CHAPTER 4

Cisco IPICS のインフラストラクチャに関する検討事項

この章では、Cisco IPICS を配置する上で注意する必要のあるインフラストラクチャの問題について説明します。

関連情報については、次のマニュアルを参照してください。

- IP マルチキャスト：『*Cisco IOS IP Multicast Configuration Guide, Release 12.4*』を参照してください。このマニュアルは次の URL から入手できます。
  http://www.cisco.com/en/US/products/ps6350/products_installation_and_configuration_guides_list.html
- QoS（Quality of Service）：『*Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.4*』を参照してください。このマニュアルは次の URL から入手できます。
  http://www.cisco.com/en/US/products/ps6350/products_installation_and_configuration_guides_list.html
- 音声の設定：『*Cisco IOS Voice Configuration Library*』を参照してください。このマニュアルは次の URL から入手できます。
  http://www.cisco.com/en/US/products/ps6350/products_installation_and_configuration_guides_list.html
- Hoot & Holler：『*Hoot & Holler Solution*』を参照してください。このマニュアルは次の URL から入手できます。
  http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns70/networking_solutions_package.html

この章では、次のトピックについて取り上げます。

WAN の考慮事項

Cisco IPICS を WAN に正しく配置するには、慎重な WAN の計画、設計、および実装が必要です。次の要素について、必ず検討してください。

- 遅延：2 サイト間の伝搬遅延は、1 km あたり 6 マイクロ秒です。この他のネットワーク遅延も発生する可能性があります。
- Quality of Service（QoS）：ネットワーク インフラストラクチャは、QoS 技術を使用して、一貫した予測可能なエンドツーエンド レベルのサービスをトラフィックに提供します。QoS が使用可能になった帯域幅を、ネットワーク インフラストラクチャに設計する必要があります。
- ジッタ：処理、キュー、バッファ、輻輳、またはパス変動遅延により、パケットがネットワークを介して受ける変動遅延です。マルチキャスト音声トラフィックのジッタは、Quality of Service（QoS）機能を使用して最小限に抑える必要があります。関連情報については、P.4-33 の「Quality of Service」を参照してください。
- パケットの損失およびエラー：ネットワークは、すべての音声トラフィックに対して、十分な優先順位付き帯域幅を提供するように設計される必要があります。標準的な QoS メカニズムを実装して、輻輳とパケット損失を回避する必要があります。関連情報については、P.4-33 の「Quality of Service」を参照してください。
- 帯域幅：予想されるコール ボリュームに対して、各サイト間で適切な帯域幅を提供してください。この帯域幅は、ネットワークを共有する他のアプリケーションおよびトラフィック用の帯域幅とは別に必要です。提供される帯域幅では、さまざまなクラスのトラフィックに優先順位付けとスケジューリングを行うために、QoS が使用可能になっていなければなりません。帯域幅は、一般的に多めに設定し、少なめにサブスクライブします。
- リモート ロケーションを使用する PMC：リモート ロケーションを選択した PMC は、SIP を使用して RMS への接続を確立します。SIP は構造上の遅延や大幅な伝送遅延の影響を受けやすいため、この種類の接続では、タイムアウトが発生することや、コールの確立に失敗することがあります。WAN 上に配置された PMC を使用していて接続性やオーディオ品質に問題があるときは、問題箇所を分離してみます。WAN 上に配置されていない、リモート PMC 接続をテストして問題を切り分けすることをお勧めします。WAN 上に配置されていない PMC で問題が再現されなかった場合は、WAN のインフラストラクチャを調査することをお勧めします。WAN での大幅な遅延やリソース不足が、問題の原因になっていないかどうかを確認します。

マルチキャスト ルーティング

シスコでは、sparse モード（SM）と dense モード（DM）の両方の Protocol Independent Multicast（PIM）ルーティング プロトコルをサポートしています。ただし、DM PIM は定期的にブロードキャストとプルーニングを実行するため、DM PIM を実稼働ネットワークで使用することはお勧めしません。

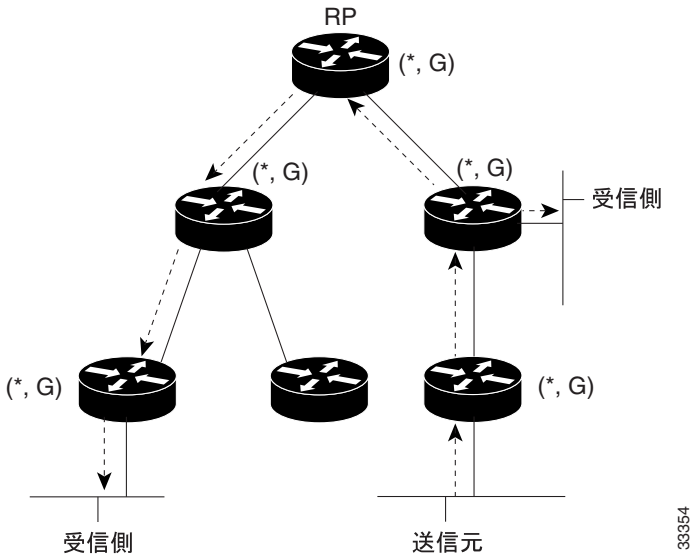
シスコは、Cisco IPICS には双方向 PIM を使用することをお勧めします。双方向 PIM は PIM プロトコル スイートを拡張したもので、双方向のデータ フローを使用した共有の希薄ツリーを実装します。PIM sparse モードとは異なり、双方向 PIM では、送信元固定状態情報をルータ内に保持しません。また、ツリーの送信元を任意の数に拡張でき、この場合の追加オーバーヘッドはごくわずかしか発生しません。

PIM SM で作成される共有ツリーは、単方向です。したがって、共有ツリーのルートである Rendezvous Point（RP; ランデブー ポイント）にデータ ストリームを伝送するには、送信元ツリーを作成する必要があります。ツリーを作成すると、ブランチを通じて下流方向の受信者にデータを転送できます。単方向モードでは、送信元データを共有ツリーの上流にある RP に伝達できません。

双方向モードでは、グループの RP をルートとする双方向共有ツリーだけにトラフィックがルーティングされます。双方向 PIM の場合、RP の IP アドレスは、この IP アドレスをルートとするすべてのルータがループなしのスパニング ツリー トポロジを確立するためのキーとして機能します。この IP アドレスは、ルータである必要はありません。PIM ドメインのどの位置からも到達できる、ネットワークでまだ割り当てられていない任意の IP アドレスを使用できます。

図 4-1 は、双方向共有ツリーを示しています。この例の場合、送信元からのデータは、共有ツリー (*, G) の上流方向に RP まで伝送されてから、共有ツリーの下流方向に流れて受信者まで到達します。送信元ツリー (S, G) を作成するための登録プロセスはありません。

図 4-1　双方向共有ツリー



双方向 PIM は PIM SM のメカニズムから派生したもので、共有ツリーの動作は多くの点で同一です。双方向 PIM では、送信元トラフィックを共有ツリー上の RP アップストリームに無条件で転送することもできます。PIM SM で提供される送信元の登録プロセスはありません。(*, G) マルチキャスト ルーティング エントリだけに基づいてすべてのルータにトラフィックを転送できるようにするには、この変更は必要かつ十分です。双方向 PIM では送信元固定状態情報が不要であり、送信元を任意の数まで拡張することができます。

Cisco IPICS 環境において、双方向 PIM は次の方法でスケーラビリティの問題を解決します。

- 共有ツリー (*, G) に基づくトラフィック転送: この機能を利用すると、チャネルごとにルーティング エントリを 1 つ作成するだけで、マルチキャスト ルーティング テーブルを拡張できます。SM の場合は、グループおよび送信元ごとにルーティング エントリが作成されます。したがって、たとえば、チャネルに 100 人の参加者がいる場合は、101 個のマルチキャスト ルーティング エントリがルーティング テーブル内に作成されます。双方向 PIM を使用する場合は、参加者の数にかかわらず、ルーティング テーブルにマルチキャスト ルーティング エントリが 1 つ作成されるだけです。
- RP へのルートに基づく Reverse Path Forwarding（RPF）の決定 : SM では、フローの送信元アドレスに基づいて (S, G) エントリの RPF が決定されます。双方向 (*, G) では、RP に基づいて RPF が決定されます。この機能により、Cisco IPICS Permanent Virtual Circuit（PVC; 相手先固定接続）上でマルチキャスト トラフィックを伝送するための ip mroute エントリを数百個も設定する必要がなくなります。双方向の場合、Cisco IPICS PVC 上でマルチキャスト トラフィックを伝送するには、ユニキャスト ルーティング プロトコルをチューニングして、RP に到達するための最善ルートとして Cisco IPICS PVC を優先指定する必要があります。

Auto-RP および 12.2(7) より前の Cisco IOS リリースを使用している場合は、sparse dense モードが必要です。Auto-RP および 12.2(7) 以降の Cisco IOS リリースを使用している場合は、**sparse mode** コマンドと **ip pim auto rp listener** コマンドを使用します。auto-rp 以外のマルチキャスト タイプでは、sparse mode を使用できます。

帯域幅の計画

Cisco IPICS を運用するための十分な帯域幅を確保するには、ネットワークを計画および配置する際に、次の事項を検討します。これらの検討事項には、次のものがあります。

- VoIP で使用されるコーデック：P.4-5 の「コーデック」を参照
- 混合される音声ストリームの数：P.4-10 の「音声ストリームの混合」を参照

また、VoIP ネットワークで使用可能な保証帯域幅について検討する必要があります。LAN と WAN の両方の帯域幅を考慮に入れ、フレームリレー、Committed Information Rate（CIR; 認定情報レート）、非同期転送モード ピーク セル レート（ATM PCR）、平均セル レート、バーストなどの要素も考慮します。詳細については、P.4-33 の「Quality of Service」を参照してください。

コーデック

Cisco IPICS は、G.711 コーデックまたは G.729a コーデックのいずれかを使用します。この項では、コーデックに関する次の事項について説明します。

- コーデックの選択（P. 4-5）
- コーデックによる帯域幅使用量の計算（P. 4-6）

（注）　Cisco IPICS ポリシー エンジンは、G.711 u-law に限りサポートします。ポリシー エンジンを使用する場合は、このコーデックを使用する必要があります。

コーデックの選択

Cisco IPICS で使用するコーデックを選択する際は、表 4-1 で説明する事項を考慮してください。

表 4-1　コーデックに関する検討事項

	G.711	G.729a
遅延	• 遅延の合計は、G.729a よりも 1 サンプルあたり 25 ms 小さくなります。 • トランスコーディングによって遅延が増大します。	• 遅延の合計は、G.711 よりも 1 サンプルあたり 25 ms 大きい。 • G.729a を使用する Cisco IPICS 環境の一部では、追加のトランスコーディングを実行して、G.729a ストリームを混合のために G.711 ストリームに変換する必要があります。この追加の DSP 処理によって、遅延が大幅に増大します。

表 4-1　コーデックに関する検討事項（続き）

	G.711	G.729a
音声品質	• VoIP の状態が良好である場合は、Mean Opinion Score（MOS; 平均オピニオン評点）で 4.1 を安定して維持できます。 • タンデム符号化に強いため、トランスコーディングによる音声品質の低下はありません。	• VoIP の状態が良好である場合、MOS は通常 3.7 になりますが、この値は G.711 よりも安定しない可能性があります。 • パケット損失が発生している状況では、G.711 と同等のパフォーマンスは維持されません。たとえば、3% の割合でパケットが損失している場合、G.711 で同様のパケット損失が発生しているときよりも音声品質への影響が大きくなることがあります。 • タンデム符号化に対して、G.711 と同等の耐性はありません。 • トランスコーディングによって、音声品質が MOS 値で 3.7 から 3.2 に低下します。
帯域幅	• 通常、G.729a の 3 倍の帯域幅を消費します。	• G.711 よりも帯域幅を節約できます。 • WAN 経由でサイトに接続する Cisco IPICS 環境の場合は、G.729a を使用することで WAN 帯域幅の消費が少なくなり、WAN のコストも削減できます。

コーデックによる帯域幅使用量の計算

この項では、コーデックに使用される帯域幅を計算する方法について説明します。

デフォルトでは、Cisco IOS はすべての VoIP トラフィック（つまり、RTP を使用するメディア トラフィック）を 50 パケット / 秒で送信します。各パケットには、音声サンプルの他に、IP、UDP、および RTP のヘッダーが含まれており、これらのヘッダーによりパケットに 40 バイトが付加されます。また、レイヤ 2 ヘッダー（フレームリレー、ポイントツーポイント プロトコル、イーサネットなど）のバイト数も各パケットに付加されます。

VoIP コールによって消費される帯域幅の量は、使用されるコーデックに依存し、次のように計算できます。消費される実際の帯域幅を特定するには、レイヤ 2 ヘッダーの適切なバイト数も加算する必要があります。

G.729a（8 KB CS-ACELP）

50 パケット / 秒

20 ms サンプル / パケット = 20 バイト

AP/UDP/RTP ヘッダー / パケット = 40 バイト

（20 バイト［ペイロード］+ 40 バイト［ヘッダー］）* 50 パケット/秒 = 3,000 バイト * 8 ビット = 24 Kbps

G.711（64 KB PCM）

50 パケット / 秒

20 ms サンプル / パケット = 20 バイト

AP/UDP/RTP ヘッダー / パケット = 40 バイト

（160 バイト［ペイロード］+ 40 バイト［ヘッダー］）* 50 パケット / 秒 = 10,000 バイト * 8 ビット = 80 Kbps

表 4-2 に、帯域幅の消費量の例を示します。詳細は次のとおりです。

- この例では、ペイロードのサイズ（バイト数）を 1 パケットあたり 20 ms サンプル、1 秒あたり 50 パケットとしています。
- 値 *n* は、セッションの音声ストリームの数と同じです。
- 帯域幅の計算では、合算帯域幅に IP/UDP/RTP ヘッダー（40 バイト）が含まれます。
- Compressed RTP（cRTP; RTP ヘッダー圧縮）により、IP/UDP/RTP ヘッダーは 1 パケットあたり 2 ～ 4 バイトに縮小します。圧縮後の帯域幅の計算では、1 パケットあたりの圧縮 IP/UDP/RTP ヘッダーを 4 バイトとしています。
- 消費される実際の帯域幅を特定するには、レイヤ 2 ヘッダーの適切なバイト数を加算する必要があります。

表 4-2　帯域幅の使用量の例

コーデック	ペイロードのサイズ（バイト数）	帯域幅 / 音声ストリーム（Kbps）		Cisco IPICS セッションごとの RTCP 帯域幅（Kbps）	例：セッション内の 1 つの音声ストリーム（Kbps）	
		無圧縮	圧縮		無圧縮	圧縮
G.729a	20	24	9.6	3.6	27.6	13.2
G.711	160	80	65.6	12.0	92.0	77.6

RFC 1889（『*RTP: A Transport Protocol for Real-Time Applications*』）に従って、RTP ストリームの RTCP トラフィックは最大で音声ストリームの 5%（RTP + RTCP）に制限されています。この制限は、Cisco IPICS セッションに参加する 3 つのストリームに適用されます。このため、「Cisco IPICS セッションごとの RTCP 帯域幅（Kbps）」は音声ストリームごとの帯域幅を 3 倍し、その積を 0.05 倍して計算されています。

キャンパス ネットワーク内部の Cisco IPICS ネットワークを設計する場合、帯域幅に関係する問題は発生しません。これは、IP マルチキャストを使用して音声ストリームを複製し、IP マルチキャスト グループにマッピングしているためです。IP マルチキャスト グループでは RMS リソースが使用されません。マルチキャストが使用可能になっていない WAN を経由してリモート ユーザが接続する場合は、RMS がマルチキャスト ストリームを IP ユニキャスト ストリームに変換し、WAN の帯域幅を節約します。IP ユニキャスト音声ストリームが RMO に到達すると、RMS は IP ユニキャスト ストリームをマルチキャスト ストリームに変換します。音声ストリームが WAN を通過するときは、RMS リソースが使用されます。このシナリオでは、RMS ゲートウェイは M1:U12:M2 接続トランク用に設定されます。詳細については、P.7-14 の「M1:U12:M2 接続トランク」を参照してください。

WAN に配置された PMC が帯域幅に及ぼす影響の例として、40 人の PMC ユーザが WAN を通じて通信するとします。各マルチキャスト音声ストリームは、IP ユニキャスト ストリームとして伝送できるように IP ユニキャスト音声ストリームに変換されますが、このシナリオの場合、チャネル数および各 PMC で使用されるコーデックのタイプによっては、それでも膨大な帯域幅が必要です。この例では、帯域幅の要件は次のようになります。

G.729a

40 人の PMC ユーザ x ユーザごとに 8 チャネル x (24 Kbps + 3.6 Kbps) = 8.832 Kbps

G.711

40 人の PMC ユーザ x ユーザごとに 8 チャネル x (80 Kbps + 12 Kbps) = 29,440 Kbps

（注）　各 Cisco IPICS ダイヤル エンジン ポートは G.711 コーデックを使用します。帯域幅の計算では、Cisco IPICS サーバと接続エンドポイント間の G.711 接続を考慮する必要があります。

cRTP、可変ペイロード サイズ、およびアグレッシブ VAD

コールが消費する帯域幅を変更するには、いくつかの方法があります。たとえば、次のような方法があります。

- RTP ヘッダーの圧縮（P. 4-8）
- 音声ペイロードの調整可能なバイト サイズ（P. 4-8）
- アグレッシブ音声アクティビティ検出（P. 4-9）

RTP ヘッダーの圧縮

P.4-5 の「コーデック」で説明したように、IP/UDP/RTP ヘッダーによって各パケットに 40 バイトが加わります。しかし、パケットのヘッダーは、コールの終了まで通常は変化しません。VoIP コールに対して cRTP を有効にすると、IP/UDP/RTP ヘッダーのサイズを 1 パケットあたり 2 ～ 4 バイトに縮小できます。

cRTP の詳細については、『*Understanding Compression (Including cRTP) and Quality of Service*』を参照してください。このマニュアルには、次の URL からアクセスできます。

http://www.cisco.com/en/US/tech/tk543/tk762/technologies_tech_note09186a0080108e2c.shtml

音声ペイロードの調整可能なバイト サイズ

各 Cisco IPICS 音声パケットに含まれる音声ペイロードのサイズは、管理者が制御できます。サイズを制御するには、VoIP ダイヤル ピアの bytes パラメータを使用します。次の例を参考にしてください。

```
dial-peer voice 1 voip
destination-pattern 4085551234
codec g729r8 bytes 40
session protocol multicast
session target ipv4:239.192.1.1:21000
```

1 パケットあたりのバイト数を変更すると、1 秒間あたりの送信パケット数が変化します。1 秒間あたりの送信パケット数は、次の例に示した方法で計算できます。

G.729a コーデック（デフォルトの 20 バイト ペイロード / パケット）

コーデックのレート：8,000 ビット / 秒 * 8 ビット = 1,000 バイト / 秒

サンプリング間隔：10 ms

デフォルトのペイロード サイズ：20 バイト / パケット（2 サンプル / パケット）

1,000 バイト / 秒 /20 バイト / パケット = 50 パケット / 秒

G.729a コーデック（VoIP ダイヤル ピアで 40 バイトを定義）

コーデックのレート：8,000 ビット / 秒 * 8 ビット = 1,000 バイト / 秒

サンプリング間隔：10 ms

ペイロード サイズ：40 バイト / パケット

1,000 バイト / 秒 /40 バイト / パケット = 25 パケット / 秒

（注）　ペイロード サイズを大きくすると、1 サンプルあたりの遅延が同じ量だけ大きくなります。たとえば、ペイロード サイズを 20 バイトから 40 バイトに増やすと、遅延が 1 サンプルあたり 20 バイト増えます。

アグレッシブ音声アクティビティ検出

Voice Activity Detection（VAD; 音声アクティビティ検出）は、会話の無音部分を DSP で動的に検出するためのメカニズムです。このような無音部分が発生しているときは、VoIP パケットがネットワークに送信されません。VAD を利用すると、VoIP コールで使用される帯域幅の量を最大で 50% 削減できます。

VAD は VoIP の帯域幅を節約しますが、LMR および PTT パケット ストリームで使用される Cisco IPICS シグナリングを阻害し、排除します。Cisco IPICS 環境で VAD を使用する場合は、この問題に注意してください。

LMR ゲートウェイ ポートを設定するときは、無線で Carrier Operated Relay（COR; 搬送波作動リレー）または Carrier Operated Squelch（COS; 搬送波作動スケルチ）がサポートされている場合、VAD を使用しないでください。COR または COS シグナリングをサポートする無線は、パケットの生成を開始するための有線シグナリングを LMR ポートに提供できます。COR または COS ゲート処理を使用すると、効率的にオーディオ入力を制御できるほか、短期間で一気に転送された音声データがドロップされることを回避できます。このようなデータは、VAD がアクティブになる値を下回っている場合があります。

環境雑音やユーザは、音声ポートごとに異なります。したがって、雑音レベルと音声レベルにもさまざまなバリエーションがあります。従来の VAD でもこのような多様性に対応できますが、この VAD はユニキャスト用に設計されたものです。帯域幅の節約よりも、良好な音声品質の確保のほうが通常は重要視されるので、一般に、従来の VAD では検出数が少なめではなく多めになります。しかし、マルチキャスト環境では、検出数が少なすぎたり多すぎたりすると音声品質が低下するため、これは望ましくありません。

アグレッシブ VAD を使用すると、マルチキャスト環境で過度の検出を避けることができます。アグレッシブ VAD を使用しているときは、未知の Signal-to-Noise Ratio（SNR; 信号対雑音比）を持った信号を DSP が検出した場合、DSP はスプリアス パケットを伝送しません。従来の VAD を使用しているときは、未知の SNR を持った信号を DSP が検出した場合、DSP はパケットの伝送を継続します。この機能により、音声ストリームに使用できるすべてのスロットが、不要なトラフィックに占有されることがあります。

アグレッシブ VAD を有効にするには、ダイヤル ピアの `vad aggressive` 設定値を有効にします。次に例を示します。

```
dial-peer voice 10 voip
destination-pattern 111
session protocol multicast
session target ipv4:239.192.1.1:21000
vad aggressive
```

音声ストリームの混合

P.2-12 の「仮想トーク グループ」で説明したように、Cisco IPICS 環境の DSP は 3 つまでの音声ストリームを混合できます。ただし、DSP は要約機能を実行しません。したがって、たとえば、3 つの G.729a ストリーム（それぞれ 24 KB、ヘッダー付き）をルータまたはゲートウェイが受信した場合、混合ストリームは 72 KB の帯域幅を消費します。VTG 内の各ユーザ、または VTG 内のチャネルが単一の混合オーディオ ストリームを受信する場合でも、DSP は単一の 24 KB ストリームを送信しません。

Cisco IPICS ネットワークで帯域幅を計画する際は、この問題について検討することが重要です。WAN の帯域幅を計画する場合は、特に重要になります。WAN の帯域幅は、多くの場合、LAN 帯域幅に比べて高価かつ貴重なものです。

Cisco Hoot & Holler 機能は 3 つまでの音声ストリームを混合するため、Cisco Hoot & Holler 機能を備えたルータが含まれている各 WAN サイトに対しては、コールごとの帯域幅の 3 倍を超える音声帯域幅をプロビジョニングする必要はありません。

（注）　VTG を通じて混合されるオーディオ チャネルの場合は、遅延が 60 ms 追加されます。

冗長 RMS 設定

この項では、Cisco IPICS 環境で冗長 RMS コンポーネントをサポートするネットワークの設定方法を例示するケース スタディについて説明します。このテスト済みのソリューションは、プライマリおよびバックアップ マルチキャスト Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）トンネルを使用します。このソリューションでは、各 RMS のループバック インターフェイスに同じ IP アドレスを割り当てます。この IP アドレスの割り当てにより、Cisco IPICS サーバは、サーバ コードを特に考慮することなく、アクティブ RMS（この例では RMS1）またはバックアップ RMS（RMS2）にアクセスできます。この方法が可能なのは、常に 1 つの RMS のみがアクティブになるように GRE トンネルが設定されているためです。プライマリ RMS へのすべての接続が失われると、フェールオーバーが発生します。プライマリ トンネルに障害が発生すると、バックアップ トンネルがアクティブになり、バックアップ RMS にアクセスできるようになります。バックアップ トンネルがアクティブになって、Cisco IPICS サーバが RMS コンフィギュレーションを同期化すると、接続が復元されます。デフォルトの同期化プロセスは 10 分ごとに実行されるので、フェールオーバーが完了するのに約 10 分かかることがあります。

このトポロジでは、アクティブ RMS に対して 2 つのパスがあります。したがって、スタンバイ RMS をアクティブにする必要があるのは、両方のパスで同時に障害が発生した場合です。アクティブな RMS 自体に障害が発生すると、バックアップ トンネルがアクティブになります。

この設定では、RMS ルータは同じハードウェア（同一スロットに同一ハードウェア モジュール）でなければなりません。

この項では、次のトピックについて取り上げます。

トポロジ

冗長 RMS 設定には、環境内の RMS ごとに 4 台のルータが必要です。このトポロジでは、シングルポイント障害はありません。この例で説明するトポロジでは、3 つのルータのコアが使用されます。ルータの 1 つの GW3 ルータにより接続が可能になります。他のルータ（GW1 および GW2）は、コアと冗長 RMS デバイス間の完全な冗長ルーティングを提供します。

コア トポロジには、VLAN 100 上の Cisco IPICS エンドポイント（Cisco IPICS サーバ、PMC、および Cisco Unified IP Phone）があります。電話機と PMC はスイッチ（オフィス スイッチと呼ばれる）に接続され、192.168.0.0/24 サブネット上に置かれています。Cisco Unified IP Phone は、VLAN 100 でもある Cisco Unified Communications Manager サーバに登録されています。各ルータは、リリース 12.4(4)T の Cisco 2811 Integrated Services Router です。

図 4-2 は、このソリューションのコア トポロジを示しています。

図 4-2　冗長 RMS コア トポロジ

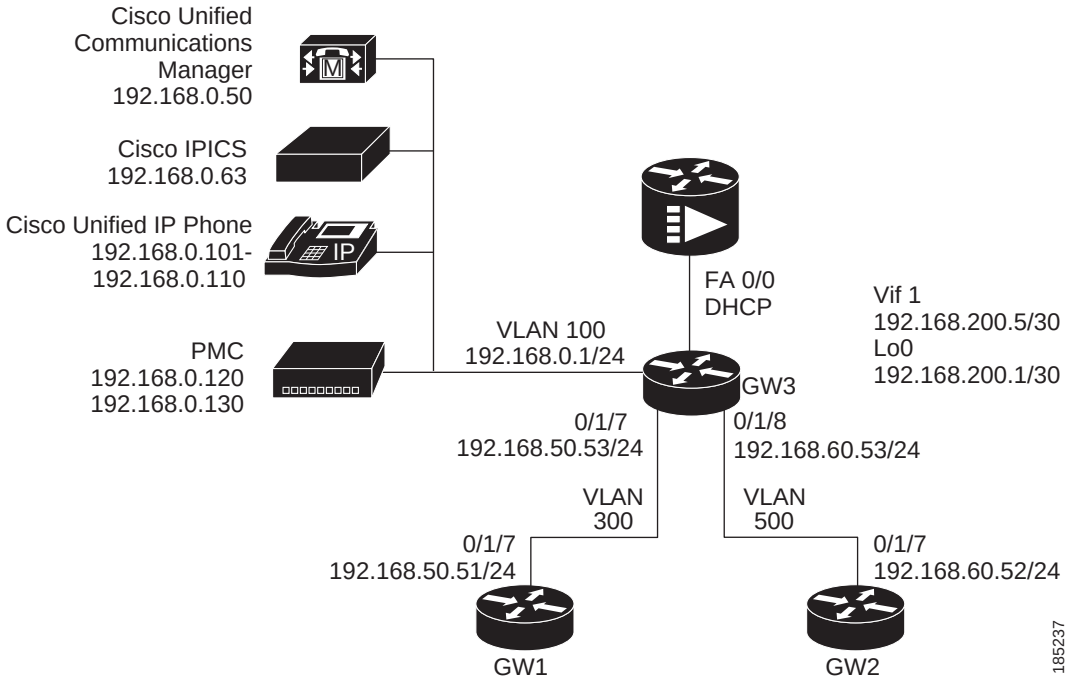
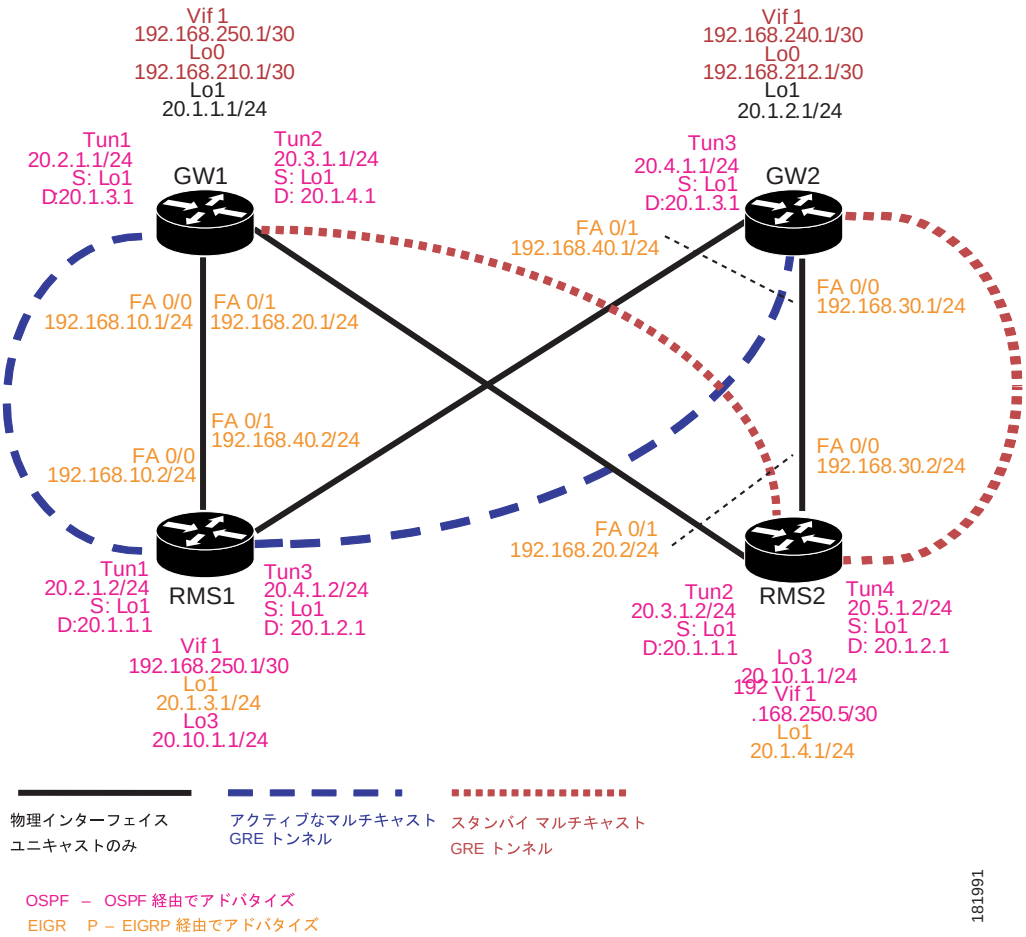


図 4-3 は、RMS ルータ（RMS1 および RMS2）がどのようにして GW1 および GW2 を経由してコアとインターフェイスで接続するのかを示しています。

図 4-3　コアとのルータ インターフェイス



ケーブル

このテスト済みソリューションでは、Cisco IPICS サーバ、Cisco Unified Communications Manager サーバ、Cisco Unified IP Phone、および PMC は、すべて GW3 の FE9 スイッチ ポートに接続されており、VLAN 100 に割り当てられています。

表 4-3 は、ルータ間のケーブル接続を示しています。

表 4-3　冗長 RMS ソリューションのケーブル

ルータ	インターフェイス	ケーブル タイプ	インターフェイス	ルータ
GW1	FA 0/0	x-over	FA 0/0	RMS1
GW1	FA 0/1	x-over	FA 0/1	RMS2
GW2	FA 0/1	x-over	FA 0/1	RMS1
GW2	FA 0/0	x-over	FA 0/0	RMS2
GW3	FA 0/1/7	ストレート	FA 0/1/7	GW1
GW3	FA 0/1/8	ストレート	FA 0/1/7	GW2

ルーティングの概要

図 4-2 で示すとおり、テスト済みソリューションには Enhanced Interior Gateway Routing Protocol（EIGRP）および Open Shortest Path First（OSPF）が実装されているため、ルートを動的にアドバタイズし、目的の接続を簡単に行うことができます。ただし、GW1 および GW2 ルータと RMS ルータ間では、任意の動的ルーティング プロトコルを使用できます。

このテスト済みソリューションの場合とは異なるルーティング プロトコルを使用する、冗長 RMS ソリューションの配置を選択する場合は、次の一般的な手順を実行してください。

1. GW1、GW2、RMS1、および RMS 2 の間の物理インターフェイスにルーティング プロトコルを設定し、ループバック 0 インターフェイスをアドバタイズします。GW1、GW2、RMS1、および RMS 2 上の ループバック 0 インターフェイスは、トンネル エンドポイントとして使用します。ルータ間でループバック インターフェイスがアドバタイズされた後、マルチキャスト GRE トンネルを設定できます。GW1 および GW2 と RMS ルータ間の物理インターフェイスは、ユニキャスト専用インターフェイスです。
2. GW1、GW2、RMS1、および RMS2 の間に、プライマリおよびバックアップ マルチキャスト GRE トンネルを設定します。トンネル エンドポイントは lo0 インターフェイスです。トンネルに 2 番目のルーティング プロトコルを設定し、他のすべてのネットワークをアドバタイズします。GW1、GW2、RMS1、および RMS2 間のすべてのマルチキャスト トラフィックは、トンネルを経由します。RMS ルータからのすべてのマルチキャスト トラフィックには、仮想インターフェイス（VIF）の発信元アドレスがあります。VIF サブネットはトンネル上でアドバタイズされるため、ゲートウェイ ルータでの RPF チェックは常に成功します。RMS へのマルチキャスト トラフィックはすべてトンネルを経由します。この場合も、静的マルチキャスト ルートは必要なく、RPF チェックは成功します。
3. RMS1 および RMS2 上の同じ IP アドレスとの別のループバック インターフェイスを設定します。このアドレスは、RMS 用に Cisco IPICS サーバに設定されているアドレスです。このアドレスを、トンネルに設定されているルーティング プロトコルに追加します。この共通 IP アドレスはトンネル上でアドバタイズされるため、ネットワークが受信するのは、アクティブ トンネル経由のアドレスの 1 つのアドバタイズに限ります。

通常の運用

通常の運用では、RMS2 へのトンネルはスタンバイ モードなので、共通ループバック アドレスはゲートウェイ ルータにアドバタイズされず、RMS2 からネットワーク内の他のアドレスへのマルチキャスト パスはありません。Cisco IPICS サーバがアクティブ RMS を制御します。ルーティングの観点からは、RMS2 上に共通ループバック アドレスは存在しません。

障害モード

RMS1 への接続が失われるのは、通常、RMS1 に障害が発生した場合に限ります。シングル ポイント障害により RMS1 へのネットワーク接続が失われることはありません。RMS1 に障害が発生すると、キープアライブ設定のためにアクティブのトンネルがタイム アウトします。トンネルがタイム アウトすると、セカンダリ トンネルがアクティブになり、共通ループバック アドレスが RMS2 によってアドバタイズされます。また、マルチキャスト トラフィックのために、RMS2 から GW1 および GW2 へのトンネルが確立されます。Cisco IPICS サーバが RMS を定期的にチェックすると（デフォルトでは、10 分ごと）、RMS2 設定が、RMS1 設定と一致するように更新されます。

フェール バック モード

RMS1 がオンラインに復帰すると、これがアクティブ RMS になり、RMS2 へのトンネルはスタンバイ モードに戻ります。

RMS1 および GW1 の設定例

次に、RMS1 の設定例を示します。

```
router eigrp 1
 network 20.1.3.0 0.0.0.255   Loopback1
 network 192.168.10.0         Fa0/0
 network 192.168.40.0         Fa0/1
 no auto-summary
!
router ospf 51
 log-adjacency-changes
 network 20.2.1.0 0.0.0.255 area 51     Tunnel 1 to GW1
 network 20.4.1.0 0.0.0.255 area 51     Tunnel 2 to GW2
 network 20.10.1.0 0.0.0.255 area 51    Loopback 3 (Common RMS address)
 network 192.168.250.0 0.0.0.3 area 51  Vif 1
```

次に、GW1 の設定例を示します。

```
router eigrp 1
 network 20.1.1.0 0.0.0.255     loopback1
 network 192.168.10.0          Fa0/0
 network 192.168.20.0          Fa0/1
 no auto-summary
!
router ospf 51
 log-adjacency-changes
network 20.2.1.0 0.0.0.255 area 51      Tunnel 1 to RMS1
 network 20.3.1.0 0.0.0.255 area 51     Tunnel 2 to RMS2
 network 192.168.50.0 0.0.0.255 area 51        VLAN 300 to Core
```

障害シナリオの動作

表 4-4 は、テスト済みの障害シナリオを示しています。

（注）　テスト済みトポロジでは、いずれかのゲートウェイと RMS 間の単一リンクで障害が発生しても、ユーザには影響ありません。これは、アクティブ RMS へのルートがまだ存在するためです。

表 4-4　テスト済みフェールオーバー シナリオ

障害	結果	備考
GW1 の電源断	GW2 トンネル 3 を経由する RMS1 へのすべてのトラフィック	ユーザに影響はありません
GW2 の電源断	GW1 トンネル 1 を経由する RMS1 へのすべてのトラフィック	ユーザに影響はありません
RMS1 の電源断	GW1 および GW2 トンネルを経由する RMS2 へのすべてのトラフィック	再度同期化されるまで停止します

警告

冗長 RMS ソリューションを実装する場合は、次の警告に注意してください。

- Cisco IPICS サーバでは、10 分ごとにポーリング ルーチンが実行されます。このルーチンは、RMS をサーバ コンフィギュレーションに同期化します。RMS1 に障害が発生すると、同期化ルーチンが RMS2 で実行されるまで、最高 10 分の遅延が発生することがあります。RMS2 の同期化に必要な時間は、ネットワーク遅延および現在設定されている RMS リソース数によって異なります。

  Cisco IPICS Administration Console から、Administration トレイのオプション ウィンドウ内の RMS Polling Frequency フィールドに新しい値を入力して、ポーリング期間を変更することができます。このトレイから手動で同期化を実行することもできます。この手順の詳細については、『*Cisco IPICS Server Administration Guide, Release 2.1(1)*』の「Performing Cisco IPICS System Administrator Tasks」の章を参照してください。
- フェールオーバー後にアクティブ RMS への接続が復元されると、システムはフォール バックします。

ルータの設定

次の項では、テスト済みソリューションにおけるルータからの **show running-config** コマンドの出力を示します。Cisco IPICS サーバによって実行された RMS 音声ポートとダイヤル ピア設定は、スペースを節約するために削除されています。

- GW1 の設定（P. 4-16）
- GW2 の設定（P. 4-19）
- GW3 の設定（P. 4-21）
- RMS1 の設定（P. 4-25）
- RMS2 の設定（P. 4-29）

GW1 の設定

次に、GW1 の設定を示します。

```
version 12.4
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service sequence-numbers
!
hostname gw1
!
boot-start-marker
boot system flash 1244t.bin
boot-end-marker
!
! card type command needed for slot 1
! card type command needed for slot 1
security passwords min-length 6
logging buffered 51200 warnings
enable password 7 0822455D0A16544541
!
aaa new-model
!
aaa authentication login default local
!
aaa session-id common
!
```

```
resource policy
!
no network-clock-participate slot 1
ip subnet-zero
no ip source-route
ip tcp synwait-time 10
!
ip cef
no ip dhcp use vrf connected
ip dhcp excluded-address 192.168.0.1
ip dhcp excluded-address 192.168.0.1 192.168.0.9
ip dhcp excluded-address 192.168.0.20 192.168.0.255
ip dhcp excluded-address 192.168.100.1
!
ip dhcp pool sub-100
   network 192.168.100.0 255.255.255.0
   default-router 192.168.0.1
   option 150 ip 192.168.0.50
   dns-server 68.87.71.226 68.87.73.242
!
ip dhcp pool sub-300
   network 192.168.1.0 255.255.255.0
   default-router 192.168.0.10
   option 150 ip 192.168.0.50
   dns-server 68.87.71.226
!
ip ftp username administrator
ip ftp password 7 121A0C041104
no ip bootp server
ip domain name gw1.cisco.com
ip multicast-routing
no ip igmp snooping
!
ftp-server enable
!
voice-card 0
 dspfarm
!
voice-card 1
 dspfarm
!
username cisco privilege 15 secret 5 $1$iLkt$2AxwmRpQ4ZnX6fDnwPiI1.
username ipics privilege 15 password 7 094F471A1A0A464058
!
interface Tunnel1
 backup interface Tunnel2
 ip address 20.2.1.1 255.255.255.0
 ip pim sparse-mode
 keepalive 7 3
 tunnel source Loopback1
 tunnel destination 20.1.3.1
!
interface Tunnel2
 ip address 20.3.1.1 255.255.255.0
 ip pim sparse-mode
 keepalive 7 3
 tunnel source Loopback1
 tunnel destination 20.1.4.1
!
interface Loopback1
 ip address 20.1.1.1 255.255.255.0
!
interface FastEthernet0/0
 description $ETH-LAN$$ETH-SW-LAUNCH$$INTF-INFO-FE 0/0$
 ip address 192.168.10.1 255.255.255.0
 no ip mroute-cache
 duplex auto
 speed auto
!
```

```
interface FastEthernet0/1
 ip address 192.168.20.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1/0
!
interface FastEthernet0/1/1
!
interface FastEthernet0/1/2
!
interface FastEthernet0/1/3
!
interface FastEthernet0/1/4
!
interface FastEthernet0/1/5
!
interface FastEthernet0/1/6
!
interface FastEthernet0/1/7
 switchport access vlan 300
 switchport mode trunk
!
interface FastEthernet0/1/8
!
interface Vlan1
 no ip address
!
interface Vlan300
 ip address 192.168.50.51 255.255.255.0
 ip pim sparse-mode
!
router eigrp 1
 network 20.1.1.0 0.0.0.255
 network 192.168.10.0
 network 192.168.20.0
 no auto-summary
!
router ospf 51
 log-adjacency-changes
 network 20.2.1.0 0.0.0.255 area 51
 network 20.3.1.0 0.0.0.255 area 51
 network 192.168.50.0 0.0.0.255 area 51
!
no ip classless
!
no ip http server
ip http authentication local
no ip http secure-server
ip http timeout-policy idle 5 life 86400 requests 10000
ip pim rp-address 192.168.0.1
!
control-plane
!
voice-port 0/2/0
 no echo-cancel enable
!
voice-port 0/2/1
!
line con 0
 transport output telnet
line aux 0
 transport output telnet
line vty 0 4
 exec-timeout 22 0
 privilege level 15
 login authentication local
 transport input ssh
line vty 5 15
```

```
 privilege level 15
 transport input ssh
!
scheduler allocate 20000 1000
!
end
```

GW2 の設定

次に、GW2 の設定を示します。

```
version 12.4
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname gw2
!
boot-start-marker
boot system flash 1244t.bin
boot-end-marker
!
! card type command needed for slot 1
! card type command needed for slot 1
security passwords min-length 6
logging buffered 51200 warnings
enable password 7 121A0C0411045D5679
!
aaa new-model
!
aaa authentication login default local
!
aaa session-id common
!
resource policy
!
no network-clock-participate slot 1
ip subnet-zero
no ip source-route
ip tcp synwait-time 10
!
ip cef
ip dhcp excluded-address 192.168.0.1 192.168.0.19
ip dhcp excluded-address 192.168.0.30 192.168.0.255
!
ip ftp username administrator
ip ftp password 7 121A0C041104
no ip bootp server
ip domain name gw2.cisco.com
ip host appstest50 192.168.0.50
ip name-server 39.9.211.2
ip name-server 204.127.198.19
ip multicast-routing
no ip igmp snooping
!
voice-card 0
 dspfarm
!
voice-card 1
 dspfarm
!
username cisco privilege 15 secret 5 $1$pNyj$Jrgp2.mRgWuks904x3CtR.
username ipics privilege 15 password 7 02050D4808095E731F
!
```

```
interface Tunnel3
 backup interface Tunnel4
 ip address 20.4.1.1 255.255.255.0
 ip pim sparse-mode
 keepalive 7 3
 tunnel source Loopback1
 tunnel destination 20.1.3.1
!
interface Tunnel4
 ip address 20.5.1.1 255.255.255.0
 ip pim sparse-mode
 keepalive 7 3
 tunnel source Loopback1
 tunnel destination 20.1.4.1
!
interface Loopback1
 ip address 20.1.2.1 255.255.255.0
!
interface FastEthernet0/0
 description $ETH-LAN$$ETH-SW-LAUNCH$$INTF-INFO-FE 0/0$
 ip address 192.168.30.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.40.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1/0
!
interface FastEthernet0/1/1
!
interface FastEthernet0/1/2
!
interface FastEthernet0/1/3
!
interface FastEthernet0/1/4
!
interface FastEthernet0/1/5
!
interface FastEthernet0/1/6
!
interface FastEthernet0/1/7
 switchport access vlan 500
 switchport mode trunk
!
interface FastEthernet0/1/8
!
interface Vlan1
 no ip address
!
interface Vlan500
 ip address 192.168.60.52 255.255.255.0
 ip pim sparse-mode
!
router eigrp 1
 network 20.1.2.0 0.0.0.255
 network 192.168.30.0
 network 192.168.40.0
 no auto-summary
!
router ospf 51
 log-adjacency-changes
 network 20.4.1.0 0.0.0.255 area 51
 network 20.5.1.0 0.0.0.255 area 51
 network 192.168.60.0 0.0.0.255 area 51
!
ip classless
```

```
!
!
no ip http server
no ip http secure-server
ip pim rp-address 192.168.0.1
!
control-plane
!
voice-port 0/2/0
!
voice-port 0/2/1
!
line con 0
 transport output telnet
line aux 0
 transport output telnet
line vty 0 4
 exec-timeout 22 0
 privilege level 15
 login authentication local
 transport input telnet ssh
line vty 5 15
 privilege level 15
 transport input telnet ssh
!
scheduler allocate 20000 1000
!
end
```

GW3 の設定

次に、GW3 の設定を示します。

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname GW3
!
boot-start-marker
boot system flash 1244t.bin
boot-end-marker
!
! card type command needed for slot 1
! card type command needed for slot 1
logging buffered 51200 warnings
enable password cisco123
!
aaa new-model
!
aaa authentication login default local
!
aaa session-id common
!
monitor session 1 source interface Fa0/1/7
monitor session 1 destination interface Fa0/1/2
!
resource policy
!
network-clock-participate slot 1
ip subnet-zero
!
!
ip cef
```

```
no ip dhcp use vrf connected
ip dhcp excluded-address 192.168.1.1
ip dhcp excluded-address 192.168.0.1 192.168.0.105
ip dhcp excluded-address 192.168.1.2
!
ip dhcp pool ipics-gw3
   network 192.168.1.0 255.255.255.0
   domain-name dbicknel.com
   dns-server 68.87.71.226
   default-router 192.168.1.1
   option 150 ip 192.168.0.50
!
ip dhcp pool ipics-gw3-0
   network 192.168.0.0 255.255.255.0
   domain-name dbicknel.com
   dns-server 38.9.211.2 68.87.221.86
   default-router 192.168.0.1
   option 150 ip 192.168.0.50
!
ip dhcp pool pool-gw3
!
ip dhcp pool ipics-gw3-100
   network 192.168.100.0 255.255.255.0
   domain-name dbicknel.com
   dns-server 68.87.71.226
   default-router 192.168.100.1
   option 150 ip 192.168.0.50
!
ip ftp username administrator
ip ftp password cisco
ip domain name cisco.com
ip multicast-routing
ip ssh version 2
no ip igmp snooping
!
voice-card 0
 dspfarm
!
voice-card 1
 dspfarm
!
voice service voip
 sip
  bind control source-interface Loopback0
  bind media source-interface Loopback0
!
voice class codec 1
 codec preference 1 g729r8
 codec preference 2 g711ulaw
!
voice class permanent 1
 signal timing oos timeout disabled
 signal keepalive disabled
 signal sequence oos no-action
!
username cisco privilege 15 secret 5 $1$ekF7$FbNJQY8sa228c7eX.YWSx/
username ipics privilege 15 password 0 cisco123
!
interface Loopback0
 ip address 192.168.200.1 255.255.255.252
 ip pim sparse-mode
!
interface Vif1
 ip address 192.168.200.5 255.255.255.252
 ip pim sparse-mode
!
interface FastEthernet0/0
 description $ETH-LAN$$ETH-SW-LAUNCH$$INTF-INFO-FE 0/0$
 ip address dhcp
```

```
 ip nat outside
 ip nat enable
 ip virtual-reassembly
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/1/0
 switchport access vlan 100
!
interface FastEthernet0/1/1
 switchport access vlan 100
 duplex full
 speed 100
!
interface FastEthernet0/1/2
 switchport access vlan 100
!
interface FastEthernet0/1/3
 switchport access vlan 100
!
interface FastEthernet0/1/4
 switchport access vlan 400
!
interface FastEthernet0/1/5
 switchport access vlan 100
!
interface FastEthernet0/1/6
 switchport access vlan 100
!
interface FastEthernet0/1/7
 switchport access vlan 300
 switchport mode trunk
!
interface FastEthernet0/1/8
 switchport access vlan 500
 switchport mode trunk
!
interface Vlan1
 no ip address
!
interface Vlan100
 ip address 192.168.0.1 255.255.255.0
 ip pim sparse-mode
 ip nat inside
 ip virtual-reassembly
!
interface Vlan200
 ip address 192.168.100.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!
interface Vlan300
 ip address 192.168.50.53 255.255.255.0
 ip pim sparse-mode
!
interface Vlan400
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!
interface Vlan500
 ip address 192.168.60.53 255.255.255.0
 ip pim sparse-mode
```

```
!
router ospf 51
 log-adjacency-changes
 network 30.1.1.0 0.0.0.255 area 51
 network 192.168.0.0 0.0.0.255 area 51
 network 192.168.1.0 0.0.0.255 area 51
 network 192.168.50.0 0.0.0.255 area 51
 network 192.168.60.0 0.0.0.255 area 51
 network 192.168.100.0 0.0.0.255 area 51
!
ip classless
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
!
ip http server
ip http access-class 23
ip http authentication local
no ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
ip pim rp-address 192.168.0.1
ip rtcp report interval 5001
ip nat inside source list 1 interface FastEthernet0/0 overload
ip nat inside source static 192.168.0.0 interface FastEthernet0/0
!
access-list 1 permit 192.168.0.0 0.0.255.255
!
control-plane
!
voice-port 0/2/0
 auto-cut-through
 operation 4-wire
 type 3
 signal lmr
 lmr e-lead voice
 lmr led-on
 no echo-cancel enable
 timeouts call-disconnect 3
 timing hookflash-in 0
 timing hangover 40
 connection trunk 10100
 description Dave-10100
!
voice-port 0/2/1
 auto-cut-through
 operation 4-wire
 type 3
 signal lmr
 lmr e-lead voice
 lmr led-on
 no echo-cancel enable
 timeouts call-disconnect 3
 timing hookflash-in 0
 timing hangover 40
 connection trunk 10200
 description Dave-10100
!
dial-peer voice 10100 voip
 description IPICS1-DP: 239.164.100.100
 destination-pattern 10100
 session protocol multicast
 session target ipv4:239.164.100.100:21000
 codec g711ulaw
 vad aggressive
!
dial-peer voice 10200 voip
 description IPICS1-DP: 239.164.100.101
 destination-pattern 10200
 session protocol multicast
 session target ipv4:239.164.100.101:21000
 codec g711ulaw
```

```
 vad aggressive
!
gateway
 timer receive-rtcp 5
 timer receive-rtp 1200
!
line con 0
line aux 0
line vty 0 4
 access-class 23 in
 privilege level 15
 transport input telnet ssh
line vty 5 15
 access-class 23 in
 privilege level 15
 transport input telnet ssh
!
scheduler allocate 20000 1000
!
end
```

RMS1 の設定

次に、RMS1 の設定を示します。

```
version 12.4
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service sequence-numbers
!
hostname rms1
!
boot-start-marker
boot system flash 1244t.bin
boot-end-marker
!
card type t1 0 2
security authentication failure rate 3 log
security passwords min-length 6
logging buffered 51200 debugging
logging console critical
enable secret 5 $1$m5L1$cYpoel6MgIGxjChhVa5Tj/
!
aaa new-model
!
aaa session-id common
!
resource policy
!
clock timezone PCTime -5
clock summer-time PCTime date Apr 6 2003 2:00 Oct 26 2003 2:00
no network-clock-participate slot 1
network-clock-participate wic 2
ip subnet-zero
no ip source-route
ip tcp synwait-time 10
!
ip cef
no ip dhcp use vrf connected
ip dhcp excluded-address 192.168.0.1
ip dhcp excluded-address 192.168.0.50 192.168.0.254
!
```

```
ip dhcp pool IPICS-RMS1
   network 192.168.100.0 255.255.255.0
   domain-name dbicknel.com
   dns-server 39.9.211.2 204.127.198.19
   default-router 192.168.100.1
   option 150 ip 192.168.0.50
!
ip ftp username administrator
ip ftp password 7 05080F1C2243
no ip bootp server
ip domain name cisco.com
ip host appstest50 192.168.0.50
ip name-server 39.9.211.2
ip name-server 204.127.198.19
ip multicast-routing
ip ssh time-out 100
ip ssh authentication-retries 2
!
voice-card 0
dspfarm
!
voice-card 1
 dspfarm
!
voice service voip
 sip
  bind media source-interface Loopback3
!
voice class codec 1
 codec preference 1 g729r8
 codec preference 2 g711ulaw
!
voice class permanent 1
 signal timing oos timeout disabled
 signal keepalive disabled
 signal sequence oos no-action
!
crypto pki trustpoint TP-self-signed-1491739863
 subject-name cn=IOS-Self-Signed-Certificate-1491739863
 revocation-check none
 rsakeypair TP-self-signed-1491739863
!
no spanning-tree vlan 1
username ipics privilege 15 secret 5 $1$rhC4$scpjqfhicEjHL7I48q8150
!
controller T1 0/2/0
 framing esf
 clock source internal
 linecode b8zs
 ds0-group 0 timeslots 24 type e&m-lmr
 ds0-group 1 timeslots 1 type e&m-lmr
 ds0-group 2 timeslots 2 type e&m-lmr
 ds0-group 3 timeslots 3 type e&m-lmr
 ds0-group 4 timeslots 4 type e&m-lmr
 ds0-group 5 timeslots 5 type e&m-lmr
 ds0-group 6 timeslots 6 type e&m-lmr
 ds0-group 7 timeslots 7 type e&m-lmr
 ds0-group 8 timeslots 8 type e&m-lmr
 ds0-group 9 timeslots 9 type e&m-lmr
 ds0-group 10 timeslots 10 type e&m-lmr
 ds0-group 11 timeslots 11 type e&m-lmr
 ds0-group 12 timeslots 12 type e&m-lmr
 ds0-group 13 timeslots 13 type e&m-lmr
 ds0-group 14 timeslots 14 type e&m-lmr
 ds0-group 15 timeslots 15 type e&m-lmr
 ds0-group 16 timeslots 16 type e&m-lmr
 ds0-group 17 timeslots 17 type e&m-lmr
 ds0-group 18 timeslots 18 type e&m-lmr
 ds0-group 19 timeslots 19 type e&m-lmr
```

```
 ds0-group 20 timeslots 20 type e&m-lmr
 ds0-group 21 timeslots 21 type e&m-lmr
 ds0-group 22 timeslots 22 type e&m-lmr
 ds0-group 23 timeslots 23 type e&m-lmr
!
controller T1 0/2/1
 framing esf
 linecode b8zs
 ds0-group 0 timeslots 24 type e&m-lmr
 ds0-group 1 timeslots 1 type e&m-lmr
 ds0-group 2 timeslots 2 type e&m-lmr
 ds0-group 3 timeslots 3 type e&m-lmr
 ds0-group 4 timeslots 4 type e&m-lmr
 ds0-group 5 timeslots 5 type e&m-lmr
 ds0-group 6 timeslots 6 type e&m-lmr
 ds0-group 7 timeslots 7 type e&m-lmr
 ds0-group 8 timeslots 8 type e&m-lmr
 ds0-group 9 timeslots 9 type e&m-lmr
 ds0-group 10 timeslots 10 type e&m-lmr
ds0-group 11 timeslots 11 type e&m-lmr
 ds0-group 12 timeslots 12 type e&m-lmr
 ds0-group 13 timeslots 13 type e&m-lmr
 ds0-group 14 timeslots 14 type e&m-lmr
 ds0-group 15 timeslots 15 type e&m-lmr
 ds0-group 16 timeslots 16 type e&m-lmr
 ds0-group 17 timeslots 17 type e&m-lmr
 ds0-group 18 timeslots 18 type e&m-lmr
 ds0-group 19 timeslots 19 type e&m-lmr
 ds0-group 20 timeslots 20 type e&m-lmr
 ds0-group 21 timeslots 21 type e&m-lmr
 ds0-group 22 timeslots 22 type e&m-lmr
 ds0-group 23 timeslots 23 type e&m-lmr
!
controller E1 1/0/0
!
controller E1 1/0/1
!
interface Tunnel1
 ip address 20.2.1.2 255.255.255.0
 ip pim sparse-mode
 tunnel source Loopback1
 tunnel destination 20.1.1.1
!
interface Tunnel2
 no ip address
!
interface Tunnel3
 ip address 20.4.1.2 255.255.255.0
 ip pim sparse-mode
 keepalive 7 3
 tunnel source Loopback1
 tunnel destination 20.1.2.1
!
interface Loopback1
 ip address 20.1.3.1 255.255.255.0
!
interface Loopback3
 ip address 20.10.1.1 255.255.255.0
!
interface Vif1
 ip address 192.168.250.1 255.255.255.252
 ip pim sparse-mode
!
interface FastEthernet0/0
 description $ETH-LAN$$ETH-SW-LAUNCH$$INTF-INFO-FE 0/0$$ES_LAN$$FW_INSIDE$
 ip address 192.168.10.2 255.255.255.0
 ip route-cache flow
 duplex auto
 speed auto
```

```
!
interface FastEthernet0/1
 ip address 192.168.40.2 255.255.255.0
 ip route-cache flow
 duplex auto
 speed auto
!
interface FastEthernet0/1/0
 switchport access vlan 100
!
interface FastEthernet0/1/1
 switchport access vlan 100
!
interface FastEthernet0/1/2
 switchport access vlan 100
!
interface FastEthernet0/1/3
 switchport access vlan 100
!
interface FastEthernet0/1/4
 switchport access vlan 100
!
interface FastEthernet0/1/5
 switchport access vlan 100
!
interface FastEthernet0/1/6
 switchport access vlan 100
!
interface FastEthernet0/1/7
 switchport access vlan 100
 shutdown
!
interface FastEthernet0/1/8
 switchport access vlan 300
 no cdp enable
!
interface Vlan1
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip route-cache flow
!
router eigrp 1
 network 20.1.3.0 0.0.0.255
 network 192.168.10.0
 network 192.168.40.0
 no auto-summary
!
router ospf 51
 log-adjacency-changes
 network 20.2.1.0 0.0.0.255 area 51
 network 20.4.1.0 0.0.0.255 area 51
 network 20.10.1.0 0.0.0.255 area 51
 network 192.168.250.0 0.0.0.3 area 51
!
ip classless
!
ip http server
ip http authentication local
no ip http secure-server
ip http timeout-policy idle 5 life 86400 requests 10000
ip pim rp-address 192.168.0.1
ip rtcp report interval 5001
!
logging trap debugging
!
control-plane
!
```

```
dial-peer voice 555 voip
 voice-class codec 1
 session protocol sipv2
 incoming called-number .
 no vad
!
gateway
 timer receive-rtcp 5
 timer receive-rtp 1200
!
line con 0
 transport output telnet
line aux 0
transport output telnet
line vty 0 4
 privilege level 15
 login authentication local
 transport input telnet ssh
line vty 5 15
 privilege level 15
 transport input telnet ssh
!
scheduler allocate 20000 1000
!
end
```

RMS2 の設定

次に、RMS2 の設定を示します。

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname rms2
!
boot-start-marker
boot system flash 1244t.bin
boot-end-marker
!
card type t1 0 2
!
aaa new-model
!
aaa session-id common
!
resource policy
!
no network-clock-participate slot 1
network-clock-participate wic 2
!
ip cef
!
ip domain name rms2.cisco.com
ip multicast-routing
ip ssh version 2
!
voice-card 0
 dspfarm
!
voice-card 1
 dspfarm
!
```

```
voice service voip
 sip
  bind media source-interface Loopback3
!
voice class codec 1
 codec preference 1 g729r8
 codec preference 2 g711ulaw
!
voice class permanent 1
 signal timing oos timeout disabled
 signal keepalive disabled
 signal sequence oos no-action
!
username ipics privilege 15 secret 5 $1$vrlI$wXX82ATUVJ5nvJrZxwEz/1
!
controller T1 0/2/0
 framing esf
 clock source internal
 linecode b8zs
 cablelength short 133
 ds0-group 0 timeslots 24 type e&m-lmr
 ds0-group 1 timeslots 1 type e&m-lmr
 ds0-group 2 timeslots 2 type e&m-lmr
 ds0-group 3 timeslots 3 type e&m-lmr
 ds0-group 4 timeslots 4 type e&m-lmr
 ds0-group 5 timeslots 5 type e&m-lmr
 ds0-group 6 timeslots 6 type e&m-lmr
 ds0-group 7 timeslots 7 type e&m-lmr
 ds0-group 8 timeslots 8 type e&m-lmr
 ds0-group 9 timeslots 9 type e&m-lmr
 ds0-group 10 timeslots 10 type e&m-lmr
 ds0-group 11 timeslots 11 type e&m-lmr
 ds0-group 12 timeslots 12 type e&m-lmr
 ds0-group 13 timeslots 13 type e&m-lmr
 ds0-group 14 timeslots 14 type e&m-lmr
 ds0-group 15 timeslots 15 type e&m-lmr
 ds0-group 16 timeslots 16 type e&m-lmr
 ds0-group 17 timeslots 17 type e&m-lmr
 ds0-group 18 timeslots 18 type e&m-lmr
 ds0-group 19 timeslots 19 type e&m-lmr
 ds0-group 20 timeslots 20 type e&m-lmr
 ds0-group 21 timeslots 21 type e&m-lmr
 ds0-group 22 timeslots 22 type e&m-lmr
 ds0-group 23 timeslots 23 type e&m-lmr
!
controller T1 0/2/1
 framing esf
 linecode b8zs
 cablelength short 133
 ds0-group 0 timeslots 24 type e&m-lmr
 ds0-group 1 timeslots 1 type e&m-lmr
 ds0-group 2 timeslots 2 type e&m-lmr
 ds0-group 3 timeslots 3 type e&m-lmr
 ds0-group 4 timeslots 4 type e&m-lmr
 ds0-group 5 timeslots 5 type e&m-lmr
 ds0-group 6 timeslots 6 type e&m-lmr
 ds0-group 7 timeslots 7 type e&m-lmr
 ds0-group 8 timeslots 8 type e&m-lmr
 ds0-group 9 timeslots 9 type e&m-lmr
 ds0-group 10 timeslots 10 type e&m-lmr
 ds0-group 11 timeslots 11 type e&m-lmr
 ds0-group 12 timeslots 12 type e&m-lmr
 ds0-group 13 timeslots 13 type e&m-lmr
 ds0-group 14 timeslots 14 type e&m-lmr
 ds0-group 15 timeslots 15 type e&m-lmr
 ds0-group 16 timeslots 16 type e&m-lmr
 ds0-group 17 timeslots 17 type e&m-lmr
 ds0-group 18 timeslots 18 type e&m-lmr
 ds0-group 19 timeslots 19 type e&m-lmr
```

```
 ds0-group 20 timeslots 20 type e&m-lmr
 ds0-group 21 timeslots 21 type e&m-lmr
 ds0-group 22 timeslots 22 type e&m-lmr
 ds0-group 23 timeslots 23 type e&m-lmr
!
interface Tunnel2
 ip address 20.3.1.2 255.255.255.0
keepalive 7 3
 tunnel source Loopback1
 tunnel destination 20.1.1.1
!
interface Tunnel3
 no ip address
!
interface Tunnel4
 ip address 20.5.1.2 255.255.255.0
 ip pim sparse-mode
 tunnel source Loopback1
 tunnel destination 20.1.2.1
!
interface Loopback1
 ip address 20.1.4.1 255.255.255.0
!
interface Loopback3
 ip address 20.10.1.1 255.255.255.0
!
interface Vif1
 ip address 192.168.250.5 255.255.255.252
 ip pim sparse-mode
!
interface FastEthernet0/0
 ip address 192.168.30.2 255.255.255.0
 ip route-cache flow
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.20.2 255.255.255.0
 ip route-cache flow
 duplex auto
 speed auto
!
interface FastEthernet0/1/0
!
interface FastEthernet0/1/1
!
interface FastEthernet0/1/2
!
interface FastEthernet0/1/3
!
interface FastEthernet0/1/4
!
interface FastEthernet0/1/5
!
interface FastEthernet0/1/6
!
interface FastEthernet0/1/7
 switchport access vlan 100
!
interface FastEthernet0/1/8
 switchport access vlan 300
!
interface Vlan1
 no ip address
!
router eigrp 1
 network 20.1.4.0 0.0.0.255
 network 192.168.20.0
 network 192.168.30.0
```

```
 no auto-summary
!
router ospf 51
 log-adjacency-changes
 network 20.3.1.0 0.0.0.255 area 51
 network 20.5.1.0 0.0.0.255 area 51
 network 20.10.1.0 0.0.0.255 area 51
network 192.168.250.4 0.0.0.3 area 51
!
!
no ip http server
no ip http secure-server
ip pim rp-address 192.168.0.1
ip rtcp report interval 5001
!
control-plane
!
dial-peer voice 555 voip
 voice-class codec 1
 session protocol sipv2
 incoming called-number .
 no vad
!
gateway
 timer receive-rtcp 5
 timer receive-rtp 1200
!
line con 0
line aux 0
line vty 0 4
 privilege level 15
 transport input ssh
line vty 5 15
 privilege level 15
 transport input telnet ssh
!
scheduler allocate 20000 1000
!
webvpn context Default_context
 ssl authenticate verify all
 !
 no inservice
!
!
end
```

Quality of Service

Cisco IPICS 環境でトール品質の VoIP QoS を実現するには、複数の QoS 機能を有効にする必要があります。この項では、ポイントツーポイント プロトコル（PPP）およびフレームリレーの WAN トポロジ、および LAN メディア上の配置で使用されるこれらの機能の概要を示します。

この項では、次のトピックについて取り上げます。

QoS の概要

QoS を導入することで、音声の遅延が一定以下に保たれ、パケットの損失が最小限に抑えられます。キャンパス LAN および WAN 環境の QoS については、次の推奨事項があります。

- 音声 RTP ストリームは、Expedited Forwarding（EF; 緊急転送）または IP precedence 5 として分類し、すべてのネットワーク要素上でプライオリティ キューに入れます。
- 音声制御トラフィックは、Assured Forwarding 31（AF31; 保証転送 31）または IP precedence 3 として分類し、すべてのネットワーク要素上でセカンド キューに入れます。

Cisco IPICS などのリアルタイム アプリケーションを配置するための VoIP ネットワークを設計する際は、音声品質に影響する可能性のある次の事項について検討してください。

- パケット損失：音声のクリッピングとスキップの原因になります。DSP で使用されている業界標準のコーデック アルゴリズムは、30 ms までの損失音声を修復できます。シスコの VoIP テクノロジーでは、VoIP パケット 1 つあたり 20 ms サンプルの音声ペイロードを使用しています。したがって、コーデックの修復アルゴリズムが機能するには、失われてもよいパケットは常に 1 つだけです。リアルタイム アプリケーションはパケットを再送信するように設計されていないため、パケット損失は深刻な問題になる場合があります。
- 遅延：遅延の長さが一定しない場合は、エンドツーエンドでの音声遅延による音声品質の低下、およびパケット損失の原因になります。バースティ データ環境でのキュー遅延など、遅延の長さが一定しない場合は、受信側でジッタ バッファ オーバーランが発生するおそれがあります。遅延が長くなると、バッファのオーバーフローやアンダーフローが発生し、人の声に不自然な停止が入る可能性があります。Cisco IPICS は PTT サービスをサポートしているため、International Telecommunication Union（ITU; 国際電気通信連合）の G.114 仕様で推奨されている通常の単方向遅延要件 150 ms は、直接には適用されません。PTT ユーザは無線プロトコルを意識しているため、ITU の G.173 仕様で示されているように、許容される遅延は 400 ms です。
- ジッタ：変化する遅延。遅延の中には許容できるものもありますが、常に変化する遅延は、DSP のバッファ処理が不安定になり、効率が低下する原因です。また、音声品質が一定しない原因にもなります。
- VoIP トラフィックに優先順位を設定する機能：Cisco IOS で使用できる IP RTP Priority や低遅延キューイングなどのキューイング技術を利用します。
- VoIP トラフィックを LAN または WAN ネットワーク用に最適化する機能：小さな VoIP パケットが大きなデータ パケットの後ろに回されて、遅延することがないようにします（「シリアル化」と呼ばれる現象）。

遅延を小さくし、ジッタとパケット損失を少なくするようにネットワークを設計して構築すると、Cisco IPICS ソリューションなどのリアルタイム アプリケーションが正常に機能できるようになります。

Cisco IOS のキューイング技術

Cisco IOS は、さまざまな QoS 機能を備えています。Cisco IPICS 環境では、次の機能が特に有効です。

- IP RTP Priority（P. 4-34）
- 低遅延キューイング（P. 4-34）

IP RTP Priority の詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Congestion Management Overview」の章を参照してください。このマニュアルには、次の URL からアクセスできます。

http://www.cisco.com/en/US/products/ps6350/products_installation_and_configuration_guides_list.html

IP RTP Priority

IP RTP Priority は、ポイントツーポイント リンクおよびフレームリレー PVC に適用できます。この機能を使用すると、Cisco IPICS パケット用として常に確保する一定量の帯域幅（KB 単位）をプロビジョニングできます。ネットワーク内に Cisco IPICS パケットが存在しない（つまり、誰も話していない）場合、この帯域幅は他のデータ アプリケーションが使用できます。この事前定義済みの帯域幅は、Weighted Fair Queuing（WFQ; 重み付け均等化キューイング）のすべての構造で、絶対プライオリティ キューとして提供されます。このプライオリティ キューへの入力基準となるのは、Cisco IPICS で IP パケットの送信に使用される UDP ポートの範囲です。

Cisco IPICS は、VoIP ダイヤル ピアに対して選択された UDP ポートと、その次の連番ポートを使用します。ポートの範囲は 21000 ～ 65534 です。最初のポートは、この範囲内の偶数番号にする必要があります。

次の例は、VoIP ダイヤル ピアに定義された UDP ポート（24100）を示しています。この場合、IP RTP Priority の範囲は 24100 ～ 24101 になります。

```
dial-peer voice 1 voip
destination-pattern 1111
session protocol multicast
codec g711ulaw
session target ipv4:239.10.0.100:24100
!
interface serial 0/0
ip address 10.1.1.1
ip rtp priority 24100 2 64
```

低遅延キューイング

低遅延キューイング（LLQ）は、ポイントツーポイント リンクおよびフレームリレー PVC に適用されます。LLQ は、IP RTP Priority と同様に絶対プライオリティ キューを作成しますが、この絶対プライオリティ キューをクラスベース WFQ（CBWFQ）内のサービス クラスとして適用します。固定的に割り当てて動的に使用するという機能は、IP RTP Priority と類似しています。

IP RTP Priority と LLQ の最も大きな違いは、LLQ では Access Control List（ACL; アクセス コントロール リスト）をプライオリティ キューへの入力基準として使用できる点です。この機能によって、プライオリティ キューにどのタイプのトラフィックを入れるかを柔軟に決定できます。

次の例は、LLQ を使用して Cisco IPICS トラフィックに優先順位を設定する方法を示しています。

```
access-list102 permit udp host 10.1.1.1 host 239.10.0.100 range 24100 24101
!
class-map voice
match access-group 102
!
policy-map policy1
class voice
priority 50
!
multilink virtual-template 1
!
interface virtual-template 1
ip address 172.17.254.161 255.255.255.248
no ip directed-broadcast
no ip mroute-cache
service-policy output policy1
ppp multilink
ppp multilink fragment-delay 20
ppp multilink interleave
!
interface serial 2/0
bandwidth 256
no ip address
no ip directed-broadcast
encapsulation ppp
no fair-queue
clockrate 256000
ppp multilink
multilink-group 1
```

フレームリレーでの QoS

Cisco IPICS をフレームリレー ネットワークに配置する場合、フレームリレーでは本来 QoS が提供されないことに注意してください。フレームリレーはベストエフォート型のサービスであり、フレームリレー クラウドでパケット損失が発生した場合の再送信は、上位層のアプリケーションで処理されることを前提としています。

フレームリレーでは、一般に次のパラメータを設定できます。

- Committed Information Rate（CIR; 認定情報レート）：特定の PVC においていつでも使用できることを、フレームリレー キャリアが保証している帯域幅量。キャリアは、CIR を超える速度でパケットが送信されることは一切保証しません。
- バースト：特定の PVC について、フレームリレー キャリアが許容している最大送信データ量。

フレームリレー サービスで QoS を提供するために、キャリアは「オーバープロビジョニング帯域幅」と呼ばれる手法を採用しています。これは、ある時点で提供可能な量よりも多くの帯域幅をキャリアが販売することです。この手法が成り立つのは、使用可能なすべての帯域幅を、すべてのフレームリレー顧客が一度に必要とすることはないためです。

フレームリレー キャリアによっては、フレームリレー ネットワークが常時使用可能であること、および顧客のパケットを一切ドロップしないことを保証している場合もあります。

フレームリレー キャリアは、次の方法を含め、さまざまな方法を採用して CIR + バースト サービスを提供しています。

- パケットに Discard Eligible（DE; 廃棄適正）を付けるかパケットをドロップする：VoIP などのリアルタイム アプリケーションは伝送に UDP を使用しているので、パケットを再送信するメカニズムが存在しません。VoIP の場合、この状態は問題になりません。ユーザは、会話の中のドロップされた単語を後で聞きたいとは思わないためです。パケット損失は、リアルタイム VoIP アプリケーションでは音の途切れや話し声の歪みの原因になるため、通常は許容できません。

- 速度が CIR を超えているすべてのパケットのバッファリング：パケット損失は発生しなくなりますが、項目数、およびフレームリレー スイッチがバッファを空にする速度が原因で、ジッタや遅延が発生する可能性があります。

表 4-5 に、フレームリレーを利用したネットワーク上に Cisco IPICS を配置する場合の重要な推奨事項の要約を示します。

表 4-5　Cisco IPICS をフレームリレー環境に配置する際の推奨事項

推奨事項	方法	備考
パケット損失またはジッタが Cisco IPICS ネットワークで発生することを避けるには、CIR を超えるトラフィックがフレームリレー ネットワークに送信されないようにします。	Cisco IOS の Frame Relay Traffic Shaping（FRTS; フレームリレー トラフィック シェーピング）機能を使用します。	ルータでトラフィックを PVC ごとに監視して、CIR を超えるトラフィックをルータが一切送信しないようにします。
フレームリレー環境では、WAN リンクを経由して送信されるパケットが CIR を超えないようにします。	フレームリレー ネットワークで FRF.12 機能を有効にします。	FRF.12 は、フレームリレー ネットワークのパケットを Open System Interconnection（OSI; オープン システム インターコネクション）モデルの第 2 層でフラグメント化して再構成する方法について規定した、フレームリレー フォーラム実装協定です。大きなデータ パケットをフラグメント化することによって Cisco IPICS パケットが小さくなるため、遅延が発生せず、シリアル化の影響も受けなくなり、Cisco IPICS パケットの遅延やジッタを解消できるようになります。フラグメンテーションと再構成は OSI モデルの第 2 層で実行されるため、上位層のプロトコル（IPX、AppleTalk、DNF ビットが設定された IP など）に悪影響を与えません。
Cisco IPICS パケットに絶対的な優先順位を与えるキューイング技術を実装します。	低遅延キューイング（LLQ）などの技術を使用します。	LLQ 機能を使用すると、クラスベース WFQ（CBWFQ）方式に絶対プライオリティ キューイングを組み入れることができます。絶対プライオリティ キューイングでは、音声などの遅延に敏感なデータをキューから取り出し、最初に（他のキューに含まれているパケットが取り出される前に）送信することで、遅延に敏感なデータを他のトラフィックよりも優先的に処理できます。

例

次の特性を備えた Cisco IPICS フレームリレー ネットワークについて考えます。

- 64 KB のフレームリレー PVC を通じて、Router-1 をハブとするハブアンドスポーク トポロジで接続された 3 台のルータがあります。
- どのルータも、WAN 上のデータおよび音声を CIR 速度のトラフィックに編成するように設定され、IP RTP Priority を使用して Cisco IPICS パケットの QoS を保証します。
- シリアル インターフェイス上でフレームリレー ブロードキャスト キューが有効になっています。
- 単一の Cisco IPICS チャネルが設定されています。

ブロードキャスト キューには、デフォルトでは 40 パケットまでしか保持されず、Cisco IPICS のコンポーネント（PMC、Cisco Unified IP Phone、RMS）はパケットを 50 パケット / 秒で伝送します。このため、音声パケットをドロップせず音声品質を維持するように、ブロードキャスト キューを設定する必要があります。ブロードキャスト キューの推奨設定は、64 8000 25（キュー サイズ 64、8,000 バイト / 秒（64,000 bps）、25 パケット / 秒）です。

フレームリレー ブロードキャスト キュー

ブロードキャスト キューは、ルーティングおよび Service Access Point（SAP; サービス アクセス ポイント）ブロードキャストをフレームリレー ネットワークで伝送する必要のある、中規模から大規模の IP ネットワークまたは IPX ネットワークで使用される機能です。ブロードキャスト キューは、通常のインターフェイス キューとは別に管理され、独自のバッファを備えており、サイズとデータレートを設定できます。

ブロードキャスト キューを有効にするには、次のインターフェイス コマンドを使用します。

frame-relay ***broadcast-queue size byte-rate packet-rate***

ブロードキャスト キューには、所定の最大伝送レート（スループット）制限があります。測定単位はバイト / 秒およびパケット / 秒です。このキューは、最高でもこのレートでしか伝送が行われないように動作します。設定された最大レート未満で伝送が実行されているときは、ブロードキャスト キューが優先されるため、ブロードキャスト キューには帯域幅が最低限割り当てられることが保証されます。この 2 つの伝送レート制限が存在するのは、インターフェイスがブロードキャストで飽和するのを避けるためです。ある瞬間における実際の制限値は、いずれか最初に到達したレート制限値です。伝送レート制限があるため、ブロードキャスト パケットを格納するための追加のバッファリングが必要です。

ブロードキャスト キューは、多数のブロードキャスト パケットを格納するように設定できます。キューのサイズは、ブロードキャスト ルーティング更新パケットの損失が発生しない値に設定する必要があります。正確なサイズは、使用されているプロトコル、およびそれぞれの更新に必要なパケット数によって異なります。問題が発生しないようにするには、データリンク接続識別子（DCLI）ごとの各プロトコルからの 1 つの完全なルーティング更新を格納できるキュー サイズに設定します。通常は、DCLI 1 つあたり 20 パケットから始めます。バイト レートは、次の両方の値未満にする必要があります。

- 最小リモート アクセス レート（バイト / 秒単位) の *n*/4 倍。*n* は、ブロードキャストの複製先となる DLCI の数です。
- ローカル アクセス レート（バイト / 秒単位）の 1/4。

バイト レートを小さめの値に設定すれば、パケット レートは大きな意味を持たなくなります。通常、パケット レートは 250 バイト パケットと仮定して設定する必要があります。**frame-relay broadcast-queue** コマンドのデフォルトは、次のとおりです。

- サイズ：64 パケット
- バイト レート：256,000 バイト / 秒
- パケット レート：36 パケット / 秒

次の設定は、受信と伝送（E&M）ポートを備えたフレームリレー接続の例です。

```
Router-1 (Hub Router)

hostname FR-1
!
ip multicast-routing
!
voice class permanent 1
 signal timing oos timeout disabled
 signal keepalive disabled
 signal sequence oos no-action
!
interface Vif1
ip address 1.1.1.1 255.255.255.0
ip pim sparse-mode
!
router rip
network 1.1.1.0
network 5.5.5.0
network 5.5.6.0
!
interface Serial0/0
no frame-relay broadcast-queue
encapsulation frame-relay
frame-relay traffic-shaping
frame-relay broadcast-queue 64 8000 250
!
interface Serial0/0.1 point-to-point
ip address 5.5.5.1 255.255.255.0
ip pim sparse-mode
frame-relay class ipics
frame-relay interface-dlci 100
frame-relay ip rtp header-compression
!
interface Serial0/0.1 point-to-point
ip address 5.5.6.1 255.255.255.0
ip pim sparse-mode
frame-relay class ipics
frame-relay interface-dlci 100
frame-relay ip rtp header-compression
!
map-class frame-relay ipics
frame-relay cir 128000
frame-relay bc 1280
frame-relay mincir 128000
no frame-relay adaptive-shaping
frame-relay fair-queue
frame-relay fragment 160
frame-relay ip rtp priority 16384 16384 128
!
voice-port 1/0/0
 connection trunk 111
 operation 4-wire
!
dial-peer voice 1 voip
 destination-pattern 111
 voice class permanent 1
 session protocol multicast
 session target ipv4:239.111.0.0:21000
 ip precedence 5
!

Router-2 (Spoke Router)

hostname FR-2
!
ip multicast-routing
!
```

```
voice class permanent 1
 signal timing oos timeout disabled
 signal keepalive disabled
 signal sequence oos no-action
!
interface Vif1
ip address 1.1.2.1 255.255.255.0
ip pim sparse-mode
!
router rip
network 1.1.2.0
network 5.5.5.0
!
interface Serial0/0
no frame-relay broadcast-queue
encapsulation frame-relay
frame-relay traffic-shaping
frame-relay broadcast-queue 64 8000 250
!
interface Serial0/0.1 point-to-point
ip address 5.5.5.2 255.255.255.0
ip pim sparse-mode
frame-relay class ipics
frame-relay interface-dlci 100
frame-relay ip rtp header-compression
!
map-class frame-relay ipics
frame-relay cir 128000
frame-relay bc 1280
frame-relay mincir 128000
no frame-relay adaptive-shaping
frame-relay fair-queue
frame-relay fragment 160
frame-relay ip rtp priority 16384 16384 128
!
voice-port 1/0/0
 connection trunk 111
 operation 4-wire
!
dial-peer voice 1 voip
 destination-pattern 111
 voice class permanent 1
 session protocol multicast
 session target ipv4:239.111.0.0:21000
 ip precedence 5
!

Router-3 (Spoke Router)

hostname FR-3
!
ip multicast-routing
!
voice class permanent 1
 signal timing oos timeout disabled
 signal keepalive disabled
 signal sequence oos no-action
!
interface Vif1
ip address 1.1.3.1 255.255.255.0
ip pim sparse-mode
!
router rip
network 1.1.3.0
network 5.5.6.0
!
interface Serial0/0
no frame-relay broadcast-queue
encapsulation frame-relay
```

```
frame-relay traffic-shaping
frame-relay broadcast-queue 64 8000 250
!
interface Serial0/0.1 point-to-point
ip address 5.5.6.2 255.255.255.0
ip pim sparse-mode
frame-relay class ipics
frame-relay interface-dlci 100
frame-relay ip rtp header-compression
!
map-class frame-relay ipics
frame-relay cir 128000
frame-relay bc 1280
frame-relay mincir 128000
no frame-relay adaptive-shaping
frame-relay fair-queue
frame-relay fragment 160
frame-relay ip rtp priority 16384 16384 128
!
voice-port 1/0/0
!connection trunk 111
!operation 4-wire
!
dial-peer voice 1 voip
!destination-pattern 111
!voice class permanent 1
!session protocol multicast
!session target ipv4:239.111.0.0:21000
!ip precedence 5
!
end
```

双方向 PIM マルチキャストの設定

2 つの PVC（1 つはチャネル トラフィック専用、もう 1 つはデータ トラフィック専用）が使用されている場合は、単方向マルチキャストよりも双方向 PIM マルチキャストを使用することをお勧めします。双方向 PIM マルチキャストの使用により、マルチキャスト トラフィックをルーティングするためにルータで必要になる、`ip mroute` エントリの数を削減できます。双方向 PIM では、ネットワーク内の 1 台のルータを Rendezvous Point（RP; ランデブー ポイント）として運用する必要があります。

次の設定例では、RP は Router-1 のループバック インターフェイスです（到達可能である限り、ネットワーク内にある任意のルータの任意のインターフェイスを RP にできます）。

```
Router-1 (RP node)

hostname bidir-rp
!
ip multicast-routing
!
voice class permanent 1
 signal timing oos timeout disabled
 signal keepalive disabled
 signal sequence oos no-action
!
voice class permanent 2
 signal timing oos timeout disabled
 signal keepalive disabled
 signal sequence oos no-action]
!
interface Loopback1
ip address 10.10.2.1 255.255.255.0
ip pim sparse-mode
!
interface Vif1
ip address 10.1.2.1 255.255.255.0
ip pim sparse-mode
load-interval 30
!
router rip
network 10.1.2.0
network 10.100.0.0
network 10.101.0.0
!
interface Serial0/0
no ip address
encapsulation frame-relay IETF
load-interval 30
no fair-queue
frame-relay traffic-shaping
frame-relay lmi-type cisco
!
interface Serial0/0.1 point-to-point
description channel pvc
bandwidth 256
ip address 10.100.100.1 255.255.255.0
ip pim sparse-mode
frame-relay interface-dlci 100
class channel
!
interface Serial0/0.2 point-to-point
description data pvc
ip address 10.101.101.1 255.255.255.0
frame-relay interface-dlci 200
class data
!
ip classless
ip pim bidir-enable
ip pim rp-address 10.10.2.1 10 override bidir
!
map-class frame-relay channel
frame-relay cir 128000
frame-relay bc 1000
frame-relay be 0
no frame-relay adaptive-shaping
!
map-class frame-relay data
frame-relay cir 768000
frame-relay mincir 128000
frame-relay adaptive-shaping becn
```

```
!
voice-port 1/0/0
 voice class permanent 1
 timeouts wait-release 3
 timing dialout-delay 70
 connection trunk 111
 operation 4-wire
 signal lmr
!
dial-peer voice 1 voip
destination-pattern 111
session protocol multicast
session target ipv4:239.111.0.0:21000
ip precedence 5
!
end

Router-2 (non-RP node)

hostname bidir-2
!
ip multicast-routing
!
voice class permanent 1
 signal timing oos timeout disabled
 signal keepalive disabled
 signal sequence oos no-action
!
voice class permanent 2
 signal timing oos timeout disabled
 signal keepalive disabled
 signal sequence oos no-action
!
interface Loopback1
ip address 10.10.3.1 255.255.255.0
ip pim sparse-mode
!
interface Vif1
ip address 10.1.3.1 255.255.255.0
ip pim sparse-mode
load-interval 30
!
router rip
network 10.1.3.0
network 10.100.0.0
network 10.101.0.0
!
interface Serial0/0
no ip address
encapsulation frame-relay IETF
load-interval 30
no fair-queue
frame-relay traffic-shaping
frame-relay lmi-type cisco
!
interface Serial0/0.1 point-to-point
description channel pvc
bandwidth 256
ip address 10.100.100.2 255.255.255.0
ip pim sparse-mode
frame-relay interface-dlci 100
class channel
!
interface Serial0/0.2 point-to-point
description data pvc
ip address 10.101.101.2 255.255.255.0
frame-relay interface-dlci 200
class data
!
```

```
ip classless
ip route 10.10.2.1 255.255.255.255 Serial0/0.1
ip pim bidir-enable
ip pim rp-address 10.10.2.1 10 bidir
!
map-class frame-relay channel
frame-relay cir 128000
frame-relay bc 1000
frame-relay be 0
no frame-relay adaptive-shaping
!
map-class frame-relay data
frame-relay cir 768000
frame-relay mincir 128000
frame-relay adaptive-shaping becn
!
voice-port 1/0/0
 voice class permanent 1
 playout-delay nominal 100
 playout-delay minimum high
 playout-delay mode adaptive
 playout-delay maximum 250
 timeouts wait-release 3
 timing dialout-delay 70
 connection trunk 111
 operation 4-wire
 signal lmr
!
dial-peer voice 1 voip
 destination-pattern 111
 session protocol multicast
 session target ipv4:239.111.0.0:21000
 ip precedence 5
```

ポイントツーポイント接続での QoS

この項では、次のいずれかのカプセル化を使用するポイントツーポイント接続がある WAN について説明します。

- ポイントツーポイント プロトコル（PPP）
- マルチリンク ポイントツーポイント プロトコル（MLPPP）
- ハイレベル データリンク コントロール（HDLC）

ポイントツーポイント回線（または専用線）の場合、保証帯域幅は問題になりませんが、これらの状況での接続速度、およびキューイングについては検討の必要があります。P.4-35 の「フレームリレーでの QoS」で説明したように、768 KB 未満のリンクでは、大きなデータ パケットをフラグメント化してシリアル化を避ける必要があります。また、Cisco IPICS パケットに絶対的な優先順位を与える、IP RTP Priority や低遅延キューイングなどのキューイング技術を使用する必要があります。

P.4-35 の「フレームリレーでの QoS」で説明した FRF.12 のフラグメンテーションおよび再構成の技術は、ポイントツーポイント リンクには適用されません。768 KB 未満のポイントツーポイント リンクでは、カプセル化にマルチリンク PPP（MLPPP）を使用します。MLPPP では、Link Fragmentation and Interleaving（LFI; リンク フラグメンテーション / インターリーブ）と呼ばれる機能が提供されます。LFI は、第 2 層でのフラグメンテーションを扱うという点で FRF.12 と動作が類似しています。

1,500 バイトのパケットは伝送遅延が 10 ms 前後を超えないため、リンク速度が 768 K を超えるネットワークでは LFI は不要です。この遅延は、ほとんどの遅延バジェットで許容範囲となるため、これらのネットワークでは HDLC または PPP カプセル化で対応できます。

次の例は、LFI を有効にした MLPPP の設定を示しています。

```
interface Serial0
bandwidth 64
no ip address
no ip directed-broadcast
encapsulation ppp
no ip route-cache
no ip mroute-cache
no fair-queue
ppp multilink
multilink-group 1
!
interface Multilink 1
ip address 10.1.1.1 255.255.255.252
no ip directed-broadcast
no ip route-cache
ip rtp header-compression iphc-format
ip tcp header-compression iphc-format
no ip mroute-cache
fair-queue 64 256 1000
ppp multilink
ppp multilink fragment-delay 10
ppp multilink interleave
multilink-group 1
ip rtp priority 16384 16383 30
!
```

LAN での QoS

LAN に QoS を導入する場合は、送信元に可能な限り近い適用場所を選定します。たとえば、Cisco IPICS サーバにマルチキャストで接続する PMC または Cisco Unified IP Phone の場合は、Cisco Catalyst スイッチに QoS を実装します。LMR の場合は、無線に接続する E&M ポート用に設定されたダイヤル ピアに QoS を実装します。

適用場所を選定するには、次の推奨事項に従います。

- 可能な場合は、必ず Differentiated Services Code Point（DSCP; DiffServ コード ポイント）マーキングを使用します。
- 相互運用性を確保し、将来の機能拡張に備えるために、標準ベースの DSCP Per-Hop Behavior（PHB）に従います。これらの標準には、次のものがあります。
  - RFC 2474 Class Selector Codepoints
  - RFC 2597 Assured Forwarding Classes
  - RFC 3246 Expedited Forwarding

（注）　SIP ベースの PMC は、音声 Virtual LAN（VLAN; バーチャル LAN）ではなくデータ VLAN 内にあるため、Cisco IPICS は PMC の QoS 設定を自動的に RMS にプッシュします。

WAN エッジでの QoS

QoS 設定がネクストホップ ルータに転送されるようにするには、WAN エッジで QoS を設定する必要があります。WAN エッジで QoS を設定する場合は、次の推奨事項に従います。

- 混合 WAN の回線レートが 100 Mbps を大幅に下回る場合は、Cisco Catalyst スイッチで出力方向シェーピングを有効にします（サポートされている場合）。
- 混合 WAN の回線レートが 100 Mbps を大幅に下回り、Catalyst スイッチがシェーピングをサポートしていない場合は、出力方向ポリシングを有効にします（サポートされている場合）。

ポリシング

ポリシングを設定するのは、割り当てられた帯域幅を超えている特定クラスのトラフィックを Discard Eligible（DE; 廃棄適正）としてマークするか、ドロップして、DoS 攻撃（サービス拒絶攻撃）やウイルス攻撃を防止するためです。ポリシングを設定する場合は、次の推奨事項に従います。

- トラフィック フローのポリシングは、送信元に可能な限り近い場所で実行します。
- 標準準拠の規則に従って、マークダウンを実行します（サポートされている場合）。
- Assured Forwarding（AF; 保証転送）トラフィック クラスをどのようにマークダウンするかは、RFC 2597 で規定されています（AF11 > AF12 > AF13）。出力キューでの DSCP ベース WRED がサポートされている場合は、この仕様に準拠する必要があります。
- Cisco Catalyst プラットフォームでは、DSCP ベースの WRED をサポートしていません。実行可能な代替手段は、Scavenger Class にマークすることです。
- AF　以外のクラスには、標準で定義されているマークダウン　スキームが存在しないため、Scavenger Class にマークすることが実行可能なオプションになります。
- 適用対象をプロファイリングして、何が「正常」フローや「異常」フローにあたるかを判断します（信頼区間 95% 以内）。
- 異常なトラフィックを Scavenger としてマークするキャンパス アクセスエッジ ポリシング機能を配置します。
- ユーザごとのマイクロフロー ポリシング機能を利用した、第 2 防衛線をディストリビューション層に配置します。
- エンドツーエンドの「ベストエフォート未満」の Scavenger Class キューイング ポリシーをプロビジョニングします。

キューイング

キューイングは、トラフィックをバッファリングすることにより、トラフィックが WAN 上で割り当てられている帯域幅からオーバーフローしないようにする手法です。サービス保証を提供するには、輻輳が生じる可能性のある、あらゆるノードでキューイングを有効にする必要があります。

キューイングを有効にする場合は、次の推奨事項に従います。

- デフォルトのベストエフォート クラス用として、リンクの帯域幅の少なくとも 25% を予約します。
- 絶対プライオリティ キューイングの量は、リンクのキャパシティの 33% に制限します。
- Scavenger キューイング クラスを有効にする場合、このクラスに割り当てる帯域幅の量は、必ず最小限に抑えます。
- Per-Hop Behavior（PHB）を安定させるには、キャンパス、WAN、および VPN に対して、プラットフォームのキャパシティに応じて一貫したキューイング ポリシーを設定します。
- すべての TCP フローに対して WRED を有効にします（サポートされている場合）。DSCP ベースの WRED を使用することをお勧めします。

信頼境界

Cisco IPICS の QoS インフラストラクチャは、信頼境界を使用して定義します。信頼境界という概念の詳細については、『*Cisco Unified Communications SRND Based on Cisco Unified CallManager 4.x*』を参照してください。このマニュアルには、次の URL からアクセスできます。

http://www.cisco.com/application/pdf/en/us/guest/products/ps5820/c2001/ccmigration_09186a00804474f2.pdf

信頼境界には、PMC（ローカルおよびリモート）、LMR、および Cisco Unified IP Phone を含めることができます。PMC および Cisco Unified IP Phone に対して IP precedence をマークする必要があります。推奨値は、（RTP などの）音声トラフィックは 5、（SIP や SCCP などの）音声シグナリングは 3 です。

LMR PTT クライアントの場合、LMR ゲートウェイでは E&M ポートからのトラフィックを IP precedence 5 にマークします。次に例を示します。

```
voice-port 1/0/0
 voice class permanent 1
 connection trunk 111
 operation 4-wire
!
dial-peer voice 111 voip
 destination-pattern 111
 session protocol multicast
 session target ipv4:239.111.0.111:21000
 ip precedence 5
!
```

リモート ロケーションを使用する PMC の場合、RMS では IP precedence 値を 5 にマークします。Cisco IPICS サーバは、PMC の QoS 設定およびその他の必要な設定を RMS サーバに提供します。

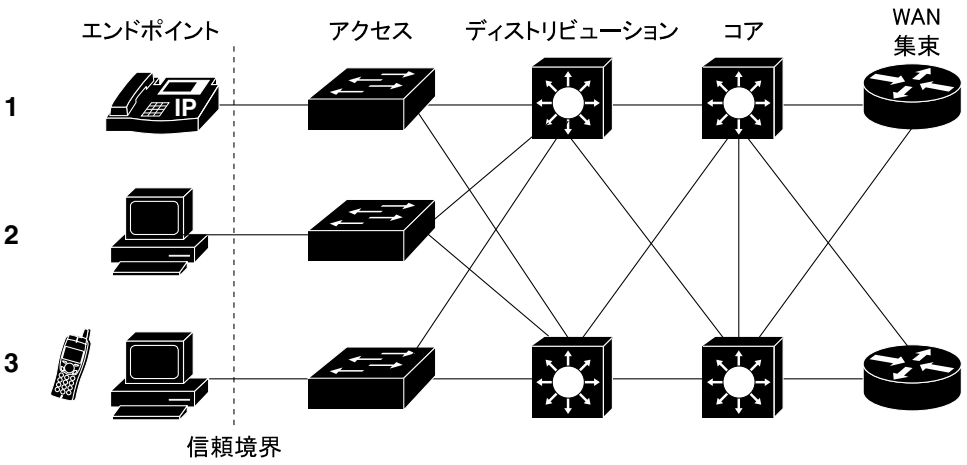
PMC、LMR、または Cisco Unified IP Phone からの Cisco IPICS トラフィック フローは、アクセス スイッチで集約され、QoS 設定はこのスイッチ上で適用されます。IP precedence のこれらの値は、いったんマークされるとネットワーク全体にわたって適用されます。

いずれかの Cisco IPICS 信頼エンドポイントが PSTN に存在する場合、これらのエンドポイントは音声ゲートウェイを経由して接続されます。Cisco 音声ゲートウェイでは、音声制御とベアラ トラフィックの IP precedence 値を 3（AF31/SC3）、DSCP 値を 5（EF/CS5）に設定できます。

VoIP ベアラ トラフィックは、可能な場合は絶対プライオリティ キューに配置されます。境界ノードは、帯域幅の枯渇やプライオリティ キューへの DoS 攻撃を避けるために、入力レベルでポリシングを実行して、VoIP トラフィックのレートを制限します。

図 4-4 は、信頼境界を示しています。

図 4-4　信頼境界



1 信頼 IP Phone PTT エンドポイント

2 信頼 PMC PTT エンドポイント

3 信頼 LMR および リモート PMC SIP エンドポイント

180572

次の例は、Cisco Catalyst 3550 でのアクセス レイヤ QoS 設定を示しています。

```
CAT3550(config)#mls qos map policed-dscp  0 24 46 to 8
! Excess traffic marked 0 or CS3 or EF will be remarked to CS1
CAT3550(config)#
CAT3550(config)#class-map match-all IPICS-VOICE
CAT3550(config-cmap)#  match access-group name IPICS-VOICE
CAT3550(config)#policy-map IPICS-PTTC
CAT3550(config-pmap)#class IPICS-VOICE
CAT3550(config-pmap-c)# set ip dscp 46
! VoIP is marked to DSCP EF
CAT3550(config-pmap-c)# police 128000 8000 exceed-action policed-dscp-transmit
! Out-of-profile IPICS VoIP (G711) is marked down to Scavenger (CS1)
CAT3550(config-pmap-c)#class IPICS-SIGNALING
CAT3550(config-pmap-c)# set ip dscp 24
! Signalling is marked to DSCP CS3
CAT3550(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
! Out-of-profile Signalling is marked down to Scavenger (CS1)
CAT3550(config-pmap-c)#class class-default
CAT3550(config-pmap-c)# set ip dscp 0
CAT3550(config-pmap-c)# police 5000000 8000 exceed-action policed-dscp-transmit
! Out-of-profile data traffic is marked down to Scavenger (CS1) 50000 (Depends on per
customer design and requirements)
CAT3550(config-pmap-c)# exit
CAT3550(config-pmap)#exit
CAT3550(config)#
CAT3550(config)#interface range FastEthernet0/1 - 48
CAT3550(config-if)# service-policy input IPICS-PTTC
! Attaching the policy map IPICS-PTTC to the interface range
CAT3550(config-if)#exit
CAT3550(config)#
CAT3550(config)#ip access-list extended IPICS-VOICE
! Extended ACL for the IPICS Address/Port ranges
CAT3550(config-ext-nacl)#
permit udp 233.0.0.0 0.255.255.255 233.0.0.0 0.255.255.255 range 21000 65534
permit udp 233.0.0.0 0.255.255.255 239.0.0.0 0.255.255.255 range 21000 65534
permit udp 239.0.0.0 0.255.255.255 233.0.0.0 0.255.255.255 range 21000 65534
permit udp 239.0.0.0 0.255.255.255 239.0.0.0 0.255.255.255 range 21000 65534
CAT3550(config-ext-nacl)#ip access-list extended IPICS-SIGNALING
! Extended ACL for the remote PMC clients
CAT3550(config-ext-nacl)# permit udp <RMS IP Address> <Any > eq 5060
! Extended ACL for the PSTN clients
CAT3550(config-ext-nacl)# permit udp <VoiceGW IP Address> <Any > eq 5060
CAT3550(config-ext-nacl)# permit tcp <Voice GW IP Address> <Any > eq 1720
CAT3550(config-ext-nacl)#end
CAT3550#
```

ポートの使用範囲

この項では、Cisco IPICS を配置した環境で使用できるポートについて説明します。この情報を参照すると、ポート レベルの QoS やファイアウォールが必要な場合に、どのように設定値を定義すると一番よいかを判断できます。ポート範囲の変更が必要になった場合は、この変更を容易に実施する方法の詳細が含まれます。

表 4-6 に、Cisco IPICS コンポーネントで使用されるデフォルト ポートを示します。

表 4-6　Cisco IPICS コンポーネントで使用されるデフォルト ポート

プロトコル	デバイス	宛先ポート	リモート デバイス
HTTP	PMC	TCP 80	Cisco IPICS サーバ
	Cisco IPICS Administration Console	TCP 80	Cisco IPICS サーバ
	Cisco Unified IP Phone	TCP 80	Cisco Unified Communications Manager、Cisco Unified Communications Manager Express
HTTPS	PMC	TCP 443	Cisco IPICS サーバ
	Cisco IPICS Administration Console	TCP 443	Cisco IPICS サーバ
SIP	PMC/ ポリシー エンジン	UDP 5060	RMS/ ポリシー エンジン SIP プロバイダー **（注）** リモート PMC から RMS、およびポリシー エンジンから SIP プロバイダーで使用されます。
RTP/RTCP	PMC	UDP 16384 ～ 32766	RMS **（注）** 音声マルチキャスト ダイヤル ピアのセッション ターゲットは、224.0.1.0 ～ 239.255.255.255 の範囲にあるマルチキャスト アドレスです。このセッション ターゲットは、セッション内のすべてのルータで同一である必要があります。オーディオ RTP ポートは 16384 ～ 32767 の範囲の偶数で、セッション内のすべてのルータで同一である必要もあります。奇数番号のポート（UDP ポート番号 + 1）は、当該セッションの RTCP トラフィックに使用されます。
	ポリシー エンジン	UDP 32768 ～ 61000	Cisco Unified Communications Manager、Cisco Unified Communications Manager Express
ICMP（PING）	PMC	ICMP	Cisco IPICS サーバ
IGMP	PMC	ICMP	マルチキャスト グループ
SSH	Cisco IPICS サーバ	TCP 22	RMS

次の各項で、関連情報について説明します。

Cisco IPICS で IP マルチキャスト アドレスを使用する場合のガイドライン

Cisco IPICS でマルチキャスト通信を使用する場合は、次のガイドラインに注意してください。

- マルチキャスト アドレスは、239.192.0.0 ～ 239.251.255.255 の範囲でのみ設定することを強くお勧めします。
- このアドレス範囲は、RFC 3171 で規定されている管理スコープ ブロックの一部であり、ローカル ドメインで使用することを意図したものです。したがって、このアドレス範囲では、既存のマルチキャスト ドメインとのアドレス指定競合が発生しにくくなります。
- Cisco IPICS では、224.0.0.0 ～ 239.255.255.255 の範囲にある IP マルチキャスト アドレスを使用できます。最初のオクテットは、224、232、233、238、または 239 で、以降のオクテットは 0 ～ 255 です。適切に使用し、望ましい結果を得るため、239.192.0.0 ～ 239.251.255.255 の範囲を使用することをお勧めします。
- 詳細については、RFC 3171『Internet Assigned Numbers Authority (IANA) Guidelines for IPv4 Multicast Address Assignment』および RFC 2365『Administratively Scoped IP Multicast』を参照してください。

マルチキャストとユニキャスト

Cisco IPICS ソリューションを設定すると、チャネルに固定マルチキャスト IP アドレスとポートのペアが割り当てられます。PMC に割り当てられるポートは、PMC で使用できるポート範囲の範囲内である必要があります。また、動的割り当てのためのマルチキャスト アドレス プールに定義されるマルチキャスト アドレスも、PMC で使用できる IP アドレス範囲の範囲内である必要があります。

PMC がリモート ロケーションを使用して接続する場合、PMC は RMS へのユニキャスト メディア接続を確立します。メディア接続に割り当てられる UDP ポートは、サポートされている範囲の中から割り当てられます。

QoS ポリシーに関する考慮事項

UDP ポート範囲に割り当てられる QoS ポリシーを定義するときは、Source Host および Destination Host のアドレスに ANY を使用することで、QoS ポリシーを PMC の UDP ポート範囲に基づいて適切に設定できます。この場合、RMS によって割り当てられる UDP ポートは考慮されないため、QoS ポリシーの単純化に役立ちます。

Cisco IPICS インフラストラクチャの保護

次の各項で、Cisco IPICS へのシステム セキュリティの導入について説明します。

Secure Sockets Layer

Cisco IPICS は、Secure Sockets Layer（SSL）を使用して PMC と Cisco IPICS サーバ間の通信を暗号化します。Cisco IPICS Administration Console にアクセスするときに管理者が使用するブラウザでは、HTTPS が使用されます。SSL を実装するには、Cisco IPICS サーバに証明書をインストールする必要があります。自己署名証明書を使用することも、セキュリティ強化のためにデジタル署名証明書を購入し、設定することもできます。また、RMS コントロールはクライアントとして SSH を使用します。

詳細については、『*Cisco IPICS Server Installation and Upgrade Guide, Release 2.1(1)*』の「Installing Third Party Certificates on the Cisco IPICS Server」の項を参照してください。

Cisco Security Agent

Cisco Security Agent（CSA）は、Cisco IPICS とは別に入手するオプションであり、Cisco IPICS サーバと PMC に侵入検知と侵入防止の機能を提供します。CSA は、攻撃に対処するのではなく、悪質な望ましくないアクティビティの発生をホスト上で防止することを目的としています。CSA は、システムに危害を及ぼすアクティビティを検出し、ブロックします。CSA には事前定義のポリシーが付属しており、ほとんどのタイプの悪質アクティビティの発生が阻止されます。悪質なアクティビティは常に不要なものであり、このレベルのセキュリティを非常に少費用で導入できます。環境のチューニングは、ほぼ必要ありません。まれにしか発生しませんが、Web サーバでの新しいユーザ アカウントの追加を CSA が阻止した場合、重要な業務アプリケーションが影響を受ける場合があります。

ファイアウォールとアクセス コントロール リスト

Cisco IPICS サーバおよびその他の Cisco IPICS コンポーネントの前面でファイアウォールとアクセス コントロール リスト（ACL）を使用すると、セキュリティの層がさらに厚くなります。たとえば、ファイアウォールまたは ACL を使用して、コール制御と管理パケットだけが Cisco IPICS サーバに到達できるようにし、Telnet や TFTP トラフィックなどの不要トラフィックをブロックします。ACL を使用すると、ネットワークにアクセスすることが事前に分かっている送信元アドレスだけにアクセスを許可できます。

ファイアウォールを使用する場合は、ファイアウォールが音声シグナリング プロトコルのステートフル インスペクションをサポートしている必要があります。Cisco IPICS は UDP ポート 21000 ～ 65534 を使用するので、このアプリケーションのサポートに必要なポートをファイアウォールが開く必要があります。また、ファイアウォールが Application Layer Gateway（ALG; アプリケーション レイヤ ゲートウェイ）機能をサポートしていることを確認してください。ALG は、シグナリング パケットを検査し、どの UDP ポートおよび RTP ストリームが使用されるかを検出して、当該 UDP ポートのためのピンホールを動的に開きます。

セキュリティに関するその他の推奨事項

Cisco IPICS ネットワークのセキュリティを強化するには、次の推奨事項に従います。

- Terminal Access Controller Access-Control System+（TACACS+）および Remote Authentication Dial In User Service（RADIUS）を使用して、非常に安全なアクセス方式をネットワークに導入します。
- セグメントの分割では、VLAN だけに依存しないようにします。さらに、ネットワークのアクセス レイヤにレイヤ 3 フィルタリングを実装します。
- 音声ネットワークとデータ ネットワークの間に、VLAN および IP フィルタを使用します。
- アウトオブバンド管理スイッチおよびルータを SSH、HTTPS、Out-Of-Band（OOB; アウトオブバンド）、許可リストなどと併用して、ネットワーク デバイスにアクセスするユーザを規制します。
- LAN スイッチ上の未使用スイッチ ポートは、無効にして未使用 VLAN に配置し、誤って使用されないようにします。
- Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）Guard や Root Guard などの、スパニング ツリー（STP）攻撃軽減ツールを使用します。
- 重要なリソースは分散して、冗長性を確保します。
- 電源スイッチへのアクセスを制限および規制します。
- Cisco IPICS サーバおよびその他のネットワーク サーバ上では、IDS Host ソフトウェアを使用して音声アプリケーションのセキュリティを確保します。

Cisco IPICS ネットワークの管理システム

Cisco IPICS ネットワークの管理および監視について計画するときは、Cisco IPICS 環境で操作によって監視できるパラメータを定義します。これらのパラメータからの出力を使用して、問題の発生を通知する一連のアラームを設定し、予防的な早期警告システムを構築します。

ネットワークに関する管理および監視のポリシーを策定した後に、次の作業を行います。

- ネットワーク内のコンポーネントごとに、当該コンポーネントについて監視対象にするパラメータを特定します。
- 特定したパラメータを監視することができる、ネットワークの管理および監視ツールを選択します。

ネットワーク全体の管理

Cisco Multicast Manager（CMM）は、マルチキャスト ネットワークの監視とトラブルシューティングを支援するために設計された、Web ベースのネットワーク管理アプリケーションです。Cisco Multicast Manager には、次の機能および利点があります。

- マルチキャスト ネットワークの問題点の早期警告
- 詳細なトラブルシューティングおよび分析機能
- オンデマンドでのリアルタイム レポート、および履歴レポート機能
- マルチキャスト対応ネットワークでの、ネットワーク使用率の最適化およびサービス配信の拡張

CMM は、レイヤ 2 スイッチを含め、Cisco IOS を実行するすべてのマルチキャスト対応デバイスを監視できます。CMM の詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/products/ps6337/index.html

Cisco IPICS ネットワークで Cisco Unified IP Phone を PTT クライアントとして使用する場合は、各種の IP テレフォニー（IPT）管理ツールを使用して、これらのデバイスを監視できます。たとえば、OpenView Gateway Statistics Utility（GSU）Reporting Solution および CiscoWorks IP Telephony Environment Monitor（ITEM）ソリューションを採用したエンタープライズ IPT 管理ソリューションを利用すると、Cisco IPT デバイス専用設計の詳細なリアルタイム障害分析を実施できます。このツールは、IPT 実装の状態を評価して、解決の必要な問題および領域を警告、通知し、IPT サービスの中断を最小限に抑えます。さらに、IPT 管理ソリューションは使用率が低いか偏っているゲートウェイ リソースを識別し、履歴に基づいてキャパシティ要件の傾向および予想を示します。

Cisco IPICS ネットワークで監視の対象になるその他の項目には、次のものがあります。

- Cisco IPICS サーバの状態
- Cisco IPICS サービスの状態
- IP ゲートウェイの状態
- Cisco Unified Communications Manager の機能
- QoS モニタリング
- レイヤ 2/3 のスイッチおよびアプリケーション