Gestió de l'ample de banda en xarxes d'àmbit educatiu

Jordi Terren Pons, Xavi Vilajosana Guillén, i David Megías Jiménez

Màster en Programari Lliure
Universitat Oberta de Catalunya, Av. Tibidabo 39-43, 08035 Barcelona, Espanya
{jterren, xvilajosana, dmejias}@uoc.edu

20 Gener, 2011

Resum. L'educació és necessàriament i especialment en el present un àrea en constant evolució. En l'actualitat dels centres educatius amb la implantació de noves tecnologies a l'aula s'observa una creixent demanda i consolidació de l'us de plataformes educatives i altres serveis en xarxa que amplien el ventall de recursos disponibles a l'aula. La incorporació de dispositius dotats de connectivitat a les aules, potenciada per l'aparició al mercat de dispositius amb prestacions que disposen d'una llarga autonomia, mínim pes, dimensions adequades i a preus assequibles, juntament amb els programes de suport de governs que en promouen i subvencionen l'ús com el projecte 1x1[26] de la Generalitat de Catalunya, han provocat en els centres educatius aquests canvis que afecten tant a les metodologies d'ensenyament com a les infraestructures de xarxa, requerint una d'adaptació d'aquestes per poder donar suport a les necessitats d'aquest nou escenari, especialment relacionades amb la gestió l'ample de banda, indispensable per poder oferir el servei de xarxa requerit per les aplicacions.

L'augment constant de la demanda de recursos de xarxa i el dèficit

de connectivitat dels centres educatius provoquen colls d'ampolla en els accessos a Internet que de no ser correctament gestionats provoquen la congestió global del sistema.

La seva gestió esdevé doncs necessària i cal destacar l'especial importància de que aquesta tingui un alt grau d'adaptació al medi, que cobreixi els patrons de necessitats i faciliti la comprensió global del sistema i en conseqüència la seva gestió.

En l'article s'analitza prèviament l'estat de l'art de la gestió de l'ample de banda en entorns educatius, presentant en base a diverses classificacions anteriors solucions i experiències proposades. Amb la proposta presentada, mitjançant els experiments de simulació efectuats i els tests en entorns reals es tracta de comprovar-ne el correcte comportament, demostrant la utilitat de la mateixa alhora de fer la gestió de l'ample de banda dels centres.

1 Introducció

El perfil dels accessos a xarxa de centres educatius, per les característiques dels seus usuaris[18], topologia i usos prioritaris té peculiaritats que s'han recollit i tingut en compte en l'elaboració del patró presentat, per tal que mitjançant aquest es pugui verificar l'encaix de la solució amb la gestió desitjada.

Un factor prioritari tingut en compte alhora de planificar el sistema ha estat l'abús de recursos de xarxa, comú en aquests entorns[19] i que es veu recolzat per el propi control de congestió del protocol tcp. Aquest abús que derivaria en un col·lapse del sistema de no ser correctament gestionat és provocat per un conjunt mínim (estimat entre 1 i 20% segons estudis) d'usuaris[18] [1] però la seva afectació sobre el sistema és global, donat que tendeix a incrementar-se en el grau en que els recursos de xarxa augmenten[13] no es considera un augment de recursos com una solució viable. Una altra dada important és que entre el 30 i 50% del temps de navegació és destinat a l'oci[20]. Serà doncs necessari disposar de mecanismes que regulin l'accés a Internet i en permetin obtenir un correcte funcionament a nivell global. L'augment de dispositius personals i no gestionats per els departaments informàtics dels centres i per tant sense garanties de configuracions ni estats fa inviable confiar la gestió distribuïda als equips finals.

En el cas concret del projecte 1x1[26], implantat per la Generalitat de Catalunya i que es troba actualment iniciant la sisena onada que es basa en treball amb materials remots, situa l'estat de la xarxa en una situació prioritària i de risc per tal de poder garantir el correcte desenvolupament de les tasques docents i l'èxit de la seva consolidació. La disponibilitat i distribució equilibrada dels recursos de xarxa, la protecció contra abusos i permetre una gestió adaptada a les necessitats creixents provocades per l'augment d'usuaris i serveis en xarxa[13], són doncs objectius prioritaris a cobrir per la solució.

Aquest desequilibri que es manté constant amb l'augment el consum alhora que es disposa de més recursos fa que solucions adaptades a previs sistemes [18] segueixin

compartint objectius i per tant siguin valida els plantejaments i alhora justifica la previsió de que aquesta línia de gestió es mantingui valida en el futur.

La distribució d'usuaris amb patrons comuns d'accés a recursos de la xarxa en els centres coincideix amb la seva ubicació física en un moment determinat, determinat per l'horari del centre. La impartició de les diferents matèries s'efectua en espais (aules) físicament independents i dins les que podem identificar 2 rols, alumne i professor. És per això que ha considerat l'aula com a com a agrupació vàlida d'usuaris per a efectuar un tractament estructurat basat en assignació de recursos en blocs.

Per al disseny i validació de la solució proposada s'ha considerat com a prerequisit mínim el proveir suport per els següents escenaris que representen situacions quotidianes en centres educatius.

Taula 1. Relació d'escenaris amb funcionament desitjat

Escenari Real	Funcionament desitjat
Escenari 1: Prohibir l'accés a recursos d'una aula.	Acció: Denegar l'accés de l'aula específica a Internet.
Situació: Realització d'un examen, els alumnes no poden consultar material.	
Escenari 2: Restringir l'accés a recursos al professor.	Acció: Només a l'equip del professor de l'aula tindrà l'accés a Internet.
Situació: Evitar distraccions durant explicacions.	
Escenari 3: El descontrol d'alumnes d'una aula no ha de destorbar el correcte funcionament de la resta d'aules del centre.	Acció: No permetre que l'abús de l'aula afecti als mínims garantits de la resta d'aules del centre. Garantir que la resta d'aules obtenen un mínim ample de banda prèviament establert.
Situació: Aula sense professor o vigilància amb alumnes navegant indiscriminadament.	
Escenari 4: El professor ha de tenir garantit i prioritzat l'accés a recursos docents respecte dels alumnes de l'aula.	Acció: Prioritzar i garantir un ample de banda prèviament especificat per l'accés a Internet de l'equip del professor, que no s'ha de veure afectat davant un possible consum excessiu dels alumnes de l'aula.
Situació: El professor explica utilitzant recursos de la xarxa i alumnes de l'aula accedeixen alhora a Internet (als mateixos o altres recursos).	
Escenari 5:	Acció:

Si no es consumeixen tots els recursos, el sobrant ha de ser aprofitable per altres que el demanin.	Una 'aula ha de tenir la possibilitat d'excedir el seu ample de banda mínim garantit en cas que el sistema no estigui utilitzant el total dels recursos de xarxa, repartint-se amb la resta d'aules que excedeixin dels seus límits garantits en la proporció que s'hagi estipulat.
Situació: El sistema esta global poc carregat però el conjunt d'una aula o vàries excedeix dels mínims prèviament especificats que té garantits.	
Escenari 6: En un moment donat una aula pot necessitar més prioritat.	Acció: Permetre assignar en un moment donat una prioritat superior a una aula en l'accés a Internet. La contundència aplicada dependrà de la criticitat de la situació. Podrà anar des de prioritzar l'accés a recursos excedents fins a la reconfiguració dels mínims garantits.
Situació: En les sessions en que els alumnes fan matriculacions massives o reserves online és interessant que l'aula on es duen a terme les gestions tingui més prioritat que la resta en l'accés del recursos excedents.	
Escenari 7: En cas de funcionament anòmal del sistema, cal poder identificar-ne l'origen.	Acció: El sistema ha de permetre mostrar l'estat del sistema d'una manera senzilla que permeti ajudar en la resolució de l'anomalia.
Situació: Es detecten problemes amb l'accés a Internet.	
Escenari 8: Cal poder fer la configuració del sistema en base a patrons en blocs lògics/físics, parlant en termes d'aules físiques, entorns (plantes), grups d'alumnes,...	Acció: La configuració ha d'estar estructurada de manera que es pugui treballar en base a blocs que representaran espais físics reals com aules als que es podran assignar configuracions en bloc.
Situació: En la configuració del sistema es rebran peticions en base a recursos necessaris per aula...	
Escenari 9: Denegació d'accés a recursos que es consideren poc indicats, amb o sense notificació.	Acció: El sistema ha de permetre denegar accés a recursos en xarxa, proveint en cas que calgui d'un avís amb el motiu.
Situació: El centre prohibeix l'accés a certs recursos de caràcter no educatiu.	
Escenari 10:	Acció:

El sistema ha de ser segur	Part de les eines utilitzades en la gestió de l'ample de banda es podran utilitzar en combinació amb aquest per proveir seguretat al sistema.
Situació: A part de les configuracions de gestió d'ample de banda ha de ser compatible amb solucions de securització del sistema.	
Escenari 11: Un mateix recurs és accedit per un gran nombre d'usuaris.	Acció: El sistema ha de proveir funcionalitat de memòria cau de recursos per tal d'evitar un consum repetitiu innecessari de recursos de Internet ,oferint a canvi una copia local.
Situació: Es demana llegir un article o descarregar un treball penjat a la plataforma educativa.	

Coneguts els requisits que marquen les diferències amb els coberts per solucions prèvies existents d'àmbit més general i allunyades de la realitat dels centres, es presenta una proposta de solució recomanada per la gestió més adaptada a l'entorn, fet que derivarà en una configuració més entenedora. En la implementació de la solució la topologia física comú en els centres ha marcat la tecnologia a utilitzar, els punts on efectuar la gestió i els blocs en que s'agrupa la distribució dels recursos d'ample de banda. El transit a gestionar, pràcticament web en la seva totalitat i sense una especial sensibilitat als retards també ha estat clau, concretament, i coincidint amb algunes fonts estudiades, el punt crític en el cas proposat és l'accés a Internet, la solució mitjançant una configuració que integra en un únic punt/equip tots els components (monitor, control i gestió) [2] dona resposta als requisits.

Pel que fa al mètode de restricció d'accés a contingut no educatiu, mentre que algunes solucions aposten per efectuar-ne una prohibició total d'accés[20], altres emfatitzen el fet que sense educar als usuaris[22] [26] en base a un ús amb sentit comú i solidaritat vers la resta d'usuaris és difícil donar solució al problema. Aquest segon grup proposa afegir un cost variable a les comunicacions variant-lo en sentit invers a la càrrega del sistema[1], de manera dinàmica o per franges horàries[9].

Es proposa la implementació de la solució situant l'equip que farà les funcions de gestió en serie amb el transit, situat entre els dispositius d'accés a Internet (independentment del tipus d'accés) i la xarxa interna del centre (o DMZ en cas d'existir). Aquesta solució serà suportada per tres eixos principals d'actuació:

- Protecció/Filtrat: Netfilter (Iptables,Nat, masquerade). L'ús principal per al projecte serà assegurar el correcte flux de les dades (per garantir l'efectivitat del gestor d'ample de banda). Serà responsable de la seguretat del sistema mitjançant patrons d'actuació en base al filtrat a nivell de ports, origen, destí o estat de des comunicacions.
- Cache: Squid [8], Mitjançant el suport del cache, a part de la funció principal d'accelerar connexions i alliberar ample de banda de la connexió a Internet (especialment en navegació guiada) s'utilitzarà per restringir l'accés a recursos no educatius.

- Gestió de l'ample de banda: Iproute2 (TC[3]), És el punt fort de la gestió, efectuarà la sectorització del trafic en base als escenaris definits fent una assignació controlada dels recursos de xarxa en funció de la configuració desitjada en cada moment.

Altres serveis implicats a destacar serà el dhcp per assignar les adreces IP que serviran posteriorment de font de classificació (es proposa assignar IP en base a MAC per als equips coneguts) i el bind9 per a la resolució de noms local que també accelerarà la navegació (i estalviarà trafic d'Internet de consultes DNS).

El fet que els escenaris a cobrir proposats, el maquinari és de propòsit general, l'us de programari lliure i el firmware dels equips de xarxa utilitzats en els tests és compatible amb una gran varietat de dispositius, permet suposar una fàcil implantació amb mínimes modificacions en altres centres educatius.

Estudiats els resultats proporcionats per l'eina Ntop (rebent el trafic global d'Internet del centre amb filtres comuns als centres prèviament aplicats mitjançant l'us de Iptables durant un període de 2 setmanes) s'observa com era d'esperar que un 99,8% del trafic és tcp i que la mida dels paquets es distribueix majoritàriament en dos grups 45% (entre 1024 i 1518 bytes) i 41,4% (entre 64 i 128 bytes).

Organització del document – La secció 2 exposa l'estat de l'art en gestió d'ample de banda emfatitzant els factors i aplicacions compatibles amb entorns educatius distribuint-los en tres vies de classificació principals. La secció 3 defineix diferents mètodes de mesurament del transit. La secció 4 defineix els principals conceptes, consideracions i programari implicats en la proposta presentada. La secció 5 exposa la solució presentada i presenta els resultats dels experiments efectuats tant en l'entorn de proves com en real.

2. Estat de l'art de la gestió de l'ample de banda en centres educatius (categories de solucions)

S'ha observat que existeixen diferents enfocaments per tal de donar solució a la gestió de l'ample de banda. En base als objectius concrets del projecte s'ha efectuat la següent classificació en base a l'observació en aquestes del punts en comú que han ajudat a guiar i justificar la solució recomanada.

2.1 Arquitectura global

Per ser la de caire més global, es proposa l'arquitectura (Intserv[2], difserv) com a una primera classificació, amb una relació directa amb la compatibilitat del maquinari de comunicacions que la implementa, malgrat en una recerca de l'estat de l'art de la gestió de l'ample de banda s'observa força més documentació sobre solucions implementant intserv, per l'entorn d'aplicació tant a nivell de topologia com de maquinari, és difserv la única que pot encaixar i per tant és l'enfoc del projecte.

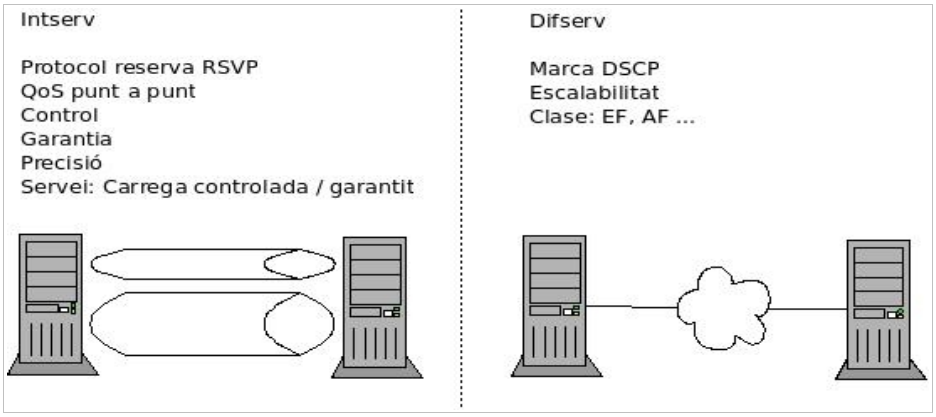
Intserv preveu una garantia de qualitat de servei punt a punt mitjançant el marcatge de

paquets (camp RSVP), fet que en permet aplicar un tracte diferencial obtenint una reserva de camins lògics entre els nodes, alguns exemples d'us d'aquesta arquitectura són ATM i MPLS, els elements que composen els sistemes són costosos, fet que influeix en la manca de simuladors, especialment de caire distribuït[13].

Per altra banda Difserv, basada en el marcatge de paquets (camp DSCP), tot i no oferir garanties de qualitat de servei (retards, disponibilitat, reserves de backup), és una arquitectura més econòmica i escalable que permet gestionar l'ample de banda, basada en 4 elements, disciplines de cua que s'assignen a la interfície o a classes i tenen el paper de decidir l'ordre dels paquets. Classes, agrupació de conjunt de paquets que tenen assignada una disciplina de cua als que s'aplica unes restriccions comunes. Filtres que determinen la classe destí de cada paquet i finalment polítiques que s'encarreguen de controlar el volum de trafic de les classes mitjançant accions de permetre, re-assignar o descartar els paquets.

En poder ser aquesta suportada per els dispositius existents en els centres i cobrir-ne les necessitats, s'ha centrat la recerca en l'observació de solucions basades en aquesta arquitectura.

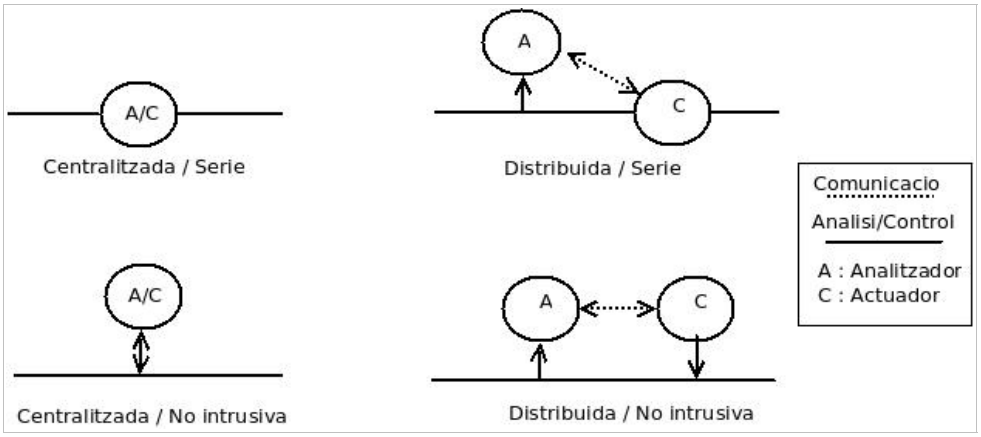
Esquema 1: Intserv vs Difserv



2.2 Topologia global

La ubicació dels elements que formen part del sistema de gestió (eines de mesurament i gestió) dona lloc a quatre possibles blocs de classificació, podent-se resumir els seus efectes en base al intrusisme de les mateixes sobre la xarxa que determina inversament el grau de control que permeten. En la solució s'ha optat per la situació en serie de tots dos elements.

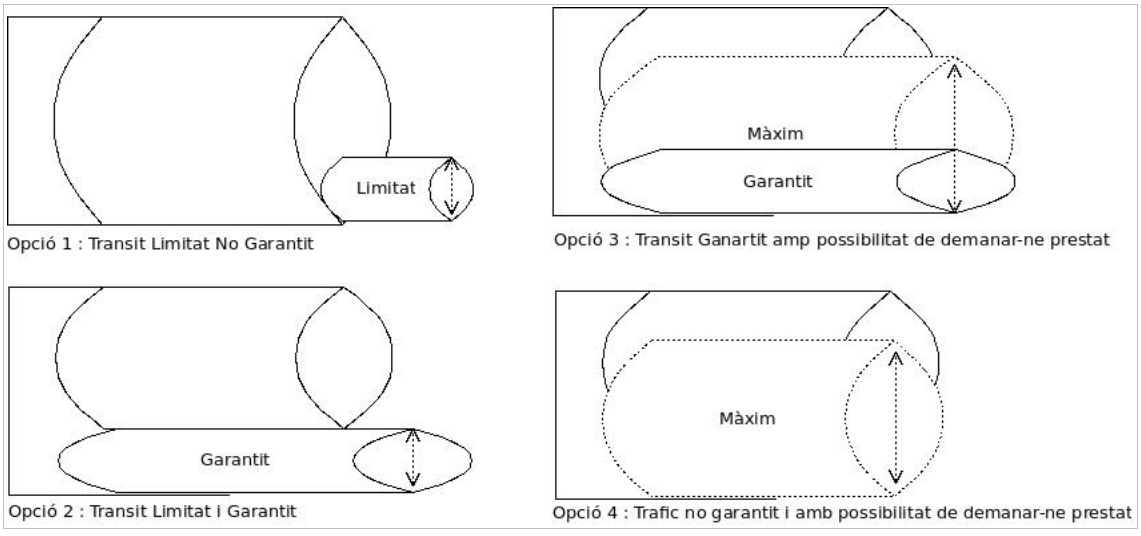
Esquema 2. Ubicacions dels elements



2.3 Classificació de les solucions

En funció de l'enfoc principal de les solucions s'observen tres blocs clarament diferenciats, les basades en l'ús de maquinari dedicat (Cisco, E-sonde...), tractant-se normalment solucions comercials d'abast força global, un segon grup inclouria les que basen la gestió principalment en sistemes de memòria cau implementades en maquinari de propòsit general i que incorporen funcionalitats extres per a la gestió de l'ample de banda (squid amb delay pools...) i per ultim les que centren el tractament a nivell de paquets (iproute2,netfilter).

Esquema 3. Possibilitats de gestió d'ample de banda



Segons les possibilitats de les limitacions i garanties d'ample de banda es presenten quatre possibles opcions que permetran diferenciar les possibilitats dels diversos enfocaments, l'opció 4 és el funcionament per defecte en sistemes sense aplicació de

gestió, les solucions basades el l'us de proxys amb funcionalitats de delay pools permeten limitar l'ample de banda, en funció de si la repartició és coincident amb la capacitat de la connexió es pot assolir l'opció 2 que tot i que garanteix un ample de banda la seva estaticitat no permet aprofitar el sobrant del sistema. Mitjançant la modificació del funcionament de les delay-pools o utilitzant la combinació amb les altres opcions es poden configurar sistemes que suportin les quatre opcions presentades en l'esquema.

2.3.1 Solucions basades en maquinari dedicat:

Dins de la classificació de maquinari dedicat s'observen dos tendències, unes orientades a la seguretat oferint una defensa perimetral mentre que altres estan orientades a la disponibilitat (conegudes com a "web application delivery"), dins d'aquest grup trobem eines amb capacitats de balanceig de connexions i alhora prioritzen o limiten les connexions en base al tipus de trafic. Una altre nomenclatura que engloba a la totalitat o gran part d'elles és el terme UTM (Unified Threat Management) que data del 2004 inventat per Charles Kolodgy, es podria definir com una solució tot en un, evolució dels tallafocs tradicionals als que s'ha afegit altra funcionalitat necessària com per exemple sistemes de detecció o prevenció d'intrusions IDS o IPS, filtratge antispam, protecció antivírica(perimetral) i filtres de contingut web i DLP (Data Loss Prevention) per evitar fugues d'informació confidencial. Cal tenir present que respecte als firewalls tradicionals, el fet de tenir més serveis implica sens dubte ser vulnerable, sigui per possibles problemes de seguretat específics d'alguna de les aplicacions com per atacs de DOS o DDOS (donada la càrrega de gestió que impliquen per exemple la funcionalitat d'antivirus i antispam), incrementant també la complexitat i temps necessari per la serva correcte configuració i manteniment.

El filtrat mitjançant maquinari dedicat permet efectuar totes les funcions en un únic equipament específic[15] (podent administrar-se també de manera remota). Proporcionant filtrat per IP, port, etc... amb més o menys funcionalitats i possibilitats de configuració depenent del model o mòduls opcionals activats. La gestió de l'ample de banda s'aconsegueix mitjançant diverses tècniques, mentre que algunes opcions comercials [11] per la seva estructura permeten regular l'ample de banda aplicant retards o eliminació de paquets o ACKS, altres manipulen diversos paràmetres dels paquets TCP, modifiquen el seu contingut (canvi mida finestra,...) o per tal d'aconseguir la gestió, Altres solucions aposten per generar-ne de nous falsejant l'origen enviant "ICMP source squench" o TCP RST amb l'objectiu d'evitar la connexió o per variar-ne paràmetres que afectin a la velocitat final de la comunicació.

El rendiment d'aquests equips es pot mesurar en base a cps (connexions per segon capa4) o tps (transaccions per segon capas7) entre d'altres, tot i que cal conèixer també les suposicions d'escenari fetes (velocitats, mida paquets, filtres aplicats,...) per a obtenir aquests resultats si en volem obtenir una justa comparació. Una comparativa a mode d'exemple de rendiment de 5 models de possible implantació a centres educatius seria:

Taula 2. Rendiment equips dedicats

Appliance	BW firewall / Polítiques	IPS/IDS	VPN	Antispam	Connexions concurrents	Sessions noves/s
Juniper SRX210	750Mbps/512	80 Mbps	75 Mbps	30 Mbps	32k - 64k	2k
Fortigate 50B	50Mbps		48 Mbps (20conc.)	19 Mbps	25k	2k
Fortigate 80C	350Mbps/2000	100Mbps	80Mbps (200)	50Mbps	100k	5k
Dlink DFL 1660	1,2Gbps/4000	400Mbps	350Mbps (2500)	225Mbps	600k	15k
E-sonde D.Mlink	24 – 60 Mbps	-	-	-	-	-

El procés de filtrat de webs d'aquests equips s'ofereix utilitzant un dels dos aplicatius principals:

- Websense : Utilitzat per exemple per solucions de Juniper, el més potent en aquest punt, amb unes 50.000.000 planes analitzades manualment i classificació agrupada per temàtiques en diversos graus de manera que podem fàcilment realitzar filtrats per conjunts.
- DansGuardian : Utilitzat per solucions com e-sonde, prop del milió de planes carregables des de llistes, menys potent que l'anterior i amb la necessitat de més configuració manual per portar-ne una actualització.

Cal tenir present l'opció de que donat que aquestes eines no son les més adequades en totes les funcionalitats, podem optar per no utilitzar algun dels mòduls de l'appliance (que no destaquin per la efectivitat en la tasca) i adquirir un maquinari especialitzat (com per exemple solucions d'antivirus perimetrals de Trend-micro, Symantec o Panda entre d'altres).

Existeixen també solucions independents combinables en que hi ha empreses que dominen el sector com per exemple en el cas dels Enterprise Firewalls, on Juniper i Check Point són les empreses líders (destacant la solució de PaloAlto Networks per ser tècnicament millor però es tracta d'una empresa encara petita). Solucions SSL VPN, en les que ho són Juniper i Cisco i Firewalls UTM-SMB (solucions SMB per empreses de menys de 1000 usuaris) on Fortinet, SonicWalk i WatchGuard lideren el mercat (curiosament Juniper, malgrat ser líder en el mercat d'aquests equips per grans empreses no s'ha centrat en aquest col·lectiu).

Totes elles disposen d'interfície web per la seva gestió però com a inconvenient destacar el fet que en ser configuracions força guiades (un dels seus clars avantatges) no permet afinar al 100% els paràmetres a baix nivell, amb els que podríem ajustar l'eficiència adaptant-los al cas concret.

Algunes de les solucions estan més enfocades a grans empreses com Juniper, Fortinet, Sonic Walk o Ciber Roam, mentre que altres son solucions orientades a SMB (empreses de menys de 1000 usuaris) com E-sonde o NX-Security Appliance (no podent-se considerar UTMs aquestes últimes per no donar cobertura a totes les funcionalitats).

Malgrat totes elles disposen de la possibilitat d'enviar via syslog per posterior anàlisis, es poden observar diferències en la qualitat de les eines de reporting, destacant de serie e-sonde i Fortigate que mitjançant l'aplicatiu fortianalizer permet combinar informes de múltiples equips. Algunes d'elles permeten mitjançant un agent en el servidor de domini l'autenticació i identificació dels usuaris integrat amb Active Directori/LDAP, mentre que en el cas de Ciber Roam, mitjançant autenticació 802.1x en permet fer el procés transparent sense necessitat de cap agent (en equips clients amb sistemes operatius actuals).

Un altre punt important a conèixer és la base sobre la que corre el sistema, malgrat el sistema operatiu JunOs de Juniper líder en el mercat dels grans centres de commutació (utilitzant BGP, enrutaments dinàmics...), utilitzat per les 100 més importants, el fet de fer només 3 mesos que està en el mercat (en els equips de la serie SRX) i ser una solució prometedora per la seva potència de cara a un futur proper, es presenta com una solució poc madura i amb alguns problemes com per exemple el modul de VPN. Les seves versions SG amb ScrenOs malgrat no ser tant potents presenten una maduresa que fa que estiguin encara tinguts en compte malgrat la seva prevista desaparició del mercat. Dlink utilitza una solució oemitzada de Clavister, cosa que la fa depenent de segons pel que fa a actualitzacions o addició de noves funcionalitats, e-sonde està basada en programari lliure i per tant dependrà de l'evolució d'aquest.

2.3.2 Solucions basades en proxy i l'ús de delay pools

S'han estudiat solucions amb sistemes proxy Squid, es tracta de gateways a nivell de capa aplicació, i per tant ha de conèixer el protocol (http, Ftp...), situació que permet aplicar filtrats a més alt nivell (contingut, grup al que pertany l'usuari, número de connexions simultànies, cadenes de text a la URL destí...).

La funcionalitat de memòria cau donat el gran volum d'accessos en paral·lel a recursos (principalment documentació) en entorns educatius és un factor clau en l'estalvi d'ample de banda. [8]. Mitjançant regles de redireccionament de Netfilter utilitzant Iptables aquest sistema pot actuar transparentment. La funcionalitat de les Delay pools programades per David Luyer [9], mereixen una especial atenció per la seva implicació en la gestió de l'ample de banda utilitzant l'algorisme Token Bucket, permeten definir tres nivells d'inclusió a les pools:

- Aggregate : A nivell de pool
- Network : A nivell de xarxa C
- Individual : A nivell de ip individual

Cadascuna de les pools es defineix mitjançant 2 paràmetres:

- max : mida màxima del pool
- restore : velocitat d'emplenament del pool

“Restore” es pot considerar de manera simplificada com la limitació d'ample de banda en connexions continues mentre que “max” seria la mida màxima del burst que acceleraria les connexions interactives com càrregues puntuals de planes web, donant una sensació de més agilitat. El seu principal inconvenient provocat per ser un mètode bastant estàtic, fer qualsevol canvi en al configuració implica modificar l'arxiu de configuració i reiniciar el servei squid.

L'utilització de les Delay Pools d'Squid per a gestionar l'ample de banda s'ha provar amb cert èxit a centres com la Universitatde Rhodes, malgrat tot s'ha provat que només és eficient si en l'avaluació es tenen en compte llargs períodes mentre que en moments puntuals la seva estaticitat no en permet una adaptació dinàmica i per tant es torna ineficient [15].

La seva aplicació en els proxys parteix del fet que tot el transit ja passa a traves d'ells i per tant n'és la ubicació natural (el fet de que totes les peticions passin a través de l'equip gestor [7] permet aconseguir no només un b per IP protocols o ports, permet també controlar l'ample de banda permès).

Hi ha diverses propostes de millora del funcionament per tal d'aconseguir un major grau de dinamicitat per cobrir els moments puntuals de pic, calent però assegurar que això no provoqui un increment de consum de recursos de memòria i procés al proxy que en malmeti el rendiment.

Permet l'addicció de funcionalitats específiques, a destacar la que proporciona Squidguard que permet fer un filtre més acurat en funció de contingut [1], podent aplicar pesos específics a cadenes de text com fan algunes solucions comercials [20] que acabaran definint la prohibició o no de l'accés al recurs. Algunes propostes a part de la memòria cau de contingut implementen fins i tot memòria cau de DNS [22]

L'opció d'us exclusiu de Squid i Delay pools per a la gestió de l'ample de banda té l'inconvenient de ser estàtica, tenir un baix rendiment i poc adaptable [9], d'aquí la proposta de la millora d'aquestes. En modificacions del codi, testades a la universitat de Moratuwa s'ha observat en tests preliminars [9] per la modificació del funcionament de les DelayPools problemes com en el cas de l'intent d'assignació proporcional en funció dels usuaris actius, a part d'haver de tenir la informació de l'estat no es pot suposar que tots els consums dels usuaris seran iguals. En l'assignació proporcional al consum demanat el problema és que la divisió és favorable al qui més consumeix. A grans trets la solució proposada és similar a la divisió de l'ample de banda en funció als usuaris actius però amb la possibilitat de prestar ample de banda restant entre usuaris, com a paràmetres importants està el valor de mínim garantit de pool que es garantirà en moments de màxim ús, mentre que quan el consum decreix s'augmenta l'ample de banda màxim de tots ells sempre que hi hagi tokens disponibles a l'anomenada Aggregate Pool.

També s'han fet modificacions al codi per tal de permetre poder compartir excedents d'ample de banda entre Pools. El funcionament de la modificació es considera positiu, s'ha provat molt efectiu en càrregues altes mentre que té com a petits inconvenients el fet que en càrregues molt baixes es nota l'overhead de l'algorisme, i les seves limitacions, a destacar el fet de que no evita la congestió del link en descàrregues grans i

no dona suport a QoS per a transit en temps real [9]. En els casos en que la classificació estigui associada a unes credencials caldrà assegurar que aquestes no siguin fàcilment sostretes o que s'en pugui fer una fàcil detecció [1].

En funció de les opcions afegides, degut a l'increment de càrrega del sistema caldrà seguir el consum de recursos de processador i memòria tot que en la implementació base de la solució en real s'ha observat que són baixos, oscil·lant entre 8 i 10% en un PIII 500 amb 512Mb de Ram Utilitzant RedHat 7.1.

2.3.3 Solucions basades en combinació de Nat, Netfilter e Iproute2

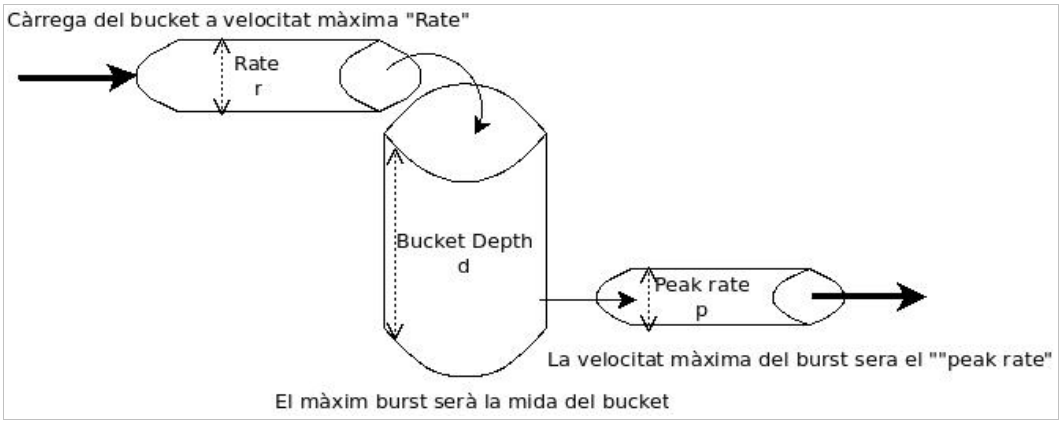
Aquest enfoc inclou les solucions basades en la combinació d'aquestes eines, mitjançant filtrats a nivell de capa 4, molt proper a solucions firewalls però complementat també amb funcionalitats de gestió de l'ample de banda i balanceig entre múltiples connexions entre d'altres. Per exemple la combinació de marcatge de paquets i polítiques d'enrutat Iptables + Iproute2 per tal d'obtenir una compartició de links d'accés amb resistència a caigudes d'algun dels links.[12]

Mitjançant l'us de Netfilter, funcionalitat interna de nuclis Linux a partir de 2.4 que proveeix suport de Statefull firewall (firewall amb coneixement d'estat, internament manté una taula amb les connexions [8] establertes al sistema) de manera que en saber l'estat de cada connexió (establerta, relacionada o nova), pot aplicar-li accions de redirecció, acceptació o denegació amb granularitat de connexió. Per tal de configurar-ne les cadenes i regles l'eina Iptables [8] en permet la seva configuració de manera estructurada, cal destacar d'importància de l'ordre en les configuracions donada la comprovació lineal a nivell intern de les regles. Tot i ser regles complexes que impliquen un coneixement del funcionament a baix nivell del sistema i de la pròpia aplicació, mitjançant l'ajut d'algunes aplicacions com Shorewall s'ofereix destinat a perfils no tant tècnics o solucions més estàndards una simplificació de les tasques de configuració de solucions gateway/firewall basades en Iptables [8].

Una de les mesures per tal de determinar l'ample de banda assolible i velocitat en un cert moment anomenat bucket/pool [2] , és un concepte utilitat en diversos mètodes gestors d'ample de banda imprescindible de tenir clar per entendre el funcionament de les diverses metodologies, es composa de tres paràmetres:

- Token bucket rate “r”: (bps) velocitat en que s'omple el bucket
- Bucket depth “b”: (b bytes) mida del bucket
- Peak rate “p”:(bit/s) velocitat màquina en que poden ser enviats paquets en períodes curts.

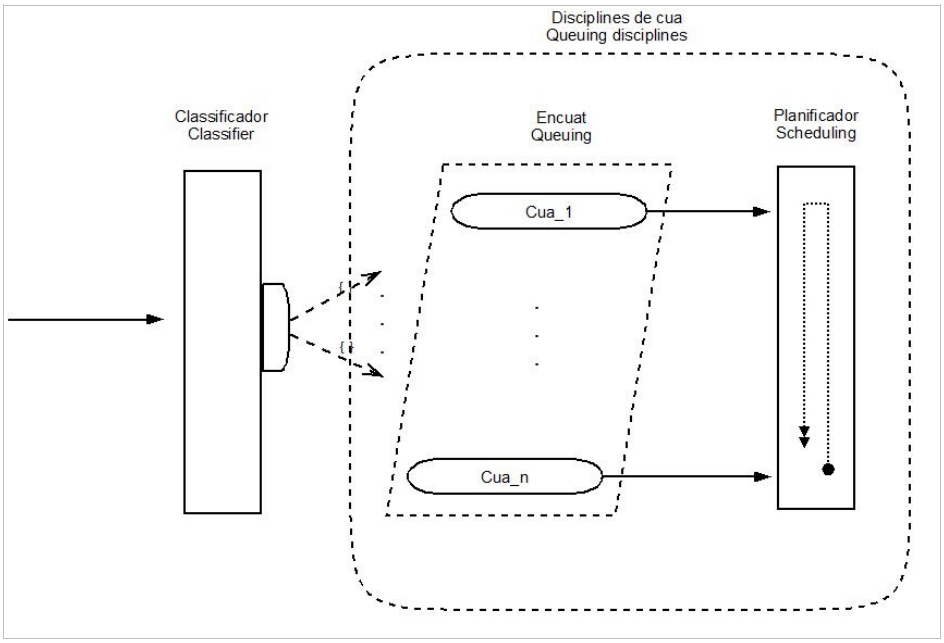
Esquema 4. Token bucket



El Control de trafic, funcionalitat del kernel implementada en Linux per Alexey Kuznetsov, inclou el conjunt de decisions i mecanismes que s'efectuen mentre el paquet està encuat i abans de ser transmès [4], consta de disciplines de cua, classes de servei, filtres i policing components.

- Disciplines de cua (qdisc): mecanismes de programari associats a la interfície, algorismes que defineixen el tracte donat a cada paquet. FIFO (en ordre), RED (Random early detection fifo), HTB(que utilitza l'algorisme TBF “tocken bucket filter”)...
- Classe de servei (class) : Té unes regles associades com l'ample de banda o burst i utilitza les disciplines de cua per complir-ho.[4]
- Filtre o classificador (filter/classifier): Definició de regles que permetran decidir a quina classe s'envia cada paquet. Cal tenir present que cada filtre té assignada una prioritat (ordenats de més a menys prioriat per si un paquet correspon amb més d'un filtre s'assigna el primer que es compleix). Poden ser basats en taules d'enrutat, classificadors u32, classificadors ToS o iptables [7].
- Organitzador/Planificador (scheduler/ Policing components) : Encarregats d'aplicar les restriccions que pertoquin, que no s'excedeixin l'ample de banda estipulat (en funció del filtre i de les disciplines de cua) [3].

Esquema 5. Disciplines de cua

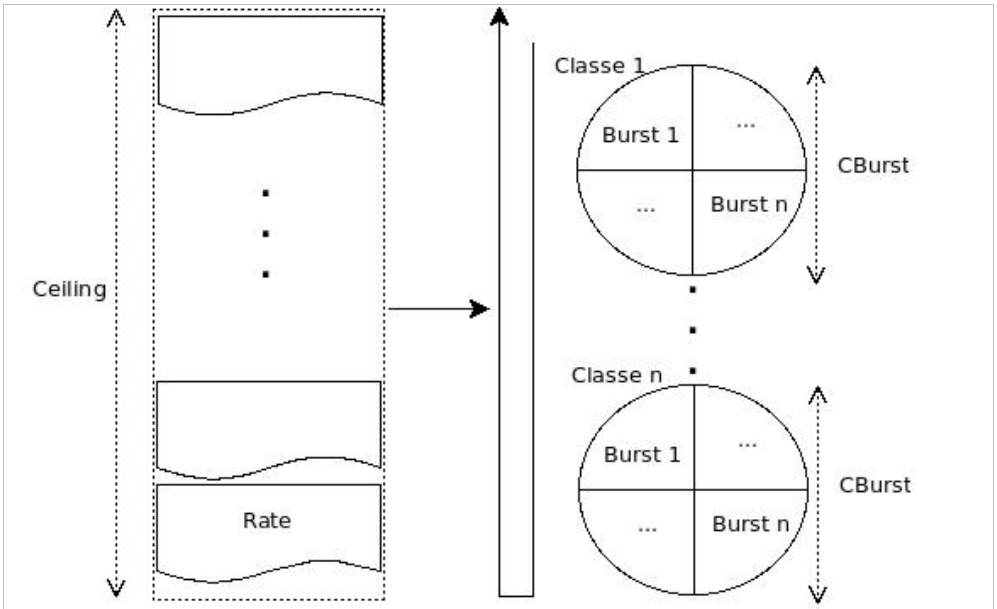


La qualitat de servei en sistemes GNU/Linux s'implementa mitjançant el comandament TC (també utilitzat internament per la configuració dels diversos components implicats en el control de trafic [3] [4]) contingut dins el paquet iproute2, programari de espai d'usuari que permet definir els elements anteriorment exposats, cues, classes i filtres, associant-les amb una interfície i configurant-ne els paràmetres desitjats. Alguns dels paràmetres a nivell conceptual més importants (no necessaris en totes les disciplines) a tenir en compte són:

- Rate: Màxim ample de banda consumible per la classe sense demanar prestat a altres.
- Ceiling: Màxim ample de banda consumible per la classe inclòs el que pot demanar prestat a altres
- Burst: Quantitat de dades que es poden transmetre a la màxima velocitat "ceiling" abans de servir al següent stream dins la mateixa classe.
- Cburst: Quantitat de dades que es poden transmetre a la velocitat "wire" abans de servir a la següent classe.

Tant cbust i burst donen els millors resultats en valors 18k per un ample de banda de 30Mbit/s segons els tests[4]. Si tenim en compte la relació lineal entre burst/cburst i l'ample de banda desitjat podem utilitzar la fórmula[4] cburst=burst (Kbytes= 18/ (30M/rate assignat)). Cal considerar que en el cas de tenir més d'un stream dins la mateixa classe, el que més transmeti serà el que més ample de banda obtindrà.

Esquema 6. Relació paràmetres configuració classes



Burst i Cburst determinaran per prioritats idèntiques i juntament amb el nombre d'usuaris el temps de retorn de l'acces al medi.

Dins la mateixa classificació s'han considerat altres solucions que incorporen el suport de scripts, interfícies i fins i tot de llenguatges per facilitar-ne la configuració, Snitch, HTB.init, basat en la configuració de solucions mitjançant l'us de disciplines de cua HTB, TCSS: "Trafic control super script", un script[7] que part de facilitar la creació d'escenaris que aplicaran TC, té certes peculiaritats en la seva configuració pel que fa als valors dels seus paràmetres, a tenir en compte el sentit del filtrat que també pot ser bidireccional i l'ús de Iptables en cas de tenir clients amb NAT que no disposaran d'IP pública per poder definir en el filtrat. aquesta solució per la seva naturalesa no permetrà filtrar a nivell de capa 7 CBQ.init, [7] aquest basat en disciplines CBQ i que amb l'opció "compile" permet generar les comandes TC de manera que pot ser utilitzat també com a manual d'us del propi comandament TC.

El llenguatge Tcng permet ser mes amigable i d'estructura més entenedora (semblant al llenguatge C) respecte a l'ús de comandaments TC[3]. Fins i tot disposa de una mena de macros que efectuen els comandaments més usuals. Un dels inconvenients de l'us de tcng, [3] és el fet de que per cada petit canvi impliqui l'aplicació de nou de totes les regles fa que el procés sigui més lent i per tant l'adaptació dinàmica a canvis poc pràctica.

A nivell tècnic la majoria de les solucions, amb més o menys funcionalitats i especificitat en generar finalment comandaments TC (de manera implícita o explicita), com s'ha comentat algunes d'elles Snitch, HTB.init, CBQ.init [7] o Tcng [3]. Altres com ZeroShell [21] presenten una solució global de fàcil configuració, fins i tot amb interfície web que en permet una gestió senzilla.

A l'igual que internament en solucions del tipus appliance, per la classificació marcant els paquets en funció de IP/Port Origen/Destí per a posterior filtre de tractament. Caldrà

fer 2 gestions, com marcar i que fer amb cada marca. Per tal de descongestionar la màquina algunes solucions proposen distribuir les tasques entre diferents equips [11]. Sobre trafic excedent, depenent de les necessitats o estat de la xarxa hi ha la possibilitat de fer DROP o aplicar retards.

Com s'ha comentat, existeixen opcions de gestió centralitzada, distribuïda, hibrida, en el cas de les no intrusives [11] que permeten (sempre situant els equips gestors en un segment amb la comunicació a gestionar accessible) mitjançant masquerade i enviament de TCP RST o ICMP-squech modificar el funcionament de les connexions permetent blocar-ne l'establiment o limitant-ne l'ample de banda. Limitacions d'aquestes serien el fet de que el protocol TCP en que es centren estigui ben implementat en els equips a gestionar i que no existeixi blocat per exemple de paquets de tipus ICMP.

Els canvis de configuració segons l'opció són gestionats manualment per un administrador, basats en franges horàries, o en base al percentatge d'utilització del link, tècniques de intel·ligència artificial, etc...

Les aplicacions que corren sobre equips de propòsit general com ALTQ[15] permeten obtenir un control a més baix nivell de l'equip i ofereixen una gran llibertat de configuració, amb l'inconvenient en molts casos de l'augment de complexitat en la instal·lació, configuració i manteniment.

L'opció proposada per a disposar de sortides redundants (permetent una major capacitat global)[12], és utilitzar Iptables i Iproute2, generant 2 cadenes on es redirigirà el transit degudament pre-marcat en funció de la sortida a assignar (internament tot el que surti per una interfície rebrà resposta per aquesta). Les passes són bàsicament 3, generar les cadenes de marcatge, configurar els filtres per que redirigeixi en funció de la marca cap a una o altre taula, en funció de la taula aplicar una o altre ruta (es recomana per poder garantir a part d'augment d'ample de banda una redundància més fiable en cas de caiguda, siguin de diferents proveïdors i tecnologies).

La recomanació en aquests casos és treballar les funcions de firewalling i gestió d'ample de banda configurat en mode bridging [7] per tal de poder en cas de necessitat (per problemes de configuració ...) permetre de manera fàcil el pas de les comunicacions sense filtrar i mantenir el sistema operatiu.

Un inconvenient en el cas de TC [3], és que una petita errada de configuració pot ser difícil de trobar donada la complexitat del llenguatge. Per altra banda el rendiment pot variar bastant en funció de la definició de les normes, tant l'organització dels filtres com de les cues. Per altra banda, l'ambigüitat en les unitats pot induir també a error (kbit pot referir-se tant a 1024 bits com a 1024 bits/s en funció del paràmetre configurat).

La solució de filtratge aplicant L7 pot en ocasions ser un inconvenient pel fet que es considera un 1% de possibilitats de fals positiu[23], es considera el DROP massa agressiu, combinat amb filtrat de ports o adreces IP atenuaria el problema però afegiria menys versatilitat a la solució.

Una limitació que a llarg termini podria arribar a ser un problema i que caldrà testar en els sistemes finals serà la capacitat o el valor màxim d'ample de banda assolible/gestionable (més fàcil d'observar en solucions de maquinari específic en la

definició de les seves prestacions com es pot veure en la taula de l'apartat anterior) per la solució basada en HTB, en l'estudi [4] es demostra que aquest és de 34Mbit/s per paquets de 64 bytes en mode forward de streams continus, s'observa una relació entre els valors de cburst/burst i la precisió i velocitat desitjada.

Certes suposicions d'algunes solucions basades en el funcionament de la pila TCP, en variar la implementació d'aquesta en diferents sistemes operatius o equips[11] no podem ser assegurades per tots els casos i confiar en elles per a fer per exemple una denegació de connexions enviant TCP RST, l'única manera d'assegurar-ho és fer-ho només contra màquines amb comportament garantit com proxys interns, i això implica la necessitat d'assegurar que tot el transit passa per ells. Alguns problemes de no tenir-ho en compte podrien ocasionar d'efecte invers al desitjat com la generació d'un gran volum de transit i el no aconseguir tallar l'establiment de la comunicació o per exemple opcions com enviar un "ICMP reject" provocant el tall de la resta de connexions actives.

Altres inconvenients d'aquests mètodes és la possibilitat de que hi hagi filtres que no deixin passar ICMP o detectin el falsejat de IP i en facin un drop.

Malgrat la simplicitat de configuració d'algunes solucions de programari que disposen de interfícies web, el fet de tractar-se de solucions generalitzables fa que hi hagi un excés d'elements de configuració que no serien necessaris, complicant-ne la configuració i en conseqüència afegint potencials problemes de seguretat.

Taula 3. Resum classificació referències

Referència / Mètode	Control Dinamic / Gestió Distribuïda	Squid - Delay Pools	TC	Programari extra	Modificacions codi	Aplicat educació	Solució / Avaluació
Squid + Quorum[1]	N/S	S	N	S	N	S	S
CBQ [2]	S/S	N	S	S	N	N	S
TCNG [3]	N/N	N	S	S	N	N	S/A
HTB [4]	N/N	N	S	S	N	N	A
IP [5]	N/N	N	S	N	N	N	A
TC + TCNG [6]	N/N	N	S	N	N	N	S/A
TCSS CBQ [7]	N/N	N	S	S ++	N	N	S/A
Squid + Squid Guard [8]	N/N	S	N	S --	N	N	A
Squid +	S/N	S/S	N	N	S	S	S

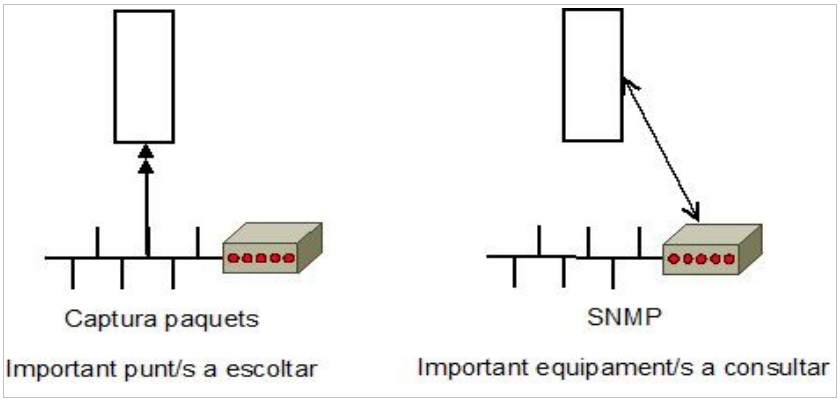
dinamic Pools [9]							
IP + TC [10]	N/N	N	S	N	N	S	S/A
RMON [11]	S/S	N	N	S	N	S	S
CBQ + SFQ [12]	S/N	N	S	S ++	N	N	S
Simulador Diffserv[13]	S/S	N	?	S	N	N	A
Analitzar, Netperf [14]	N/N	N	-	S	N	N	A
Proxy + Hash ACL [15]	S/S	S/S	S	S	S xx	S	S
Eines i mètriques [16]	N/N	N	N	S	N	N	A
SNMP [17]	S/S	N	N	N	N	N	S/A
HTB + Diffserv [18] *	S/N	S/S	S	S	N	S	S/A
Cisco [19]	N/S	N	N	N	N	S	S
E-Sonde [20]	N/N	N	N	N	N	S	S
ZeroShell [21]	N/N	S/S	S	S	S	N	S
Accelerate Intternet [22] *	N/N	S/S	S	S	N	S	A
Firewalls [23]	N/N	N	S	N	N	N	A
Squid [24]	N/N	S/S	N	N	N	N	A
Firewall QoS L7 [25]	N/N	N	N	S	N	N	A
Generalitat 1x1 [26-29]	N-S/N	N	S	S	S	S	S
Iproute2[30]	-/-	N	S	N	N	N	-

++ = Scripts
-- = Dans Guardian
x = No basat en squid tot i que el pot incorporar-lo internament
xx = ACLs

2.4. Mètodes de mesurament

Principalment es proposen 2 variants que poden complementar-se alhora d'obtenir informació sobre l'estat de la xarxa. Captura de paquets TCP Packet capture [9] [11] i consultes periòdiques i recepció de traps SNMP (implementat en algunes solucions mitjançant MIT SNMP development kit [9]). En totes dues variants caldrà conèixer la topologia de la xarxa i l'objectiu a avaluar per tal de decidir el punt ideal on aplicar el mètode, així com definir-ne la periodicitat.

Esquema 7. Punt de mesura



L'estimació [14] de l'ample de banda engloba tant el conjunt de tècniques com les eines i mètriques utilitzades.

Per tal d'estimar l'ample de banda es controlen diversos paràmetres que afecten a la transmissió de dades i funcionament general, a part de poder servir per a mesurar l'estat de la xarxa permeten fer la comparativa de les pròpies eines en funció dels resultats obtinguts mesurant entorns i situacions idèntiques com la Capacitat global, l'ample de banda disponible i el bulk transfer capacity. Cal tenir present que segons quin mètode utilitzem i en funció del punt/s de gestió/monitorització serà només aplicable a certes condicions (per exemple no podrem saber la capacitat si hi ha alguna transmissió en curs).

Independentment del mètode utilitzat, les etapes en que es divideix el procés són dues [14]:

- Mesurament : Amb o sense suport de generació de paquets automatitzada en base a un patró definit i mesurament de la recepció.
- Estimació : Procés estadístic-heurístic dels resultats depenent del model de xarxa (algunes de les eines utilitzen l'estimació en temps real per poder canviar el patró de generació i d'aquesta manera guanyar en precisió).

Per poder efectuar una comparació de diverses eines cal tenir disponibles els valors de paràmetres com la precisió (afectació de diversos nivells de càrrega en la precisió dels resultats), eficiència, velocitat (límits màxims i mínims de treball) , estabilitat i d'altres com per exemple la necessitat de tenir privilegis de superusuari, eficiència en el tractament de l'asimetria o la versatilitat de paràmetres a incorporar. També caldrà tenir presents les limitacions com:

- L'execució de les eines es fa en sistemes que no son en temps real i per tant dependents de factors externs
- Rellotges de baixa resolució limiten la precisió en càlculs.
- La velocitat I/O dels sistemes base afectaran també al funcionament de l'eina.

Un altre punt a tenir en compte alhora de poder efectuar comparatives és el format de log, es recomana Net Logger ULM Log. I és important tenir en compte també com es defineix el temps.

En entorns sectoritzats o amb més d'un punt critic serà interessant optar per un monitorització distribuït per conèixer l'estat de la xarxa a cada sector [2] mitjançant mesuraments de l'estat de la xarxa actius (via SNMP o escoltes de xarxa), passius (mitjançant un estudi dels logs) o una combinació d'ambdós. Dels problemes de treballar amb una gestió distribuïda, a part de tenir més punts de fallada i un cost més elevat, serà també important l'augment del transit per els missatges de control, aquest excés es resolt de diferent maneres, utilitzant UDP en comptes de TCP, enviant en blocs a l'estil de format de fitxer [1] o usant un protocol eficient específic com COPS [2].

Malgrat en la definició de la solució proposada per a centres educatius es parla molt de sectors, aquests seran lògics, i cal tenir també present que aquests entorns tindran principalment un únic punt crític que serà l'accés a Internet i per tant no serà necessària la monitorització distribuïda.

Per tal de fer avaluacions disposem de solucions que emulen l'escenari de xarxa complet com Nist o Dummynet entre d'altres, així com generadors/analitzadors de trafic, podent tractar-se de programari per córrer sobre maquinari d'ús comú o ser una solució basada en dispositius específics com IXIA[4] , cal conèixer les prestacions limitacions de l'eina utilitzada per tal de poder decidir si és valida per ser aplicada en l'entorn a estudiar (per exemple, IXIA no permet transmetre en paral·lel per varies interfícies, en fa un round-robin per simular-ho).

Malgrat la majoria de simuladors no proveeixen d'un entorn global simulat, i la majoria són centralitzats, alguns són distribuïts [13], fins i tot alguns permeten a part de definir una topologia física virtual, el fet de simular caigudes i restauracions de nodes.

Cal tenir present els possibles blocats de certs tipus de paquets que poden influït per exemple en la recepció de paquets SNMP o ICMP [11].

Com a paràmetres a monitoritzar per conèixer l'estat de la xarxa, depenent de l'objectiu es pot considerar el més optim[11], ocupació del link, ample de banda consumit per certs serveis, ample de banda consumit per certs grups de Ips etc... Per tal de poder dissenyar aquesta classificació caldrà conèixer les peculiaritats de la xarxa per saber quins serveis seran crítics, els seus valors òptims, així com la divisió física/lògica d'agrupació d'equips/usuaris que es decideixi. L'algorisme treballa mitjançant les estadístiques

recollides i en cas de ser font de dades de gestió les polítiques de control definides en cas de que no es compleixin les condicions poden per exemple blocar la connexió fins que les condicions la fan viable.

Algunes solucions [13] proposen l'us d'algorismes d'anàlisi de l'estat de la xarxa mitjançant escoltes o l'us de protocols com l'SNMP (calculant el CBP "call blocking probability"), proveint proactivitat, permetent una reacció davant la previsió d'arribar a un estat de congestió , evitant arribar a l'estat de saturació, reconfigurant els filtres en funció per exemple de la càrrega de l'enllaç, horaris...

Cal tenir present que les ADSL (principals tecnologies utilitzades per accessos a Internet als centres educatius a Catalunya) poden variar el seu rendiment amb el temps, i que no es pot garantir un servei constant, podent haver-hi en zones problemes de sobrecontractació que implicarà un baix rendiment de les línies [12]. És per això que caldrà fer-ne un previ test i mantenir-ne un seguiment.

Com a opció utilitzada per algunes eines de d'estimació d'ample de banda destaca la proposta de retroalimentació del generador [14] mitjançant un component que executi un anàlisi estadístic/heurístic del transit per tal de poder incrementar la precisió en la generació de trafic amb paràmetres estipulats.

3. Definicions i conceptes implicats en la gestió de ample de banda

3.1 Terminologia

Dins la terminologia utilitzada, els següents conceptes s'han considerat clau per tal d'ajudar en la comprensió de les avaluacions i comparacions efectuades, alhora d'evitar possibles males interpretacions.

- HTB : Disciplina de cua "Hierarchical token buckets" de tipus classful, basada en l'algorisme TBF, utilitzat també en solucions Cisco. En tests efectuats amb generadors de trafic Ixia s'ha comprovat una precisió de 2Mbps [4]. També ha estat utilitzada en els primers tests del treball amb el firmware DD-Wrt i finalment proposada com troncal en la solució definitiva. És una versió amb similars característiques que CBQ però sense necessitat d'especificar molts dels paràmetres d'aquesta.
- NAT: [8] Traducció d'adreces internes no adreçables des d'Internet, anomenat emmascarament, mitjançant l'us d'una taula que en manté l'estat de relacions.
- Balanceig de carrega: pot ser assignant en ordre paritari o assignant pesos a cada connexió. Pot ser per interfície física o utilitzant una única interfície. Pot ser assolit de diferents maneres, per exemple utilitzant en comandament ip route amb l'atribut weight [4]. No s'ha de confondre amb gestió de l'ample de banda.
- Burst: Bloc de paquets enviats en cada stream (de cop).
- Ingres/Egress: En funció del sentit del trafic i punt on es faci el control obtindrem més o menys possibilitats de funcionalitat[3]. Ingres permetrà classificació prèvia (marcatge) o DROP mentre que Egress permet la gestió de trafic i encuament.

- Capacitat[16]: velocitat de transferència de dades a nivell IP màxima (burst màxim, no constant), la velocitat contractada de les línies ADSL seria la capacitat. Depèn de la tecnologia utilitzada. Quan es parla de l'accés global del sistema estarem parlant de capacitat.
- Ample de banda[16] : Per a la gestió de la capacitat no utilitzada en un període de temps, parlarem d'ample de banda disponible.
- TCP Throughput i Bulk Capacity[16] : s'utilitzen per referir-se al rendiment a nivell TCP,
- Delay: Latència. Temps que triga en transmetre's un bit d'origen a destí. (concretament s'inclourà delay per el procés decisions de d'encuat i en l'encuat mentre esta en la cua)
- PDV: Paquet delay variation: diferencia de delays entre paquets correlatius, s'evita en aplicacions multimèdia (vídeos flv...) omplint un buffer previ.
- Jitter: Variabilitat en les latències (delays).
- Tcp-window: El propi funcionament intern de tcp fa que es trigui en assolir la velocitat desitjada, és per tant que en cas de completa llibertat (dins de cada zona tractada/aula) els fluxos amb més prolongats en el temps en reben és i es veu la corba “d'acceleració”.
- ACL (Squid): Agrupacions utilitzades per permetre o efectuar denegacions en bloc.
- Proxy transparent: Configuració del proxy i iptables per tal de dirigir el trafic web cap al proxy.
- Hit/Miss (Squid): Encert o fallida alhora de consultar a la caché per l'existència d'un element.

3.2. Consideracions i programari utilitzat

Per facilitar el seguiment dels resultats dels tests, s'ha decidit unificar mesures, la decisió d'utilitzar com a mesura per definir l'ample de banda consumit en un cert moment ha estat kbps (kbits/s) s'ha optat per bps en comptes de Bps per ser aquesta la més utilitzada per els ISPs.

La majoria de centres educatius disposen d'un únic punt d'accés a Internet amb o sense balanceig, és aquest doncs el coll d'ampolla on es perden i retarden els paquets [15] , fet que s'ha tingut en compte alhora de decidir-lo com a punt d'aplicació de la gestió.

El programari utilitzat per la realització dels tests ha estat principalment:

- Generació/recepció de trafic: Iperf, Jperf, ping, wget, ethtloop, firefox
- Formatació de resultats: gawk, sed
- Estudi del trafic: ntop, wireshark, logs d'squid, squidclient, iperf i jperf, iftop, watch...
- Automatització dels tests: cron

- Accés remot : openssh
- Generació de gràfiques anàlisi resultats: calc, gnuplot,rrdtool
- Mode actiu: iperf/jperf/ping/wget
- Mode pasiu: wireshark, ntop, tc show, squidclient

Els resultats han estat presentats en forma de gràfiques per estimar aquesta coma millor opció per a la seva comprensió donat l'elevat volum de dades tractat.

L'eina Iperf ha estat utilitzada per a testar l'equipament de comunicacions intern però degut a l'asimetria de les connexions ADSL no és útil per a fer tests de capacitat de les connexions a Internet.

Els valors mesurats principalment en la proposta són de rate retornats per Iperf, la velocitat mitjana de descàrrega retornada per wget, els valors de velocitat retornats per l'eina de test i els valors de rate (de 10segons) retornat per la comanda d'estat de classes de tc. Altres valors de suport emmagatzemats malgrat han estat inclosos en els resultats han estat la memòria consumida per el sistema, nombre i mida dels fitxers tractats en una descàrrega, numero de paquets prestats o demanats per la classe.

Els objectius dels valors de limit utilitzats és maximitzar l'aprofitament dels recursos de xarxa, evitant la penalització d'ample de banda dels Hits i l'us de buffers de dispositius de xarxa.

Els formats de les dades es fan intencionadament compatibles amb l'eina rrd-tool per tal de poder integrar-la en un futur amb el sistema obtenint un monitoratge fàcil en temps real. L'aplicació de millores com el balanceig de sortida entre més connexions a Internet és perfectament compatible amb el sistema de gestió essent únicament necessaris canvis en els paràmetres.

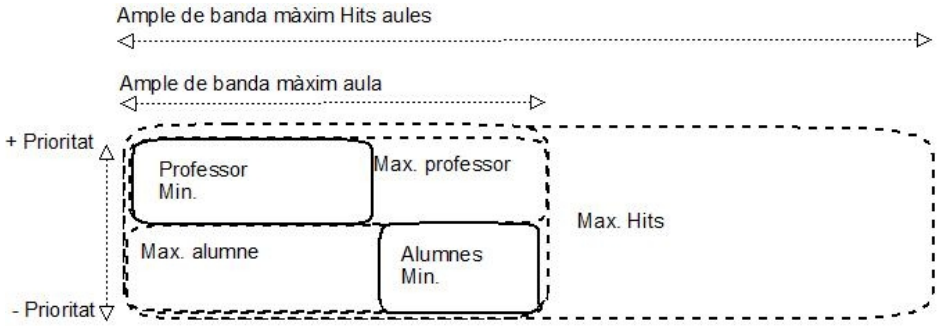
Es proposa aplicar també una priorització de paquets ACK a la interfície de sortida per tal de que pujades sostingudes no afectin a les descàrregues.

En la implementació en real en els qdiscs finals s'ha implementat la disciplina de cua SFQ per garantir un repartiment de trafic just entre els fluxos (cal tenir clar però que és entre fluxos i no per usuaris).

4. Descripció de la solució i prova de concepte de implementació

La solució proposada basada en sectorització en base a les aules físiques seguirà el següent esquema lògic. Com a mesura comuna el ample de banda màxim de les aules serà la capacitat de la suma d'accessos a Internet del centre mentre que l'ample de banda màxim de Hits dependrà de la capacitat màxima de l'equipament de xarxa intern del centre. Ambdues situacions amb l'objectiu d'evitar l'us de buffers en els dispositius que a part de possibles saturacions implicarien la pèrdua del control de la gestió.

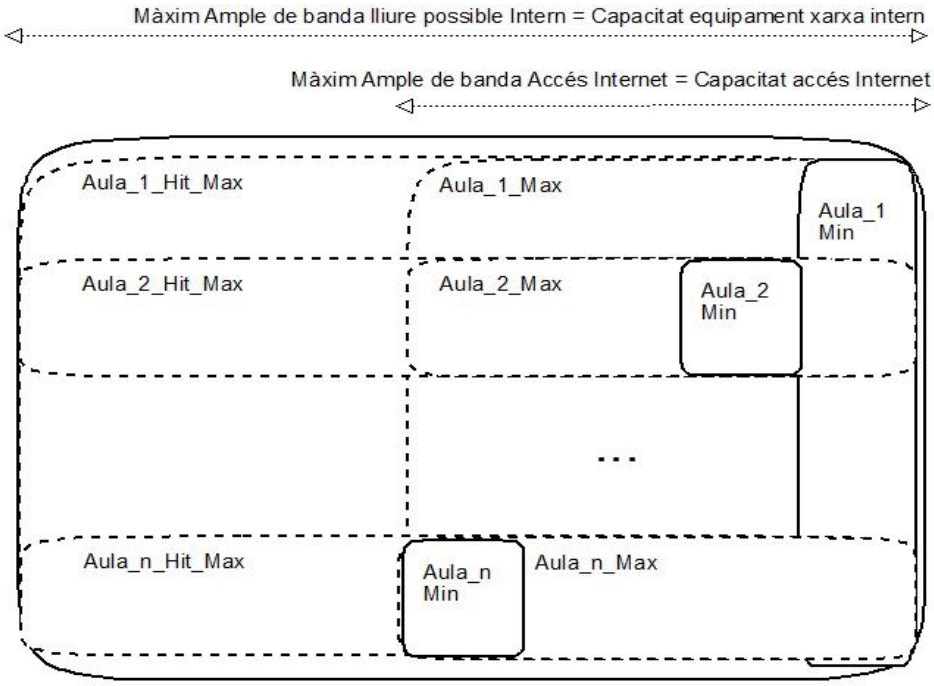
Esquema 8. Assignacions aula



Com es pot veure en l'esquema 8, l'ample de banda mínim garantit del professor és superior al de l'alumnat i alhora té més prioritat en cas d'utilitzar-ne l'excedent.

En el següent esquema es mostra el comportament desitjat en el repartiment d'ample de banda entre aules.

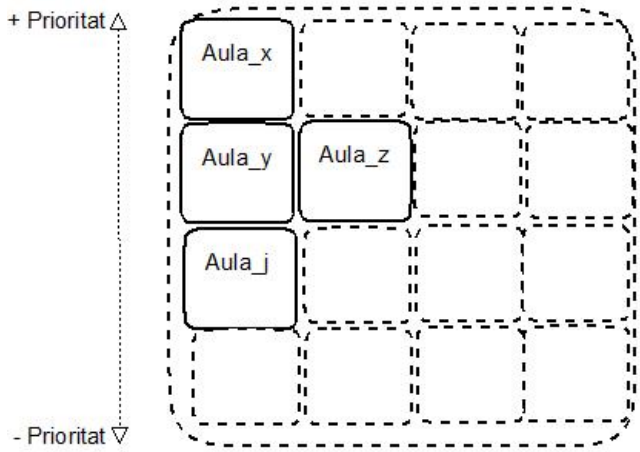
Esquema 9. Assignacions entre aules



Cada aula disposarà d'un mínim garantit, la suma dels mínims coincidirà amb la suma de capacitats dels accessos a Internet del centre. En cas de no ser consumit l'ample de banda restant podrà ser utilitzat per la resta d'aules en que la demanda d'ample de banda superi els seus mínims.

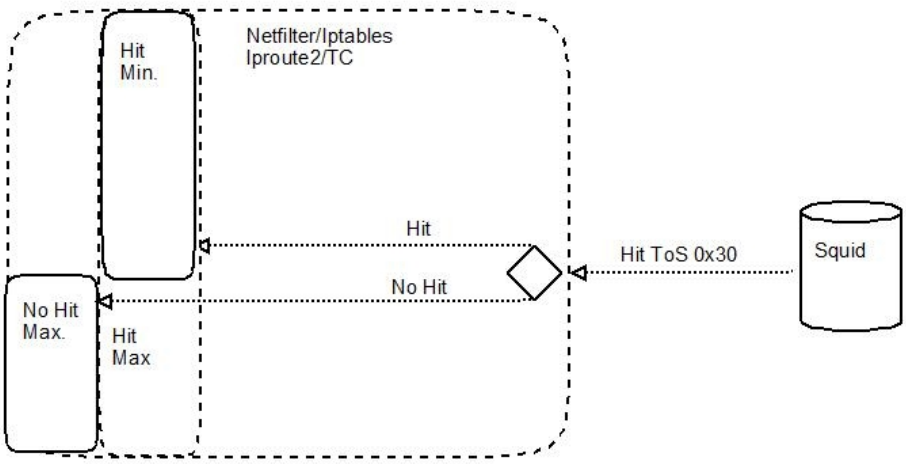
En l'accés a l'ample de banda excedent les aules s'ordenaran en base a les prioritats especificades i que podran ser canviades en qualsevol moment per adaptar-se a situacions. El sistema permet configurar assignant prioritats a les aules des d'una manera totalment equitativa fins a configuracions en que cada aula tingui una prioritat diferent com mostra l'esquema 10.

Esquema 10. prioritització aules



Per tal d'aprofitar al màxim l'us del proxy amb memòria cau, les consultes servides per aquest directament de memòria s'hauran de tractar de manera diferent evitant que siguin restringides a la capacitat dels accessos a Internet (que no utilitzen) i puguin assolir la resta d'ample de banda disponible assolible per els dispositius.

Esquema 11. Diferenciació Hits

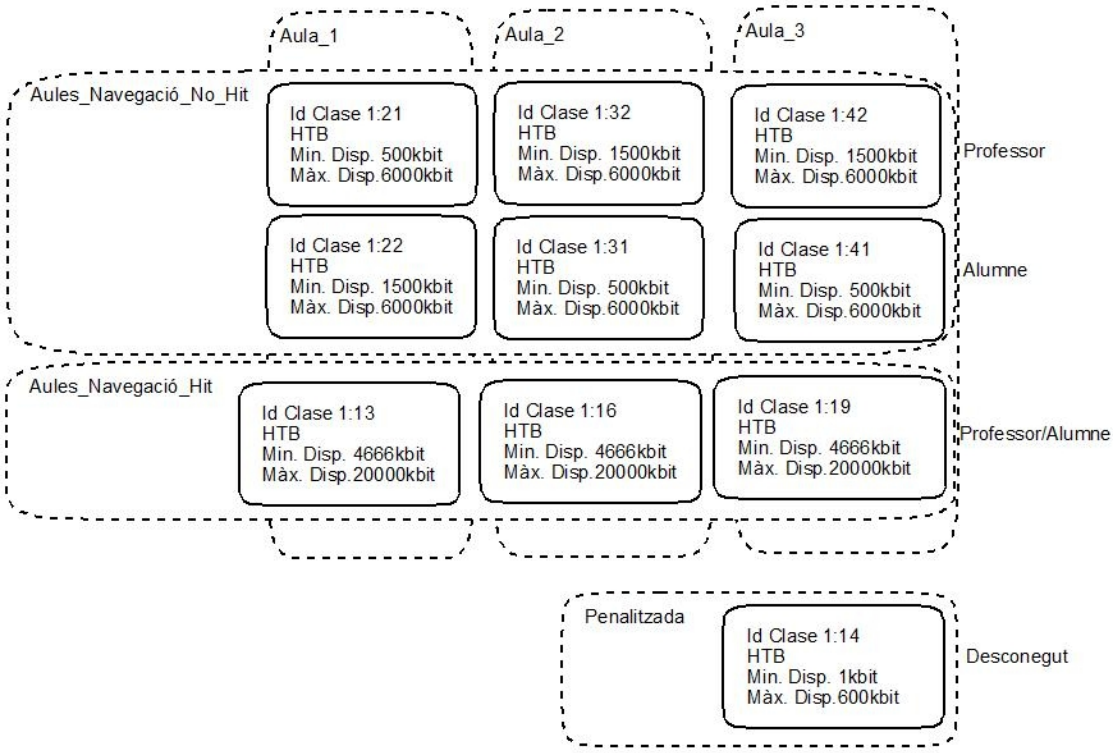


La implementació d'aquest sistema per donar resposta als requeriments, a part de la possibilitat d'assignació d'adreces dinàmica mitjançant DHCP en funció de la MAC del client i configuració del proxy en mode transparent per facilitar tasques de configuració. Tindrà el següent traspas parlant en termes de classes.

En l'esquema es mostra que el trafic de cada aula quedarà ordenat en quatre classes, cadascuna correspondrà a un dels següents cassos:

- Classe normal professors 1:22/32/42: Trafic de professor que es descarrega directament d'Internet
- Classe normal alumnes 1:11/21/31:Trafic d'alumnat que es descarrega directament d'Internet
- Classe Hit de l'aula 1:13/16/19: Trafic d'alumnat o professorat (degudament prioritzats) que es descarrega de la memòria cau del proxy.
- Classe Penalitzada 1:14: Trafic de fonts no controlades.

Esquema 12. Esquema implementació amb classes HTB

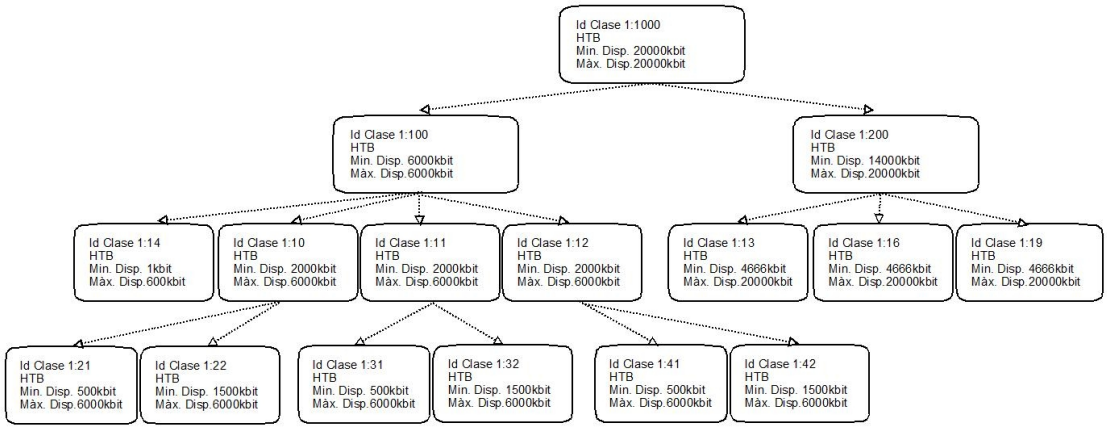


Com a disciplina de cua que complís els prerequisits de permetre prioritats, tenir sub-classes i funcionalitat de gestió de l'ample de banda s'ha decidit utilitzar HTB enfront d'altres com CBQ per proveir similars funcionalitats amb més senzillesa de configuració (més paràmetres autocalculats i donat que les suposicions de mida de paquets es corresponen amb els valors de l'estudi previ de la xarxa).

A nivell de root es disposa d'una classe que limitarà el global del trafic al màxim de la interfície física de l'equip i dos sub-classes que representaran el trafic Hit i no Hit respectivament i que tindran com a límits la capacitat màxima assolible per

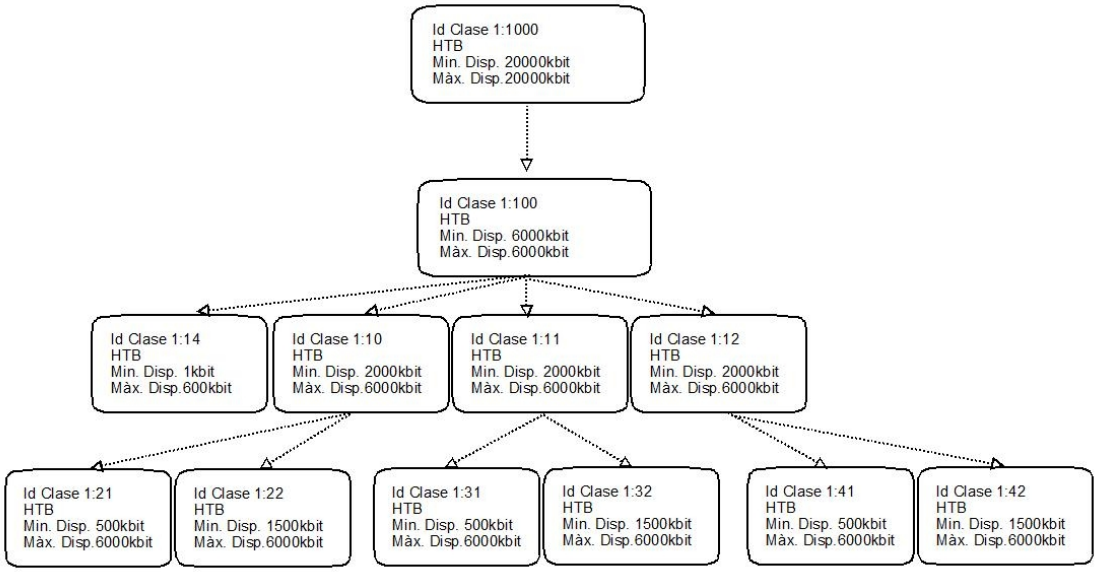
l'equipament de xarxa intern i la capacitat de la suma d'accessos a Internet del centre respectivament.

Esquema 13: Arbre global de classes



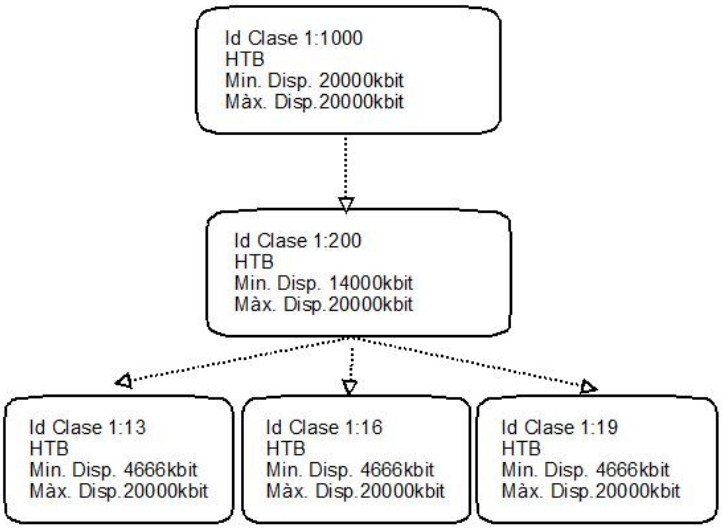
De la branca no Hit cal destacar que la seva classe principal ja estarà limitada a la capacitat de la suma d'accessos a Internet del centre (6000kbit/s en l'exemple) i que aquest màxim coincidirà amb els de les aules per tal que cadascuna independentment el pugui assolir en cas d'estar disponible.

Esquema 14: Detall branca trafic no Hit



A la branca Hit malgrat els límits coincidiran amb la capacitat màxima de l'equipament del centre, el mínim garantit serà el resultat de sostreure d'aquest el mínim garantit de la branca no Hit amb la que comparteix arrel 14000kbit/s en l'exemple).

Esquema: 15: Detall branca trafic Hit

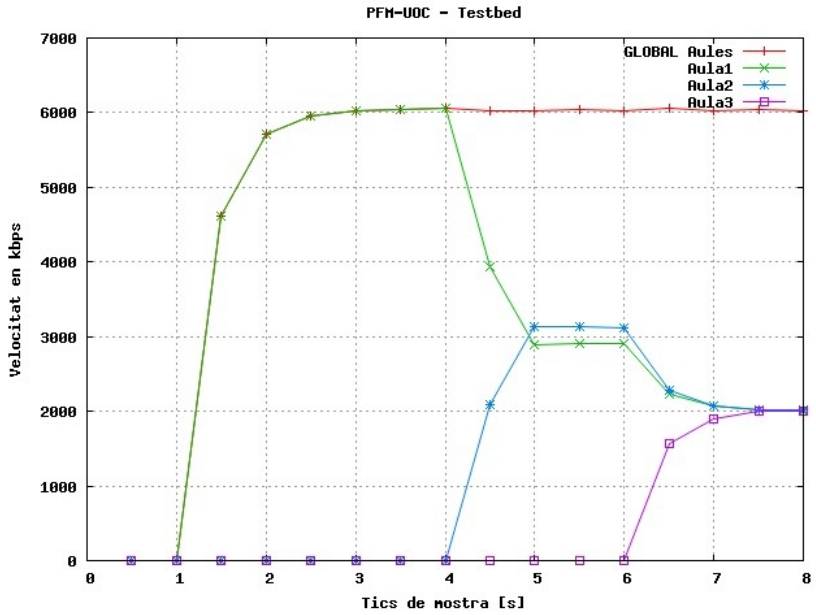


5. Resultats dels experiments

5.1 Test_1. Simulació: Aules amb accés a Internet sense memòria cau

El primer test efectuat mitjançant l'us de l'eina Ethloop s'ha testat la configuració exposada en l'anterior apartat simulant un accés seqüencial a Internet de les aules.

Gràfica 1: Accés seqüencial Aules no Hit



T1: Aula 1 accedeix a Internet demanant 8000kbps

El trafic queda limitat per el sistema gestor als 6000kbps

T4: Aula 2 accedeix a Internet demanant 8000kbps

El trafic queda limitat per el sistema gestor als 6000kbps i repartit a parts iguals per les dues aules que l'utilitzen (3000kbps/aula).

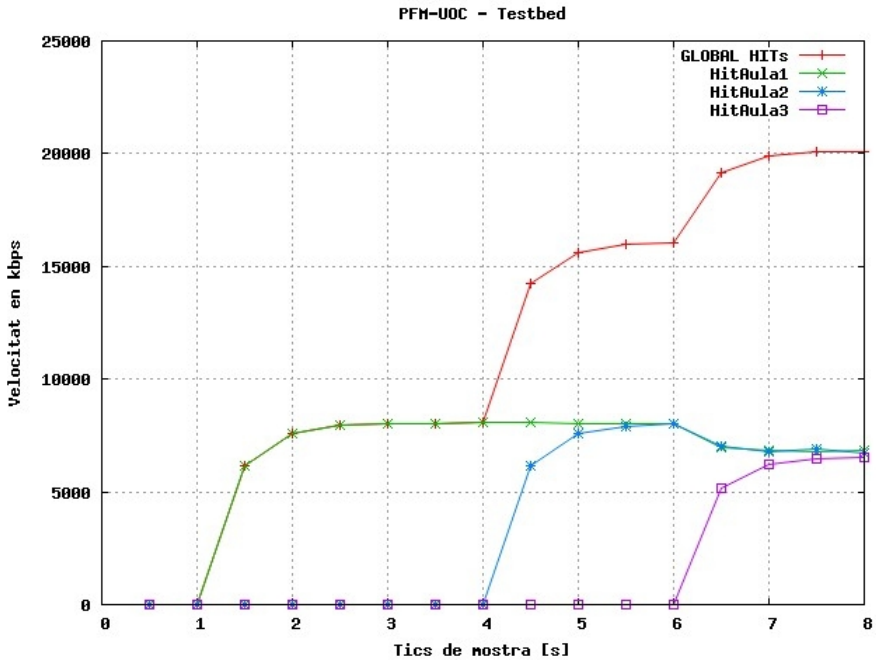
T6: Aula 4 accedeix a Internet demanant 8000kbps

El trafic queda limitat per el sistema gestor als 6000kbps i repartit a parts iguals per les tres aules que l'utilitzen (2000kbps/aula).

5.2 Test_2. Simulació: Aules amb accés a Internet utilitzant memòria cau

Aquest segon test pretén demostrar que si l'anterior situació es donés amb situació de Hit, els límits variarien (fins al màxim global definit donat que no hi ha més transmissions) i que les igualtats es mantenen.

Gràfica 2: Accés seqüencial Aules Hit



T1: Aula 1 accedeix a Internet demanant 8000kbps fent Hit a la memòria cau

En ser Hit i haver-hi ample de banda disponible i ser la demanda inferior al permès en cas de Hit aquest pot assolir els 8000kbps demanats.

T4: Aula 2 accedeix a Internet demanant 8000kbps fent Hit a la memòria cau

En ser Hit i haver-hi ample de banda disponible i ser la demanda inferior al permès en cas de hit aquest pot assolir els 8000kbps. Malgrat la suma dels dos Hits supera els13500kbps de rate assignat s'utilitza el lliure restant per arribar als 16000.

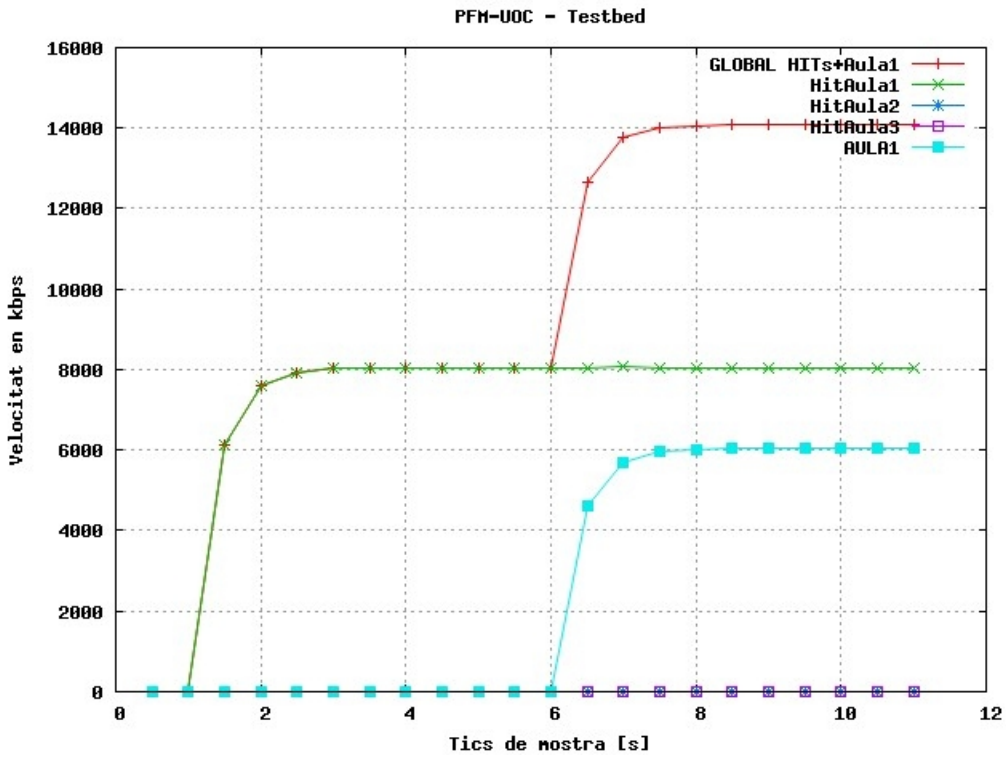
T6: Aula 4 accedeix a Internet demanant 8000kbps fent Hit a la memòria cau

El trafic queda limitat per el sistema gestor als 20000kbps repartit a parts iguals per les tres aules que han fet Hit.

5.3 Test_3. Simulació: Accés amb Hit combinat amb accés normal

Amb aquest test es pretén demostrar que si una aula té trafic Hit i s'origina trafic directe el sistema permet independentment que aquests assoleixin els seus màxims fixats en cas de disposar d'ample de banda disponible.

Gràfica 3: Accés combinat Hit i no Hit



T1: Aula 1 accedeix a Internet demanant 8000kbps fent Hit a la memòria cau

En ser hit i haver-hi ample de banda disponible i ser la demanda inferior al permès en cas de hit aquest pot assolir els 8000kbps.

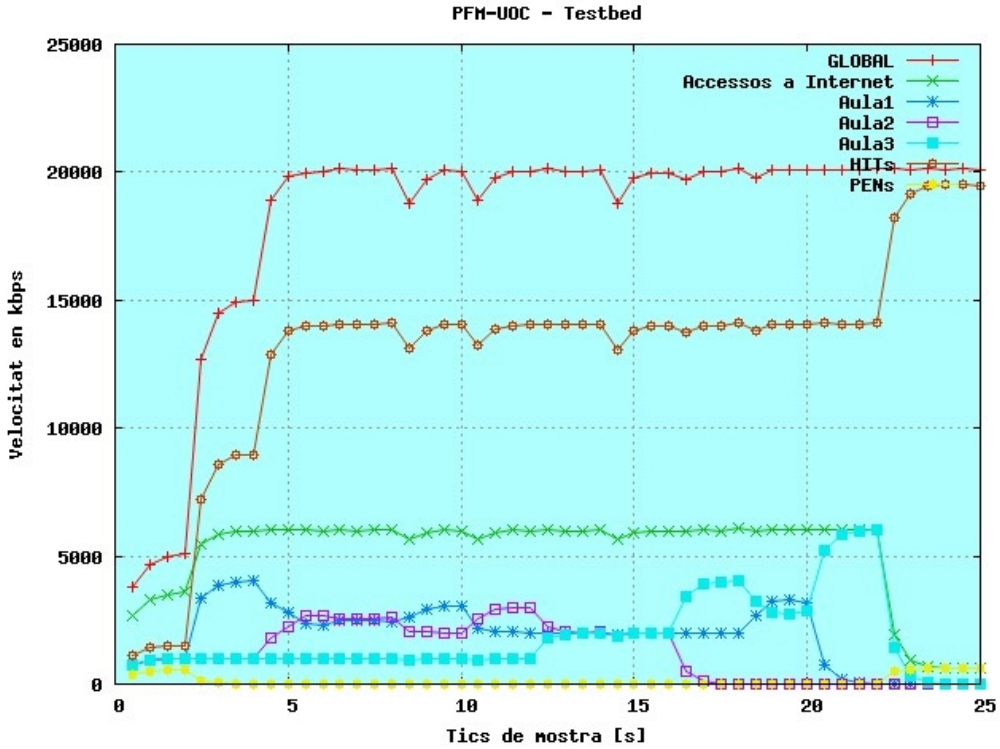
T6: Aula 1 accedeix a Internet demanant 8000kbps sense fer Hit

Es manté l'assignació dels 8000kbps al Hit i no haver-hi consum s'assoleix el màxim permès per l'aula 6000kbps (que es composen dels 2000kbps de l'aula més 4000kbps demanats prestats a les altres dues).

5.4. Test 4. Simulació: Test global de situacions simultànies

En aquesta simulació, juntament amb la suposició que els Hits provenen realment de la memòria cau es demostra el compliment dels patrons prèviament especificats en la taula1 [taula1], alhora que es pot observar la coordinació del sistema davant dels continus canvis de situació i configuració.

Gràfica 4: Test global



- Esdeveniment_0: (Temps 0s)

  Inicien tots els fluxos menys la més prioritària (aula2) demanen 500kbps, En estar dins dels rates i haver-hi ample de banda disponible assoleixen l'ample de banda desitjat.

- Esdeveniment_1: (temps: segon 1)

  Espontani sense acreditació accedeix a Internet demanant 8000kbps, comença a consumir ample de banda.

- Esdeveniment_2: (temps: segon 2)

  Classe_normal_aula1 passa del seu mínim i demanarà el restant com que passarà del global es limitarà automàticament. Malgrat demanen el mateix ample de banda, les classes de l'aula 1 (la prioritària representa el professor) el rebran en una proporció 1/3 degut a la proporció dels seus "rate" que actuen donant pes a cadascuna la classe 1(alumne) no baixarà dels seus 500 kbps garantits la classe 2 (professor) no baixarà dels seus 1500 kbps garantits la classe global no baixarà dels seus 2000 kbps garantits Si no hi ha trafic a prestar relació (1/3) Ex: 500/1500 (T15)

- Esdeveniment_3: (temps: segon 2)

  Hit produït a l'aula 1, té ample restant (no hi ha més hits) Assoleix sense problemes el bw demanat, la classe està per sota del seu rate garantit 14000kbit. (No hi arriba a la gràfica per manca de temps d'estabilitzar-se).

- Esdeveniment_4: (temps: segon 4)

  Les 2 classes de l'aula 2 demanen ample de banda. La classe 2 no baixarà els seus 500k garantits La classe 1 no baixarà els seus 1500k garantits. Si xarxa global saturada: reben els seus mínims en proporció 1/3 Ex: 500/1500 (T11-T12), si hi ha bw disponible sobrant: reben el restant en una proporció 1/3: Ex: 500+250/1500+500(T7)
- Esdeveniment_5: (temps: segon 4)

  Hit a la classe 2 demana 8000000kbps com que hi ha ocupat per hits de una altra aula i la suma supera el màxim permès global (per no saturar wifi) s'assigna el mínim assignat a cada aula (per els hits) (7000kbps cadascun estabilitzat al segon6)
- Esdeveniment_6: (temps: segon 6)

  El hit de l'aula 3 s'amplia per descarregues de vídeos a 8 mbps = 1000000kbps Aquesta ampliació no afecta el normal funcionament del sistema només al trafic existent de Hits. Com que aula2 i 1 estan també sobre màxims es reparteixen el 33% de l'ample de banda disponible per Hits, es a dir els mínims rate 4666kbps per hits d'aula
- Esdeveniment_7: (temps: segon 8)

  Es prioritza l'aula 1, el trafic fins ara equitativament repartit entre la classe 1 i 2 passa a ser prioritàriament assignat a l'aula1.
- Esdeveniment_8: (temps: segon 10)

  Es prioritza l'aula 2, el trafic fins ara prioritzat a l'aula 1 passa a ser prioritàriament assignat a l'aula2.
- Esdeveniment_9: (temps: segon 12)

  Aula 3 demana més ample de banda i com que el té garantit les altres 2 deixen de rebre part del sobrant d'aquesta que fins ara utilitzaven. Les tres aules reben el seu rate garantit
- Esdeveniment_10: (temps: segon 14)

  Es prioritza l'aula 3 com que totes superen els màxims aquest canvi no té cap efecte, segueixen rebent les 3 el garantit.

  ** Una opció per obtenir també prioritat i fins i tot en aquest casos de sobre -màxims obtingui més ample de banda serà canviar els rates en comptes de les prioritats, o fer els dos canvis alhora.
- Esdeveniment_11: (temps: segon 16)

  Es prohibeix accés a Internet a aula 2 de les dues classes restants s'endú la major part del sobrant la 3 que és la més prioritària
- Esdeveniment_12: (temps: segon 18)

  L'aula 3 torna a tenir la mateixa prioritat que la resta d'aules, l'ample de banda es reparteix equitativament entre les que n'estan consumint.
- Esdeveniment_13: (temps: segon 20)

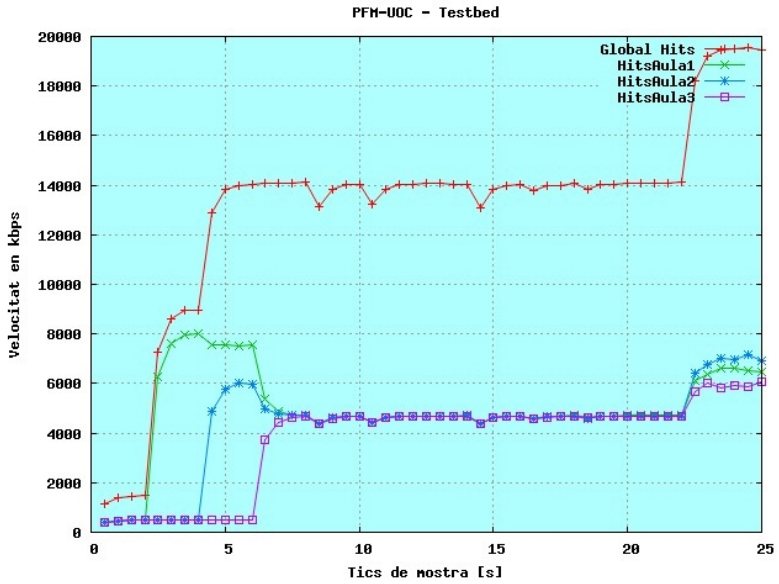
  La aula 1 deixa de transmetre, l'aula 3 es queda amb tot l'ample de banda.
- Esdeveniment_14: (temps: segon 22)

  L'aula 3 deixa de transmetre, com que hi ha hits en totes les aules aquests es reparteixen tot l'ample de banda restant fins al llindar dels 20000000kbps menys

els consumits per la classe menys prioritària a la que s'ha assignat 600kbps consumibles només si no hi ha trafic saturat a les aules.

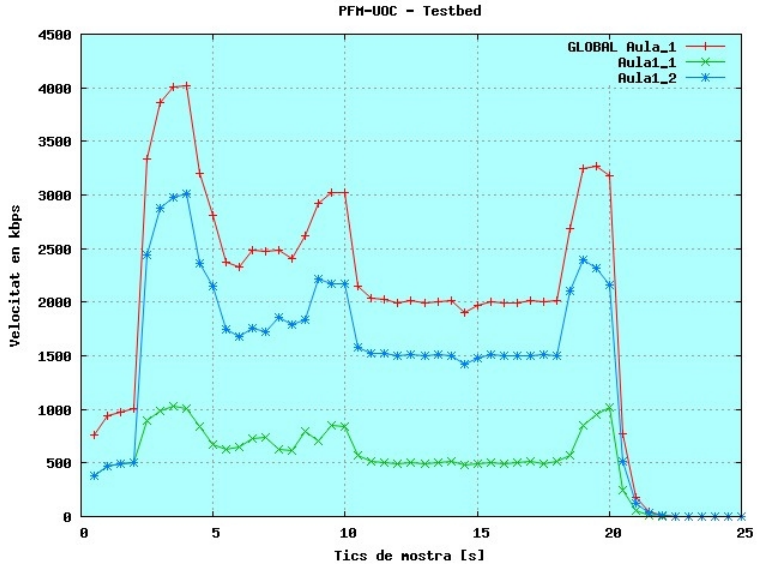
En la gràfica dels consums de trafic Hit per aules es mostra que l'assignació d'ample de banda és equitativa i que mentre el sistema esta saturat queda limitat als mínims garantits mentre que quan el sistema es descarrega s'aprofita l'ample de banda sobrant, assignat també manera equitativa.

Gràfica 5: Filtrat per Hits

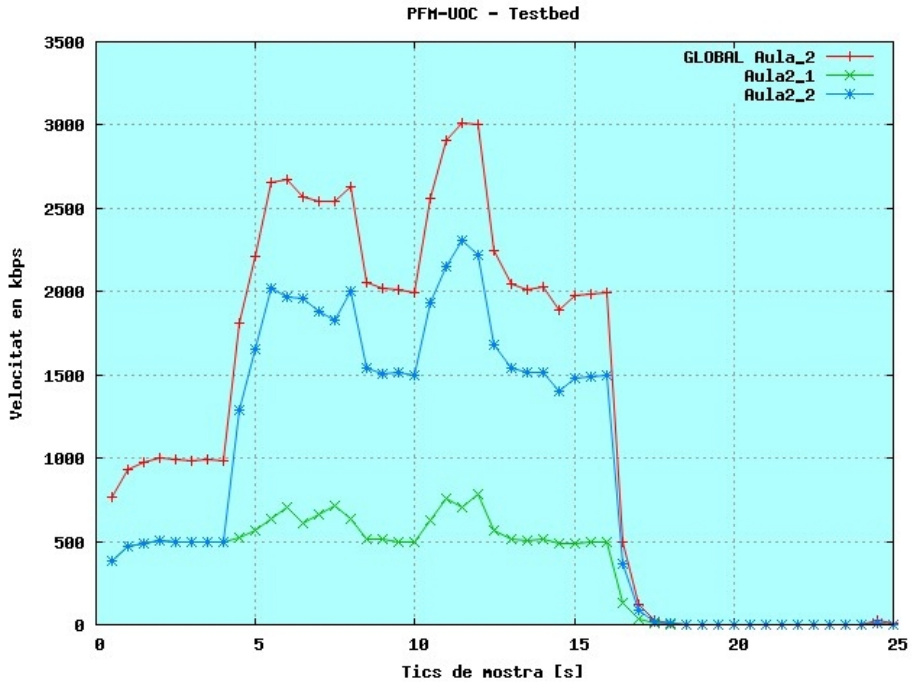


En les gràfiques filtrades per trafic d'aula es mostra la prioritat dels fluxos de professor, essent major l'assignació de trafic mínim 500/1500kbps i mantenint la proporció (1/3) per el trafic demanat prestat.

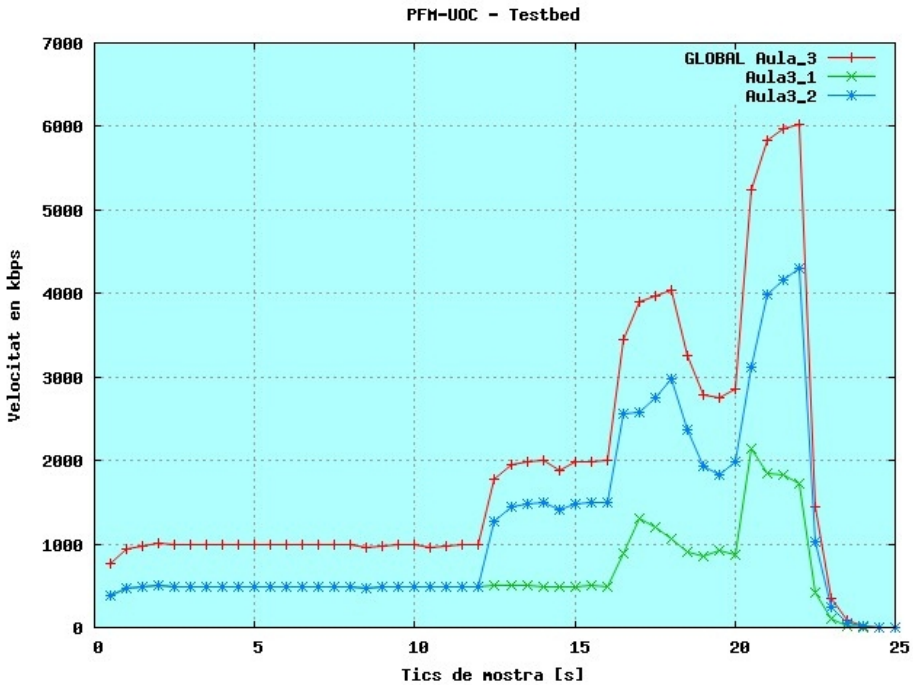
Gràfica 6: Filtrat per consums de l'aula1



Gràfica 7: Filtrar per consums de l'aula2

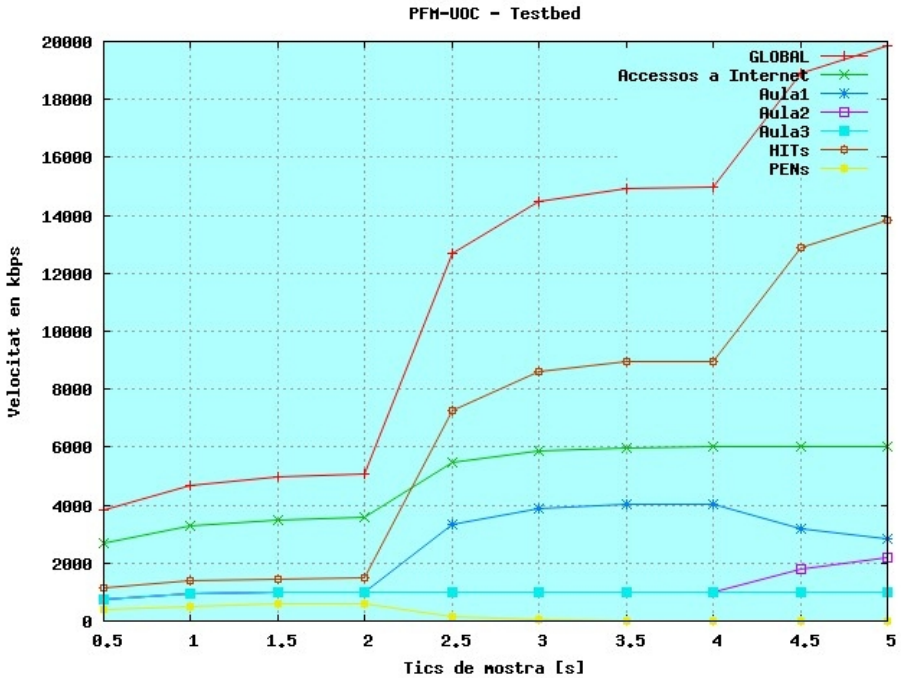


Gràfica 8: Filtrat per consums de l'aula3

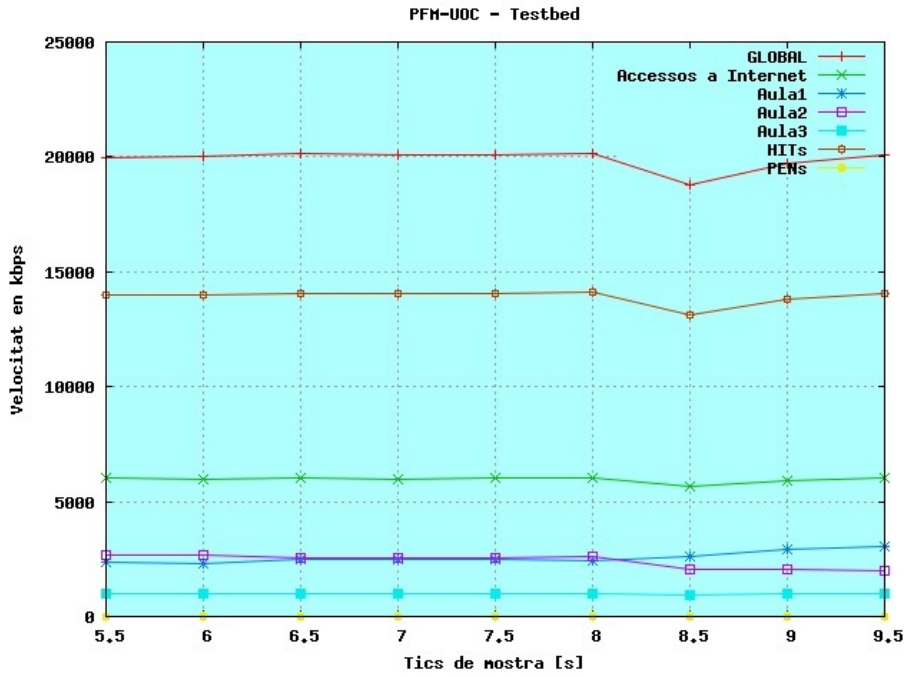


Per poder fer un seguiment més detallat dels anteriors esdeveniments s'aporten les gràfiques en intervals de 5 segons.

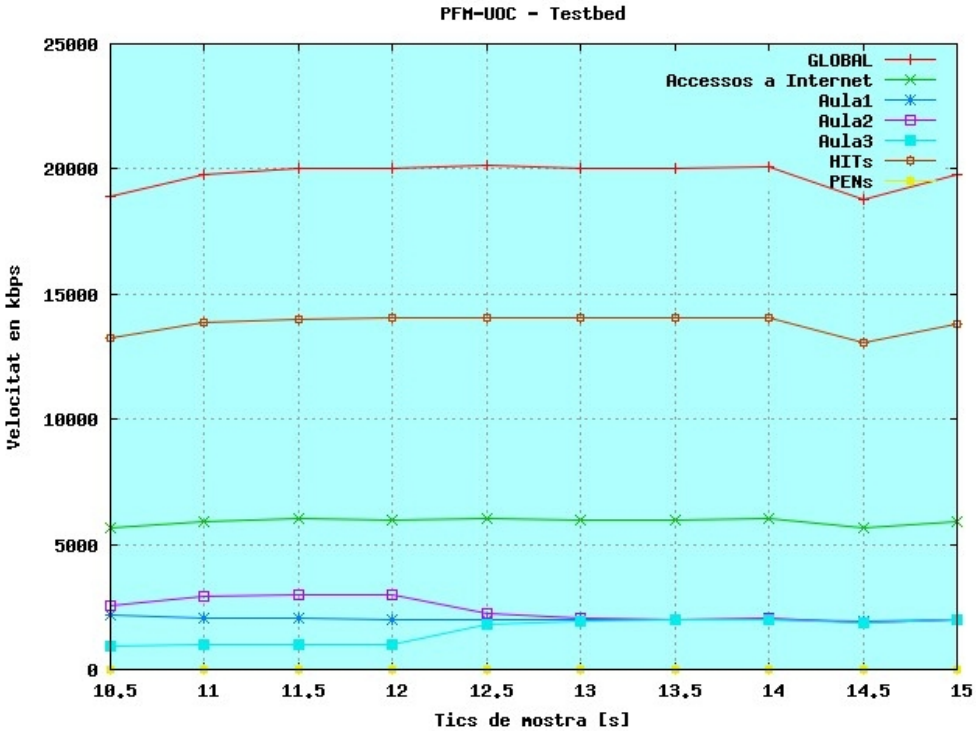
Gràfica 9: Detall global temps 1s-5s



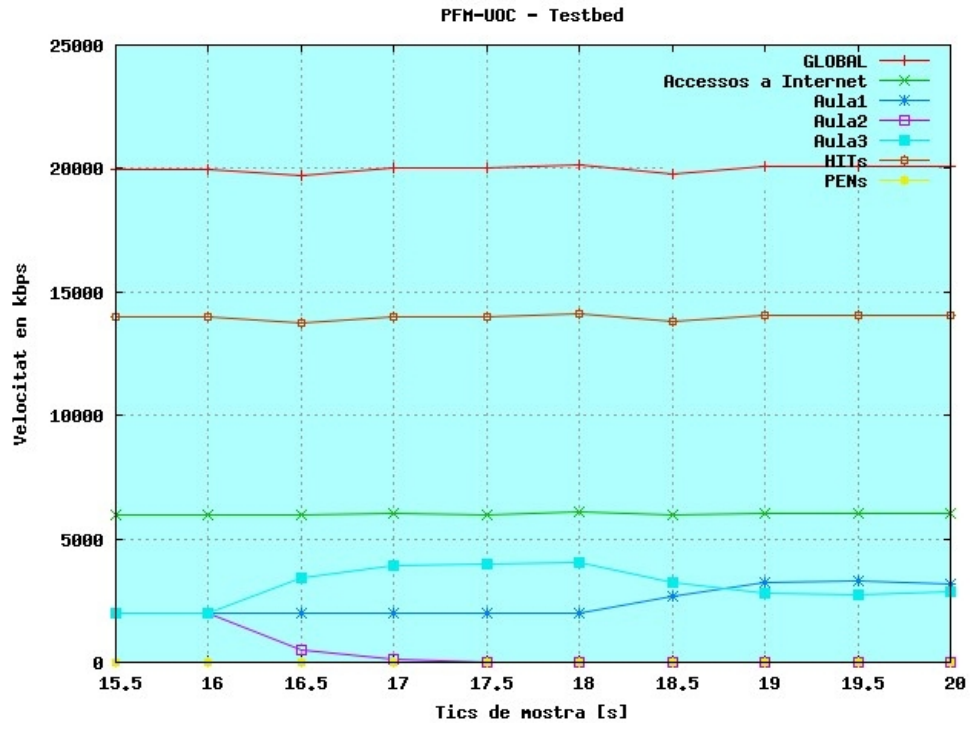
Gràfica 10: Detall global temps 5s-10s



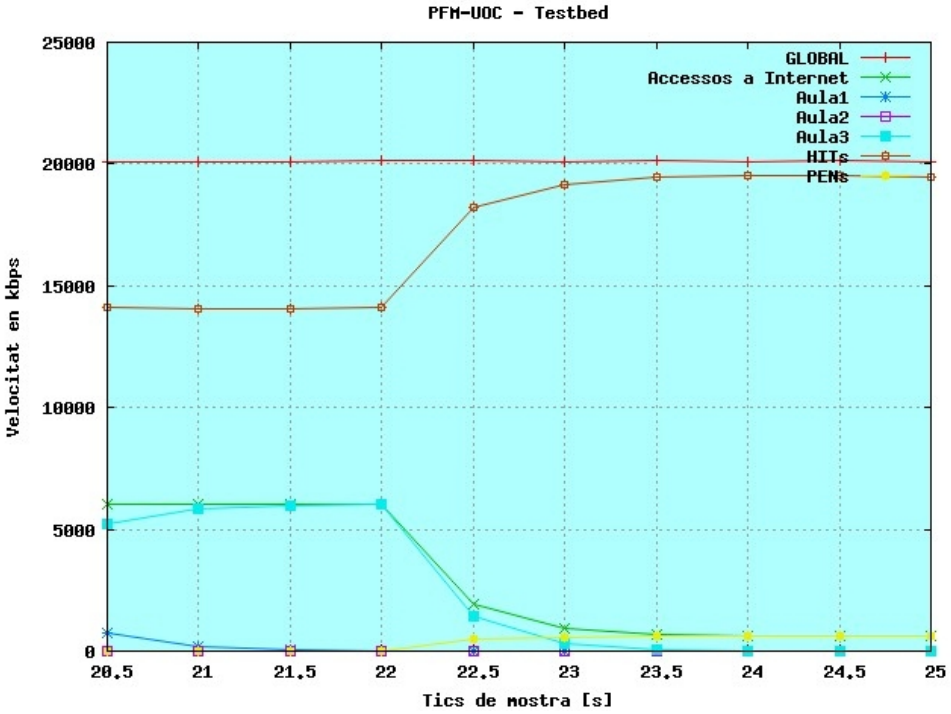
Gràfica 11: Detall global temps 10s-15s



Gràfica 12: Detall global temps 15s-20s



Gràfica 13: Detall global temps 20s-25s



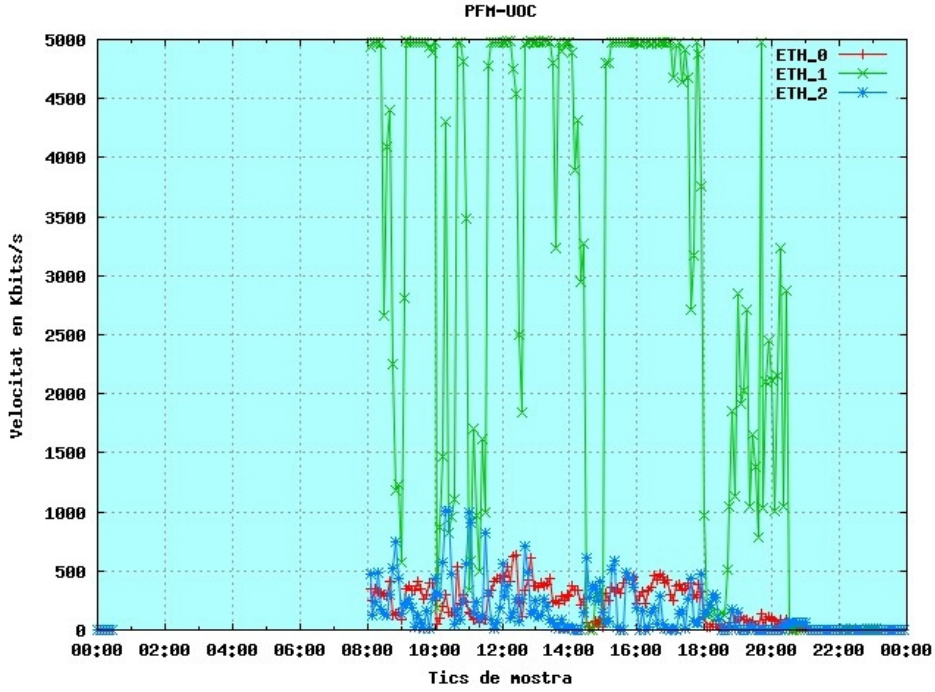
5.5. Test 5. Test en Real: Prova de concepte divisió trafic amb compartició

Per poder avaluar una prova de concepte de la gestió en real s'implementa la funcionalitat base de compartició de l'ample de banda amb mínims garantits i llindar superior per evitar l'us dels buffers de l'equipament de connexió a Internet. S'ha limitat la capacitat del sistema a 5000kbps de baixada (eth0) i a 640kbps de pujada (eth1). Assignant a cada aula una mateixa prioritat i ample de banda mínim garantit (capacitat total/numero d'aules). La interfície (eth2) comparteix la connexió a Internet i té la limitació a 1000kbps de manera que en cas de saturació de les dues no se superin els 6000kbps que és la capacitat màxima que s'ha suposat de la connexió a Internet.

Les gràfiques generades a partir de la recollida de dades d'estat cada 5 minuts (concretament de la velocitat mitjana els últims 10 segons de cada classe retornat per ts class show) permeten mostrar el funcionament efectiu de la limitació d'ample de banda a 5000kbps mentre que demostren que de no estar limitat per el sistema gestor seria l'equipament d'accés a Internet qui hauria de gestionar-ho (sense garanties ni control del repartiment de l'ample de banda) i per tant en justifiquen la seva implantació.

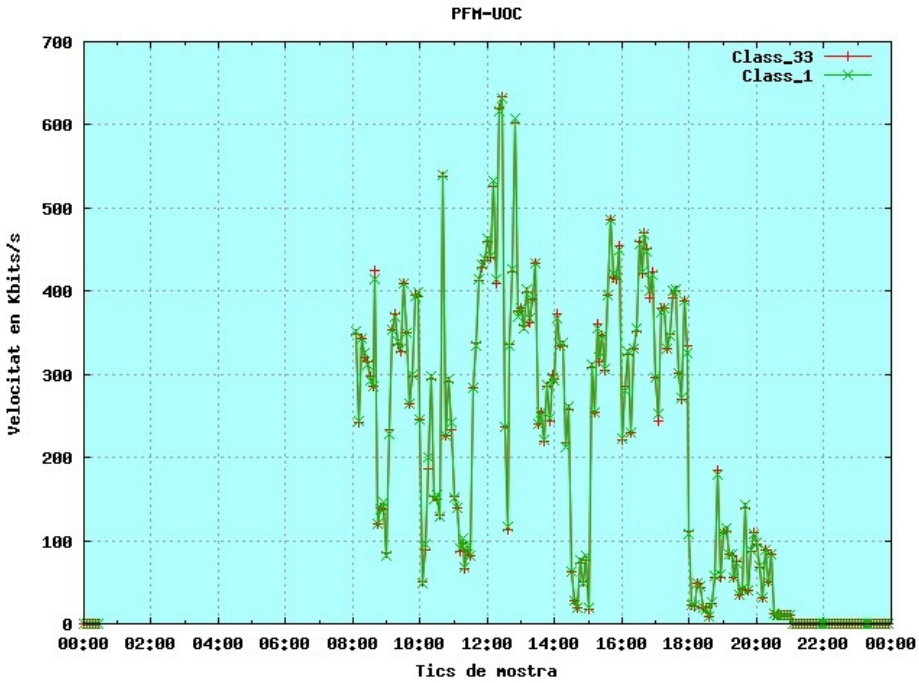
El patró global de consum mostra que al migdia (14:30h-15:00h), interval en que no s'imparteixen classes el consum del sistema va a mínims, un descens del consum tot i que menys pronunciat es dona alhora d'esmorçar (11:00h-11:30h). En aquest punt es pot observar que la interfície eth2 en ser accessible en aquest període marca els màxims, el seguiment i confirmació d'aquests podrien ajudar a afinar el sistema..

Gràfica 14: Detall globals totes interfícies (eth0,eth1,eth2)



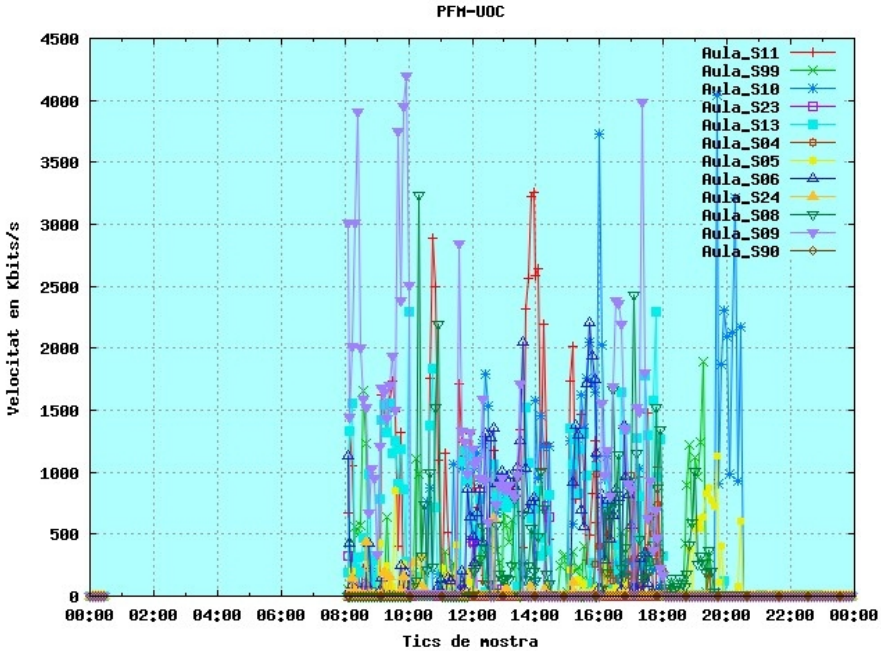
En la gràfica 4 permet observar el treball limitador a 5000kbps del sistema gestor aplicat sobre eth1, de 1000kbps sobre eth2 i de 640 sobre eth0.

Gràfica 15: Detall globals filtrat per eth0



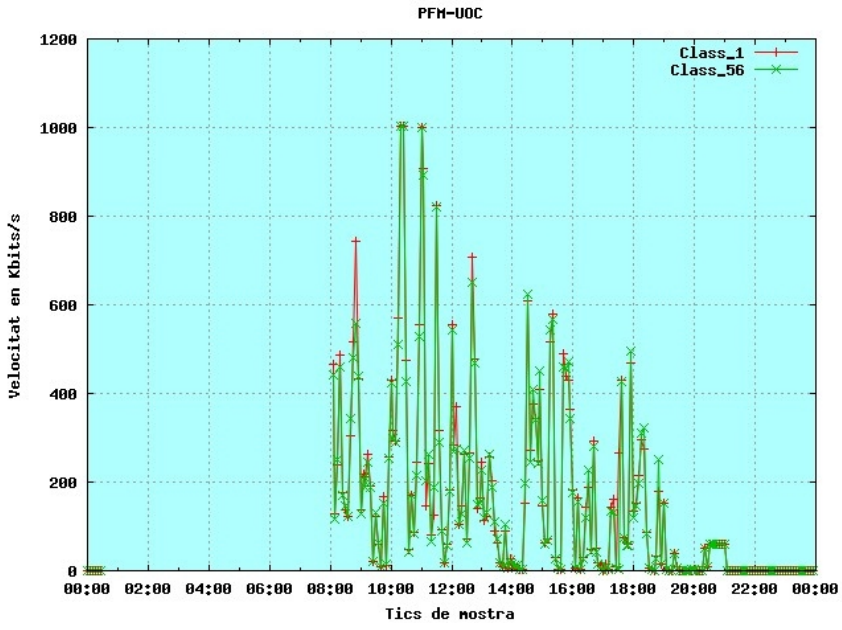
En la gràfica 16 es mostra la concurrència d'accessos de les diferents aules, el consum per aula no arriba a 4500kbps en cap moment, o bé no s'excedeix d'aquest consum o bé el sistema no disposa de més ample de banda degut al consum d'altres aules.

Gràfica 16: Detall globals filtrat per eth1



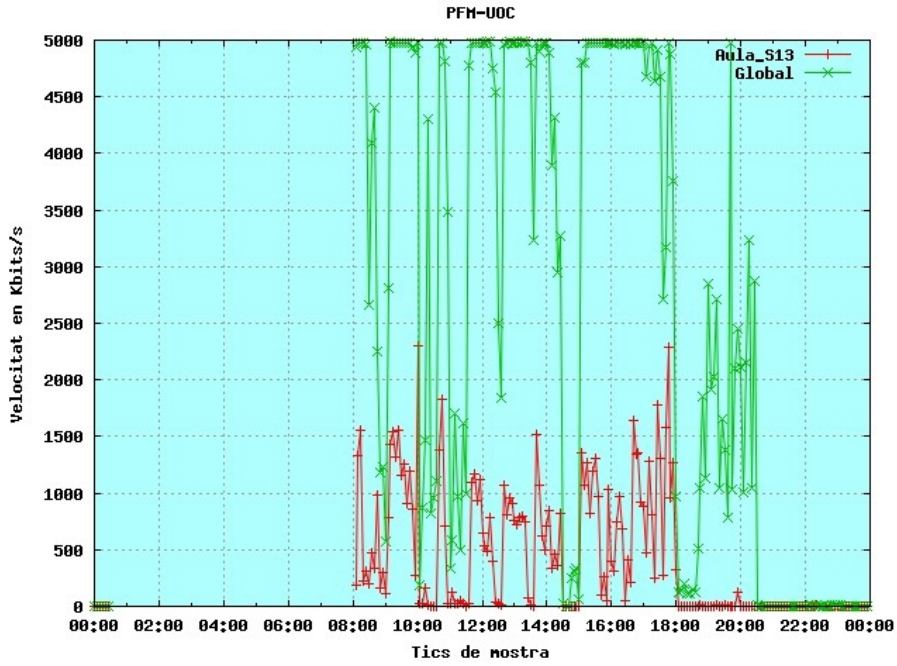
En el detall mostrat en la gràfica 17 es mostra que la interfície 17 que només gestiona una aula pràcticament no arriba a consumir el seu ample de banda màxim 1000kbps. L'estudi del seguiment d'aquestes dades permetrà fer una millor configuració del sistema.

Gràfica 17: Detall globals filtrat per eth2

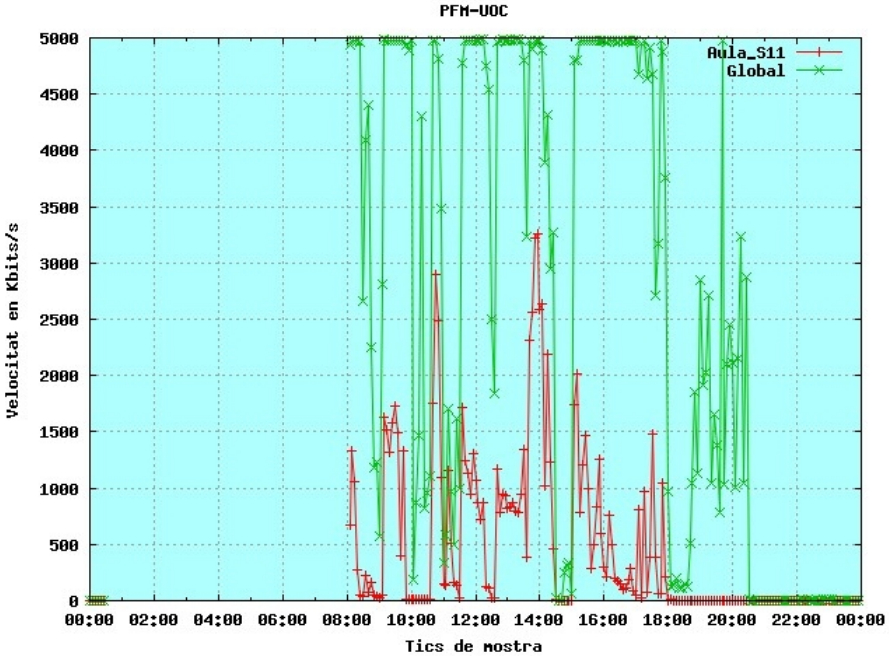


En la gràfica 18 de l'aula 13 es pot veure el seu patró d'us, destacant que no s'en fa us des de les 18h, aquesta dada si es pot demostrar que és un patró repetitiu pot ajudar a configurar el sistema de manera semi-dinàmica. El mateix podríem fer amb els resultats de la gràfica 19 corresponent a l'aula S11.

Grafica 18: Detall globals filtrat per Aula13

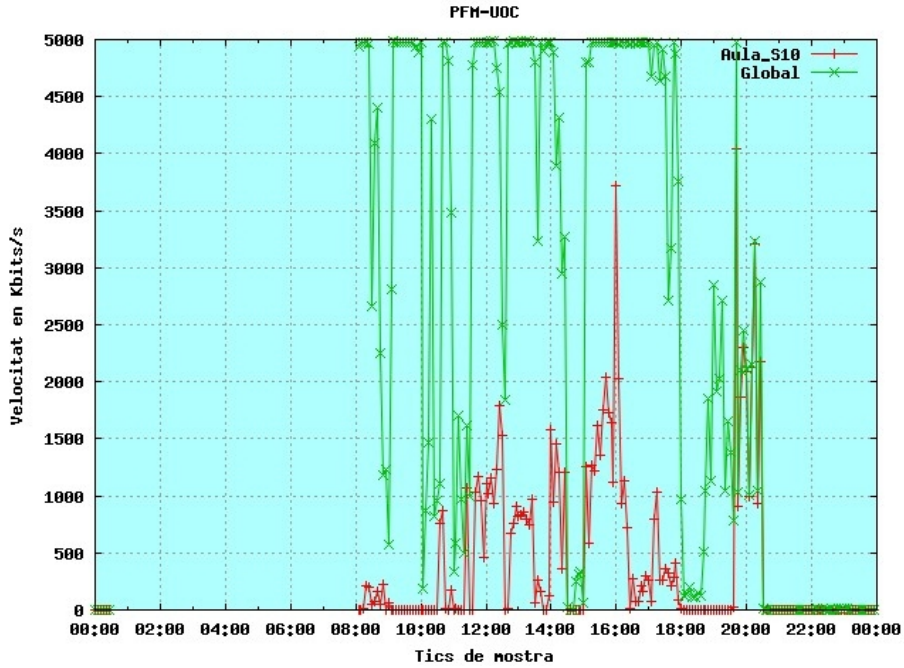


Gràfica 19: Detall globals filtrat per AulaS11



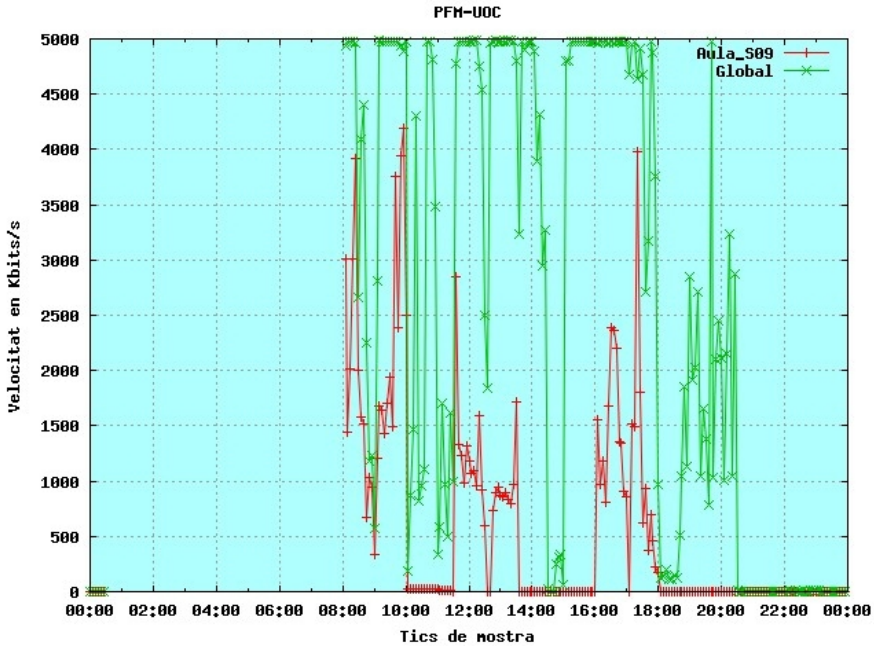
El la gràfica 20 de l'aula S10 es pot comprovar que en estar el sistema més lliure a partir de les 18h si en necessita pot consumir més ample de banda.

Grafica 20: Detall globals filtrat per AulaS10



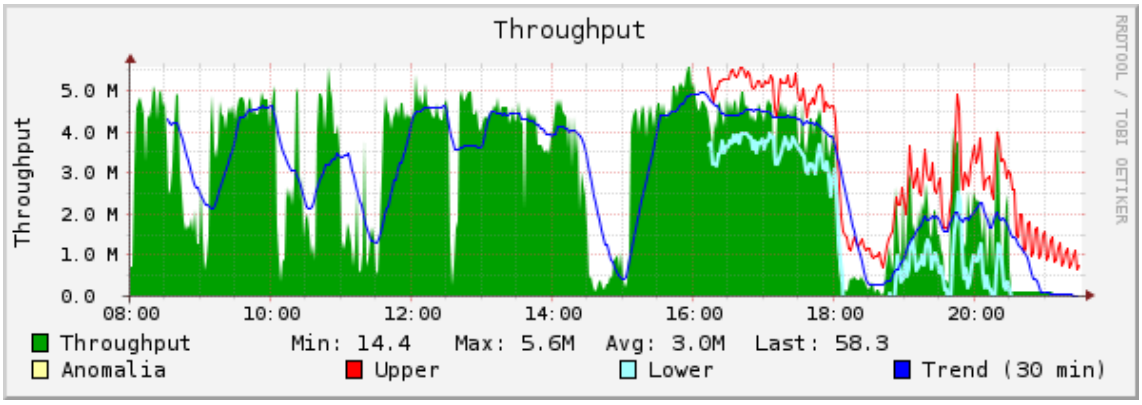
La gràfica 21 de l'aula 10 mostra un fet similar però en aquest cas amb els consums abans de les 10h.

Gràfica 21: Detall globals filtrat per AulaS09



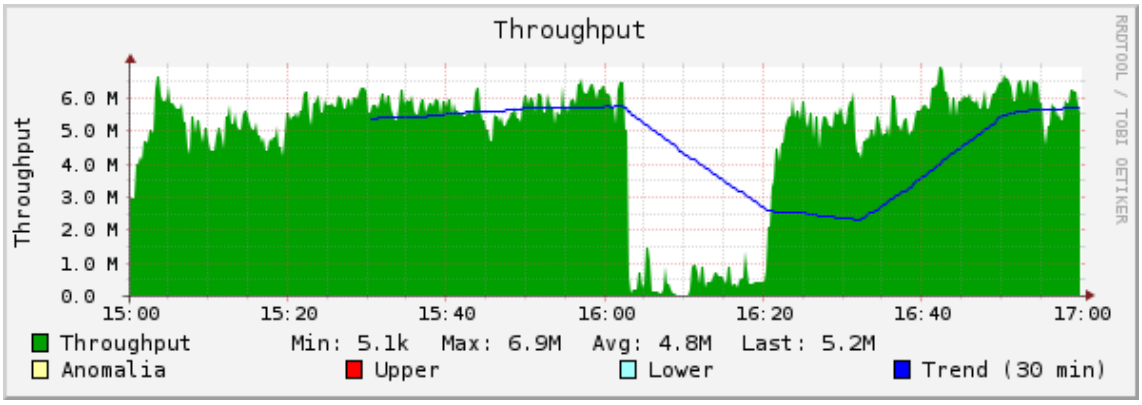
Per tal de verificar les dades anteriors (no només l'origen, també els scripts intermedis amb que s'han recollit, formatat, convertit i mostrat les dades), s'utilitza la gràfica generada utilitzant el programari Ntop (en un equip diferent, fent la mesura en el punt de connexió del centre amb Internet). Evidentment només podrem confirmar els globals, la distribució no ens la permetrà mostrar.

Gràfica 22: Resultats globals eina Ntop



En el cas de pujar excessivament els límits (per poder fer la comparació simulant que no hi ha cap gestió d'ample de banda) i fer actuar els buffers de l'equipament de connexió a Internet, en no estar preparats per suportar un consum constant amb volums alts de connexions podrien provocar situacions de saturació i talls com la que s'observa en la següent gràfica 23.

Gràfica 23: Configuració per simulació de sistema sense gestió



5.6 Test6: Comunicació Squid – TC

Aquesta configuració és indispensable per a que els Hits puguin rebre més ample de banda. Marcatge de paquets "Hit" (camp ToS) mitjançant squid. S'ha testat que Squid en la seva versió 2,7 (cal destacar que aquesta funcionalitat és diferent a versions anteriors i no esta portada encara a la versió 3) l'opció de marcatge de paquets. S'han provat amb

èxit 2 configuracions, la primera utilitzant el marcatge en el camp de ToS que és remarcat des de Iptables per posteriorment ser classificat des de TC i la segona més directe assignant directament una classe al paquet mitjançant Iptables. L'observació del transit mitjançant l'eina de captura Wireshark i la comanda *tc class show*, combinat amb els fitxers de log del Squid ha permès confirmar que aquests són marcats correctament en cas de Hit.

Al fitxer squid.conf cal fer els següents canvis:

```
server_persistent_connections off
zph_mode tos
zph_local 0x30
```

Dins del script de creació de l'entorn de cues i classes s'han testat amb èxit dos possibles configuracions:

- Opció 1 (amb iptables i tc filter):

```
iptables -t mangle -A POSTROUTING -o eth0 -p tcp --sport 3128 -m tos --tos 0x30
-j MARK --set-mark 30
tc filter add dev eth0 parent 1: protocol ip handle 30 fw classid 1:300
```

- Opció 2 (directe des de iptables):

```
iptables -t mangle -A POSTROUTING -o eth0 -p tcp --sport 3128 -m tos --tos 0x30
-j CLASSIFY --set-class 1:300
```

5.7 Test7: Cache de contingut multimèdia de Youtube i Vimeo

Per tal de potenciar l'aprofitament d'aquesta configuració s'ha fet una prova de concepte de descàrrega de contingut que en situacions normals no és desat en memòria cau (comportament derivat de l'ús de CDNs i alhora forçat per els servidors modificant intencionadament la url).

Per a dur a terme la prova s'ha modificat la configuració de Squid de manera que les peticions cap a servidors de Vimeo i Youtube reescriguin les Urls que s'utilitzen com a hash al desar-les a la cache de squid.

En el següent llistat s'observa que els primers dos accessos al vídeo no han fet Hit (RELEASE), concretament es veu que el segon varia en itag que és el referent a la qualitat demanada. En la tercera i quarta petició es mostra que ja s'ha fet Hit (SWAPOUT) tant per una com per altra qualitat. Les peticions han estat efectuades des d'equips diferents.

Llistat 1: Store.log

```
1294257966.478 RELEASE -1 FFFFFFFF A8765D22E67FED9CB4178FB39A22FF4B  200
1294257915 1262026994 1294282500 video/x-flv 14312139/1533307 GET
http://v7.cache1.c.youtube.com/videoplayback?ip=0.0.0.0&sparams=id%2Cexpire%2Cip
```

%2Cipbits%2Citag%2Calgorithm%2Cburst%2Cfactor%2Coc%3AU0dYSVJTUF9FSkNNOF9KTVRJ&algorithm=throttle-factor&**itag=5**&ipbits=0&burst=40&sver=3&expire=1294282800&key=yt1&signature=D3733C3BCE89CCDBAF131BF2B34B960919A82265.5BFAFCC7C811C0E5AF69D880F6B7BAFA495DB1EF&factor=1.25&**id=ecff0b62bdbe98e8**&begin=26819&redirect_counter=1

1294258031.326 **RELEASE** -1 FFFFFFFF F4F79A5AAC850F5B647D40F604FE9ED2 200 1294257986 1262028673 1294282500 video/x-flv 29359962/677020 GET http://tc.v14.cache5.c.youtube.com/videoplayback?ip=0.0.0.0&sparams=id%2Cexpire%2Cip%2Cipbits%2Citag%2Calgorithm%2Cburst%2Cfactor%2Coc%3AU0dYSVJTUF9FSkNNOF9KTVRJ&algorithm=throttle-factor&**itag=35**&ipbits=0&burst=40&sver=3&expire=1294282800&key=yt1&signature=7152A6DED00A99358E5870E339DCCDBF31C8144C.9B997485E75EAD32EC38CC55523274E4421C596E&factor=1.25&**id=ecff0b62bdbe98e8**&begin=46680&redirect_counter=1

1294258295.976 **SWAPOUT** 00 00000234 882E7B24E168BCBBE569C0BE145A0051 200 1294257937 1262026994 1294282500 video/x-flv 15390549/15390549 GET http://tc.v15.cache6.c.youtube.com/videoplayback?ip=0.0.0.0&sparams=id%2Cexpire%2Cip%2Cipbits%2Citag%2Calgorithm%2Cburst%2Cfactor%2Coc%3AU0dYSVJTUF9FSkNNOF9KTVRJ&algorithm=throttle-factor&**itag=5**&ipbits=0&burst=40&sver=3&expire=1294282800&key=yt1&signature=D3733C3BCE89CCDBAF131BF2B34B960919A82265.5BFAFCC7C811C0E5AF69D880F6B7BAFA495DB1EF&factor=1.25&id=**ecff0b62bdbe98e8**&redirect_counter=1

1294258367.133 **SWAPOUT** 00 00000236 F72DF189015D9D19E95FE291C6CC477E 200 1294257993 1262028673 1294282500 video/x-flv 34048701/34048701 GET http://tc.v14.cache5.c.youtube.com/videoplayback?ip=0.0.0.0&sparams=id%2Cexpire%2Cip%2Cipbits%2Citag%2Calgorithm%2Cburst%2Cfactor%2Coc%3AU0dYSVJTUF9FSkNNOF9KTVRJ&algorithm=throttle-factor&**itag=35**&ipbits=0&burst=40&sver=3&expire=1294282800&key=yt1&signature=7152A6DED00A99358E5870E339DCCDBF31C8144C.9B997485E75EAD32EC38CC55523274E4421C596E&factor=1.25&**id=ecff0b62bdbe98e8**&redirect_counter=1

En el següent llistat es mostra com es modifica la URL, es pot comprovar que malgrat les URLs són diferents el retorn del script perl per cada adreça que representa en realitat un mateix vídeo/resolució retorna una mateixa adreça. Com es pot veure els accessos són amb ips diferents i malgrat el servidor genera intencionadament adreces diferents és capaç de retornar la mateixa cadena i per tant es desa només un cop a cache. En els tests s'ha demostrat que malgrat el vídeo no hagi estat encara completament desat per el primer usuari en rebre una nova petició aquest segon rep directament la part desada per el primer.

Llistat 1: Log de seguiment generat per el script perl de rescriptura

EL QUE REBO: 0 http://v8.cache2.c.youtube.com/videoplayback?ip=0.0.0.0&sparams=id%2Cexpire%2Cip%2Cipbits%2Citag%2Calgorithm%2Cburst%2Cfactor%2Coc%3AU0dYSVZNVl9FSkNNOF9OR1pF&fexp=903903&algorithm=throttle-factor&itag=34&ipbits=0&burst=40&sver=3&expire=1294628400&key=yt1&signature=0EB835693C460B2D6FCCD1481E1411946C254514.820BF60D0B6507117291AA8031E1901D94DF0E08&factor=1.25&id=**d5c856038cb8e7d5**&redirect_counter=1 **10.0.0.107**/- - GET -

El QUE RETORNO1: 0 http://v-youtube.INTERN/videoplayback?ID=d5c856038cb8e7d5&itag=34&ordre=reves-RC 10.0.0.107/- - GET -
El QUE RETORNO2: 0 http://v-youtube.INTERN/videoplayback?ID=d5c856038cb8e7d5&itag=34&ordre=reves-RC

EL QUE REBO: 0 http://v8.cache2.c.youtube.com/videoplayback?ip=0.0.0.0&sparams=id%2Cexpire%2Cip%2Cipbits%2Citag%2Calgorithm%2Cburst%2Cfactor%2Coc%3AU0dYSVZNVl9FSkNNOF9OR1pF&fexp=903903&algorithm=throttle-factor&itag=34&ipbits=0&burst=40&sver=3&expire=1294628400&key=yt1&signature=0EB835693C460B2D6FCCD1481E1411946C254514.820BF60D0B6507117291AA8031E1901D94DF0E08&factor=1.25&id=**d5c856038cb8e7d5**&redirect_counter=1 **10.0.0.103**/- - GET -

El QUE RETORNO1: 0 http://v-youtube.INTERN/videoplayback?ID=d5c856038cb8e7d5&itag=34&ordre=reves-RC 10.0.0.103/- - GET -
El QUE RETORNO2: 0 http://v-youtube.INTERN/videoplayback?ID=d5c856038cb8e7d5&itag=34&ordre=reves-RC

Conclusions

En l'article s'ha presentat el desenvolupament i aplicació d'un possible enfoc de solució a la congestió dels accessos a Internet dels centres educatius mitjançant l'aplicació d'una gestió de l'ample de banda basada en la representació d'analogies a situacions i entorns reals, una visió que facilita la comprensió dels conceptes gestionats. Des de la fase d'identificació de necessitats i característiques del escenaris específics a cobrir, la realització d'una prova de concepte en un entorn simulat i finalment el test d'implantació parcial en un entorn real. A través d'aquest desenvolupament, s'ha demostrat la validesa d'aquest enfoc per cobrir les principals necessitats de gestió de l'ample de banda dels centres educatius, així com la possible integració amb entorns actuals i alguns exemples de les possibilitats d'ampliació de funcionalitats en ser un sistema obert.

Addicionalment, l'apartat dedicat a l'estat de l'art, presenta un complet estudi de solucions existents representatives que mitjançant diversos enfocaments tracten de donar resposta a les necessitats de gestió de l'ample de banda. Donada la diversitat de solucions, s'han proposat diverses possibles classificacions que en faciliten alhora la seva comparació amb la solució proposada. Es destacable la orientació cal a l'àmbit empresarial que s'observa en la majoria de solucions existents estudiades, fet que provoca que no s'adaptin de manera directe o amb facilitat a les necessitats específiques d'entorns educatius.

A través del desenvolupament de la solució, s'aprecia i demostra la necessària transversalitat de la mateixa, per poder oferir una solució eficient cal tractar el problema de manera global des de diferents vessants, cal destacar també l'especial importància de la interacció entre aquestes. Tant en el cor de la classificació de l'assignació de l'ample de banda com en la comunicació entre processos implicats pren una especial rellevància el marcatge de paquets. Un clar exemple seria la comunicació entre el Proxy (Squid) i el balancejador de càrrega de paquets (IPRoute/TC) en els casos d'encert de caché “Hit” mitjançant el marcatge de paquets[test6].

Com a conclusió, al llarg del treball realitzat, es pot apreciar que l'aplicació del sistema de gestió d'ample de banda proposat permet millorar la gestió de l'accés a Internet dels centres educatius, usual coll d'ampolla i origen de la majoria de problemes de connectivitat, garantint l'assignació dels recursos especificats per aula independentment de la complexitat o càrrega de la resta de la xarxa, i permetent aplicar de manera senzilla patrons de funcionament en base a casos reals, factor que en facilita les tasques de gestió, comprensió i seguiment de l'estat global del sistema.

Donada la seva coincidència de la gestió amb conceptes i situacions reals, es preveu que pot ser fàcil una configuració d'eines accessibles al professorat per tal de poder permetre'ls disposar de les accions de configuració bàsica de les aules en base a un possible conjunt d'estats predefinits que implementin els escenaris descrits.

Com treball futur seria convenient l'aplicació en real de la totalitat del sistema per a poder-ne valorar el global de possibilitats, efectuant tests amb altres disciplines de cua amb més possibilitats (gestió de retards...) i afegint balanceig de càrrega d'accessos a Internet. També seria interessant disposar d'un entorn preferiblement web accessible al

professorat (prèvia validació) que permetes rebre informació gràfica i actual de l'estat del sistema, així com la possibilitat d'aplicació dels diferents patrons com restricció o priorització d'aules). La automatització dinàmica de patrons d'assignació de recursos en base a calendaris o observació de patrons repetitius de comportament del sistema també es podria contemplar.

Bibliografia

1. QUORUM: Prepaid Internet at the University of Zululand, Soren Aalto. : Linux Journal (issue 103)
2. A measurement-based approach for dynamic QoS adaptation in DiffServ networks, Toufik Ahmed, Raouf Boutaba, Ahmed Mehaoua. : Computer Communications 28 2020–2033 (2005)
3. Linux Traffic Control - Next Generation, Werner Almesberger. : Linux-Kongress 2002 / Sourceforge.net
4. Kernel Korner - Analysis of the HTB Queuing Discipline, Yaron Benita : Linux Journal (issue 131)
5. Guide to IP Layer Network Administration with Linux – Ver. 0.4.4, Martin A. Brown. :Http://www.linux-ip.net
6. Traffic Control HOWTO - Rev 1.0.2, Martin A. Brown. : Http://www.inux-ip.net
7. Control de ancho de banda,Arturo A. Busleiman. : GNU/Linux Users 2.1
8. Proxy Transparente con Squid y Netfilter,Arturo A. Busleiman. : SoloLinuxGNU / Linux Users 2.2
9. Using Dynamic Delay Pools for Bandwidth Management, Gihan Dias, Chamara Gunaratne : http://2002.iwcw.org/papers/18500234.pdf (2002)
10. Linux Advanced Routing & Traffic Control – V1.0.0, Bert Hubert, Thomas Graf, Gregory Maxwell, Remco van Mook, Martijn van Oosterhout, Paul B Schroeder, Jasper Spaans, Pedro Larroy : http://lartc.org/
11. Nonintrusive TCP Connection Admission Control for Bandwidth Management of an Internet Access Link, Anurag Kumar, Malati Hegde, S.V.R. Anand, B.N. Bindu, Dinesh Thirumurthy and Arzad A. Kherani. : IEEE Communications Magazine Volume 38 (p 160-167)
12. Policy Routing for Fun and Profit,David Mandelstam, Nenad Corbic. : Linux Journal (issue 121)
13. A Distributed Simulator for Network Resource Management Investigation, Josep Marzo Pere , Josep L. Marzo , Pere Vilà , Lluís Fàbrega , Daniel Massague. : Computer Communications Journal Elsevier (Volume 26, pag. 1782--1791)
14. Comparative Analysis of Active Bandwidth Estimation Tools, Federico Montesino-Pouzols. : Passive and active network measurement: 5th international workshop, PAM (2004)

15. A Bandwidth Management and Pricing Proxy, Austin Poulton, Peter Clayton and F F Jacot-Guillarmod. : http://www.cs.ru.ac.za/research/austin/publications/satnac2000.pdf
16. Bandwidth Estimation: Metrics, Measurement Techniques, and Tools ,R. S. Prasad , M. Murray , C. Dovrolis , K. Claffy , Ravi Prasad , Constantinos Dovrolis Georgia. : IEEE Network Volume 17 Issue 6
17. Gestió de xarxes Internet basada en SNMP ,Rodriguez Rodríguez, Pere; March Hermo, Maribel : http://openaccess.uoc.edu
18. Implementing bandwidth management in a low-bandwidth environment, Wambua, Joseph Kimaili. : Uganda Scholarly Digital Library – Makerere University – Theses & Dissertations (CIT)
19. Cisco Bandwidth Control for Education Networks, Cisco Systems. : www.cisco.com
20. E-SONDE Internet Tutor, E-sonde network monitoring : www.e-sonde.com
21. Router/Bridge Linux Firewall, Zero shell Net Services – Fulvio Ricciardi. : www.zeroshell.net
22. How To Accelerate Your Internet, Flickenger R., Belcher M., Canessa E., Zennaro M. http://bwmo.net (INASP/ICTP) ISBN: 0-9778093-1-5
23. Linux Firewalls and QoSDesigning and Implementing Linux Firewalls and QoS using netfilter, iproute2, NAT and l7-filter, Lucian Gheorghe. : Packt publishing - ISBN : 1904811655
24. Squid: The Definitive Guide, Duane Wessels , O'Reilly Media - ISBN: 9780596001629”
25. Building Internet Firewalls, Elizabeth D. Zwicky, Brent Chapman , O'Relly - ISBN: 1-56592-871-7
26. SAU virtual del Projecte 1x1, Generalitat de Catalunya. : http://imae.wikispaces.com
27. Innovació educativa – EduCAT 1x1, Generalitat de Catalunya. : www.gencat.cat
28. P1x1-Eq-Proxy Equipament de funcionalitat Proxy-cache, Generalitat de Catalunya. : http://imae.wikispaces.com
29. Projecte eduCAT1x1, Xtec. : www.xtec.cat
30. Iproute2, Stephen Hemminger, Alexey Kuznetsov. : http://www.linuxfoundation.org