iSCSI într-un centru de date (data center),adaptoarele de magistrală ale calculatorului gazdă pot fi utilizate în servere, împreună cu dispozitivele de stocare iSCSI şi o combinaţie de comutatoare IP şi Ethernet. Comutatoarele şi rutoarele IP pot fi utilizate doar dacă se cere.

Aplicaţii pentru reţele de stocare iSCSI

Aplicaţiile pentru reţelele de stocare iSCSI pot fi:

- cu ajutorul infrastructurii pentru reţeaua de stocare, utilizatorii pot uni mai multe dispozitive de stocare cu mai multe servere permiţând o utilizare mai bună a resurselor, o administrare mai simplă a spaţiului de stocare şi o expansiune mai facilă a infrastructurii de stocare;
- operaţii de backup mai rapide decât cele anterioare.

Operaţiile de backup din trecut se rezumau la operaţii la nivel de fişier de-a lungul reţelelor locale IP. În prezent se operează la nivel de bloc de date de-a lungul reţelelor de stocare IP. Această facilitate accelerează salvarea transparentă, oferă flexibilitate utilizatorilor pentru a folosi reţelele IP partajate sau dedicate pentru operaţiile de stocare.

- acces la locaţii îndepărtate şi la capacităţi de stocare în afara celor folosite.

Cu ajutorul reţelelor de stocare bazate pe IP, utilizatorii pot avea cu uşurinţă acces la locaţii secundare aflate la distanţă de-a lungul reţelelor IP metropolitane sau larg răspândite geografic. Site-urile aflate la distanţă pot fi utilizate pentru backup offsite, pentru clustering sau mirroring. Backup offsite este o stocare date în afara calculatorului (CD, DVD) şi se poate folosi de către oricine, nu doar de firme.În plus utilizatorul poate alege să se conecteze la furnizori de servicii de stocare la cerere.

Aplicaţiile pentru legarea iSCSI la canal de fibră

Aplicaţiile pentru legarea iSCSI la canal de fibră (FC) pot fi:

- acces prin IP la mediile de stocare;

Folosind adaptoare iSCSI în servere, utilizatorii pot beneficia de acees la resursele de stocare FC de-a lungul unei reţele IP. Această flexibilitate permite utilizatorilor să aibă acces nelimitat la servere, extinzând astfel accesul la mediul de stocare. De exemplu, informaţiile din bazele de date din servere pot fi direct accesate printr-o reţea IP.

- salvare transparentă la distanţă pentru utilizatori.

Utilizarea reţelelor IP, în combinaţie cu iSCSI şi rutoare sau comutatoare de stocare IP,permite pentru utilizatori backup la distanţă. Site-urile de la distanţă pot opera independent, acum beneficiind de resursele de stocare ale serverelor iSCSI pentru spaţii de stocare FC pentru salvarea transparentă şi refacere. Această aplicaţie permite administratorilor de centre de date să centralizeze datele firmelor într-o singură locaţie în loc să ofere multor utilizatori îndepărtaţi administrare sofisticată pentru spaţii de stocare aflate în diferite locaţii. [4]

Bibliografie

[1] http://en.wikipedia.org/wiki/Quality_of_service#Mechanisms
[2] http://en.wikipedia.org/wiki/Internet_protocol_television
[3] http://en.wikipedia.org/wiki/Voice_over_IP
[4] http://en.wikipedia.org/wiki/ISCSI
[5] http://cisconet.com/qos/qos-general/127-easy-qos-101-qos-protocols.html

Mănucă Adrian, 441A

Suportul QoS în Windows

QoS(Quality of Service) conține un set de tehnologii pentru administrarea traficului în rețea printr-o manieră eficientă a costului pentru a îmbunătăți experiența cu utilizatorul casnic și utilizatorul din mediul enterprise. Tehnologiile QoS permit măsurarea lărgimii de bandă(viteza de transfer), detecția schimbărilor condițiilor/regulilor din rețea (precum congestia sau disponibilitatea de lărgime de bandă) și prioritizează traficul sau îl reglează.

De exemplu, QoS poate fi aplicat pentru a prioritiza livrarea de trafic senzitiv la latență (precum aplicații de voce sau video) și pentru a controla impactul traficului ulterior insenzitiv precum transferurile bulk de date. Oferirea de livrare prioritizată pentru trafic TCP/IP necesită suport de la gazde și dispozitive din infrastructura rețelei. În cele ce urmează se vor descrie metodele pentru a utiliza QoS sub gazdele bazate pe Microsoft Windows.

Problema principală pentru definirea QoS pentru rețelele TCP/IP este cum să se facă specificarea și oferirea livrării de trafic IP. Deși RFC 791 pentru IP a definit câmpul Tipul de Serviciu(Type Of Service) cu posibilitatea de a specifica anterioritatea, întârzierea, debitul de transfer, siguranța, caracteristici de cost, IP este în esență cel mai bun efort, tehnologia bazată de pe interschimbare de pachete datagramă care tratează tipic fiecare pachet ca primul venit, primul servit. (FIFO).[1][2]

Configurarea livrării prioritizate

Pentru a oferi serviciul de livrare prioritizată există câteva posibilități. Se poate configura infrastructura rețelei pentru a oferi manevrare specială pentru trafic marcat, și atunci gazdele să-și marcheze traficul din exterior. Alternativ, gazdele pot programa dinamic infrastructura rețelei pentru a oferi manevrare specială bazată pe caracteristicile traficului extern (precum adrese și numere de porturi).

Pentru traficul TCP/IP, se pot utiliza câteva metode diferite pentru a oferi livrare prioritizată. De exemplu, stratul de Interfață Network pentru Ethernet, etichetarea IEEE 802.1p va marca cadrele trimise de o gazdă pentru livrare prioritizată utilizând un câmp de 3 biți de Prioritate în header-ul VLAN al cadrului Ethernet. Header-ul(antetul) VLAN este plasat în interiorul antetului Ethernet, între câmpul Adresă Sursă și cel de Lungime (pentru un cadru IEEE 802.3) sau âmpul EtherType (la cadrul Ethernet II).

Implementarea etichetării 802.1p pe gazdă necesită ca adaptorul de rețea și driverul dispozitivului să suporte 802.1p și ca adaptorul de rețea să aibă suportul 802.1p activat. Se poate activa suportul 802.1p din tab-ul Advanced din proprietățile driverului pentru adaptorul de rețea. Switch-urile Ethernet trebuie de asemenea să aibă suportul 802.1p activat.

La stratul Network Interface pentru wireless IEEE 802.11, certificarea alianței Wi-Fi pentru Multimedia (WMM) definește 4 categorii de acces pentru a prioritiza traficul în rețea. Aceste categorii de acces sunt (în ordinea priorității cele mai mari la cea mai mică) voce, video, cel mai bun efort, fundal. Suportul gazdei pentru prioritizare WMM necesită ca ambele adaptoare wireless și driverele lor să suporte WMM. Punctele de acces wireless trebuie să aibă WMM activat.

La stratul Internet, se pot utiliza Servicii Diferențiate și setul de valori pentru Puncte Cod ale Serviciilor Diferențiate (DSCP) în antetul IP. După definiția din RFC 2472, valoarea DSCP este de 6 biți MSB pentru câmpul IPv4 TOS și în câmpul Traffic Class al IPv6.

Cele mai moderne routere enterprise suportă diferențiere de trafic DSCP, dar este de regulă dezactivată implicit. Pe durata forwarding(redirecționării), routerele capabile DSCP citesc valoarea DSCP și plasează pachetul într-o coadă specifică. De exemplu, se poate configura routerul pentru a plasa pachetele redirecționate în prioritate înaltă, cel mai bun efort, sau mai jos decât cozile pentru cel mai bun efort bazate pe valorile DSCP definite. Prin configurarea cozilor și valorilor DSCP, traficul marcat DSCP poate avea niveluri diferențiate de serviciu. De exemplu, traficul de rețea cu misiune critică obține redirecționare preferențială și nu este întârziat de alte date bulk din trafic cu prioritate scăzută. Specificația WMM definește cum WMM accesează categoriile la valori DSCP. Un punct de acces(AP) wiress capabil WMM citește valoarea DSCP și manevrează traficul bazat pe categoria lui de acces.

La stratul Internet, se poate de asemenea utiliza RSVP(Resource Reservation Protocol), un protocol de semnalizare definit în RFC 2205. Gazdele pot utiliza acest protocol pentru a încerca să rezerve lărgime de bandă peste o rețea la un punct de capăt. RSVP nu este implementat la scară largă în rețele, totuși, și nu este suportat încă în Windows XP, Server 2003, Vista sau Server 2008.

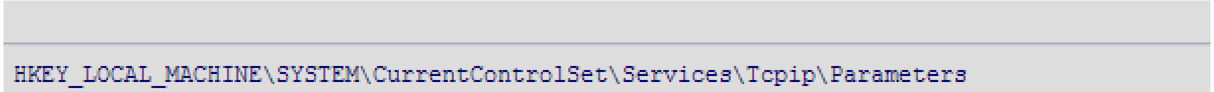
Pentru a trimite pachete marcate pentru livrare prioritizată, aplicațiile sau componentele sistemului de operare trebuie să fie capabile să specifice valori fie pentru prioritate 802.1p ori pentru DSCP.

În continuare se va descrie cum componentele Windows sau aplicațiile Windows pot specifica priorități 802.1p pentru cadre Ethernet sau valori DSCP pentru traficul TCP/IP. [1]

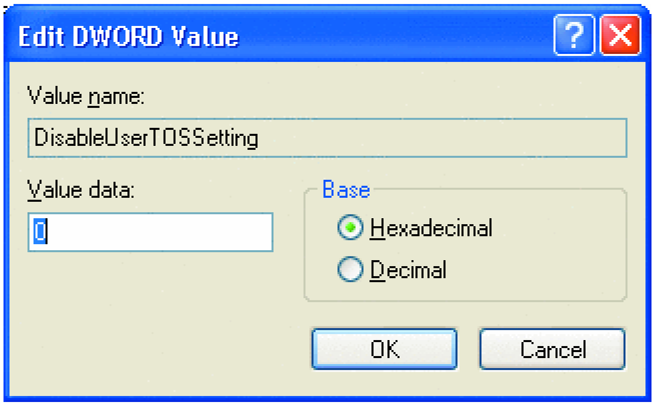
QoS în Windows XP și Windows Server 2003

Windows XP și Windows Server 2003 oferă API-uri pentru desemnarea de parametri QoS pentru trafic. Dezvoltatorii de aplicații pot utiliza Socket-uri Windows (Winsock) și API-uri Generic QoS (GQoS) pentru a aplica parametri QoS la nivelul aplicației pe un socket. Administratorii de rețea pot utiliza unelte de management al traficului scrise pentru a apela API-uri de Traffic Control(TC) pentru aa aplica parametri QoS la nivelul gazdei.

Se pot utiliza Winsock și opțiunea de socket IP_TOS pentru a seta valoarea DSCP pentru pachete externe pentru un socket. Totuși, implicit, stiva TCP/IP ignoră opțiunea socket IP_TOS. Pentru a utiliza IP_TOS trebuie creată și setată o valoare DWORD în Regiștrii Windows DisableUserTOSSetting=0 sub cheia de registru următoare:



```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
```



Value name: DisableUserTOSSetting

Value data: 0

Base: ● Hexadecimal ○ Decimal

Setarea valorii de registru pentru DisableUserTOSSetting

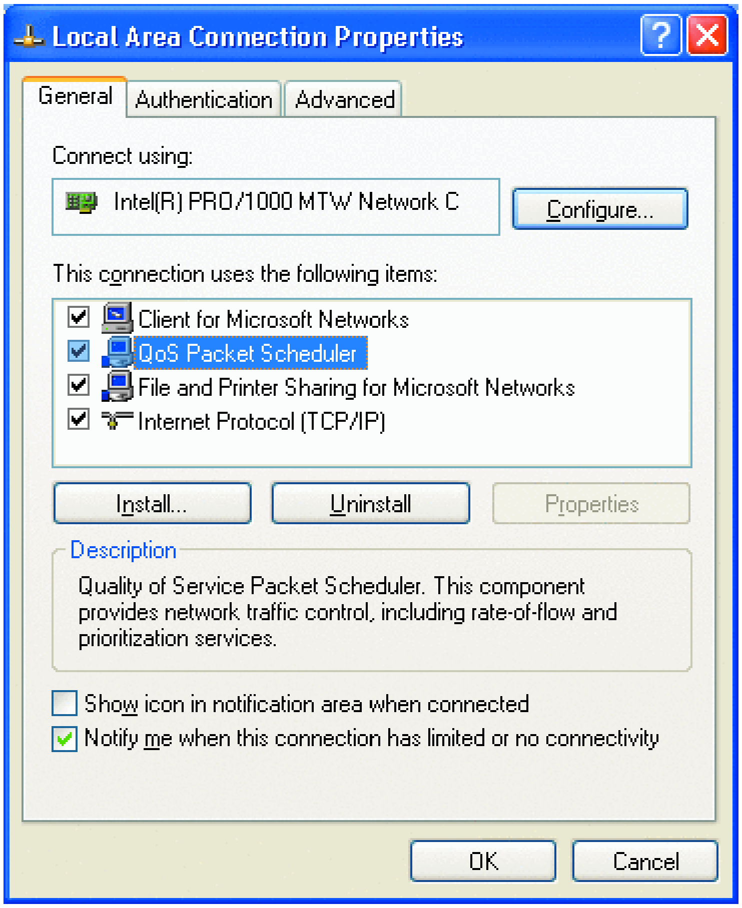
Computerul trebuie repornit pentru ca setarea să aibă efect.

Pentru a specifica valoarea DSCP pentru trafic fără a fi necesar să se utilizeze opțiunea socket IP_TOS, se pot utiliza și API-uri GQoS. GQoS este o parte din Windows Sockets 2.0 (Winsock 2). Cele mai multe aplicații cu suport QoS utilizează API-uri GQoS pentru a invoca capibilități QoS în Windows. GQoS în Windows XP SP2 permite unei aplicații să seteze o valoare DSCP și să regleze traficul extern. Pentru a seta o prioritate 802.1p pe calculatoare cu Windows XP SP2 trebuie utilizat TC API.

TC API oferă acces la mecanismele de control al traficului care reglează traficul în rețea pe gazda locală. Permite acces direct asupra valori DSCP, etichete 802.1p, și rata de reglare(throttle). Administratorii de rețea pot utiliza programe de management al traficului pentru a invoca TC API direct în numele aplicațiilor care nu au suport QoS. Datorită faptului că este un API de nivel mai jos decât GQoS API, TC API necesită privilegii de administrator.

Spre deosebire de GQoS API, TC API permite trafic din aplicații multiple pe aceeași gazdă pentru a fi agregate într-un singur flux QoS. Ca parte a acestei agregări, traficul poate fi identificat ca o combinație adreselor IP de sursă și destinație, porturi pentru sursă și destinație și combinație de protocoale (TCP sau UDP). De exemplu, tot traficul pentru o adresă IP de destinație specifică poate fi inclus într-un singur flux QoS pentru orice port sursă sau de destinație, indifirent de aplicația de pe gazdă. API-ul GQoS, pe de altă parte, permite unei aplicații să-și definească propriul tratament QoS pentru datele trimise pe un socket.

Pentru a suporta QoS, calculatoarele cu sisteme de operare Windows XP și Windows Server 2003 trebuie să aibă instalată și activată componenta QoS Packet Scheduler din proprietățile conexiunii de rețea din folderul Network Connections. Componenta QoS Packet Scheduler (Psched.sys) este instalată și activată implicit pe calculatoarele cu Windows XP. Pe calculatoarele cu Windows Server 2003 poate fi instalată. [1]



Connect using:
Intel(R) PRO/1000 MTW Network C

This connection uses the following items:
☑ Client for Microsoft Networks
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol (TCP/IP)

Description

Quality of Service Packet Scheduler. This component provides network traffic control, including rate-of-flow and prioritization services.

☐ Show icon in notification area when connected
☑ Notify me when this connection has limited or no connectivity

Configurarea QoS Packet Scheduler

[1]

Windows XP implementează o schemă DRR (Deficit Round Robin) când sistemul de operare utilizează un link slab. Această schemă a fost valabilă și în Windows 2000. Implicit, această schemă este activată în Windows XP când un link slab este detectat. Această schemă alocă câteva fluxuri de date și asignează noi fluxuri de date pentru aplicație la aceste fluxuri. Aceste fluxuri sunt automat servite într-o manieră Round Robin. Această configurație permite răspuns mai bun și performanță pentru comunicațiile în rețea și nu necesită configurații manuale. [5]

Ca și în Windows 2000, programele beneficiază de avantajul QoS prin API-uri QoS în Windows XP. 100% din lărgimea de bandă este disponibil pentru a fi partajat de toate programele doar dacă un program specifică o cerere de prioritate pe bandă. Această lărgime de bandă rezervată este încă disponibilă celorlalte programe dacă programul cu prioritate nu trimite date. Implicit, programele pot rezerva o viteză de transfer de 20% din viteza link-ului pe ficare interfață din calculator. Dacă programul care rezervă banda nu trimite date suficiente pentru a o utiliza, partea neutilizată a benzii rezervate este disponibilă pentru alte fluxuri de date pe aceeași gazdă. [5]

QoS în Windows Vista și Windows Server 2008

Suportul QoS în Windows Vista și Windows Server 2008 a fost îmbunătățit și simplificat. Pentru staff-ul IT este posibil acum să utilizeze politici bazate pe QoS pentru a seta valori DSCP și pentru a controla rata de trimitere de pachete a unei aplicații fără a fi nevoie de alte API-uri sau de modificarea aplicațiilor existente. Pentru dezvoltatori, GQoS și TC API sunt suportate, deși suportul pentru aceste API-uri nu mai este plănuit în versiunile viitoare de Windows. În plus, opțiunea IP_TOS Winsock a fost eliminată. Pentru a înlocui GQoS și API-urile TC și pentru a simplifica suportul QoS în aplicațiile viitoare sau în versiunile lor actualizate(noi), Windows Vista și Windows Server 2008 suportă noul API QoS2, cunoscut și ca Quality Windows Audio-Video Experience (qWAVE).

Politicile bazate pe QoS în Windows Server 2008 și Windows Vista permit experiențe cu utilizatorul mai bune, controlul costului de viteză de transfer(lărgime de bandă - bandwidth), sau negociere a nivelurilor de servicii cu furnizori de bandă sau departamente business. Se pot administra vitezele de transfer indiferent de aplicație și peste o infrastructură Active Directory® . Pentru că administrarea traficului are loc sub stratul(nivelul) aplicației, aplicațiile existente nu necesită modificări pentru management de trafic bazat pe politici QoS.

Setările bazate pe politicile QoS în Windows Server 2008 și Windows Vista permit prioritizarea sau administrarea ratei de trimitere pentru trafic extern bazat pe următoarele condiții:

- Trimiterea aplicației (cale executabilă și nume)
- Adrese sursă sau destinație IPv4 sau IPv6 sau prefixe din adrese
- Protocol(TCP, UDP sau amândouă)
- Porturi sursă sau destinație sau game de porturi (TCP sau UDP)

Politicile QoS sunt aplicate unei sesiuni de login sau unui computer ca parte dintr-un Group Policy object(GPO) care este legat de un container Active Directory precum domeniu, site, unitate organizațională (OU), sau un grup de securitate. Ca parte a Group Policy, politicile QoS se construiesc deasupra managementului Active Directory existent al infrastructurii.

Politicile bazate pe QoS permit definirea priorității traficului. Se poate configura o politică QoS pentru a marca trafic extern IPv4 sau IPv6 cu o valoare specifică DSCP. Se poate de asemenea administra utilizarea lărgimii de bandă pentru trafic extern. Se poate configura o politică QoS cu o rată de reglare pentru trafic extern. Cu throttling, componentele QoS limitează traficul extern agregat la o rată specifică. Pentru computere, se poate administra utilizarea lărgimii de bandă pentru trafic intern, configurând setări avansate pentru a specifica debitul intern pentru trafic TCP prin setarea unei valori maxime pentru recepția dimensiunii ferestrei TCP.

În Windows Vista și Windows Server 2008, QoS Packet Scheduler este instalat și activat implicit. Componenta Pacer.sys esteun nou driver filtru ușor Network Device Interface Specification (NDIS) 6.0 care controlează programarea pachetelor pentru politici QoS și pentru traficul aplicațiilor ce au activat QoS. Pacer.sys înlocuiește Psched.sys din Windows XP și Server 2003.

Pentru a lansa politici QoS pe intranet, se configurează politici QoS bazate pe utilizator sau computer și se aplică la containerul Active Directory potrivit. Calculatoarele cu Windows Vista și Windows Server 2008 descarcă și aplică setările lor de politici QoS când actualizează User Configuration sau Computer Configuration Group Policy.

Deoarece rețelele sunt partajate în număr tot mai mare atât de date cât și de aplicații audio-video(AV), o soluție QoS e necesară astfel traficul AV independent de timp poate fi tratat preferențial peste traficul de date. În plus, rețelele devin în număr tot mai mare și wireless, ceea ce introduce complicații în plus pentru latență și aplicații sensizitive la viteza de transfer.

Caracteristica qWAVE din Windows Vista oferă o colecție de module software corelate QoS care adresează provocările rețelei introduse de aplicații AV și rețele wireless. qWAVE este integrat în subsistemul QoS și lucrează cu tehnologii multiple de prioritate a stratului de pachete din interfața de Internet și Rețea/Network. qWAVE suportă fluxuri AV multiple (flux de cereri de QoS în timp real) și fluxuri de date (flux de cel mai bun efort, e-mail si transfer de fișiere) simultan.

Colecția de tehnologii qWAVE detectează și monitorizează lărgimea de bandă LAN, descoperă capabilitățile QoS ale rețelei, și furnizează control distribuit pentru utilizare consistentă a vitezei de transfer în rețea. Aceste tehnologii activează tehnicii avansate de streaming AV astfel încât aplicațțile pot să se adapteze dinamic la schimbările condițiilor din rețea, și sunt disponibile numai pentru dezvoltatori prin API-ul QoS2. [1]

Crearea și editarea unei politici QoS în Windows 7 și Windows Server 2008 R2

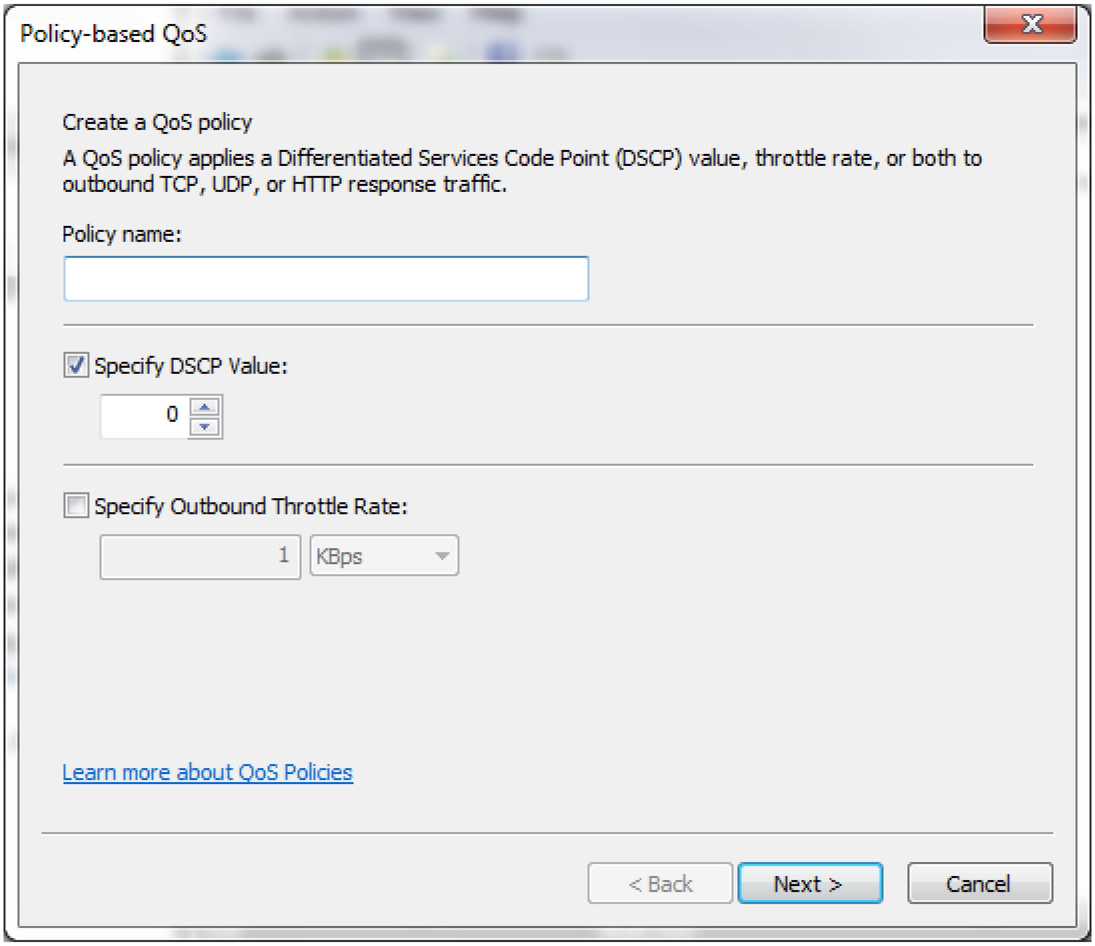
Pentru a crea sau edita o politică QoS se utilizează Group Policy Management Console (GPMC). Când se editează un obiect Group Policy (GPO), politicile QoS se găsesc în Computer Configuration\Policies\Windows Settings or User Configuration\Policies\Windows Settings în Editorul Group Policy Management (gpedit.msc)

Politicile QoS se aplică computerului indiferent de utilizatorul logat.

Când se creează o nouă politică QoS, 4 pagini de tip Wizard ne ghidează prin configurarea politicii. Pentru editare se procedeaza la fel, doar ca se modifica ce s-a creat deja.

*Pagina 1 a Wizard-ului : **Policy Profile** tab*

Item	Detalii
Policy name	Se introduce un nume pentru politica QoS care va fi un identificator unic pentru aceasta.
Specify DSCP value	Se selectează checkbox-ul pentru a activa marcarea DSCP, și apoi se introduce o valoare între 0 și 63.
Specify throttle rate	Se selectează checkbox-ul pentru a activa reglarea traficului extern, și apoi se specifică o valoare mai mare ca 1 ori în kilobytes per secundă (**KBps**) ori în megabytes per secundă (**MBps**).


Policy-based QoS

Create a QoS policy

A QoS policy applies a Differentiated Services Code Point (DSCP) value, throttle rate, or both to outbound TCP, UDP, or HTTP response traffic.

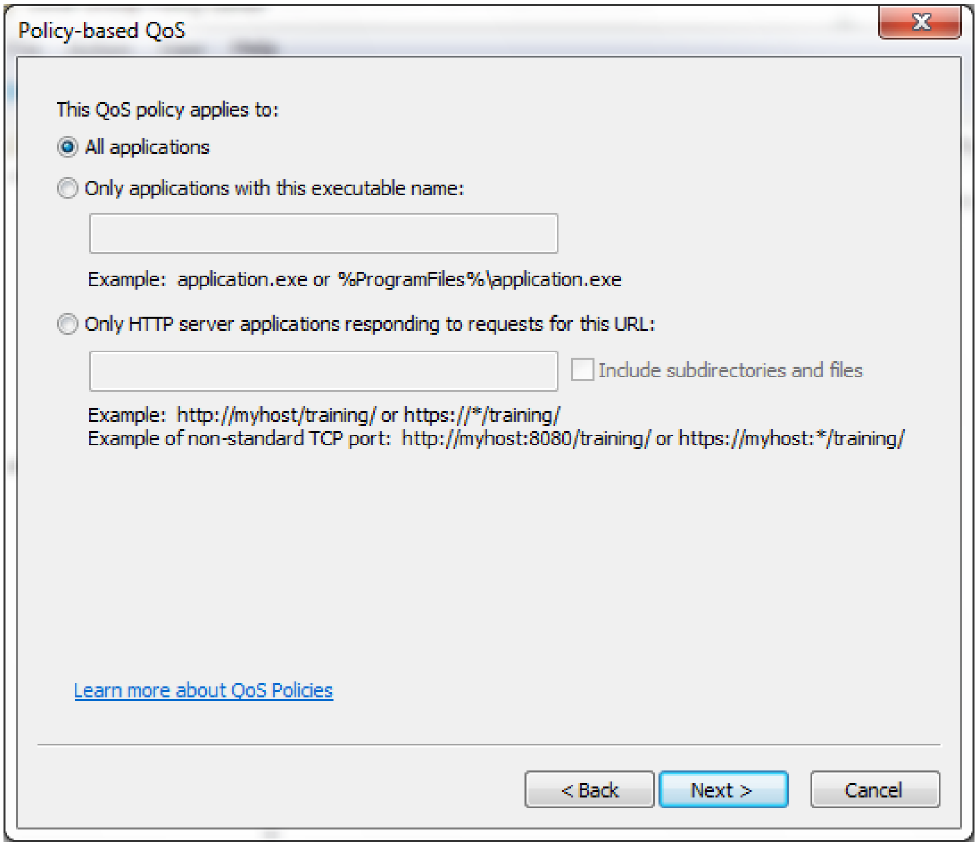
Policy name:

☑ Specify DSCP Value: 0

☐ Specify Outbound Throttle Rate: 1 KBps

*Pagina 2 a Wizard-ului: **Application Name or URL tab***

Item	Detalii
All applications	Implicit. Aplică valoarea DSCP și rata de throttle specificată pe pagina 1 a Wizard-ului (**Policy Profile**) traficului extern, indiferent de aplicație.
Only applications with this executable name	Aplică valoarea DSCP și rata de throttle specificată (la tab-ul Policy Profile) traficului extern doar pentru aplicația specificată. Numele fișierului executabil trebuie să se termine cu extensia .exe. Se poate include calea fișierului în numele aplicației, și calea poate include variabile de mediu (exemplu: %ProgramFiles%/MyApplication Path/MyApp.exe). Calea aplicației nu poate include un link simbolic
Only HTTP server applications responding to requests from this URL	Aplică valoarea DSCP și rata throttle specificate (pe pagina 1) traficului extern care răspunde unei adrese URL. URL-urile HTTP și HTTPS sunt suportate. URL-ul poate include caractere wildcards și poate specifica un nume de gazdă și număr de port. Se selectează checkbox-ul **Include subdirectories and files** pentru a aplica setările managementului de trafic pentru toate subdirectoarele și fișierele URL-ului.



This QoS policy applies to:

- ● All applications
- ○ Only applications with this executable name:

  Example: application.exe or %ProgramFiles%\application.exe
- ○ Only HTTP server applications responding to requests for this URL:

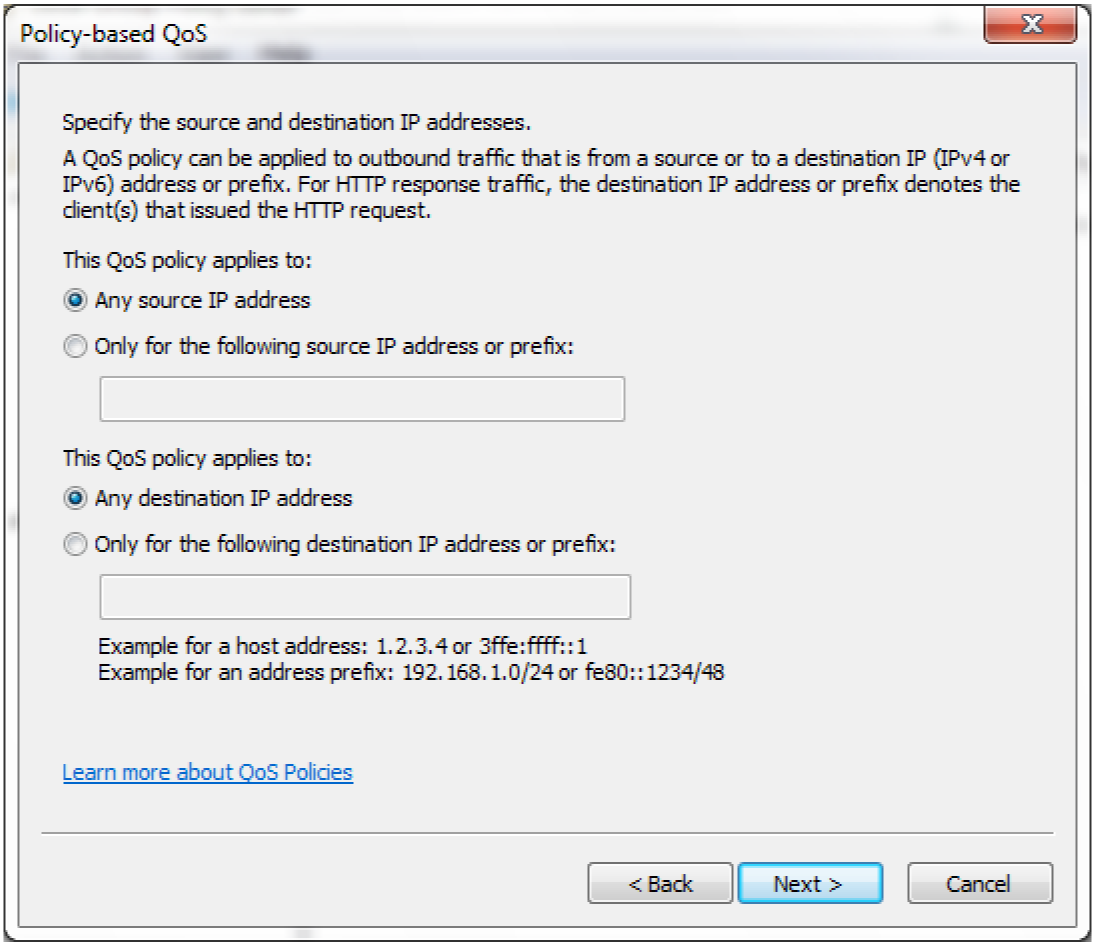
  ☐ Include subdirectories and files

  Example: http://myhost/training/ or https://*/training/
  Example of non-standard TCP port: http://myhost:8080/training/ or https://myhost:*/training/

IP Addresses tab (pagina 3 a Wizard-ului)

Item	**Detalii**
Any source IP address	Implicit. Aplică valoarea DSCP și rata de throttle specificată pe pagina 1.
Only for the following source IP address or prefix	Aplică valoarea DSCP și rata de throttle specificată la pagina 1 pentru trafic extern de la o adresă IP sursă specificată. Formatul adresei poate fi: • O adresă IPv4 precum 1.2.3.4. Dacă adresa este de definită de RFC 1918 cu link-local scope, trebuie să utilizeze notație cu lungimea prefixului. • O adresă IPv4 utilizând notația lungimii prefixului de adresă precum 192.168.1.0/24. • O adresă IPv6, precum 3ffe:ffff::1. Trebuie să utilizeze notație cu

	prefix dacă e link-local scope. - O adresă IPv6 cu prefix, precum fe80::1234/48.
Any destination IP address	Implicit. Aplică valoarea DSCP și rata de throttle specificate (în pagina 1) traficului extern, indiferent de adresa IP sau trafic.
Only for the following destination IP address or prefix	Aplică valoarea DSCP sau rata de throttle pe Policy Profile tab(pagina 1) traficului extern legat de o adresă IP destinație care se specifică. Se poate specifica adresa IP în oricare din aceste formate: - O adresă IPv4 precum 1.2.3.4. Dacă adresa este de definită de RFC 1918 cu link-local scope, trebuie să utilizeze notație cu lungimea prefixului. - O adresă IPv4 utilizând notația lungimii prefixului de adresă precum 192.168.1.0/24. - O adresă IPv6, precum 3ffe:ffff::1. Trebuie să utilizeze notație cu prefix dacă e link-local scope. - O adresă IPv6 cu prefix, precum fe80::1234/48.



Specify the source and destination IP addresses.

A QoS policy can be applied to outbound traffic that is from a source or to a destination IP (IPv4 or IPv6) address or prefix. For HTTP response traffic, the destination IP address or prefix denotes the client(s) that issued the HTTP request.

This QoS policy applies to:

● Any source IP address

○ Only for the following source IP address or prefix:

This QoS policy applies to:

● Any destination IP address

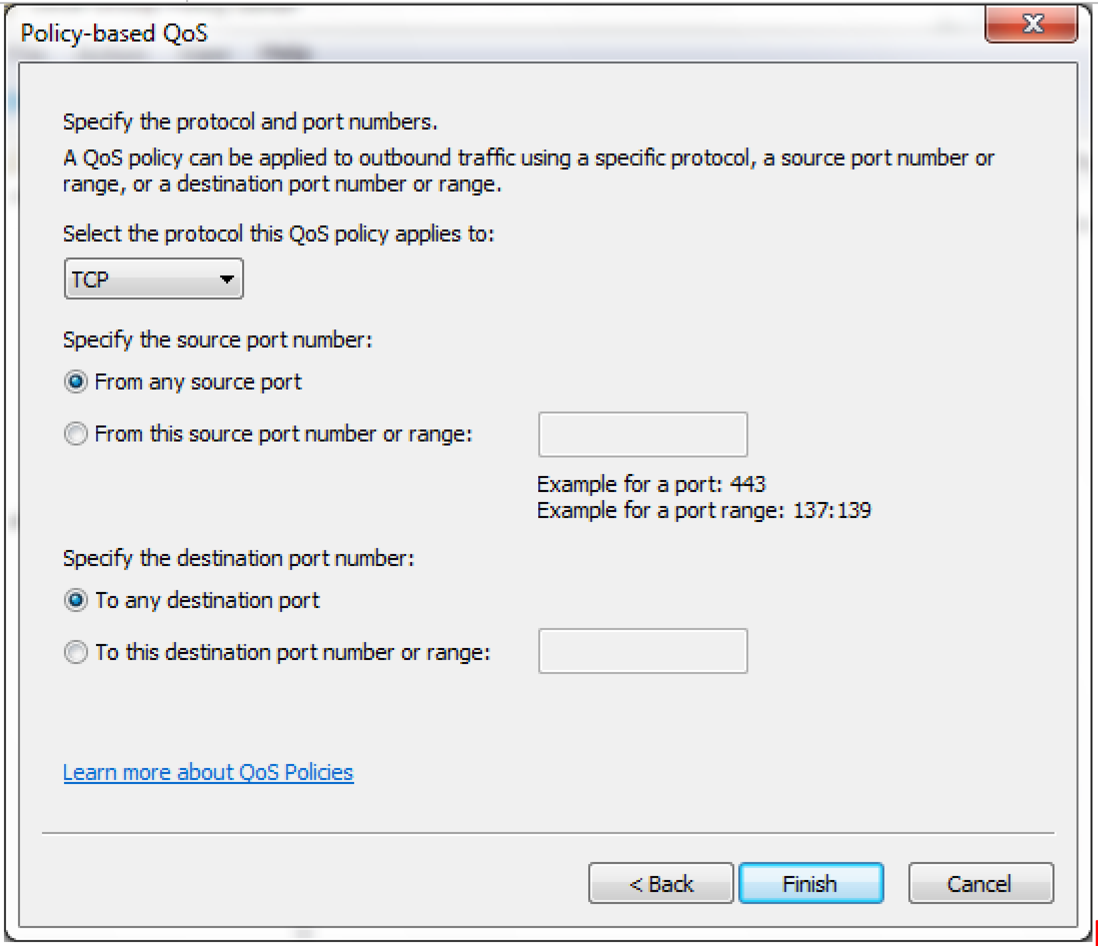
○ Only for the following destination IP address or prefix:

Example for a host address: 1.2.3.4 or 3ffe:ffff::1
Example for an address prefix: 192.168.1.0/24 or fe80::1234/48

Protocols and Ports tab (**Wizard page 4**)

Item	**Detalii**
Select the protocol this QoS policy applies to:	Alege aplicarea valorii DSCP și a ratei de throttle specificată la pagina 1(**Policy Profile**). Pentru trafic extern TCP, UDP sau amândouă.
From any source port	Aplică valoarea DSCP și rata de throttle specificate pe pagina 1 pentru trafic extern, indiferent de numărul portului sursă al traficului.
From this source port number or	Aplică valoarea DSCP și rata de throttle specificate pe pagina 1 doar pentru trafic cu numărul portului sursă sau gama specificate. Se poate introduce un număr de port între 1 și 65535 sau o gamă de porturi, în

range	formatul „Low:High”(Mic:Mare), unde Low și High reprezintă limitele inferioare și superioare ale gamei de porturi. Low și High trebuie să reprezinte un număr între 1 și 65535. Nu se permite spațiu între două puncte (:) și numere.
To any destination port	Aplică valoarea DSCP și rata de throttle specificate pe pagina 1 pentru traficul extern, indiferent de numărul portului destinație al traficului.
To this destination port number or range	Aplică valoarea DSCP și rata de throttle specificate pe pagina 1 doar pentru trafic cu numărul portului destinație sau gama specificate. Se poate introduce un număr de port între 1 și 65535 sau o gamă de porturi, în formatul „Low:High”(Mic:Mare), unde Low și High reprezintă limitele inferioare și superioare ale gamei de porturi. Low și High trebuie să reprezinte un număr între 1 și 65535. Nu se permite spațiu între două puncte (:) și numere.



Policy-based QoS

Specify the protocol and port numbers.

A QoS policy can be applied to outbound traffic using a specific protocol, a source port number or range, or a destination port number or range.

Select the protocol this QoS policy applies to: TCP

Specify the source port number:

● From any source port

○ From this source port number or range:

Example for a port: 443
Example for a port range: 137:139

Specify the destination port number:

● To any destination port

○ To this destination port number or range:

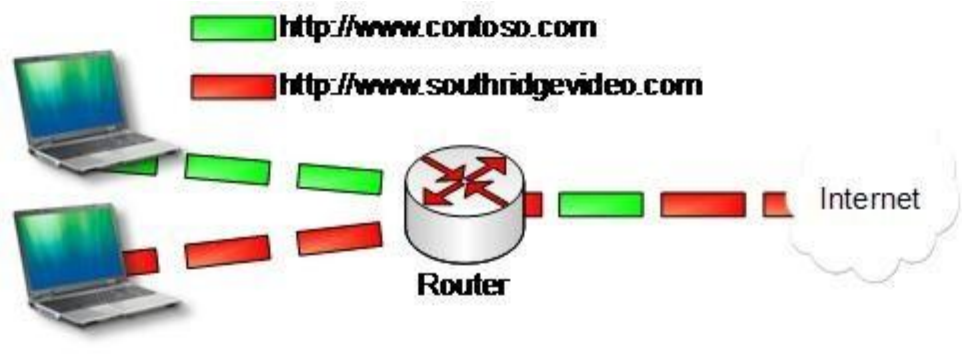
[3]

QoS bazat pe URL în Windows 7 și Windows Server 2008 R2 (URL-based QoS)

Adăugarea de lărgime de bandă nu poate rezolva orice problemă din rețea. Orice conexiune de rețea, când este utilizată la maxim, va cauza încetinirea comunicațiilor în timp ce routerul este forțat să așeze în coadă traficul extern. Asta se întâmplă deseori cu o conexiune WAN sau Internet deoarece traficul de la clienți multipli pe un high-speed LAN trebuie să partajeze o conexiune de viteză mai mică.

De exemplu, dacă o organizație are o conexiune LAN 1000 Mbps și o conexiune Internet 10 Mbps, calculatoarele pot trimite cereri în LAN router-ului mult mai rapid decât ar putea redirecționa routerul cererile către Internet. În acest scenariu, router-ul trebuie să mențină cererile externe în coadă și să trimită fiecare cerere când mai multă bandă este disponibilă. Implicit, router-ele trimit trafic extern din coadă pe principiul FIFO(first-in, first-out). Așadar, traficul critic ar putea aștepta în coadă în urma traficului mai puțin critic.

Figura de mai jos ilustrează 2 clienți trimițând trafic către 2 site-uri Web: www.contoso.com (un website critic intern) și www.southridgevideo.com (un site Web personal non-critic). După cum figura demonstrează, router-ul tratează pachetele la fel, și pachetele destinate pentru www.southridgevideo.com pot fi trimite după pachetele destinate pentru www.contoso.com



Fără QoS traficul cu prioritate joasă poate fi trimis înainte de traficul cu prioritate mare.

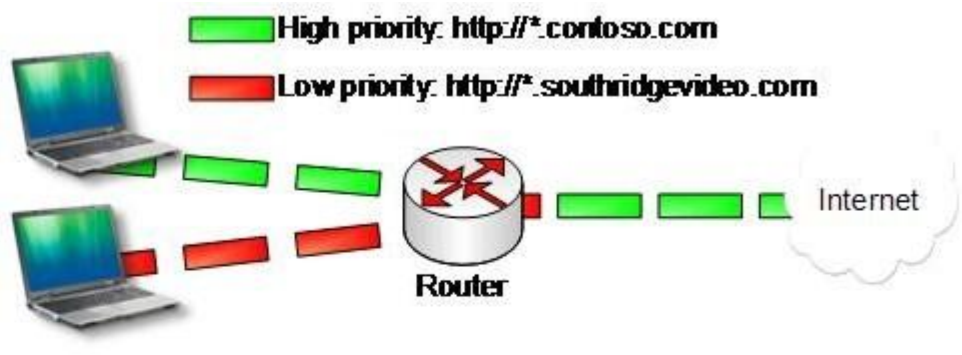
Când profesioniștii IT configurează QoS, Windows marchează pachetele externe cu un număr DSCP (Differentiated Services Code Point). Router-ele examinează această valoare DSCP pentru a determina prioritatea pachetului. Dacă o conexiune de rețea este utilizată la maxim și router-ul ține pachetele într-o coadă, pachetele cu prioritate mai mare sunt trimite înaintea pachetelor cu prioritate joasă, suprapunând comportamentul implicit FIFO. Așadar, QoS poate menține sensibilitatea răspunsului la aplicații critice de rețea chiar și când rețeaua e ocupată.

La versiunile anterioare de Windows, profesioniștii IT puteau specifica aplicațiilor adrese IP, numere de porturi pentru a determina prioritățile QoS. Cu acest nivel de detaliu, profesioniștii IT puteau prioritiza traficul din baza de date peste Web și trafic e-mail – o capabilitate utilă. Aceștia puteau de asemenea să prioritizeze traficul către un server critic peste traficul unui server mai puțin critic.

Totuși, odată cu creșterea de servicii Web și consolidarea aplicațiilor server, profesioniștii IT ar avea nevoie de control mai fin asupra modului în care Windows prioritizează traficul Web. De exemplu, un singur server intranet ar putea găzdui o aplicație service client critică și un forum de discuții non-critic pe același server. Serviciile Web sau aplicațiile pe un singur server partajează o adresă IP comună, limitând valoarea prioritizării bazate pe IP. Profesioniștii IT ar trebui să poată atribui priorități diferite aplicațiilor Web și site-urilor pe un singur server.

Windows 7 permite profesioniștilor IT să prioritizeze traficul Web bazat pe URL. Cu QoS bazat pe URL, profesioniștii IT pot să se asigure că traficul Web important este procesat înainte de traficul mai puțin important, îmbunătățindu-se performanța în rețelele ocupate. Astfel, profesioniștii IT pot atribui prioritate mai mare traficului Web pentru site-uri Web interne critice decât site-urilor Web externe, maximizându-se performanța când rețeaua este ocupată. Similar, dacă utilizatorii vizitează site-uri Web nerelatate cu munca de la birou, ce consumă o parte mare din banda rețelei, profesioniștii IT pot atribui acelui trafic o prioritate mică așa că traficul celălalt nu e afectat.

Cu QoS bazat pe URL, profesioniștii pot de asemenea să configureze o parte din calea URL(Uniform Resource Identifier). De exemplu, profesioniștii IT pot atribui adresei http://contoso.com/cust_serv/ o prioritate mare și la http://contoso.com/forum/ o prioritate joasă. Profesioniștii IT pot configura QoS utilizând setările Group Policy (gpedit.msc).



QoS bazat pe URL permite profesioniștilor IT să prioritizeze traficul Web

[4]

QoS în Windows Server 2012.

Implementarea QoS în Windows Server 2008 R2 e mai mult o soluție de throttling a lărgimii de bandă decât un sistem de rezervare de bandă propriu-zis din punct de vedere tehnic. În Windows Server 2008 R2 implementarea QoS permitea unui administrator să dicteze cantitatea maximă de bandă pe care o putea consuma o mașină virtuală. Aceasta este o tehnologie similară cu cea de la ISP.

Chiar dacă conceptul de throttling încă există în Windows server 2012, Microsoft a mai introdus conceptul de **minimum bandwidth**(viteză de transfer/lărgime de bandă minimă). Minimum bandwidth este o tehnologie de rezervare de bandă care face posibilul de a asigura că diverse tipuri de trafic de rețea primesc întotdeauna lărgimea de bandă de care au nevoie. Asta e într-adevăr o calitate QoS.

Desigur că cel mai mare beneficiu la utilizarea acestei maniere e că acest concept de bandă minimă face posibilul de a rezerva banda în așa fel încât asigură ca fiecare mașină virtuală (Hyper-V) primește suficientă bandă pentru sarcina sa. Dar nu e singurul beneficiu.

În Hyper-V sunt 4 tipuri de trafic de rețea: normal/regular, storage, live migration, cluster.

Un al doilea beneficiu e că Windows Server 2012 va face posibilul de a diferenția diversele tipuri de trafic în rețea care snt produse de mașini virtuale. De exemplu, un administrator poate rezerva mai multă bandă pentru trafic *storage* decât pentru trafic r*egular*.

[6]

Bibliografie

- **(1)The Cable Guy - QoS Support in Windows(XP,Vista,Server 2008), Joseph Davies (**http://technet.microsoft.com/ro-ro/magazine/2007.02.cableguy(en-us).aspx)
- **(2)Quality of Service (QoS) in Windows (**http://technet.microsoft.com/en-us/network/bb530836.aspx**)**
- **(3)Creating and editing a QoS policy in Windows 7 and Windows Server 2008 R2 (**http://technet.microsoft.com/library/cc771283.aspx**)**
- **(4)URL-based QoS (**http://technet.microsoft.com/library/dd637810(WS.10).aspx)
- **(5)Windows XP Quality of Service (QoS) enhancements and behavior (**http://support.microsoft.com/kb/316666**)**
- **(6)QoS in Windows Server 2012 (**http://www.windowsnetworking.com/articles-tutorials/windows-server-2012/QoS-Windows-Server-2012-Part2.html**)**

Notă: Capturile de ecran pentru *Configurarea(crearea,editarea) unei politici QoS în Windows 7* au fost realizate de mine. Orice altă poză aparține autorului articolului referit în bibliografie.

Țulucescu Alexandru, 441A

Suportul pentru QoS in Linux

Kernel-ul Linux proceseaza pachetele primite si genereaza pachetele care sunt trimise in retea. Demultiplexorul de intrare examineaza pachetele primite pentru a determina daca pachetele sunt destinate pentru nodul local. Daca da, acestea sunt trimise la stratul superior pentru prelucrare ulterioara. Daca nu, trimite pachetele la blocul de expediere. Blocul de expediere, care poate, de asemenea, a primit pachetele generate local din stratul superior, se uiti in tabela de rutare si determina urmatorul hop pentru pachet. Dupa aceasta, pune in coada pachetele care trebuie transmise pe interfata de iesire. In acest moment de control traficului din Linux intra in joc. Controlul traficului din Linux poate fi folosit pentru a construi o combinatie complexa de discipline de punere in coada, clase si filtre care controleaza pachetele care sunt trimise pe interfata de iesire.

Din punct de vedere al implementarii, asta inseamna ca atunci cand disciplinele de punere in coada sunt create pentru un dispozitiv, un pointer la coada se mentine in structura (in include/netdevice.h). Stratul IP, dupa adaugarea informatiilor de antet necesare intr-un pachet (in net/ipv4/ip_output.c), apeleaza functia dev_queue_xmit (in net/core/dev.c).

Suportul pentru QoS in Linux este format din urmatoarele trei blocuri de baza, si anume:

- **Discipline de punere in coada**
- **Clasa**
- **Filtre/Politici**

Disciplinele punere in coada formeaza un block de baza pentru suportul pentru QoS in Linux. Se prezinta, de asemenea, diferitele discipline de punere in coada care sunt suportate in linux. Fiecare dispozitiv de retea are o coada de asteptare asociata. Exista 11 tipuri de discipline de punere in coada, care sunt in prezent suportate in Linux, acestea include:

- Coada Bazata pe Clasa (CBQ)
- Fluxul Galeata cu Jetoane (TBF)
- Clark-Shenker-Zhang (CSZ)
- Primul venit, primulafara (FIFO)
- Prioritate
- Egalizator de Trafic(TEQL)
- Coada Stohastica (SFQ)
- Modul de Transfer Asincron (ATM)
- Detectie Devreme Aleatoare (RED)
- RED Generalizat (GRED)
- Marker Diff-Serv (DS_MARK)

Cozile sunt identificate printr-un handle <numar major:numar minor> unde numarul minor este zero pentru cozi. Handle-urile sunt folosite pentru a asocia clasele cu disciplinele de punere in coada. Clasele sunt discutate in subsectiunea urmatoare.

Disciplinele de punere in coada si clasele sunt legate una de alta. Prezenta claselor si semanticilor lor sunt proprietati fundamentale ale disciplinelor de punere in coada. In schimb, filtrele pot fi combinate arbitrar cu disciplinele de apunere incoada si clasele, cat timp disciplinele de punere incoada au clase. Nu toate disciplinele de punere in coada sunt asociate cu clase. De exemplu, Fluxul Galeata cu Jetoane (TBF) nu are nici o clasa asociata.

Unul dintre principalele avantaje ale suportului pentru QoS in Linux este flexibilitatea cu care combinatiile de cozi si clase pot fi create. Fiecare disciplina de punere in coada poate avea mai multe clase. Aceste clase nu stocheaza pachetele, dar in schimb, utilizaeaza o alta disciplina punere in coada in acest scop, care, la randul ei, poate avea mai multe clase si asa mai departe. Aceasta flexibilitate face suportul pentru QoS in Linux unic.

Atunci cand un nucleu Linux configurat pentru suport pentru QoS este pornit, functia net_dev_init (in net/core/dev.c) apeleaza functia pktsched_init (in net/sched/sch_api.c) pentru a initializa unitatea de control al traficului in kernel-ul Linux. In pktsched_init, disciplinele de punere incoada care au fost compilate in kernel sunt toate inregistrate si initializate. Pointerii pentru accesarea functiilor tc_ctl_qdisc, tc_dump_qdisc, tc_ctl_tclass si tc_dump_tclass, care sunt folositi pentru a efectua diferite operatii pe discipline de punere in coada si clase sunt, de asemenea, initializate in pktsched_init.

Functiile care sunt suportate pe discipline de punere in coada diferite sunt prezentate in sectiunile urmatoare. Aceste functii sunt definite in structura Qdisc_ops din include/net/pkt_sched.h si sunt:

- Enqueue
- Dequeue
- Requeue
- Drop
- Init
- Reset
- Destroy
- Dump

Functia Enqueue pune in coada un pachet cu disciplina de punere in coada. Pachetele sunt puse in coada in felul urmator. Dupa cum am aratat mai sus in sectiunea anterioara, cand stratul IP solicita dev_queue_xmit, functia enqueue a disciplinei de punere in coada atasata dispozitivului este apelata.

In functia enqueue a unei discipline de punere in coada, filtrele sunt rulate unul cate unul, pana cand se produce o potrivire. Odata ce are loc potrivirea, functia enqueue a disciplinei de punere incoada "detinuta" de acea clasa este executata.

Functia cbq_classify este utilizata pentru a aplica filtrele si pentru a determina clasa din care face parte pachetul. Dupa aceea, functia enqueue a disciplinei de punere in coada detinuta de acea clasa este apelata. Aceasta disciplina de punere in coada poate avea propriile sale clase, care, la randul lor, pot fi asociate cu alte discipline de punere incoada, si asa mai departe, ceea ce face utilizarea flexibila, astfel cum a fost discutat anterior.

In acest punct, este important de mentionat ca, atunci cand o clasa este creat, disciplina de punere in coada implicita pe care o detine este o coada FIFO cu prioritati.

Acest lucru poate fi schimbat prin facerea unei operatii de draft, care va fi discutata mai tarziu in sectiunea despre clase.

Functia Dequeue scoate din coada un pachet pentru trimitere. Returneaza urmatorul pachet care trebuie sa fie trimis pe interfata de iesire. Acest pachet este determinat de planificatorul din disciplina depunere in coada. Planificatorul poate fi foarte complicat pentru discipline de punere in coada complexe, cum ar fi CBQ. In acelasi timp, acesta poate fi foarte simplu, in cazul unei cozi FIFO.

Dupa ce am prezentat functia dequeue a disciplinelor de asteptare, sa prezentam acum locurile in care functia de dequeue este invocata. Ori de cate ori un pachet este pus in coada in dev_queue_xmit, functia qdisc_wakeup (in include/net/pkt_sched.h) este invocata intr-o incercare de a trimite pachetul care tocmai a fost pus in coada. qdisc_wakeup invoca functia qdisc_restart (in net/sched/sch_generic.c), care invoca functia dequeue a disciplinei de punere in coada atasata la aparat. Functia dequeue returneaza urmatorul pachet care trebuie sa fie trimis pe interfata. Apoi qdisc_restart invoca hard_start_xmit al dispozitivului pentru a trimite pachete la dispsozitiv. Daca hard_start_xmit nu reuseste pentru un anumit motiv, pachetul este repus in coada in disciplina de punere incoada coada. Functia requeue este discutata intr-o sectiune ulterioara.

qdisc_wakeup mai poate fi invocat si din de handle-urile watchdog timer in planificatoarele CBQ, TBF și CSZ. In functia dequeue ale acestor discipline de punere in coada, cand un pachet este scos dincoada pentru a fi trimis pe interfata de iesire, un watchdog timer este initiat. Daca dintr-un anumit motiv, qdisc_restart nu trimite pachetul la timp, watchdog timer-ul se opreste si se apeleaza qdisc_restart.

Functia Requeue a unei discipline de punere in coada repune in coada un pachet pentru transmisie. Dupa scoaterea pachetului din coada, daca dintr-un un motiv oarecare, pachetul nu se transmite, pachetul trebuie pus inapoi in coada la aceeasi pozitie din care a fost scos din coada. Motivele pentru care hard_start_xmit esueaza sunt:

- Dispozitivul nu-si poate stabili starea de ocupat inaintea transmisiei
- Dispozitivul are el insusi bug-uri
- Optiunea fastroute este activata

Pentru o coada FIFO simpla, functia requeue ar trebui sa puna pachetul inapoi la capul cozii. Funcția requeue este diferita de functia enqueue, pentru ca functia requeue ar trebui sa puna pachetul anapoi in acelasi loc de unde a fost scos din coada, si nu ar trebui sa apare in statisticile care sunt cozii, deoarece a fost deja procesat de catre o functie enqueue.

Functia Init a unei discipline de punere in coada este folosita pentru a initializa si configura parametrii unei discipline de punere in coada atunci cand este creata. Functiei init ii pot fi pasate argumentele utilizate pentru configurarea disciplinei de punere in coada. Fiecare dintre disciplinele de punere in coada au nevoie de seturi diferite de parametri in timpul procesului de configurare initiala. Acesti parametri vor fi discutati in detaliu in cadrul prezentarii utilizarii caracteristicilor de control al traficului in Linux. Toate fisierele aferente planificatorului, de exemplu, sch_cbq.c, sch_tbf.c etc contin structura de date a planificatorului, adica parametrii care vor fi utilizati de planificator pentru determinarea urmatorului pachet care trebuie trimis. Aceasta structura de date poate fi foarte simpla pentru anumite discipline de punere in coada, de exemplu, FIFO cu prioritati, sau poate fi foarte complicata pentru anumite discipline de punere in coada, de exemplu CBQ.

Singurii parametrii de care nevoie un planificator FIFO este lungimea maxima a cozii.

Functia Reset a unei discipline punere in coada este folosit pentru a reseta disciplina de de punere in coada la starea sa initiala. Ea sterge toate disciplinele de asteptare, cronometrele sint oprite, etc. Resetarea unei discipline de punere in coada mai face o resetare a disciplinei de punere in coada a claselor ale acestei discipline de punere in coada.

Functia Destroy a unei discipline de asteptare este utilizat pentru a elimina disciplina de punere in coada. Se mai elimina, de asemenea, toate clasele și filtrele asociate cu disciplina de punere in coada. Acest lucru este pus in aplicare in functia de qdisc_destroy (in net/sched/ sch_generic.c).

Functia Dump este utilizata pentru a sterge date de diagnosticare asociate cu o disciplina de punere in coada. Fiecare disciplina de punere in coada mentine date diferite de diagnosticare care sunt sterse atunci cand functia de dump este invocata.

Clasele

Dupa cum am mentionat inainte, cozile si clase sunt legate una de alta. Fiecare clasa detine o coada, care in mod implicit este o coada FIFO. Atunci cand functia enqueue a unei discipline de punere in coada este apelata, disciplina de punere in coada aplica filtrele pentru a determina clasa din care face parte pachetul. Apoi apeleaza functia enqueue a disciplinei de punere in coada care este deținuta de aceasta clasa.

Exista doua modalitati prin care o clasa poate fi identificata. Una dintre ele este prin identificatorul de clasa, care este specificat de utilizator. Celalalt identificator, care este utilizat in cadrul kernel-ului pentru a identifica o clasa, este identificatorul intern. Acest ID este unic si este atribuit de disciplina de punere in coada. ID-ul de clasa este de tip u32, in timp ce ID-ul intern este un numar intreg lung fara semn. Cele mai multe functii in clase folosesc ID-ul intern pentru a identifica clasa. Totusi exista cateva functii (cum ar fi functiile get si change, care vor fi discutate mai tarziu) care utilizeaza si ID-ul de clasa.

Mai multe ID-uri de clasa se pot mapa la acelasi ID-ul intern, totusi ID-ul de clasa va transmite informatii suplimentare de la clasificator la disciplina de punere in coada sau la clasa.

ID-ul de clasa, similar cu un identificator de disciplina de punere in coada, este structurat in forma unui <numar major:numarul minor>. Numarul major corespunde instantei lor de disciplina de punere in coada in timp ce numarul minor identifica clasa din acea instanta.

Nu toate disciplinele de punere in coada suporta clase. Cei care suporta clase sunt disciplinele de punere in coada CBQ, DS_MARK, CSZ și p-FIFO. Restul disciplinelor de punere in coada nu suporta clase. Acum se vor prezenta functiile care pot fi efectuate pe clase. Aceste functii sunt definite in structura Qdisc_class_ops din include/net/pkt_sched.h. Urmatoarele operațiuni sunt permise pentru manipularea claselor in cadrul diferitelor discipline de punere in coada care suporta clase. Acesta este definit in include/net/pkt_sched.h.

- Graft
- Get
- Put
- Change
- Delete
- Walk
- Tcf_chain
- Bind_tcf
- Unbind_tcf
- Dump_class

Funcția Graft aplicata unei clase este folosita pentru a atasa o disciplina noua de punere in coada intr-o clasa. Dupa cum sa mentionat in secțiunea anterioara, disciplina punere in coada implicita atasata unei clase atunci cand este creata, este o coada FIFO. Pentru a schimba aceasta disciplina de punere in coada, o operațiune de graft se face pe clasa.

Functia Get este folosita pentru a returna ID-ul intern al unei clase, fiind dat ID-ul clasei sale. Functia get incrementeaza numarul de utilizari a clasei.

Functia Put este invocata atunci cand o clasa referita anterior folosind funcția get este de-referintiata. Aceasta decrementeaza numarul de utilizari a clasei. Daca numarul de utilizari ajunge la zero, put poate elimina clasa in sine.

Functia Change aplicata unei clase este folosita pentru a schimba proprietatile asociate unei clase. Totusi, funcția change este mai este utilizata pentru a crea clase uneori.

Functia Delete aplicata unei clase este folosita pentru a sterge clasa. Ea determina utilizarea clasei, prin verificarea numarului de referinte, si, dacs este zero, dezactiveaza si elimina clasa.

Funcția Walk aplicata unei clase este folosita pentru a itera peste toate clasele unei discipline de punere in coada si invoca o funcție de callback pentru fiecare clasa. Este de obicei folosita pentru a obtine date de diagnosticare pentru toate clasele unei discipline de punere in coada.

Functia tcf_chain aplicata unei clase este utilizata pentru a returna ancora la lista de filtre care sunt asociate cu o clasa. Fiecare clasa este asociata cu o lista de filtre, care sunt folosite pentru a identifica pachetele care apartin unei anumite clase. Dupa cum sa menționat mai sus, pachetele cu proprietati diferite pot sa se mapeze la aceeasi clasa. De exemplu, pachetele din doua surse diferite pot sa se mapeze la aceeași clasa. Ca urmare, pot exista mai multe filtre asociate unei clase. Filtrele sunt discutate in detaliu in sectiunea urmatoare.

Functia bind_tcf este folosita pentru a atasa o instanta a unui filtru la o clasa.

Funcția unbind_tcf este utilizata pentru a elimina o instanta a unui filtru atasata unei clase.

Functia dump class aplicata unei clase este folosita pentru a sterge date de diagnosticare privind clasa. Exista multe date despre clase care sunt mentinute si funcția dump este folosita pentru a observa aceste valori.

Filtrele sunt utilizate pentru a clasifica pachetele pe baza anumitor proprietati ale pachetelor, de exemplu, byte-ul TOS din header-ul IP, adresele IP, numerele de port etc. Este invocata atunci cand functia enqueue a unei discipline de punere in coada este invocata. Disciplinele de punere in coada folosesc filtrele pentru a atribui pachetele primite la una din clase.

Filtrele pot fi mentinute pe clasa sau pe disciplina de punere in coada pe baza modului in care e facuta disciplina de punere in coada. Dupa cum am mentionat in sectiunea anterioara, filtrele sunt menținute in listele filtre. Lista de filtre este specificata ca o struct tcf_proto, din include/net/pkt_cls.h.

Aceasta structura este folosita pentru a reprezenta listele de filtre si este mentinuta de clasele si disciplinele de punere in coada. De exemplu, structura cbq_class din net/sched/sch_cbq.c mentine lista de filtre utilizand structura tcf_proto. Functia tcf_chain aplicata claselor, descrisa in sectiunea anterioara, este utilizata pentru a rturna ancora lunei liste de filtre, care poate fi folosita pentru a traversa lista de filtre. Listele de filtre sunt ordonate dupa prioritate, in ordine crescatoare. De asemenea, intrarile sunt keyed de catre protocolul pentru care se aplica, de exemplu, IP, UDP, etc. Filtrele pentru acelasi protocol la aceeasi lista de filtre trebuie sa aiba valori diferite ale prioritatii. Numerele de protocol sunt folosite in skb->protocol si sunt definite in include/linux/if_ether.h.

Filtrele mai pot avea si o structura interna: aceasta poate controla elementele interne, care sunt referite printr-un handle. Acestea sunt handle-uri lungi de 32-biti, dar nu sunt impartite in numere majore si minore, ca ID-urile de clasa. Handle-ul 0 se refera la filtrul in sine. Ca si clasele, filtrele au mai au si un ID intern, care poate fi obtinut cu ajutorul unei functii get.

Atunci cand functia enqueue a unei discipline este invocata, functia tc_classify din include/net/pkt_cls.h este invocata pentru a clasifica pachetul.

Acum se vor prezenta functiile care pot fi efectuate pe filtre. Functiile sunt definite in structura tc_proto_ops din include/net/pkt_cls.h.

- Classify
- Init
- Destroy
- Get
- Put
- Change

- Delete
- Walk
- Dump

Functia <u>Classify</u> aplicata unui filtru este folosita pentru a potrivi un pachet cu o clasa pe baza unor anumite proprietati ale pachetului. Rezultatul oricarei clasificari poate fi una din patru valori de returnare din functia tcf_police din net/sched/police.c și anume TC_POLICE_UNSPEC, TC_POLICE_OK, TC_POLICE_RECLASSIFY sau TC_POLICE_SHOT. Policer-ul este discutat mai in detaliu in sectiunea urmatoare. In acest punct, este suficient sa se inteleaga ca functia tc_classify returneaza TC_POLICE_UNSPEC atunci cand nici un filtru potrivit nu este gasit pentru pachet. Daca nu, clasificatorul completeaza structura tcf_result (definita in include/net/pkt_cls.h) si il returneaza. Structura tcf_result contine ID-ul intern, precum si ID-ul de clasa a clasei in care apartine pachetul.

Clasificatorul de rute clasifica pachetele pe baza pe adresa IP-ului de destinatie. In functia route_classify, destinatia este asociata cu o structura dst_entry (in include/net/dst.h). ID-ul de clasa al clasei este stocat in campul tclassid din structura dst_entry. Daca destinatia la care pachetul trebuie sa fie trimis este determinata, ID-ul de clasa corespunzator este returnat in structura tcf_result. In general, filtrele sunt mai asociate si cu policers, pentru a determina daca un flux este in profil.

Functia <u>Init</u> aplicata unui filtru este folosita pentru a initializa parametrii unui filtru.

Structura tcindex_data, a carei definitie este disponibil in net/sched/cls_tcindex.c, este initializata in functia tcindex_init. Masca si shiftarea, care sunt utilizate in combinatie pentru a determina daca un handle este setate la 0xFFFF și respectiv 0. Detaliile cu privire la clasificatorul tcindex sunt discutate in detaliu mai tarziu. Functia de init este invocata din functia de tc_ctl_tfilter dinn net/sched/cls_api.c, care se apleleaza ori de cate ori un filtru este adaugat, eliminat sau modificat.

Functia <u>Destroy</u> aplicata unui filtru este utilizata pentru a elimina un filtru. Funcția cbq_destroy care a fost discutata anterior, mai apeleaza, de asemenea, si sunctia destroy. Daca filtrul sau oricare din elementele sale sunt inregistrate in clase, functia destroy aplicata unui filtru apeleaza functia unbind_tcf pentru a-l de-inregistra de la acele clase. Functia unbind_tcf a fost discutat in sectiunea anterioara la clase.Mai elimina, de asemenea, orice policer care a fost atasat la filtru.

Functia <u>Get</u>. Dupa cum sa mentionat anterior, fiecare filtru are un ID intern corespunzator handle-ului. Aceasta mapare poate fi obțtnuta cu ajutorul functiei get aplicata filtrului. Acest lucru este similar cu funcția get aplicata unei clase. Structura tcf_result, care este folosita in cazul claselor, este utilizata si in cazul filtrelor.

Functia Put aplicata unei clase este utilizata pentru a de-referentia un filtru de care a fost anterior referentiat cu functia get. Dar, in general, funcția put nu este niciodata invocata. O analiza a fisierelor clasificatorului (fisierele din net/sched/ care incep cu prefixul cls) va indica acest lucru.

Functia Change aplicata unui filtru este folosita pentru a schimba proprietatile unui filtru. Este similara cu functia change aplicata claselor si disciplinelor de punere in coada. Parametrii de configurare sunt pasati folosindu-se un mecanism care este similar cu modul in care parametrii sunt pasati pentru clase si disciplinele de punere in coada. Atunci cand functia de change este invocata pentru un filtru, daca se adauga elemente noi la filtru, sau daca se adauga un nou filtru la o clasa, functia unbind_tcf este apelata pentru a elimina legatura dintre clasa și filtru, care este apoi urmata de functia pe bind_tcf aplicata unei clasa pentru a lega filtrul cu proprietatile noi la clasa. Daca vreun policer este atasat la filtru, apoi proprietatile lui sunt, de asemenea, modificate.

Functia Delete aplicata unui filtru este folosita pentru stergerea unui anumit element al filtrului. Asa cum a fost discutat anterior, pentru a sterge intregul filtru, funcția destroy este invocata pentru filtru. Ca si în cazul funcției destroy, functia delete apleleaza functia unbind_tcf pentru clasa la care elementul este atasat. Policer-ul atasat elementului este, de asemenea, eliminat.

Functia Walk aplicata unui filtru este folosita pentru a itera peste toate elementele unui filtru si invoca o funcție de callback pentru fiecare element. Este de obicei folosita pentru a obtine date de diagnosticare pentru toate elementele unui filtru.

Functia Dump aplicata unui filtru este folosita pentru a sterge date de diagnosticare despre filtrul si una sau mai multe elemente. Exista multe date despre filtre care sunt mentinute și funcția dump este folosita pentru a obtine aceste valori.

Bibliografie

QoS Support in Linux - http://qos.ittc.ku.edu/howto/node3.html