Implementazione di Quality of Service

Sommario

Introduzione

Questo documento fornisce alcune linee guida di alto livello per l'implementazione di Quality of Service (QoS) in una rete che funge da trasporto per più applicazioni, incluse le applicazioni sensibili al ritardo e a uso intensivo di larghezza di banda. Queste applicazioni possono migliorare i processi aziendali, ma estendere le risorse di rete. QoS può fornire servizi sicuri, prevedibili, misurabili e garantiti a queste applicazioni gestendo il ritardo, le variazioni di ritardo (jitter), la larghezza di banda e la perdita di pacchetti in una rete.

Quali applicazioni richiedono QoS?

Determinare innanzitutto le applicazioni business-critical che richiedono protezione. Potrebbe essere necessario esaminare tutte le applicazioni in competizione per le risorse di rete. In questo caso, utilizzare Netflow Accounting, Network-based Application Recognition (NBAR) o QoS Device Manager (QDM) per analizzare i modelli di traffico nella rete.

NetFlow Accounting fornisce dettagli sul traffico di rete e può essere utilizzato per acquisire la classificazione del traffico o la precedenza associata a ciascun flusso.

NBAR è uno strumento di classificazione in grado di identificare il traffico fino al livello dell'applicazione. Fornisce statistiche per interfaccia, per protocollo e bidirezionali per ciascun flusso di traffico che attraversa un'interfaccia. NBAR opera anche nella classificazione delle sottoporte; ricerca e identificazione oltre le porte delle applicazioni.

QDM è un'applicazione di gestione della rete basata sul Web che fornisce un'interfaccia grafica utente facile da utilizzare per la configurazione e il monitoraggio di funzionalità QoS avanzate

basate su IP nei router.

Comprensione delle caratteristiche delle applicazioni

Èimportante comprendere le caratteristiche delle applicazioni che richiedono protezione. Alcune applicazioni tendono ad essere sensibili alla latenza o alla perdita di pacchetti, mentre altre sono considerate "aggressive" perché sono frammentate o consumano molta larghezza di banda. Se l'applicazione è frammentata, determinare se è presente una frammentazione costante o piccola. Le dimensioni del pacchetto dell'applicazione sono grandi o piccole? L'applicazione è basata su TCP o UDP?

Caratteristica	Orientamento
Applicazione sensibile al ritardo o alla perdita. (voce e video in tempo reale)	*Non* utilizzare il WRED (Weighted Random Early Detection), il traffic shaping, la frammentazione (FRF-12) o l'applicazione di policy. Per questo tipo di traffico, è necessario implementare LLQ (Low Latency Queuing) e utilizzare una coda di priorità per il traffico sensibile al ritardo.
Applicazione che è costantemente bursty o è un hog larghezza di banda. (FTP e HTTP)	Utilizzare WRED, policing, traffic shaping o CBWFQ (Weighted Fair Queueing) basato su classi per garantire la larghezza di banda.
Applicazione basata su TCP.	Usare WRED poiché i pacchetti persi causano il backoff del TCP e quindi il riavvio utilizzando l'algoritmo di avvio lento. Se il traffico è basato su UDP e non modifica il suo comportamento quando i pacchetti vengono scartati, non utilizzare WRED. Utilizzare Policing se è necessario limitare la velocità dell'applicazione; in caso contrario, lascia che i pacchetti scendano.

Conoscenza della topologia di rete

Alcuni dispositivi potrebbero richiedere un aggiornamento del sistema operativo IOS per sfruttare le funzionalità QoS che si desidera implementare. I diagrammi della topologia di rete, delle configurazioni dei router e della versione software su ciascun dispositivo consentono di stimare il numero di dispositivi che richiedono un aggiornamento IOS. Per informazioni sulle icone che possono aiutare a creare i diagrammi di rete, consultare la Cisco Icon Library.

- Valutare l'utilizzo della CPU su ciascun router durante i periodi di traffico intenso per decidere come distribuire le funzionalità QoS tra i dispositivi per condividere il carico.
- Classificare i tipi di traffico business-critical e le interfacce attraversate dal traffico. Decidere quali gruppi di priorità o classi creare per raggiungere gli obiettivi QoS della rete.
- Determinare il ritardo massimo che le applicazioni più critiche possono gestire e regolare i parametri della frammentazione all'interno dei condizionatori del traffico (traffic shaper o policer) per far fronte a questo ritardo.
- Scopri le tariffe supportate su ciascuna interfaccia: PVC o sottointerfacce e configurare la larghezza di banda in modo che corrisponda.
- Identificare i collegamenti lenti per determinare dove si trovano i colli di bottiglia nella rete e decidere come applicare i meccanismi di efficienza del collegamento alle interfacce appropriate.
- Calcolare il sovraccarico di layer 2 e layer 3 per ciascun tipo di supporto che trasporterà il traffico business critical. In questo modo sarà possibile calcolare la corretta quantità di larghezza di banda necessaria per ogni classe.
- Un'altra informazione fondamentale è se si desidera proteggere il traffico in base all'applicazione, all'origine e alla destinazione IP o a entrambi.

Collega dimensioni intestazione livello

Tipo di supporto	Intestazione livello collegamento
Ethernet	14 Byte
PPP	6 Byte
Frame Relay	4 Byte
ATM	5 byte/cella

Creazione di classi in base ai criteri

Una volta determinate le applicazioni che richiedono QoS e i criteri di classificazione da utilizzare (in base alle caratteristiche delle applicazioni), è possibile creare classi basate su queste informazioni.

Creazione di un criterio per contrassegnare ogni classe

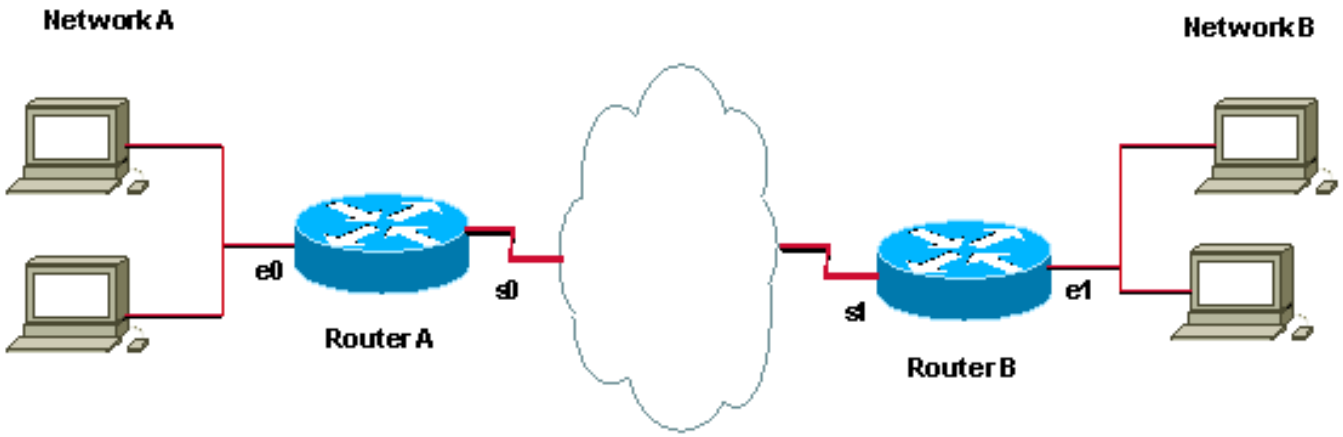
Creare una policy per contrassegnare ogni classe di traffico con i valori di priorità appropriati (utilizzare DSCP (Differentiated Services Control Point) o IP Precedence). Il traffico viene contrassegnato quando arriva al router sull'interfaccia in entrata. I contrassegni verranno usati per gestire il traffico quando lascia il router sull'interfaccia di uscita.

Lavorare dal bordo verso il centro

Lavorare dal router più vicino al traffico verso il nucleo. Applicare il contrassegno sull'interfaccia in entrata del router. Nella topologia riportata di seguito, il router A è la posizione più logica per contrassegnare il traffico e applicare i criteri per i dati provenienti dalla rete A e destinati al router B. Il traffico verrà contrassegnato quando entra nell'interfaccia Ethernet0 del router A e il criterio QoS verrà applicato all'interfaccia Serial0 del router A quando lascia il router. Se si deve applicare

lo stesso criterio in entrambe le direzioni (in modo che il traffico proveniente dalla rete B e destinato alla rete A riceva lo stesso trattamento), il traffico proveniente dalla rete B deve essere contrassegnato in quanto entra nell'interfaccia Ethernet1 del router B e gestito quando lascia il router sull'interfaccia Serial1.

Quando il traffico è contrassegnato sull'interfaccia in entrata su un router, mantiene gli stessi contrassegni come attraversano più hop (a meno che non venga nuovamente contrassegnato). In genere, il traffico deve essere contrassegnato solo una volta. I criteri QoS possono essere applicati a hop aggiuntivi basati su questi contrassegni. È necessario riapplicare il contrassegno solo se il traffico proviene da un dominio non trusted.



Creazione della policy per il traffico

Dopo aver contrassegnato il traffico, è possibile utilizzare i contrassegni per creare una policy ed eseguire la classificazione del traffico sugli altri segmenti della rete. È consigliabile semplificare la policy utilizzando non più di quattro classi.

Se possibile, implementare e testare un'implementazione QoS in un ambiente lab. Distribuirlo nella rete attiva dopo aver ottenuto i risultati desiderati.

Applicazione del criterio

Applicare il criterio nella direzione appropriata. Decidere se il criterio deve essere applicato in una direzione o in entrambe. Contrassegnare sempre e gestire il traffico il più vicino possibile all'origine, come descritto nella sezione Creazione di un criterio per contrassegnare ogni classe di questo documento.

Èconsigliabile applicare lo stesso criterio in entrambe le direzioni per filtrare il traffico in arrivo e in arrivo da entrambi i lati del sito. Ciò significa che è necessario applicare lo stesso criterio alla porta in uscita sull'interfaccia seriale del router A e sull'interfaccia seriale del router B.

Utilizzo di QoS Policy Manager (QPM) per monitorare gli effetti dei criteri

Utilizzare QPM come sistema completo per il controllo centralizzato delle policy e l'implementazione automatizzata e affidabile delle policy.

Raccomandazioni QoS per scopi generali

Di seguito è riportato un elenco delle categorie QOS e di alcune delle funzioni QOS più diffuse associate a ciascuna categoria.

Categoria	Funzioni QoS associate
Modello di servizio QoS	QoS con provisioning (Diffserv) quando possibile o segnalato (RSVP) quando necessario.
Classificazione/contrassegno	Punti di codice Diffserv o ID gruppo qos.
Gestione delle congestioni	LLQ o CBWFQ.
Prevenzione delle congestioni	Diffserv conforme WRED.
Efficienza collegamento	MLPPP, LFI, FRF.11, FRF.12, CRTP
Segnalazione	RSVP, QPB
Traffic Conditioner/Policing	GTS (Class Based Policer) e FRTS (Generic Traffic Shaping).
Configurazione/monitoraggio	QPM, CLI (Command Line Interface) QoS modulare, QDM

Informazioni correlate

- Pagina di supporto QoS
- Pagina di supporto per i protocolli di routing IP
- Pagina di supporto per il routing IP
- Pagina di supporto del protocollo IS-IS
- Supporto tecnico – Cisco Systems