Uso di Cisco Service Assurance Agent e Internetwork Performance Monitor per gestire la qualità del servizio nelle reti Voice over IP

Sommario

Introduzione

In questo documento viene descritto l'utilizzo di Cisco Service Assurance Agent (SAA) e Internetwork Performance Monitor (IPM) per misurare la qualità del servizio (QoS) nelle reti Voice over IP (VoIP). Queste informazioni si basano su un progetto di telefonia IP reale. Questo documento si concentra sull'applicazione dei prodotti, non sui prodotti stessi. È necessario avere già familiarità con Cisco ASA e IPM e avere accesso alla documentazione del prodotto richiesta. Per riferimenti ad altra documentazione, vedere Informazioni correlate.

Nota: la funzionalità Cisco ASA nel software Cisco IOS® era nota in precedenza come Response Time Reporter (RTR).

Quando si gestisce una rete VoIP su larga scala, è necessario disporre degli strumenti necessari per monitorare e segnalare in modo obiettivo la qualità della voce nella rete. Non è possibile basarsi esclusivamente sul feedback degli utenti, in quanto spesso è soggettivo e incompleto. I problemi di qualità della voce in genere derivano da problemi QoS di rete. Quindi, quando si identificano i problemi di qualità vocale, è necessario un secondo strumento per gestire e monitorare la QoS della rete. Nell'esempio riportato in questo documento vengono usati Cisco ASA e IPM.

Cisco Voice Manager (CVM) viene utilizzato con Telemate.net per gestire la qualità vocale. Riporta la qualità vocale delle chiamate tramite il fattore di riduzione di valore/riduzione di valore pianificazione calcolata (ICPIF) calcolato da un gateway Cisco IOS per ciascuna chiamata. Questo consente al gestore della rete di identificare i siti con problemi di scarsa qualità vocale. Per ulteriori informazioni, fare riferimento a Gestione della qualità vocale con Cisco Voice Manager (CVM) e Telemate.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware, ma gli esempi riportati sono relativi alle seguenti versioni software e hardware:

- Cisco IOS Software Release 12.1(4)
- IPM 2.5 per Windows NT
- Catalyst serie 4500 switch

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Problemi QoS in una rete VoIP

Diversi fattori possono peggiorare la qualità della voce in una rete voce pacchettizzata:

- Perdita di pacchetti
- Ritardo eccessivo
- Instabilità eccessiva

Èparticolarmente importante monitorare queste cifre su base continuativa, se i servizi a commutazione di pacchetto sono utilizzati nella WAN (ad esempio, ATM, Frame Relay o IP Virtual Private Network). In diversi scenari, la congestione della rete vettore, una configurazione errata del traffic shaping sui dispositivi periferici o una configurazione errata del policing sul lato vettore possono causare perdite di pacchetti o buffer eccessivi. Quando il vettore scarta i pacchetti, non ci sono evidenze evidenti sui dispositivi periferici. Pertanto, è necessario uno strumento end-to-end come Cisco ASA in grado di iniettare traffico in entrata e di convalidare il corretto arrivo del traffico in uscita.

Gestione di QoS con Cisco ASA e IPM

I componenti Cisco ASA e IPM sono tre:

- Sonda RTR
- risponditore RTR
- console IPM

La sonda RTR invia una sequenza di pacchetti al risponditore RTR. Il risponditore RTR li ruota e li invia alla sonda. Questa semplice operazione consente alla sonda di misurare la perdita del pacchetto e il ritardo di andata e ritorno. Per misurare il jitter, la sonda invia un pacchetto di controllo al responder prima di avviare il burst del pacchetto. Il pacchetto di controllo indica al risponditore il numero di millisecondi (ms) che ci si aspetta tra ciascun pacchetto della frammentazione. Il responder misura quindi il ritardo tra i pacchetti durante la frammentazione e

qualsiasi deviazione dall'intervallo previsto viene registrata come jitter.

La console IPM controlla il monitoraggio QoS. Il sistema programma le richieste RTR con le informazioni richieste tramite il protocollo SNMP (Simple Network Management Protocol). Raccoglie inoltre i risultati tramite SNMP. Sulle sonde RTR, non è richiesta alcuna configurazione dell'interfaccia della riga di comando Cisco IOS.

Eseguire il comando di configurazione globale **rtr responder** per configurare manualmente i risponditori RTR.

Le sonde RTR e i risponditori devono eseguire il software Cisco IOS versione 12.0(5)T o successive. Si consiglia l'ultima release di manutenzione della versione mainstream 12.1. Le sonde RTR e i risponditori negli esempi in questo documento sono in esecuzione nella versione 12.1(4). La versione IPM in uso è IPM 2.5 per Windows NT. Una patch è disponibile su Cisco.com per questa versione. Questa patch è importante, in quanto corregge un problema in cui IPM configura le sonde RTR con un'impostazione di precedenza IP errata.

Progettazione

Prima di distribuire una soluzione ASA e IPM Cisco, è necessario eseguire alcune operazioni di progettazione tenendo presenti le seguenti considerazioni:

- Posizionamento di sonde e risponditori RTR
- Tipo di traffico inviato dalla sonda al risponditore

Quando si decide la posizione delle sonde e dei risponditori, è necessario tenere in considerazione una serie di fattori. In primo luogo, si desidera che la misurazione QoS copra ogni sito, non solo i siti con problemi. Ciò è dovuto al fatto che i valori di ritardo e di jitter segnalati da IPM per un determinato sito sono più utili rispetto ad altri siti della stessa rete. Pertanto, si desidera misurare i siti con una buona qualità del servizio *e una* scarsa qualità del servizio. Inoltre, un sito con prestazioni soddisfacenti potrebbe diventare un sito con prestazioni insoddisfacenti domani, a causa di modifiche dei modelli di traffico o della rete. È necessario rilevare questa condizione prima che influisca sulla qualità della voce e venga segnalata dagli utenti.

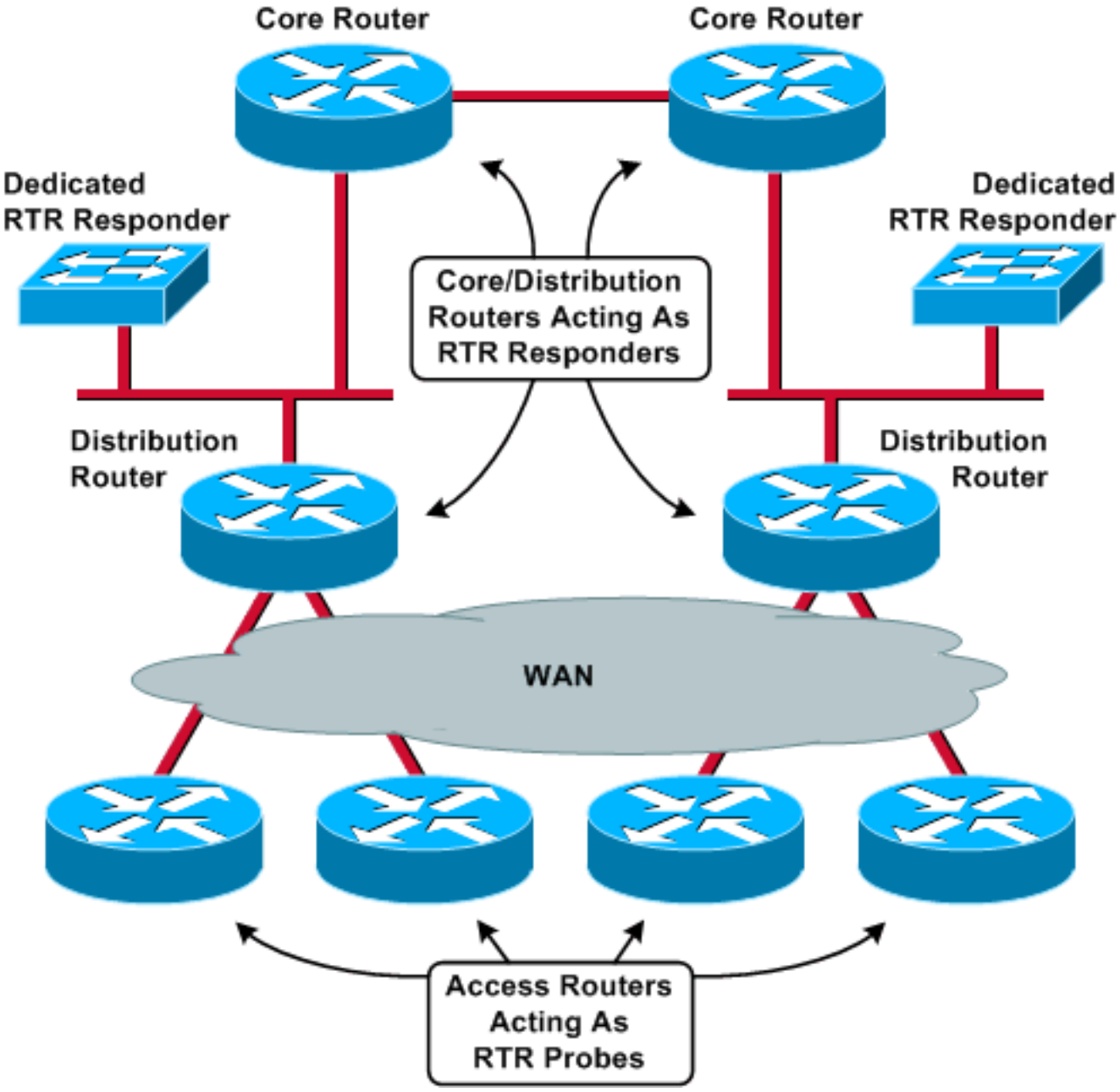
In secondo luogo, l'utilizzo della CPU è importante. Un router già occupato potrebbe non essere in grado di servire il componente RTR nel tempo previsto, e ciò potrebbe causare una distorsione dei risultati. Inoltre, se si posizionano troppe istanze di probe su un singolo router, è possibile che si verifichino problemi di utilizzo della CPU anche se non ne esisteva prima. L'approccio scelto per l'esempio di rete in questo documento (e dovrebbe funzionare nella maggior parte delle reti) è di posizionare le sonde RTR sui router remoti/filiali. Questi router in genere connettono una singola LAN a un servizio WAN relativamente lento. Di conseguenza, i router delle filiali spesso hanno un utilizzo della CPU molto basso e possono gestire facilmente il protocollo RTR. L'altro vantaggio di questo progetto è la distribuzione del carico sul maggior numero possibile di router. Tenere presente che è più facile essere una sonda che rispondere, in quanto le sonde richiedono una certa quantità di polling SNMP.

Con questo progetto, i risponditori RTR devono essere posizionati nel nucleo. I risponditori saranno più impegnati delle sonde, perché risponderanno a molte sonde. In questo modo, un solido design installa router dedicati che agiscono unicamente come responder. La maggior parte delle organizzazioni dispone di router ritirati che possono eseguire questa funzione. È sufficiente un router con interfaccia Ethernet. In alternativa, i router di core/distribuzione possono fungere da risponditori. Il diagramma di rete illustrato in questa sezione illustra entrambi gli scenari.

Distribuire il carico sul maggior numero di router possibile e monitorare l'utilizzo della CPU RTR con questo comando:

```
Router# show processes cpu | i Rtt|PID

PID  Runtime(ms)  Invoked  uSecs  5Sec   1Min   5Min    TTY Process
67           0         7      0   0.00%  0.00%  0.00%   0 Rtt Responder
```



Quando si confrontano i probe con i responder, si consiglia di mantenere una topologia coerente tra probe e responder. Ad esempio, tutte le sonde e i risponditori devono essere separati dallo stesso numero di router, switch e collegamenti WAN. Solo così i risultati IPM possono essere confrontati direttamente tra i siti.

In questo esempio sono presenti 200 siti remoti e quattro siti di core/distribuzione. uno switch Catalyst 4500 installato in ciascuna sede di distribuzione opera come risponditore RTR dedicato. Ognuno dei 200 router remoti funge da sonda RTR. Ogni sonda è destinata al responder che si trova nel sito di distribuzione connesso direttamente.

Gli picchi di traffico inviati dalle sonde ai risponditori devono ricevere dalla rete gli stessi livelli QoS

dati alla voce. Ciò potrebbe significare che è necessario regolare le configurazioni di priorità LLQ (Low Latence Queueing) o RTP (Routing Table Protocol) sul router, in modo che il traffico proveniente dalle sonde RTR sia soggetto a una rigorosa coda di priorità. Quando si configura la sonda per i pacchetti RTP, è possibile controllare solo la porta UDP (User Datagram Protocol) di destinazione e non la porta di origine. Una tipica configurazione di router LLQ in questa rete di esempio ha elenchi degli accessi che classificano specificamente i pacchetti RTR nella stessa coda della voce:

```
class-map VoiceRTP
  match access-group name IP-RTP

policy-map 192Kbps_site
  class VoiceRTP
    priority 110

ip access-list extended IP-RTP
  deny   ip any any fragments
  permit udp 10.0.16.0 0.255.239.255
             range 16384 32768 10.0.16.0 0.255.239.255
             range 16384 32768 precedence critical
  permit udp any any eq 20000 precedence critical
  permit udp any eq 20000 any precedence critical
```

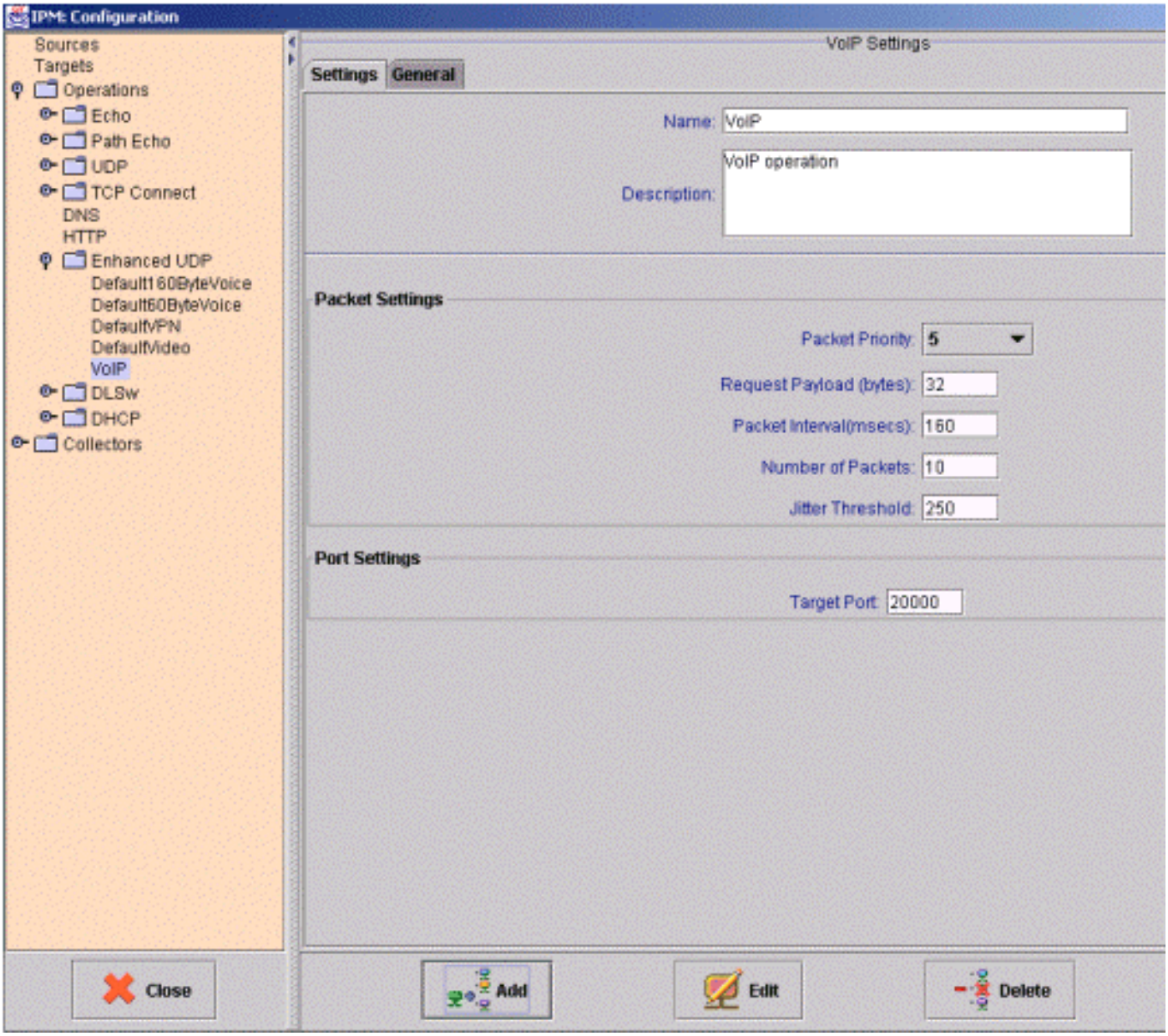
L'elenco degli accessi IP-RTP ha le seguenti linee di classificazione:

- `deny ip any fragments`Negare qualsiasi frammento IP, in quanto un elenco degli accessi di livello 4 lo consente implicitamente.
- `permettere udp 10.0.16.0 0.255.239.255 intervallo 16384 32768 10.0.16.0 0.255.239.255 intervallo 16384 32768 precedenza critico`Autorizzare i pacchetti RTP da subnet voce con precedenza IP impostata su 5.
- `consenti udp qualsiasi valore critico eq 2000`Consente l'invio di pacchetti RTP dalla sonda RTR al risponditore RTR.
- `consenti udp any eq 2000 any precedence critical`Permette ai pacchetti RTP dal risponditore RTR di tornare alla sonda RTR.

L'aggiunta del traffico RTR non provoca una sovrascrittura delle code LLQ e la perdita di pacchetti voce reali. L'operazione IPM **Default60ByteVoice** standard invia burst di pacchetti RTP con questi parametri:

- Payload richiesta: 60 byte**Nota:** questa è l'intestazione e la voce RTP. Aggiungere 28 byte (IP/UDP) per ottenere le dimensioni del datagramma L3.
- Intervallo: 20 ms
- Numero di pacchetti: 10

Ciò significa che, durante un burst, RTR consuma 35,2 Kbs di larghezza di banda LLQ. Se la larghezza di banda non è sufficiente per LLQ, creare una nuova operazione IPM e aumentare l'intervallo del pacchetto. Con i parametri mostrati in questa finestra di configurazione IPM, una frammentazione consuma solo 1 Kbps di larghezza di banda:



Risultati

La tabella riportata in questa sezione è un esempio di report IPM. Questo report contiene tre istanze di probe RTR. Tenere presente che una sonda fisica può essere configurata con più istanze di sonda RTR destinate a risponditori diversi o che utilizzano payload diversi.

Daily Jitter Summary Report 11/15/2000										
Collector Info		Round Trip Latency		Src Dest Jitter		Dest Src Jitter		Completions		
Collector	Operation	Avg	Avg Max	Avg	Avg Max	Avg	Avg Max	Trys	Over %	Error %
haw-WN	VoIP	72.71	102.79	1.74	7.65	2.62	25.88	1440	0%	0%
	Last Week	75.65	105.41	1.73	4.16	4.97	24.18	10113	0%	1%
	Last Month	74.89	103.01	1.70	3.77	6.74	24.98	7822	0%	1%
wat-WN	VoIP	72.27	121.88	2.17	12.50	3.19	39.13	1447	0%	1%
	Last Week	75.45	112.96	1.99	5.18	5.40	31.21	10127	0%	1%
	Last Month	74.00	110.51	1.83	4.91	6.44	29.76	7826	0%	1%
sfd-WN	VoIP	70.43	114.13	1.80	8.08	2.68	32.08	1440	0%	0%
	Last Week	73.92	112.17	1.75	4.68	4.94	30.19	10098	0%	1%
	Last Month	72.90	104.13	1.79	4.82	6.41	27.30	7831	0%	1%

Il significato di ciascuna colonna è il seguente:

Media:

IPM calcola una media per ogni ora di campionamento. Queste medie orarie vengono quindi calcolate su un periodo più lungo per ottenere le medie giornaliere, settimanali o mensili. In altre parole, per il report giornaliero, IPM calcola la media di ogni ora per le ultime 24 ore. La media giornaliera viene quindi calcolata come media di queste 24 medie.

Media max:

Questo valore corrisponde alla media di tutti i valori massimi orari per ogni giorno, settimana e mese del grafico. In altre parole, per il report giornaliero, IPM prende il campione più grande segnalato nelle ultime 24 ore. La media massima giornaliera viene quindi calcolata come media di questi 24 campioni.

Superiore a %:

La percentuale di campioni che hanno superato la soglia configurata per l'agente di raccolta.

Errore %:

Percentuale di pacchetti per i quali si è verificato un errore. Una sonda jitter segnala diversi tipi di errori:

- Perdita di pacchetti SD - Pacchetti persi tra origine e destinazione
- Perdita di pacchetti DS - Pacchetti persi tra destinazione e origine
- Aziende: il numero di volte in cui non è stato possibile avviare un'operazione di round-trip time (RTT) perché non era stata completata un'operazione RTT precedente.
- Sequenza: il numero di completamenti di operazioni RTT ricevuti con un identificatore di sequenza imprevisto. Di seguito sono riportate alcune possibili cause di questo problema:È

stato ricevuto un pacchetto duplicato.Risposta ricevuta dopo il timeout.È stato ricevuto un pacchetto danneggiato che non è stato rilevato.
- Gocce (Drops) - Numero di occasioni in cui si è verificata una delle seguenti situazioni:Impossibile avviare un'operazione RTT. Alcune risorse interne necessarie non sono disponibili, ad esempio la memoria o il sottosistema SNA (Systems Network Architecture)Impossibile riconoscere il completamento dell'operazione.
- MIA (Missing in Action) - Numero di pacchetti persi per i quali non è possibile determinare alcuna direzione.
- In ritardo: il numero di pacchetti arrivati dopo il timeout.

La domanda che sorge da queste informazioni è quale ritardo, jitter e valori di errore sono accettabili in una rete VoIP. Purtroppo non esiste una risposta semplice a questa domanda. I valori accettabili dipendono dal tipo di codec, dalle dimensioni del buffer di jitter e da altri fattori. Inoltre, esistono interdipendenze tra queste variabili. Una perdita di pacchetto più elevata può significare che è possibile tollerare una minore instabilità.

Il modo migliore per ottenere un ritardo accettabile e cifre instabili consiste nel confrontare siti simili nella stessa rete. Se tutti i siti a 192 Kbps collegati a cui è applicato un solo jitter segnalano valori di jitter intorno a 50 ms e il sito rimanente segnala un jitter di 100 ms, si verifica un problema, indipendentemente dai valori nominali. L'IPM è in grado di fornire una misurazione continua del ritardo e dell'instabilità 24 ore su 24, 7 giorni su 7 per l'intera rete e può fornire una base da utilizzare come parametro di riferimento per i confronti di ritardo e instabilità.

Gli errori sono tuttavia diversi. In linea di principio, qualsiasi percentuale di errore diversa da zero è un segnale d'allarme. Ai pacchetti RTR viene assegnato lo stesso trattamento QoS dei pacchetti voce. Se il controllo QoS della rete e l'ammissione delle chiamate sono efficaci, nessun livello di congestione dovrebbe causare la perdita dei pacchetti o ritardi eccessivi per i pacchetti voce o RTR. Pertanto, è possibile prevedere che i conteggi degli errori IPM siano pari a zero. Gli unici errori che possono essere considerati "normali" sono gli errori CRC (Cyclic Redundancy Check), che tuttavia dovrebbero essere rari in un'infrastruttura di qualità. Se sono frequenti, rappresentano un rischio per la qualità della voce.

Informazioni correlate

- **Lettura consigliata:** Risoluzione dei problemi di Cisco IP Telephony
- Documentazione e supporto tecnico – Cisco Systems