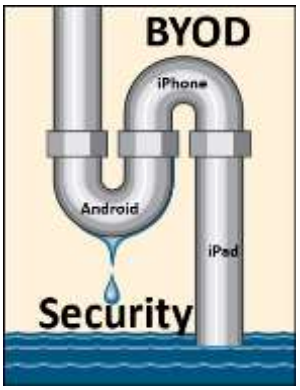
White Paper

Nell'ambito di un recente studio in cui si è monitorata la larghezza di banda, impiegata da un dipendente che utilizzava due dispositivi iOS (iPhone e iPad), è stato rilevato che, entro un arco di appena due settimane, l'impatto sulla rete aziendale era oltre 53 GB. Dal 2009 l'adozione dei dispositivi **BYOD** "**BringYour Own Device**" è aumentata di 15 volte, con 1,02 miliardi di dispositivi previsti entro la fine dell'anno. Secondo il recente studio "**Global Mobility Study**", condotto da IDG Research Services, il 71% dei dipendenti dichiara di accedere alla rete aziendale utilizzando il proprio smartphone personale. In un mese, il peso di questi dispositivi sulla larghezza di banda aziendale può variare da 4 a oltre 200 GB. Dal 2009 ad oggi sono stati venduti oltre un miliardo di smartphone e tablet Apple iOS e Google Android. Questi dispositivi consumano una notevole quantità di banda, gravano sulla struttura aziendale e sottraggono risorse a tutte le altre applicazioni presenti sulla rete. Gli IT Manager non possono nulla contro la necessità/voglia di connessione che sembra aver pervaso ogni utenza ed ogni persona che per il 90% delle volte utilizza le risorse aziendali per soddisfare quella che è diventata una vera e propria smania.

Per rispondere a questa smisurata richiesta di connettività la maggior parte degli amministratori di rete hanno aumentato a dismisura la capacità dei loro Link ad internet senza però riuscire a colmare la richiesta. Per assurdo si è riscontrato che più venivano aumentate le risorse trasmissive e più calava il livello del servizio. I dati del traffico relativi alle reti mobili e alle connessioni domestiche a banda larga, nonché gli aggiornamenti di software e applicazioni, che richiedono una connessione Wi-Fi, indicano in modo incontrovertibile che tale attività grava in modo sproporzionato sulla rete delle aziende. Al tempo stesso, le imprese non dispongono di strumenti in grado di visualizzare o monitorare l'attività di questi dispositivi che rappresentano molto spesso enormi falle di sicurezza. **Ma come mai? Cosa accade?**

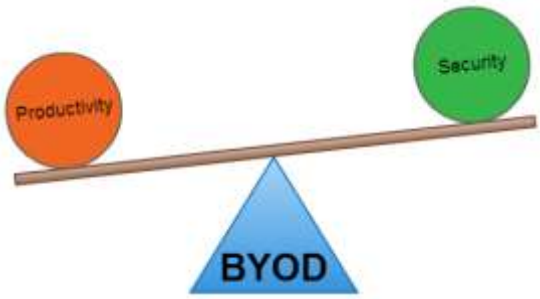


Proviamo a verificarlo insieme.

E' ormai noto che gli utenti hanno una vera e propria rete privata costituita dai loro referenti (conoscenti, amici, parenti) e uno storage personale spesso posto in Cloud al quale si connettono tramite la rete aziendale. Questa frenesia comporta il collasso dell'infrastruttura informatica. Fra le attività degli smartphone e più in particolare dei device mobili che comportano l'uso e l'abuso di banda sono incluse:

- **Aggiornamenti del sistema operativo:** gli utenti richiedono che i dispositivi vengano connessi a un computer o a una rete Wi-Fi, affinché sia possibile eseguire il download di sistemi operativi che raggiungono migliaia di megabyte. Di conseguenza, un singolo device mobile può sovraccaricare, senza difficoltà, la banda aziendale con un solo clic, a discapito delle reti e delle applicazioni business.

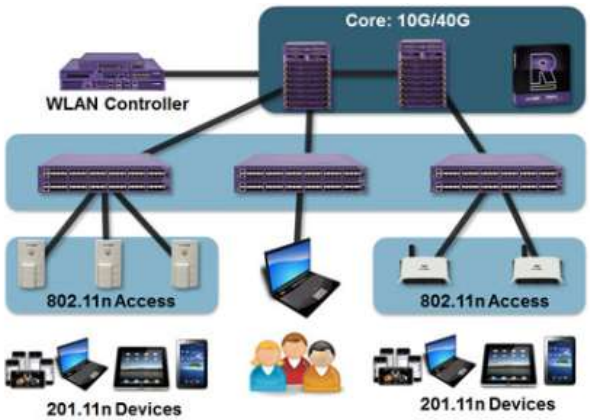
- **Download di applicazioni:** un utente scarica in media più di 40 applicazioni, accedendo ad iTunes di Apple e Google Play, dove sono facilmente accessibili circa 1,2 milioni di app. Le loro dimensioni possono variare da una quantità minima a migliaia di megabyte. Inoltre, i loro aggiornamenti sono file di immagine, pertanto, l'impatto sull'ampiezza di banda equivale più o meno al primo download dell'applicazione stessa con ogni nuovo aggiornamento.



- **Caricamento di foto e video:** le fotocamere integrate negli smartphone sono capaci di acquisire immagini, la maggior parte delle quali ad alta risoluzione. Chiunque può scattare foto (da 1 a 3 MB) o girare video (25 - 230 MB al minuto) e caricarli rapidamente su piattaforme come iCloud o Flickr per condividerli con i propri colleghi, amici o familiari. Allo stesso modo tali foto e video possono essere scaricati senza difficoltà dai colleghi, raddoppiandone l'impatto sulla rete.
- **Download di video e risorse multimediali:** grazie a contenuti video resi immediatamente disponibili per il download attraverso iTunes, Amazon e siti simili, gli utenti possono consumare la banda aziendale come mai era successo prima. I video in HD impiegano mediamente 3 GB o più e una stagione completa di una serie TV richiede dimensioni persino maggiori. Inoltre, i dispositivi mobili forniscono agli utenti l'accesso diretto alle raccolte, sempre più diffuse, di contenuti video su Internet. Mediamente, un video su YouTube richiede 500 Kbps per essere scaricato, pertanto, un singolo utente in un ufficio remoto con una connessione T1 consumerà il 33% della larghezza di banda per tutta la durata del video.

- **Backup nella risorsa di archiviazione del cloud:** iCloud offre agli utenti 5 GB di spazio di archiviazione gratuita nel cloud per la sincronizzazione di contenuti come foto, e-mail, musica, video e applicazioni con tutti i dispositivi connessi. I backup incrementali vengono eseguiti quotidianamente e variano da pochi kilobyte fino a raggiungere i 20 megabyte, a seconda della quantità di nuovi dati da sincronizzare. Ad esempio, i calendari e i segnalibri Web sono di piccole dimensioni, mentre le e-mail, le foto e i video richiedono una disponibilità di banda maggiore.

C'è poi un malcostume sempre più diffuso che vede i dispositivi mobili essere utilizzati sul posto di lavoro per attività ricreative esattamente come i laptop o i computer aziendali. Questo fraudolento utilizzo aumenta la congestione della rete. Tuttavia, poiché questi devices non sono registrati né rilasciati dall'azienda, molti dipartimenti IT non hanno chiaro il numero dei dispositivi connessi alla rete, quali applicazioni utilizzino o quanta ampiezza di banda consumino. E ancora più importante, non dispongono di mezzi per controllarne l'impatto. In assenza di strumenti di gestione del traffico efficaci, le divisioni IT sono impotenti di fronte all'avvento del fenomeno **BYOD**.



Vitalize your IT

Per contenere l'impatto che tale tendenza ha sulla rete, è necessario che le aziende dispongano di:

- **Visibilità:** il monitoraggio in tempo reale, di tutte le applicazioni e dei contenuti Web sulla rete aziendale, offre la visibilità del traffico generato dal **BYOD** su milioni di siti di contenuti multimediali e migliaia di applicazioni.
- **Controllo:** le policy **QoS** permettono agli amministratori di rete di limitare il downstream **BYOD** e il traffico di upstream in porzioni gestibili della capacità di rete, abilitando i burst laddove le applicazioni aziendali, con priorità maggiore, non richiedano l'ampiezza di banda.
- **Ottimizzazione/Accelerazione:** l'ottimizzazione dei protocolli, combinata "all'object caching" del sistema operativo o ai download delle applicazioni o dei contenuti multimediali on-demand, permette di ridurre l'impatto dei **BYOD** mediante l'abilitazione di iniziative video aziendali, quali corsi di formazione, comunicazioni e accesso ai documenti.

Cyberoam offre alle aziende la visibilità e il controllo del traffico dei dispositivi mobili sulla rete, il controllo dell'utilizzo di applicazioni in grado di consumare in modo eccessivo la larghezza di banda e influire negativamente sulle prestazioni delle applicazioni critiche. Questi device si integrano con sistemi già presenti o possono andare a sostituire i firewall esistenti, consentendo alle aziende di visualizzare e controllare il traffico degli aggiornamenti software Apple, iTunes, del browser Safari, DropBox, iOS e quant' altro. Grazie a queste soluzioni le aziende possono ridurre il peso che le iniziative **BYOD** creano sulla banda aziendale.

Non aggiungete **banda**. **GESTITELA**.

La Bandwidth Management **Cyberoam**, basata sull'identità dell'utente "Layer 8", garantisce la disponibilità di banda alle applicazioni negli ambienti cloud e SaaS permettendo di limitare l'abuso di banda durante le fasi P2P o in altre situazioni non legate al business.

Alcuni vantaggi

Visibilità in tempo reale dell'utilizzo della banda e degli utenti che la usano, applicazioni e protocolli: il modulo Traffic Discovery di **Cyberoam** consente di osservare in tempo reale il traffico sulla rete differenziandolo per applicazioni e utenti utilizzando filtri e S/W che lavorano dal Layer 2 "data link" al livello 8 "livello utente". Questa attività realizza un report molto dettagliato sul reale stato d'uso della rete nel suo insieme. Si ottengono così allarmi in tempo reale per l'utilizzo non produttivo o pericoloso delle risorse, consentendo a coloro che ne hanno diritto la navigazione e scoraggiando o bloccando tutto il resto.

Controllo dell'utilizzo della banda da parte di applicazioni e siti: è possibile stabilire limiti di banda individuali o per gruppi riferiti ad applicazioni, gruppi di utenti e siti web, migliorando così la sicurezza e la produttività. Alcuni esempi sono:

- banda dedicata al VoIP;

Vitalize your IT

- allocazione limitata ai siti contenenti video, musica e immagini non d'interesse per il business;
- impostazione ad un livello basso (64 kbps) per il trasferimento dei file nelle applicazioni di messaggistica istantanea;
- riduzione a zero per il P2P;
- limitazione dell'accesso a specifiche applicazioni secondo orari e tempi predefiniti. Un esempio in questo senso può essere l'abilitazione di YouTube e Gmail tra le 17:00 e le 18:00.

Controllo dell'utilizzo della banda in funzione dell'utente "layer8:

- assegnare quote di banda, restringendo la velocità di upload e download a seconda dell'utente connesso;
- gestire la banda dedicata all'utente: ad esempio, la banda dedicata al CEO diversa dagli operatori o dal reparto Marketing,
- consentire l'accesso a Youtube solo dopo l'orario d'ufficio e l'accesso a Gmail solo in caso di disponibilità di banda in eccesso.

Web Filtering

HTTP e HTTPS: controllo e visibilità completi.
Il premiato web filtering di **Cyberoam** offre uno dei più completi database di URL, con milioni di voci raggruppate in più di 82 categorie. Distribuito unitamente alle appliance UTM e Wi-Fi di **Cyberoam**, blocca l'accesso a siti pericolosi, prevenendo attacchi dovuti a malware, phishing, pharming e contenuti indesiderati che potrebbero generare responsabilità legali e perdite finanziarie dirette.
Le policy basate sull'identità dell'utente "Layer 8" di **Cyberoam** assicurano controlli di accesso granulari al web, impedendo la perdita di dati e produttività. Un'ampia copertura del web e i controlli granulari fanno del web filtering di **Cyberoam** la scelta giusta tanto per le grandi che per le piccole imprese.

Caratteristica	Descrizione	Benefici
Categorizzazione del web	Database installato nell'appliance Più di 82 categorie web Categorie personalizzate Aggiornamenti automatici mediante WebCat, il motore di categorizzazione dei siti web	Riduzione del tempo di risposta e limitazione delle questioni relative alla privacy Web filtering completo e specifico per l'azienda
Opzioni per il Web Filtering:	URL Parole chiave Tipo di file Database	Web filtering omnicomprensivo
Sicurezza Wi-Fi	Blocco dei proxy e dei software per il tunnelling di terze parti Blocco delle pagine cache di Google Blocco delle URL embedded nei siti web Uso delle 'safe search' nei motori di ricerca Blocco delle URL che contengono malware, phishing e pharming Blocco di applet Java, cookie, e ActiveX	Integrazione con i moduli antivirus e antispyware e IPS per una sicurezza del web e dei contenuti completa. Minimizzazione dei bypass accidentali o intenzionali mediante eliminazione dei siti dannosi dai risultati delle ricerche
Controlli HTTPS	Possibilità di osservare il traffico HTTPS criptato Blocco di upload e download non autorizzati su HTTP e HTTPS Blocco dei siti HTTPS non autorizzati, maligni e illegali	Prevenzione del data leakage Prevenzione dell'uso scorretto del mezzo codificato per effettuare attacchi mediante malware e trasferimenti non autorizzati dei dati Controllo della responsabilità legale
Conformità alle norme in vigore	Implementazione della *Internet Safety Policy* Membro attivo della Internet Watch Foundation (IWF) nel Regno Unito Prevenzione del data leakage	Conformità CIPA e supporto ai finanziamenti E-Rate HIPAA PCI DSS

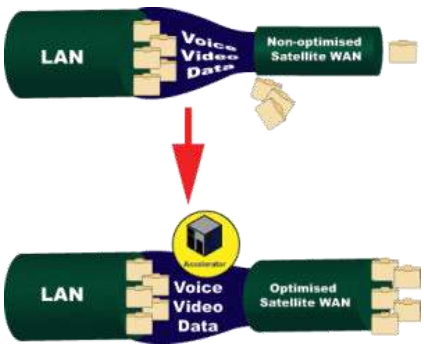
Policy basate sull'identità presso il Layer 8	Policy basate su nome utente, gruppo, esigenze di lavoro Controllo degli accessi in base a pianificazioni temporali Autenticazione degli utenti mediante ADS, RADIUS, SSO, local e thin client	Sicurezza e flessibilità elevate Protezione dalle perdite di produttività Integrazione con un insieme di meccanismi di autenticazione esistenti
Sostituisce quanto di meglio c'è sul mercato	Abbonamenti 'singoli' o 'per appliance', a differenza di quelli 'per utente' Messaggi personalizzati per gli utenti con motivazione per il blocco del sito web Allocazione della banda in base a categoria e priorità Quote di dati e banda a seconda delle categorie web e dell'orario	La giusta soluzione per rimpiazzare le migliori soluzioni sul mercato e raggiungere un livello di sicurezza completo e comunque dall'ottimo rapporto tra costo ed efficacia Educazione degli utenti all'impiego delle migliori prassi nell'uso del web Assegnazione garantita di banda alle applicazioni fondamentali per il business Protezione dalle perdite di produttività

Bandwidth Management

Migliora la **performance** della rete e la **produttività**

La Bandwidth Management di **Cyberoam** permette di controllare la banda partendo dal "Layer 8" e cioè dall'identità dell'utente, in modo da prevenire la congestione e l'abuso della banda stessa e di garantire l'ottimizzazione della stessa al fine di un maggior ritorno degli investimenti effettuati dall'azienda.

La soluzione concede maggiore priorità alle applicazioni e agli utenti fondamentali per il business mediante controlli granulari, supportando le installazioni del Cloud e dei SaaS e riducendo le spese relative all'acquisto della banda.



Caratteristiche	Descrizione	Benefici
Allocazione della banda Layer 7 e 8	⇢ Allocazione della banda secondo priorità fissate per le applicazioni e gli utenti fondamentali per il business ⇢ Priorità basate su provenienza, destinazione, utente, servizio, gruppo di servizi	⇢ QoS garantita per le applicazioni fondamentali per il business come VoIP e CRM ⇢ Supporto alle necessità di banda per il Cloud e le applicazioni SaaS ⇢ Prevenzione della congestione e dell'abuso della banda
Allocazione secondo la categoria web	⇢ Allocazione della banda secondo le categorie dei siti web: webmail, social media, ludici, di intrattenimento, ecc. ⇢ Limiti di upload e download ⇢ Policy sul Layer 8 basate sull'identità, con allocazione a seconda della categoria	⇢ Maggior produttività grazie al web filtering
Allocazione in base al tempo	⇢ Allocazione pianificata della banda in base all'orario ⇢ Banda dedicata alle applicazioni fondamentali per il business durante i periodi pianificati	⇢ Bilanciamento dei massimi e minimi di banda ⇢ QoS garantita per le applicazioni fondamentali per il business
Banda dedicata e dedicabile	⇢ Banda dedicata costante agli utenti fondamentali ⇢ Policy per l'assegnazione automatica di banda disponibile ad altre applicazioni	⇢ Uso ottimale della banda disponibile ⇢ Limitazione delle spese per l'acquisto di banda ⇢ Ritorno sugli investimenti assicurato

Logging e reportistica	Rapporti sulla banda delle diverse connessioni alla WAN	Utilizzo ottimale e verificabile della banda
	Scelta tra reportistica installata nell'appliance o centralizzata mediante Central Console e iView Cyberoam	Identificazione degli attacchi alla rete mediante rilevamento di consumi eccessivi di banda
		Supporto al rispetto delle norme in vigore

Il mercato non ha ancora favorito la nascita di servizi **QoS end-to-end**, ovvero in grado di garantire vincoli sulla **QoS** di un flusso di dati scambiati tra utenti remoti. Alcuni credono che una rete "stupida" cioè sovradimensionata, che offra cioè sufficiente banda per la maggior parte delle applicazioni e per la maggior parte del tempo, sia già economicamente la migliore soluzione possibile, mostrando poco interesse a supportare applicazioni non-standard capaci di **QoS**. La rete Internet ha già accordi complessi tra i provider e sembra che ci sia poco entusiasmo nel supportare il **QoS** attraverso connessioni che interessano reti appartenenti a provider diversi, o sugli accordi circa le politiche che dovrebbero essere sostenute al fine di poterle supportare.

Ma proviamo a capire cos'è il **QOS.**

Applicazioni che richiedono QoS

Il modello di **QoS** originale di Internet, ovvero **nessuna QoS**, è adatto ad applicazioni elastiche, che possono funzionare anche su reti con prestazioni molto degradate, e viceversa usare tutta la banda a disposizione se questa è abbondante. Altri tipi di servizio sono invece chiamati inelastici, ovvero richiedono un certo livello di banda per funzionare. Se ne ottengono di più non la sfruttano e se ne ottengono di meno non funzionano affatto. Sono proprio queste applicazioni che rendono necessaria l'adozione di misure per garantire una certa QoS**.**

Applicazioni che richiedono una QoS **sono ad esempio le seguenti:**

- multimedia streaming: può richiedere un throughput garantito;
- telefonia VoIP può richiedere vincoli molto stretti sul ritardo e sulla variabilità del ritardo (jitter);
- emulazione di collegamenti dedicati richiede sia un throughput garantito che un ritardo massimo limitato;
- un'applicazione critica per la sicurezza, come la chirurgia remota, può richiedere un

livello garantito di disponibilità, ciò è chiamato anche "hard **QoS**".

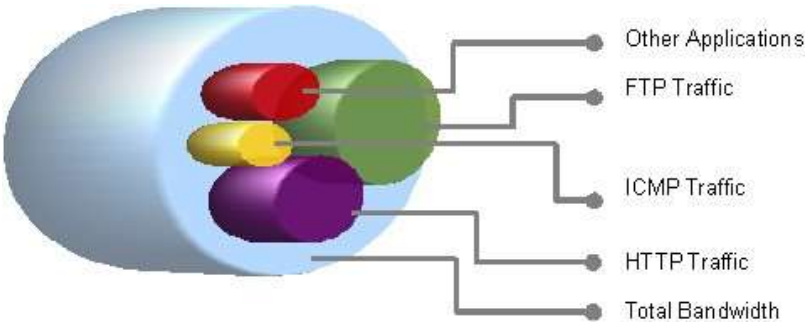
In contesti lavorativi, può accadere che vengano definiti dei requisiti di **QoS** anche per applicazioni che non sono intrinsecamente elastiche, per garantire livelli adeguati di produttività. Ad esempio, "il terminale dell'agenzia di viaggi deve riuscire a completare la transazione entro 10 s nel 98% dei casi". Spesso però un requisito di questo tipo richiede di intervenire sia sulla rete che sul sistema informativo che eroga il servizio (ad esempio, allestire un numero adeguato di server).

Meccanismi di QoS in Internet

Quando è stata creata Internet, non era stata percepita la necessità di **QoS** per le applicazioni. Infatti l'intera Internet segue la filosofia del "best effort", cioè il sistema garantisce di fare tutto il possibile per portare a termine un'operazione, ma non garantisce affatto che l'operazione verrà compiuta, né in che modo. Anche se il protocollo IP prevede 4 bit per il tipo di servizio "type of service" e 3 per la precedenza di ciascun pacchetto, questi bit sono largamente inutilizzati. Al crescere del numero e tipologie di servizi e del traffico offerto rispetto alle capacità della rete il problema della qualità del servizio ha cominciato a divenire importante e sempre più considerato.

Ci sono fondamentalmente due modi per fornire garanzie sulla qualità del servizio.

- **Overprovisioning.** Il primo metodo, detto overprovisioning "sovradimensionamento", consiste nel fornire risorse di rete, di trasmissione, memorizzazione ed elaborazione in abbondanza, abbastanza da soddisfare la domanda di picco attesa, con un sostanziale margine di sicurezza. Una soluzione semplice, ma alcuni credono che in pratica sia troppo costosa e non sia applicabile se la domanda di picco cresce più velocemente di quando predetto: disporre nuove risorse richiede infatti sempre tempo.
- **Priorità.** L'alternativa è amministrare la banda disponibile, facendo in modo che i pacchetti che giungono ad un nodo di rete "router" subiscano un trattamento differenziato ovvero quelli a cui deve essere garantita una certa **QoS** ricevano in particolar modo un trattamento privilegiato. Per ottenere questo, bisogna risolvere due problemi:



- **Identificare i pacchetti che devono ricevere un trattamento privilegiato (**classificazione o discriminazione del traffico**).**
- **Applicare a questi pacchetti identificati una disciplina di coda "**queue discipline**"**

che garantisca le prestazioni necessarie da applicare poi sulle porte o interfacce di uscita dei router.

Classificazione

I metodi strutturati per identificare il traffico da privilegiare sono:

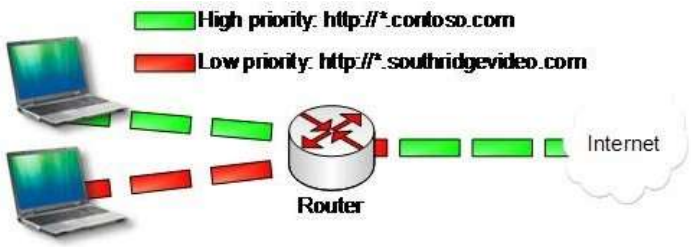
- **Integrated services**, basato sulle prenotazioni: prima di iniziare una sessione che ha dei requisiti di **QoS**, l'applicazione deve "chiedere" alla rete se questa può garantire le prestazioni necessarie "admission control": la rete valuta se dispone delle risorse adeguate e in caso positivo accetta la prenotazione concedendo il servizio richiesto.

- **Differentiated services**, prevede che gli utenti della rete stipulino a priori un contratto che definisca la quantità massima di traffico "privilegiato" che essi possono generare e marchino tale traffico utilizzando il campo Type of Service "TOS" dell'header IP. In questo caso quindi le prenotazioni sono rigidamente "statiche".

Soprattutto nelle reti di piccole dimensioni, è possibile utilizzare metodi più semplici, che prevedono di identificare manualmente sui router il traffico a cui dare priorità, tipicamente usando delle liste di controllo degli accessi (ACL).

Discipline di coda

In un router che non applichi politiche di qualità del servizio, i pacchetti vengono trasmessi sulle porte in uscita nell'ordine in cui sono arrivati. Una disciplina di coda, o scheduling dei pacchetti, consiste essenzialmente nel gestire per ciascuna porta diverse code in uscita, in cui i pacchetti vengono classificati. La disciplina di coda stabilisce in quale ordine verranno prelevati i pacchetti dalle varie code.



Esempi di disciplina di coda:

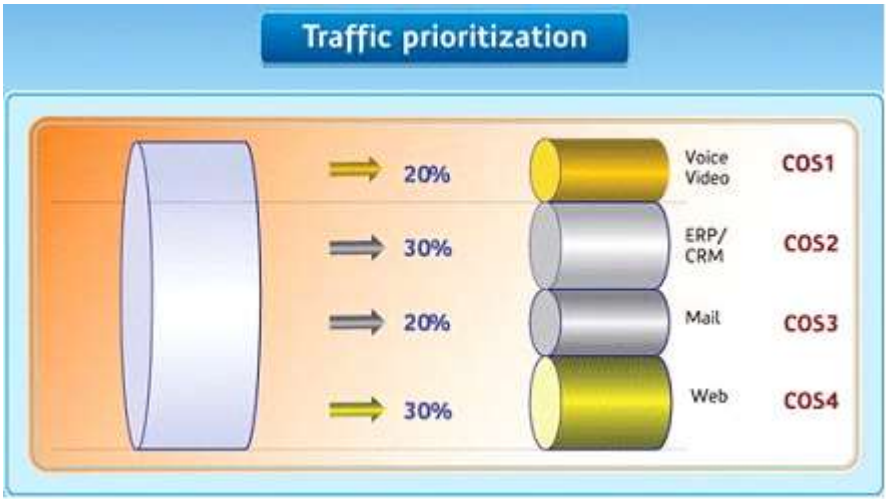
- **Priorità stretta**: le code sono ordinate per priorità. Ogni volta che si deve trasmettere un pacchetto, si preleva dalla coda quello a priorità più alta e lo si spedisce. In questo modo, un'applicazione di priorità superiore alle altre può monopolizzare l'intera banda disponibile, a danno di quelle a priorità inferiore (**starving**).
- **Weighted round robin**: viene prelevato a turno un pacchetto da ciascuna coda. In questo modo si garantisce che tutte le classi di applicazioni potranno trasmettere. Il "weighted" significa che a ciascuna coda può essere attribuito un peso, ovvero una frazione della banda disponibile, e i pacchetti vengono prelevati in modo da garantire questa banda disponibile. Se una classe di traffico in un certo momento non utilizza la banda allocata, questa è utilizzabile dalle altre "bandwidth borrowing".
- Discipline di coda più avanzate, come **Hierarchical Packet Fair Queueing (H-PFQ)** e **Hierarchical Fair Service Curve (H-FSC)**, permettono di esprimere per ciascuna coda sia un requisito sulla banda che uno sul ritardo. Al momento, sono disponibili solo su router software, basati su BSD o linux.

Altri strumenti utilizzati per amministrare la banda disponibile:

- **RED** "Random Early Detection o Rilevazione casuale anticipata": quando si approssima la congestione, la rete scarta arbitrariamente una piccola percentuale del traffico. Questo viene interpretato da TCP come un'indicazione di congestione, abbassando la quantità di traffico inviata. Un caso particolare di questa tecnica chiamato WRED "Weighted Random Early Detection" permette di distinguere il flusso di traffico dal quale iniziare a scartare i pacchetti in presenza di congestione. Con il **WRED** è possibile definire delle soglie di utilizzo del link che, una volta raggiunte, provocano lo scarto di pacchetti appartenenti a specifiche classi di traffico. Così al raggiungimento della prima soglia verranno scartati solo pacchetti di flussi poco importanti, mentre al raggiungimento di soglie di utilizzo via via più alte verranno scartati anche pacchetti appartenenti a flussi di traffico più importanti. Il "weighted" significa che la classe di traffico che sperimenterà il maggior numero di pacchetti droppati sarà quella associata alla soglia più bassa. La definizione delle soglie di utilizzo e dei diversi flussi di traffico è fatta su base configurazione.
- **Rate limiting**: una classe di traffico può essere limitata in modo che non utilizzi più di una certa banda.

Nozione di qualità di servizio

Il termine **QoS,** acronimo di "Quality of Service", in italiano **<Qualità di Servizio>,** applicata alle reti a commutazione di pacchetti, reti basate sull'utilizzazione di router, la **QoS** designa l'attitudine di garantire un livello accettabile di perdita di pacchetti, definiti contrattualmente, per un dato uso (VOIP, videoconferenza, ecc).



In effetti, contrariamente alle reti a commutazione di circuiti, come le reti telefoniche commutate, dove un circuito di comunicazione è dedicato durante tutta la durata della comunicazione, è impossibile predire su internet il percorso effettuato dai differenti pacchetti. Così, non c'è nessuna garanzia che una comunicazione richiedente una banda regolare abbia luogo senza problemi. Ed ecco perché esistono dei meccanismi, detti di **QoS**, che permettono di differenziare i diversi flussi di rete e riservare una parte della banda per quelli che richiedono un servizio continuo, senza interruzioni.

Livello di servizio

Il termine «**Livello di servizio**» in inglese "Service level" definisce il livello di esigenza per la capacità di una rete di fornire un servizio point to point con un dato traffico. Si definiscono generalmente tre livelli di **QoS** :

- **Al meglio delle possibilità** in inglese "best effort", che non fornisce nessuna differenza tra i diversi flussi di rete e non da nessuna garanzia del livello di servizio. Questo livello di servizio è anche detto **lack of QoS**.

- **Servizio differenziato** in inglese "differenciated service" o **soft QoS**, che permette di definire dei livelli di priorità ai diversi flussi di rete senza tuttavia una garanzia effettiva.
- **Servizio garantito** in inglese "guaranteed service" o **hard QoS**, che consiste nel riservare delle risorse di rete per alcuni tipi di flussi. Il meccanismo principale usato per ottenere un simile livello è l'**RSVP** "Resource reSerVation Protocol".

Criteri di qualità di servizio

I principali criteri che permettono di apprezzare la qualità del servizio sono i seguenti :

- **Larghezza di banda** in inglese "bandwidth", che definisce il volume massimo delle informazioni "bit" per unità di tempo.
- **Jitter** : rappresenta la fluttuazione del segnale digitale, nel tempo o in fase.
- **Latenza**, **periodo** o **tempo di risposta** in inglese "delay" che caratterizza il ritardo tra l'emissione e la ricezione di un pacchetto.
- **Perdita di pacchetto** in inglese "packet loss" che corrisponde alla non consegna di un pacchetto di dati. Per la maggior parte delle volte dovuta ad una saturazione di rete.

- **Disequenziamento** in inglese "desequencing". Si tratta di una modifica dell'ordine di spedizione e di conseguenza di arrivo dei pacchetti dati.

Come abbiamo visto, lo sviluppo della tecnologia, oltre a fornire alle aziende strumenti incredibili per l'incremento e la gestione del business, comporta anche dei rischi notevoli che, se sottovalutati o addirittura non considerati, possono dilatare i costi e contrarre le prestazioni.

Abbiamo visto che aumentare la disponibilità di banda per far fronte alla crescente domanda di connettività non è quasi mai la strada giusta, per cui, prima di mettere mano al portafoglio facendo solo la gioia dei provviders rileggete queste poche pagine e scoprirete che la soluzione si chiama **Gestione di Banda e Q.O.S.**

Cyberoam GOLD PARTNER

Il Tuo EterNet Team