Verwendung von Cisco Service Assurance Agent und Internetwork Performance Monitor zur Verwaltung der Quality of Service in Voice over IP-Netzwerken

Inhalt

Einführung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Konventionen
QoS-Probleme in einem VoIP-Netzwerk
Management von QoS mit Cisco SAA und IPM
Design
Ergebnisse
Zugehörige Informationen

Einführung

Dieses Dokument beschreibt die Verwendung von Cisco Service Assurance Agent (SAA) und Internetwork Performance Monitor (IPM) zur Messung der Quality of Service (QoS) in VoIP-Netzwerken. Diese Informationen basieren auf einem echten IP-Telefonieprojekt. Dieses Dokument konzentriert sich auf die Anwendung der Produkte, nicht auf die Produkte selbst. Sie sollten bereits mit Cisco SAA und IPM vertraut sein und Zugriff auf die erforderliche Produktdokumentation haben. Siehe Verwandte Informationen für Verweise auf andere Dokumentation.

Hinweis: Die Cisco SAA-Funktion in der Cisco IOS®-Software war zuvor als Response Time Reporter (RTR) bekannt.

Wenn Sie ein umfangreiches VoIP-Netzwerk verwalten, müssen Sie über die erforderlichen Tools verfügen, um die Sprachqualität im Netzwerk objektiv zu überwachen und Berichte darüber zu erstellen. Es ist nicht möglich, sich nur auf das Feedback der Benutzer zu verlassen, da es oft subjektiv und unvollständig ist. Probleme bei der Sprachqualität sind in der Regel auf QoS-Probleme im Netzwerk zurückzuführen. Wenn Sie Probleme bei der Sprachqualität identifizieren, benötigen Sie ein zweites Tool, um die Netzwerk-QoS zu verwalten und zu überwachen. Im Beispiel in diesem Dokument werden dazu Cisco SAA und IPM verwendet.

Cisco Voice Manager (CVM) wird zusammen mit Telemate.net für die Verwaltung der Sprachqualität verwendet. Die Sprachqualität von Anrufen wird über den Impairment/Calculated Planning Impairment Factor (ICPIF) gemeldet, der von einem Cisco IOS-Gateway für jeden Anruf

berechnet wird. So kann der Netzwerkmanager Standorte identifizieren, die unter schlechter Sprachqualität leiden. Weitere Informationen finden Sie unter Verwalten der Sprachqualität mit Cisco Voice Manager (CVM) und Telemate.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- oder Hardwareversionen beschränkt, die Beispiele in diesem Dokument verwenden jedoch die folgenden Software- und Hardwareversionen:

- Cisco IOS Softwareversion 12.1(4)
- IPM 2.5 für Windows NT
- Catalyst Switch der Serie 4500

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

QoS-Probleme in einem VoIP-Netzwerk

Eine Reihe von Faktoren können die Sprachqualität in einem Sprachnetzwerk beeinträchtigen:

- Paketverlust
- Übermäßige Verzögerung
- Übermäßiger Jitter

Es ist besonders wichtig, dass Sie diese Zahlen kontinuierlich überwachen, wenn im WAN Paketvermittlungsdienste (z. B. ATM, Frame Relay oder IP Virtual Private Network) verwendet werden. Es gibt zahlreiche Szenarien, in denen Überlastungen im Carrier-Netzwerk, falsch konfiguriertes Traffic-Shaping auf den Edge-Geräten oder falsch konfigurierte Richtlinien auf der Carrier-Seite Paketverluste oder übermäßige Pufferung verursachen können. Wenn der Carrier Pakete verwirft, gibt es keine offensichtlichen Hinweise auf die Edge-Geräte. Aus diesem Grund benötigen Sie ein End-to-End-Tool wie die Cisco SAA, das den Datenverkehr an den Eingang einspeist und die erfolgreiche Ankunft am Ausgang validiert.

Management von QoS mit Cisco SAA und IPM

Es gibt drei Komponenten von Cisco SAA und IPM:

- RTR-Sonde
- RTR-Responder
- IPM-Konsole

Die RTR-Sonde sendet einen Burst von Paketen an den RTR-Responder. Der RTR-Responder

dreht sie um und sendet sie zurück an die Sonde. Dieser einfache Vorgang ermöglicht der Sonde die Messung von Paketverlusten und Round-Trip-Verzögerungen. Um Jitter zu messen, sendet die Sonde ein Kontrollpaket an den Responder, bevor es den Paket-Burst initiiert. Das Steuerungspaket informiert den Responder darüber, wie viele Millisekunden (ms) zwischen jedem Paket im Burst zu erwarten sind. Der Responder misst dann die Verzögerung zwischen den Paketen während des Bursts, und jede Abweichung vom erwarteten Intervall wird als Jitter aufgezeichnet.

Die IPM-Konsole steuert die QoS-Überwachung. Die RTR-Tests werden mithilfe des Simple Network Management Protocol (SNMP) mit relevanten Informationen programmiert. Die Ergebnisse werden auch über SNMP erfasst. Für die RTR-Tests ist keine Cisco IOS-Konfiguration für die Befehlszeilenschnittstelle erforderlich.

Geben Sie den globalen Konfigurationsbefehl **rtr responder** ein, um die RTR-Responder manuell zu konfigurieren.

Die RTR-Tests und -Responder müssen die Cisco IOS Software Version 12.0(5)T oder höher ausführen. Die neueste Wartungsversion von 12.1 Mainstream wird empfohlen. Die RTR-Tests und -Responder in den Beispielen in diesem Dokument laufen auf Version 12.1(4). Die verwendete IPM-Version ist IPM 2.5 für Windows NT. Für diese Version ist ein Patch auf Cisco.com verfügbar. Dieser Patch ist wichtig, da er ein Problem behebt, bei dem IPM die RTR-Tests mit einer falschen IP Precedence-Einstellung konfiguriert.

Design

Bevor Sie eine Cisco SAA- und IPM-Lösung bereitstellen, müssen Sie bei der Planung folgende Aspekte berücksichtigen:

- Positionierung von RTR-Sonden und Einsatzkräften
- Datenverkehrstyp, der von der Sonde an den Responder gesendet wird

Es gibt eine Reihe von Aspekten, die Sie berücksichtigen sollten, wenn Sie über die Anordnung von Sonden und Einsatzkräften entscheiden. Zunächst sollten die QoS-Messungen alle Standorte abdecken, nicht nur Problemstandorte. Der Grund hierfür ist, dass die von IPM für eine bestimmte Site gemeldeten Verzögerungen und Jitter im Vergleich zu anderen Standorten im gleichen Netzwerk am nützlichsten sind. Daher sollten Standorte mit guter QoS *und* schlechter QoS gemessen werden. Zudem kann eine leistungsstarke Website morgen aufgrund von Änderungen der Datenverkehrsmuster oder Netzwerkänderungen zu einer schlecht funktionierenden Website werden. Sie sollten dies erkennen, bevor es sich auf die Sprachqualität auswirkt und von den Benutzern gemeldet wird.

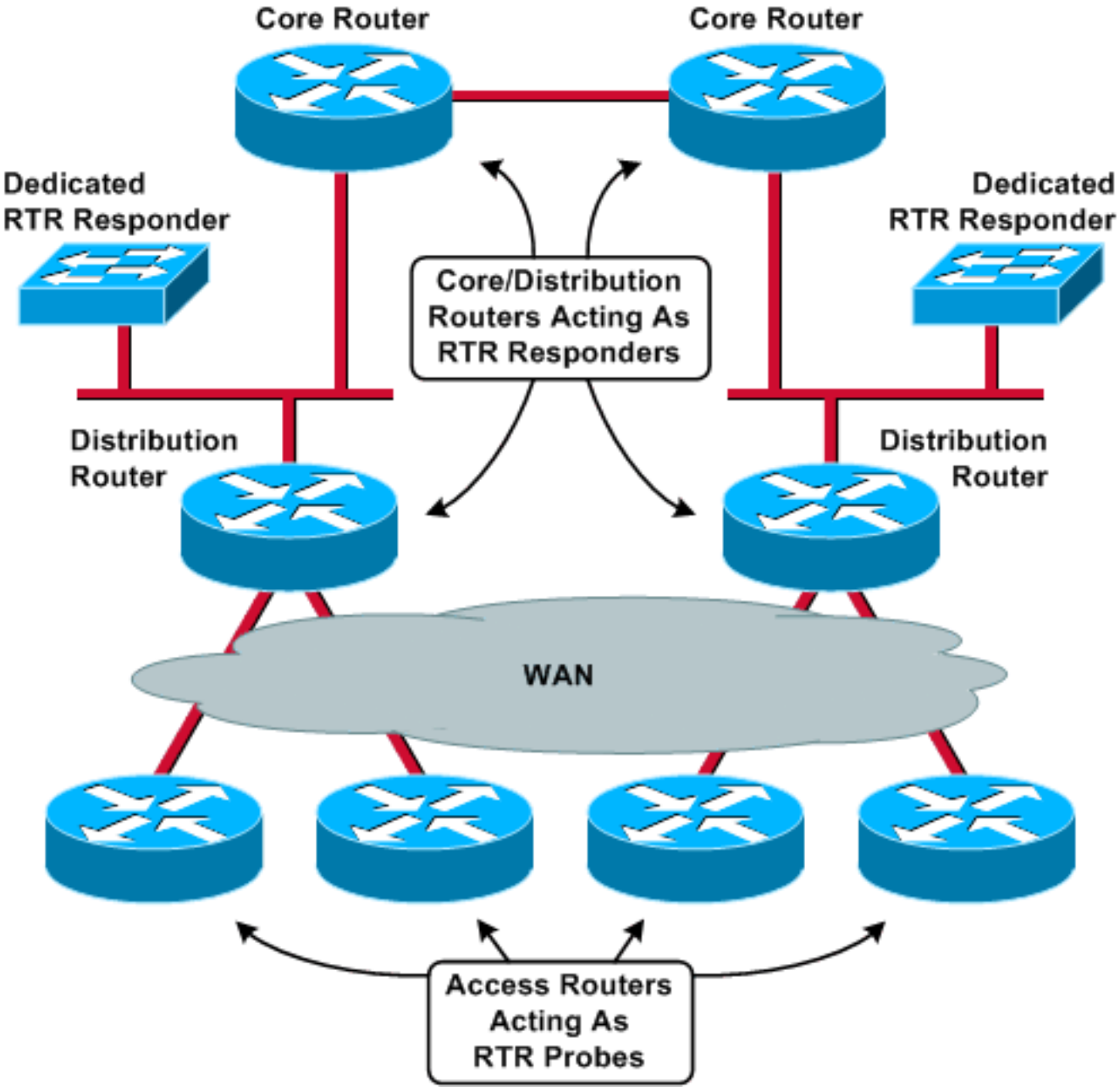
Zweitens ist die CPU-Auslastung wichtig. Ein bereits ausgelasteter Router kann die RTR-Komponente möglicherweise nicht rechtzeitig warten, was zu Verzerrungen der Ergebnisse führen kann. Wenn Sie zu viele Testinstanzen auf einem einzelnen Router platzieren, können Sie auch Probleme bei der CPU-Auslastung verursachen, obwohl noch keine vorhanden war. Der in diesem Dokument für das Beispielnetzwerk gewählte Ansatz (und dies sollte in den meisten Netzwerken funktionieren) besteht darin, die RTR-Tests auf den Routern der Außenstelle bzw. der Außenstelle zu platzieren. Diese Router verbinden in der Regel ein einzelnes LAN mit einem relativ langsamen WAN-Service. Daher verfügen Zweigstellen-Router häufig über eine sehr geringe CPU-Auslastung und können problemlos mit RTR arbeiten. Der andere Vorteil dieses Designs besteht darin, dass Sie die Last auf so viele Router wie möglich verteilen. Beachten Sie, dass es mehr darum geht, eine Anfrage zu stellen als ein Responder zu sein, da die Tests eine bestimmte Menge SNMP-Abfragen durchführen.

Bei diesem Design müssen die RTR-Responder im Core platziert werden. Die Einsatzkräfte werden mehr arbeiten als die Probes, weil sie auf viele Sonden reagieren werden. Bei einem robusten Design werden dedizierte Router bereitgestellt, die nur als Responder fungieren. Die meisten Unternehmen haben Router in der Regaleinheit eingestellt, die diese Funktion ausführen können. Jeder Router mit einer Ethernet-Schnittstelle reicht aus. Alternativ können Core-/Distribution-Router doppelt so viele Einsatzkräfte leisten wie Responder. Das Netzwerkdiagramm in diesem Abschnitt zeigt beide Szenarien.

Verteilen Sie die Last mit dem folgenden Befehl auf so viele Router wie möglich, und überwachen Sie die RTR-CPU-Auslastung:

```
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
```



Wenn Sie Tests mit Respondern abgleichen, wird empfohlen, eine konsistente Topologie zwischen Sonde und Responder beizubehalten. Beispielsweise sollten alle Sonden und Responder durch dieselbe Anzahl von Routern, Switches und WAN-Verbindungen getrennt

werden. Erst dann können die Ergebnisse von IPM direkt zwischen den Standorten verglichen werden.

In diesem Beispiel gibt es 200 Remote-Standorte und vier Core-/Distribution-Standorte. Ein Catalyst 4500 an jedem Vertriebsstandort fungiert als dedizierter RTR-Responder. Jeder der 200 Remote-Router dient als RTR-Anfrage. Jede Anfrage bezieht sich auf den Responder, der sich am direkt verbundenen Verteilungsstandort befindet.

Die Datenverkehrsspitzen, die von den Sonden an die Einsatzkräfte gesendet werden, müssen vom Netzwerk dieselben QoS-Level erhalten wie die Sprachübertragung. Dies kann bedeuten, dass Sie die Prioritätskonfigurationen für Low Latency Queueing (LLQ) oder Routing Table Protocol (RTP) auf dem Router anpassen müssen, sodass der Datenverkehr von den RTR-Datensammlern einer strikten Prioritätswarteschlange unterliegt. Wenn Sie die Anfrage für RTP-Pakete konfigurieren, kann nur der Ziel-UDP-Port (User Datagram Protocol) und nicht der Quellport gesteuert werden. Eine typische Konfiguration eines LLQ-Routers in diesem Beispiel verfügt über Zugriffslisten, die die RTR-Pakete gezielt in dieselbe Warteschlange wie Sprache klassifizieren:

```
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
```

Die IP-RTP-Zugriffsliste weist die folgenden Klassifizierungslinien auf:

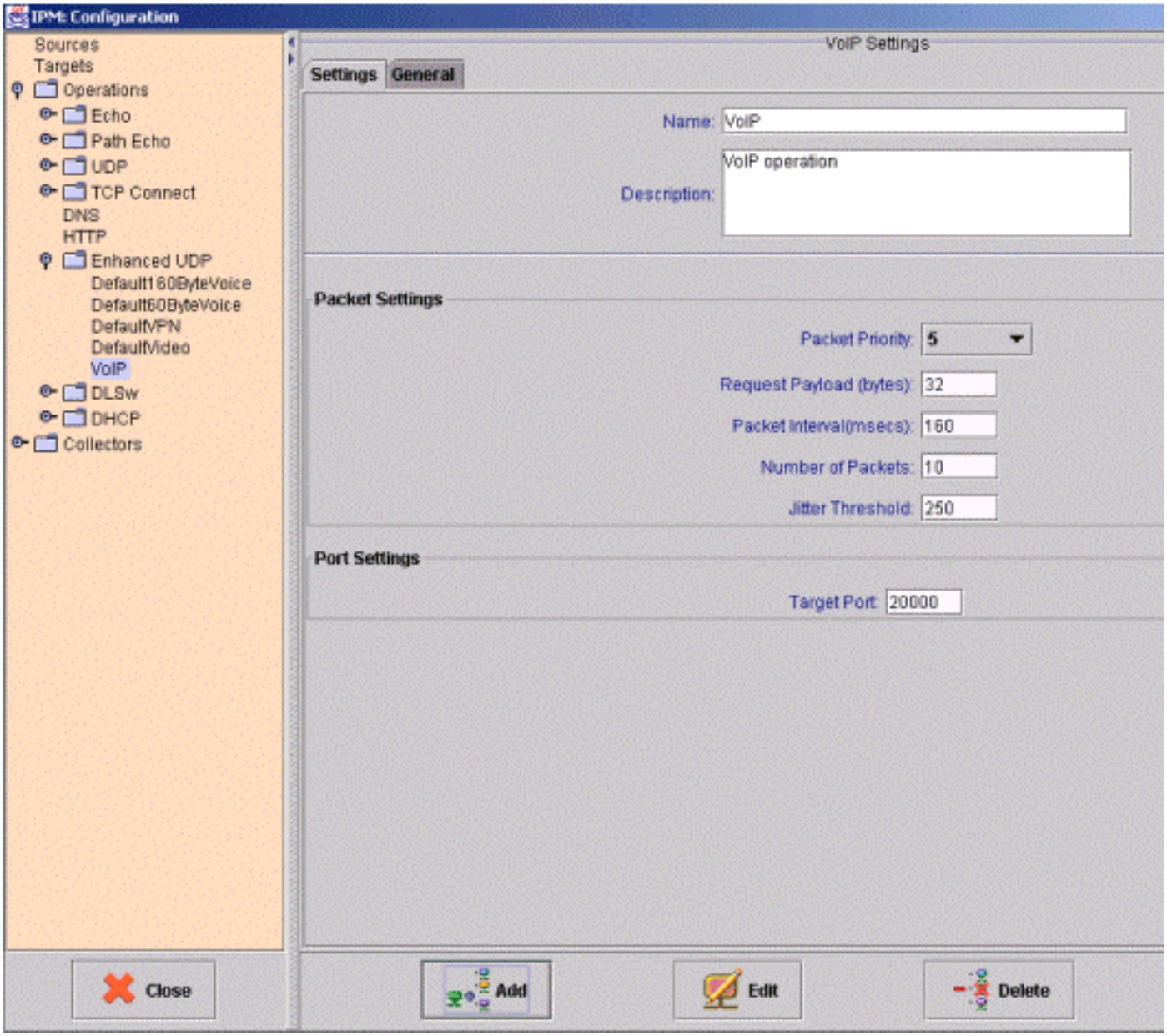
- `Fragmente ablehnen`Verweigern Sie jedes IP-Fragment, da eine Zugriffsliste für Layer 4 dies implizit zulässt.
- `permit udp 10.0.16.0 0.255.239.255 range 16384 32768 10.0.16.0 0.255.239.255 range 16384 32766 8 Rangfolgen entscheidend`RTP-Pakete von Sprach-Subnetzen mit IP-Rangfolge auf 5 zulassen.
- `permit udp any eq 2000 priority critical`RTP-Pakete von der RTR-Anfrage an den RTR-Responder senden.
- `zulässt udp alle EQ 2000 alle kritischen Vorrang`RTP-Pakete vom RTR-Responder können zurück zur RTR-Anfrage gesendet werden.

Achten Sie darauf, dass durch Hinzufügen von RTR-Datenverkehr die LLQ-Warteschlangen nicht überbelegt werden und echte Sprachpakete verworfen werden. Der standardmäßige **Default60ByteVoice** IPM-Vorgang sendet RTP-Pakete mit den folgenden Parametern, die zu Spitzenzeiten übertragen werden:

- Payload anfordern: 60 Byte**Hinweis:** Dies ist der RTP-Header und die Sprache. Fügen Sie 28 Byte (IP/UDP) hinzu, um die L3-Datagrammgröße abzurufen.
- Intervall: 20 ms
- Anzahl der Pakete: 10

Dies bedeutet, dass RTR während eines Bursts 35,2 Kbit/s an LLQ-Bandbreite beansprucht.

Wenn keine ausreichende Bandbreite für LLQ vorhanden ist, erstellen Sie einen neuen IPM-Vorgang und erhöhen das Paketintervall. Mit den in diesem IPM-Konfigurationsfenster angezeigten Parametern belegt ein Burst nur 1 Kbit/s Bandbreite:



Ergebnisse

Die Tabelle in diesem Abschnitt ist ein Beispiel für einen IPM-Bericht. Dieser Bericht enthält drei RTR-Testinstanzen. Beachten Sie, dass eine physische Sonde mit mehreren RTR-Testinstanzen konfiguriert werden kann, die auf unterschiedliche Einsatzkräfte abzielen oder unterschiedliche Payloads verwenden.

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%

Dies sind die Bedeutungen der einzelnen Spalten:

Durchschn.:

IPM berechnet einen Durchschnitt für jede Stunde der Probenahme. Diese stündlichen Durchschnittswerte werden dann über einen längeren Zeitraum gemittelt, um die täglichen, wöchentlichen oder monatlichen Durchschnittswerte zu erhalten. Mit anderen Worten berechnet IPM für den täglichen Bericht den Durchschnitt der letzten 24 Stunden für jede Stunde. Anschließend berechnet sie den Tagesmittelwert als den Durchschnitt dieser 24 Durchschnittswerte.

Durchschn. max.:

Dieser Wert ist der Durchschnitt aller Stundenmaximen für jeden Tag, jede Woche und jeden Monat im Diagramm. Mit anderen Worten: Für den täglichen Bericht nimmt IPM die größte Stichprobe ein, die innerhalb der letzten 24 Stunden gemeldet wurde. Anschließend berechnet er den täglichen Höchstwert als Durchschnitt dieser 24 Proben.

Mehr als %:

Dies ist der Prozentsatz der Stichproben, die den konfigurierten Grenzwert für den Collector überschritten haben.

Fehler %:

Dies ist der Prozentsatz der Pakete, bei denen ein Fehler aufgetreten ist. Ein Jitter-Test meldet verschiedene Fehlertypen:

- SD-Paketverlust - verlorene Pakete zwischen Quelle und Ziel
- DS-Paketverlust - verlorene Pakete zwischen Ziel und Quelle
- Busies - Die Anzahl der Fälle, in denen eine Round-Trip Time (RTT)-Operation nicht initiiert werden konnte, weil ein früherer RTT-Vorgang nicht abgeschlossen war

- Sequence (Folge) - Die Anzahl der RTT-Operationen, die mit einer unerwarteten Sequenzkennung abgeschlossen wurden. Dies sind einige mögliche Gründe dafür:Ein doppeltes Paket wurde empfangen.Nach Ablauf der Zeitspanne wurde eine Antwort empfangen.Ein beschädigtes Paket wurde empfangen und nicht erkannt.
- Drops (Verwerfen): Die Anzahl der Ereignisse, bei denen einer dieser Ereignisse aufgetreten ist:Ein RTT-Vorgang konnte nicht initiiert werden, da eine erforderliche interne Ressource nicht verfügbar war (z. B. Speicher oder das System Network Architecture (SNA)-Subsystem)Der Abschluss des Vorgangs konnte nicht erkannt werden.
- MIA (Missing in Action) (In Aktion fehlt): Die Anzahl der verlorenen Pakete, für die keine Richtung bestimmt werden kann.
- Verspätet - Die Anzahl der Pakete, die nach dem Timeout eintrafen.

Die Frage, die sich aus diesen Informationen ergibt, ist, welche Verzögerungs-, Jitter- und Fehlerwerte in einem VoIP-Netzwerk akzeptabel sind. Leider gibt es keine einfache Antwort auf diese Frage. Akzeptable Werte sind vom Codec-Typ, der Größe des Jitter-Puffers und anderen Faktoren abhängig. Darüber hinaus gibt es Wechselbeziehungen zwischen diesen Variablen. Ein höherer Paketverlust kann bedeuten, dass weniger Jitter toleriert werden kann.

Die beste Möglichkeit, zuverlässige Zahlen zu Verzögerungen und Jitter zu erhalten, besteht darin, ähnliche Standorte im gleichen Netzwerk zu vergleichen. Wenn alle 192 mit Kbit/s verbundenen Standorte, aber nur ein Bericht Jitter-Werte von etwa 50 ms und der verbleibende Standort 100 ms Jitter meldet, dann gibt es ein Problem, unabhängig von den Nominalwerten. IPM bietet eine kontinuierliche Messung von Verzögerungen und Jittern rund um die Uhr für das gesamte Netzwerk und kann als Vergleichsbasis für Verzögerungen und Jitter dienen.

Fehler sind jedoch anders. Grundsätzlich ist jeder Fehlerprozentsatz mit Ausnahme von Null eine rote Markierung. Den RTR-Paketen wird dieselbe QoS-Behandlung wie Sprachpakete gewährt. Wenn die Netzwerk-QoS und die Anrufzugangskontrolle stabil sind, darf keine Überlastung Paketverluste oder übermäßige Verzögerungen bei Sprach- oder RTR-Paketen verursachen. Daher können Sie davon ausgehen, dass die Anzahl der IPM-Fehler 0 beträgt. Die einzigen Fehler, die als "normal" angesehen werden können, sind CRC-Fehler (zyklische Redundanzprüfung), die jedoch in einer Qualitätsinfrastruktur selten vorkommen sollten. Wenn sie häufig auftreten, stellen sie ein Risiko für die Sprachqualität dar.

Zugehörige Informationen

- **Empfohlene Lektüre:** Fehlerbehebung bei Cisco IP-Telefonie
- Technischer Support und Dokumentation - Cisco Systems