

Uso del agente de la garantía de servicio de Cisco e Internetwork Performance Monitor para administrar la calidad del servicio en redes de voz sobre IP

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Problemas de QoS en una red VoIP](#)

[Manejo de QoS con Cisco SAA y IPM](#)

[Diseño](#)

[Resultados](#)

[Información Relacionada](#)

[Introducción](#)

Este documento describe el uso del Cisco Service Assurance Agent (SAA) y del Internetwork Performance Monitor (IPM) de medir el Calidad de Servicio (QoS) en las redes de la voz sobre IP (VoIP). Esta información se basa en un del mundo real proyecto de telefonía IP. Este documento se centra en la aplicación de los Productos, no en los Productos ellos mismos. Usted debe ya ser familiar con Cisco SAA y IPM y tener acceso a la Documentación del Producto requerida. [Vea la Información Relacionada para las referencias de otra documentación.](#)

Note: La funcionalidad SAA de Cisco en el software de Cisco IOS® era conocida antes como Response Time Reporter (RTR).

Cuando usted está manejando una red VoIP a gran escala, usted debe tener las herramientas necesarias monitorea y señala objetivo sobre la Calidad de voz en la red. No es posible confiar en los comentarios del usuario solamente, porque es a menudo subjetiva e incompleta. Los problemas de calidad de voz provienen generalmente de problemas de red de QoS. Así pues, cuando usted identifica los problemas de calidad de voz, usted necesita una segunda herramienta manejar y monitorear la red QoS. El ejemplo en este documento utiliza Cisco SAA y el para este propósito IPM.

El Cisco Voice Manager (CVM) se utiliza con Telemate.net para manejar la Calidad de voz. Señala sobre la Calidad de voz de las llamadas vía la debilitación/el Calculated Planning Impairment Factor (ICPIF) que es calculada por un Cisco IOS Gateway para cada llamada. Esto permite que el administrador de la red identifique los sitios que sufren de la calidad de voz

deficiente. Refiera a la [administración de calidad de voz con el Cisco Voice Manager \(CVM\) y al Telemate](#) para más información.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no se restringe a las versiones de software y hardware específicas, pero los ejemplos en este documento utilizan estas versiones de software y hardware:

- Cisco IOS Software Release 12.1(4)
- IPM 2.5 para el Windows NT
- Catalyst 4500 Series Switch

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Problemas de QoS en una red VoIP

Varios factores pueden degradar la Calidad de voz en una red de voz empaquetada:

- Pérdida del paquete
- Retraso excesivo
- Fluctuación excesiva

Es determinado importante que usted monitorea estas figuras sobre una base permanente, si utilizan a los servicios conmutados por paquetes en WAN (por ejemplo, atmósfera, Frame Relay, o IP Virtual Private Network). Hay los varios escenarios donde la congestión en la red portadora, el modelado de tráfico mal configurado en los dispositivos de borde, o el policing mal configurado en el costado de la portadora pueden causar la pérdida del paquete o el excesivo almacenamiento en el búfer. Cuando el portador está cayendo los paquetes, no hay evidencia obvia en los dispositivos de borde. Por lo tanto, usted necesita una herramienta de punta a punta como Cisco SAA que pueda inyectar el tráfico en el ingreso y valida a su llegada exitosa en la salida.

Manejo de QoS con Cisco SAA y IPM

Hay tres Cisco SAA y componentes IPM:

- sonda RTR
- respondedor RTR
- Consola IPM

El sondeo de RTR envía una ráfaga de paquetes al receptor de RTR. El respondedor RTR les da la vuelta y las devuelve para que sean sondeadas. Este funcionamiento simple permite que la

sonda mide la pérdida del paquete y el retardo de ida y vuelta. Para medir el jitter, la sonda envía un paquete de control al respondedor antes de que inicie la ráfaga de paquetes. El paquete de control informa al respondedor cuántos milisegundos (ms) a esperar entre cada paquete en la explosión. El respondedor mide el retraso entre paquetes durante la ráfaga y cualquier desvío del intervalo esperado se graba como fluctuación.

La consola IPM controla la supervisión de calidad de servicio (QoS). Programa las sondas RTR con la información pertinente vía el Simple Network Management Protocol (SNMP). También recoge los resultados vía SNMP. No se requiere ninguna configuración del Cisco IOS de la interfaz de la línea de comandos en las sondas RTR.

Publique el comando global configuration del **respondedor del rtr**, de configurar manualmente a los respondedores RTR.

Las sondas y los respondedores RTR deben funcionar con el Cisco IOS Software Release 12.0(5)T o Posterior. Se recomienda la última versión estándar de mantenimiento 12.1. Las sondas y los respondedores RTR en los ejemplos en este documento están funcionando con la versión 12.1(4). La versión IPM funcionando es IPM 2.5 para el Windows NT. Una corrección está disponible en el cisco.com para esta versión. Esta corrección es importante, pues repara un problema donde el IPM configura las sondas RTR con un incorrecto configuración de precedencia IP.

Diseño

Antes de que usted despliegue Cisco SAA y solución IPM, usted debe hacer un cierto trabajo del diseño con estas consideraciones en la mente:

- Colocación de las sondas y de los respondedores RTR
- Tipo de tráfico que se envía de la sonda al respondedor

Hay varias cosas a tomar en la consideración cuando usted decide sobre la colocación de las sondas y de los respondedores. En primer lugar, necesita que la medición QoS cubra cada sitio no sólo los sitios con problemas. Esto es porque los números de la fluctuación y retraso que los informes IPM para un sitio dado son los más útiles cuando están comparados a otros sitios de la misma red. Así, usted quiere medir los sitios con buen QoS y QoS pobre. También, un sitio de funcionamiento satisfactorio puede vencer un sitio de pobre-ejecución mañana, a los cambios en los patrones de tráfico o los cambios de la red. Usted querrá detectar esto antes de que afecte a la Calidad de voz y sea señalada por los usuarios.

En segundo lugar, el uso de la CPU es importante. Ya un router ocupado puede no poder mantener al componente del RTR a tiempo, y éste puede sesgar los resultados. También, si usted pone demasiados casos de la sonda en cualquier único router, usted puede ser que cree CPU elevada los problemas de utilización aunque existió ninguno antes. El acercamiento elegido para la red de muestra en este documento (y éste debe trabajar en la mayoría de las redes) es poner las sondas RTR en el telecontrol/el Routers de sucursales. Estos routers típicamente conectan un solo LAN a un servicio del WAN relativamente lento. Por lo tanto, los routers de rama a menudo utilizan muy poco la CPU y se adaptan fácilmente a RTR. La otra ventaja de este diseño es que usted distribuye la carga a través de tanto Routers como sea posible. Tenga presente que es más trabajo a ser una sonda que ser un respondedor, pues las sondas toman una determinada cantidad de Consulta SNMP.

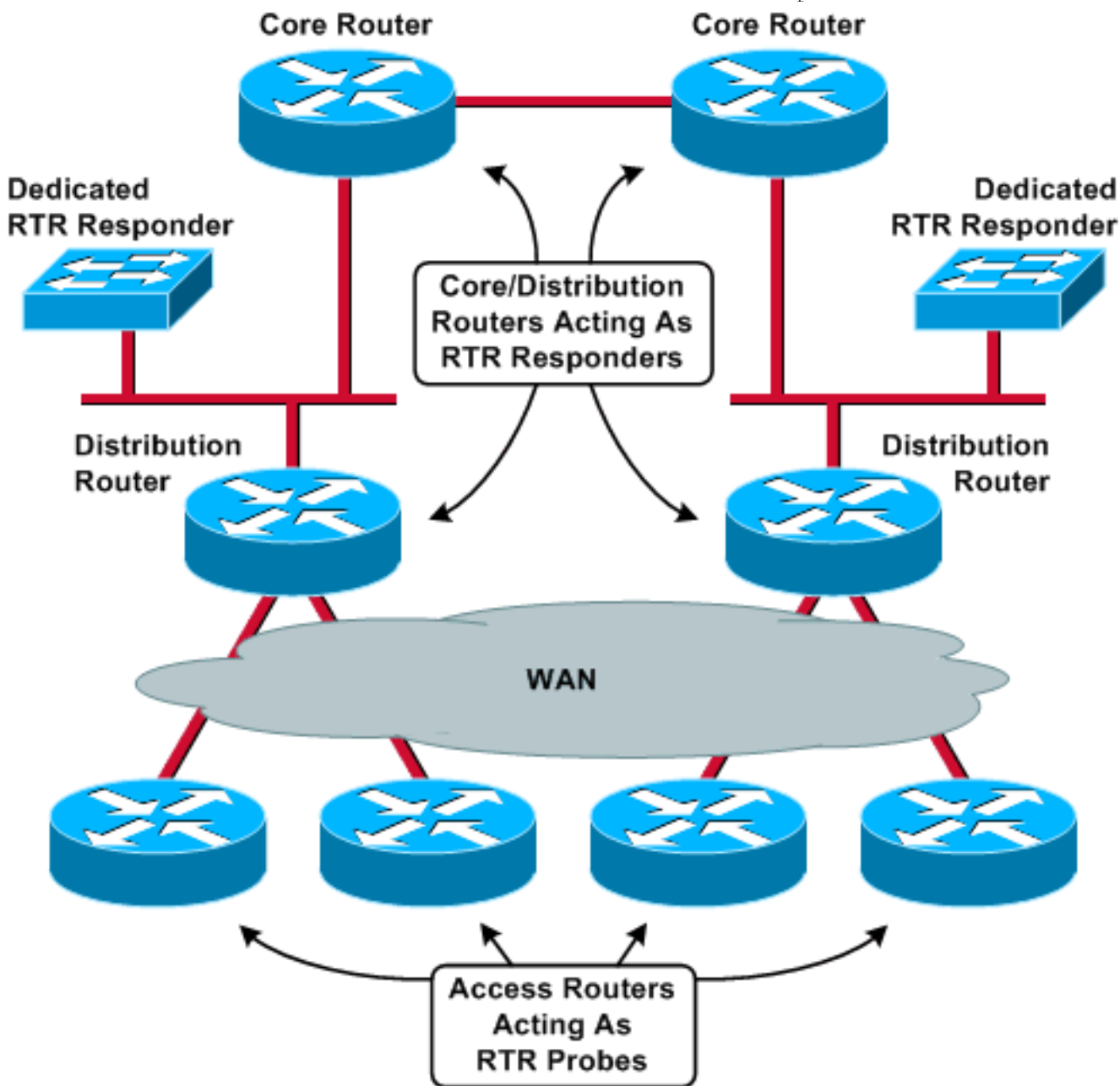
Con este diseño, los respondedores RTR deben ser colocados en la base. Los respondedores estarán más ocupados que las sondas, porque responderán a muchas sondas. Así, un diseño

robusto despliega a los routers dedicados que actúan solamente como respondedores. La mayoría de las organizaciones han retirado al Routers en el estante que puede realizar esta función. Cualquier router con una interfaz Ethernet será suficiente. Alternativamente, la base/los routers de distribución puede doblar como respondedores. El diagrama de la red en esta sección representa ambos escenarios.

Separe la carga a través de tanto Routers como sea posible, y monitoree el USO de la CPU RTR con este 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



Cuando usted está correspondiendo con las sondas con los respondedores, se recomienda que usted mantiene una topología consistente entre la sonda y el respondedor. Por ejemplo, todos los sondeos y los receptores deben estar separados por la misma cantidad de routers, switches y links WAN. Entonces se pueden los resultados IPM comparar solamente directamente entre los sitios.

En este ejemplo, hay 200 sitios remotos y cuatro sitios de núcleo/distribución. Un Catalyst 4500 en cada sitio de distribución actúa como respondedor RTR dedicado. Cada uno de los 200 routers remotos actúa como sonda RTR. Cada sonda apunta al respondedor que está situado en el sitio de distribución directamente conectado.

La red debe asignar a las ráfagas de tráfico enviadas por las sondas a los respondedores los mismos niveles de QoS que proporciona a la voz. Esto puede significar que usted tiene que ajustar el low latency queueing (LLQ) o las configuraciones de prioridad del (RTP) del protocolo de la tabla de ruteo en el router, de modo que el tráfico de las sondas RTR esté conforme a los Datos en espera de prioridad estricta. Cuando usted está configurando la sonda para los paquetes RTP, sólo el puerto del User Datagram Protocol (UDP) del destino puede ser controlado y no el puerto de origen. Una configuración del router típica LLQ en esta red de muestra tiene Listas de acceso que clasifiquen específicamente los paquetes RTR en la misma cola que la Voz:

```
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

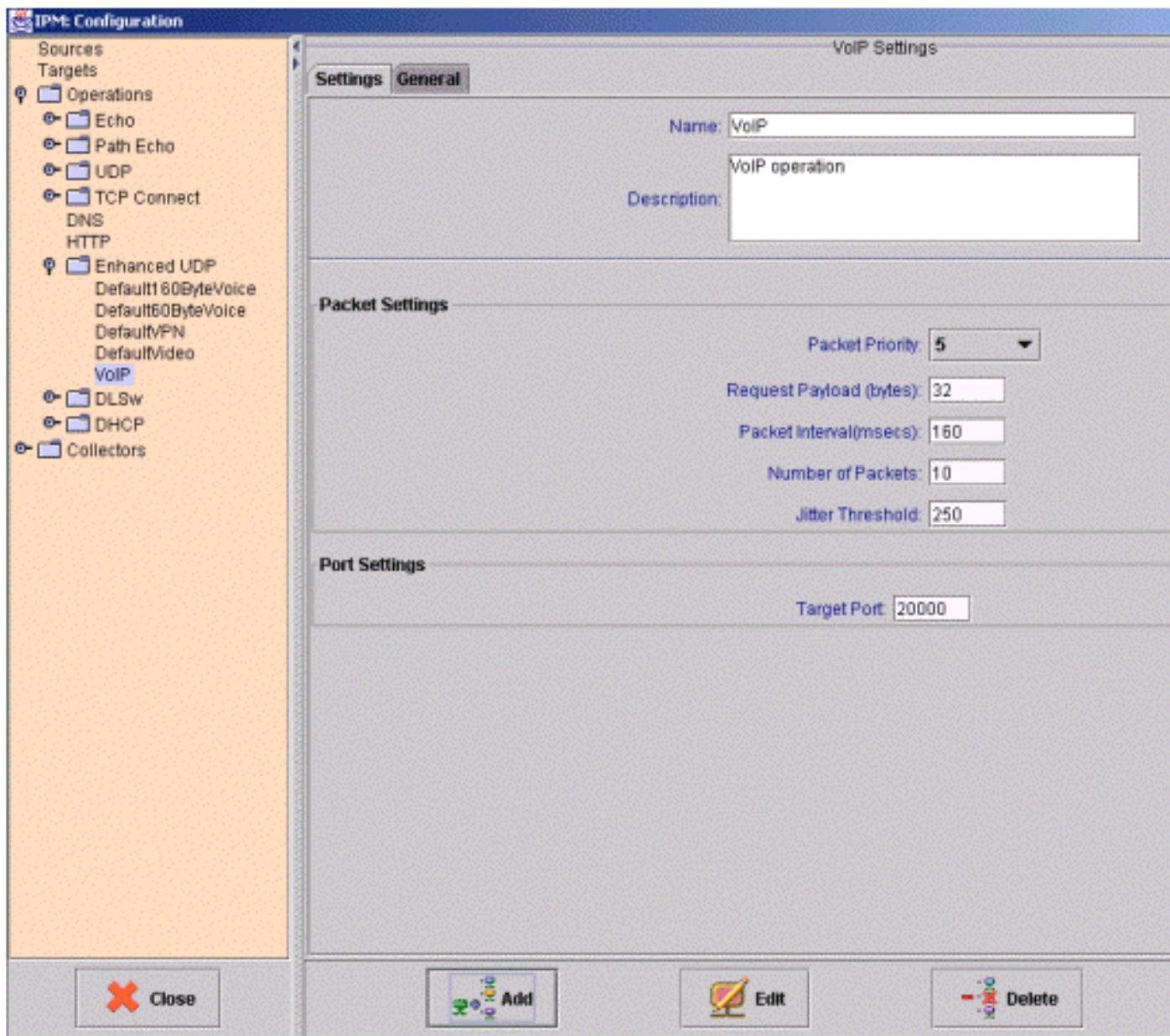
La lista de acceso IP RTP tiene estas líneas que clasifican:

- `deny ip any any` Niegue cualquier fragmento IP, como una lista de acceso de la capa 4 permite implícito éstos.
- `permit ip 10.0.16.0 0.255.239.255 32768` la precedencia del rango 16384 de 10.0.16.0 0.255.239.255 32768 crítica Paquetes con licencia RTP de los subnets de la voz con la prioridad IP fijada a 5.
- `permit udp 10.0.16.0 0.255.239.255 32768` Paquetes con licencia RTP de la sonda RTR que va al respondedor RTR.
- `permit udp 10.0.16.0 0.255.239.255 32768` Paquetes con licencia RTP del respondedor RTR que va de regreso a la sonda RTR.

Tenga cuidado que la adición de tráfico RTR no hace las colas de administración del tráfico LLQ ser paquetes de voz reales con demasiada demanda y de la causa que se caerán. La operación IPM estándar `Default60ByteVoice` envía las explosiones de los paquetes RTP con estos parámetros:

- Payload de la petición: 60 bytes **Note:** Éste es el encabezado RTP y la voz. Agregue 28 bytes (IP/UDP) para conseguir el tamaño del datagrama L3.
- Intervalo: 20 ms
- Número de paquetes: 10

Esto significa que, durante una explosión, el RTR consume 35.2 Kbs del ancho de banda LLQ. Si el ancho de banda no es suficiente para LLQ, cree una nueva operación IPM e incremente el intervalo del paquete. Con los parámetros mostrados en esta ventana de configuración IPM, una explosión consume solamente 1 kbps del ancho de banda:



Resultados

La tabla en esta sección es un ejemplo de un informe IPM. Este informe contiene tres instancias de sonda RTR. Tenga presente que una sonda física se puede configurar con los casos múltiples de la sonda RTR que apuntan a diversos respondedores o utilizan diversas cargas útiles.

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%

Éstos son los significados de cada uno de las columnas:

Avg:

IPM calcula un promedio para cada hora de muestreo. Estos promedios horarios luego son promediados en un período más largo para así obtener los promedios diario, semanal y mensual. Es decir para el informe diario, el IPM calcula la media para cada hora para las últimas 24 horas. Entonces calcula la media diaria como la media de estas 24 medias.

Máximo promedio:

Este valor es la media de todos los máximos por hora para cada día, semana, y mes en la carta. Es decir para el informe diario, el IPM recoge la muestra más grande señalada dentro de cada uno de las últimas 24 horas. Entonces calcula la media máxima diaria como la media de estas 24 muestras.

Sobre %:

Éste es el porcentaje de las muestras que estaban sobre el umbral configurado para el colector.

Error %:

Éste es el porcentaje de paquetes con errores. Una sonda del jitter señala varios tipos de errores:

- Pérdida del paquete SD — Packets Lost entre la fuente y el destino
- Pérdida del paquete DS — Packets Lost entre el destino y la fuente
- Busies — El número de ocasiones cuando una operación del Round-Trip Time (RTT) no podría ser iniciada porque una operación de RTT previa no había sido completada
- Secuencia — El número de realizaciones de la operación RTT recibidas con un identificador de secuencia inesperada. Éstas son algunas razones posibles por las que ésta pudo ocurrir: Un paquete duplicado fue recibido. Una respuesta fue recibida después de que tuviera

sincronizado-hacia fuera. Un paquete corrupto fue recibido y no detectado.

- Descensos — El número de ocasiones cuando ocurrió cualquiera de éstos: Una operación RTT no podría ser iniciada porque un cierto recurso interno necesario no estaba disponible (por ejemplo, memoria o el subsistema del [SNA] de la Arquitectura de red de sistemas) La realización de la operación no podía ser reconocida.
- MIA (Desaparecido en acción) — El número de paquetes se pierden que para que ninguna dirección puede ser determinada.
- Tarde — El número de paquetes que llegaron después del descanso.

La pregunta que surge de esta información es qué valores de error, fluctuación y retraso son aceptables en una red VoIP. Desafortunadamente, no hay respuesta sencilla a esta pregunta. Los valores aceptables dependen del tipo de códec, del tamaño del búfer de fluctuación y de otros factores. Además, hay interdependencias entre estas variables. Una mayor pérdida de paquetes puede significar que se tolerará un menor nivel de fluctuación.

El mejor método para obtener cifras de retardo y fluctuación factibles es comparar sitios similares en la misma red. Si los 192 Kbps-asociaron los sitios pero los valores de un jitter del informe alrededor del ms 50, y el jitter restante del ms de los informes 100 del sitio, después hay un problema, sin importar los valores nominales. El IPM puede proporcionar la medida en curso de la fluctuación y retraso 24x7 para toda la red, y puede proporcionar una línea de fondo para utilizar como la prueba patrón para las comparaciones de la fluctuación y retraso.

Los errores son diferentes, sin embargo. En principio, cualquier porcentaje de error con excepción de cero es una indicación roja. A los paquetes RTR se les da el mismo tratamiento QoS que a los paquetes de voz. Si la red QoS y el control de la admisión de llamada es robusta, ningún nivel de congestión debería causar la pérdida de paquetes o un retardo excesivo para los paquetes de voz o RTR. Por lo tanto, usted puede esperar que las cuentas de errores IPM sean cero. Los únicos errores que se podrían considerar “normales” son errores de la verificación por redundancia cíclica (CRC), pero éstos deben ser raros en una infraestructura de calidad. Si son frecuentes, constituyen un riesgo a la Calidad de voz.

[Información Relacionada](#)

- **Bibliografía recomendada:** [Troubleshooting de Cisco IP Telephony](#) 
- [Soporte Técnico y Documentación - Cisco Systems](#)