

Usando o Agente de Garantia de Serviço da Cisco e o Monitor de Desempenho Inter-redes para gerenciar a qualidade do software em redes de voz sobre IP

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Questões de QoS em uma rede VoIP](#)

[Controlando QoS com Cisco SAA e IPM](#)

[Projeto](#)

[Resultados](#)

[Informações Relacionadas](#)

[Introdução](#)

Este documento descreve o uso do Cisco Service Assurance Agent (SAA) e do Internetwork Performance Monitor (IPM) medir o Qualidade de Serviço (QoS) na Voz sobre redes IP (VoIP). Esta informação é baseada em um projeto de telefonia IP do mundo real. Este documento centra-se no aplicativo do Produtos, não sobre o Produtos ele mesmo. Você deve já ser familiar com Cisco SAA e IPM e ter o acesso à documentação do produto exigida. Veja a [informação relacionada](#) para referências à outra documentação.

Note: A funcionalidade SAA Cisco no software de Cisco IOS® foi sabida anteriormente como o Response Time Reporter (RTR).

Quando você está controlando uma rede voip de larga escala, você deve ter as ferramentas necessárias objetivamente monitora e relata na Qualidade de voz na rede. Não é praticável confiar no feedback de usuário apenas, porque está frequentemente subjetiva e incompleta. Problemas de qualidade de voz geralmente se originam de problemas de QoS da rede. Assim, quando você identifica questões de qualidade de voz, você precisa uma segunda ferramenta de controlar e monitorar a rede QoS. O exemplo neste documento usa Cisco SAA e IPM por esse motivo.

O Cisco Voice Manager (CVM) é usado com Telemate.net para controlar a Qualidade de voz. Relata na Qualidade de voz dos atendimentos através do prejuízo/fator de defeito planejando calculado (ICPIF) que está calculado por um Cisco IOS gateway para cada atendimento. Isto permite que a gerente de rede identifique os locais que sofrem da qualidade de voz deficiente.

Refira o [controlando a qualidade de voz com Cisco Voice Manager \(CVM\) e o Telemate](#) para mais informação.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não é restringido à versão de software ou hardware específica, mas os exemplos neste documento usam esta versão de software e hardware:

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Questões de QoS em uma rede VoIP

Diversos fatores podem degradar a Qualidade de voz em uma rede de voz empacotada:

- Perda de pacotes
- Atraso excessivo
- Atraso do sincronismo excessivo

É particularmente importante que você monitorea estas figuras numa base permanente, se os serviços de pacote comutado são usados em WAN (por exemplo, ATM, Frame Relay, ou IP Virtual Private Network). Há os cenários numerosos onde a congestão na rede do portador, o modelagem de tráfego desconfigurado nos dispositivos de ponta, ou o policiamento desconfigurado no lado de portadora podem causar a perda de pacotes ou o buffer excessivo. Quando o portador está deixando cair pacotes, não há nenhuma evidência óbvia nos dispositivos de ponta. Consequentemente, você precisa uma ferramenta fim-a-fim como Cisco SAA que pode injetar o tráfego no ingresso e valida sua chegada bem-sucedida na saída.

Controlando QoS com Cisco SAA e IPM

Há três Cisco SAA e uns componentes IPM:

- Prova RTR
- Respondedor RTR
- Console do IPM

A prova de RTR envia um burst de pacotes ao respondedor de RTR. O respondedor RTR os recupera e os envia de volta para a prova. Esta operação simples permite que a ponta de prova meça a perda de pacotes e o retardo de round trip. Para medir o tremor, a ponta de prova envia

um pacote de controle ao que responde antes que inicie a intermitência de pacote de informação. O pacote de controle informa o que responde quantos milissegundos (Senhora) a esperar entre cada pacote na explosão. O respondedor mede o retardo entre pacotes durante a intermitência e qualquer desvio do intervalo esperado é registrado como atraso de sincronismo.

O console IPM controla o monitoramento de QoS. Programa as pontas de prova RTR com a informação relevante através do Simple Network Management Protocol (SNMP). Também coleta os resultados via SNMP. Nenhuma configuração do IOS da Cisco da interface de linha de comando é exigida nas pontas de prova RTR.

Emita o comando global configuration do **que responde do rtr**, configurar manualmente os respondedores de RTR.

O RTR sonda e os que responde devem executar o Cisco IOS Software Release 12.0(5)T ou Mais Recente. A versão de manutenção mais recente do mainstream 12.1 é recomendada. O RTR sonda e os que responde nos exemplos neste documento estão executando a liberação 12.1(4). A versão IPM no uso é IPM 2.5 para o Windows NT. Uma correção de programa está disponível no cisco.com para esta versão. Esta correção de programa é importante, porque fixa um problema onde o IPM configure as pontas de prova RTR com uma configuração de precedência IP incorreta.

Projeto

Antes que você distribua Cisco SAA e solução IPM, você deve fazer algum trabalho do projeto com estas considerações na mente:

- Colocação de pontas de prova e de que responde RTR
- Tipo de tráfego que é enviado da ponta de prova ao que responde

Há um número de coisas a tomar na consideração quando você decide sobre a colocação das pontas de prova e dos que responde. Primeiramente, você quer que a medição de QoS abranja todos as estações, e não somente as estações com problemas. Isto é porque os números do retardo e tremulação que os relatórios IPM para um local dado são os mais úteis quando comparados a outros locais na mesma rede. Assim, você quer medir locais com bom QoS e o QoS deficiente. Também, um local de funcionamento satisfatório pode tornar-se um local de execução amanhã, devido às mudanças nos testes padrão de tráfego ou nas alterações de rede. Você quer detectar este antes que afete a Qualidade de voz e for relatado pelos usuários.

Segundo, a utilização da CPU é importante. Já um roteador ocupado não pode prestar serviços de manutenção em tempo oportuno ao componente RTR, e este pode enviar os resultados. Também, se você coloca exemplos demais da ponta de prova em qualquer roteador único, você pode criar problemas da utilização elevada da CPU mesmo que nenhuns existissem antes. A aproximação escolhida para a rede de exemplo neste documento (e neste deve trabalhar na maioria de redes) é colocar as pontas de prova RTR no remoto/Roteadores secundários. Este Roteadores conecta tipicamente um único LAN relativamente a um serviço do WAN lento. Então, roteadores filiais costumam ter uma utilização de CPU muito baixa e podem facilmente lidar com RTR. O outro benefício deste projeto é que você distribui a carga através de tanto como Roteadores como possível. Mantenha na mente que é mais trabalho a ser uma ponta de prova do que para ser um que responde, como pontas de prova tomam uma certa quantidade de polling snmp.

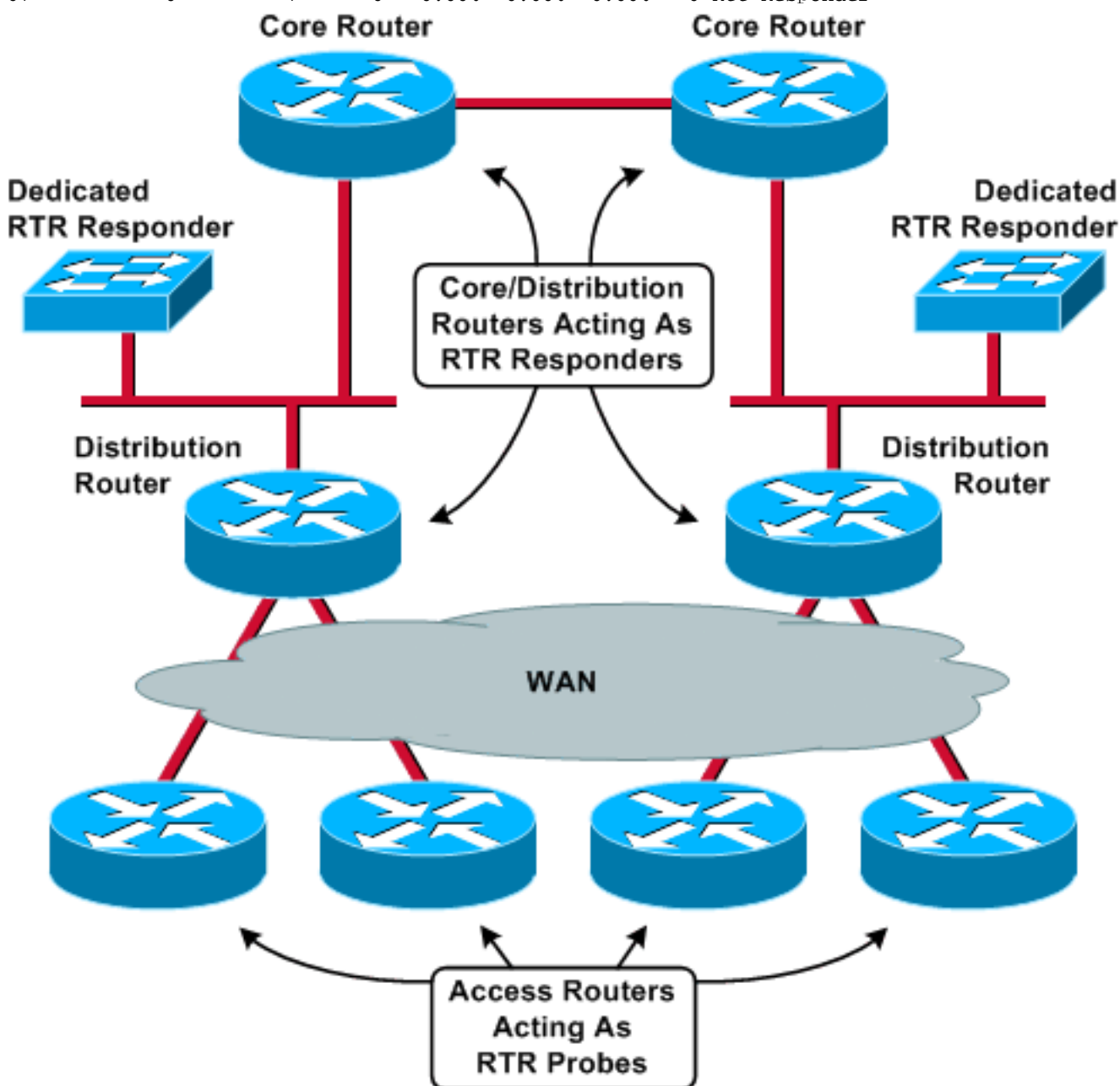
Com este projeto, os respondedores de RTR devem ser colocados no núcleo. Os que responde

serão mais ocupados do que as pontas de prova, porque estarão respondendo a muitas pontas de prova. Assim, um projeto robusto distribui os roteadores dedicados que atuam unicamente como que responde. A maioria de organizações aposentaram-se o Roteadores na prateleira que pode executar esta função. Qualquer roteador com uma interface Ethernet é suficiente. Alternativamente, o núcleo/roteadores de distribuição pode dobrar como que responde. O diagrama da rede nesta seção descreve ambas as encenações.

Espalhe a carga através de tanto Roteadores como possível, e monitore o USO de CPU RTR com 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



Quando você está combinando pontas de prova com os que responde, recomenda-se que você mantém uma topologia consistente entre a ponta de prova e o que responde. Por exemplo, todas as pontas de prova e que responde devem ser separados pelo mesmo número de Roteadores, de Switches, e de links MACILENTOS. Somente então podem os resultados IPM diretamente ser

comparados entre locais.

Neste exemplo, há 200 locais remotos e quatro sites central/de distribuição. Um Catalyst 4500 em cada centro de distribuição atua como um respondedor de RTR dedicado. Cada um dos 200 roteadores remotos atua como uma ponta de prova RTR. Cada ponta de prova visa o que responde que é ficado situado no centro de distribuição diretamente conectado.

As intermitências do tráfego enviado pelas sondas aos respondedores devem receber da rede os mesmos níveis de QoS atribuídos à voz. Isto pode significar que você tem que ajustar o low latency queueing (LLQ) ou configurações de prioridade do protocolo de tabela de roteamento (RTP) no roteador, de modo que o tráfego das pontas de prova RTR seja sujeito ao Enfileiramento de prioridade estrita. Quando você configurar a ponta de prova para pacotes RTP, simplesmente a porta do User Datagram Protocol (UDP) do destino pode ser controlada e não a porta de origem. Uma configuração de roteador típica LLQ nesta rede de exemplo tem as Listas de acesso que classificam especificamente os pacotes de RTR na mesma fila que a 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

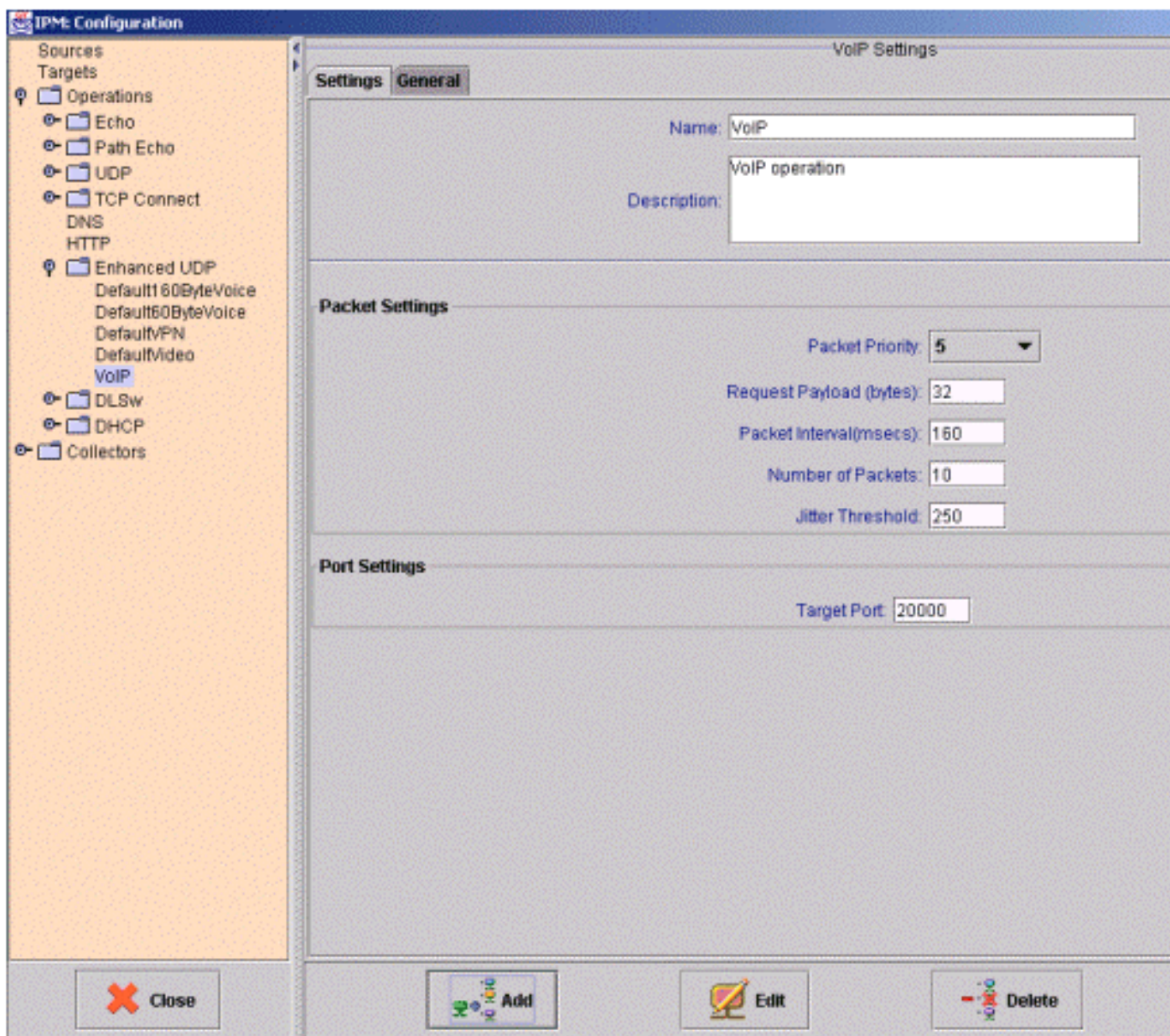
A lista de acesso IP-RTP tem estas linhas de classificação:

- `deny ip any any` Negue todo o fragmento IP, como uma lista de acessos da camada 4 permite implicitamente estes.
- `permit ip 10.0.16.0 0.255.239.255 32768` Permita a escala 16384 UDP 10.0.16.0 0.255.239.255 32768 a precedência da escala 16384 de 10.0.16.0 0.255.239.255 32768 crítica Permita pacotes RTP das sub-redes da Voz com a Precedência IP ajustada ao 5.
- `permit ip 10.0.16.0 0.255.239.255 32768` Permita o UDP toda a qualquer precedência do eq 20000 crítica Permita pacotes RTP da ponta de prova RTR que vai ao respondedor de RTR.
- `permit ip 10.0.16.0 0.255.239.255 32768` Permita o UDP todo o eq 20000 qualquer precedência crítica Permita pacotes RTP do respondedor de RTR que vai para trás à ponta de prova RTR.

Seja cuidadoso que a adição de tráfego RTR não faz com as filas LLQ sobre-estejam subscritas e façam com que os pacotes de voz reais estejam deixados cair. A operação do IPM do padrão **Default60ByteVoice** envia explosões dos pacotes RTP com estes parâmetros:

- Payload do pedido: 60 bytes **Note:** Esta é o cabeçalho de RTP e a Voz. Adicionar 28 bytes (IP/UDP) para obter o tamanho do datagrama L3.
- Intervalo: 20 ms
- Número de pacotes: 10

Isto significa que, durante uma explosão, o RTR consome 35.2 Kbs da largura de banda de LLQ. Se não houver largura de banda suficiente para o LLQ, crie então uma nova operação IPM e aumente o intervalo do pacote. Com os parâmetros mostrados nesta janela de configuração IPM, uma explosão consome os kbps somente 1 da largura de banda:



Resultados

A tabela nesta seção é um exemplo de um relatório IPM. Esse relatório contém três instâncias de prova de RTR. Mantenha na mente que uma ponta de prova física pode ser configurada com exemplos múltiplos da ponta de prova RTR que visam que responde diferentes ou usam cargas úteis diferentes.

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%

Estes são os significados de cada um das colunas:

Médio:

O IPM calcula uma média para cada hora de amostragem. Essas médias em horas são então calculadas em um período mais longo para obter-se médias diárias, semanais ou mensais. Ou seja para os relatórios diários, o IPM calcula a média para cada hora para as 24 horas passadas. Calcula então a média diária como a média destas 24 médias.

Méd. Máx.:

Este valor é a média de todos os máximos de hora em hora para cada dia, semana, e mês na carta. Ou seja para os relatórios diários, o IPM toma a amostra a maior relatada dentro de cada um das 24 horas passadas. Calcula então a média máxima diária como a média destas 24 amostras.

Sobre %:

Esta é a porcentagem das amostras que estavam sobre o limiar configurado para o coletor.

Erro %:

Esta é a porcentagem de pacotes que encontraram um erro. Uma ponta de prova do tremor relata diversos tipos de erros:

- Perda de pacotes SD — Packets Lost entre a fonte e o destino
- Perda de pacotes DS — Packets Lost entre o destino e a fonte
- Busies — O número de ocasiões quando uma operação do Round-Trip Time (RTT) não poderia ser iniciada porque uma operação RTT anterior não tinha sido terminada
- Sequência — O número de conclusões da operação RTT recebidas com um identificador de sequência inesperado. Estas são algumas razões possíveis pelas quais esta pôde

ocorrer:Um pacote duplicado foi recebido.Uma resposta foi recebida depois que teve programado-para fora.Um pacote corrompido foi recebido e não detectado.

- Gotas — O número de ocasiões quando qualquer uma destes ocorreu:Uma operação RTT não poderia ser iniciada porque alguns recursos internos necessários não estavam disponíveis (por exemplo, memória ou o subsistema do [SNA] da arquitetura de rede de sistemas)A conclusão da operação não podia ser reconhecida.
- MIA (ausente em ação) — O número de pacotes que são perdidos para que nenhum sentido pode ser determinado.
- Tarde — O número de pacotes que chegaram após o intervalo.

A questão que surge dessas informações é que os valores de retardo, atraso de sincronismo e erro são aceitáveis em uma rede VoIP. Infelizmente, não há nenhuma resposta simples a esta pergunta. Os valores aceitáveis dependem do tipo de codec, da variação de sinal, do tamanho do buffer e de outros fatores. Além, há umas interdependências entre estas variáveis. Uma perda de pacotes mais alta pode significar uma tolerância menor a variações de sinal.

A melhor forma de obter cenários de retardo trabalháveis e de sincronismo é comparar os sites semelhantes nessa mesma rede. Se todos os 192 Kbps-anexaram locais mas valores de um tremor do relatório em torno da Senhora dos 50 pés, e o tremor restante da Senhora dos relatórios 100 do local, a seguir há um problema, apesar dos valores nominais. O IPM pode fornecer medida em curso do retardo e tremulação 24x7 para a toda a rede, e pode fornecer uma linha de base para usar-se como a avaliação de desempenho para comparações do retardo e tremulação.

Os erros são uns diferentes, contudo. Em princípio, qualquer porcentagem de erro a não ser zero é um flag vermelho. O mesmo tratamento de QoS é dado para pacotes de RTR como pacotes de voz. Se a rede QoS e o controle de admissão de chamada forem robustos, nenhum nível de congestionamento deverá causar a perda de pacote ou o retardo excessivo de pacotes de voz ou RTR. Conseqüentemente, você pode esperar os contagens de erro IPM ser zero. Os únicos erros que poderiam ser considerados “normal” são erros da verificação de redundância cíclica (CRC), mas estes devem ser raros em uma infraestruturade qualidade. Se são frequentes, constituem um risco à Qualidade de voz.

[Informações Relacionadas](#)

- **Leitura Recomendada:** [Troubleshooting da Telefonia IP Cisco](#) 
- [Suporte Técnico e Documentação - Cisco Systems](#)