

Implementazione delle soluzioni QoS per la videoconferenza H.323 su IP

ID documento: 21662

Aggiornato: 15 feb 2008



[Scarica PDF](#)

[Stampa](#)

[Feedback](#)

Prodotti correlati

- [Contrassegno pacchetti QoS](#)
- [H.323](#)

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Premesse](#)

[H.323](#)

[Caratterizzazione del traffico di videoconferenza](#)

[Pianificazione della capacità](#)

[Scenario di esempio](#)

[Determinazione del consumo di larghezza di banda per chiamata](#)

[Audio H.323](#)

[Video H.323](#)

[Classificazione](#)

[Selezionare un meccanismo di accodamento fantasia](#)

[Modello/schema di definizione delle priorità](#)

[La voce e il video devono condividere LLQ?](#)

[CAC](#)

[Traffic Shaping](#)

[Interoperabilità con i terminali H.323](#)

[Esempio di configurazione](#)

[Informazioni correlate](#)

[Discussioni correlate nella Cisco Support Community](#)

Introduzione

H.323 è lo standard riconosciuto a livello globale per le conferenze multimediali in una rete IP. In questo documento vengono illustrati gli strumenti per implementare la Quality of Service (QoS) per le videoconferenze H.323 su una WAN aziendale con collegamenti relativamente a bassa velocità.

Prerequisiti

Requisiti

Questo documento è utile per conoscere i seguenti argomenti:

- I componenti di un sistema conforme allo standard H.323. I componenti includono, tra l'altro, terminali, gateway, gatekeeper, controller multipoint (MC), processori multipoint (MP) e unità di controllo multipoint (MCU). Per ulteriori informazioni, fare riferimento al [white paper: distribuzione di applicazioni H.323 in reti Cisco](#) per ulteriori informazioni.
- Le soluzioni di videoconferenza Cisco H.323, che includono MCU e gateway, nonché il gatekeeper e il proxy Multimedia Conference Manager (MCM). Per i link a informazioni sulle soluzioni di videoconferenza Cisco, vedere la sezione "Informazioni correlate" di questo documento.
- H.323. Il gruppo di endpoint H.323 si verifica in zone, che sono vantaggi amministrativi simili a un DNS (Domain Name System). Ogni zona ha un gatekeeper che gestisce tutti gli endpoint.
- Piani di composizione. Fare riferimento al *Capitolo 5: Architettura del dial plan e configurazione* della [soluzione Cisco AVVID, telefonia IP: Cisco CallManager release 3.0\(5\)](#) per ulteriori informazioni.
- Tecniche di controllo di ammissione di chiamata (CAC), che includono la segnalazione dei requisiti delle risorse tramite il protocollo RSVP (Resource Reservation Protocol).

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento [Cisco sulle convenzioni nei suggerimenti tecnici](#).

Premesse

La maggior parte delle reti attualmente supporta uno o più dei seguenti tipi di traffico video:

Tipo di video	Caratteristiche del traffico
Videoconferenza	Larghezza di banda di piccoli gruppi bidirezionali: Uno o più flussi per utente
Video on demand	Larghezza di banda unidirezionale point-to-point (modello pull): Un flusso per

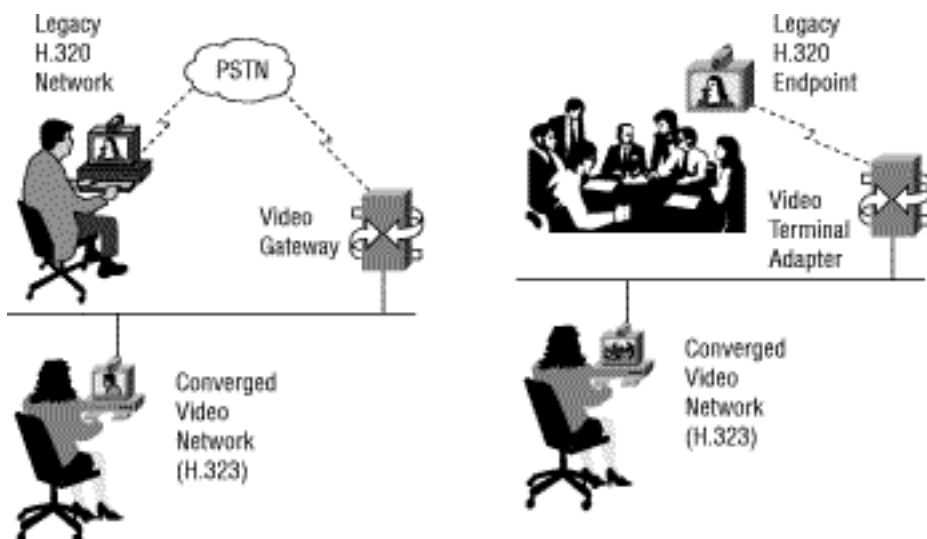
	utente
Trasmissione video (programmata)	Larghezza di banda unidirezionale, uno-a-molti (modello push): Un flusso per utenti illimitati (IP multicast)

Allo stesso tempo, molte aziende esaminano l'infrastruttura di rete dati, voce e video esistente e spesso separata per determinare il modo più efficiente per riunire queste reti in un'infrastruttura IP. In queste reti convergenti, la funzionalità QoS è obbligatoria in qualsiasi potenziale punto di congestione della rete. QoS garantisce che il traffico sensibile al ritardo e alla perdita di dati, il video in tempo reale e la voce passino senza ostacoli, in relazione alle applicazioni dati a tolleranza di caduta. In particolare, QoS è fondamentale sul router edge WAN. Qui, centinaia di megabit di traffico potenziale si aggregano in collegamenti a velocità più lenta nel raggio dei kilobit o dei megabit al secondo.

H.323

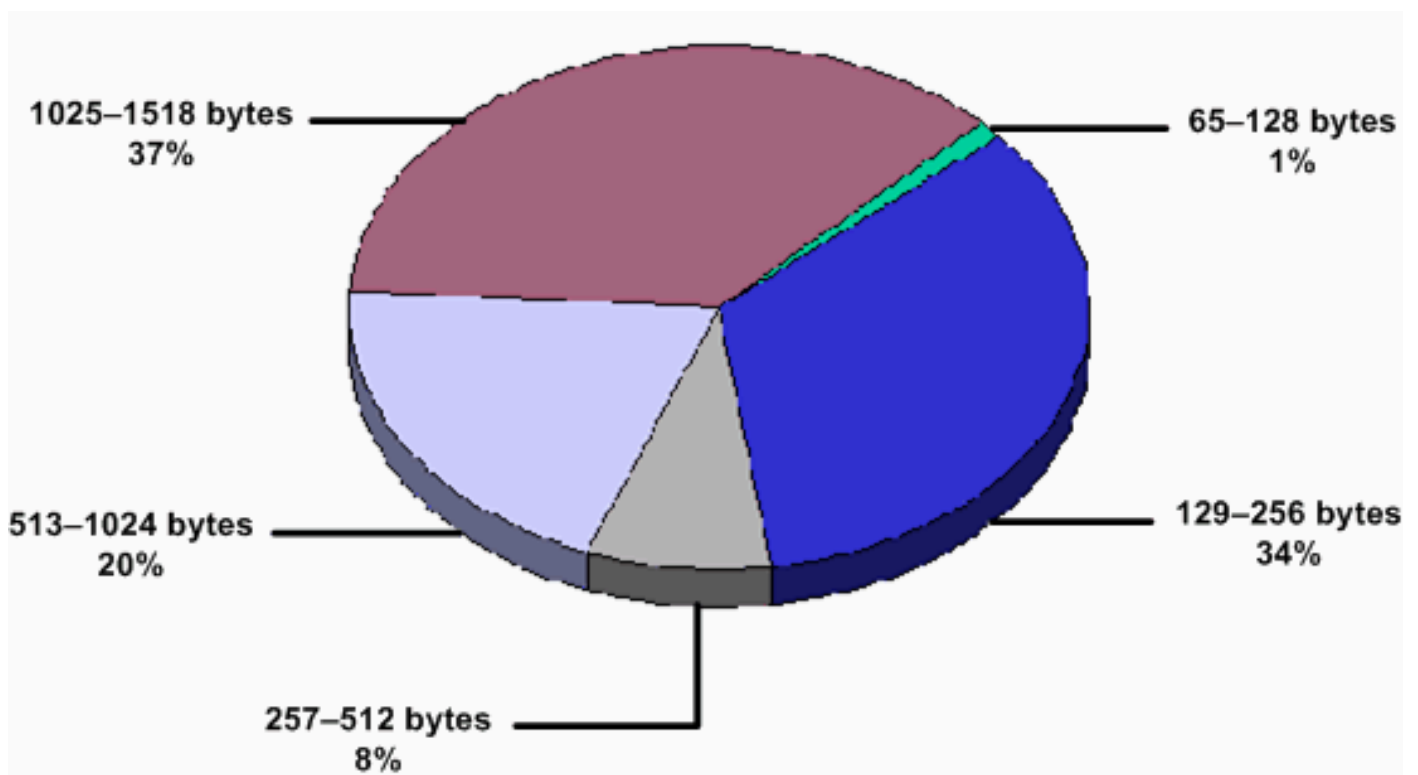
Molte applicazioni di videoconferenza IP utilizzano la suite di protocolli H.323. L'H.323 dell'Unione Internazionale delle Telecomunicazioni (ITU) definisce uno standard internazionale per i contenuti multimediali su reti IP. L'ITU ha approvato la prima versione dello standard H.323 nel 1996. La versione corrente è la 4. Molte applicazioni ora utilizzano comunemente sistemi video H.323 basati su LAN. Un'applicazione di esempio è Microsoft NetMeeting, che utilizza H.323 per la videoconferenza e la collaborazione condivisa.

In precedenza, i sistemi di videoconferenza basati sullo standard H.320 erano comuni. Ogni sistema disponeva di una connessione PSTN (Public Switched Telephone Network). Come mostra la parte sinistra della figura in questa sezione, oggi è possibile utilizzare gateway video per la comunicazione tra la rete convergente H.323 e la rete video legacy. Il lato destro della figura mostra come è possibile utilizzare adattatori terminali video per collegare facilmente singoli endpoint H.320 in una rete H.323.

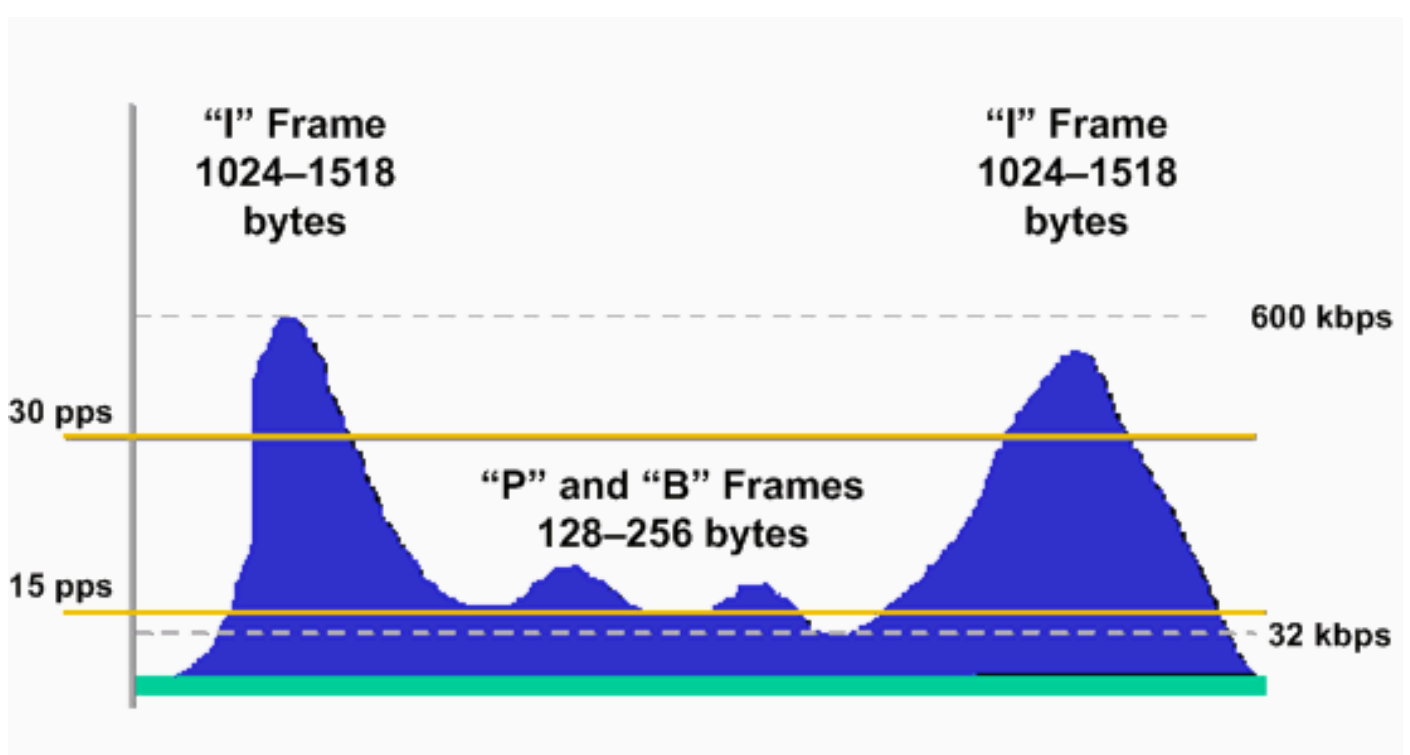


Caratterizzazione del traffico di videoconferenza

A differenza della voce, il video ha un packet rate molto elevato ed estremamente variabile con una media molto più elevata di unità di trasmissione massima (MTU). La figura mostra una tipica suddivisione del traffico delle videoconferenze per dimensioni dei pacchetti:



Un flusso di traffico di videoconferenza è costituito da due tipi di frame, come illustrato nella figura seguente:



Il fotogramma "I" è un campione completo del video. I frame "P" e "B" utilizzano la quantizzazione tramite vettori di movimento e algoritmi di previsione.

[Pianificazione della capacità](#)

Prima di inserire il traffico video su una rete, assicurarsi che esista una larghezza di banda adeguata per tutte le applicazioni necessarie. Calcolare innanzitutto i requisiti minimi di larghezza di banda per ogni applicazione principale, ad esempio voce, video e dati. La somma rappresenta il

requisito minimo di larghezza di banda per ogni collegamento specifico. Questa quantità non dovrebbe consumare più del 75% della larghezza di banda totale disponibile su quel collegamento. Questa regola del 75% presume che una certa larghezza di banda sia necessaria per il traffico di sovraccarico. Esempi di sovraccarico di traffico includono aggiornamenti del protocollo di routing e pacchetti keepalive di layer 2, nonché applicazioni aggiuntive, ad esempio la posta elettronica e il traffico HTTP. Il traffico voce e video non occupi più del 33% della capacità del collegamento. In questo [scenario di esempio](#) viene illustrata la pianificazione della capacità su una rete convergente.

Scenario di esempio

Un sito ha una capacità di collegamento di 1,544 Mbps e contiene due terminali video che supportano una velocità di trasferimento dati massima di 256 Kbps ciascuno. Sebbene la velocità delle due videochiamate sia pari a 512 kbps, aggiungere il 20% alla velocità dati della chiamata per tenere conto del sovraccarico. Il 20% è una percentuale conservativa che garantisce una corretta pianificazione della capacità nella maggior parte degli ambienti. È possibile iniziare con un ulteriore 20% per il sovraccarico e poi regolare questo valore, più alto o più basso, con i risultati del monitor come base.

Provisioning della coda di priorità per una larghezza di banda sufficiente a consentire a entrambi i terminali video di effettuare una chiamata attiva sulla WAN simultaneamente senza la possibilità di un sovraccarico della coda di priorità. In questo scenario di esempio, se si aggiunge un terzo terminale video, è necessario implementare una forma di CAC.

Determinazione del consumo di larghezza di banda per chiamata

Con la pianificazione della capacità, uno dei concetti più critici da comprendere è la quantità di larghezza di banda utilizzata per ogni chiamata. In questa sezione viene elencata la larghezza di banda utilizzata da ciascun codec (codec). Per ulteriori informazioni, fare riferimento a [Consumo della larghezza di banda per chiamata Voice over IP](#).

Audio H.323

I segnali audio contengono un suono digitalizzato e compresso (di solito parlato). H.323 supporta algoritmi comprovati audio codec standard ITU. Gli algoritmi supportati includono:

- G.711 - 3,1 kilohertz (kHz) a 48, 56 e 64 kbps (telefonia normale)
- G.722—7 kHz a 48, 56 e 64 kbps
- G.728—3,1 kHz a 16 kbps
- G.723—modalità 5.3 e 6.3 kbps

La scelta del codec appropriato riflette i compromessi tra qualità del parlato, velocità di trasmissione, potenza di elaborazione e ritardo del segnale.

Video H.323

In base allo standard H.323, le capacità video nei terminali H.323 sono opzionali. Tuttavia, quando si implementano i terminali H.323, questi devono supportare il codec H.261, con supporto opzionale per lo standard H.263.

- H.261—Codec video per servizi audiovisivi a multipli di 64 kbps. I dispositivi conformi allo standard H.261 codificano completamente i frame iniziali. I dispositivi codificano quindi solo le differenze tra il frame iniziale e quello successivo per la trasmissione di pacchetti minima. La compensazione opzionale del movimento migliora la qualità delle immagini.
- H.263—Codec video per POTS (Video Plain Old Telephone Service). Lo standard H.263 è un aggiornamento compatibile con lo standard H.261. H.263 migliora in modo significativo la qualità dell'immagine con una tecnica di stima del movimento di mezzo pixel, come è un requisito. I miglioramenti derivano anche da frame previsti e da una tabella di codici Huffman, con ottimizzazione per trasmissioni a bassa velocità di trasmissione. Lo standard H.263 definisce cinque formati di immagine standard, come mostra la Tabella 1 nel documento [White Paper: Implementazione delle applicazioni H.323 in reti Cisco](#).

Classificazione

Per fornire adeguate garanzie QoS al traffico video, i dispositivi di rete devono essere in grado di identificare tale traffico.

Il modello di QoS DiffServ (Differated Services, DiffServ) utilizza i valori DSCP (DiffServ code point) per separare il traffico in classi. DiffServ definisce i due insiemi di valori DSCP seguenti:

- Expedited Forwarding (EF) - Fornisce un unico valore DSCP (101110) che fornisce ai pacchetti contrassegnati il livello di servizio più alto dalla rete. Cisco implementa il servizio EF tramite LLQ (Low Latency Queueing). In genere, l'EF mantiene la coda ad alta priorità molto piccola per controllare il ritardo e prevenire la fame del traffico a bassa priorità. Di conseguenza, i pacchetti possono essere scartati, se la coda è piena. In genere, EF è più appropriato per il VoIP.
- Assured Forwarding (AF) - Fornisce quattro classi, ciascuna con tre livelli di precedenza al rilascio.

Per ulteriori informazioni su DSCP, vedere [Implementazione di criteri Quality of Service con DSCP](#).

In generale, le guide alla progettazione Cisco consigliano AF41 (valore DSCP 100010) per i video. Non c'è alcun vantaggio se si tratta la parte audio dei flussi video meglio dei pacchetti video in un'applicazione di videoconferenza IP. Pertanto, utilizzate AF41 come valore DSCP per i supporti voce e video in una videoconferenza.

Al layer 2, è possibile utilizzare i 3 bit CoS (Class of Service) nel campo IEEE 802.1p, che fa parte del tag IEEE 802.1Q.

Attualmente non esistono standard che descrivono quale valore sia più appropriato per una videoconferenza IP. Tuttavia, Cisco normalmente consiglia questo schema di contrassegno per le reti multiservice:

Tipo di traffico	CoS Layer 2	Precedenza IP layer 3	DSCP layer 3
Voice RTP ¹	5	5	EF
Controllo vocale	3	3	AF31

Videoconferenza	4	4	AF41
Video in streaming (IP/TV)	1	1	AF13
Dati	0-2	0-2	0-AF23

¹ RTP = Real-Time Transport Protocol

In questa tabella vengono assegnati valori di classificazione e contrassegno separati per video e videoconferenze in streaming. Lo streaming video ha una migliore capacità di memorizzare i flussi e gestire il ritardo e l'instabilità. Pertanto, lo streaming video richiede livelli QoS diversi.

Inoltre, è possibile separare le parti di controllo e i dati dei flussi di videoconferenza. Per separare queste due porzioni dei flussi, contrassegnare il controllo con AF31 e i dati con AF41. Tuttavia, questo progetto non è il migliore. Non tutti gli endpoint consentono di contrassegnare il portatore e di controllare il traffico in modo diverso e un proxy Cisco contrassegna tutto il traffico di videoconferenza con un unico valore. Inoltre, i bit rate del traffico di controllo sono trascurabili, rispetto ai bit rate delle videochiamate.

Eeguire la classificazione il più vicino possibile all'origine. I partner video di terze parti VCON, PictureTel e Polycom possono impostare i bit di precedenza IP. Se il terminale H.323 non imposta alcun valore di intestazione, è possibile contrassegnare i pacchetti nei seguenti punti della rete:

- Una porta dello switch di layer 3 Per ulteriori informazioni, fare riferimento a [Configurazione di QoS](#).
- Cisco IOS? router che utilizza il contrassegno basato su classiper ulteriori informazioni, fare riferimento a [Configurazione del contrassegno pacchetti basato su classi](#).
- Router Cisco IOS che utilizza la funzionalità Cisco MCM
- Un proxy/gatekeeper H.323 che funziona su un router WAN remoto

[Selezionare un meccanismo di accodamento fantasia](#)

Il software Cisco IOS include ora diversi meccanismi di coda. Questi meccanismi soddisfano le esigenze del tipo di traffico che entra nella rete e dei supporti ad ampio raggio attraversati dal traffico. In qualsiasi momento in cui vi sia un potenziale punto di congestione nella rete, è necessario utilizzare tecniche di coda appropriate. La coda garantisce che il traffico sensibile al ritardo e alla perdita di dati, come voce e video in tempo reale, passi senza ostacoli, in relazione alle applicazioni dati a tolleranza di perdita. In genere, l'interruzione si verifica sul router edge WAN. Qui, centinaia di megabit di traffico potenziale si aggregano in collegamenti a velocità più lenta nel raggio dei kilobit o dei megabit al secondo.

Configurare i metodi di coda più recenti con i comandi dell'interfaccia della riga di comando (CLI) (MQC) QoS modulare. Con MQC, specificare una larghezza di banda minima garantita con il comando **bandwidth**. Specificare la priorità assoluta da rimuovere dalla coda a livello di interfaccia con il comando **priority**. Il comando **bandwidth** implementa il protocollo CBWFQ (Class-Based Weighted Fair Queueing) e il comando **priority** implementa LLQ. Per ulteriori informazioni, fare riferimento a [Confronto tra la larghezza di banda e i comandi di priorità di un criterio del servizio QoS](#).

[Modello/schema di definizione delle priorità](#)

Cisco consiglia questo modello o schema di assegnazione di priorità su una rete multiservice:

Tipo di collegamento dati	Versione minima del software Cisco IOS	Classificazione	Assegnazione di priorità	LFI	Traffic Shaping
Linee seriali	Software Cisco IOS release 12.0(7)T	DSCP = EF per la voce; DSCP = AF41 per tutto il traffico di videoconferenze; DSCP = AF31 per il traffico di controllo vocale; le altre classi di traffico hanno una classificazione univoca.	LLQ con CBWFQ	MLP ²	—
Frame Relay	Software Cisco IOS release 12.1(2)T	DSCP = EF per la voce; DSCP = AF41 per video; DSCP = AF31 per il traffico di controllo vocale; le altre classi di traffico hanno una classificazione univoca.	LLQ con CBWFQ	FR F.12	Forma il traffico verso CIR ³ .
ATM	Software Cisco IOS release 12.1(DSCP = EF per la voce; DSCP = AF41 per video; DSCP = AF31 per il traffico di	LLQ con CBWFQ	MLP over ATM	Forma il traffico alla porzione garantita della larghezza di banda.

	5)T	controllo vocale; le altre classi di traffico hanno una classificazione univoca.			
ATM e Frame Relay	Software Cisco IOS release 12.1(5)T	DSCP = EF per la voce; DSCP = AF41 per video; DSCP = AF31 per il traffico di controllo vocale; le altre classi di traffico hanno una classificazione univoca.	LLQ con CBWFQ	MLP su ATM e Frame Relay	Forma il traffico alla porzione garantita della larghezza di banda sul collegamento più lento.

¹ LFI = Link Fragmentation and Interleaving

² MLP = Multilink PPP

³ CIR = tasso informazioni vincolate

In questo elenco vengono illustrati alcuni punti chiave del modello/schema di assegnazione delle priorità.

- La voce entra in una coda con funzionalità PQ (Priority Queuing) e riceve una larghezza di banda di 48 kbps. Il criterio di ingresso di questa coda è il valore DSCP di EF o un valore di precedenza IP di 5. Il traffico superiore a 48 kbps diminuisce in caso di congestione dell'interfaccia. Pertanto, utilizzare un meccanismo di controllo di ammissione per garantire che il traffico non superi questo valore.
- Il traffico delle videoconferenze entra in una coda con funzionalità PQ e riceve una larghezza di banda della velocità dati della chiamata più il 20%. Il criterio di ingresso a questa coda è un valore DSCP di AF41 o un valore di precedenza IP di 4. Il traffico in eccesso rispetto alla velocità dei dati della chiamata diminuisce in caso di congestione dell'interfaccia. Pertanto, come nel caso della voce, è **necessario** utilizzare un meccanismo di controllo di ammissione per garantire che il traffico non superi questo valore. Utilizzare il proxy per l'accesso alla coda, in particolare se non è stata configurata l'attendibilità su ogni porta dello switch. Per l'accesso in coda in siti di piccole dimensioni con pochi terminali video, utilizzare gli Access Control List (ACL) con l'indirizzo IP del terminale video come base. L'uso degli ACL protegge gli utenti non autorizzati che contrassegnano il traffico con IP precedenza 4. Questo contrassegno ignora il gatekeeper o CAC e influenza tutto il video nel PQ. **Nota:** il traffico video unidirezionale, ad esempio IP/TV, deve utilizzare CBWFQ con il comando **bandwidth**. Le tolleranze di ritardo sono maggiori.

- La congestione dei collegamenti WAN può completamente affamare i protocolli di segnalazione del controllo vocale. In questo caso, i telefoni IP non possono completare le chiamate sulla WAN IP. Il traffico del protocollo di controllo vocale, come H.323 e il protocollo Skinny Client Control Protocol, richiede una coda equa ponderata basata su classi con una larghezza di banda minima configurabile pari a un valore DSCP di AF31. Questo valore DSCP è correlato a un valore di precedenza IP pari a 3.
- Il traffico SNA (Systems Network Architecture) entra in una coda con una larghezza di banda specificata di 56 kbps. L'operazione di accodamento all'interno di questa classe è FIFO, con un'allocazione della larghezza di banda minima di 56 kbps. Il traffico di questa classe che supera i 56 kbps entra nella coda predefinita. Il criterio di ingresso per questa coda può essere rappresentato dai numeri di porta TCP, un indirizzo di layer 3, la precedenza IP o un DSCP.

Tutto il traffico rimanente può entrare in una coda predefinita. Se si specifica una larghezza di banda, l'operazione di accodamento è FIFO. In alternativa, se si specifica la parola chiave fair, l'operazione è WFQ (weighted fair queuing).

Inoltre, non effettuare videoconferenze con velocità di collegamento inferiori a 768 kbps. Sui collegamenti a bassa velocità di trasmissione, l'uso di RTP compresso (cRTP) e LFI può ridurre gli effetti della serializzazione e del ritardo delle code.

Non utilizzare il protocollo cRTP con videoconferenze IP. In questo elenco vengono illustrate le procedure ottimali per cRTP:

- Utilizzare cRTP solo con codec voce a bassa velocità in bit, ad esempio G.729. Se si utilizza G.711 come codec audio per una chiamata vocale o di videoconferenza, i miglioramenti statistici della velocità di trasmissione ottenuti con cRTP non sono sufficienti per giustificare l'uso di cRTP.
- Utilizzare cRTP solo quando la voce con bassa velocità di trasmissione è una percentuale significativa del carico offerto. In generale, questa funzione è utile solo quando la voce a bassa velocità di trasmissione è superiore al 30% del carico offerto a un circuito.
- cRTP può influire sulle prestazioni di inoltro. Monitorare l'utilizzo della CPU dopo aver abilitato la funzione.

[La voce e il video devono condividere LLQ?](#)

Con i criteri del servizio QoS multiservice viene spesso presa in considerazione la possibilità di configurare il traffico delle conferenze voce e video come classi di priorità. Questa considerazione deriva dal fatto che LLQ attualmente supporta una singola coda con priorità rigorosa, anche quando sono state configurate più classi per la definizione di priorità. Quando si configurano le classi VoIP e video con priorità, il traffico proveniente da entrambe le classi viene inserito in un'unica coda. Di conseguenza, è possibile scegliere di non inserire il video nella coda di priorità per i motivi seguenti:

- I pacchetti video sono molto più grandi dei pacchetti voce. I pacchetti video hanno generalmente le stesse dimensioni della MTU massima del collegamento. Con il marchio EF, i pacchetti video possono entrare nella stessa coda di priorità della voce. Se un pacchetto VoIP piccolo entra nella coda dietro un pacchetto video grande, o dietro diversi pacchetti di questo tipo, il ritardo nel pacchetto VoIP aumenta. Il ritardo può essere considerevole e influisce negativamente sulle prestazioni delle applicazioni VoIP.

- Poiché la maggior parte delle code EF sono molto piccole, possono causare la perdita di pacchetti quando vengono utilizzate per il traffico video.

Cisco ha eseguito test che hanno inserito il video nella coda delle priorità. I test sono stati condotti con velocità di collegamento superiori a 768 kbps e con CAC appropriato per evitare un'iscrizione eccessiva. Cisco ha rilevato che il posizionamento del video nella coda di priorità non ha introdotto un aumento notevole del ritardo nei pacchetti voce.

In generale, potete selezionare uno di questi modelli. Cisco ha testato entrambi i modelli:

- Voce, video e audio nella coda delle priorità e provisioning appropriato
- Voce nella coda di priorità, con video e audio in una coda di larghezza di banda

Un terzo approccio è quello di separare i componenti audio della videoconferenza. In altre parole, posizionate il componente audio nella coda di priorità e il componente video in una coda di larghezza di banda. Tuttavia, i coder video tendono ad avere ritardi di codifica più lunghi rispetto ai coder voce. Pertanto, se si attribuisce priorità assoluta ai flussi audio di una videoconferenza, i flussi audio arrivano in anticipo e vengono mantenuti in modo da ottenere la sincronizzazione labiale. Pertanto, non vi è alcun vantaggio se si mettono in coda pacchetti voce associati a una videoconferenza con un servizio migliore rispetto a quello ricevuto dai pacchetti video.

Se si sceglie di inserire video e voce nella coda di priorità, contrassegnare i tipi di traffico con valori DSCP diversi. Se si contrassegnano i tipi di traffico con valori DSCP diversi, è possibile utilizzare un'istruzione di priorità diversa nei criteri del servizio QoS per controllare il video. In particolare, il video può richiedere un parametro burst maggiore.

CAC

La definizione delle priorità del traffico risolve solo in parte la sfida della fornitura QoS per i video su IP. Una soluzione completa richiede CAC.

Il CAC, o controllo della larghezza di banda, è necessario per evitare sottoscrizioni eccessive delle risorse di rete. Nelle videoconferenze, il rifiuto di un terminale video che richiede risorse di rete è necessario per mantenere la qualità degli stream video esistenti se il nuovo terminale supera la larghezza di banda disponibile. In altre parole, CAC protegge il video dai video.

In generale, esistono tre schemi per la fornitura di CAC per le videochiamate:

- Limitare il numero di terminali video. In particolare, nei siti remoti senza un gatekeeper H.323, esiste un solo modo per controllare l'uso della larghezza di banda per i video attraverso un particolare collegamento, come una WAN. In questo caso, è necessario limitare fisicamente il numero di terminali video nei siti remoti. Fornire una larghezza di banda sufficiente nella coda di priorità per supportare la velocità massima di trasmissione dati di tutti gli endpoint video in un particolare sito. **Nota:** assegnare alla coda priorità la velocità massima di trasferimento dati dei terminali video più il 20%. Il 20% aggiuntivo consente di gestire le reti IP e il sovraccarico del trasporto.
- Utilizzare il CAC gatekeeper per impostare i limiti di larghezza di banda per le chiamate interzona e intrazona per singola sessione. È possibile combinare il CAC gatekeeper con un proxy, che fornisce un singolo punto di accesso alla coda delle priorità. Questo singolo punto di accesso impedisce che i flussi video non autorizzati sovrascrivano la coda di priorità. Per accedere al proxy, è necessario registrare i terminali video presso il gatekeeper. La configurazione gatekeeper consente una larghezza di banda video massima al di fuori della

zona locale. Questa larghezza di banda massima deve corrispondere al provisioning della larghezza di banda della coda di priorità per garantire il corretto funzionamento della coda. Queste linee guida si applicano solo agli ambienti hub e spoke. I gatekeeper utilizzano la modalità diretta e non consentono ai gatekeeper intermedi di dedurre la larghezza di banda dai collegamenti.

- Implementare gli endpoint per i quali è stato abilitato RSVP. Gli endpoint utilizzano i messaggi RSVP per descrivere il profilo del traffico e richiedere il servizio necessario. I dispositivi di rete compatibili con RSVP sul percorso end-to-end leggono questi messaggi RSVP e decidono se concedere o negare la richiesta di prenotazione. I dispositivi comunicano la loro decisione all'endpoint tramite un altro messaggio RSVP. L'endpoint e la sua applicazione decidono quindi se adeguarsi alle condizioni di rete disponibili attraverso l'interruzione della conferenza o una riduzione dei requisiti.

L'Appendice II dello standard H.323 versione 4 descrive un approccio per l'uso di RSVP. I punti principali sono i seguenti:

- Quando si effettua una chiamata, un endpoint comunica la capacità dell'endpoint di riservare risorse al gatekeeper. Il gatekeeper indica quindi se è consigliabile un tentativo di prenotazione delle risorse dell'endpoint.
- Durante la fase H.245, gli endpoint indicano se possono segnalare la prenotazione delle risorse. Sulla base di queste informazioni, gli endpoint decidono se procedere con la chiamata.
- L'invio di messaggi di prenotazione RSVP può avvenire dopo l'apertura dei canali logici ma prima dell'uso dei canali logici per i pacchetti di dati.

Traffic Shaping

L'uso di Frame Relay per la connettività WAN introduce un altro requisito QoS. In particolare, quando un sito centrale ad alta velocità alimenta uno o più siti remoti a velocità inferiore, il sito centrale può sovraccaricare sia la larghezza di banda fisica che quella CIR del sito remoto. Per evitare l'invio di una larghezza di banda eccessiva a un sito remoto, implementare il traffic shaping sul router del sito centrale. Per ulteriori informazioni sul traffic shaping Frame Relay, consultare le seguenti risorse:

- [Configurazione di Frame Relay Traffic Shaping su router 7200 e piattaforme inferiori](#)
- [VoIP over Frame Relay con qualità del servizio \(frammentazione, Traffic Shaping, priorità LLQ / IP RTP\)](#)

Interoperabilità con i terminali H.323

Le reti di videoconferenza H.323 sono composte solitamente da cinque componenti funzionali:

- Terminali video
- Gatekeeper
- Gateway
- MCU
- Proxy

Cisco offre soluzioni di prodotto per tutti questi componenti, ad eccezione dei terminali video. La

prova dimostra che i prodotti Cisco H.323 interagiscono con terminali di terze parti H.323.

In alcuni casi, questi terminali offrono strumenti QoS per garantire la soddisfazione dei parametri di ritardo e perdita del traffico video a fronte di flussi di dati imprevedibili. Ad esempio, Polycom Viewstation tiene traccia di tutti i pacchetti video dopo la definizione di una chiamata. Polycom Viewstation indica la latenza media e il numero di pacchetti video o audio persi. Questo strumento supporta anche il debug con output leggibile. Questi debug possono aiutare a indicare la causa di un problema che non è rilevabile attraverso l'analisi dell'uscita video. Per ulteriori informazioni, consultare il documento [How to Configure Video over IP for Polycom Video Units](#) (Come configurare il video su IP per le unità video Polycom).

Esempio di configurazione

In questa configurazione di esempio viene illustrato come applicare LLQ al traffico di videoconferenza che attraversa un collegamento WAN:

Esempio di configurazione	
<pre> Sample Configuration class-map Video-Conf match access-group 102 class-map Streaming-Video match access-group 103 ! policy-map QoS-Policy class Video-Conf priority 450 30000 class Streaming-Video bandwidth 150 class class-default fair-queue ! ! -- Video-Conf Traffic access-list 102 permit ip any any dscp cs4 access-list 102 permit ip any any dscp af41 ! ! -- Streaming Traffic access-list 103 permit ip any any dscp cs1 access-list 103 permit ip any any dscp af13 </pre>	

Dopo aver creato una mappa dei criteri QoS, applicare i criteri con il comando **service-policy**. Il tipo di interfaccia a cui viene applicato il criterio determina le posizioni di applicazione del comando. Seguono alcuni esempi:

Tipo di interfaccia	Esempio di configurazione
Linea in leasing	<code>line interface multilink1</code> <code>service-policy output QoS-Policy</code>
PVC	

1 ATM	<pre>interface atm 1/0.1 point pvc 1/50 service-policy output QoS-Policy</pre>
Frame Relay VC ²	<pre>map-class frame-relay vcofr frame cir 128000 frame mincir 64000 frame bc 1000 frame frag 160 service-policy output QoS-policy</pre> <p>Nota: sui Cisco serie 7500 con QoS distribuito, utilizzare i comandi DTS³. Fare riferimento a Frame Relay Traffic Shaping con QoS distribuito sui Cisco serie 7500.</p>

¹ PVC = circuito virtuale permanente

² VC = circuito virtuale

³ DTS = traffic shaping distribuito

[Informazioni correlate](#)

- [Standard ITU H.323](#)
- [Controllo dell'ingresso di chiamata per gateway VoIP H.323](#)
- [Panoramica delle tecnologie di internetworking: Quality of Service Networking](#)
- [Pagina di supporto QoS](#)
- [Supporto tecnico – Cisco Systems](#)

Questo documento ti è stato utile? [Sì](#) [No](#)

Grazie per il feedback.

[Apri una richiesta di assistenza](#) (È necessario un [contratto di servizio Cisco](#).)

Discussioni correlate nella Cisco Support Community

La [Cisco Support Community](#) è un forum in cui puoi fare domande e rispondere, condividere suggerimenti e collaborare con i tuoi colleghi.

Per informazioni sulle convenzioni usate in questo documento, consultare il documento [Cisco sulle convenzioni nei suggerimenti tecnici](#).

Aggiornato: 15 feb 2008

ID documento: 21662