CHAPTER 11

データ通信要件の決定

ICM システムには、十分なリアルタイム応答性と耐障害性を備えた、信頼性の高いネットワークが必要になります。ICM システムはミッション クリティカルな耐障害性システムであるため、何らかの理由でノードがオフラインになった場合に迅速に対応できる必要があります。場合によっては、通信パスを切り替えたり、別のノードをアクティブにしたりして、システムを中断せずに稼働し続けることが求められます。

ノード障害に対応する以外にも、障害の発生したノードを診断して、できるだけ早くサービスに復帰させる必要があります。多くの場合、Wide Area Network（WAN; ワイドエリア ネットワーク）を介して ICM の診断プロシージャを実行することになります。

また、ICM システムは、Interexchange Carriers（IXC; 長距離通信会社）からのルート要求に対して、特定の最小タイムアウト期間内に応答する必要があります。たとえば、AT&T インテリジェント コール処理ネットワークからルート要求を受信した場合は、200 ミリ秒以内に応答する必要があります。これは、地理的に分散している ICM 構成の場合、セントラル コントローラの両サイドにある NIC および CallRouter と通信を行ってルート応答するまでの全処理を、200 ミリ秒のタイムアウト期間内に完了する必要があることを意味します。

この章では、ICM システムをインストールするためのネットワーク ファシリティの準備について説明します。この章では、次のタスクを完了します。

- **ビジブル ネットワークおよびプライベート ネットワークの要件を決定します。**ICM ネットワークは、最低の帯域幅要件および遅延要件を満たす必要があります。

- **IP アドレスを割り当てます。**システムの各サイトの ICM ノードについて、IP アドレス要件を評価します。
- **IP アドレス ワークシートに記録します。**第 13 章「IP アドレス ワークシート」のワークシートを使用して、IP アドレスを割り当てます。
- **追加のネットワーク　ハードウェアを注文します。** ネットワーク　ファシリティの準備では、ルータ、ブリッジ、ケーブルなどの発注が必要になる場合があります。

この章では、ICM ネットワークを構成して既存のネットワークに統合するオプションについても説明します。

ICM サイト

ICM システムは、多数のコンピュータまたはノードで構成されます。通常、それらのコンピュータやノードは複数のサイトに配置されます。ICM システムは、3 ～ 50 以上の任意のサイトに分散できます。各サイトには 1 つまたは複数のノードが含まれます。ICM システムには、サイト内やサイト間でノードを相互接続するためのネットワークがいくつか必要になります。

ICM サイトの基本的なタイプとして、次の 3 つがあります。

- **セントラル サイト**：セントラル コントローラ（つまり CallRouter と Logger）の一方または両方のサイドが含まれます。ネットワーク インターフェイス コントローラが含まれる場合もあります。セントラル サイトにはアドミン ワークステーションとペリフェラル ゲートウェイが含まれることもあります。
- **コンタクト センター サイト**：1 つまたは複数のペリフェラル ゲートウェイ（PG）が含まれます。アドミン ワークステーションが含まれる場合もあります。このサイトでは、エージェント、電話アプリケーション、および CTI アプリケーションもサポートされます。
- **管理サイト**：1 つまたは複数のアドミン ワークステーションが含まれます。

これらのサイトを 2 つ以上組み合せた ICM サイトも存在します。たとえば、1 つの場所がセントラル サイトとコンタクト センター サイトを兼ねる場合もあります。

ICM ネットワーク

ICM システムでは、それぞれ独立した 3 つの通信ネットワークを使用します。

- **プライベート ネットワーク**：外部から干渉を受けない、特定のノードどうしで通信を行うための専用ネットワークです。このネットワークでは、システムの同期を維持し復元するために必要なデータがやりとりされます。プライベート ネットワークは、これ以外の目的では使用しません。
- **ビジブル ネットワーク**：セントラル コントローラがローカル ノードやリモート ノードと通信するための共有ネットワークです。このネットワークでは、同期化されているシステムの各サイドと外部システムとの間のトラフィックがやりとりされます。ビジブル ネットワークは、ノード障害とネットワーク障害を区別するための代替ネットワークとして、耐障害性ソフトウェアによって使用される場合もあります。
- **シグナリング アクセス ネットワーク**：このネットワークは、ICM システムをキャリア ネットワークまたはクライアント ネットワークに接続します。SAN が実装されている場合、ICM システムはプライベート ネットワークではなく SAN を使用して、キャリア ネットワークと通信します。シグナリング アクセス ネットワークが使用されるのは、提供されている環境だけです。

図 11-1 は、セントラル コントローラの 2 つのサイド、コンタクト センター サイト、および管理サイトを示しています。デュプレックス構成のセントラル コントローラの両サイドは、プライベート WAN でリンクされています。コンタクト センターと管理サイトは、ビジブル WAN を通してセントラル コントローラの各サイドにリンクされています。各サイト内のノードはローカルエリア ネットワーク（LAN）でリンクされています。

図 11-1　ICM システム ネットワークの概要

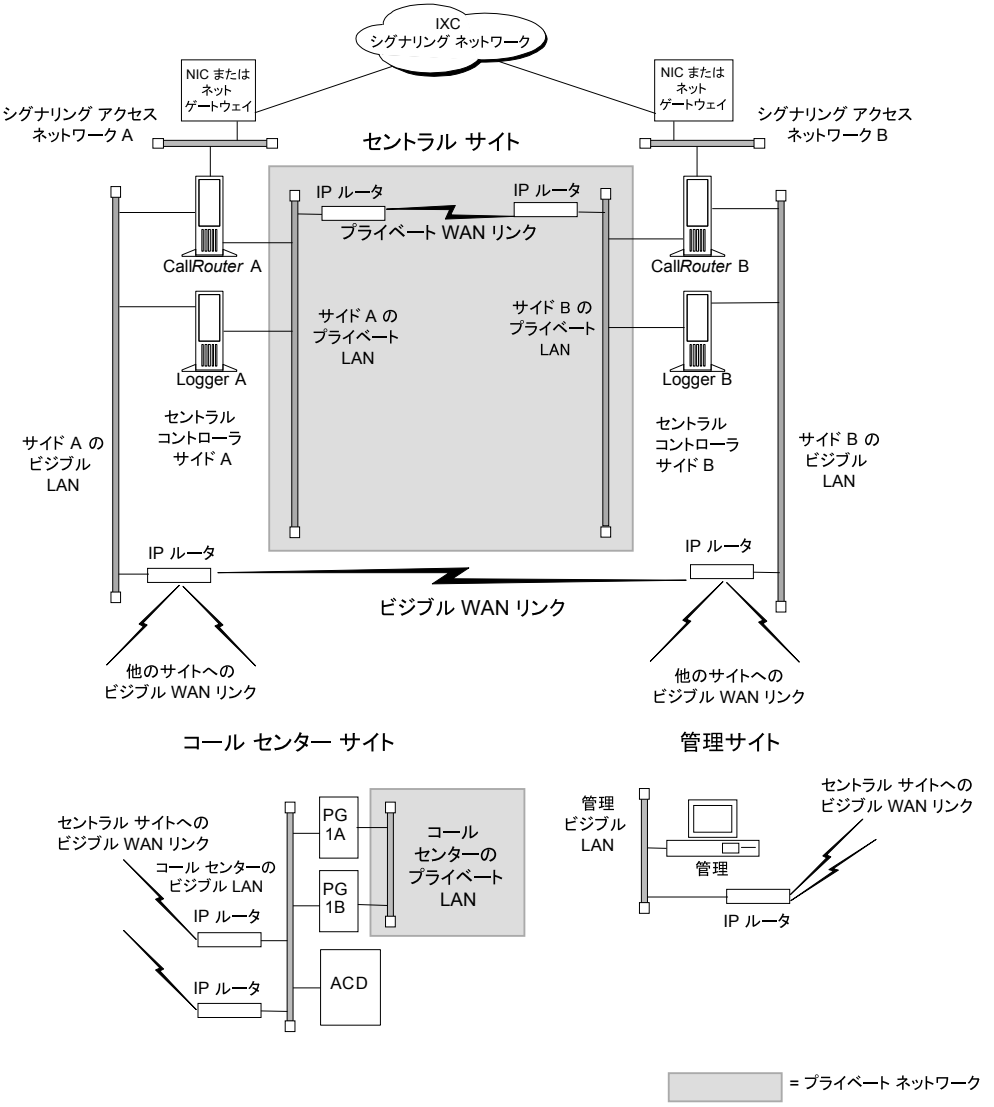


図 11-1 では、セントラル コントローラの 2 つのサイドは地理的に離れています。プライベート ネットワークおよびビジブル ネットワークのワイドエリア ネットワーク接続は、*WAN リンク*と呼ばれています。通常、ICM システムの WAN リンクは高アベイラビリティ回線になります。これらのリンクでは、遅延特性がきわめて低く予期可能であることが必要とされます。このため、一部のタイプの WAN サービス（たとえばパケット ルーティングなど）は ICM システムの WAN リンクに使用できません。

プライベート WAN リンクとビジブル WAN リンク

デュプレックス構成の ICM セントラル コントローラの 2 つのサイドは、単一のプライベート ネットワークを共有しており、*プライベート WAN リンク*を通してリンクされています。また、*ビジブル WAN リンク*を通して 2 つのサイドを接続するビジブル ネットワークを共有しています。高レベルの耐障害性を確保するには、プライベート WAN リンクとビジブル WAN リンクをそれぞれ独立させる（別のトランクを使用し、場合によっては異なるサービス プロバイダーを使用する）必要があります。

セントラル コントローラの 2 つのサイドが併設される場合、サイト間のビジブル WAN リンクは不要です。リモート コンタクト センター サイトへの標準のビジブル WAN リンクが、両サイド間に必要な接続性を提供します。セントラル コントローラの併設構成では、プライベート ネットワークはイーサネット スイッチを使用して、ローカルで実装されます。

リモート コンタクト センターは、ビジブル ネットワークを通してセントラル コントローラの各サイドに接続します。コンタクト センターへの各ビジブル WAN リンクには、コンタクト センターの PG と AW をサポートするだけの十分な帯域幅が必要です。帯域幅の要求は、構成（コール負荷やエージェントの数など）によって大きく変化します。

コンタクト センターがセントラル コントローラの一方のサイドと併設される場合、PG と AW はそのサイドのビジブル LAN に接続されます。PG と AW は、セントラル コントローラのもう一方のサイドにビジブル WAN リンクを通して接続されます。このような構成では、セントラル コントローラの両サイド間に直接のビジブル WAN リンクを用意して、両サイド間に十分な接続性を確保する必要があります。オプションとして、LAN ブリッジを配備して PG を AW LAN セグメントから分離し、LAN の停止に対する保護能力を強化できます。

（注）　併設構成のセントラル コントローラの例については、「セントラル サイト」（P.11-26）の項を参照してください。

シグナリング アクセス ネットワーク

CallRouter マシンは、Signaling Access Network（SAN; シグナリング アクセス ネットワーク）を通して IXC シグナリング ネットワークに接続します。CallRouter 内の別個の LAN インターフェイス カードが、SAN 専用として使用されます。デュプレックス構成システムの各サイドにある NIC は、SAN によって IXC シグナリング ネットワークに接続されます。多くの場合、NIC ソフトウェアは CallRouter コンピュータで実行されます。図 11-1 では、説明をわかりやすくするために、SAN に設置された独立したコンピュータとして NIC が示されています。

SAN に ICM ネットワーク ゲートウェイというノードが設置され、SS7 ベースの一部のネットワークとのインターフェイスに使用される場合もあります。ICM ネットワーク ゲートウェイは、SS7 プロトコルのハンドリング サービスを提供する専用マシンです。

ローカルエリア ネットワーク

ICM システムでは、ローカルエリア ネットワークの接続にイーサネットを使用します。アーキテクチャの観点からは、どのイーサネット トポロジを採用するかはあまり重要ではありません。ただし、ネットワーク管理またはシステム管理の観点からは、採用するトポロジに考慮が必要になる場合があります。プライベート、ビジブル、およびシグナリング アクセスの LAN には、通常 UTP が使用されます。

3 つのネットワーク（プライベート、ビジブル、およびシグナリング）は、それぞれ異なる LAN セグメントにする必要があります。つまり、CallRouter マシンで 3 つのイーサネット カードが必要になります。

ネットワーク帯域幅の要求

一般的な ICM システムにおけるビジブル ネットワークの帯域幅要求は、コール データを搬送するネットワークで 1 コール当たり約 1,000 バイトです。たとえば、コンタクト センター サイトで 1 秒当たり 15 コールを管理するリモート PG は、ビジブル WAN を通してセントラル サイトに毎秒 15,000 バイトのデータを転送する必要があります（パケットのオーバーヘッドを除いた場合、合計 120,000 ビット / 秒）。

デュプレックス構成のセントラル コントローラの両サイドをつなぐプライベート WAN には、全 ACD サイトの総コール負荷をサポートできるだけの帯域幅が必要です。また、耐障害性のメッセージングや同期化が行えるように、帯域幅にある程度のバースト耐性と十分なキャパシティを確保することも必要になります。

表 11-1 に、ICM システム内のビジブル ネットワークおよびプライベート ネットワークのネットワーク回線要件を示します。

表 11-1　ネットワーク回線要件

ネットワーク	目的	ファシリティ	最低帯域幅
プライベート WAN	デュプレックス構成の分散された ICM セントラル コントローラの両サイドを接続する専用パス。	T1	T1 専用線
ビジブル WAN	リモート サイトにある PG と AW を、ICM セントラル コントローラの各サイドに接続する回線。	通常 T1 またはフラクショナル T1。	128 Kbps 専用線[1]
シグナリング アクセス ネットワーク	NIC を IXC キャリア ネットワークまたはクライアント ネットワークに接続するローカルエリア ネットワーク。[2]	イーサネット シールドなしツイストペア（UTP）。	100 Mbps
ビジブル LAN およびプライベート LAN	セントラル サイトの ICM ノードを、リモート コンタクト センター サイトの PG および AW に接続するローカルエリア ネットワーク（図 11-1 の例を参照）。	イーサネット シールドなしツイストペア（UTP）。シスコでは、管理可能ハブの使用を必須としています。	100 Mbps

1. 負荷によって異なります。Quality of Service（QoS）対応ネットワークに必要な最低帯域幅の計算方法については、「QoS 帯域幅要求の計算」（P.11-19）の項を参照してください。
2. Sprint NIC の場合、ローカル イーサネット シグナリング アクセス ネットワークは実装されません。その代わりに、CallRouter プラットフォームの X.25 WAN カードがシグナリング アクセス ネットワークとして機能し、CallRouter - NIC マシンを IXC シグナリング ネットワークに接続します。

ビジブル WAN に、追加の帯域幅が必要になる場合があります。実際の要件は、コール負荷、ACD の数、エージェントの数、管理サイトの数など、さまざまな要因によって変化します。

（注）　ネットワークで Cisco ICM Quality of Service（QoS）機能を利用する場合は、帯域幅に関する追加の考慮事項について、「Cisco ICM QoS」（P.11-14）を参照してください。

ネットワーク遅延の要件

ICM システムは、リアルタイムの耐障害性分散システムです。ICM システムの WAN リンクでは、システムのリアルタイム特性を維持し、耐障害性に使用される方式をサポートするために、遅延特性がきわめて低く予期可能であることが必要とされます。これは、次のような重要な部分について特に必要とされます。

- CallRouter/NIC と IXC の間のルート要求およびルート応答。この通信では、キャリア ネットワークの厳しいメッセージ遅延要件を満たす必要があります。
- PG からのポストルーティング要求や CallRouter からのルート応答に関わる通信。オンラインの発信者が、適切なエージェントによるコール応答を期待している状況であるため、この通信も高速で行われる必要があります。
- コンタクト センターのリアルタイム状態に関する、PG から CallRouter への通信。CallRouter はコンタクト センターからの最新データに基づいてルーティングを決定するため、この情報が必要になります。

ICM システムの 3 つの耐障害性メカニズムでは、信頼できる、低遅延の通信が必要とされます。3 つのメカニズムとは、ハートビート検出、同期、および状態転送です。

（注）　ネットワークで Cisco ICM Quality of Service（QoS）機能を利用する場合は、遅延に関する追加の考慮事項について、「Cisco ICM QoS」（P.11-14）を参照してください。

ハートビート検出

耐障害性の設計の一環として、ICM システムは、何らかの理由（通常、ノードまたはネットワーク リンクの障害）でコンポーネントがオフラインになった場合に迅速に対応できる必要があります。システムの重要コンポーネントは、オンラインであることを知らせるために、ネットワークに向けて短いメッセージを定期的に送信しています。このメッセージを*ハートビート*と呼びます。

通信を行う ICM コンポーネントは、一定の間隔で互いにハートビートを送信しています。ハートビートの受信に連続 5 回失敗した場合は、コンポーネントまたはネットワーク リンクに障害が発生していると判断して、回復処理を開始します。表 11-2 に、ハートビートを送信するノード、ハートビートが送信されるネットワーク、およびハートビートの送信頻度を示します。

表 11-2　ハートビートの設定

ノード	中	間隔
AT&T NIC（またはネットワーク ゲートウェイ）から CallRouter	シグナリング アクセス ネットワーク	200 ミリ秒
CallRouter から CallRouter	プライベート ネットワーク	100 ミリ秒
PG から CallRouter	ビジブル ネットワーク	400 ミリ秒
PG から PG（デュプレックス構成の場合）	プライベート ネットワーク	100 ミリ秒

デュプレックス構成の ICM セントラル コントローラの両サイドでは、相手が正しく稼働しているかどうかを互いに定期的にテストしています。表 11-2 に示すとおり、プライベート ネットワークを介した CallRouter 間のネットワーク遅延では、100 ミリ秒のラウンドトリップ メッセージングをサポートする必要があります。プライベート ネットワークの帯域幅が不十分な場合、パケットを IP ルータでフラグメント化して、長いメッセージ (1,500 バイトを超えるメッセージ）が流れるのを防止する必要があります。このような長いメッセージは User Diagram Protocol（UDP）パケットの転送遅延の原因となります。これはセントラル コントローラのもう一方のサイドがまだ稼働中であることを示すものです。

（注） ICM 5.0(0) 以降では、UDP の代わりに TCP キープアライブが使用されています。ただし、5.0(0) より前の PG が 5.0(0) または 6.0(0) セントラル コントローラとともに使用されている場合は、UDP が引き続き使用される場合があります（アップグレード中を除き、この構成はサポートされません）。ICM 7.0(0) では UDP は使用されません。

その他の耐障害性要件として、セントラル コントローラのもう一方のサイドがメッセージのコピーの受信について確認応答するまで、メッセージを解放して NIC または PG に戻すことができないという要件があります。このため、キャリア ネットワークで課せられる 200 ミリ秒の応答時間要件を満たし、キューイングにかかる時間もある程度考慮すると、100 ミリ秒のラウンドトリップ要件が課せられることになります。

リモート PG から CallRouter へのハートビートは、ビジブル WAN 上の他のネットワーク トラフィックと競合します。

同期

デュプレックス構成のセントラル コントローラでは、プライベート ネットワークにより、両サイドの CallRouter と Logger が同期した状態で実行されます。これは、システムの両サイドの CallRouter プロセスと Logger プロセスが同一の入力を受信して、同じ出力を生成するという意味です。

同期を行うために、CallRouter または Logger に対する各メッセージは、CallRouter ノード上で実行されるシンクロナイザ プロセスで受信されます。*シンクロナイザ*は、もう一方のサイドのシンクロナイザにプライベート ネットワーク経由でメッセージを転送します。シンクロナイザは、そのメッセージから重複を取り除いて CallRouter プロセスに渡します。Logger に対するメッセージである場合は、CallRouter がメッセージを Logger に渡します（図 11-2）。

図 11-2　　シンクロナイザの役割

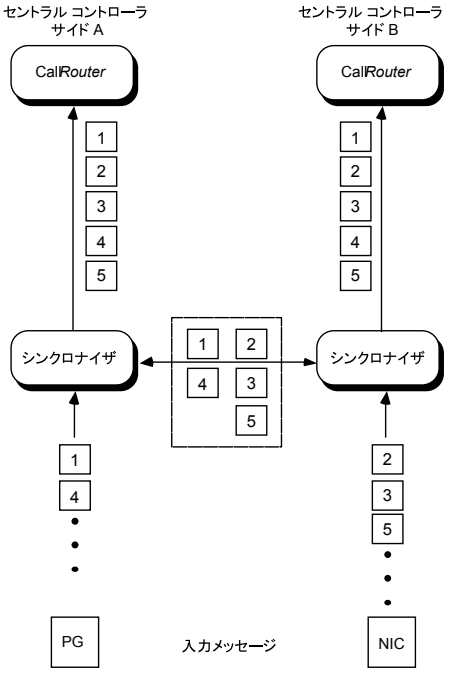


図 11-2 は、シンクロナイザが入力メッセージを組み合せて、セントラル コントローラの各サイドに対して同様にメッセージを送信する方法を示しています。両方の CallRouter が同じ入力を受信して、同じ出力を生成します。シンクロナイザにより、セントラル コントローラの両サイドで、同一コールに対して同じ宛先が返され、データベースに同じデータが書き込まれます。

状態転送

ICM システムの耐障害性により、障害発生後にノードが再始動されます。しかし、障害の発生したノードが再始動する際、メモリ内の変数値は最新の値ではなくなっています。ICM システムは、サービスにノードを戻す前に、もう一方のサイドの自身のピアから値を取得して、回復するノードにコピーする必要があります。つまり、稼働中のマシンの状態を回復対象のマシンに転送する必要があります。この転送はプライベート ネットワークを通して行われます。

この状態転送は、障害の発生後、同期対象 MDS クライアントが再始動した後に行われます（MDS クライアントとは、PG、Logger、CallRouter などです）。

異なるファシリティ

セントラル コントローラ間のプライベート WAN（セントラル コントローラが地理的に分散しているとき）とビジブル WAN は別々のファシリティ上にあることが**必要です**。回線と IP ルータは別のものを使用する必要があります。さらに保護を強化するには、プライベート WAN リンクとビジブル WAN リンクに別々のルートを使用したり、別のサービス プロバイダーを使用することも考えられます。このようにしないと、単一のネットワーク障害が原因で ICM プライベート WAN とビジブル WAN の両方が使用できなくなるリスクを抱えることになります。

たとえば、プライベート WAN に障害が発生したり、セントラル コントローラの 1 つのサイドのビジブル WAN リンクに障害が発生しても、ICM システムはコールのルーティングを継続して、通常どおりに機能し続けます。しかし、プライベート WAN とビジブル WAN が同じファシリティ上にあり、同時に障害が発生した場合、システムの耐障害性は失われます。このシナリオでは、セントラル コントローラのいずれかのサイドのノードの 1 つに障害が発生すると、システム処理が中断します。プライベート WAN とビジブル WAN を別々のファシリティでプロビジョニングすることで、このような潜在的な障害ポイントを排除できます。

Cisco ICM QoS

この項では、Cisco ICM Quality of Service（QoS）機能について説明します。また、QoS を使用した ICM ネットワークのプランニングおよび展開に関する考慮事項を紹介します。

Quality of Service（QoS）について

QoS は、データ通信ネットワークのパフォーマンス レベルを定義するための機能セットです。QoS ではネットワーク トラフィックに対して差別化サービスを作成できるため、特定のネットワーク トラフィックに対してよりよいサービスを提供できます。たとえば、QoS を使用すると、重要なトラフィックの帯域幅を増やし、重要でないトラフィックには少ない帯域幅を割り当てることで、安定したネットワーク応答を実現できます。これにより、高価なネットワーク接続の効率的な使用や、ネットワーク カスタマーとのサービス レベル契約の締結が可能になります。また、ICM コンポーネントとの接続のために専用線を敷設する必要がなくなります。

QoS 機能により、ICM ソフトウェアは次のようなアーキテクチャ面の制限を克服できます。

- ICM ソフトウェアには専用線が必要です。これは、費用効果が高く転送キャパシティのあるコンバージド ネットワークに、ICM を展開できないということを意味します。
- LAN セグメント間での輻輳制御メカニズムの欠如。LAN リソースは一般的に WAN リソースよりも安価であるため、これが問題になることはあまりありません。しかし、LAN でマルチメディア アプリケーションの使用が多くなると、LAN スイッチ経由の遅延が問題になることがあります。このような遅延については、QoS テクノロジー 802.1p が対応しています。
- シスコの Architecture for Voice, Video and Integrated Data（AVVID）企業ネットワーク アーキテクチャのサポートの欠如。AVVID は、コンバージド ネットワーク環境へのミッション クリティカル アプリケーションの統合を最適化するためのネットワーク設計の原則を定義します。QoS は AVVID の主要テクノロジーです。Cisco AVVID ネットワークに適切に展開するには、ICM を AVVID に準拠させる必要があります。

- 問題のある UDP ハートビート。UDP ハートビートの使用は、ファイアウォールや Network Address Translation（NAT; ネットワーク アドレス変換）環境では、ICM 展開を不必要に複雑にします。この理由から、ICM QoS 実装では UDP ハートビートに代わって TCP キープアライブ メッセージが使用されます。

QoS を実装するには、ネットワーク デバイス（ルータおよびスイッチ）に QoS ポリシーを定義し、それらのポリシーを DSCP マーキング、IP precedence、IP アドレス、ポートなどに基づいてトラフィックに適用します。

QoS は特に、インターフェイスを通るトラフィック量がインターフェイスの帯域幅より多いときに効果を発揮します。帯域幅を超えるトラフィックがインターフェイスを通る場合、パケットが 1 つ以上のキューを形成し、デバイスは次に送信するパケットをそこから選択します。デバイスまたはインターフェイスでキューイングのプロパティを設定することで、キューに対するサービスの提供方法を制御できます。このようにして、トラフィックの優先順位を決定できます。

ICM 7.0(0) は、パブリック ネットワーク リンク（PG を CC に接続する）とプライベート ネットワーク リンク（PG または CC のデュプレックス構成のサイドを接続する）の両方において、DSCP マーキングと 802.1p マーキングをサポートしています。

Cisco ICM QoS の導入

QoS の導入と実装のプロセスは、シスコ システム エンジニア、ICM 展開グループ、およびシスコ パートナーが共同でサポートする作業です。これらのシスコ担当者は、QoS の導入を計画しているお客様を次のように支援します。

- カスタマー要件を定義する。シスコ プロフェッショナル サービスおよびシスコ パートナは、お客様の ICM 展開に関する履歴情報や QoS 帯域幅計算ツールを使用して、お客様の要件を評価します（「QoS 帯域幅要求の計算」（P.11-19）を参照）。
- お客様の QoS 移行計画の ICM の部分を評価する。
- お客様と協議して、シスコが提供するサポート　レベルを明記した作業明細書を作成する。

ICM 環境における QoS 対応ネットワークの実装を計画する際、上記のタスクのほか、次のようなタスクについて検討が必要になります。

- トラフィックをマーキングする場所の決定
- QoS マーキングの決定
- 帯域幅要求の算出
- Microsoft Packet Scheduler のインストール（オプション）
- 802.1p 対応ネットワーク コンポーネントのインストールと設定（オプション）
- IP ルータでの QoS の設定

トラフィックをマーキングする場所

QoS のプランニングでは、トラフィックをマーキングする場所（アプリケーション内またはネットワーク エッジ）についての検討が必要になります。アプリケーション内でトラフィックをマーキングすれば、トラフィックを分類するためのアクセス リストが IP ルータまたはスイッチに保存されます。これは、IP アドレス、ポート、およびその他の TCP/IP ヘッダー フィールド（または、これらのいずれかの情報）でトラフィック フローを区別できない場合に使用できる唯一のオプションです。すでに説明したとおり、現在 ICM ではセントラル コントローラと PG 間のビジブル ネットワーク接続、および、Router または PG のデュプレックス構成のサイド間のプライベート ネットワーク接続における DSCP マーキングをサポートしています。また、Windows Packet Scheduler とともに展開した場合、シェーピングと 802.1p もサポートされます。

ICM サーバでマーキングが行われない場合や QoS 信頼が無効な場合、エッジ IP ルータまたはスイッチで、トラフィックのマーキングや再マーキングを行うことが可能です。ネットワーク内の優先権のないユーザが、自身のパケットの DSCP または 802.1p の値を不正に高く設定して、優先的にサービスを受けようとする行為を防止するために、QoS 信頼が無効にされる場合があります。エッジ ルータおよびエッジ スイッチでの分類基準の定義については、次の項の表 11-3 および表 11-4 を参照してください。

QoS マーキングの決定

ICM QoS のデフォルト マーキングは、Cisco AVVID の推奨事項に準拠するように設定されています（必要であれば、設定を上書きできます）。Cisco AVVID のパケット分類の詳細については、『*Cisco AVVID Solution IP Telephony QoS Classification*』を参照してください。

QoS を実装する前は、IP ベースの優先順位付けが使用され、外部で確認可能な 2 つの優先順位レベル（高および高以外）が付与されます。しかし内部的には、アプリケーション メッセージには 3 つの優先順位（高、中、および低）があります。パブリック ネットワークでは、中優先順位メッセージは高優先順位メッセージと同じように高い IP 接続で送信されます。しかし、プライベート ネットワークでは、中優先順位メッセージは、高ではない IP 接続で送信されます。

表 11-3 と表 11-4 に、パブリック ネットワーク接続とプライベート ネットワーク接続における各優先順位の IP アドレスとポート、遅延要件、およびデフォルト マーキングを示します。

表 11-3　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）と遅延要件

優先順位	IP アドレスとポート	遅延要件	DSCP / 802.1p マーキング
高	パブリックの高 IP および高優先順位接続ポート	200 ミリ秒	AF31 / 3
中	パブリックの高 IP および中優先順位接続ポート	1,000 ミリ秒	AF31 / 3
低	パブリックの高ではない IP および低優先順位接続ポート	5 秒	AF11 / 1

表 11-4　プライベート ネットワーク トラフィックのマーキング（デフォルト）と遅延要件

優先順位	IP アドレスとポート	遅延要件	DSCP / 802.1p マーキング
高	プライベートの高 IP および高優先順位接続ポート	100 ミリ秒（50 ミリ秒を推奨）	AF31 / 3
中	プライベートの高ではない IP および中優先順位接続ポート	1,000 ミリ秒	AF11 / 1
低	プライベートの高ではない IP および低優先順位接続ポート	1,000 ミリ秒	AF11 / 1

（注） Microsoft Packet Scheduler では、ベスト エフォートを除いてサポートされるマーキング レベルは最大 2 つです。そのため、中優先順位トラフィックは、高優先順位トラフィック（パブリック ネットワークの場合）または低優先順位トラフィック（プライベート ネットワークの場合）のいずれかと同じマーキングになります。これは、IP ベースの優先順位付与方式と同じで、ネットワークの観点からは優先順位レベルは失われません。Packet Scheduler をバイパスした場合は 3 つのマーキング レベルが使用されるので、中優先順位メッセージに対するマーキングが変わってきます。

（注） シスコではコールシグナリング トラフィックに対する QoS マーキングとして、DSCP CS3 を推奨しています。これは、RFC 2474 で規定されている Class-Selector コード ポイントに、Assured Forwarding Per-Hop Behavior で行われるようなマークダウンと積極的な廃棄が課せられないからです。一部の Cisco IP テレフォニー製品はすでに、DSCP CS3 のコールシグナリング マーキングに移行しています。この移行期間が終了するまでは、両方のコード ポイント（CS3 と AF31）をコールシグナリング マーキングとして確保しておく必要があります。ICM QoS マーキングの設定は ICM のセットアップで行います。デフォルトの Assured Forwarding コード ポイントは、既存のインフラストラクチャに合わせて Class-Selector コード ポイントに変更できます。

QoS 帯域幅要求の計算

QoS を使用することで帯域幅使用率が少なくなりネットワークのスループットは向上しますが、パスの物理的な帯域幅を十分に確保しない限り、ネットワークの輻輳は避けられません。ICM では、各優先順位に対する帯域幅の要求は、トラフィック量と遅延要件で決まります。これは、コール負荷、トラフィック構成、コール コンテキスト情報、構成設定などの要因から、ICM システムによって大きく異なります。

シスコでは、シスコ システム エンジニア、ICM 展開グループ およびシスコ パートナーがトラフィック量や帯域幅の要求を調査する際に使用できる、帯域幅カルキュレータとサイジング用のワークシートを提供しています。

- ACD/CallManager PG から CC の帯域幅カルキュレータ
- VRU PG から CC の帯域幅カルキュレータ
- Router プライベート リンクのサイジング用ワークシート
- PG プライベート リンクのサイジング用ワークシート

（注） ネットワーク管理者は、各優先順位における ICM フローの帯域幅の要求を明確に理解し、ネットワーク ルータまたはスイッチで QoS ポリシーの帯域幅を定義する際の考慮要素に含める必要があります。

（注） ICM アプリケーションは Resource Reservation Protocol（RSVP; リソース予約プロトコル）を認識しないので、Integrated Service（IntServ; 統合サービス）はサポートされません。Packet Scheduler を使用する場合、QoS 帯域幅予約はシェーピングの目的でローカルのボックス内だけで行われます。ネットワークでは予約は行われません。

Microsoft Packet Scheduler のインストール

（注） ICM DSCP マーキングは Packet Scheduler を使用しても使用しなくても行うことができます。シスコでは、次の場合を除き、Packet Scheduler は使用しないことを推奨しています。

1. 帯域幅の要求が明確に理解され、設定されており、

2. コンバージド ネットワーク リンクで輻輳が時折発生し、発信元における ICM トラフィックのシェーピングが役に立つ場合。

注意 Microsoft Packet Scheduler を使用するとシェーピング機能と 802.1p 機能が利用できますが、ICM 7.0 とともに使用する場合、次のような重大なリスクがあります。

1. いくつかの欠陥が Microsoft に報告されています。一部の修正プログラムは Microsoft からすでにリリースされていますが、修正プログラムがまだリリースされていないものもあります。

2. シェーピング帯域幅の設定が低すぎる場合、Packet Scheduler により過度の遅延が発生し、タイムアウト コール、キューのオーバーフロー、およびバッファの消耗の原因になることがあります。

3. WAN との通信で LAN がボトルネックになっていなければ、ICM サーバにおけるシェーピングは必要ないか、効果がありません。QoS 対応のネットワークの方が、リソースの使用率に基づいたトラフィックのシェーピング、キューイング、およびポリシングでより多くの効果を発揮します。

Microsoft Packet Scheduler は Windows Server 2003 QoS ソリューションを構成する主要コンポーネントです。このコンポーネントは、特定のフローで許可されるデータ量、パケットをいつネットワークに送出するか、およびそれらの（転送準備の整った）パケットの送信順序を規制します。

Packet Scheduler のインストールは必須ではありません。また、ICM 7.0 では、推奨されていません。ただし、次のような利点を得ることができます。

- Packet Scheduler のシェーピング機能は、特定期間内の転送ピークを平坦化することで、ICM 転送のバースト特性を緩和します。このため、ネットワーク使用率を平坦化して、ネットワークのより安定的な使用に寄与します。
- Windows Server 2003 の 802.1p タギングは、Packet Scheduler がインストールされている場合にだけ利用できます。802.1p を使用しないと、LAN セグメント内で、優先順位付けされたデータ転送がベストエフォートの転送よりもよいサービスを受けられるという物理的な保証はなくなります。

Microsoft Packet Scheduler をインストールするには、*CallRouter マシンと PG マシンの両方*で、次の手順を行います。

（注） Packet Scheduler をインストールすると、現在のすべての TCP 接続が終了されます。Packet Scheduler のインストール時にマシンの再ブートは不要ですが、現在の TCP 接続は終了されてしまいます。このため、重要な接続が行われているときは、Packet Scheduler をインストールしないでください。

ステップ 1　［ネットワーク接続］を開きます。

ステップ 2　QoS パケット スケジューラをインストールするネットワーク接続（パブリック ビジブル）を右クリックします。［プロパティ］を選択します。

ステップ 3　［インストール］ボタンをクリックします。［ネットワーク　コンポーネントの種類の選択］ダイアログボックスが表示されます。

ステップ 4　［サービス］を選択して、［追加］ボタンを選択します。［ネットワーク サービスの選択］ダイアログボックスが表示されます。

ステップ 5　［QoS　パケット　スケジューラ］を選択します。［OK］をクリックして、インストール プロセスを開始します。

802.1p 対応コンポーネントのインストールと設定

（注） 802.1p の使用はオプションです。しかし、「Microsoft Packet Scheduler のインストール」（P.11-20）で説明した理由から、802.1p が必要になる場合があります。

802.1p では、レイヤ 2 MAC ヘッダーで 3 つのビットを設定することで、優先順位クラスを表現しています。このバイナリ値は 0 ～ 7 で、8 つの優先順位クラス（サービス クラスと呼ぶ）を表しています。ICM では、デフォルトの 802.1p 設定は Cisco AVVID 推奨に準拠しています。具体的には、高および中優先順位のトラフィックには値 3 が使用され、低優先順位のトラフィックには値 1 が使用されます。Cisco AVVID のパケット分類の詳細については、『*Cisco AVVID Solution IP Telephony QoS Classification*』を参照してください。

QoS 実装の一部として 802.1p マーキング機能を有効にするには、次のタスクを実行する必要があります。

- 「Microsoft Packet Scheduler のインストール」（P.11-20）の説明に従って、Microsoft Packet Scheduler をインストールして有効にする。
- 802.1p 対応 NIC を、QoS 対応 ICM コンピュータ（Router および PG）にインストールする。
- NIC のプロパティの［詳細設定］タブで、802.1p を有効にする。802.1p を有効にするには、一般的に **QoS パケット タギング**などの名称で示された選択肢を有効にします。
- LAN セグメントに 802.1p 対応スイッチをインストールする。
- 802.1p 対応スイッチを設定して、その設定を Router または PG（または、その両方）の設定と合わせる。

（注） NIC カードは、ICM ソフトウェアをインストールする*前に*インストールしてください。ICM ソフトウェアのインストール後に NIC カードをインストールした場合、ICM ソフトウェアの再インストールが必要になります。

AVVID 対応キャンパス ネットワークの設計、スイッチの選定、および QoS 設定コマンドの詳細については、『*Cisco AVVID Network Infrastructure Enterprise Quality of Service Design*』を参照してください。

IP ルータでの QoS の設定

AVVID 対応 WAN の設計、ルータの選定、および QoS 設定コマンドの詳細については、『*Cisco AVVID Network Infrastructure Enterprise Quality of Service Design*』を参照してください。

その他のタスク

この項では、これまで説明した導入タスクの後に実行する追加のタスクについて簡単に説明します。これらのタスクを実行することにより、QoS 対応ネットワークが適正かつ効率的に稼働するようになります。

ICM QoS の設定

ICM QoS 設定の詳細については、『*ICM Installation Guide for Cisco ICM Enterprise Edition*』を参照してください。

パフォーマンス モニタリング

Windows のパフォーマンス モニタを使用して、QoS 対応接続に関連するパフォーマンス カウンタを追跡できます。Windows のパフォーマンス モニタの使用については、『*ICM Administration Guide for Cisco ICM Enterprise Edition*』を参照してください。

（注） オペレーティング　システムのバージョンによって、このツールの名前はシステム モニタになっている場合があります。

QoS の詳細

次のシスコの資料には、QoS に関する詳細が記載されています。シスコのほとんどの資料には、シスコの Web サイト（http://www.cisco.com）からアクセスできます。

- 『*Cisco IP Contact Center Enterprise Edition ネットワーク デザイン (SRND) Releases 5.0/6.0*』
- 『*Cisco IP Contact Center Enterprise Edition ネットワーク デザイン（SRND）Releases 7.0*』
- 『*Cisco AVVID Network Infrastructure Overview*』
- 『*Cisco AVVID Network Infrastructure Enterprise Quality of Service Design*』
- 『*Cisco AVVID Solution: IP Telephony QoS Classification*』
- 『*Planning for Quality of Service*』
- 『*Quality of Service Networking*』
- 『*Cisco IP Telephony QoS Design Guide*』

Active Directory のモデル

Microsoft Windows Active Directory はネットワーク リソースを管理するための中央リポジトリを提供します。ICM ソフトウェアでは Active Directory サービスを使用して、設定やレポーティング タスクをユーザが実行する際のアクセス権限を制御します。Active Directory サービスは、ICM ソフトウェアのさまざまなコンポーネントにもアクセス権を付与します。たとえば、ディストリビュータに Logger データベースを読み取るアクセス権を付与します。

ICM リリース 7.0(0) は、Windows 2000 と Windows 2003 の Active Directory ドメインをサポートしています。ネイティブ モードが必要になります。ICM ユーザの設定データは Active Directory の Organizational Units（OU; 組織単位）に保存されます。

詳細については、『*Cisco ICM/IPCC Enterprise & Hosted Editions ステージング ガイド*』を参照してください。

TCP/IP 設定

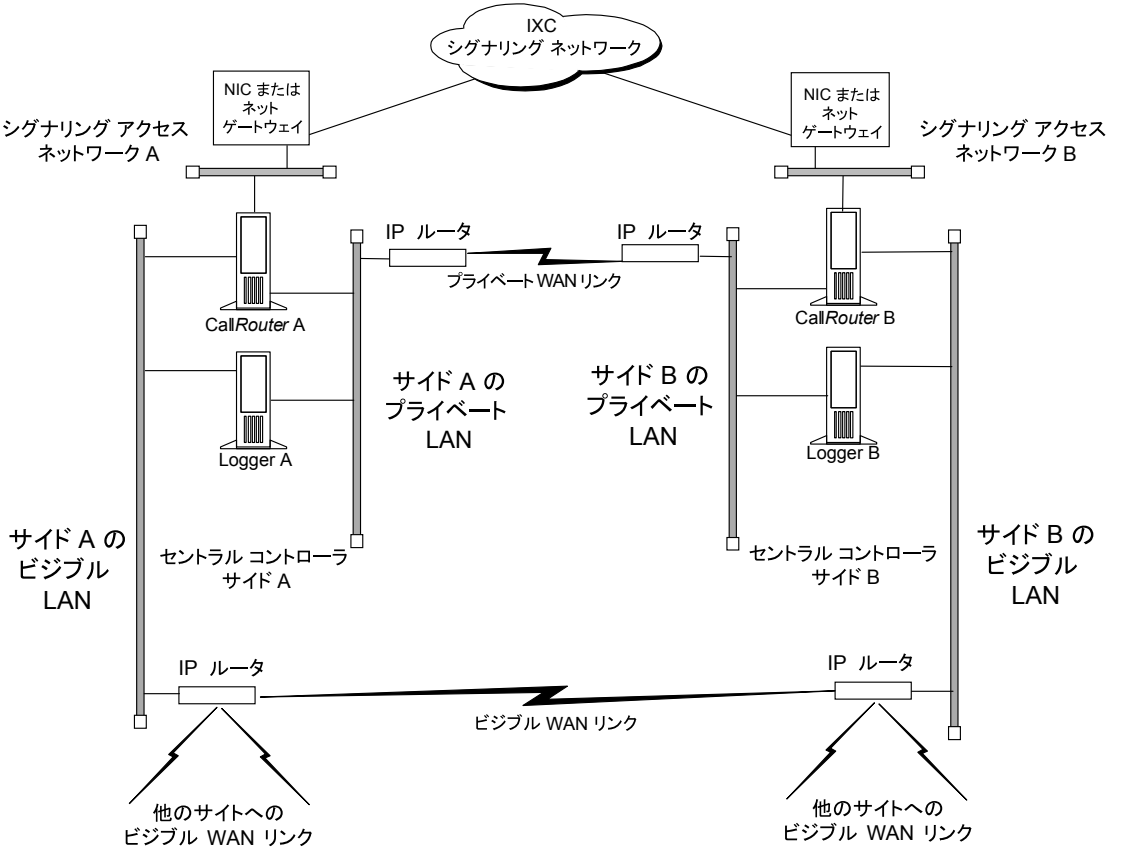
Windows Server 2003 のノードの IP アドレスを設定するには、［インターネット プロトコル（TCP/IP）のプロパティ］ダイアログボックスを使用します。このダイアログボックスを表示するには、［スタート］メニューで［設定］、［ネットワーク接続］、［ローカル エリア接続］の順にクリックします。［ローカル エリア接続の状態］ウィンドウで、［プロパティ］をクリックします。［インターネット プロトコル（TCP/IP）］を選択して、［プロパティ］をクリックします。

［次の IP アドレスを使用する］を選択します。IP アドレスを入力して［OK］をクリックします。他の IP アドレスも入力する場合は、［インターネット プロトコル（TCP/IP）のプロパティ］ウィンドウを再度開き、［詳細設定］ボタンをクリックします。表示された［TCP/IP 詳細設定］ウィンドウで、追加の IP アドレスを入力します。

セントラル サイト

セントラル コントローラの各サイドには、CallRouter、Logger、および Network Interface Controller（NIC; ネットワーク インターフェイス コントローラ）が含まれます。これらは、3 つのノードに配置される場合もありますし、2 つまたは 1 つのノードに配置されることもあります。説明をわかりやすくするため、NIC は独立したノードとして示されていますが、実際には CallRouter ノード内のプロセスとして実装されます。図 11-3 に示すように、セントラル コントローラの 2 つのサイドが、2 つの異なるセントラル サイトにある場合があります。

図 11-3　　地理的に分散したセントラル コントローラ

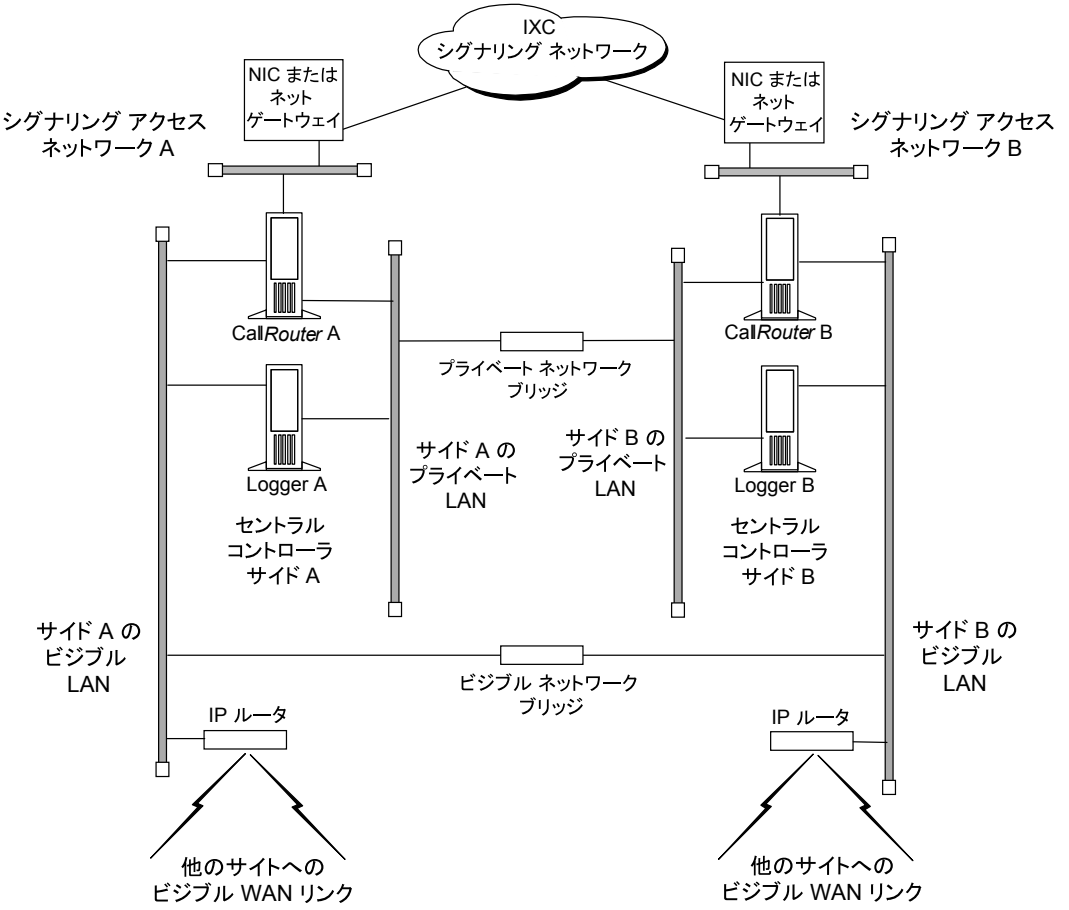


プライベート ネットワークは、セントラル コントローラの一方のサイドのノード間、およびシステムの両サイドのノード間の ICM システム トラフィックを搬送します。 セントラル　コントローラの両サイド間のトラフィックには、CallRouter と Logger の間の同期メッセージングと状態転送メッセージングが含まれます。同じサイドにある CallRouter と Logger の間の通信のほとんどは、プライベート ネットワークを通して行われます。

プライベート WAN リンク（図 11-3 を参照）は、ICM システムの全体的な応答性において重要な意味を持ちます。このリンクには、同時発生するシンクロナイザ トラフィックと状態転送トラフィックを処理するだけの帯域幅が必要です。また、回復動作の一環として追加データが転送される場合に備えて、その分の帯域幅を残しておく必要があります。プライベート WAN リンクはセントラル コントローラの同期トラフィックと状態転送トラフィックを搬送する**唯一のリンク**なので、ネットワーク停止の発生に備え、何らかのバックアップ サービスを準備しておくことが望まれます。

プライベート ネットワーク上の IP ルータは、常にトラフィックの優先順位付けを使用し、IP フラグメンテーションも頻繁に使用します。これにより、高優先順位の ICM システム トラフィックに極端なキューイング遅延が発生しないようにしています。図 11-4 に示すように、セントラル コントローラの両サイドが 1 つのサイトに併設される場合もあります。

図 11-4　併設のセントラル コントローラ



併設構成のセントラル コントローラでは、耐障害性を得るため、サイド A とサイド B のプライベート イーサネット LAN がイーサネット スイッチで分離されています。このプライベート ネットワーク ブリッジは、図 11-3 にあるプライベート WAN リンクの代替になっています。また、ビジブル ネットワーク ブリッジは、サイド A とサイド B のビジブル ネットワークを接続しています。

ビジブル ネットワーク

各セントラル サイトには、そのサイト内のノードを接続するビジブル ネットワークがあります。サイト間の通信を行うため、セントラル コントローラの各サイドでは、1 つの IP ルータをビジブル LAN 上に配置する必要があります。

（注） 地理的に分散したデュプレックス構成のセントラル コントローラの 1 つのサイドにペリフェラル ゲートウェイを併設する場合は、2 つのセントラル サイトのビジブル WAN IP ルータを結ぶ直接接続が必要になります。これにより、セントラル コントローラの両サイド間に適切なビジブル ネットワークの接続性を得られます。

IP ルータには LAN 上のアドレスが 1 つ必要になります。また、IP ルータには、各コンタクト センターのビジブル LAN および各管理サイトのビジブル LAN への**スタティック ルート**を定義する必要があります。

ビジブル IP ルータの設定

ネットワークの最適な調整を実現するために、発信元または宛先のポート番号の範囲に基づいてパケットに優先順位を付与できる IP ルータを使用する必要があります。通常は、特定の発信ネットワーク パケットに高い優先順位を付与するように IP ルータを設定する必要があります。また、ビジブル WAN で使用可能な帯域幅によっては、IP フラグメンテーションの設定が必要になる場合もあります。表 11-5 に、ビジブル ネットワーク IP ルータの設定を示します。

表 11-5　セントラル サイトのビジブル IP ルータの設定

属性	要件
IP アドレス	アドレスが 1 つ必要。
デフォルト ゲートウェイ	ある場合は、ネットワーク ブリッジ（またはブリッジとして使用する IP ルータ）。ない場合は、IP ルータにデフォルト ゲートウェイはありません。

表 11-5　セントラル サイトのビジブル IP ルータの設定（続き）

属性	要件
スタティック ルート	各リモート コンタクト センター サイトと各管理サイトで、ビジブル LAN へのスタティック ルートを定義します。セントラル サイトが地理的に離れている場合は、もう一方のセントラル サイトへのスタティック ルートを追加します。
その他	プリセットされているルーティング プロトコルを無効にします。 特定のネットワーク パケットに高い優先順位を付与します。 キューイング遅延を制限する必要がある場合は、フラグメンテーションを使用します。

表 11-6 に示すように、パケットへの優先順位付与が必要になる場合があります。

表 11-6　セントラル サイトからのビジブル ネットワーク パケットの優先順位

パケットの種類	高優先順位	低優先順位
TCP	CallRouter の高優先順位アドレス（パケットの発信元アドレスから派生）から受信した場合。	それ以外のアドレスから受信した場合。
UDP[1]	発信元または宛先のポート番号の範囲が、39000 ～ 39999 の場合。[2]	その他のすべての UDP パケット

1. CallRouter と PG の両方で ICM リリース 5.0(0) 以降が実行されている場合は、ハートビートは使用されません。その代わりに TCP が使用されます。これは PG パスに基づいて判別されます。
2. ポート番号の範囲に基づいた優先順位付与を IP ルータで設定できない場合は、すべての UDP パケットに高優先順位を付与します。

ポストルーティングまたは変換ルートを使用するコンタクト センターへの最大キューイング遅延は 50 ミリ秒で、その他のコンタクト センター サイトへの最大キューイング遅延は 200 ミリ秒です。この要件を満たすために、フラグメンテーションの実装が必要になる場合があります。

プライベート ネットワーク

各セントラル サイトには、サイト専用のプライベート LAN も必要です。セントラル コントローラの両サイドが地理的に離れている場合、それぞれのプライベート LAN に 1 つの IP ルータを配置して、2 つのサイドをプライベート WAN で接続します。

セントラル コントローラの 2 つのサイドが併設されている場合、プライベート LAN 上に IP ルータを配置する必要はありません。2 つのセントラル サイトが地理的に離れている場合は、各サイドで IP ルータをプライベート ネットワークに配置する必要があります。

表 11-7 に、プライベート ネットワークの IP ルータの設定を示します。

表 11-7　セントラル サイトのプライベート IP ルータの設定

設定	要件
IP アドレス	プライベート LAN 上のアドレスが 1 つ必要。
デフォルト ゲートウェイ	なし
スタティック ルート	もう一方のセントラル サイトのプライベート LAN へのスタティック ルートを 1 つ定義します。
その他	プリセットされているルーティング プロトコルを無効にします。 特定のネットワーク パケットに高い優先順位を付与します。

表 11-8 に、プライベート ネットワーク パケットに優先順位を付与する方法を示します。

表 11-8　セントラル サイトからのプライベート ネットワーク パケットの優先順位

パケットの種類	高優先順位	低優先順位
TCP	発信元アドレスがローカル CallRouter の高優先順位アドレスである場合。または、宛先アドレスがもう一方の CallRouter の高優先順位アドレスである場合。	その他のすべての TCP パケット
UDP	発信元または宛先のポート番号の範囲が、39000 ～ 39999 の場合。[1]	その他のすべての UDP パケット

1.　ポート番号の範囲に基づいた優先順位付与を IP ルータで設定できない場合は、すべての UDP パケットに高優先順位を付与します。

シグナリング アクセス ネットワーク

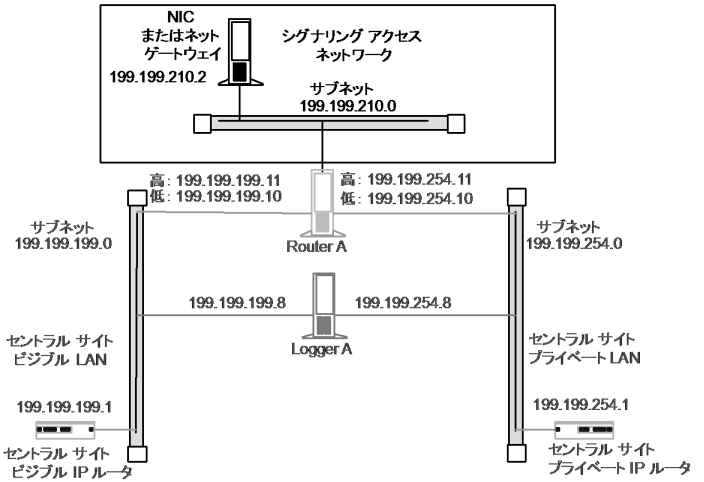
各セントラル サイトには、サイト専用の Signaling Access Network（SAN; シグナリング アクセス ネットワーク）が必要です。ICM システムはシグナリング アクセス ネットワークを使用して IXC シグナリング ネットワークと通信します。MCI、AT&T、Nortel、および Stentor の NIC 用のシグナリング アクセス ネットワークは、イーサネット LAN として実装されます。この LAN は ICM プライベート LAN とは分離されています。

Sprint NIC の構成では、CallRouter プラットフォームの Eicon X.25 WAN カードを通してシグナリング アクセス ネットワークが実装されます。ICM システムは、これらのカードを使用して IXC シグナリング ネットワークに接続します。IXC シグナリング ネットワークへの X.25 リンクがシグナリング アクセス ネットワークとみなされます。この構成では、イーサネット シグナリング アクセス ネットワークを別途用意する必要がありません。

図 11-5 は、単一のセントラル サイトの一般的なシグナリング アクセス ネットワークです。2 つのサイドが地理的に分散していることを想定しています。

（注） これ以降の図に示されている IP アドレスは例です。貴社のネットワークのアドレスを使用してください。

図 11-5　セントラル サイトのシグナリング アクセス ネットワーク



CallRouter ノード

CallRouter は、ビジブル LAN を通してビジブル ネットワークに接続します。プライベート ネットワークには、プライベート LAN を通して接続します。CallRouter はシグナリング アクセス ネットワークにも接続しています（図 11-6 を参照）。

図 11-6　CallRouter のネットワーク接続

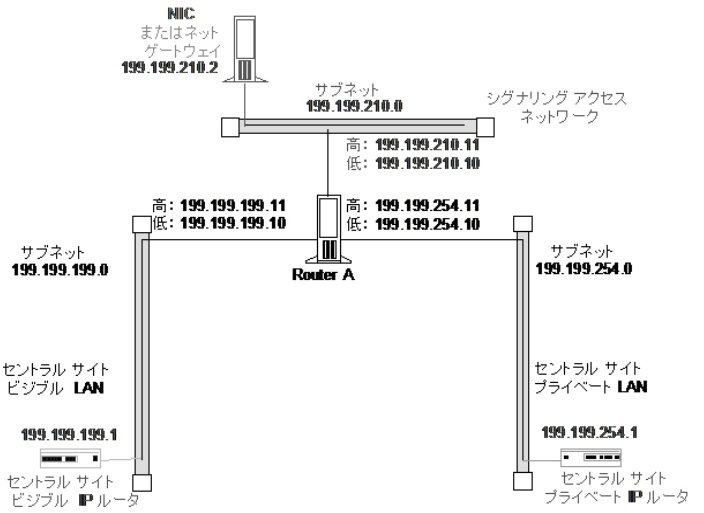


図 11-6 に示すように、CallRouter には、ビジブル LAN 上に 2 つ、プライベート LAN 上に 2 つ、シグナリング アクセス LAN 上に 2 つのアドレスが必要です。これにより ICM システムは、高優先順位ネットワーク トラフィックと低優先順位トラフィックを分離できます。

表 11-9 に、CallRouter のビジブル ネットワークの設定を示します。

表 11-9　CallRouter ビジブル ネットワーク設定

設定	要件
IP アドレス	2 つ必要。高優先順位データと低（標準）優先順位データ用にそれぞれ 1 つずつ。QoS を使用する場合、必要になるアドレスは 1 つだけです。
デフォルト　ゲートウェイ	ビジブル ネットワーク IP ルータ
スタティック ルート	なし。
その他	優先および代替 DNS サーバ。「Active Directory のモデル」（P.11-25）を参照してください。

表 11-10 に、CallRouter のプライベート ネットワークの設定を示します。

表 11-10　CallRouter プライベート ネットワーク設定

設定	要件
IP アドレス	2 つ必要。高優先順位データと低（標準）優先順位データ用にそれぞれ 1 つずつ。
デフォルト ゲートウェイ	なし （デフォルト ゲートウェイはビジブル LAN 上）。
スタティック ルート	セントラル コントローラの両サイドが地理的に離れている場合、セントラル コントローラのもう一方のサイドのプライベート LAN のサブネット アドレスへのスタティック ルートを 1 つ定義します。
その他	プライベート LAN で Windows Server 2003 ネットワーキングを無効にします。

（注） プライベート LAN で Windows Server 2003 ネットワーキングを無効にする方法については、この項の後半で説明します。

表 11-11 に、CallRouter のシグナリング アクセス ネットワークの設定を示します。

表 11-11　CallRouter シグナリング アクセス LAN 設定

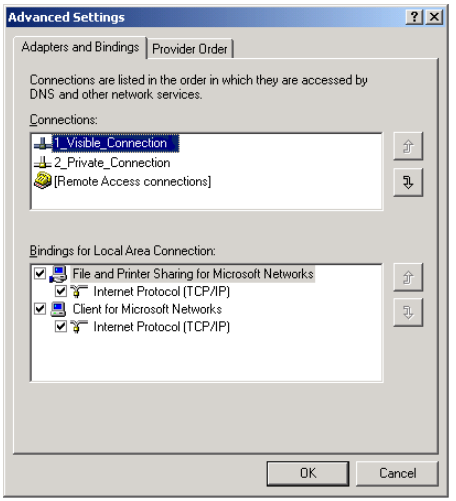
設定	要件
IP アドレス	2 つ必要になる可能性があります。2 つ目は ICM サービス プロバイダー用のサービサビリティ インターフェイスとして機能します。
デフォルト ゲートウェイ	なし。
スタティック ルート	なし。
その他	シグナリング アクセス ネットワークで Windows Server 2003 ネットワーキングを無効にします。

Windows 2000 Server および Windows Server 2003 ネットワーキングの無効化

ICM プライベート ネットワークに接続するマシンのプライベート LAN アダプタで、ネットワーク バインディングを無効にする必要があります。

プライベート LAN インターフェイスで Windows 2000 Server および Windows Server 2003 ネットワーキングを無効にするには、［ネットワーク接続］ウィンドウを使用します。Windows 2000 Server または 2003 のデスクトップ上にある［マイ ネットワーク］アイコンを右クリックします。［ネットワーク接続］ウィンドウが表示されます（［マイ コンピュータ］アイコンを右クリックして［エクスプローラ］を選択し、［マイ ネットワーク］を右クリックして［プロパティ］を選択する方法もあります）。

［詳細設定］、［詳細設定］の順に選択し、［詳細設定］ウィンドウを表示します。

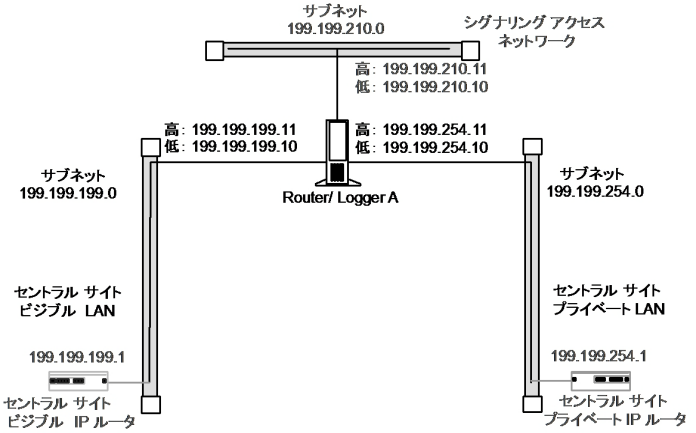


リストの先頭にビジブル ネットワーク接続が表示され、次にプライベート ネットワークが表示されていることを確認します。ウィンドウの右側にある矢印のボタンで、ネットワーク接続の表示順序を変更できます。プライベート ネットワーク接続を選択して、［Microsoft ネットワーク用ファイルとプリンタ共有］と［Microsoft ネットワーク用クライアント］の両方を無効にします。

Logger ノード

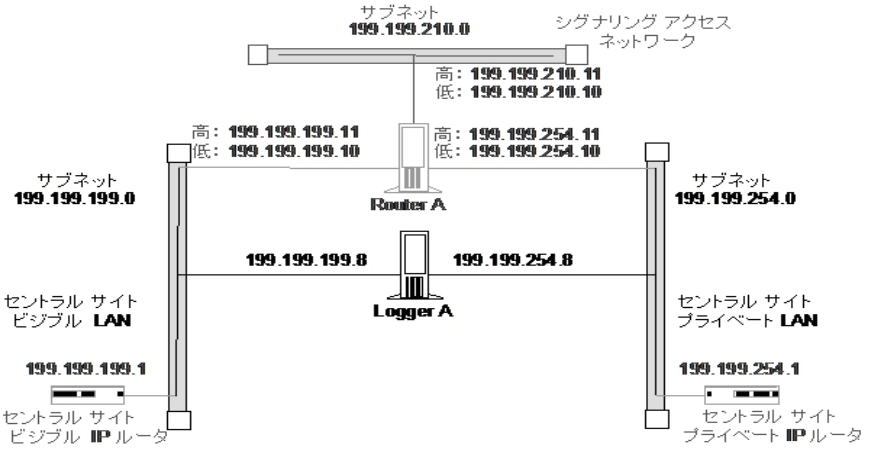
図 11-7 のように、Logger は CallRouter と同じノードに配置したり、図 11-8 のように別のノードに配置することもできます。

図 11-7　CallRouter と Logger の組み合せ



CallRouter と Logger を同じノードに配置する場合、Logger に特別な要件はありません。ビジブルおよびプライベート ネットワークのノード用に定義された低優先順位アドレスを使用します。CallRouter と Logger が別々のノードに配置される場合、Logger にビジブルおよびプライベート LAN への専用の接続が必要になります（図 11-8 を参照）。

図 11-8　別ノード上の Logger



図に示されている IP アドレスのほか、Logger ノードでは、ビジブル ネットワーク上のアドレスがさらに 2 つ必要になる場合があります。これらのアドレスは、ICM サポート プロバイダーの Distributed Diagnostic and Service Network（DDSN）によるダイヤルイン接続用です。

表 11-12 に、Logger のビジブル ネットワーク接続について示します。

表 11-12　Logger ビジブル ネットワーク設定

設定	要件
IP アドレス	アドレスが 3 つ必要。1 つは通常のデータ用、残りは DDSN ダイヤルアップ接続用。
デフォルト ゲートウェイ	ビジブル ネットワーク IP ルータ
スタティック ルート	なし。
その他	優先および代替 DNS サーバ。「Active Directory のモデル」（P.11-25）を参照してください。

表 11-13 に、Logger のプライベート ネットワークの設定を示します。

表 11-13　Logger プライベート ネットワーク設定

設定	要件
IP アドレス	アドレスが 1 つ必要。
デフォルト　ゲートウェイ	なし（デフォルト ゲートウェイはビジブル LAN 上）。
スタティック ルート	セントラル コントローラの両サイドが地理的に離れている場合、セントラル コントローラのもう一方のサイドのプライベート LAN のサブネット アドレスへのスタティック ルートを 1 つ定義します。
その他	プライベート LAN インターフェイスで Windows 2000 Server または Windows Server 2003 ネットワーキングを無効にします（詳細は、「Windows 2000 Server および Windows Server 2003 ネットワーキングの無効化」（P.11-36）を参照）。

Logger が CallRouter と同じコンピュータ上にある場合、CallRouter で必要とされるビジブルおよびプライベート ネットワーク IP の設定だけが必要となります。

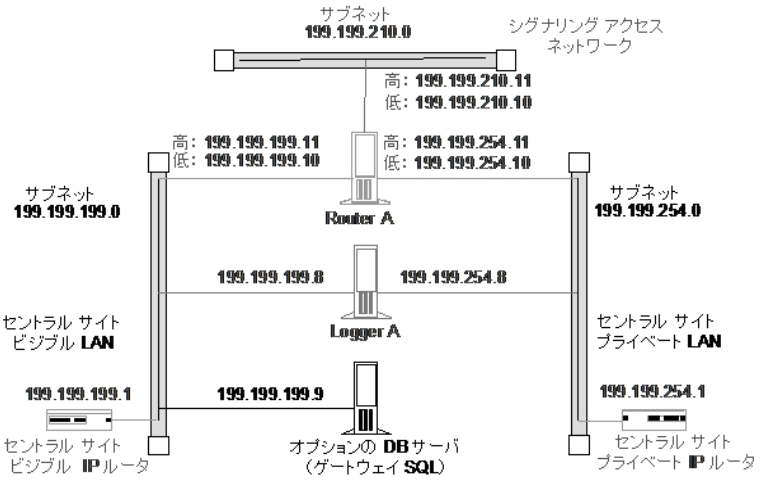
Logger が別のノードに配置される場合、プライベート LAN インターフェイスでネットワーキングを無効にする必要があります（CallRouter と同様）。

CallRouter の場合、ICMEXEC.BAT でスタティック ルートを定義します。

オプションのデータベース サーバのプラットフォーム

Cisco ICM ゲートウェイ SQL オプションを注文した場合は、追加の SQL Server データベース プラットフォームを設定する必要があります。データベース サーバには、1 つの IP アドレスと、ICM ビジブル ネットワークへの 1 つの接続が必要です（図 11-9 を参照）。

図 11-9　　オプションのデータベース サーバ



ICM ネットワーク ゲートウェイ

ICM ネットワーク ゲートウェイが、SS7 ネットワーク環境のシグナリング アクセス ネットワーク上に展開される場合があります。ICM ネットワーク ゲートウェイは、SS7 プロトコルのハンドリングを行う専用 Windows Server 2003 マシンです。ICM ネットワーク ゲートウェイを使用する場合、CallRouter マシンに NIC ソフトウェアがインストールされ、別のゲートウェイ マシンが CallRouter とキャリアの SS7 シグナリング ネットワーク間のインターフェイスとして使用されます。

ネットワーク ゲートウェイは専用マシンにインストールされます。これは、シグナリング アクセス ネットワーク（SAN）と ICM ビジブル ネットワークの両方に接続します。ビジブル ネットワーク接続は、管理およびメンテナンスのためだけに使用されます。ICM ネットワーク ゲートウェイは、セントラル サイトの他のノードや、他のサイトのノードへの接続は持ちません。たとえば、システムのもう一方のサイドのネットワーク ゲートウェイと、プライベート ネットワークを介して通信することは**ありません**。

ICM ネットワーク ゲートウェイは、IXC シグナリング ネットワークへのシグナリング リンクを最大 16 本（PCI カード 4 枚）サポートします。このためホスト サーバでは、4 本のシグナリング リンクにつき空き PCI スロットが 1 つ必要になります。各アダプタ カードが 4 本のリンクをサポートし、各リンクにそれぞれ V.35 インターフェイスがあります。

表 11-14 に、ICM ネットワーク ゲートウェイのシグナリング アクセス ネットワーク要件を示します。

表 11-14　ICM ネットワーク ゲートウェイ シグナリング アクセス ネットワーク設定

設定	要件
IP アドレス	アドレスが 1 つ必要。
デフォルト ゲートウェイ	なし。
スタティック ルート	なし。
その他	HOSTS ファイルが設定され、CONFIG.SYS および AUTOEXEC.BAT ファイルに変更が加えられます。これらの設定を変更する場合は、事前に ICM サポート プロバイダーに相談してください。

表 11-15 に、ICM ネットワーク ゲートウェイのビジブル ネットワーク要件を示します。

表 11-15　ICM ネットワーク ゲートウェイ ビジブル ネットワーク設定

設定	要件
IP アドレス	アドレスが 1 つ必要。
デフォルト ゲートウェイ	ビジブル ネットワーク IP ルータ
スタティック ルート	なし。
その他	HOSTS ファイルが設定され、CONFIG.SYS および AUTOEXEC.BAT ファイルに変更が加えられます。これらの設定を変更する場合は、事前に ICM サポート プロバイダーに相談してください。

セントラル サイトのアドミン ワークステーション

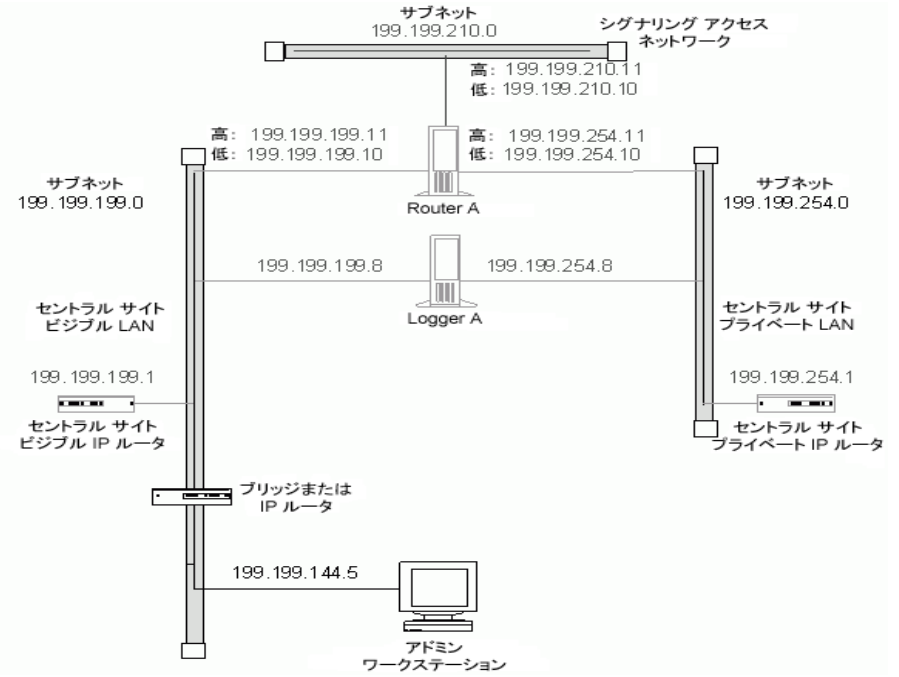
CallRouter、Logger、および PG は、イーサネット スイッチを使用してアドミン ワークステーション LAN セグメントから分離する必要があります。これにより、1 つのネットワーク問題が他のネットワークに波及するのを制限できます。セントラル コントローラおよび PG をアドミン ワークステーション LAN セグメントから分離することで、ネットワーク ハードウェア障害やソフトウェア障害（たとえば、オープン イーサネット タップやネットワーク エラー バースト）から重要なコンポーネントを保護できます。

LAN 停止に対する保護機能をさらに強化するには、ブリッジの代わりに IP ルータを使用します。分離した LAN 上に、別のコンタクト センター コンピュータおよびアプリケーションとともにアドミン ワークステーションを配置します。このような場合には、IP ルータを使用する方が適しています。LAN ブリッジは、LAN の一方のサイドから別のサイドにネットワーク エラー バーストを転送する傾向があります。IP ルータは他の LAN にネットワーク エラーを転送しないので、より適したファイアウォールを実現できます。

アドミン ワークステーションは、ICM ソフトウェアから見ることができるネットワークに配置する必要があります。

図 11-10 に、LAN ブリッジまたは IP ルータを使用して、PG とセントラル コントローラをアドミン ワークステーション LAN セグメントから分離する方法を示します。

図 11-10　セントラル サイトのアドミン ワークステーション



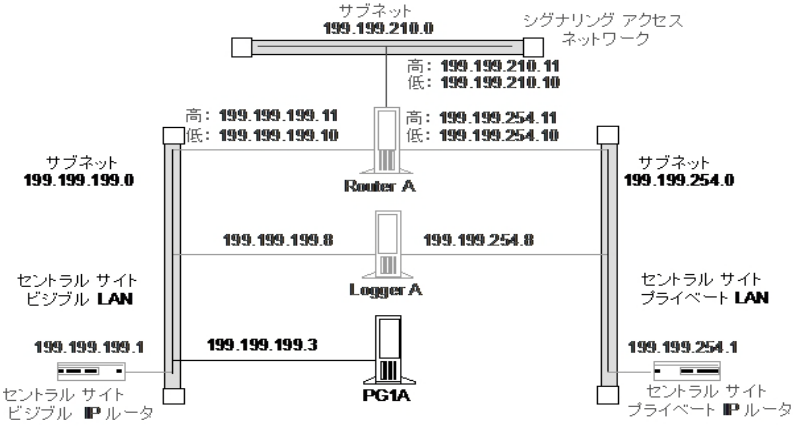
（注） アドミン ワークステーションの構成の詳細については、「管理サイト」（P.11-54）を参照してください。

セントラル サイトのペリフェラル ゲートウェイ

セントラル コントローラの 1 つのサイドまたは両サイドに併設されるペリフェラル ゲートウェイ（PG）は、CallRouter ノードおよび Logger ノードと同じビジブル LAN セグメントを共有できます。PG はビジブル LAN を通してローカル CallRouter と通信できます。セントラル コントローラの両サイドが地理的に離れている場合、PG はビジブル IP ルータおよび WAN リンクを通してもう一方のサイドと通信します（セントラル コントローラの両サイドが PG と併設されている場合、PG はビジブル LAN を通して両サイドと通信します）。

図 11-11 に、セントラル サイトに配置された PG のネットワーク接続を示します。

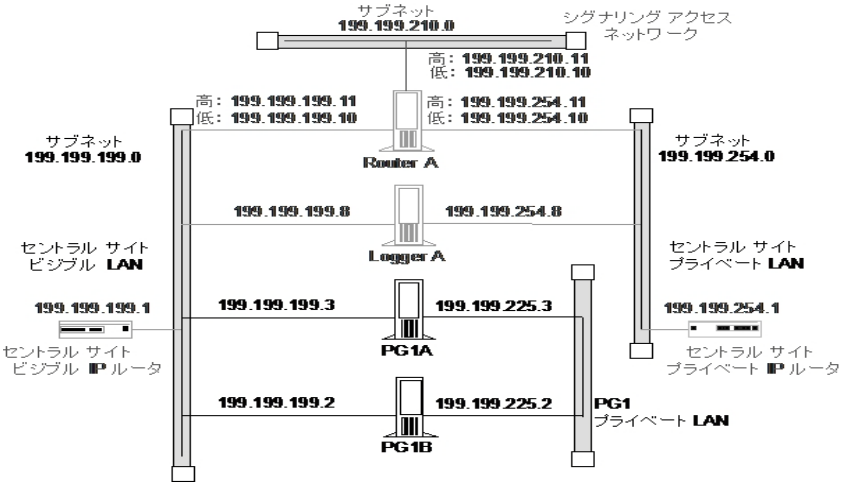
図 11-11　セントラル サイトのペリフェラル ゲートウェイ



ACD 自体をビジブル LAN 上に配置することも可能です。

PG がデュプレックス構成である場合は、2 つの PG を別個のプライベート ネットワークを通して接続する必要があります（CallRouter および Logger と同じプライベート ネットワークを使用することはできません）。図 11-12 を参照してください。

図 11-12　セントラル サイトのデュプレックス構成のペリフェラル ゲートウェイ



デュプレックス構成の PG のペアがサイト内に複数ある場合は、各ペアに対して専用のプライベート LAN を用意する必要があります。PG 用のプライベート LAN は、PG 間での同期および状態転送に使用されます。これ以外の目的では使用されません。

（注） 地理的に分散したセントラル コントローラの 1 つのサイドにペリフェラル ゲートウェイを配置する場合は、2 つのセントラル サイトのビジブル WAN IP ルータを直接接続する WAN リンクが必要になります。これにより、セントラル コントローラの両サイド間に適切なビジブル ネットワークの接続性を得られます。PG ネットワーキングの要件の詳細については、次の「コンタクト センター サイト」の項を参照してください。

コンタクト センター サイト

各コンタクト センター サイトには、ACD とペリフェラル ゲートウェイ（PG）が少なくとも 1 つずつと、オプションで 1 つまたは複数のアドミン ワークステーションが含まれます。コンタクト センターに Interactive Voice Response（IVR; 対話式音声自動応答）ユニットが含まれる場合もあります。耐障害性を実現するには、デュプレックス構成の PG ペアをコンタクト センター サイトに配置する必要があります。

リモート コンタクト センターの複合には、ビジブル ネットワークを通してアクセスします。一般的には、複数のアクセス パスと複数の IP ルータが使用されます。コンタクト センター サイトには、セントラル コントローラと通信を行うために、ビジブル ネットワーク上に IP ルータを少なくとも 1 つ配置する必要があります。耐障害性を最大限に高めるには、サイトに 2 つの IP ルータを配置し、それぞれをセントラル コントローラの 1 つのサイドに接続します。

（注） ICM ペリフェラル ゲートウェイ ソフトウェアのインストールと設定の詳細については、『*ICM Installation Guide for Cisco ICM Enterprise Edition*』を参照してください。

シンプレックス構成の PG サイト

図 11-13 は、シンプレックス構成の PG とアドミン ワークステーションを使用するコンタクト センター構成オプションの 1 つです。このサイトには ACD および IVR システムがあります。IVR PG ソフトウェアと ACD PG ソフトウェアは、同じサーバ ハードウェア プラットフォームにインストールされる場合があります。

図 11-13　シンプレックス構成 PG のコンタクト センター

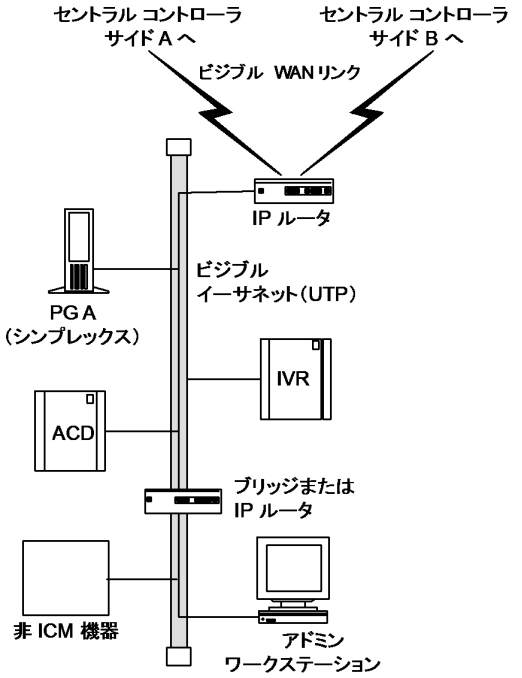


図 11-13 では、PG と AW が単一のイーサネット LAN と IP ルータを共有しています。IP ルータは優先順位付与と IP フラグメンテーションによって、高優先順位の ICM システム トラフィックに対するキューイング遅延を最小化しています。PG、ACD、IVR、および IP ルータは、ブリッジや IP ルータを使用して別のデバイスから分離する必要があります。分離することによって、他の機器やネットワークが原因で発生するネットワーク停止から重要な ICM コンポーネントを保護できます。

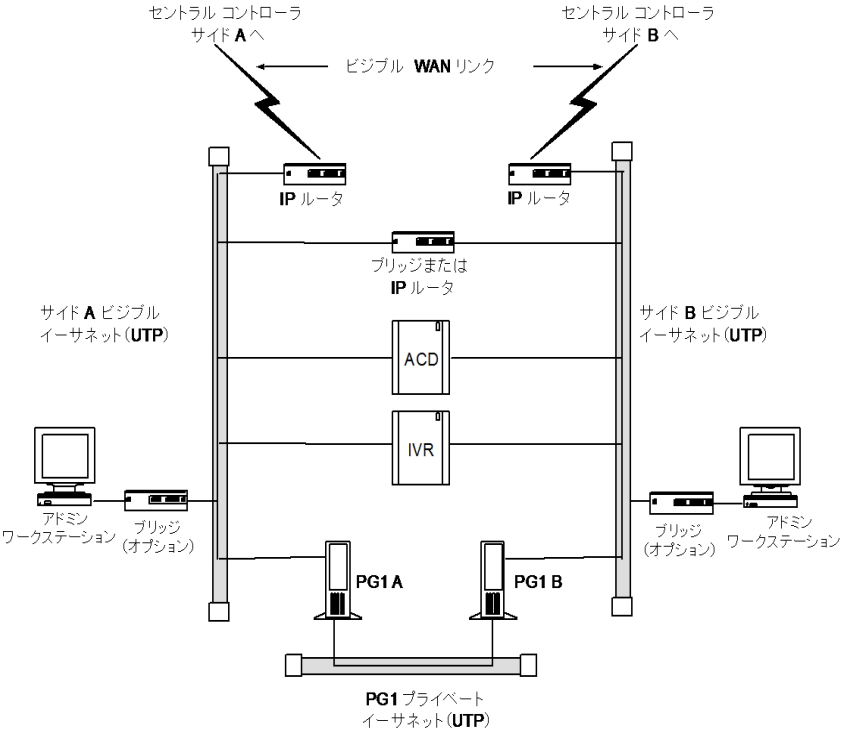
図 11-13 に示したコンタクト センターの例は、耐障害性の低い構成です。この構成を推奨するのは、耐障害性を持たせないサイト（たとえば、PG が 1 つのコンタクト センター サイトや、AW だけで構成される管理サイト）だけです。シンプレックス構成の PG は、単一障害点を意味します。PG に障害が発生すると、コ

ンタクト センターから CallRouter へのリアルタイム データの流れが停止し、ポストルーティングおよび変換ルートの使用が妨げられます。デュプレックス構成の PG を使用することで、潜在的な障害から保護できます。

デュプレックス構成の PG サイト

デュプレックス構成の PG を使用すれば、より高い耐障害性が実現できます。図 11-14 を参照してください。

図 11-14　耐障害性を備えたコンタクト センター



2 つの PG 間の直接通信を可能にするために、PG プライベート LAN が追加されています。デュプレックス構成の PG のペアがサイト内に複数ある場合は、各 PG ペアに対して専用のプライベート LAN を用意する必要があります。

コンタクト センターの耐障害性をさらに高めるには、各 PG を専用のビジブル LAN と IP ルータとともに配備します。これにより、LAN が単一障害点になることを回避できます。各 PG は、専用の LAN および IP ルータを使用して、セントラル コントローラの 1 つのサイドと通信します。

IP ルータを 2 つではなく 1 つしか使用しない場合は、コンタクト センター サイトに単一障害点を潜在させることになります。IP ルータに障害が発生すると、コンタクト センターから CallRouter へのリアルタイム データの流れが停止し、セントラル コントローラからアドミン ワークステーションへの監視データの流れも停止します。また、このコンタクト センターへのポストルーティングおよび変換ルートの使用も妨げられます。

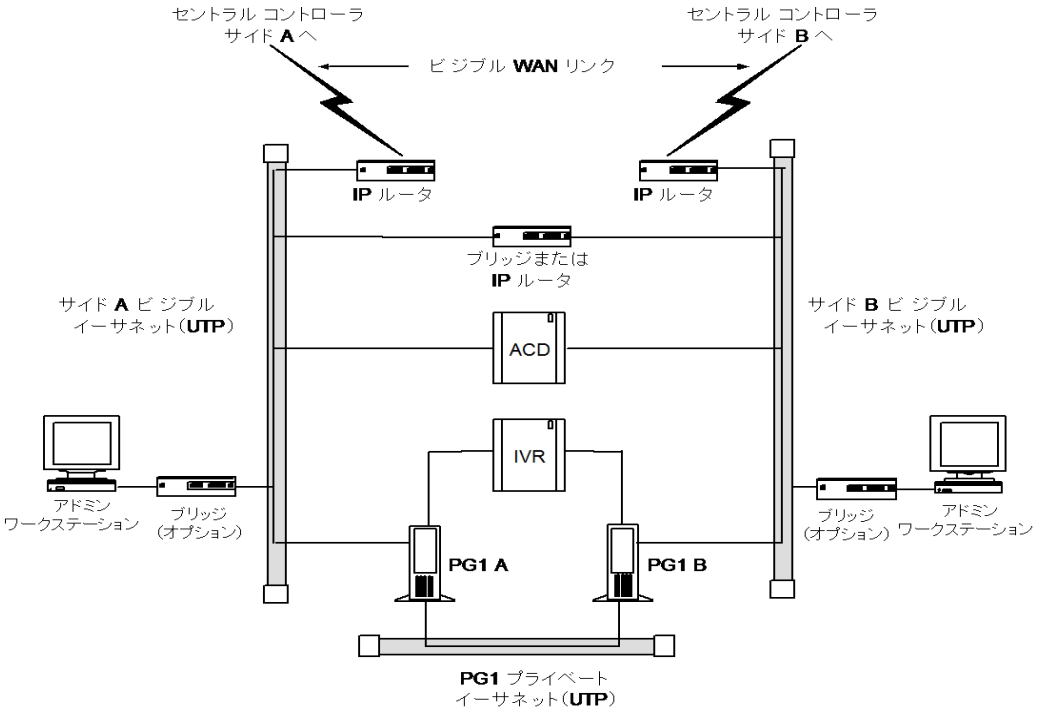
図 11-14 の 2 つの IP ルータのうちの 1 つは、PG のデフォルト ゲートウェイとして機能します。デフォルトでは、PG はセントラル コントローラのそのサイドと通信します。PG には、もう一方の IP ルータを経由してセントラル コントローラのもう一方のサイドへ向かうスタティック ルートが定義されている必要があります。

各 PG には、ICM サポート プロバイダーの Distributed Diagnostic and Service Network（DDSN）によるダイヤルイン アクセスを許可するモデムが搭載されている場合があります。この場合 PG には、ビジブル ネットワーク上の標準のアドレスに加え、ダイヤルイン アクセス用のビジブル LAN アドレスがさらに 2 つ必要になります。

分離された IVR LAN のあるデュプレックス構成の PG サイト

コンタクト センターの別の構成として、IVR の管理を厳重に保護する必要がある場合や、セキュリティ上の問題がある場合に使用される構成があります。図 11-15 は、このような場合に使用する、耐障害性を備えたコンタクト センター サイトの構成例です。

図 11-15　耐障害性を備えたコンタクト センター - 分離された LAN 上の IVR



このオプションでは、別の CTI アプリケーションが ACD とインターフェイスする必要があるという想定から、ビジブル LAN 上に ACD が配置されています。この代わりに、IVR システムと同じ LAN 上に ACD を配置する方法もあります。

PG ネットワーク設定

表 11-16 に、シンプレックス構成 PG のネットワーク設定を示します。

表 11-16　シンプレックス構成 PG ネットワーク設定

設定	要件
IP アドレス	ビジブル LAN 上のアドレスが 3 つ必要になる場合があります。1 つは通常のデータ用、残りは DDSN 用です。
デフォルト ゲートウェイ	ビジブル ネットワーク IP ルータの 1 つを、PG のデフォルト ゲートウェイとして定義します。
スタティック ルート	デフォルト ゲートウェイ IP ルータでターゲットにされていないセントラル サイトのビジブル LAN へのスタティック ルートを 1 つ定義します。
その他	優先および代替 DNS サーバ。「Active Directory のモデル」（P.11-25）を参照してください。

表 11-17 に、デュプレックス構成 PG のネットワーク設定を示します。

表 11-17　デュプレックス構成 PG ネットワーク設定

設定	要件
IP アドレス	各 PG にはビジブル LAN 上のアドレスが 3 つ（通常トラフィック用に 1 つ、DDSN ダイヤルアップ接続用に 2 つ）と、プライベート LAN 上のアドレスが 2 つ（1 つは高優先順位データ用、もう 1 つは低優先順位データ用）必要になります。
デフォルト ゲートウェイ	ビジブル ネットワーク IP ルータの 1 つを、各 PG のデフォルト ゲートウェイとして定義します。両方の PG のデフォルト ゲートウェイとして同じ IP ルータを使用**しないでください**。
スタティック ルート	各 PG には、デフォルト ゲートウェイ IP ルータでターゲットにされていないセントラル コントローラのサイドへのスタティック ルートが必要になります。

表 11-17　デュプレックス構成 PG ネットワーク設定（続き）

設定	要件
その他	優先および代替 DNS サーバ。「Active Directory のモデル」（P.11-25）を参照してください。

（注） ペリフェラル ゲートウェイを ACD に接続する方法の詳細については、第 5 章「ペリフェラル ゲートウェイの構成」を参照してください。

コンタクト センターの IP ルータ

IP ルータには LAN 上のアドレスが 1 つ必要になります。また、PG のデフォルト ゲートウェイ IP ルータでターゲットにされていないセントラル コントローラのサイド（セントラル サイトのビジブル LAN）へのスタティック ルートを、IP ルータで定義する必要があります。

ネットワークの最適な調整を実現するために、発信元または宛先のポート番号の範囲に基づいてパケットに優先順位を付与できる IP ルータを使用する必要があります。通常は、特定の発信ネットワーク パケットに高い優先順位を付与するように IP ルータを設定する必要があります。また、ビジブル WAN で使用可能な帯域幅によっては、IP フラグメンテーションの設定が必要になる場合もあります。

表 11-18 に、IP ルータの設定を示します。

表 11-18　コンタクト センター IP ルータ設定

設定	要件
IP アドレス	各 IP ルータにはビジブル LAN 上のアドレスが 1 つ必要になります。
デフォルト ゲートウェイ	ある場合は、ネットワーク ブリッジまたはブリッジとして使用する IP ルータ。ない場合は、IP ルータにデフォルト ゲートウェイはありません。
スタティック ルート	各 IP ルータには、1 つのセントラル サイトのビジブル LAN に対するスタティック ルートが必要です。

表 11-18　コンタクト センター IP ルータ設定（続き）

設定	要件
その他	プリセットされているルーティング プロトコルを無効にします。 特定のネットワーク パケットに高い優先順位を付与します。 キューイング遅延を制限する必要がある場合は、フラグメンテーションを使用します。

パケットの優先順位については、表 11-19 を参照してください。

表 11-19　コンタクト センターのパケットの優先順位

パケットの種類	高優先順位	低優先順位
TCP	CallRouter の高優先順位アドレス（パケットの宛先アドレスから派生）に送信した場合。	それ以外のアドレスに送信した場合。
UDP	発信元または宛先のポート番号の範囲が、39000 ～ 39999 の場合。[1]	その他のすべての UDP パケット

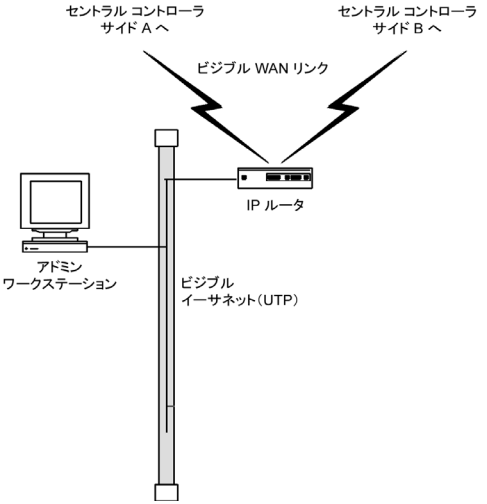
1. ポート番号の範囲に基づいた優先順位付与を IP ルータで設定できない場合は、すべての UDP パケットに高優先順位を付与します。

ポストルーティングまたは変換ルートを使用するサイトでは最大キューイング遅延は 50 ミリ秒で、それ以外は 200 ミリ秒です。この要件を満たすために、フラグメンテーションの実装が必要になる場合があります。

管理サイト

管理サイトには 1 つまたは複数のアドミン ワークステーションが含まれます。各管理サイトには、1 つのビジブル LAN とセントラル サイトと通信するための IP ルータが必要です。管理サイトにはプライベート LAN は不要です（図 11-16 を参照）。

図 11-16　管理サイトの構成



複数のアドミン ワークステーションを単一の LAN に配置できます。