



帯域幅のプロビジョニングおよび QoS に関する考慮事項

この章では、IPCC Enterprise ネットワーク アーキテクチャ、ネットワークの配置特性、および IPCC ネットワークのプロビジョニング要件の概要について説明します。ネットワーク アーキテクチャの最も重要な概念には、ネットワーク セグメント、キープアライブ（ハートビート）トラフィック、フローの分類、IP ベースの優先順位付けとセグメント化、帯域幅と遅延の要件などがあります。WAN を介したリモート コンポーネント間のネットワーク トラフィック フローについて、WAN トラフィック フローに適切な QoS を適用する方法に関する推奨事項など、プロビジョニングのガイドラインが示されています。IPCC アーキテクチャおよびさまざまなコンポーネントのインターネットワーキングの詳細については、「[アーキテクチャの概要](#)」(P.1-1) を参照してください。

Cisco IP Contact Center (IPCC) は、従来、専用のポイントツーポイント専用回線ネットワーク接続を使用して、「プライベート」（二重化されたコントローラ、左右）または「パブリック」（セントラル コントローラに対するペリフェラル ゲートウェイ）の WAN ネットワークシステムに配置されていました。最適なネットワーク パフォーマンス特性（およびフォールトトレラントフェールオーバー メカニズムのためのルートの多様性）が IPCC アプリケーションに提供されるのは、自前の専用設備、冗長性を備えた IP ルータ、適切なプライオリティ キューイングが揃っている場合に限られます。

現在すでに複数のトラフィック クラスを共有するネットワークを使用している大企業は、当然のことながら専用ネットワークへの追加投資が必要な状況への後戻りを好まず、現状のインフラストラクチャの維持を望んでいます。ネットワークの集約がコストと運用の効率性を両立させます。そのためのサポートこそが、Cisco Powered Networks の主要な側面となります。

IPCC Enterprise Release 5.0 以降では、IPCC のパブリック パスにおけるアプリケーション レイヤの QoS パケット マーキングが IPCC アプリケーション内からサポートされているため、音声・データ統合ネットワーク環境が QoS に対応している場合に WAN の配置が容易になります。パブリック ネットワークを介した QoS 配置を採用することで 1 つの音声・データ統合ネットワークを互いに離れた場所にあるペリフェラル ゲートウェイ (PG) に分散でき、同時に厳密な ICM/IPCC トラフィック遅延、帯域幅、リアルタイム性を要求する製品に対する対応トラフィックの優先順位付けの要求を満たすことができます。この章では、WAN を介したトラフィック フローの QoS の構成に関する推奨事項について説明します。主に、リモート PG をセントラル コントローラに接続するパブリック ネットワークについて説明します。

従来から、QoS に関しては Integrated Services (IntServ; 統合化サービス) と Differentiated Services (DiffServ; 差別化サービス) の 2 種類のモデルが利用されてきました。IntServ モデルでは、Resource Reservation Protocol (RSVP; リソース予約プロトコル) を使用してネットワークの各フローに必要な QoS が提示され予約されます。IntServ ではパスのすべてのルータに膨大な量の予約に関する状

態情報を維持する必要があるため、スケーラビリティが問題となります。一方、DiffServ ではトラフィックがさまざまなクラスに分類され、ネットワークの各ノードにおいてクラスごとに指定された転送処理がそれぞれのトラフィック クラスに適用されます。DiffServ は、大まかでスケーラブルなエンドツーエンドの QoS ソリューションとして、より広範に使用され、受け入れられています。IPCC アプリケーションは RSVP を想定していないため、IntServ をサポートしていません。この章の QoS に関する考慮事項は、DiffServ に基づいています。

IPCC の配置を成功させるには、適切な帯域幅のプロビジョニングが決定的に重要になります。この章で紹介する帯域幅のガイドラインとその適用例を、必要な帯域幅のプロビジョニングを行う際の参考としてください。

IPCC ネットワーク アーキテクチャの概要

IPCC は分散された復元力のあるフォールト トレラントなネットワーク アプリケーションです。IPCC は、ネットワーク インフラストラクチャがリアルタイム データ転送要件を満たすのに十分な性能を備えているかに大きく依存しています。適切に設計された IPCC ネットワークの特徴としては、妥当な帯域幅、短い遅延、特定の UDP または TCP アプリケーション トラフィックに優先順位を付ける仕組みがあげられます。これらの設計要件は、二重化された特定の Cisco Intelligent Contact Management (ICM) ノード（すなわちセントラル コントローラとペリフェラル ゲートウェイ）の間でフォールト トレラントにメッセージを同期させたり、時間的精度が要求されるシステムのステータス データ（エージェントの状態、コールの統計値、トランクの情報など）のシステム内での配送を確実に行うために必要となります。コール センター状態の正確な更新と正確なリアルタイム レポート データの取得のために、セントラル コントローラに対して PG データの迅速な配送が必要になります。

IP Telephony 環境では、WAN および LAN のトラフィックを次に示すカテゴリにグループ化できます。

- 音声およびビデオのトラフィック
音声コール（音声キャリア ストリーム）は、PSTN ゲートウェイ ポート、IP IVR Q ポイント（ポート）、IP 電話など、さまざまなエンドポイント間の実際の音声データが含まれている Real-Time Transport Protocol (RTP) パケットで構成されています。
- コール制御トラフィック
コール制御は、コールのエンドポイントによって異なる、H.323、MGCP、SCCP、TAPI/JTAPI のいずれかのプロトコルに基づくパケットから構成されています。コール制御機能には、コールをセットアップ、管理、ティアダウン、またはリダイレクトする機能が含まれます。IPCC の場合、制御トラフィックには、音声コールのペリフェラル ターゲット（エージェント、スキルグループ、サービスなど）とその他のメディア終端リソース（IP IVR ポートなど）へのルーティングおよびペリフェラル リソース ステータスのリアルタイム更新に必要なルーティングおよびサービスの制御メッセージが含まれます。
- データ トラフィック
データ トラフィックには、電子メールや Web のような通常のトラフィックと、スクリーン ポップやその他の優先順位付きのデータのようなエージェント デスクトップに送信される CTI データベース アプリケーションのトラフィックの両方が含まれます。IPCC の優先順位付きデータには、レポートと構成の更新を行うイベントのような、非リアルタイムのシステム ステータスに関連付けられているデータが含まれます。

この章では主に、リモートのペリフェラル ゲートウェイ (PG) と ICM セントラル コントローラ (CC) の間、PG またはセントラル コントローラのサイド A とサイド B の間のネットワーク パス、およびデスクトップ アプリケーションと CTI OS あるいは Cisco Agent Desktop サーバの間の CTI フローで使用されるデータ フローと帯域幅のタイプについて説明します。また、必要な帯域幅の見積りに役立ち、必要に応じてこれらのネットワーク セグメントの QoS をプロビジョニングするためのガイドラインおよび例について説明します。

ここで説明するフローでは、上に述べた 3 つのトラフィック グループのうち後の 2 つがカプセル化されます。残りの 1 つであるメディア（音声とビデオ）ストリームは主に Cisco CallManager とそのエンドポイントの間で保持されるため、音声およびビデオのプロビジョニングについてはここで説明しません。

IPCC エージェントに対するコールで生成される音声 RTP ストリームおよびさまざまなプロトコルで生成される関連コール制御トラフィックの帯域幅の見積りについては、次の URL にある『Cisco IP Telephony Solution Reference Network Design (SRND)』を参照してください。

www.cisco.com/go/srnd

さまざまな HTTP、電子メール、および IPCC 以外のその他のミッションクリティカルなトラフィックから構成されるデータ トラフィックは、どのような統合および配置モデルを採用するかによって異なります。この章では、このタイプのトラフィックについては説明しません。データ トラフィックの適切なネットワーク設計については、次の URL にある『Network Infrastructure and Quality of Service (QoS)』を参照してください。

www.cisco.com/go/srnd

ネットワーク セグメント

IPCC で採用されているフォールト トレラント アーキテクチャには、2 つの独立した通信ネットワークが必要です。「プライベート ネットワーク」（専用パス）では、システム間の同期を維持および復元し、Message Delivery Subsystem (MDS) のクライアントが通信できるようにするために必要なトラフィックが送信されます。「パブリック ネットワーク」では、同期されたシステムの各サイドと外部システムの間でトラフィックが送信されます。またパブリック ネットワークは、フォールト トレランス ソフトウェアでノードの障害とネットワークの障害を切り分けるための代替パスとして使用されます。



(注)

このマニュアルでは「パブリック ネットワーク」と「ビジブル ネットワーク」の 2 つの用語を同じ意味で使用しています。

3 番目のネットワークであるシグナリング アクセス ネットワークは、ICM システムに配置され、キャリア ネットワーク (PSTN) とも直接通信し、ホステッド ICM/IPCC アーキテクチャを構成します。この章では、シグナリング アクセス ネットワークについては説明しません。

図 8-1 に、(サイド A とサイド B が併設された) 2 つの PG と、異なる場所に設置された 2 つの Call Router サーバで構成される基本的な IPCC Enterprise システムのネットワークセグメントを示します。

図 8-1 IPCC Enterprise システムのパブリックおよびプライベート ネットワーク セグメントの例

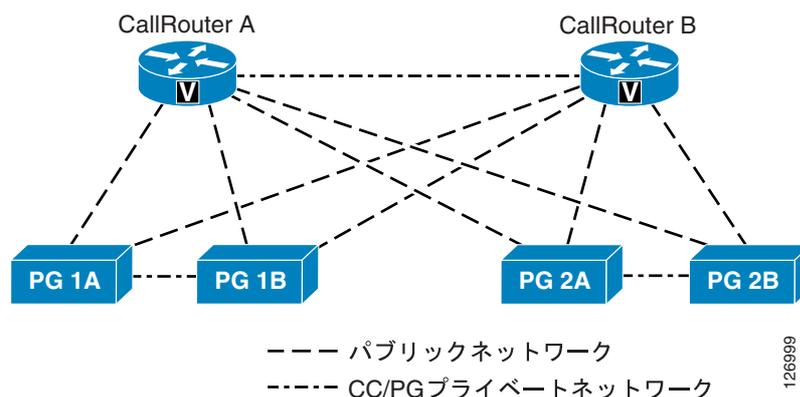


図 8-1 には、次の注が適用されます。

- プライベート ネットワークでは、CallRouter または PG ペアの二重化サイド間の ICM トラフィックが送信される。このトラフィックは主に、同期データと制御メッセージで構成されています。またこのトラフィックでは、分離された状態から回復するときに二重化サイドを再同期するために必要となる状態転送も送信されます。ルータ プロセスおよびその Logger プロセスが別個のノードで配置される場合、これらのノード間のほとんどの通信もプライベート ネットワークを介して行われます。
- WAN を介して配置された場合は Cisco ICM 全体のレスポンスにおいてプライベート リンクがクリティカルな要素となり、積極的な遅延要件を満たす必要があります。プライベート リンクは同時期および状態転送トラフィックを処理するのに十分な帯域幅を持つ必要があります。また、回復操作の一部として追加データが転送された場合に備えて、十分な帯域幅を残しておく必要もあります。プライベート ネットワークの IP ルータでは、通常、プライオリティ キューイング (ICM プライベートの high/non-high IP アドレス、および UDP ハートビートの場合はポート番号に基づく) を使用して、高優先順位の ICM トラフィックのキューイング遅延が長くなり過ぎないようにします。
- パブリック ネットワークでは、セントラル コントローラとコール センター (PG および AW) の間のトラフィックが送信される。パブリック ネットワークは、セントラル コントローラの 2 つのサイドが相互に分離した場合にどちらのサイドの優位を守るかを判断するために使用されるセントラル コントローラの代替パスの役割を果たすこともできます。パブリック ネットワークを使用して同期制御トラフィックが送信されることはありません。
- リモート コールセンターは、パブリック ネットワークを介してセントラル コントローラの各サイドに接続される。コールセンターへの各 WAN リンクには、コールセンターで PG および AW をサポートするための適切な帯域幅がある必要があります。パブリック ネットワークの IP ルータでは、IP ベースのプライオリティ キューイングまたは QoS を使用して、ICM トラフィック クラスが遅延およびジッタの許容範囲内で処理されるようにします。
- セントラル コントローラの 1 つのサイドに対してローカルなコールセンター (PG と AW) は、パブリック イーサネットを介してローカルセントラル コントローラ サイドに接続され、パブリック WAN リンクを介してリモートセントラル コントローラ サイドに接続される。この配置では、パブリック WAN ネットワークによってサイド A とサイド B が接続される必要があります。オプションとして、ブリッジを配置して PG を AW LAN セグメントから分離し、LAN 停止からの保護を強化することもできます。
- 必要な耐障害性を実現するには、プライベート WAN リンクがパブリック WAN リンクから完全に独立している必要があります (別々の IP ルータ、ネットワーク セグメントまたはパスなど)。独立した WAN リンクによって、パブリックおよびプライベート ネットワーク間でシングル ポイント障害が完全に分離されます。また、PG から CallRouter へのルート多様性をネットワーク全体で維持できるように、ネットワークを横断するパブリック ネットワーク WAN セグメントを配置する必要があります。PG から CallRouter への複数のセッションで共通のパスが選択されないようにルーティングを設定してください (共通のパスが選択されると、そこが共通の障害ポイントになります。図 8-1 を参照)。

UDP ハートビートおよび TCP キープアライブ

UDP ハートビート設計の主な目的は、回線に障害が発生したかどうかを検出することです。検出はハートビート損失の方向に基づき、接続のいずれかの端から行われます。接続の両端では、他方の端に定期的に (通常、100 または 400 ミリ秒ごと) ハートビートが送信され、各端は他方からの類似したハートビートを探します。いずれかの端が 5 回連続してハートビートを受信しなかった場合 (つまり、ハートビート間隔の 5 倍の時間、ハートビートを受信しなかった場合)、この状態を検出したサイドでは問題が発生したものと判断され、アプリケーションによってソケット接続が閉じられます。この時点で、通常、閉じたサイドから TCP リセット メッセージが生成されます。ハートビートの損失は、次のようなさまざまな理由によって発生します。ネットワーク障害、ハートビートを送信するプロセスの失敗、送信プロセスが常駐するマシンのシャットダウン、UDP パケットが適切に優先順位付けされていないなどです。

ハートビートには、複数のパラメータが関連付けられています。通常、これらのパラメータはシステムのデフォルト値に設定しておきます。これらの値の一部は接続が確立されたときに指定されます。その他の値は、Microsoft Windows 2000 レジストリの値を設定することにより指定できます。最も重要な値は、次の 2 つです。

- ハートビートの間隔の長さ
- 回線に障害が発生しているかどうかを判断するためにシステムで使用される受信されなかったハートビートの数（現在、5 としてハードコードされている）

セントラル サイト間のハートビートの間隔のデフォルト値は 100 ミリ秒です。つまり、1 つのサイトでは、500 ミリ秒以内に回線または他のサイトの障害を検出できます。ICM Release 5.0 より以前では、セントラル サイトとペリフェラル ゲートウェイの間のデフォルト ハートビート間隔は 400 秒でした。つまり、この場合、回線障害のしきい値は 2 秒です。

ICM Release 5.0 および 6.0 では、ICM QoS 実装の一部として、セントラル コントローラをペリフェラル ゲートウェイに接続するパブリック ネットワークの UDP ハートビートが TCP キープアライブ メッセージに置き換えられます（例外として、ICM Release 5.0 または 6.0 のセントラル コントローラが Release 5.0 より以前の PG と通話する場合には、通信は自動的に UDP メカニズムに戻ります）。二重化されたサイトを接続するプライベート ネットワークでは、UDP ハートビートは変更されないうまとなります。

TCP スタックにある TCP キープアライブ機能によって稼働上の問題点が検出された場合は、サーバ/クライアント サイドが終了します。TCP キープアライブ機能は、接続が一定期間アイドル状態になった後、その接続を介してプローブ パケット（つまり、キープアライブ パケット）を送信することによって動作します。他方のサイドからのキープアライブ応答がない場合、その接続は停止しているとみなされます。Microsoft Windows 2000 を使用すると、接続ごとにキープアライブ パラメータを指定できます。ICM パブリック接続の場合は、キープアライブ タイムアウトが 5*400 秒に設定されています。つまり、Release 5.0 より以前の UDP ハートビートの場合と同様に、障害が 2 秒後に検出されます。

TCP キープアライブに移行した理由は、次のとおりです。

- UDP ハートビートを使用すると、ファイアウォール環境での配置が複雑になる。ハートビート通信のダイナミック ポート割り当てによって、広範囲なポート番号を開く必要があり、ファイアウォール デバイスの本来の目的が満たされません。
- 音声・データ統合ネットワークでは、ルータでネットワークの輻輳状態を処理するために使用されるアルゴリズムによって、TCP および UDP に異なる影響が与えられます。これにより UDP ハートビート トラフィックに発生した遅延および輻輳は、TCP 接続にはあまり影響しない場合があります。

IP ベースの優先順位付けおよび QoS

トラフィックの優先順位付けが必要となるのは、簡単に言えば大量の低優先順位トラフィックが高優先順位トラフィックの前に来て、受信側への高優先順位パケットの配信の遅延が発生する可能性があるためです。低速ネットワーク フローでは、ネットワークで単一の大きな（たとえば、1500 バイト）パケットにかかる時間（およびこのパケットによる後続パケットの遅延）が、100 ミリ秒を超える場合があります。この遅延によって、1 つ以上のハートビートが確実に失われます。この状況を回避するには、低優先順位トラフィックのアプリケーションでより小さい Maximum Transmission Unit (MTU; 最大伝送ユニット) サイズを使用して、高優先順位パケットが先に送信されるようにします（回線の MTU サイズは、回線帯域幅の機能として、PG のセットアップ時に設定されたとおりにアプリケーション内から計算されます）。

適切に優先順位付けされていないネットワークでは、通常、アプリケーションの負荷が増加したとき、または（より悪い場合）ネットワークに共有トラフィックが配置されたときに、ハートビートの損失によりコールのタイムアウトおよび問題が発生します。よく見られる第 2 の影響は、極端な遅延状態による送信サイドのアプリケーションバッファプールの枯渇です。

ICM アプリケーションでは、高、中、低の 3 つの優先順位が使用されます。ただし、QoS 以前のネットワークでは、発信元および宛先 IP アドレス (UDP ハートビートの場合はネットワークの UDP ポート範囲) で識別される 2 つの優先順位だけが効果的に認識されていました (高優先順位トラフィックは別個の IP 宛先アドレスに送信されていました)。IP ベースの優先順位付けを使用したアプローチでは、高優先順位 IP アドレスの TCP パケットと UDP ハートビートをその他のトラフィックより優先するように、プライオリティ キューイングを使用した IP ルータを構成します。

QoS に対応したネットワークでは、IP アドレスではなく QoS のマーキングに基づいて、パケットに優先順位が付けられた処理 (キューイング、スケジューリング、およびポリシー設定) が適用されます。ICM Release 6.0 には、パブリック ネットワーク トラフィックに対するレイヤ 3 DSCP およびレイヤ 2 802.1p (Microsoft Windows Packet Scheduler を使用) のマーキング機能があります。パブリック ネットワークが QoS のマーキングに対応している場合、トラフィックのマーキングは、パブリック Network Interface Controller (NIC; ネットワーク インターフェイス コントローラ) で二重化された IP アドレスを設定する必要がなくなることを意味します。

トラフィック フロー

この項では、パブリックおよびプライベート ネットワークのトラフィック フローについて簡単に説明します。

パブリック ネットワークのトラフィック フロー

アクティブ PG では、各コールセンター サイトのエージェント、コール、キューなどに関連した状態情報によりセントラル コントローラの Call Router が継続的に更新されます。このタイプの PG からセントラル コントローラへのトラフィックは、リアルタイム トラフィックです。また、PG では、30 分ごとに 30 分間の履歴データが送信されます。履歴データは低優先順位ですが、30 分以内にセントラル サイトに送信される必要があります (次の 30 分間のデータに備えるため)。

PG が開始されると、セントラル サイトから設定データが提供され、PG で監視する必要があるエージェント、トランクなどが認識されます。この設定のダウンロードによって、ネットワーク帯域幅が一時的に非常に大きくなる場合があります。

要約すると、PG からセントラル コントローラへのトラフィック フローは次の各フローに分類されます。

- 高優先順位：ルーティングおよび Device Management Protocol (DMP) 制御トラフィックが含まれます。パブリック高優先順位 IP アドレスを使用して TCP で送信されます。
- ハートビート トラフィック：パブリック高優先順位 IP アドレスの UDP メッセージで、ポート範囲は 39500 ~ 39999 です。ハートビートは、PG とセントラル コントローラの間で 400 ミリ秒間隔で双方向に送信されます。UDP ハートビート トラフィックは、セントラル コントローラが Release 5.0 より以前の PG と通信していない場合は、存在しません。
- 中優先順位トラフィック：PG からセントラル コントローラへのリアルタイム トラフィックおよび設定要求が含まれます。中優先順位トラフィックは、パブリック高優先順位 IP アドレスを使用して TCP で送信されます。
- 低優先順位トラフィック：履歴データ トラフィック、CC からの設定トラフィック、およびコール クローズ通知が含まれます。低優先順位トラフィックは、パブリック高優先順位 IP アドレスを使用して TCP で送信されます。

アドミンワークステーション (AW) は、通常、ACD サイトに配置され、PG で使用される物理 WAN/LAN 回線を共有します。この場合、AW のネットワーク アクティビティをネットワーク帯域幅計算に組み込む必要があります。このマニュアルでは、AW トラフィックの帯域幅サイズについては説明しません。

プライベート ネットワークのトラフィック フロー

重要な Message Delivery Service (MDS) クライアント (Router または OPC) に対するトラフィックは、プライベート リンクを経由して他方のサイドに送信されます。

次に、プライベート トラフィックの要約を示します。

- 高優先順位トラフィック：PIM CTI Server、Logger などの MDS クライアント プロセスからのルーティング、MDS 制御トラフィック、およびその他のトラフィックが含まれます。プライベート高優先順位 IP アドレスを使用して TCP で送信されます。
- ハートビートトラフィック：プライベート高優先順位 IP アドレスの UDP メッセージで、ポート範囲は 39500 ~ 39999 です。二重化されたサイド間で 100 ミリ秒間隔で双方向に転送されます。
- 中優先順位および低優先順位トラフィック：セントラル コントローラの場合、このトラフィックには、ルーティング クライアントから供給される共有データに加え、Call Router 状態転送などの (ルート制御以外の) Call Router メッセージ (独立したセッション) が含まれます。OPC (PG) の場合、このトラフィックには、ルート制御以外の共有の周辺装置トラフィックおよびレポーティングトラフィックが含まれます。このクラスのトラフィックは、中優先順位および低優先順位として指定されている TCP セッション内で、それぞれプライベート高優先順位以外の IP アドレスを使用して送信されます。
- 状態転送トラフィック：Router、OPC、およびその他の同期プロセスの状態同期メッセージ。プライベート高優先順位以外の IP アドレスを使用して TCP で送信されます。

帯域幅と遅延の要件

一時的な境界の状態（起動設定の負荷など）や特定の設定のサイズもトラフィックの量に影響を与えますが、セントラル コントローラ（Call Router）とペリフェラル ゲートウェイの間で送受信されるトラフィックの量は、そのサイトのコール負荷に大きく影響します。安定状態で動作するリリース 5.0 以前の ICM ソフトウェアに最適なデータ量の目安は、周辺装置に到達したコール 1 件につき 1,000 バイト（8 KB）のデータです。このデータは通常、PG からセントラル コントローラに送信されます。このため、周辺装置で 1 秒当たり 10 のコールが処理されている場合、1 秒当たり 10,000 バイト（80 KB）のデータがセントラル コントローラに送信されます。このデータの大半は、低優先順位パスで送信されます。高パス帯域幅に対する低パス帯域幅の比率は、配置の特性（実行されているポストルーティングの程度が最も重要）によって異なりますが、通常、約 10 ~ 30 % です。ポストルート要求が発行されるたびに、高優先順位パスのデータは 200 ~ 300 バイト増加します。トランスレーションルートでは、コールごとに反対方向の（CallRouter から PG への）データが発生します。このデータのサイズは、デスクトップに送信されるコール コンテキストの量に完全に依存します。

ACD および VRU があるサイトには、2 つの周辺装置があり、帯域幅要件の計算では、両方の周辺機器を考慮に入れる必要があります。たとえば、1 秒当たり 10 のコールを受信する周辺装置が 4 つあるサイトは、通常、帯域幅が 320 kbps となるように設定されている必要があります。目安は 1 コールにつき 1,000 バイトですが、システムの運用が開始された後は、実際の動作を監視し、十分な帯域幅があるかどうかを確認する必要があります（ICM は、各パスの CallRouter サイドと PG サイドの両方でデータ送信統計を監視します）。

ここで説明した目安と例は、5.0 より以前の ICM リリースに適用され、ここでは参考までに説明しています。ICM Release 5.0 および 6.0 には 2 つの帯域幅カルキュレータがあり、帯域幅要件をより正確に見積もることができます。詳細については、「[帯域幅のサイジング](#)」(P.8-11) を参照してください。

ICM が設計どおりに機能するためには、帯域幅の要件と同様に、遅延の要件も満たされている必要があります。CallRouter ノードと PG ノードに二重化されたサイドツーサイドのプライベート ネットワークにおける一方向の最大遅延は 100 ミリ秒です（推奨値は 50 ミリ秒です）。PG から CallRouter へのパスが設計どおりのパフォーマンスを発揮するためには、一方向の遅延を 200 ミリ秒以下にする必要があります。このような遅延要件を満たすか、または超えることは、ICM ポストルーティングやトランスレーションルートを使用する環境で特に重要となります。

前述のとおり、ICM 帯域幅および遅延設計は、基礎となる IP 優先順位付け方式によって大きく異なります。適切な優先順位付けが行われていない場合、WAN 接続は失敗します。Cisco ICM サポート チームには、適切な優先順位付けを示し、配置認定の一部のレベルの帯域利用率モデルを実行できるカスタム ツール（クライアント/サーバなど）があります。

最終的なネットワーク設計によっては、ICM 以外のトラフィック フローと同時に ICM トラフィックの優先順位付けを実現するために、共有ネットワーク環境において IP キューイング戦略が必要になります。このキューイング戦略は、トラフィック プロファイルおよび帯域幅の可用性によって大きく異なります。前述のとおり、製品の厳密な帯域幅、遅延、および優先順位付け要求が満たされない限り、共有ネットワークは成功しません。

ネットワークのプロビジョニング

ここでは、次の項目について説明します。

- QoS (P.8-9)
- 帯域幅のサイジング (P.8-11)
- CTI OS Agent Desktop の帯域幅の要件 (P.8-12)
- Cisco Agent Desktop Release 6.0 の帯域幅の要件 (P.8-14)

QoS

ここでは、次の項目について説明します。

- QoS の計画 (P.8-9)
- パブリック ネットワークのマーキング要件 (P.8-9)
- IP デバイスでの QoS の設定 (P.8-10)
- パフォーマンス モニタリング (P.8-11)

QoS の計画

QoS の計画では、アプリケーションまたはネットワーク エッジのいずれかでトラフィックにマークすべきかについて不明であることがよくあります。アプリケーションでトラフィックにマークすると、IP ルータおよびスイッチにトラフィックを分類するアクセス リストを節約できます。トラフィック フローが IP アドレス、ポート、またはその他の TCP/IP ヘッダー フィールドによって区別されない場合は、アプリケーションでトラフィックにマークする必要があります。前述のとおり、ICM では現在、セントラル コントローラと PG の間のパブリック ネットワーク接続での DSCP マーキングがサポートされています。また、Microsoft Windows Packet Scheduler を使用して配置すると、ICM ではシェーピングと 802.1p が提供されます。シェーピング機能によって指定された期間の送信ピークがなだらかになり、ネットワークの使用状況がなだらかになるため、ICM 送信のパースト性が軽減されます。LAN QoS 処理メカニズムである 802.1p 機能を使用すると、レイヤ 2 ネットワーク セグメントが輻輳しても低優先順位パケットよりも先に高優先順位のパケットがネットワークに入ります。

発信元でトラフィックがマークされていない場合、またはネットワーク内の非プライオリティ ユーザが自分のパケットの DSCP 値または 802.1p 値を不正に設定することによってプライオリティ サービスを受けることを防ぐために QoS 信頼を無効にしている場合は、エッジルータおよびスイッチでトラフィックをマークまたは再マークすることができます。エッジルータおよびスイッチでの分類基準の定義については、表 8-1 を参照してください。

パブリック ネットワークのマーキング要件

ICM QoS マーキングは、Cisco IP Telephony の推奨値に準拠して設定されていますが、必要に応じて上書きできます。表 8-1 に、各優先順位のフローに関連付けられているパブリック ネットワーク トラフィック、遅延要件、IP アドレス、およびポートを示します。

Cisco IP Telephony パケットの分類の詳細については、次の URL にある『Cisco IP Telephony Solution Reference Network Design (SRND) guide』を参照してください。

www.cisco.com/go/srnd



(注) シスコでは、音声制御プロトコルのマーキングを DSCP 26 (PHB AF31) から DSCP 24 (PHB CS3) に変更し始めています。ただし、多くの製品では、シグナリングトラフィックが DSCP 26 (PHB AF31) としてマーキングされています。このため、シスコでは、コールシグナリングに対して暫定的に AF31 と CS3 の両方を予約しておくことをお勧めします。

表 8-1 パブリック ネットワーク トラフィックのマーキング (デフォルト) および遅延要件

優先順位	IP アドレスとポート	遅延要件	Packet Scheduler を使用する DSCP/802.1p	Packet Scheduler を使用しない DSCP/802.1p
高	高優先順位パブリック IP アドレス および高優先順位接続ポート	200 ミリ秒	AF31 / 3	AF31 / 3
中	高優先順位パブリック IP アドレス および中優先順位接続ポート	1,000 ミリ秒	AF31 / 3	AF21 / 2
低	高優先順位以外のパブリック IP アドレス および低優先順位接続ポート	5 秒	AF11 / 1	AF11 / 1

IP デバイスでの QoS の設定

この項では、QoS の典型的な設定例について説明します。Cisco AVVID キャンパス ネットワーク設計、スイッチ選択、および QoS の設定コマンドの詳細については、次の URL にある『Cisco AVVID Network Infrastructure』を参照してください。

http://www.cisco.com/en/US/netsol/ns340/ns19/ns24/networking_solutions_packages_list.html



(注) このマニュアルでは「パブリック ネットワーク」と「ビジブル ネットワーク」の 2 つの用語を同じ意味で使用しています。

IP スイッチでの 802.1q トランクの設定

802.1p が対象となる機能であり、ビジブルネットワーク NIC カードで 802.1p タギングが有効になっている場合は、次の設定例で示されているように、ICM サーバが接続されるスイッチポートを 802.1q トランクとして設定する必要があります。

```
switchport mode trunk
switchport trunk encapsulation dot1q
switchport trunk native vlan [data/native VLAN #]
switchport voice vlan [voice VLAN #]
switchport priority-extend trust
spanning-tree portfast
```

QoS 信頼の設定

ICM DSCP マーキングが信頼されている場合は、次のコマンドによって IP スイッチポートの信頼が有効になります。

```
mls qos
interface mod/port
mls qos trust dscp
```

トラフィックを分類するための QoS クラスの設定

ICM トラフィックが 2 つのレベル（高の AF31 と高以外の AF11）でマーキングされている場合は、次のクラス マップを使用して、2 つのレベルを識別できます。

```
class-map match-all ICM_Visible_High
  match ip dscp af31
class-map match-all ICM_Visible_NonHigh
  match ip dscp af11
```

分類されたトラフィックで動作するための QoS ポリシーの設定

次のポリシー マップによって、ICM 高優先順位トラフィックがプライオリティ キューに入り、最小および最大帯域幅が 500 kbps が保証されます。高優先順位以外のトラフィックは、最小帯域幅 250 kbps が割り当てられます。

```
policy-map Queuing_T1
  class ICM_Visible_High
    priority 500
  class ICM_Visible_NonHigh
    bandwidth 250
```

インターフェイスへの QoS ポリシーの適用

次のコマンドによって、QoS ポリシーが送信方向のインターフェイスに適用されます。

```
interface mod/port
  service-policy output Queuing_T1
```

パフォーマンス モニタリング

QoS に対応したプロセスが起動し、実行されると、Microsoft Windows Performance Monitor (PerfMon) を使用して、基礎となるリンクに関連付けられているパフォーマンスを追跡できます。このように PerfMon を使用するには、次の URL にある『Cisco ICM Enterprise Edition Administration Guide』を参照してください。

http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_administration_guides_list.html

帯域幅のサイジング

この項では、パブリック（ビジブル）およびプライベート ネットワークの帯域幅のサイジングについて簡単に説明します。

IPCC プライベート ネットワークの帯域幅

IPCC では通常、プライベート パス フロー（セントラル コントローラ および PG）専用のネットワーク セグメントを用いるため、WAN をまたいで IPCC をクラスタ化する場合以外は特定のセグメントの帯域幅計算は必要ありません。このためシスコでは、このための帯域幅カルキュレータを提供していません。経験則では、セントラル コントローラ プライベート パスに最小でも T1 リンクを、また PG プライベート パスに最小でも T1 リンクをそれぞれ用意します。

IPCC パブリック ネットワークの帯域幅

専用のツールを使用して、次のパブリック ネットワーク リンクに必要な帯域幅を計算できます。

ICM センtral コントローラから Cisco CallManager PG へのリンク

シスコ パートナーおよびシスコの従業員が ICM センtral コントローラと Cisco CallManager の間に必要な帯域幅を計算する場合は、ツールを利用できます。このツールは、次の URL にあります。

http://www.cisco.com/partner/WWChannels/technologies/resources/IPCC_resources.html

ICM センtral コントローラから IP IVR または ISN PG へのリンク

シスコ パートナーおよびシスコの従業員が ICM センtral コントローラと IP IVR PG の間に必要な帯域幅を計算する場合は、ツールを利用できます。このツールは、次の URL にあります。

http://www.cisco.com/partner/WWChannels/technologies/resources/IPCC_resources.html

現在のところ ICM センtral コントローラと ISN PG の通信に対応するツールは提供していません。ただし、試験結果によると、ICM センtral コントローラと IP IVR PG の間に必要な帯域幅を計算するツールで 1 つのフィールドの値を置き換えることによって、ISN の場合に対しても正確な計算値が得られることが示されています。

[Average number of RUN VRU script nodes] フィールドを、ISN と対話する ICM スクリプトのノード数に置き換えて値を代入します。

CTI OS Agent Desktop の帯域幅の要件

この項では、CTI OS Agent Desktop と CTI OS サーバとの間におけるトラフィックと帯域幅の要件について説明します。これらの要件は、特に、エージェントが WAN リンクを介してリモートになっている場合に、エージェントと CTI OS サーバ間で必要とされるネットワーク帯域幅のプロビジョニングと QoS において重要となります。エージェントがレイヤ 2 を介してローカルになっている場合でも、定期的発生するバースト性トラフィックについて把握しておくことが重要です。これは、このトラフィックが原因で帯域幅と QoS 割り当て方式に問題が生じたり、ネットワークを経由するその他の重要なトラフィックに影響がある可能性があるためです。

CTI-OS クライアント/サーバのトラフィック フローおよび帯域幅の要件

CTI OS (Release 4.6.2、5.x、および 6.x) では、エージェント スキル グループ統計情報が、10 秒ごとにすべてのエージェントに自動的に送信されます。このトラフィックが原因で、WAN リンクを介したリモート IPCC エージェントでコール処理が集中的に行われている場合に、帯域幅と QoS 割り当て方式に問題が生じます。

統計情報は、エージェントのスクリーン ポップや制御データと同じ TCP 接続で送信されます。また、送信は、同じ CTI OS サーバにログインしているすべてのエージェントで同期されます。この送信によって、10 秒ごとにトラフィックが大幅に急増し、エージェントの制御トラフィックと同じトラフィック キューに影響を与えます。

ネットワークの帯域幅の要件は、表 8-2 に示すように、エージェント スキル グループ メンバーシップの関数として直線的に増加します。ネットワークの全体的な負荷に占めるシステム コール制御トラフィックの影響は比較的小さいものの、10 秒のスキル グループ統計情報は、ネットワーク キャパシティに対して最も重要なサイジング基準となります。

表 8-2 エージェント スキル グループ メンバーシップの関数としての CTI OS の帯域幅の要件 (20,000 BHCA)

通信方向	測定タイプ	スキル グループ数				
		1	3	5	7	9
CTI OS サーバから CTI OS エージェントへ	エージェントごとの平均 Bps	584	1500	2468	3296	4332
	単一のエージェントに関して 1 秒単位でサンプリングされた最大 Bps	4846	13229	21996	26133	39147
CTI OS エージェントから CTI OS サーバへ	エージェントごとの平均 Bps	241	287	306	260	336
	単一のエージェントに関して 1 秒単位でサンプリングされた最大 Bps	1309	1746	2155	1280	2155

CTI OS サーバと CTI OS Agent Desktop のベスト プラクティスとオプション

帯域幅の要件を軽減するには、次のオプションを組み合わせで使用します。

より少ない統計情報の設定

CTI OS では、システム管理者はレジストリに、すべての CTI OS クライアントに送信する統計情報項目を指定できます。統計の選択は、各統計情報パケットのサイズに影響を与えるため、ネットワークトラフィックにも影響を与えます。設定する統計情報を少なくすると、エージェントに送信されるトラフィックが低減します。この場合、統計情報をエージェントごとに指定することはできません。エージェント統計情報の詳細については、次の URL にある『*CTI OS System Manager's Guide*』を参照してください。

<http://www.cisco.com/univercd/cc/td/doc/product/icm/icmentpr/icm60doc/icm6cti/ctios60/>

リモート ブランチでの別の CTI OS サーバのインストール

このシナリオでは、セントラル サイトの CTI OS サーバとリモート サイトの CTI OS サーバとの間に必要な帯域幅は、各リモート エージェントが毎回 1 つのセントラル CTI OS サーバにアクセスする場合に必要な帯域幅と比較してわずかになります。この帯域幅 (セントラル サイトの CTI OS サーバリモート サイトの CTI OS サーバ間) は、次のように計算できます。

$$(3000 \text{ バイト}) * (\text{毎秒コール数}) = 24 \text{ kbps} * (\text{毎秒コール数})$$

たとえば、コールセンター (1 つのリモート エージェントだけではなくすべてのエージェント) が 3600 BHCA (毎秒 1 コールに相当) を処理する場合、リモート エージェント数にかかわらず必要となる WAN リンクの帯域幅は 24 kbps だけになります。このトラフィック フローには、優先順位が付けられ、AF21 または AF11 とマーキングされる必要があります。また、この場合、リンクを経由するその他のトラフィックも帯域幅計算に組み込まれ、適切な分類でマーキングされる必要があります。

エージェントごとの統計情報のオフ

複数の接続プロファイルを使用して、エージェントごとに統計情報をオフにできます。たとえば、リモート エージェントで統計情報がオフになった接続プロファイルが使用されている場合、これらのクライアント接続では、CTI OS サーバと Agent Desktop または Supervisor Desktop との間に統計情報トラフィックがなくなります。このオプションを使用すると、リモート ロケーションにある個別の CTI OS サーバが必要なくなることがあります。

リモート サイトで統計情報トラフィックをより制限できる場合でも、リモート スーパーバイザまたは選択したエージェントは、統計情報がオンになっている異なる接続プロファイルを使用して統計情報を記録できます。

リモート エージェントのグループ統計情報がオフになっており、スーパーバイザがエージェント スキル グループ統計情報を確認する場合は、スーパーバイザは統計情報がオンになっている別の接続プロファイルを使用できます。この場合、スーパーバイザに送信されるトラフィック量はかなり少なくなります。各スキル グループとエージェント（スーパーバイザ）について、スキル グループ統計情報メッセージの packetsize は固定されています。このため、2 つのスキル グループに属するエージェントは 2 つの packetsize を受信し、5 つのスキル グループを監視するスーパーバイザは 5 つの packetsize を受信します。リモート サイトに 10 のエージェントと 1 つのスーパーバイザがあり、すべて同じ 2 つのスキル グループに設定されている（IPCC では、スーパーバイザは、そのエージェント チームのエージェントが属しているスキル グループのすべての統計情報を確認できます）場合、スーパーバイザだけが統計情報をオンにして 2 つのスキル グループを監視し、エージェントが統計情報をオフにすると、この方法によってスキル グループ統計情報トラフィックが 90% 低減されます。

また、メイン ロケーションでは、エージェントがスキル グループ統計情報をオンにする場合、スーパーバイザが異なる接続プロファイルを使用していると、リモート ロケーションへのトラフィックに影響を与えることなくこのことを行うことができます。この場合にも、追加の CTI OS サーバは必要ありません。

リモート ロケーションが複数あり、スーパーバイザだけが統計情報を確認する場合は、すべてのリモート スーパーバイザの接続プロファイルが 1 つあるだけで十分です。

CTI OS でのすべてのスキル グループ統計情報のオフ

スキル グループ統計情報が必要ない場合は、すべてオフにしてください。これにより、CTI OS サーバと Agent Desktop または Supervisor Desktop との間の接続が切断され、すべての統計情報トラフィックがなくなります。

Cisco Agent Desktop Release 6.0 の帯域幅の要件

この項では、Cisco Agent Desktop および Supervisor Desktop アプリケーションとこれらのアプリケーションが実行されるネットワークの帯域幅の要件について説明します。この項で示されているコール シナリオおよびデータは、すべて Cisco Agent Desktop ソフトウェア電話 (softphone) を使用してテストされています。レポートされている帯域幅の使用状況は、特定のシナリオで送信される合計バイト数を示しています。この数値には、コール制御および CTI サービスから返される CTI イベントの帯域幅が含まれています。デフォルトでは、Cisco Desktop アプリケーションと CTI OS サーバとの間のすべての通信は、サーバポート 42028 を介して行われます。

コール制御による帯域幅の使用

この項では、Cisco Agent Desktop と CTI OS サーバ間の次のタイプのコール制御通信に関する帯域幅の使用データについて説明します。

- ハートビートおよびスキル統計情報 (P.8-15)
- エージェント状態の変更 (P.8-15)
- 一般的なコール シナリオ (P.8-16)

ハートビートおよびスキル統計情報

表 8-3 に、ハートビートおよびスキル統計情報に関する、Cisco Agent Desktop および CTI OS と Cisco Agent Desktop サーバの間の帯域幅の使用状況を示します。このタイプのデータは、エージェントの現在の処理内容にかかわらず、ログインしているエージェントとの間で、設定されたインターバルで受け渡されます。これらのスキル グループ統計情報のリフレッシュ インターバルのデフォルト設定は 10 秒です。このリフレッシュ インターバルは、CTI OS で設定できます。また、スキル グループ統計情報は、次の URL にある『Cisco Agent Desktop Installation Guide』で説明されているように CTI OS で設定されています。

<http://www.cisco.com>

表 8-3 ハートビートおよびスキル統計情報に関する帯域幅の使用状況（平均 Byte Per Second）

サーバ	Cisco Agent Desktop へ		Cisco Agent Desktop から	
	1つのスキル	5つのスキル	1つのスキル	5つのスキル
CTI OS	49	234	7	28
Cisco Agent Desktop Base	2	2	2	2
Cisco Agent Desktop Recording	0	0	0	0
Cisco Agent Desktop VoIP Monitor	0	0	0	0
合計	51	236	9	30

CTI OS から Cisco Agent Desktop への帯域幅は、次のとおりです。

$$2.1 \text{ Bps} + (\text{スキル数} * 46.4 \text{ Bps})$$

Cisco Agent Desktop から CTI OS への帯域幅は、次のとおりです。

$$1.1 \text{ Bps} + (\text{スキル数} * 5.4 \text{ Bps})$$

例

エージェントごとのスキルが 10 個のリモート エージェントが 25 名ある場合、WAN を介して CTI OS サーバからデスクトップに送信される毎秒バイト数 (Bps) は、次のように計算できます。

$$25 \text{ エージェント} * (2.1 \text{ Bps} + (10 \text{ スキル} * 46.4 \text{ Bps})) = 11,653 \text{ Bps}$$

$$11,653 \text{ Bps} * \text{バイトごとに 8 ビット} = 93,220 \text{ 平均 Bps} = 93.22 \text{ kbps}$$

エージェント状態の変更

表 8-4 に、エージェント状態が受信可から受信不可に変更され、原因コードが入力されときの帯域幅の使用状況を示します。

表 8-4 エージェント状態の変更に関する帯域幅の使用状況（平均 Byte Per Second）

サーバ	Cisco Agent Desktop へ		Cisco Agent Desktop から	
	1つのスキル	5つのスキル	1つのスキル	5つのスキル
CTI OS	2043	6883	523	739
Cisco Agent Desktop Base	268	268	638	638
Cisco Agent Desktop Recording	0	0	0	0
Cisco Agent Desktop VoIP Monitor	0	0	0	0
合計	2311	7151	1161	1377

例

エージェントごとのスキルが 5 個のリモート エージェントが 25 名あるときに、それぞれのエージェント状態が一度に変更された場合、CTI OS サーバから Cisco Agent Desktop に送信される合計バイト数は次のようになります。

$$25 * 6883 = 151,4263 \text{ バイト}$$

一般的なコール シナリオ

表 8-5 に、一般的なコール シナリオに必要な帯域幅を示します。このコール シナリオでは、Cisco Agent Desktop を使用して次の機能を実行します。

- 作業可能状態からのエージェントの遷移
- softphone コントロールを使用した着信 ACD コールへの応答
- 作業可能状態へのエージェントの配置
- softphone コントロールを使用したコールの切断
- ラップアップ データの選択

このシナリオでは、エージェントに対して Expanded Call Context (ECC; 拡張コール コンテキスト) 変数を提示します。各 ECC 変数の長さは、ワーストケース シナリオを想定した場合、20 バイトになります。

表 8-5 一般的なコール シナリオに関する帯域幅の使用状況 (平均 Byte Per Second)

サービス	Cisco Agent Desktop へ				Cisco Agent Desktop から			
	1つのスキル		5つのスキル		1つのスキル		5つのスキル	
	1つのECC	5つのECC	1つのECC	5つのECC	1つのECC	5つのECC	1つのECC	5つのECC
CTI OS	19683	20199	30804	31263	2371	2371	2749	2749
Cisco Agent Desktop Base	4274	5882	4674	5942	6716	6832	6726	6894
Cisco Agent Desktop Recording	0	0	0	0	0	0	0	0
Cisco Agent Desktop VoIP Monitor	0	0	0	0	0	0	0	0
合計	23957	26081	35478	37205	9087	9203	9475	9643

例

スキルが 5 個、ECC 変数が 5 個であるリモート エージェントが 25 名あり、混雑時にはそれぞれのエージェントが 20 のコールに応答するとします。また、全二重ネットワークであり、送信帯域幅と受信帯域幅のうち大きい方（この場合は 37,205 バイト）を使用するとします。

$$\text{コールごとに } 37,205 \text{ バイト} * 25 \text{ エージェント} * \text{毎時 } 20 \text{ コール} = \text{毎時 } 18,602,500 \text{ バイト}$$

$$(\text{毎時 } 18,602,500 \text{ バイト}) / (\text{毎時 } 3600 \text{ 秒}) = 5,167 \text{ Bps}$$



(注)

Cisco Agent Desktop および Cisco Supervisor Desktop は両方ともプロファイルを始動時に一度だけ読み取ってキャッシュするため、LDAP へのアクセスは計算に含まれていません。この例の数値は、進行中のコールではなく、試行されたコールまたは完了したコールに基づいています。使用される帯域幅はコールごとの数値で、コールの長さには依存しません（音声トラフィックを除き、1 分のコールと 10 分のコールは、通常、同じ帯域幅を使用します）。例では、コールの転送、保留、または会議の場合に生成される追加トラフィックは考慮されていません。

必要なその他の RTP およびシグナリング マーキング以外に、監視、録音、および再生用の RTP パケットにもマーキングするようにしてください。トラフィックのマーキングの詳細については、次の URL にある『Cisco IP Telephony Solution Reference Network Design (SRND)』を参照してください。

www.cisco.com/go/srnd

サイレント モニタリングによる帯域幅の使用

Cisco Agent Desktop Release 4.6 から、デスクトップ モニタリングが新規機能として導入されています。中央集中型 VoIP モニタ サービスを使用する代わりに、Cisco Agent Desktop の各インストールには、デスクトップ モニタ サービスと呼ばれる縮小型の VoIP サービスが含まれています。このサービスでは、このデスクトップにログインしているエージェントのすべてのサイレント モニタリング要求と録音要求が行われます。

デスクトップ モニタ サービスの帯域幅の要件は、監視要求の観点から見ると VoIP モニタ サービスの要求と同一になりますが、デスクトップ モニタ サービスに送信される要求数は大幅に少なくなります。

複数の Cisco Agent Desktop スーパーバイザから同じエージェント内線に対する複数のサイレント モニタリング要求を行うことができます。この場合、各監視要求には、デスクトップの追加のコール用の帯域幅が必要となります。VoIP モニタ サービスとは異なり、デスクトップ モニタに送信できる録音要求の最大数は 1 つになります。

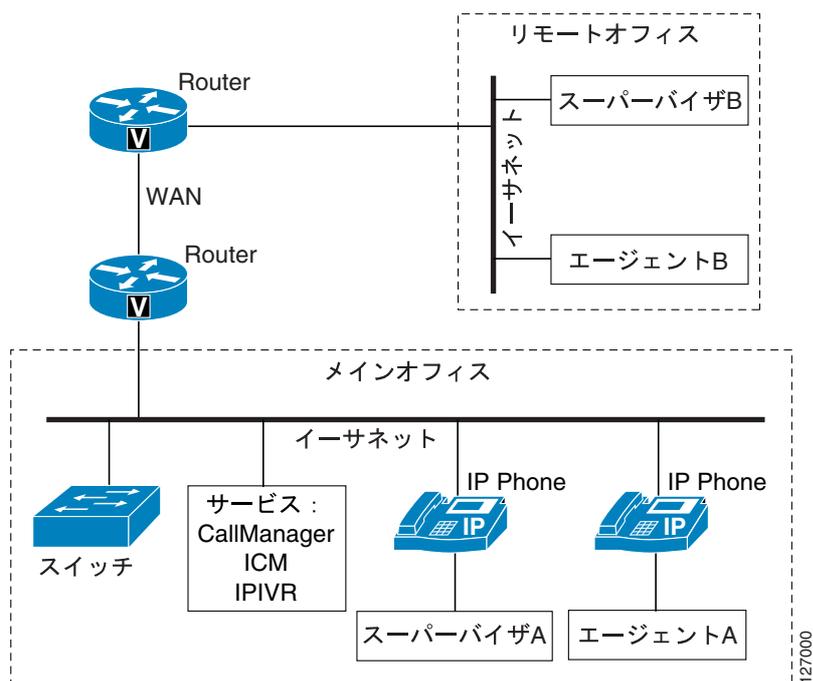
同時監視要求と録音要求の最大数は 21 です (チームごとの許可されている 20 のスーパーバイザそれぞれからの 1 つの監視要求に 1 つの録音要求を加えたもの)。実際には、一度に行われる同時監視 / 録音要求は、通常は 3 ~ 5 未満です。

この説明では、5 つの同時監視 / 録音セッションを使用して、Cisco Agent Desktop の単一のインストールがデスクトップ モニタをサポートする場合の帯域幅の要件の平均を計算します。

IP トラフィック フローのサイレント モニタリング

図 8-2 に、メイン オフィスとリモート オフィスを示します。メイン オフィスでは、リモート オフィスと共有するさまざまな Cisco Desktop サービスとスイッチが使用されています。メイン オフィスとリモート オフィスの両方で、Cisco Agent Desktop エージェントとスーパーバイザが使用されています。この図では、すべてのエージェントとスーパーバイザが同じ Logical Contact Center (LCC; 論理コンタクトセンター) の同じチームに属しています。

図 8-2 コンタクトセンターのモデル



メイン オフィスでは、エージェントとスーパーバイザが IP Phone を使用しています。リモート オフィスでは、エージェントとスーパーバイザはメディア終端 softphone を使用しています。

Cisco Supervisor Desktop へのモニタ サービスの帯域幅の要件

モニタ サービスと監視スーパーバイザ間のトラフィックは、1 つの IP 電話コール (RTP データ ストリーム 2 つ) の帯域幅と等しくなります (「モニタ サービス」とは、VoIP モニタ サービスとデスクトップ モニタ サービスの両方を指します)。

帯域幅を計算する場合、RTP パケット サイズに、ネットワークを介して RTP データを転送するときには使用されるネットワーク プロトコルの追加オーバーヘッドを加える必要があります。

20 ミリ秒の会話データを送信する G.711 パケットの場合は、64 kbps のネットワーク帯域幅が必要となります (表 8-6 を参照してください)。これらのパケットは、4 レイヤのネットワーク プロトコル (RTP、UDP、IP、および Ethernet) によってカプセル化されます。これらのプロトコルによって、それぞれ独自のヘッダー情報が G.711 データに追加されます。これにより、イーサネット フレームにいったんまとめられた G.711 データでは、ネットワーク上を流れるときにデータ ストリームごとに 87.2 kbps の帯域幅が必要となります。IP 電話コールは、2 つのストリーム (A から B へと B から A へ) で構成されています。G.711 コーデックを使用する IP 電話コールの場合、両方のストリームに 87.2 kbps が必要となります。

表 8-6 2 つのデータ ストリームの帯域幅の要件

コーデック	監視スーパーバイザごとの平均 kbps	監視スーパーバイザごとの最大 kbps ¹
G.711	174.4	174.4
G.711 (無音圧縮付き)	61	174.4
G.729	62.4	62.4
G.729 (無音圧縮付き)	21.8	62.4

1. 瞬時最大帯域幅。キャパシティが固定されている物理チャネルで無音圧縮が使用されている場合、音声信号が存在するときにすべての最大帯域幅が必要となるため、このメトリックを考慮する必要があります。

全二重接続の場合、帯域幅速度は、着信トラフィックと発信トラフィックの両方に適用されます (たとえば、100 Mbps の接続の場合、100 Mbps のアップロード帯域幅と 100 Mbps のダウンロード帯域幅があります)。このため、IP 電話コールでは、単一のデータ ストリームに相当する帯域幅が消費されます。このシナリオでは、無音圧縮のない G.711 IP 電話コールに、87.2 kbps の使用可能帯域幅が必要となります。

モニタ サービスでは、監視されるコールそれぞれに対して 2 つのストリーム (両方ともサービスから要求者に送信されます) が送信されます。つまり、監視セッションそれぞれに関して、帯域幅の要件は 2 つのストリーム用となります (G.711 コーデックを使用した 174.4 kbps)。

VoIP モニタ サービスを使用してエージェントの内線を監視している場合、VoIP モニタ サービスとスーパーバイザのコンピュータの間にこの帯域幅が必要となります。図 8-2 では、スーパーバイザ A がエージェント A を監視する場合、メイン オフィス LAN でこの帯域幅が必要となります。リモート オフィスでスーパーバイザ A がエージェント B で監視する場合、リモート オフィスで別の VoIP モニタ サービスが必要となります (図 8-2 を参照)。帯域幅の要件は、WAN リンクにも適用されます。

デスクトップ モニタが使用されている場合、帯域幅の要件は、エージェントのデスクトップとスーパーバイザのデスクトップとの間の帯域幅になります。スーパーバイザ A がエージェント A を監視する場合、メイン オフィス LAN でこの帯域幅が必要となります。リモート オフィスでスーパーバイザ A がエージェント B を監視する場合、帯域幅の要件は、WAN リンクにも適用されます。

録音および統計情報サービスへのモニタ サービスの帯域幅の要件

録音および統計情報サービスは、エージェントの会話を録音する場合に使用されます。録音および統計情報サービスとモニタ サービス間の帯域幅の要件については、表 8-6 を参照してください。

Cisco Supervisor Desktop への録音サービスの帯域幅の要件

Cisco Agent Desktop Release 6.0 では、新しい録音サービスが導入されています。このサービスでは、録音再生用にスーパーバイザに RTP ストリームが送信されます。RTP ストリームに使用される帯域幅は、サイレント モニタリングと同一になります。詳細については、表 8-6 を参照してください。

デスクトップ モニタの帯域幅の要件

VoIP モニタ サービスを使用してコールを監視および録音している場合、サービスのネットワーク接続での帯域幅の要件は、2 つの音声データ ストリームになります。

デスクトップ モニタ サービスが使用されている場合、IP 電話コールはデスクトップ モニタ サービスと同じエージェントで受信されるため、帯域幅の要件に IP 電話コールの追加の負荷が追加されます。

いずれの場合も、帯域幅の要件は、モニタ サービスと要求者との間の帯域幅となります。

- VoIP モニタ サービスからスーパーバイザへ
- エージェント デスクトップからスーパーバイザへ
- VoIP サービスから録音および統計情報サービスへ
- エージェント デスクトップから録音および統計情報サービスへ

表 8-7 および表 8-8 に、単一のデスクトップ モニタ サービスで処理される同時監視セッションに必要なとされる、使用可能な合計帯域幅のパーセンテージを示します。

次の注は、表 8-7 および表 8-8 に示されているデスクトップ モニタ サービスの帯域幅の要件にも適用されます。

- 帯域幅の値は、指定された接続の最も適切な速度に基づいて計算されます。接続の実際の速度は、さまざまな要因により、示されている最高速度とは異なることがあります。
- 帯域幅の要件は、アップロード速度に基づいています。ダウンロード速度は、IP 電話コールの着信ストリームにだけ影響を与えます。

■ ネットワークのプロビジョニング

- データは、無音圧縮のないコーデックを示しています。無音圧縮がある場合、使用される帯域幅は小さくなります。
- 示されているデータには、監視されているコールの会話の品質は考慮されていません。帯域幅の要件が使用可能な帯域幅に近づき、その他のアプリケーションがネットワークへのアクセスを共有する必要がある場合、音声パケットの遅延（パケットの遅延）が、監視されている会話の品質に影響を与えることがあります。ただし、遅延は、録音された会話の品質に影響を与えません。
- データは、監視および録音に必要な帯域幅だけを示しています。データには、本マニュアルのその他の項で説明しているその他の Cisco Agent Desktop モジュールの帯域幅の要件は含まれていません。

表 8-7 無音圧縮なしで G.711 コーデックを使用した同時監視セッションに必要とされる使用可能なアップロード帯域幅のパーセンテージ

同時監視セッション数	必要とされる使用可能なアップロード帯域幅のパーセンテージ							
	100 Mbps	10 Mbps	1.544 Mbps	640 kbps	256 kbps	128 kbps	64 kbps	56 kbps
コールだけ	0.1	0.9	5.6	13.6	34.1	68.1	NS ¹	NS
1	0.3	2.6	16.8	40.9	NS	NS	NS	NS
2	0.4	4.4	28.1	68.1	NS	NS	NS	NS
3	0.6	6.1	39.3	95.4	NS	NS	NS	NS
4	0.8	7.8	50.5	NS	NS	NS	NS	NS
5	1.0	9.6	61.7	NS	NS	NS	NS	NS
6	1.1	11.3	72.9	NS	NS	NS	NS	NS
7	1.3	13.1	84.2	NS	NS	NS	NS	NS
8	1.5	14.8	95.4	NS	NS	NS	NS	NS
9	1.7	16.6	NS	NS	NS	NS	NS	NS
10	1.8	18.3	NS	NS	NS	NS	NS	NS

1. NS は、サポートされていないことを示します。接続の帯域幅は、多数の同時監視セッションのサポートに十分な大きさではありません。

表 8-8 無音圧縮なしで G.729 コーデックを使用した同時監視セッションに必要とされる使用可能なアップロード帯域幅のパーセンテージ

同時監視セッション数	必要とされる使用可能な帯域幅のパーセンテージ							
	100 Mbps	10 Mbps	1.544 Mbps	640 kbps	256 kbps	128 kbps	64 kbps	56 kbps
コールだけ	0.0	0.3	2.0	4.9	12.2	24.4	48.8	55.7
1	0.1	0.9	6.0	14.6	36.6	73.1	NS ¹	NS
2	0.2	1.6	10.0	24.4	60.9	NS	NS	NS
3	0.2	2.2	14.1	34.1	85.3	NS	NS	NS
4	0.3	2.8	18.1	43.9	NS	NS	NS	NS
5	0.3	3.4	22.1	53.6	NS	NS	NS	NS
6	0.4	4.1	26.1	63.4	NS	NS	NS	NS
7	0.5	4.7	30.1	73.1	NS	NS	NS	NS
8	0.5	5.3	34.1	82.9	NS	NS	NS	NS
9	0.6	5.9	38.1	92.6	NS	NS	NS	NS
10	0.7	6.6	42.2	NS	NS	NS	NS	NS

1. NS は、サポートされていないことを示します。接続の帯域幅は、多数の同時監視セッションのサポートに十分な大きさではありません。

VoIP モニタ サービスの帯域幅の要件

次の注は、表 8-9 および表 8-10 に示されている VoIP モニタ サービスの帯域幅の要件に適用されません。

- VoIP モニタ サービスは、より高い負荷を処理するよう設計されているため、監視セッション数はデスクトップ モニタ サービスの場合よりも多くなります。
- 帯域幅の要件は、アップロード速度に基づいています。ダウンロード速度は、IP 電話コールの着信ストリームにだけ影響を与えます。
- 速度の遅い接続の一部は、VoIP モニタ サービスでサポートされていないため、表 8-9 および表 8-10 に示されていません。
- 表 8-9 および表 8-10 の値は、指定された接続の最も適切な速度に基づいて計算されます。接続の実際の速度は、さまざまな要因により、示されている最高速度とは異なることがあります。
- データは、無音圧縮のないコーデックを示しています。無音圧縮がある場合、使用される帯域幅は小さくなります。
- 示されているデータには、監視されているコールの会話の品質は考慮されていません。帯域幅の要件が使用可能な帯域幅に近づき、その他のアプリケーションがネットワークへのアクセスを共有する必要がある場合、音声パケットの遅延（パケットの遅延）が、監視されている会話の品質に影響を与えることがあります。ただし、遅延は、録音された会話の品質に影響を与えません。
- データは、監視および録音に必要な帯域幅だけを示しています。データには、本マニュアルのその他の項で説明しているその他の Cisco Agent Desktop モジュールの帯域幅の要件は含まれていません。

表 8-9 無音圧縮なしで G.711 コーデックを使用した同時監視セッションに必要とされる使用可能なアップロード帯域幅のパーセンテージ

同時監視セッション数	必要とされる使用可能なアップロード帯域幅のパーセンテージ		
	100 Mbps	10 Mbps	1.544 Mbps
1	0.2	1.7	11.2
5	0.9	8.7	56.1
10	1.7	17.4	NS ¹
15	2.6	26.2	NS
20	3.5	34.9	NS
25	4.4	43.6	NS
30	5.2	52.3	NS
35	6.1	61.0	NS
40	7.0	69.8	NS
45	7.8	78.5	NS
50	8.7	87.2	NS

1. NS は、サポートされていないことを示します。接続の帯域幅は、多数の同時監視セッションのサポートに十分な大きさではありません。

表 8-10 無音圧縮なしで G.729 コーデックを使用した同時監視セッションに必要とされる使用可能なアップロード帯域幅のパーセンテージ

同時監視セッション数	必要とされる使用可能なアップロード帯域幅のパーセンテージ		
	100 Mbps	10 Mbps	1.544 Mbps
1	0.1	0.6	4.0
5	0.3	3.1	20.1
10	0.6	6.2	40.2
15	0.9	9.4	60.2
20	1.2	12.5	80.3
25	1.6	15.6	NS ¹
30	1.9	18.7	NS
35	2.2	21.8	NS
40	2.5	25.0	NS
45	2.8	28.1	NS
50	3.1	31.2	NS

1. NS は、サポートされていないことを示します。接続の帯域幅は、多数の同時監視セッションのサポートに十分な大きさではありません。

Cisco Desktop Base サービスへの Cisco Supervisor Desktop の帯域幅の要件

前の項で説明されている帯域幅の要件以外に、Cisco Supervisor Desktop から Cisco Agent Desktop Base サービスへのトラフィックがあります。

スーパーバイザのチームのエージェントごとに、2 キロバイトのコールごとの帯域幅が Cisco Supervisor Desktop とチャット サービス間で送信されています (表 8-11 を参照)。

表 8-11 一般的なエージェント コールの Cisco Supervisor Desktop の帯域幅

サービス	Cisco Supervisor Desktop へ	Cisco Supervisor Desktop から
CTI OS	0	0
Cisco Agent Desktop Base	1650	550
Cisco Agent Desktop Recording	0	0
Cisco Agent Desktop VoIP Monitor	0	0
合計	1650	550

同じ一般的なコール シナリオを使用して、Cisco Agent Desktop と Cisco Supervisor Desktop の帯域幅測定値をキャプチャしています。詳細については、「一般的なコール シナリオ」(P.8-16) を参照してください。

スーパーバイザのチームにエージェントが 10 名あり、それぞれのエージェントが毎時 20 のコールを受信する場合、トラフィックは次のようになります。

$$\begin{aligned}
 &10 \text{ エージェント} * \text{毎時 } 20 \text{ コール} = \text{毎時 } 200 \text{ コール} \\
 &200 \text{ コール} * \text{コールごとに } 1650 \text{ バイト} = \text{毎時 } 330,000 \text{ バイト} \\
 &(330,000 \text{ バイト}) / (\text{毎時 } 3600 \text{ 秒}) = 92 \text{ kBps} \\
 &92 \text{ kBps} * \text{バイトごとに } 8 \text{ ビット} = 736 \text{ kbps}
 \end{aligned}$$

スーパーバイザがレポートを表示しているか、サイレント モニタ セッションが開始または停止された場合は、追加のトラフィックが送信されます。

エージェント詳細レポート

このレポートは、30 秒ごとに自動的にリフレッシュされます。表 8-12 に、レポート要求ごとの帯域幅の使用状況を示します。

表 8-12 エージェント詳細レポートの帯域幅の使用状況（レポートごとの平均バイト）

サービス	エージェント詳細レポート	
	Cisco Supervisor Desktop へ	Cisco Supervisor Desktop から
CTI OS	0	0
Cisco Agent Desktop Base	220	200
Cisco Agent Desktop Recording	0	0
Cisco Agent Desktop VoIP Monitor	0	0
合計	220	200

エージェント詳細レポートを表示しているスーパーバイザの帯域幅は、次のようになります。

$$\begin{aligned} & \text{要求ごとに 220 バイト} * \text{毎分 2 要求} = \text{毎分 440 バイト} \\ & (\text{毎分 440 バイト}) / (\text{毎分 60 秒}) = 7 \text{ Bps} \end{aligned}$$

チーム エージェント統計情報レポート

この機能は、スーパーバイザがレポートを開いた場合に発生する一度だけの転送です（自動的にリフレッシュされません）。スーパーバイザは、レポートを手動でリフレッシュできます。表 8-13 に、レポート要求ごとの帯域幅の使用状況を示します。

表 8-13 チーム エージェント統計情報レポートの帯域幅の使用状況（レポートごとの平均バイト）

サービス	チーム エージェント統計情報レポート	
	Cisco Supervisor Desktop へ	Cisco Supervisor Desktop から
CTI OS	0	0
Cisco Agent Desktop Base	エージェントごとに 250	200
Cisco Agent Desktop Recording	0	0
Cisco Agent Desktop VoIP Monitor	0	0
合計	エージェントごとに 250	200

チーム スキル統計情報レポート

このレポートは、30 秒ごとに自動的にリフレッシュされます。表 8-14 に、レポート要求ごとの帯域幅の使用状況を示します。

表 8-14 チーム スキル統計情報レポートの帯域幅の使用状況（レポートごとの平均バイト）

サービス	チーム スキル統計情報レポート	
	Cisco Supervisor Desktop へ	Cisco Supervisor Desktop から
CTI OS	0	0
Cisco Agent Desktop Base	スキルごとに 250	200
Cisco Agent Desktop Recording	0	0
Cisco Agent Desktop VoIP Monitor	0	0
合計	スキルごとに 250	200

チーム内の 10 のスキルを含むチーム スキル統計情報レポートを表示しているスーパーバイザの帯域幅は、次のようになります。

$$\begin{aligned} & \text{スキルごとに } 250 \text{ バイト} * 10 \text{ スキル} * \text{毎分 } 2 \text{ 要求} = \text{毎分 } 5000 \text{ バイト} \\ & (\text{毎分 } 5000 \text{ バイト}) / (\text{毎分 } 60 \text{ 秒}) = 83 \text{ Bps} \end{aligned}$$

監視要求の開始および停止

サイレント モニタリング セッションの開始または停止を要求すると、表 8-15 に示されているように、要求ごとに一度だけ帯域幅が使用されます。

表 8-15 サイレント モニタリングを開始または停止する場合の帯域幅の使用状況（要求ごとの平均バイト）

サービス	モニタリングの開始		モニタリングの停止	
	Cisco Supervisor Desktop へ	Cisco Supervisor Desktop から	Cisco Supervisor Desktop へ	Cisco Supervisor Desktop から
CTI OS	0	0	0	0
Cisco Agent Desktop Base	775	450	0	0
Cisco Agent Desktop Recording	0	0	0	0
Cisco Agent Desktop VoIP Monitor	275	500	150	325
合計	1050	950	150	325

サービスの配置に関する推奨事項

表 8-16 に、デスクトップへの帯域幅を最小限に抑えるためのサービスの配置に関する推奨事項の概要を示します。これらの推奨事項は、中央集中型のコール処理およびリモート エージェントを使用する配置に適用されます。

表 8-16 サービスの配置に関する推奨事項

サービス	場所	理由
Cisco Agent Desktop Base サービス	セントラル	中央集中型 IPCC コンポーネントへの送受信トラフィックは、デスクトップへの送受信トラフィックを上回ります。
VoIP モニタ サービス	リモート（エージェントの近く）	サービスへのエージェント トラフィックのスパイク。サイレント モニタリングと録音の場合は、これは推奨事項ではなく要件となります。
録音サービス	1 つの場所にある場合はエージェントとスーパーバイザの近く。1 つの場所がない場合は中央	CTI がありません。デスクトップへの送受信トラフィックおよび VoIP モニタ サービスからのトラフィックが多くあります。
Cisco Desktop Supervisor	エージェントと同じ場所	VoIP モニタ サービスの近く。

リモート ロケーションが複数ある場合は、リモート ロケーションそれぞれに VoIP モニタ サービスがある必要があります。複数の VoIP モニタ サービスは、単一の論理コンタクトセンターでサポートされています。録音および統計情報サービスは、WAN 接続でトラフィックを処理できる場合、中央の場所に移動できます。処理できない場合は、各サイトに、独自の論理コンタクトセンターがあり、Cisco Desktop ソフトウェアがインストールされている必要があります。

QoS に関する考慮事項

重要でプライオリティ キューに入れる必要のあるトラフィック フローを考慮する場合、これらのトラフィックを次の重要度順でランク付けします。

1. 顧客への対応状況
2. エージェントの対応状況
3. スーパーバイザの対応状況
4. 管理者の対応状況

サービス間のフローのこのランク付けでは、エンタープライズ サービスと CTI サービス（コール イベント）の間のトラフィックが最も重要となります。表 8-16 に示されているサービスの配置に関する推奨事項に基づいて、両方のサービスが中央の場所にある必要があります。ただし、QoS に関する考慮事項が適用されます。

このトラフィックは、音声コール制御およびシグナリング トラフィックと同様に、AF31 に分類される必要があります。また、Cisco Agent Desktop と CTI サービス（コール イベント、コール制御）間の送受信トラフィックも優先順位が付けられ、AF31 に分類される必要があります。

IP Phone エージェントの場合、IP Phone エージェント サービスと CTI サービスとの間の通信も重要となります。これは、この通信が、エージェントがエージェント状態をどれだけすばやく変更できるかに影響を及ぼすためです。このトラフィックも AF31 に分類される必要があります。



(注)

シスコでは、音声制御プロトコルのマーキングを DSCP 26 (PHB AF31) から DSCP 24 (PHB CS3) に変更し始めています。ただし、多くの製品では、シグナリング トラフィックが DSCP 26 (PHB AF31) としてマーキングされています。このため、シスコでは、コール シグナリングに対して暫定的に AF31 と CS3 の両方を予約しておくことをお勧めします。

Cisco Agent Desktop からチャット サービス（エージェント情報、コール ステータス）への送受信トラフィックはそれほど重要ではなく、AF21 または AF11 に分類される必要があります。

Cisco Desktop コンポーネントによるポートの使用

ネットワークの使用状況の詳細については、次の URL にある『Cisco Contact Center Product Port Utilization Guide』を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/icm/port_uti/index.htm

Desktop アプリケーションでは、サイレント モニタリング、録音、および録音再生用にデスクトップ モニタ ソフトウェア、VoIP モニタ サービス、または録音サービスから受け取る RTP パケットにだけタグが付けられます。

Citrix シンクライアント環境への Cisco Agent Desktop Release 6.0 の統合

Citrix シンクライアント環境に Cisco Agent Desktop Release 6.0 アプリケーションをインストールするためのガイダンスについては、次の URL にある『Integrating CAD 6.0 into a Citrix Thin-Client Environment』のマニュアルを参照してください。

http://www.cisco.com/application/pdf/en/us/partner/products/ps427/c1244/cdcont_0900aecd800e9db4.pdf

