Cisco サービス保証エージェントとインターネットワーク パフォーマンス モニタを使用した Voice over IP ネットワークの QoS 管理

内容

概要

このドキュメントでは、Cisco サービス保証エージェント（CSAA）とインターネットワーク パフォーマンス モニタ（IPM）を使用して、Voice over IP（VoIP）ネットワークの Quality of Service（QoS）を測定する方法について説明します。この情報は実際の IP テレフォニー プロジェクトに基づいています。このドキュメントでは、製品そのものではなく、製品のアプリケーションを中心に扱っています。ここでは、読者がすでに Cisco SAA と IPM について十分理解していて、必要な製品ドキュメントを使用できることを前提としています。その他の参考となるドキュメントについては、「関連情報」を参照してください。

注：Cisco IOS®ソフトウェアのCisco SAA機能は、以前はResponse Time Reporter(RTR)と呼ばれていました。

大規模なVoIPネットワークを管理する場合、ネットワーク内の音声品質を客観的に監視し、レポートするために必要なツールが必要です。多くの場合、主観的で不完全であるため、ユーザのフィードバックだけに頼ることは不可能です。一般に、音声品質の問題はネットワーク QoS の問題から生じます。したがって、音声品質の問題を特定する際には、ネットワークQoSを管理および監視するための2番目のツールが必要です。このドキュメントの例では、Cisco SAAとIPMを使用しています。

Cisco Voice Manager(CVM)は、音声品質を管理するためにTelemate.netとともに使用されます。各コールのCisco IOSゲートウェイによって計算されるImpairment/Calculated Planning Impairment Factor(ICPIF)を使用して、コールの音声品質をレポートします。ネットワーク管理者はこれを利用して、音声品質の悪いサイトを特定できます。詳細は、『Cisco Voice Manager(CVM)およびTelemateを使用した音声品質の管理』を参照してください。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントは、特定のソフトウェアまたはハードウェアのバージョンに限定されるものではありませんが、このドキュメントの例では、次のソフトウェアおよびハードウェアのバージョンを使用しています。

- Cisco IOS(R) ソフトウェア リリース 12.1(4)
- IPM 2.5 for Windows NT
- Catalyst 4500 シリーズ スイッチ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

VoIP ネットワークでの QOS 問題

パケット化された音声ネットワークでは、次のようないくつかの要因によって音声品質が劣化する可能性があります。

- パケット損失
- 過度の遅延
- 過度のジッタ

WANでパケット交換サービス（ATM、フレームリレー、IPバーチャルプライベートネットワークなど）が使用されている場合は、これらの数値を継続的に監視することが特に重要です。 キャリアネットワークの輻輳、エッジデバイスのトラフィックシェーピングの設定ミス、またはキャリア側のポリシングの設定ミスがパケット損失や過剰なバッファリングを引き起こすシナリオは数多くあります。キャリアがパケットをドロップしている場合、エッジデバイスに明らかな証拠はありません。したがって、Cisco SAAのようなエンドツーエンドのツールが必要です。このツールを使用すると、入力でトラフィックを注入し、出力での正常な着信を検証できます。

Cisco SAAおよびIPMによるQoSの管理

Cisco SAAおよびIPMには、次の3つのコンポーネントがあります。

- RTR プローブ
- RTR レスポンダ
- IPM コンソール

RTR プローブは RTR レスポンダにパケットのバーストを送信します。続いて RTR レスポンダはそれらのパケットを方向転換し、プローブに送り返します。この単純な操作を通じて、プローブはパケット損失と往復の遅延を測定します。ジッタを測定するために、プローブはパケットバーストを開始する前にレスポンダに制御パケットを送信します。制御パケットは、バースト内の各パケット間で予想されるミリ秒(ms)を応答側に通知します。レスポンダはバースト中にパケット

間の遅延を測定し、想定されている間隔からのずれがジッタとして記録されます。

IPM コンソールは QOS モニタリングを制御します。Simple Network Management Protocol (SNMP ; 簡易ネットワーク管理プロトコル) を介して、RTRプローブに関連情報をプログラムします。 また、SNMP 経由で結果を収集します。RTRプローブでは、コマンドラインインターフェイス(CLI)のCisco IOS設定は必要ありません。

rtr responderグローバル**設定コマンド**を発行して、RTRレスポンダを手動で設定します。

RTRプローブとレスポンダは、Cisco IOSソフトウェアリリース12.0(5)T以降を実行する必要があります。12.1 メインストリームの最新のメンテナンス リリースが推奨されます。このドキュメントの例にあるRTRプローブとレスポンダは、リリース12.1(4)を実行しています。 使用中のIPMバージョンは、IPM 2.5 for Windows NTです。このバージョンのパッチはCisco.comで入手できます。このパッチは、IPMが誤ったIP Precedence設定でRTRプローブを設定する問題を解決するため、重要です。

設計

Cisco SAAおよびIPMソリューションを導入する前に、次の点を考慮して設計作業を行う必要があります。

- RTR プローブおよびレスポンダの配置
- プローブからレスポンダに送信されるトラフィックタイプ

プローブとレスポンダの配置を決定する際には、考慮すべき事項がいくつかあります。まず、QOS 測定は問題のあるサイトだけでなく、すべてのサイトを対象にする必要があります。これは、IPMが特定のサイトに関してレポートする遅延とジッタの数が、同じネットワーク内の他のサイトと比較して最も有用であるためです。したがって、良好なQoSと低いQoSを持つサイトを測定する必要があります。また、トラフィックパターンの変化やネットワークの変化により、パフォーマンスの良いサイトが明日、パフォーマンスの悪いサイトになる可能性があります。これは、音声品質に影響を与え、ユーザから報告される前に検出する必要があります。

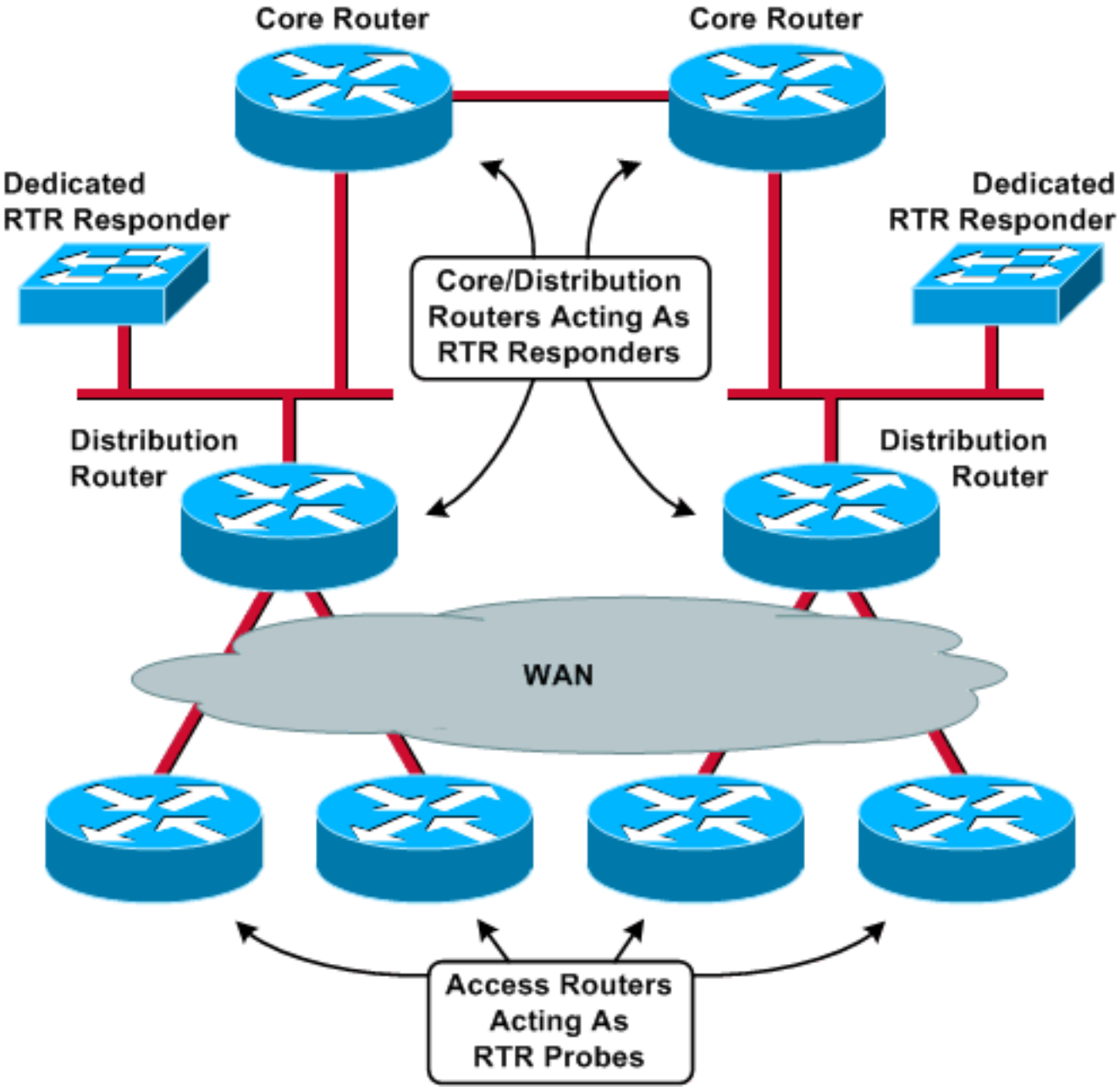
次に、CPU 使用率が重要です。すでにビジー状態のルータがRTRコンポーネントにタイムリーにサービスを提供できない可能性があり、結果が歪む可能性があります。また、1つのルータに多数のプローブインスタンスを配置すると、以前に存在するCPU使用率の高い問題が発生する可能性があります。このドキュメントの例のネットワークに対して選択したアプローチ (ほとんどのネットワークで動作します) は、RTRプローブをリモート/ブランチルータに配置することです。一般に、これらのルータは単一の LAN を比較的低速な WAN サービスに接続します。そのため、ブランチ ルータは CPU 使用率が低いことが多く、RTR に容易に対処できます。この設計のもう1つの利点は、できるだけ多くのルータに負荷を分散することです。プローブは特定の量のSNMPポーリングを受け取るため、レスポンダよりもプローブのほうが効率的であることに注意してください。

この設計では、RTRレスポンダをコアに配置する必要があります。レスポンダは多くのプローブに応答するため、プローブよりもビジーになります。したがって、堅牢な設計では、レスポンダとしてのみ動作する専用ルータを導入します。ほとんどの組織では、この機能を実行できるのに、使用していないルータがシェルフ内にあります。イーサネット インターフェイスを備えているすべてのルータを使用できます。または、コア/ディストリビューションルータをレスポンダとして2倍にすることもできます。このセクションのネットワーク図は、両方のシナリオを示しています。

できるだけ多くのルータに負荷を分散し、次のコマンドを使用してRTRのCPU使用率をモニタします。

```
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
```



プローブとレスポンダを照合する場合は、プローブとレスポンダの間で一貫したトポロジを維持することを推奨します。たとえば、プローブとレスポンダはすべて、同じ数のルータ、スイッチ、および WAN リンクによって区切られていることが望まれます。IPMの結果は、サイト間で直接比較できます。

この例では、200のリモートサイトと4つのコア/ディストリビューションサイトがあります。各ディストリビューションサイトのCatalyst 4500は、専用のRTRレスポンダとして機能します。200個の各リモートルータはRTRプローブとして機能します。各プローブは、直接接続されたディストリビューションサイトにあるレスポンダを対象としています。

プローブからレスポンダに送信されるトラフィックのバーストは、ネットワークによって、音声に与えられたものと同じ QOS レベルを与えられる必要があります。これは、RTRプローブからのトラフィックが完全優先キューイングの対象となるように、ルータの低遅延キューイング(LLQ)またはRouting Table Protocol(RTP)プライオリティ設定を調整する必要があることを意味し

ます。RTPパケットのプローブを設定する場合、送信元ポートではなく、宛先ユーザデータグラムプロトコル(UDP)ポートだけを制御できます。この例のネットワークの一般的なLLQルータ設定には、RTRパケットを音声と同じキューに特に分類するアクセスリストがあります。

```
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
```

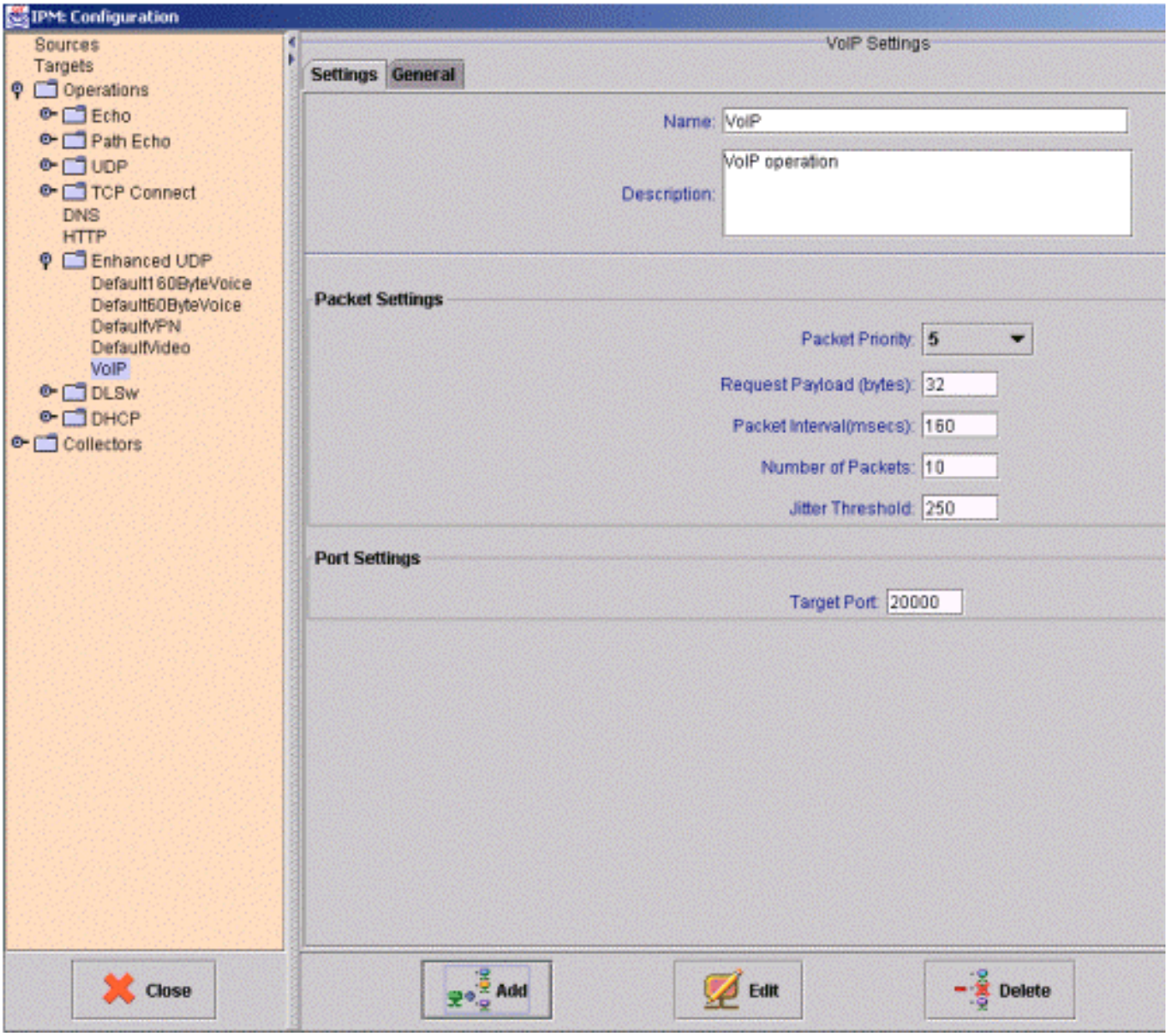
IP-RTPアクセスリストには、次の分類ラインがあります。

- `deny ip any any fragments`レイヤ4アクセスリストがこれらのフラグメントを暗黙的に許可するため、IPフラグメントを拒否します。
- `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`音声サブネットからの RTP パケットを許可し、IP 優先順位を 5 に設定します。
- `permit udp any any eq 20000 precedence critical`RTR プローブから RTR レスポンダに向かう RTP パケットを許可します。
- `permit udp any eq 20000 any precedence critical`RTR レスポンダから RTR プローブに向かう RTP パケットを許可します。

RTRトラフィックを追加しても、LLQキューがオーバーサブスクライブされたり、実際の音声パケットがドロップされたりすることはないことに注意してください。標準のDefault60ByteVoice IPM操作では、次のパラメータを使用してRTPパケットのバーストが送信されます。

- 要求ペイロード：60 bytes**注：**これはRTPヘッダーと音声です。28バイト(IP/UDP)を追加して、L3データグラムサイズを取得します。
- 間隔:20 ms
- パケット数：10

これは、バースト時にRTRがLLQ帯域幅の35.2 Kbsを消費することを意味します。LLQ 用に十分な帯域幅がない場合は、新しい IPM 操作を作成し、パケット間隔を増やします。このIPM設定ウィンドウに示されているパラメータでは、バーストが消費する帯域幅は1 Kbpsだけです。



成果

このセクションの表は、IPMレポートの例です。このレポートには、RTR プローブの 3 つのインスタンスが含まれています。1つの物理プローブに、異なるレスポンダを対象とする複数のRTRプローブインスタンスを設定したり、異なるペイロードを使用したりすることに注意してください。

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%

各カラムの意味は次のとおりです。

Avg:

IPM は 1 時間のサンプリングごとに平均を算出します。これらの毎時平均はさらに長い時間にわたって平均化され、日次、週次、または月次の平均が算出されます。つまり、日次レポートでは、過去24時間の各時間の平均が計算されます。次に、これらの24の平均の平均として日次平均を計算します。

Avg Max:

この値は、グラフの各日、週、および月のすべての時間単位の最大値の平均です。つまり、日次レポートでは、IPMは過去24時間以内に報告された最大のサンプルを取ります。次に、これらの24個のサンプルの平均として日次最大平均を計算します。

Over %:

これは、コレクタに設定されたしきい値を超えたサンプルの割合です。

Error %:

これは、エラーが発生したパケットのパーセンテージです。ジッタプローブは、次の複数のタイプのエラーを報告します。

- SDパケット損失：送信元と宛先の間でパケットが失われる
- DSパケット損失：宛先と送信元の間で失われたパケット
- [Busies]：以前のRTT操作が完了しなかったために、ラウンドトリップ時間(RTT)操作を開始できなかった回数
- Sequence：予期しないシーケンス識別子で受信されたRTT操作の完了の数。この問題が発生する可能性がある理由としては、次のものがあります。重複パケットを受信しました。タイムアウト後に応答を受信しました。破損したパケットが受信され、検出されませんでした。

- Drops：次のいずれかが発生した回数。必要な内部リソース(メモリやシステムネットワークアーキテクチャ(SNA)サブシステムなど)が利用できないため、RTT操作を開始できませんでした操作の完了を認識できませんでした。
- MIA(Missing in Action)：方向を判別できない損失パケットの数。
- Late：タイムアウト後に到着したパケットの数。

これらの情報から、VoIP ネットワークではどれくらいの遅延、ジッタ、および エラーの値が許容されるのかという疑問が生じます。残念ながら、この質問に対する簡単な答えはありません。許容される値は、コーデック タイプやジッタ バッファ サイズなどの要因によって異なります。さらに、これらの変数の間には相互依存関係があります。パケット損失が大きいほど、許容されるジッタは小さくなります。

実行可能な遅延とジッタの値を取得する最適な方法は、同じネットワーク内にある類似したサイトと比較することです。192 Kbps接続のサイトすべてで、1つのレポートのジッタ値が約50ミリ秒で、残りのサイトで100ミリ秒のジッタが報告された場合、公称値に関係なく問題があります。IPMは、ネットワーク全体で24時間365日の継続的な遅延とジッタの測定を可能にし、遅延とジッタの比較のベンチマークとして使用するベースラインを提供できます。

ただし、エラーは異なります。原則として、ゼロ以外のエラー率は赤いフラグです。RTR パケットには音声パケットと同じ QoS 処理が行われます。ネットワーク QoS とコール アドミッション制御が強固であれば、どのようなレベルの輻輳が生じても、音声または RTR パケットについてパケット損失や過度の遅延が起こることはありません。したがって、IPMエラーカウントがゼロであると予想できます。「正常」と見なされる可能性のあるエラーはCyclic Redundancy Check（CRC；巡回冗長検査）エラーだけですが、これらは品質インフラストラクチャでは稀です。頻繁に使用される場合、音声品質のリスクとなります。

関連情報

- **推奨文献：**Cisco IP Telephony のトラブルシューティング
- テクニカル サポートとドキュメント – Cisco Systems