CHAPTER 3

ネットワーク インフラストラクチャ

この章では、企業環境で Cisco Unified Communications システムを構築するために必要なネットワーク インフラストラクチャの要件について説明します。図 3-1 はネットワーク インフラストラクチャを形成する各種のデバイスの役割を示し、表 3-1 はこれらの各役割をサポートするために必要な機能を要約したものです。

Unified Communications には、IP パケット損失、パケット遅延、および遅延変動（またはジッタ）について厳しい要件があります。したがって、ネットワーク全体の Cisco スイッチおよびルータで使用できる QoS メカニズムの大部分を使用可能にする必要があります。これと同じ理由で、可用性の高いインフラストラクチャを保証するには、ネットワーク障害またはトポロジ変更の発生後に迅速に収束する、冗長なデバイスおよびネットワーク リンクも重要です。

次の項では、関連するネットワーク インフラストラクチャの機能について説明します。

- 「LAN インフラストラクチャ」（P.3-4）
- 「WAN インフラストラクチャ」（P.3-36）
- 「ワイヤレス LAN インフラストラクチャ」（P.3-57）

図 3-1　一般的なキャンパス ネットワーク インフラストラクチャ

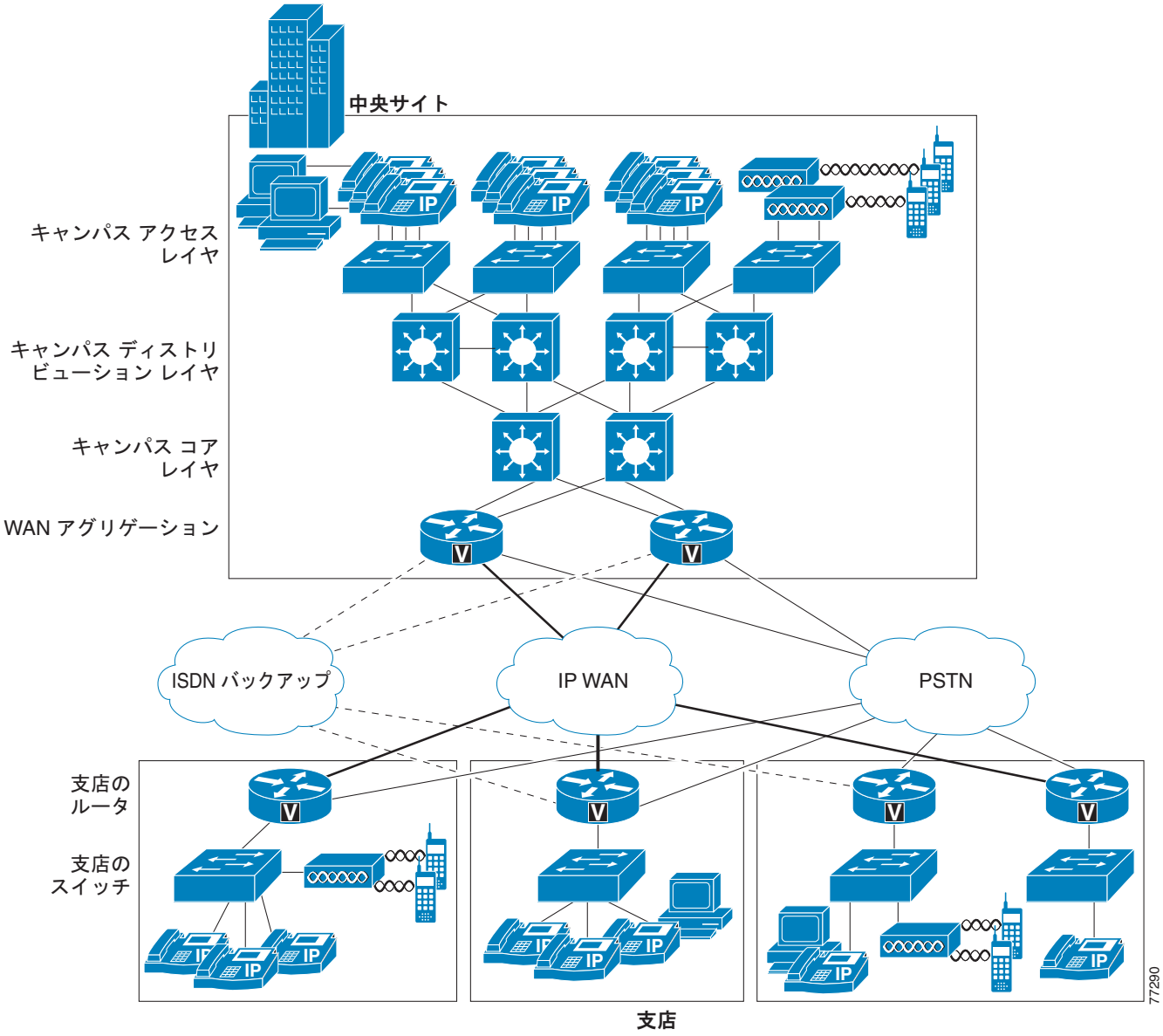


表 3-1　ネットワーク インフラストラクチャ内の役割に必要な機能

インフラストラクチャの役割	必要な機能
キャンパス アクセス スイッチ	• インライン パワー[1] • 複数キュー サポート • 802.1p および 802.1Q • 高速リンク コンバージェンス
キャンパス ディストリビューション スイッチまたはコア スイッチ	• 複数キュー サポート • 802.1p および 802.1Q • トラフィック分類 • トラフィック再分類
WAN アグリゲーション ルータ（ネットワークのハブ サイト）	• 複数キュー サポート • トラフィック シェーピング • リンク フラグメンテーション/インターリーブ（LFI）[2] • リンク効率化 • トラフィック分類 • トラフィック再分類 • 802.1p および 802.1Q
支店ルータ（スポーク サイト）	• 複数キュー サポート • LFI[2] • リンク効率化 • トラフィック分類 • トラフィック再分類 • 802.1p および 802.1Q
支店または小規模サイトのスイッチ	• インライン パワー[1] • 複数キュー サポート • 802.1p および 802.1Q

1. 推奨作業です。
2. リンク速度が 786 kbps を下回る場合。

この章の新規情報

表 3-2 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

表 3-2　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所	改訂日
細部の訂正および変更	この章の各項で説明	2011 年 6 月 2 日
仮想 Unified Communications システム	「Cisco UCS B シリーズ ブレード サーバを使用した仮想 Unified Communications に関する QoS 設計上の考慮事項」（P.3-20）	2010 年 4 月 2 日
Cisco IOS Service Advertisement Framework（SAF）	「Service Advertisement Framework（SAF）」（P.3-64）	2010 年 4 月 2 日

LAN インフラストラクチャ

統合されたネットワーク上で Unified Communications を正常に動作させるには、キャンパス LAN インフラストラクチャの設計が極めて重要です。LAN インフラストラクチャを適切に設計するには、次の基本的な設定と設計に関するベスト プラクティスに従って、可用性の高いネットワークを配置する必要があります。さらに、LAN インフラストラクチャを適切に設計するには、ネットワーク上にエンドツーエンド QoS を配置する必要もあります。次の項では、これらの要件について説明します。

- 「ハイ アベイラビリティのための LAN 設計」（P.3-4）
- 「LAN の QoS」（P.3-15）

ハイ アベイラビリティのための LAN 設計

LAN を適切に設計するには、堅牢かつ冗長なネットワークをトップダウン方式で構築する必要があります。LAN をレイヤ モデルとして構築し（図 3-1 を参照）、LAN インフラストラクチャのモデルを 1 段階ずつ開発することで、可用性の高い、耐障害性のある冗長なネットワークを構築できます。これらのレイヤを適切に設計してから、追加のネットワーク機能を提供するために、DHCP や TFTP などのネットワーク サービスを追加できます。次の項では、インフラストラクチャのレイヤとネットワーク サービスについて説明します。

- 「キャンパス アクセス レイヤ」（P.3-5）
- 「キャンパス ディストリビューション レイヤ」（P.3-10）
- 「キャンパス コア レイヤ」（P.3-12）
- 「ネットワーク サービス」（P.3-22）

キャンパスの設計の詳細については、次の Web サイトで入手可能な『*Design Zone for Campus*』を参照してください。

http://www.cisco.com/go/designzone

キャンパス アクセス レイヤ

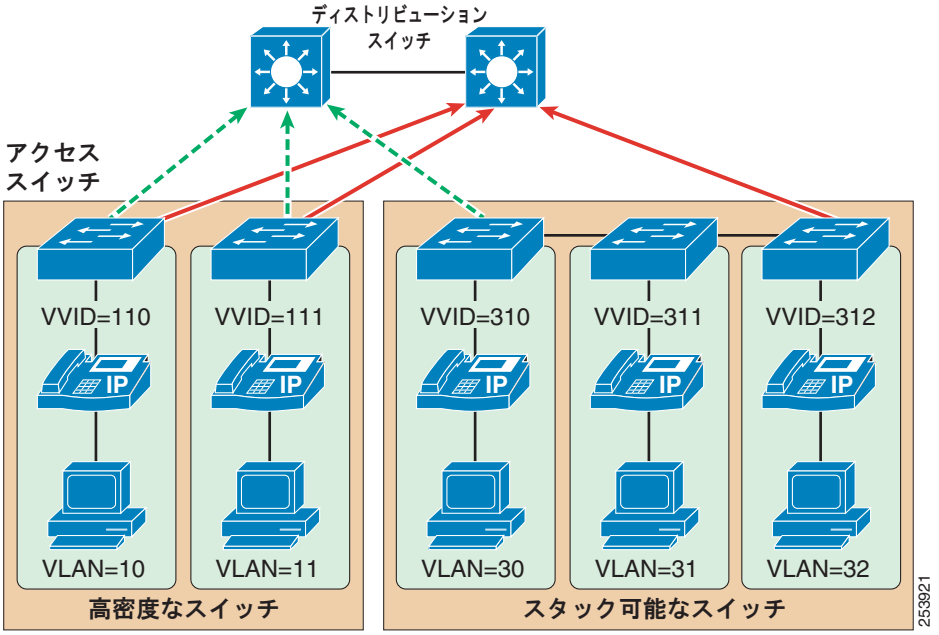
キャンパス LAN のアクセス レイヤに含まれるネットワーク部分は、デスクトップ ポートからワイヤリング クローゼット スイッチまでです。従来、アクセス レイヤ スイッチはディストリビューション レイヤへのレイヤ 2 アップリンクを持つレイヤ 2 デバイスとして設定されてきました。レイヤ 2 およびレイヤ 2 アクセス設計に対応するスパニング ツリーの推奨事項は、十分に実証されており、次に簡単に説明します。レイヤ 3 プロトコルをサポートする最新の Cisco Catalyst スイッチでは、新しいルーテッド アクセス設計が可能となり、コンバージェンス時間と設計の簡素化における改善が行われています。ルーテッド アクセス設計については、「ルーテッド アクセス レイヤ設計」（P.3-8）の項で詳しく説明します。

レイヤ 2 アクセス設計の推奨事項

アクセス レイヤを適切に設計するには、最初に、Virtual LAN（VLAN）ごとに単一の IP サブネットを割り当てます。一般に、VLAN は、複数のワイヤリング クローゼット スイッチにまたがってはいけません。つまり、ある VLAN が存在するアクセス レイヤ スイッチは 1 つだけである必要があります（図 3-2 を参照）。この方法にすると、レイヤ 2 からトポロジ上のループが排除されるため、スパニング ツリーのコンバージェンスによってフローが一時的に中断することがなくなります。ただし、標準ベースの IEEE 802.1w Rapid Spanning Tree Protocol（RSTP）と 802.1s Multiple Instance Spanning Tree Protocol（MISTP）を導入すると、スパニング ツリーが収束する速度が大幅に高くなる可能性があります。さらに重要なことに、VLAN を単一のアクセス レイヤ スイッチに限定すると、ブロードキャスト ドメインのサイズが制限されます。単一の VLAN またはブロードキャスト ドメインにある多数のデバイスによって、大量のブロードキャスト トラフィックが定期的に生成される可能性があり、これが問題となる場合があります。そのため、VLAN ごとのデバイス数を 512 程度に制限することを推奨します。この数は、2 つのクラス C サブネット（つまり、23 ビットのサブネットがマスクされたクラス C アドレス）に相当します。キャンパス アクセス レイヤの詳細については、http://www.cisco.com/en/US/products/hw/switches/index.html で入手可能なマニュアルを参照してください。

（注）　単一の Unified Communications VLAN におけるデバイス数を 512 ほどに制限する推奨事項は、ただ単に VLAN ブロードキャスト トラフィックの量を制御するためにだけ、必要な事項ではありません。Linux ベースの Unified CM サーバ プラットフォームでは、ARP キャッシュには 1024 デバイスの絶対的な制限があります。1024 を超えるデバイスを含む IP サブネットのある VLAN に Unified CM をインストールすると、Unified CM サーバの ARP キャッシュがすぐに満杯になる可能性があり、Unified CM サーバとその他の Unified Communications のエンドポイント間の通信に深刻な影響を及ぼす場合があります。Windows ベースの Unified CM サーバ プラットフォームで ARP キャッシュ サイズが動的に拡大される場合であっても、Unified CM サーバ プラットフォームで使用するオペレーティング システムに関係なく、任意の VLAN 内のデバイスを 512 に制限することを強く推奨します。

図 3-2　音声とデータに対応するアクセス レイヤ スイッチと VLAN



音声を配置する場合は、アクセス レイヤで、次の 2 つの VLAN を有効にすることを推奨します。1 つはデータ トラフィックに対応するネイティブ VLAN（図 3-2 の VLAN 10、11、30、31、および 32）で、もう 1 つは音声トラフィックに対応する、Cisco IOS の Voice VLAN または CatOS の Auxiliary VLAN（図 3-2 の VVID 110、111、310、311、および 312）です。

次の理由により、音声とデータの VLAN を分離することを推奨します。

- アドレス スペースの確保と、外部ネットワークからの音声デバイスの保護

  Voice VLAN または Auxiliary VLAN 上で電話機のプライベート アドレッシングを行うと、アドレスの確保が保証され、パブリック ネットワークを介して電話機に直接アクセスできないことが保証されます。PC とサーバは、一般に、パブリックにルーティングされるサブネット アドレスを使用してアドレス指定されます。ただし、音声エンドポイントは、RFC 1918 プライベート サブネット アドレスを使用してアドレス指定されることがあります。

- QoS 信頼性境界の音声デバイスへの拡張

  QoS 信頼性境界を音声デバイスに拡張し、次に、QoS 機能を PC や他のデータ デバイスに拡張できます。

- 悪質なネットワーク攻撃からの保護

  VLAN アクセス コントロール、802.1Q、および 802.1p タギングを使用すると、音声デバイスを悪質な内部および外部ネットワーク攻撃から保護できます。このような攻撃には、ワーム、Denial of Service（DoS; サービス拒否）攻撃、データ デバイスがパケット タギングによってプライオリティ キューにアクセスする攻撃などがあります。

- 管理および設定の容易性

  アクセス レイヤで音声とデータの VLAN を分離すると、管理が容易になり、QoS 設定が簡素化されます。

高品質の音声を提供し、すべての音声機能セットを利用するには、アクセス レイヤで次の機能をサポートする必要があります。

- 電話機が接続されているポート上でレイヤ 2 CoS パケット マーキングを適切に処理するための 802.1Q トランキングおよび 802.1p
- RTP 音声パケット ストリームのプライオリティ キューイングを行う複数の出力キュー
- トラフィックを分類または再分類し、ネットワーク信頼性境界を設定する機能
- インライン パワー機能（インライン パワー機能は必須ではありませんが、アクセス レイヤ スイッチに使用することを強く推奨します）
- レイヤ 3 認識と、QoS アクセス コントロール リストを実装する機能（これらの機能が推奨されるのは、ソフトフォン アプリケーションを実行する PC など、拡張された信頼性境界を利用できない特定の Unified Communications エンドポイントを使用する場合です）

Spanning Tree Protocol（STP）

コンバージェンス時間を最小限に抑え、レイヤ 2 の耐障害性を最大限に高めるには、次の STP 機能を有効にします。

- PortFast

  すべてのアクセス ポート上で PortFast を有効にします。これらのポートに接続されている電話機、PC、またはサーバは、STP 動作に影響する可能性のあるブリッジ プロトコル データ ユニット（BPDU）を転送しません。PortFast により、電話機または PC が、ポートに接続されたときに、STP が収束するのを待たずにただちにトラフィックの送受信を開始できることが保証されます。

- ルート ガードまたは BPDU ガード

  すべてのアクセス ポート上でルート ガードまたは BPDU ガードを有効にすると、スパニング ツリーのルートになる可能性のある不良スイッチの導入を防止できるので、STP の再コンバージェンス イベントが発生したり、ネットワーク トラフィック フローが中断したりすることがなくなります。BPDU ガードによって **errdisable** 状態に設定されたポートについては、手動で再度有効にするか、または設定期間の経過後に errdisable 状態から自動的にポートを再度有効にするようにスイッチを設定する必要があります。

- UplinkFast と BackboneFast

  必要に応じてこれらの機能を有効にすると、レイヤ 2 ネットワークで変更が生じた場合に、STP ができるだけ迅速にコンバージしてハイ アベイラビリティを実現することが保証されます。シスコ製のスタック可能なスイッチを使用する場合は、Cross-Stack UplinkFast（CSUF）を有効にして、スタック内のスイッチに障害が発生したときにフェールオーバーおよびコンバージェンスが迅速に行われるようにします。

- 単方向リンク検出（UDLD）

  この機能を有効にすると、リンク障害や誤作動が発生したときのネットワーク上のコンバージェンスとダウンタイムが低減されるため、ネットワーク サービスの中断が最小限に抑えられることが保証されます。UDLD は、トラフィックが一方向に流れているリンクを検出し、サービスを落とします。この機能により、障害リンクが、スパニング ツリーおよびルーティング プロトコルによってネットワーク トポロジの一部と誤って見なされることが防止されます。

（注） RSTP 802.1w が導入されていれば、PortFast や UplinkFast などの機能は必要ありません。これは、これらのメカニズムはこの標準に組み込まれているためです。RSTP が Catalyst スイッチ上で有効になっていれば、これらのコマンドは必要ありません。

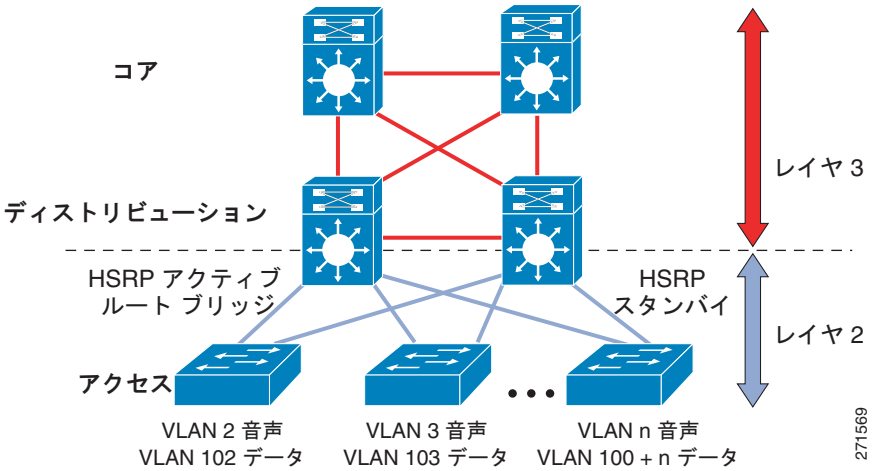
ルーテッド アクセス レイヤ設計

簡素化された設定、一般的なエンドツーエンドのトラブルシューティング ツール、および高速コンバージェンスを必要とするキャンパス設計では、アクセス レイヤ（ルーテッド アクセス）でのレイヤ 3 スイッチングとディストリビューション レイヤでのレイヤ 3 スイッチングを組み合せて使用する階層設計が音声およびデータ トラフィック フローの復旧時間を最小にします。

アクセス レイヤへの L2/L3 境界の移行

一般的な階層キャンパス設計では、ディストリビューション レイヤは、レイヤ 2、レイヤ 3、およびレイヤ 4 プロトコルとサービスの組み合せを使用して、最適なコンバージェンス、スケーラビリティ、セキュリティ、および管理性を提供します。最も一般的なディストリビューション レイヤの設定では、アクセス スイッチは高速トランク ポート上のトラフィックをディストリビューション スイッチに転送するレイヤ 2 スイッチとして設定されます。ディストリビューション スイッチは、図 3-3 に示すように、ダウンストリーム アクセス スイッチ トランク上のレイヤ 2 スイッチングとネットワークのコアに向けてのアップストリーム ポート上のレイヤ 3 スイッチングの両方をサポートするように設定されます。

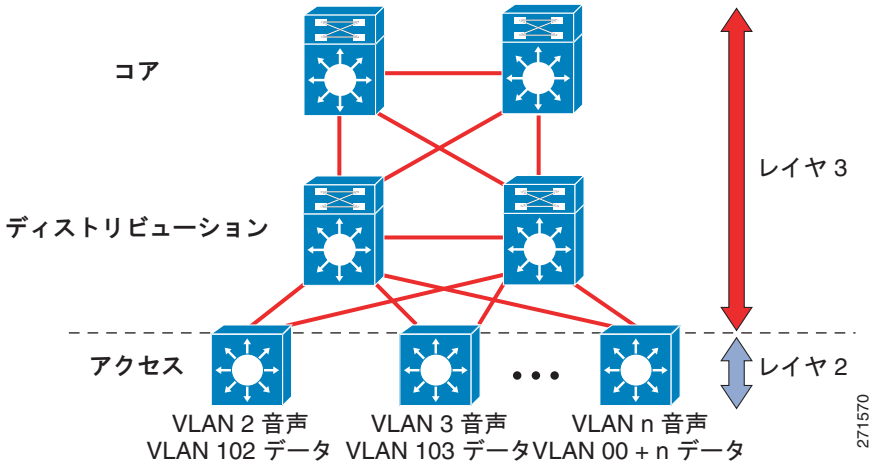
図 3-3　　従来のキャンパス設計：レイヤ 3 ディストリビューションを使用したレイヤ 2 アクセス



この設計におけるディストリビューション スイッチの目的は、キャンパスのブリッジされたレイヤ 2 部分とルーティングされたレイヤ 3 部分の間に、デフォルト ゲートウェイ、レイヤ 3 ポリシー制御、および必要なすべてのマルチキャスト サービスのサポートを含む境界機能を提供することです。

従来のディストリビューション レイヤ モデル（図 3-3 に示される）に対する代替設定は、アクセス スイッチが完全なレイヤ 3 ルーティング ノード（レイヤ 2 スイッチングとレイヤ 3 スイッチングの両方を提供する）として機能し、ディストリビューションにアクセスするレイヤ 2 アップリンク トランクがレイヤ 3 ポイントツーポイント ルーテッド リンクに置き換えられるものです。レイヤ 2/3 の境界がディストリビューション スイッチからアクセス スイッチに移動する（図 3-4 に示されるように）この代替設定は、大規模な設計の変更のように見えますが、実際には設計上の現在のベスト プラクティスの拡張です。

図 3-4　ルーテッド アクセス キャンパス設計：レイヤ 3 ディストリビューションを使用したレイヤ 3 アクセス



従来のレイヤ 2 とレイヤ 3 ルーテッド アクセス設計の両方で、各アクセス スイッチは固有の音声およびデータ VLAN によって設定されます。レイヤ 3 設計では、これらの VLAN のデフォルト ゲートウェイとルート ブリッジは、ディストリビューション スイッチからアクセス スイッチに単純に移動します。すべての端末とデフォルト ゲートウェイに対するアドレッシングは同様です。VLAN および特定のポート設定は、アクセス スイッチ上で変わりません。各 VLAN のルータ インターフェイス設定、アクセス リスト、「ip helper」、およびその他すべての設定は同様のままですが、ディストリビューション スイッチではなくアクセス スイッチで定義された VLAN Switched Virtual Interface（SVI）上で設定されます。

アクセス スイッチに向かってのレイヤ 3 インターフェイスの移動に関連付けられた、いくつかの重要な設定変更があります。VLAN はすべてローカルになっているので、Hot Standby Router Protocol（HSRP; ホットスタンバイ ルータ プロトコル）または Gateway Load Balancing Protocol（GLBP; ゲートウェイ ロード バランシング プロトコル）の仮想ゲートウェイ アドレスを「ルータ」インターフェイスとして設定する必要がなくなりました。同様に、各 VLAN で単一のマルチキャスト ルータを使用する場合、PIM 照会間隔の調整などの従来のマルチキャストの調整を行ったり、代表ルータをアクティブな HSRP ゲートウェイと必ず同期させたりする必要はありません。

ルーテッド アクセス コンバージェンス

レイヤ 3 アクセス設計の使用には、次のような多くの潜在的利点があります。

- コンバージェンスの改善
- マルチキャスト設定の簡素化
- 動的なトラフィック ロード バランシング
- 単一のコントロール プレーン
- 単一セットのトラブルシューティング ツール（ping、traceroute など）

これらの利点のうち、最も重要なものは、おそらく Enhanced Interior Gateway Routing Protocol（EIGRP）または Open Shortest Path First（OSPF）をルーティング プロトコルとして使用して設定されたルーテッド アクセス設計を使用した場合のネットワーク コンバージェンス時間の改善です。最適なレイヤ 2 アクセス設計（スパニング ツリー ループあり、ループなしのいずれか）のコンバージェンス時間とレイヤ 3 アクセス設計のコンバージェンス時間を比較した場合、レイヤ 2 設計の 800 ～ 900 ms からレイヤ 3 アクセス設計の 200 ms 未満まで、4 倍のコンバージェンス時間の改善が得られます。

ルーテッド アクセス設計の詳細については、次の Web サイトにある『*High Availability Campus Network Design – Routed Access Layer using EIGRP or OSPF*』ドキュメントを参照してください。

http://www.cisco.com/application/pdf/en/us/guest/netsol/ns432/c649/ccmigration_09186a0080811468.pdf

キャンパス ディストリビューション レイヤ

キャンパス LAN のディストリビューション レイヤに含まれるネットワーク部分は、ワイヤリング クローゼット スイッチからネクストホップ スイッチまでです。キャンパス ディストリビューション レイヤ スイッチの詳細については、次の Web サイトで入手可能な製品マニュアルを参照してください。

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

ディストリビューション レイヤでは、冗長性を確保してハイ アベイラビリティを保証することが重要です。たとえば、ディストリビューション レイヤ スイッチ（またはルータ）とアクセス レイヤ スイッチの間に冗長なリンクを確保します。レイヤ 2 にトポロジ上のループが発生しないようにするには、可能であれば、冗長なディストリビューション スイッチ間の接続にレイヤ 3 リンクを使用します。

ファーストホップ冗長プロトコル

ディストリビューション スイッチが L2/L3 境界となるキャンパス階層モデルでは、サポートする L2 ドメイン全体のデフォルト ゲートウェイとしても動作します。この環境は大規模になることがあり、デフォルト ゲートウェイとして動作するデバイスが停止した場合、大きな障害が発生する可能性があるので、いくつかの冗長性の形式が必要になります。

Gateway Load Balancing Protocol（GLBP; ゲートウェイ ロード バランシング プロトコル）、Hot Standby Router Protocol（HSRP; ホットスタンバイ ルータ プロトコル）、および Virtual Router Redundancy Protocol（VRRP; 仮想ルータ冗長プロトコル）は、すべてのファーストホップ冗長プロトコルです。シスコは、必要なデフォルト ゲートウェイの冗長性に対応するために、最初に HSRP を開発しました。その後、Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）は、Virtual Router Redundancy Protocol（VRRP; 仮想ルータ冗長プロトコル）をデフォルト ゲートウェイの冗長性を備える標準ベースの方法として承認しました。最近になって、シスコは、HSRP および VRRP の両方に固有の制限の一部を解消するために、GLBP を開発しました。

Cisco 機能拡張に対応する HSRP および VRRP は、両方ともデフォルト ゲートウェイをバックアップする堅固な方法を備え、適切に調整された場合、冗長なディストリビューション スイッチに 1 秒未満でフェールオーバーを提供できます。

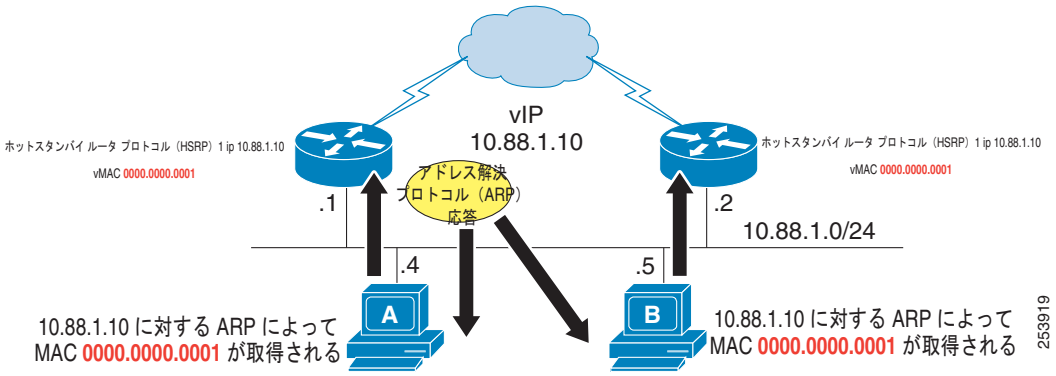
Gateway Load Balancing Protocol（GLBP）

HSRP および VRRP と同様に、シスコの Gateway Load Balancing Protocol（GLBP）は、障害の発生したルータや回線からのデータ トラフィックを保護すると共に、冗長ルータのグループ間のパケット ロード シェアリングを可能にします。デフォルト ゲートウェイの冗長性を提供するために HSRP または VRRP が使用される場合、ピア関係にあるバックアップ メンバーは、処理を引き継ぎ、トラフィックをアクティブに転送するために、発生する障害イベントを待機してアイドル状態となります。

GLBP を開発する以前は、アップリンクをより効率的に利用する方法は実装および管理が困難でした。ある手法では、HSRP および STP/RSTP ルートが、あるピアを目指す偶数の VLAN と別のピアを目指す奇数の VLAN を持つディストリビューション ノード ピア間で交互に使用されました。別の手法では、1 つのインターフェイス上で複数の HSRP グループを使用し、DHCP を使用して複数のデフォルト ゲートウェイ間で交互に使用されました。これらの手法は動作しましたが、設定、保守、または管理の観点から見たときに最適ではありませんでした。

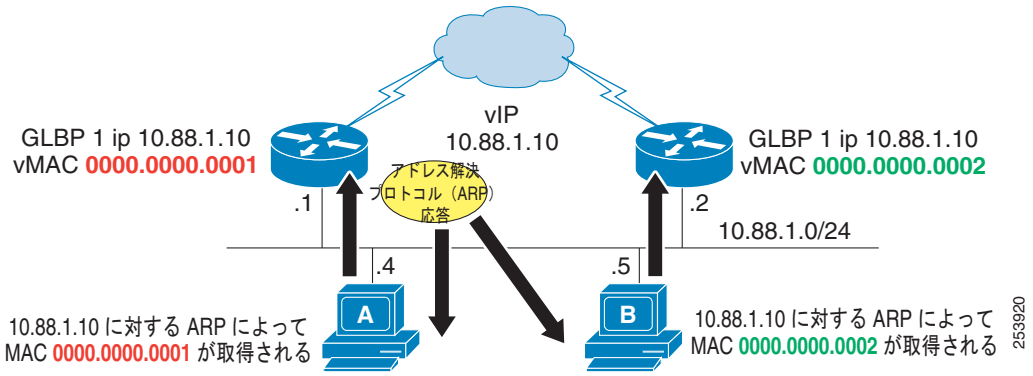
GLBP は HSRP と同じように設定され、機能します。HSRP では、Address Resolution Protocol（ARP; アドレス解決プロトコル）を使用してデフォルト ゲートウェイの物理 MAC アドレスを取得するときに、単一の仮想 MAC アドレスがエンドポイントに指定されます（図 3-5 を参照）。

図 3-5　HSRP では 1 つの仮想 MAC アドレスを使用



2 つの仮想 MAC アドレスが、各 GLBP ピアに 1 つずつ GLBP とともに存在します（図 3-6 を参照）。エンドポイントが ARP を使用してデフォルト ゲートウェイを決定する場合、仮想 MAC アドレスがラウンドロビン方式で照合されます。フェールオーバーとコンバージェンスは、HSRP と同様に動作します。バックアップ ピアは、障害が発生したデバイスの仮想 MAC アドレスを想定して、障害が発生したピアへのトラフィックの転送を開始します。

図 3-6　GLBP では各 GLBP ピアに 1 つずつ、2 つの仮想 MAC アドレスを使用



最終的には、より均等なアップリンクの利用が最小の設定で実現します。副次的な効果として、アップリンクまたはプライマリ ディストリビューション ノードのコンバージェンス イベントがホスト数の半分だけに影響を与え、コンバージェンス イベントの影響を平均 50% 未満にします。

HSRP、VRRP、および GLBP の詳細については、次の Web サイトにある『*Campus Network for High Availability Design Guide*』を参照してください。

http://www.cisco.com/application/pdf/en/us/guest/netsol/ns431/c649/ccmigration_09186a008093b876.pdf

ルーティング プロトコル

高速コンバージェンス、ロード バランシング、および耐障害性を保証するには、ディストリビューション レイヤで、OSPF や EIGRP などのレイヤ 3 ルーティング プロトコルを設定します。コンバージェンス時間を最適化および制御する場合や、複数のパスおよびデバイスにトラフィックを分散させる場合は、ルーティング プロトコル タイマー、パスまたはリンク コスト、およびアドレス サマリーなどのパラメータを使用します。また、**passive-interface** コマンドを使用して、ルーティングに関するネイバー ルータとの隣接関係がアクセス レイヤを介して形成されることを防止することを推奨します。このような隣接関係は、一般には必要ありません。これらの隣接関係があると、余分な CPU オーバーヘッドが作成され、メモリの消費量が増加します。これは、ルーティング プロトコルがこれらの隣接関係をトラッキングするためです。アクセス レイヤ方向のすべてのインターフェイス上で **passive-interface** コマンドを使用すると、ルーティング アップデートがこれらのインターフェイスから送信されることが防止されます。したがって、ネイバー ルータとの隣接関係は形成されません。

キャンパス コア レイヤ

キャンパス LAN のコア レイヤに含まれるネットワーク部分は、ディストリビューション ルータまたはレイヤ 3 スイッチから 1 つまたは複数のハイエンド コア レイヤ 3 スイッチまたはルータまでです。コア レイヤのレイヤ 3 対応 Catalyst スイッチは、多数のキャンパス ディストリビューション レイヤに相互接続性を提供できます。キャンパス コア レイヤ スイッチの詳細については、http://www.cisco.com/en/US/products/hw/switches/index.html で入手可能なマニュアルを参照してください。

コア レイヤにおいても、ハイ アベイラビリティを保証するために、次のタイプの冗長性を確保することが非常に重要です。

- 冗長なリンクまたはケーブル パス

  この冗長性により、ダウンまたは誤作動しているリンクを迂回してトラフィックを再ルーティングできることが保証されます。

- 冗長なデバイス

  この冗長性により、デバイスに障害が発生したときに、その障害デバイスが実行していたタスクをネットワーク内の別のデバイスが引き継げることが保証されます。

- 冗長なデバイス サブシステム

  この冗長性により、デバイス内で複数の電源およびモジュールを使用できることが保証されます。その結果、これらのコンポーネントのいずれかに障害が発生してもデバイスは機能し続けることができます。

Cisco Catalyst 6500 Virtual Switching System（VSS）1440 を使用すると、2 つの Catalyst 6500 スーパーバイザ エンジンを一緒にプールして 1 つのエンジンとして機能させることにより、これらすべての領域で冗長性を確保できます。VSS の詳細については、次の Web サイトで入手可能な製品マニュアルを参照してください。

http://www.cisco.com/en/US/products/ps9336/index.html

コア レイヤのルーティング プロトコルは、パスの冗長性と高速コンバージェンスにあわせて再度設定および最適化する必要があります。ネットワーク接続はレイヤ 3 でルーティングされる必要があるため、コアに STP を含めないでください。最終的に、コア デバイスとディストリビューション デバイス間の各リンクは、独自の VLAN またはサブネットに属し、30 ビット サブネット マスクを使用して設定される必要があります。

データ センターとサーバ ファーム

一般に、メディア リソース サーバなどの Cisco Unified Communications Manager（Unified CM）クラスタ サーバは、ファイアウォールで保護されたデータ センターまたはサーバ ファーム環境に配置されます。また、カンファレンス ブリッジ、DSP またはトランスコーダ ファーム、メディア ターミネーション ポイントなどの、集中型ゲートウェイと集中型ハードウェア メディア リソースも、データ センターまたはサーバ ファームに配置されることがあります。Cisco Unified Communications Manager（Unified CM）クラスタ サーバおよびメディア リソースに関連したファイアウォールの配置は、ネットワークにおけるセキュリティの設計および実装方法に影響を与える可能性があります。Unified Communications システムに関連したファイアウォール配置の設計ガイドラインについては、「ファイアウォール」（P.4-25）を参照してください。

これらのサーバとリソースは音声ネットワークにおいて重要であるため、すべての Unified CM クラスタ サーバ、集中型音声ゲートウェイ、および集中型ハードウェア リソースは、複数の物理スイッチに分散させ、可能であればキャンパス内の複数の物理ロケーションにも分散させることを推奨します。このようにリソースを分散させると、ハードウェア障害（スイッチやスイッチのライン カードの障害など）が発生しても、少なくともクラスタ内の一部のサーバを使用して、引き続きテレフォニー サービスを提供できることが保証されます。また、一部のゲートウェイとハードウェア リソースを使用して、引き続き公衆網へのアクセスと付加サービスを提供することもできます。物理的に分散させるだけでなく、これらのサーバ、ゲートウェイ、およびハードウェア リソースを別の VLAN またはサブネットに分散させる必要もあります。そのように分散させると、特定の VLAN 上でブロードキャスト ストームまたは DoS 攻撃が発生しても、一部の音声接続およびサービスは中断されずに済みます。

Power over Ethernet（PoE）

PoE（またはインライン パワー）は、標準的なイーサネット Unshielded Twisted-Pair（UTP; シールドなしツイストペア）ケーブルを介して供給される 48 V DC 電源です。IP Phone や、Aironet Wireless Access Points などのインライン Powered Device（PD; 受電装置）は、壁面コンセントを使用する代わりに、インライン パワー対応の Catalyst イーサネット スイッチや他のインライン Power Source Equipment（PSE）によって供給される電力を受けられます。デフォルトでは、インライン パワーは、すべてのインライン パワー対応 Catalyst スイッチ上で有効になっています。

インライン パワー対応のスイッチを Uninterruptible Power Supplies（UPS; 無停電電源装置）と共に配置すると、電源障害の発生中も IP Phone が電力を継続して受けることが保証されます。この電源障害の発生中にテレフォニー ネットワークの残りの部分が使用可能であれば、IP Phone はコールの発信および受信を継続して行うことができます。IP Phone でインライン パワー駆動型イーサネット ポートを使用するには、インライン パワー対応のスイッチをワイヤリング クローゼット内のキャンパス アクセス レイヤに配置する必要があります。この配置により、壁面コンセントが不要になります。

注意　PoE を提供するためにパワー インジェクタまたは電源パッチパネルを使用すると、デバイスによっては損傷することがあります。これは、電力が常にイーサネット ペア線に供給されるためです。PoE スイッチ ポートは、PoE を必要とするデバイスが存在するかどうかを自動的に検出してから、ポートごとに PoE を有効にします。

シスコでは現在、Cisco PoE インライン パワーのほかに、IEEE 802.3af PoE 標準をサポートしています。大部分の Cisco スイッチおよび Cisco Unified IP Phone は、802.3af 標準に準拠しています。802.3af PoE 標準をサポートする Cisco Unified IP Phone については、「エンドポイント機能の要約」（P.18-53）を参照してください。

カテゴリ 3 ケーブリング

カテゴリ 3 ケーブリングを IP コミュニケーションに使用できるのは、次の条件を満たす場合です。

- PC ポートを持ち、そのポートに PC が接続された電話機は、10 Mb 全二重に設定されている必要があります。

  このように設定する場合は、アップストリーム スイッチ ポート、電話機のスイッチ ポートと PC ポート、および PC の NIC ポートを 10 Mb 全二重に固定して設定する必要があります。どのポートも、自動ネゴシエーションには設定しないでください。必要であれば、電話機の PC ポートを 10 Mb 半二重に固定して設定してもかまいません。これにより、PC の NIC が 10 Mb 半二重にネゴシエートするようになります（PC の NIC が自動ネゴシエーションに設定されていることを前提とします）。この設定が受け入れられるのは、電話機とアップストリーム スイッチ ポート間のアップリンクが 10 Mb 全二重に設定されている場合です。

- PC ポートを持たずに 10 Mb スイッチ ポートを持つ電話機は、10 Mb 半二重に自動ネゴシエートできるようになっている必要があります。

  これらの電話機では 10 Mb イーサネットだけがサポートされ、電話機のポートを手動で設定変更することができないため、アップストリーム スイッチ ポートを、自動ネゴシエーションまたは 10 Mb 半二重に設定する必要があります。どちらの場合も、これらの電話機は 10 Mb 半二重にネゴシエートします。

- PC ポートを持つが、そのポートに PC が接続されていない電話機は、10 Mb 半二重にネゴシエートできるようにしてもかまいません。

  これらの電話機をデフォルトのスイッチ ポート設定である自動ネゴシエーションのままにした場合、アップストリーム スイッチ ポートを 10 Mb 半二重に設定すると、これらの電話機は 10Mb 半二重に戻ります。

（注） Cisco Unified IP Phone 7912 については、PC が接続されているときには、カテゴリ 3 ケーブルと共に使用しないでください。これは、この電話機のスイッチ ポートと PC ポートを 10 Mb 全二重にすることができないためです。

IBM タイプ 1A および 2A ケーブリング

IBM Cabling System（ICS）またはトークン リング シールド付きツイストペア タイプ 1A または 2A ケーブリングを IP コミュニケーションに使用できるのは、次の条件を満たす場合です。

- ケーブル長は 100 メートル以下にする必要があります。
- Universal Data Connector（UDC）から RJ-45 イーサネット標準に変換する場合は、インピーダンス整合していないアダプタを使用する必要があります。

（注） トークン リング ケーブルにあるツイストペアは 2 組だけです。したがって、IP Phone へのインライン パワーはサポートされますが、ミッドスパンの給電（Cisco Inline Power と 802.3af を使用する）はペア線を 3 組以上必要とするためサポートされません。

（注） 1000 BASE-T は 4 つのツイストペアが必要になるため、ギガビット イーサネットは IBM 配線システムではサポートされません。Cisco IP Phone 上の 10/100/1000 BASE-T イーサネット インターフェイスと組み合せて IBM 配線システムが使用される場合、サポートされる速度は 10 Mbps と 100 Mbps だけです。

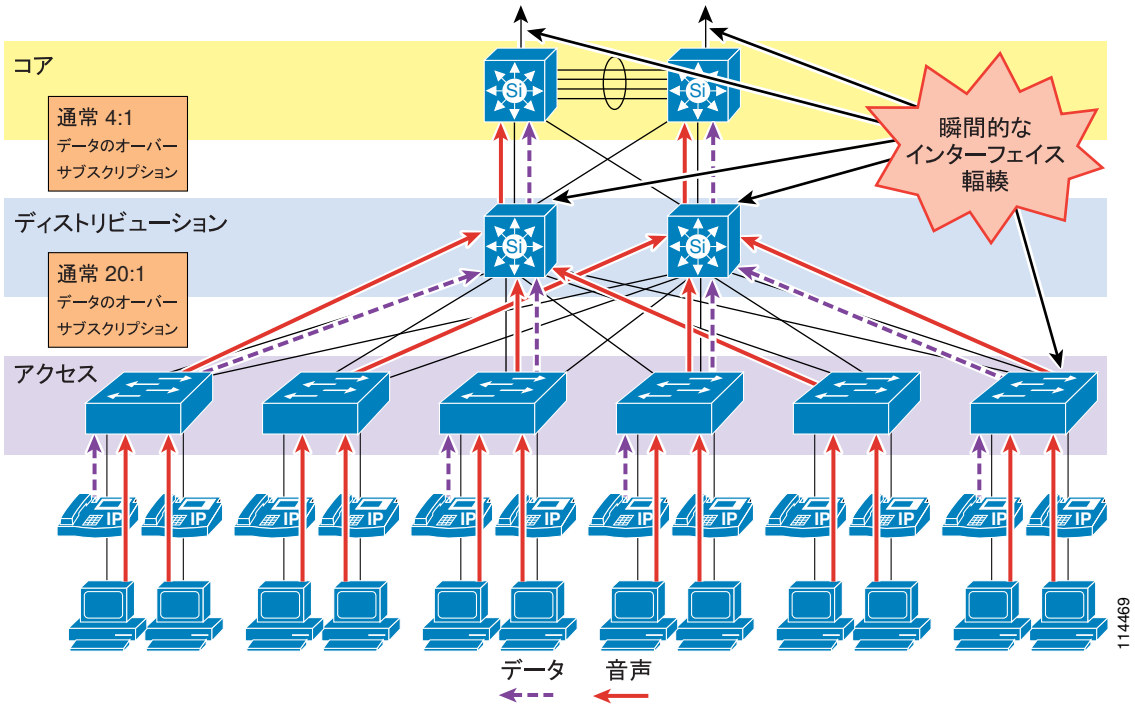
ネットワーク上でデータを伝送しても、ケーブル プラントの品質を十分にテストしたことにならない場合があります。これは、このようなテストでは、準拠に起因しない問題が判明しない場合があるためです。したがって、お客様は、タイプ 1A および 2A ケーブリングの設置がイーサネット標準に準拠していることを確認するために、ケーブル プラントの調査を実施することを推奨します。

LAN の QoS

最近まで、データ トラフィックにはもともと非同期性があること、およびバッファのオーバーフローとパケット損失に耐えるネットワーク デバイスの機能により、企業キャンパスでは、QoS は問題になりませんでした。しかし、音声やデータなどの新しいアプリケーションでは、パケット損失や遅延の影響を受けやすいので、バッファと帯域幅の不足が、企業キャンパスにおける主要な QoS の問題となります。

図 3-7 は、LAN インフラストラクチャで発生する一般的なオーバーサブスクリプションを示しています。

図 3-7　LAN におけるデータ トラフィックのオーバーサブスクリプション



このオーバーサブスクリプションが発生すると、個々のトラフィック量の影響や、複数の独立したトラフィック送信元の累積効果も加わって、出力インターフェイスのバッファが瞬時に満杯になる場合があります。そのため、さらにパケットが出力バッファに入力される場合は、パケットがドロップします。キャンパス スイッチはハードウェアベースのバッファを使用していますが、バッファはインターフェイス速度の点でルータの WAN インターフェイスよりもはるかに遅いため、存続期間の短いトラフィック バーストであっても、バッファのオーバーフローとパケットのドロップが発生する可能性が高くなります。

ファイル共有などのアプリケーション（ピアツーピアとサーバベースの両方）、リモート ネットワーク上のストレージ、ネットワークベースのバックアップ ソフトウェア、およびサイズの大きな添付ファイルを持つ電子メールによって、ネットワークの輻輳がより頻繁に発生したり、より長期間発生したり

する場合があります。最近のワーム攻撃の弊害に、膨大な量のネットワーク トラフィック（ユニキャスト ベースとブロードキャストストーム ベースの両方）があります。この攻撃により、ネットワークの輻輳が増加します。バッファの管理ポリシーが適用されていない場合は、すべてのトラフィックにおいて、LAN の損失、遅延、およびジッタ特性が影響を受けることがあります。

また、冗長なネットワーク要素の障害による影響も考慮する必要があります。この障害により、トポロジ変更が発生します。たとえば、ディストリビューション スイッチに障害が発生した場合は、すべてのトラフィック フローが残りのディストリビューション スイッチを介して再度確立されます。障害の発生前にロード バランシング設計によって 2 つのサイト間で負荷が共有されていても、障害の発生後にすべてのフローが単一のスイッチに集中すると、出力バッファが、通常では発生しない状況に陥る可能性があります。

音声などのアプリケーションの場合、このパケット損失と遅延は、重大な音声品質の低下を招きます。したがって、これらのバッファを管理し、パケットの損失、遅延、および遅延変動（ジッタ）を最小限に抑えるために、QoS ツールが必要です。

ネットワーク全体でトラフィックを管理し、音声品質を保証するには、次のタイプの QoS ツールが必要です。

- トラフィック分類

  分類では、ネットワークの Class of Service（CoS; サービス クラス）に関する要件を示す特定のプライオリティがパケットにマークされます。このパケット マーキングが信頼される地点とされない地点の間は、信頼性境界と見なされます。信頼性は、一般に、音声デバイス（電話機）までは拡張されますが、データ デバイス（PC）には拡張されません。

- キューイングまたはスケジューリング

  インターフェイス キューイングまたはスケジューリングでは、ネットワーク全体で処理を高速化するため、パケットが分類に基づいて複数のキューのいずれかに割り当てられます。

- 帯域幅のプロビジョニング

  プロビジョニングでは、すべてのアプリケーションおよび要素のオーバーヘッドに必要な帯域幅が正確に計算されます。

次の項では、これらの QoS メカニズムをキャンパス環境で使用する方法について説明します。

- 「トラフィック分類」（P.3-16）
- 「インターフェイス キューイング」（P.3-18）
- 「帯域幅のプロビジョニング」（P.3-19）
- 「QoS が使用されない場合の IP コミュニケーションの障害」（P.3-19）

トラフィック分類

可能な限りネットワーク エッジの近くでトラフィックを分類したり、マークすることは、常に Cisco ネットワーク デザイン アーキテクチャの必要不可欠となる部分でした。トラフィック分類は、キャンパス スイッチおよび WAN インターフェイス内で使用される各種キューイング体系にアクセスするための基本的基準です。Cisco IP Phone は、音声制御シグナリングと音声 RTP ストリームを送信元でマークします。その際は、表 3-3 に示されている値に従います。IP Phone は、このようにトラフィック フローを分類可能であり、実際に分類する必要があります。

表 3-3 は、LAN インフラストラクチャのトラフィックを分類する場合の要件をリストしています。

表 3-3　各種タイプのネットワーク トラフィックのトラフィック分類ガイドライン

	レイヤ 3 分類			レイヤ 2 分類
アプリケーション	タイプ オブ サービス（ToS） IP Precedence（IPP）	Per-Hop Behavior（PHB）	Differentiated Services Code Point（DSCP）	サービス クラス（CoS）
ルーティング	6	CS6	48	6
音声 Real-Time Transport Protocol（RTP）	5	EF	46	5
ビデオ会議	4	AF41	34	4
ストリーミング ビデオ	4	CS4	32	4
コール シグナリング[1]	3	CS3（現行） AF31（以前）	24（現行） 26（以前）	3
トランザクション データ	2	AF21	18	2
ネットワーク管理	2	CS2	16	2
Scavenger	1	CS1	8	1
ベストエフォート型	0	0	0	0

1. 呼制御シグナリング トラフィック用の推奨 DSCP/PHB マーキングは、26/AF31 から 24/CS3 に変更されています。シスコではこの変更を反映するようにマーキングを移行しましたが、一部の製品は、引き続きシグナリング トラフィックを 26/AF31 としてマークします。したがって、当面は、コール シグナリング用に AF31 と CS3 の両方を予約することを推奨します。

トラフィック分類の詳細については、次の Web サイトで入手可能な『*Enterprise QoS Solution Reference Network Design (SRND)*』を参照してください。

http://www.cisco.com/go/designzone

ビデオ テレフォニーのトラフィック分類

IP ビデオ テレフォニーに関係する主なクラスは、次のとおりです。

- 音声

  音声は、CoS 5（IP Precedence 5、PHB EF、または DSCP 46）に分類されます。

- ビデオ会議

  ビデオ会議は、CoS 4（IP Precedence 4、PHB AF41、または DSCP 34）に分類されます。

- コール シグナリング

  音声およびビデオ会議のコール シグナリングは、CoS 3（IP Precedence 3、PHB CS3、または DSCP 24）に分類されるようになりましたが、以前は PHB AF31 または DSCP 26 に分類されていました。

Cisco Unified Communications ネットワークでは、これらの分類をベスト プラクティスとして強く推奨します。

ビデオ コールと音声専用コール間の QoS マーキングの相違点

コールの音声コンポーネントは、進行中のコールのタイプに応じて、2 つのいずれかに分類できます。音声だけの通話呼のメディアは、CoS 5（IP Precedence 5 または PHB EF）に分類されますが、ビデオ会議の音声チャネルのメディアは CoS 4（IP Precedence 4 または PHB AF41）に分類されます。すべ

ての Cisco IP Video Telephony 製品は、Cisco Corporate QoS Baseline 標準に準拠し、ビデオ コールのオーディオ チャネルとビデオ チャネルの両方が CoS 4（IP Precedence 4 または PHB AF41）にマークされている必要があります。この推奨事項には次の理由がありますが、これら以外にもあります。

- オーディオ チャネルとビデオ チャネルのリップシンクを維持する。
- オーディオだけのコールとビデオ コールに個別のクラスを提供する。

シグナリング クラスは、すべての音声シグナリング プロトコル（SCCP、MGCP など）、およびビデオ シグナリング プロトコル（SCCP、H.225、RAS、CAST など）に適用されます。これらのプロトコルについては、「ソフトウェアベースのエンドポイント」（P.18-41）の項で詳しく説明します。

推奨クラスを使用する場合、最初の手順は、パケットを分類する場所（トラフィックの QoS 分類でトラフィックを最初にマークするデバイス）の決定です。トラフィックをマークまたは分類する場所は、基本的には 2 箇所あります。

- 発信元エンドポイント：分類はアップストリーム スイッチおよびルータで信頼されます。
- スイッチまたはルータ：エンドポイントにパケットを分類する機能がない場合、または正しく分類されない場合。

Trusted Relay Point（TRP）を使用した QoS の強制

Trusted Relay Point (TRP) は、エンドポイントからのメディア フローの DSCP 値の強制および再マーキングに使用できます。この機能により、QoS がローカルに変更されている可能性がある、ソフトフォンなどのエンドポイントからのメディアに QoS を強制的に適用できます。この場合、メディアの QoS 値はローカルに変更されている可能性があります。

TRP は、既存の Cisco IOS Media Termination Point（MTP）機能に基づくメディア リソースです。

エンドポイントを「信頼できるリレーポイントを使用（Use Trusted Relay Point)」に設定し、すべてのコールに対して TRP を呼び出すことができます。

QoS の強制では、TRP は Unified CM のサービス パラメータでメディア用に設定された QoS 値を使用して、エンドポイントからのメディア ストリームで QoS 値を再マーキングし、強制的に適用します。

TRP 機能は、Cisco IOS MTP とトランスコーディング リソースによってサポートされます（Unified CM を使用して、MTP またはトランスコーディング リソースで [Enable TRP] チェックボックスをオンにして、TRP 機能をアクティブにします)。

インターフェイス キューイング

レイヤ 2（CoS）とレイヤ 3（DSCP または PHB）でパケットを適切なタグでマークしたら、この分類に基づいてトラフィックのスケジューリングまたはキューイングを行うようにネットワークを設定することが重要です。この設定により、各クラスのトラフィックに対して、必要なサービスがネットワークから提供されます。キャンパス スイッチ上で QoS を使用可能にすることにより、すべての音声トラフィックを個別のキューを使用するように設定できます。この設定により、インターフェイス バッファが即時に満杯になるときでも、音声パケットがドロップする可能性を事実上なくすことができます。

ネットワーク管理ツールが、キャンパス ネットワークが輻輳していないことを示す場合がありますが、それでも音声品質を保証するためには、QoS ツールが必要です。ネットワーク管理ツールは、サンプルの期間全体の平均的な輻輳しか示しません。この平均値は便利ですが、キャンパス インターフェイス上の輻輳のピークを示しません。

キャンパス内の送信インターフェイス バッファは、ネットワーク トラフィック自体にバースト性があるため、短い時間間隔で散発的に輻輳する傾向があります。輻輳が起きると、その送信インターフェイスを宛先とするすべてのパケットがドロップされます。音声トラフィックのドロップを防止する唯一の方法は、キャンパス スイッチ上で複数のキューを設定することです。このため、ポートごとに 2 つ以上の出力キューを持ち、レイヤ 2、レイヤ 3、またはその両方の QoS 分類に基づいてこれらのキュー

にパケットを送信する機能を持つスイッチを常に使用することを推奨します。大部分の Cisco Catalyst スイッチは、ポートごとに 2 つ以上の出力キューをサポートしています。Cisco Catalyst スイッチのインターフェイス キューイング機能の詳細については、http://www.cisco.com/en/US/products/hw/switches/index.html にあるマニュアルを参照してください。

帯域幅のプロビジョニング

キャンパス LAN では、帯域幅プロビジョニングの推奨事項は、「*プロビジョニングは多めに、サブスクリプションは少なめに*」という標語に集約できます。この標語は、使用可能な帯域幅は常に負荷よりも相当量広くし、LAN リンク上に定常的な輻輳がないように、LAN インフラストラクチャを慎重に設計するという意味です。

統合されたネットワークに流れ込む音声トラフィックが増加することは、ネットワーク トラフィックの負荷全体が大幅に増加することを意味するわけではありません。したがって、帯域幅のプロビジョニングを行う場合は、常に、データ トラフィック要件の要求に従います。この設計目標は、テレフォニー シグナリングまたはメディア フローによって通過するデータ トラフィックの大規模な輻輳がすべてのリンク上で発生しないようにすることにあります。単一の G.711 音声コールの帯域幅要件（約 86 Kbps）とファストイーサネット リンクそのものの帯域幅（100 Mbps）を比較してわかるのは、音声は LAN 内でネットワークの輻輳を引き起こすトラフィックのソースではなく、むしろ LAN ネットワークの輻輳から保護されるトラフィック フローであるということです。

QoS が使用されない場合の IP コミュニケーションの障害

QoS が配置されていないと、パケット ドロップや大幅な遅延およびジッタが発生して、テレフォニー サービスの障害を引き起こすことがあります。メディア パケットにドロップ、遅延、およびジッタが発生すると、クリック音が聞こえる、音声が異常になる、無音状態が長期間続く、およびエコーが聞こえるなど、ユーザが知覚できる影響が現れます。

シグナリング パケットが同様の状況になった場合は、ユーザ入力に対する反応が遅い（ダイヤル トーンの遅延など）、応答しても呼出音が続く、および最初のダイヤルが無効になった（したがって電話を切ってリダイヤルする必要がある）とユーザが思い込んで二重に番号をダイヤルすることなど、ユーザが知覚できる障害が発生します。さらに極端なケースとしては、エンドポイントが再初期化される、コールが終了する、および拠点で SRST 機能が誤動作する（ゲートウェイ コールの中断を引き起こす）ことなどが挙げられます。

これらの影響は、すべての配置モデルに現れます。ただし、単一サイト（キャンパス）配置では、リンクの中断が続くことによってこのような状況が発生する可能性は低くなります。これは、一般に LAN 環境にはより大きな帯域幅が配置される（最小リンクは 100 Mbps）ので、残りの帯域幅の一部を IP コミュニケーション システムに使用できるためです。

WAN ベースの配置モデルでは、トラフィックの輻輳によって、リンクの中断が続いたり、より高い頻度で発生したりする可能性が高くなります。これは、使用可能な帯域幅が LAN よりもはるかに小さい（一般に 2 Mbps 未満）ためです。そのため、リンクがより簡単に飽和します。リンクの中断は、エンドポイントと Unified CM サーバ間のシグナリング トラフィックも遅延またはドロップする可能性があるので、音声メディアがパケット ネットワークを通過するかどうかに関係なく、ユーザに大きな影響を与える場合があります。

Cisco UCS B シリーズ ブレード サーバを使用した仮想 Unified Communications に関する QoS 設計上の考慮事項

仮想化された Unified Communications ソリューションでは、Cisco Unified Communications 製品を、サポート対象のハイパーバイザ、サーバ、およびストレージ製品の選択セット上で仮想マシンとして実行できます。仮想 Unified Communications ソリューションの最も重要なコンポーネントは、Cisco Unified Computing System（UCS）プラットフォームとハイパーバイザ仮想化テクノロジーです。仮想化された Unified Communications の設計には、QoS に関して、次のような特別な考慮事項があります。Cisco Unified Computing System（UCS）アーキテクチャ、アプリケーション仮想化のハイパーバイザ テクノロジー、および Storage Area Networking（SAN; ストレージ エリア ネットワーキング）の概念の詳細については、「仮想サーバでの Unified Communications の配置」（P.5-59）を参照してください。

仮想化された環境では、Cisco Unified Communications Manager（Unified CM）のような Unified Communications アプリケーションが、仮想マシンとして VMware 上で実行されます。これらの Unified Communications 仮想マシンは、Media Convergence Server（MCS）配置のハードウェアベースのイーサネット スイッチではなく、仮想ソフトウェア スイッチに接続されます。次のタイプの仮想ソフトウェア スイッチを使用できます。

- ローカルの VMware vSwitch

  VMware ESXi ハイパーバイザのすべてのエディションで使用可能であり、VMware ライセンス方式の種類に依存しません。仮想ソフトウェア スイッチングは、仮想マシンが実行しているローカルの物理ブレード サーバに限定されます。

- 分散型の VMware vSwitch

  VMware ESXi ハイパーバイザの Enterprise Plus Edition に限り使用可能です。分散仮想ソフトウェア スイッチングは、複数の物理ブレードにまたがることができ、ソフトウェア スイッチの管理を簡素化します。

- Cisco Nexus 1000V スイッチ

  シスコには、Nexus 1000 仮想（1000V）スイッチと呼ばれるソフトウェア スイッチがあります。Cisco Nexus 1000V には、VMware ESXi の Enterprise Plus Edition が必要です。これは、複数の VMware ホストおよび仮想マシンで認識可能な分散仮想スイッチです。Cisco Nexus 1000V シリーズは、ポリシーベースの仮想マシン接続、モバイルの仮想マシン セキュリティ、拡張 QoS、およびネットワーク ポリシーを提供します。

仮想接続の観点から見ると、各仮想マシンは、ブレード サーバに配置されている上記の仮想スイッチのいずれかに接続できます。ブレード サーバは、UCS シャーシ内のファブリック エクステンダから UCS ファブリック インターコネクト スイッチ（Cisco UCS 6100 シリーズなど）を経由して、ネットワークの残りの部分に物理的に接続します。UCS ファブリック インターコネクト スイッチは、お客様の 1 Gb または 10 Gb イーサネット LAN および FC SAN と物理的配線が接続される場所です。

トラフィック フローの観点から見ると、仮想マシンからのトラフィックは、最初にソフトウェア仮想スイッチ（VMware vSwitch、VMware の分散 vSwitch、または Cisco Nexus 1000V スイッチなど）に転送されます。続いて、仮想スイッチは、ブレード サーバのネットワーク アダプタおよびファブリック エクステンダを介して、トラフィックを物理的な UCS ファブリック インターコネクト スイッチ（UCS 6100 シリーズ）に送信します。UCS ファブリック インターコネクト スイッチは、IP およびファイバ チャネル SAN トラフィックの両方を単線の Fiber Channel over Ethernet（FCoE）を介して伝送します。UCS ファブリック インターコネクト スイッチは IP トラフィックを IP スイッチ（Cisco Catalyst または Nexus シリーズ スイッチ）に送信し、IP スイッチは SAN トラフィックをファイバ チャネル SAN スイッチ（Cisco MDS シリーズ スイッチなど）に送信します。

標準的なスイッチング要素の QoS 動作

デフォルトでは、UCS 6100 シリーズのファブリック インターコネクト スイッチ内で、SAN スイッチに送信されるすべての Fiber Channel（FC; ファイバ チャネル）に対して優先度の QoS クラスが自動的に作成されます。この FC QoS クラスにドロップ ポリシーはなく、すべての FC トラフィックに 3 のレイヤ 2 CoS 値が付けられます。デフォルトでは、音声シグナリングおよびメディア トラフィックを含む他のすべてのトラフィック（イーサネットおよび IP）が、Best Effort QoS クラスに分類されます。

VMware のローカル vSwitch、VMware の分散 vSwitch、および UCS 6100 シリーズ スイッチでは、L3 DSCP 値を L2 CoS 値にマッピングできません。トラフィックは、L2 CoS だけに基づいて、UCS 6100 スイッチ内で優先順位を付けたり解除したりできます。

（注）　Unified Communications アプリケーションは、L3 DSCP 値だけを付けます（音声シグナリングに対する CS3 など）。ただし、ブレード サーバのネットワーク アダプタから発信されたすべてのトラフィックに、単一の L2 CoS 値を付けることができます。

Nexus 1000V ソフトウェア スイッチには、Catalyst シリーズ スイッチなどの従来のシスコ製物理スイッチのように、L3 DSCP 値を L2 CoS 値に、およびその逆にマッピングする機能があります。そのため、Unified Communications トラフィックが仮想マシンを離れて Nexus 1000V スイッチに到達したときに、その L3 DSCP 値を対応する L2 CoS 値にマッピングできます。続いて、UCS 6100 スイッチ内で、L2 CoS 値に基づいてこのトラフィックに優先順位を付けたり解除したりできます。

たとえば、CS3 の値が L3 DSCP の音声シグナリング トラフィックは、Nexus 1000V によって 3 の L2 CoS 値にマップされます。すべての Fibre Channel over Ethernet（FCoE）トラフィックは、Cisco UCS によって 3 の L2 CoS 値にマークされます。音声シグナリング トラフィックと FCoE トラフィックが Cisco UCS 6100 ファブリック インターコネクト スイッチに入力された場合は、どちらも 3 の CoS 値を伝送します。この状況では、音声シグナリング トラフィックが、ファイバ チャネル プライオリティ クラスを使用してキューとスケジューリングを共有することによって、無損失動作が実現します（UCS 6100 ファブリック インターコネクト スイッチ内の CoS 3 のファイバ チャネル プライオリティ クラスは、そのクラスが他のタイプのトラフィックと共有できないことを意味しているわけではありません）。

一方、FCoE トラフィックの L2 CoS 値はデフォルト値の 3 から別の値に変更することができ、CoS 3 は音声シグナリング トラフィック専用として保存できます。ただし、FCoE CoS の値が 3 に設定されなかった場合に一部の Converged Network Adapter（CNA; 統合型ネットワーク アダプタ）で問題が発生するため、このアプローチは推奨できません。

輻輳シナリオ

物理的なサーバ設計では、ハード ドライブは MCS サーバにローカルに接続され、SCSI トラフィックがイーサネット IP トラフィックと競合することはありません。

UCS B シリーズ システムを使用する仮想 Unified Communications の設計は、従来の MCS ベースの設計とは異なります。仮想 Unified Communications の設計では、ハード ドライブがリモートで、FC SAN を介してアクセスされるため、FC SAN トラフィックが帯域幅を得るために UCS 6100 シリーズ スイッチ内でイーサネット IP トラフィックと競合する可能性があります。UCS 6100 スイッチ内に FC トラフィックのドロップ ポリシーがないため、この結果として、音声関連の IP トラフィック（シグナリングおよびメディア）がドロップされる可能性があります。ただし、UCS 6100 スイッチでは高キャパシティのスイッチング ファブリックが提供されており、さらにサーバ ブレードごとの使用可能な帯域幅が一般的な Unified Communications アプリケーションの最大トラフィック要件を大幅に上回っているため、この輻輳またはオーバーサブスクリプションのシナリオが発生する可能性は非常に低くなります。

設計に関する推奨事項

Nexus 1000V は、仮想化されたデータ センターには不可欠で他の仮想スイッチ実装では使用できない拡張 QoS およびその他の機能（ACL、DHCP スヌーピング、IP ソース ガード、SPAN など）を提供します。Cisco Unified Communications アプリケーションを UCS B シリーズ システムで稼動している他の多くの仮想マシンとともに配置するような大規模データ センターの実装では、L3 DSCP 値を L2 CoS 値にマッピングする機能を有効にして、Nexus 1000V スイッチを使用することを推奨します。その他の Unified Communications 配置の場合、Nexus 1000V を使用するかどうかの決定は、UCS アーキテクチャ内で Unified Communications アプリケーションが使用できる帯域幅に応じて、ケースバイケースで変わります。輻輳シナリオが発生する可能性がある場合は、Nexus 1000V スイッチを配置する必要があります。

すべての仮想スイッチに配置できる代替ソリューションは、すべてのトラフィックに **Platinum**（CoS=5、ドロップ ポリシーなし）の QoS ポリシーを設定するように、Unified Communications サーバ ブレード上のすべての物理ネットワーク アダプタを設定することです。同じ UCS システムまたはシャーシで稼動している他のアプリケーションはすべて、QoS ポリシーを**ベストエフォート**に設定する必要があります。このアプローチのデメリットは、すべての非音声トラフィック（バックアップ、CDR、ログ、Web トラフィックなど）を含む仮想 Unified Communications アプリケーションのすべてのトラフィック タイプで、CoS 値が Platinum に設定されることです。このソリューションは最適ではありませんが、Unified Communications アプリケーションのトラフィックの優先順位を、FC SAN 行きのトラフィックの優先順位まで上げ、これによってトラフィック ドロップの可能性を減らします。

ネットワーク サービス

IP Communications システムの配置には、構造化されて可用性と回復力が高いネットワーク インフラストラクチャの調和の取れた設計、および Domain Name System（DNS; ドメイン ネーム システム）、DHCP（Dynamic Host Configuration Protocol）、TFTP（Trivial File Transfer Protocol）、Network Time Protocol（NTP; ネットワーク タイム プロトコル）を含むネットワーク サービスの統合セットが必要です。

ドメイン ネーム システム（DNS）

DNS を使用すると、ホスト名およびネットワーク サービスをネットワーク（複数可）内の IP アドレスにマッピングできます。ネットワーク内に配置された DNS サーバは、ネットワーク サービスをホスト名にマッピングし、次にホスト名を IP アドレスにマッピングするデータベースを備えています。ネットワーク上のデバイスは、DNS サーバに照会して、ネットワークにある他のデバイスの IP アドレスを受信できます。そのため、ネットワーク デバイス間の通信が容易になります。

DNS などの 1 つのネットワークサービスに完全に依存することは、重要な Unified Communications システムを配置するときに、リスク要素になることがあります。DNS サーバが使用不能になった場合、ネットワーク デバイスがそのサーバを利用してホスト名から IP アドレスへのマッピングを取得しているときは、通信に障害が発生することがあります。このため、ハイ アベイラビリティが要求されるネットワークでは、Unified CM と Unified Communications エンドポイント間の通信は、DNS 名前解決に依存しないことを推奨します。

標準配置では、Unified CM、ゲートウェイ、およびエンドポイント デバイスを設定して、ホスト名ではなく IP アドレスを使用することを推奨します。エンドポイント デバイス設定では、DNS サーバのアドレス、ホスト名、およびドメイン名などの DNS パラメータを設定することは推奨できません。初めて Unified CM クラスタにパブリッシャ ノードをインストールするとき、パブリッシャは、システムに提供したホスト名によってサーバ テーブルで参照されます。その後のサブスクライバのインストールおよび設定、またはエンドポイントの定義の前に、このサーバ エントリをパブリッシャのホスト名ではなく IP アドレスに変更する必要があります。クラスタに追加する各サブスクライバは、ホスト名で

はなく IP アドレスで、同じサーバ テーブルに定義する必要があります。各サブスクライバは、1 デバイスずつこのサーバ テーブルに追加する必要があります。新しいサブスクライバをインストールするときに定義する場合を除き、存在しないサブスクライバは定義しないでください。

パブリッシャおよびサブスクライバをインストールするときは、システム管理の目的で特に DNS が必要な場合を除き、DNS を有効にするオプションを選択しないことを推奨します。DNS を有効にする場合も、IP Communications エンドポイント、ゲートウェイ、および Unified CM サーバの設定では、DNS 名を使用しないことを強く推奨します。クラスタのサーバで DNS を有効にした場合でも、そのクラスタ外のデバイスとの通信にだけ使用して、クラスタ内サーバ間通信には使用しないでください。

Cisco Unified CM 5.0 以降のリリースでは、HOSTS ファイルまたは LHOSTS ファイルを手動で設定できません。HOSTS テーブルのローカル バージョンが各クラスタのパブリッシャによって自動的に構築され、セキュア通信チャネルを介してすべてのサブスクライバ ノードに配布されます。セキュアなクラスタ内通信には、このローカル テーブルが使用されます。テーブルには、Unified CM サーバ以外のエンドポイントのアドレスまたは名前は含まれていません。LMHOSTS ファイルは存在せず、Cisco Unified CM 5.0 以降のリリースでは使用されません。

DNS を使用した Unified CM の配置

場合によっては、DNS を設定および使用することが避けられないことがあります。たとえば、IP Communications ネットワーク内での IP Phone と Unified CM 間の通信に Network Address Translation（NAT; ネットワーク アドレス変換）が必要な場合、NAT 変換後のアドレスがネットワーク ホスト デバイスに正しくマッピングされることを保証するには、DNS が必要です。同様に、ホスト名をセカンダリ バックアップ サイトの IP アドレスにマッピングすることで、障害発生時にネットワークのフェールオーバーが正常に行われることを保証するには、一部の IP テレフォニー ディザスタ リカバリ ネットワーク設定で DNS を利用する必要があります。

このどちらかの状況で DNS の設定が必要になった場合は、DNS サーバを地理的に冗長な方式で配置する必要があります。この配置により、一方の DNS サーバに障害が発生しても、IP テレフォニー デバイス間のネットワーク通信が妨げられることはありません。DNS サーバを冗長にすると、一方の DNS サーバで障害が発生しても、引き続き、DNS を利用してネットワーク上で通信するデバイスが、バックアップまたはセカンダリ DNS サーバから、ホスト名から IP アドレスへのマッピングを受信できることが保証されます。

（注）　ローカルの HOSTS ファイルまたは DNS 照会によるクラスタ内のホスト名解決が実行されるのは、サブシステムの初期化時（サーバのブートアップ時）だけです。結果として、クラスタ内のサーバが、HOSTS ファイルまたは DNS サーバ上で変更された DNS 名を解決できるようにするには、クラスタ内のすべてのサーバ上で Cisco CallManager サービスを再起動する必要があります。

Unified CM は DNS を使用して次を実行できます。

- 簡素化されたシステム管理を提供する
- 完全修飾ドメイン名（FQDN）をトランク宛先の IP アドレスに解決する
- 完全修飾ドメイン名をドメイン名に基づく SIP ルート パターンの IP アドレスに解決する
- サービス（SRV）レコードをホスト名に解決し、SIP トランク宛先の IP アドレスに解決する

DNS を使用する場合、各 Unified CM クラスタを、より大きな組織の DNS ドメインの有効なサブドメインのメンバーとして定義し、各 Cisco MCS サーバ上に DNS ドメインを定義し、各 MCS サーバ上にプライマリおよびセカンダリの DNS サーバのアドレスを定義することを推奨します。

表 3-4 に、DNS サーバが Unified CM 環境で A レコード（ホスト名から IP アドレスへの解決）、Cname レコード（エイリアス）、および SRV レコード（冗長性とロード バランシング用のサービス レコード）を使用できる例を示します。

表 3-4　Unified CM における DNS の使用例

ホスト名	タイプ	TTL	データ
CUCM-Admin.cluster1.cisco.com	ホスト（A）	12 時間	182.10.10.1
CUCM1.cluster1.cisco.com	ホスト（A）	デフォルト	182.10.10.1
CUCM2.cluster1.cisco.com	ホスト（A）	デフォルト	182.10.10.2
CUCM3.cluster1.cisco.com	ホスト（A）	デフォルト	182.10.10.3
CUCM4.cluster1.cisco.com	ホスト（A）	デフォルト	182.10.10.4
TFTP-server1.cluster1.cisco.com	ホスト（A）	12 時間	182.10.10.11
TFTP-server2.cluster1.cisco.com	ホスト（A）	12 時間	182.10.10.12
www.CUCM-Admin.cisco.com	エイリアス（CNAME）	デフォルト	CUCM-Admin.cluster1.cisco.com
_sip._tcp.cluster1.cisco.com	サービス（SRV）	デフォルト	CUCM1.cluster1.cisco.com
_sip._tcp.cluster1.cisco.com	サービス（SRV）	デフォルト	CUCM2.cluster1.cisco.com
_sip._tcp.cluster1.cisco.com	サービス（SRV）	デフォルト	CUCM3.cluster1.cisco.com
_sip._tcp.cluster1.cisco.com	サービス（SRV）	デフォルト	CUCM4.cluster1.cisco.com

Dynamic Host Configuration Protocol（DHCP）

DHCP は、ネットワーク上のホストが、IP アドレス、サブネット マスク、デフォルト ゲートウェイ、および TFTP サーバ アドレスなどの初期設定情報を取得するために使用します。DHCP により、各ホストに IP アドレスやその他の設定情報を手動で設定する管理負担が軽減されます。また、DHCP により、デバイスをサブネット間で移動したときに、ネットワーク設定が自動的に再設定されます。設定情報はネットワーク内にある DHCP サーバから提供されます。このとき、DHCP サーバは、DHCP 対応のクライアントから送信される DHCP 要求に応答します。

これらのデバイスの配置を簡素化するには、DHCP を使用するように IP Communications エンドポイントを設定する必要があります。任意の RFC 2131 準拠 DHCP サーバを使用して、IP Communications ネットワーク デバイスに設定情報を提供できます。既存のデータ専用ネットワークに IP テレフォニー デバイスを配置する場合、作業としては、この新しい音声デバイスに対応する DHCP 音声スコープを既存の DHCP サーバに追加するだけで済みます。IP テレフォニー デバイスは、DHCP サーバを利用して IP 設定情報を取得するように設定されているため、DHCP サーバは冗長な方式で配置する必要があります。テレフォニー ネットワークには、2 つ以上の DHCP サーバを配置する必要があります。この配置により、いずれかのサーバに障害が発生しても、他のサーバが引き続き DHCP クライアント要求に応答できます。また、DHCP サーバに、ネットワーク内の DHCP に依存するクライアントすべてを処理するのに十分な IP サブネット アドレスが設定されていることを確認する必要があります。

DHCP オプション 150

IP テレフォニー エンドポイントでは、DHCP オプション 150 を利用することで、TFTP を実行するサーバから入手可能なテレフォニー設定情報の送信元を特定するように設定できます。

単一の TFTP サーバがすべての配置済みエンドポイントにサービスを提供するという最も単純な設定では、オプション 150 は、システムの指定 TFTP サーバを指す単一の IP アドレスとして配布されます。2 つの TFTP サーバが同じクラスタ内にある配置の場合、DHCP スコープは、オプション 150 で 2 つの IP アドレスを配布することもできます。プライマリ TFTP サーバにアクセスできなくなった場合、電話機は 2 つめのアドレスを使用します。その結果、冗長性が確保されます。TFTP サーバ間で冗長性とロード シェアリングの両方を実現するには、DHCP スコープの半分において 2 つの TFTP サーバ アドレスが逆の順序になるように、オプション 150 を設定します。

（注）　プライマリ TFTP サーバが使用可能でも、要求されたファイルを電話機に付与できない場合（たとえば、要求元の電話機がそのクラスタ上に設定されていない場合）、その電話機はセカンダリ TFTP サーバへのアクセスを試みません。

オプション 150 には直接 IP アドレスを使用する（つまり、DNS サービスを利用しない）ことを強く推奨します。これは、このように設定することで、電話機のブートアップおよび登録プロセス中に DNS サービスの可用性に依存しなくなるためです。

（注）　IP Phone はオプション 150 で最大 2 つの TFTP サーバをサポートしますが、Unified CM クラスタには 3 つ以上の TFTP サーバを設定できます。たとえば、Unified CM システムが 3 つの別々のサイトで WAN を介してクラスタリングされている場合は、3 つの TFTP サーバを（サイトごとに 1 つ）配置できます。次に、オプション 150 内にそのサイトの TFTP サーバを含む DHCP スコープを、各サイト内の電話機に付与できます。このように設定すると、TFTP サービスがエンドポイントに近くなるため、遅延が低減されるほか、サイト間で障害が分離される（1 つのサイトの障害が別のサイトの TFTP サービスに影響しない）ことが保証されます。

電源復帰後の電話機による DHCP オペレーション

電話機の電源が切断され、DHCP サーバがオフラインになっている間に復旧した場合、電話機は DHCP を使用して IP アドレス指定情報を取得しようとします（通常動作）。DHCP サーバからの応答がない場合、電話機は以前に受信した DHCP 情報を再利用して Unified CM に登録します。

DHCP のリース期間

DHCP のリース期間は、ネットワーク環境に応じて設定します。PC とテレフォニー デバイスが長期間にわたって同じ場所にある、ほとんど変化のないネットワークでは、DHCP のリース期間を長くする（たとえば、1 週間にする）ことを推奨します。リース期間を短くすると、DHCP 設定の更新頻度が高くなるため、ネットワーク上の DHCP トラフィック量が増加します。逆に、ラップトップやワイヤレス テレフォニー デバイスなどのモバイル デバイスを多数含むネットワークでは、DHCP のリース期間を短くして（たとえば、1 日間にして）、DHCP で管理するサブネット アドレスが枯渇することを防止する必要があります。モバイル デバイスは、一般に、IP アドレスを短期間使用し、その後は DHCP の更新や新しいアドレスを長期間要求しない場合があります。リース期間を長くすると、この IP アドレスは一定期間拘束されるため、使用されなくなった場合でも再割り当てされなくなります。

Cisco Unified IP Phone は、DHCP サーバのスコープ設定で指定された、DHCP のリース期間の条件に従います。DHCP サーバが最後に正常に応答してからリース期間の半分が経過すると、IP Phone はリースの更新を要求します。この DHCP クライアント要求が DHCP サーバによって応答されると、IP Phone は、次のリース期間にわたって IP スコープ（つまり、IP アドレス、デフォルト ゲートウェイ、サブネット マスク、DNS サーバ（オプション）、および TFTP サーバ（オプション））を継続使用できるようになります。DHCP サーバが使用不能になると、IP Phone はその DHCP リースを更新できません。さらに、リースが期限切れになるとすぐに、IP Phone はその IP 設定を開放するため、Unified CM から登録解除（アンレジスタ）されます。この状態は、DHCP サーバが別の有効なスコープを付与するまで継続されます。

集中型コール処理配置では、リモート サイトが中央の DHCP サーバを使用するように設定されている場合（Cisco IOS の IP ヘルパー アドレスなどの DHCP リレー エージェントを利用して）、および中央サイトへの接続が切断された場合、支店内の IP Phone はその DHCP スコープのリースを更新できなくなります。この場合、支店の IP Phone では、その DHCP のリースが期限切れになる危険性があります。その結果、その IP アドレスが使用できなくなり、サービスが中断されます。電話機はリース期間の半分が経過した時点でそのリースの更新を試みるという事実を考えると、DHCP サーバが到達不能になってからリース期間の半分が経過するとすぐに、DHCP のリースが期限切れになる可能性があり

ます。たとえば、DHCP スコープが 4 日間に設定されている場合、WAN の障害によって支店内の電話機が DHCP サーバを使用できなくなったときは、その電話機はリース期間の半分（この場合は 2 日間）が経過した時点でリースを更新できなくなります。IP Phone は、WAN に障害が発生してから最短で 2 日後に機能を停止する可能性があります。ただし、その時点までに WAN が復旧して、DHCP サーバが使用可能になった場合は除きます。WAN の接続障害が続くと、WAN に障害が発生してから遅くとも 4 日後には、すべての電話機の DHCP スコープが期限切れになります。

次のいずれかの方法によって、この状況を緩和できます。

- DHCP スコープのリース期間を長くする（たとえば、8 日間以上にします）

  この方法を使用すると、システム管理者は、少なくともリース期間の半分の時間を費やして、DHCP の到達不能に関するすべての問題に対処できます。また、リース期間が長ければ、リースの更新に関連するネットワーク トラフィックの頻度が減少します。

- 共存 DHCP サーバの機能を設定する（たとえば、支店の Cisco IOS ルータ上で DHCP サーバ機能を実行します）

  このアプローチは、WAN 接続の中断の影響を受けません。このアプローチを使用すると、IP アドレスの管理が分散されるため、各拠点で設定を更新する作業が発生します（詳細については、「DHCP のネットワーク配置」（P.3-26）を参照してください）。

（注）　「*共存*」という用語は、同じ物理的な場所にある複数のデバイスを指します。これらのデバイスの間に WAN または MAN 接続はありません。

DHCP のネットワーク配置

IP テレフォニー ネットワーク内に DHCP 機能を配置するためのオプションには、次の 2 つがあります。

- 中央の DHCP サーバ

  一般に、単一サイトのキャンパス IP テレフォニー配置の場合は、DHCP サーバをキャンパス内の中央ロケーションに設置する必要があります。前にも説明したように、冗長な DHCP サーバを配置する必要があります。集中型マルチサイト Unified CM 配置の場合と同様に、IP テレフォニー配置にもリモートの拠点テレフォニー サイトを含める場合は、中央サーバを使用して、リモート サイト内のデバイスに DHCP サービスを提供できます。このタイプの配置では、支店ルータのインターフェイス上で **ip helper-address** を設定する必要があります。冗長な DHCP サーバを中央サイトに配置する場合は、両方のサーバの IP アドレスを **ip helper-address** として設定する必要があることに留意してください。また、支店側のテレフォニー デバイスが中央の DHCP サーバを利用する場合、2 つのサイト間で WAN リンクに障害が発生すると、支店サイトのデバイスは、DHCP 要求を送信することも、DHCP 応答を受信することもできなくなります。

（注）　デフォルトでは、**service dhcp** は Cisco IOS デバイス上で有効になっていますが、設定には表示されません。このサービスを支店ルータ上で無効にしないでください。無効にすると、デバイス上で DHCP リレー エージェントが無効になり、**ip helper-address** コンフィギュレーション コマンドが動作しなくなります。

- 中央の DHCP サーバとリモート サイトの Cisco IOS DHCP サーバ

  集中型マルチサイト Unified CM 配置で使用する DHCP を設定する場合は、中央の DHCP サーバを使用して、中央にあるデバイスに DHCP サービスを提供できます。リモート デバイスは、ローカルに設置されたサーバから、またはリモート サイトにある Cisco IOS ルータから、DHCP サー

ビスを受信できます。このタイプの配置では、WAN に障害が発生しても、リモートのテレフォニー デバイスから DHCP サービスを使用できることが保証されます。例 3-1 は、Cisco IOS DHCP サーバの基本的なコンフィギュレーション コマンドを示しています。

例 3-1　Cisco IOS DHCP サーバのコンフィギュレーション コマンド

```
! Activate DHCP Service on the IOS Device

service dhcp

! Specify any IP Address or IP Address Range to be excluded from the DHCP pool

ip dhcp excluded-address <ip-address>|<ip-address-low> <ip-address-high>

! Specify the name of this specific DHCP pool, the subnet and mask for this
! pool, the default gateway and up to four TFTP

ip dhcp pool <dhcp-pool name>
   network <ip-subnet> <mask>
   default-router <default-gateway-ip>
   option 150 ip <tftp-server-ip-1> ...

! Note: IP phones use only the first two addresses supplied in the option 150
! field even if more than two are configured.
```

Unified CM DHCP サーバ（スタンドアロン サーバと共存サーバの比較）

ほとんどのネットワーク インフラストラクチャで、通常、DHCP サーバは専用のマシンで、そのネットワークで使用する DNS サービスと Windows Internet Naming Service（WINS）サービスを組み合せて実行します。場合によっては、クラスタに登録されているデバイスが 1000 以下の小規模な Unified CM の配置では、DHCP サーバを Unified CM サーバで実行して、これらのデバイスをサポートできます。ただし、Unified CM 上で実行する他の重要なサービスとの CPU 競合などの考えられるリソースの競合を回避するために、DHCP サーバの機能を専用サーバに移動することを推奨します。クラスタに 1000 を超えるデバイスが登録されている場合は、DHCP を Unified CM サーバでは*実行しない*で、専用のスタンドアロン サーバで実行する必要があります。

（注）　「*共存*」という用語は、同じサーバ上で複数のサービスまたはアプリケーションが実行されている状態を指します。

トリビアル ファイル転送プロトコル（TFTP）

Cisco Unified CM システムにおいて、IP Phone などのエンドポイントは、TFTP プロセスを利用して設定ファイル、ソフトウェア イメージ、およびその他のエンドポイント固有の情報を取得します。シスコの TFTP サービスは、1 つ以上の Unified CM サーバで実行できるファイル サービス システムです。このサービスは、設定ファイルを構築し、ファームウェア ファイル、リンガー ファイル、デバイス コンフィギュレーション ファイルなどをエンドポイントに提供します。

TFTP ファイル システムは、次のような複数のファイル タイプを保持できます。

- 電話機設定ファイル
- 電話機ファームウェア ファイル
- Certificate Trust List（CTL）ファイル
- Identity Trust List（ITL）ファイル

- トーン ローカリゼーション ファイル
- ユーザ インターフェイス（UI）ローカリゼーションおよび辞書ファイル
- リンガー ファイル
- ソフトキー ファイル
- SIP 電話機のダイヤル プラン ファイル

TFTP サーバは、変更できないタイプ（電話機のファームウェア ファイルなど）と変更できるタイプ（設定ファイルなど）の 2 つのタイプのファイルを管理し、提供します。

一般的な設定ファイルには、デバイス（SCCP または SIP 電話機など）の Unified CM の優先順位順に並べられたリスト、デバイスがこれらの Unified CM に接続する TCP ポート、および実行可能なロード識別子があります。選択したデバイスの設定ファイルには、メッセージのロケール情報と URL、ディレクトリ、サービス、および電話機の情報ボタンなどが含まれています。

デバイスの設定が変更されると、TFTP サーバは Unified CM データベースから関連する情報をプルして、設定ファイルを再構築します。その後、電話機をリセットすると、新しいファイルが電話機にダウンロードされます。たとえば、1 台の電話機の設定ファイルが変更された場合（エクステンション モビリティのログインまたはログアウト時など）、そのファイルだけが再構築されて、電話機にダウンロードされます。ただし、デバイス プールの設定の詳細が変更された場合（プライマリ Unified CM サーバが変更された場合など）、このデバイス プール内のすべてのデバイスに対して、設定ファイルを再構築し、ダウンロードする必要があります。多数のデバイスが含まれているデバイス プールでは、このファイル再構築プロセスがサーバのパフォーマンスに影響を及ぼす可能性があります。

（注） Cisco Unified CM 6.1 よりも前のリリースでは、TFTP サーバは、変更されたファイルを再構築するために、パブリッシャのデータベースから情報をプルしました。Unified CM 6.1 以降のリリースでは、TFTP サーバは、共存するサブスクライバ サーバ上のデータベースからローカル データベースの読み取りを実行できます。ローカル データベースの読み取りは、パブリッシャが使用できない場合にユーザ方向機能を保持するなどの利点を提供するだけではなく、WAN を介したクラスタリングを通じて、複数の TFTP サーバの分散を可能にします（WAN を介したクラスタリングと同じ遅延規則が、登録済み電話機を持つサーバに関して TFTP サーバに適用されます）。この設定により、TFTP サービスがエンドポイントに近くなるため、遅延が低減されるほか、サイト間で障害が分離されることが保証されます。

デバイスが TFTP サーバに設定ファイルを要求すると、TFTP サーバは、内部キャッシュ、ディスク、さらには代替 Cisco ファイル サーバ（指定されている場合）内の設定ファイルを検索します。TFTP サーバが設定ファイルを検出すると、デバイスにそのファイルを送信します。設定ファイルに Unified CM 名が含まれている場合、デバイスは DNS を使用して名前を解決し、Unified CM に接続できます。デバイスが IP アドレスまたは名前を受信しない場合、TFTP サーバの名前または IP アドレスを使用して登録接続を試行します。TFTP サーバが設定ファイルを検出できない場合、「ファイルが見つかりませんでした」というメッセージをデバイスに送信します。

TFTP サーバが設定ファイルを再構築している最中、または要求の最大数を処理している最中に設定ファイルを要求したデバイスは、後で設定ファイルを要求するようにデバイスに指示するメッセージを TFTP サーバから受信します。Maximum Serving Count サービス パラメータは、TFTP サーバが同時に処理できる要求の最大数を指定し、設定できます（デフォルト値 = 500 の要求）。同じサーバ上で、TFTP サービスが他の Cisco CallManager サービスと一緒に実行されている場合、デフォルト値を使用します。専用 TFTP サーバでは、Maximum Serving Count として、シングル プロセッサ システムの場合 1500、デュアル プロセッサ システムの場合 3000 の推奨値を使用します。

Cisco Unified IP Phone 8900 シリーズおよび 9900 シリーズは、TFTP よりも大幅に高速な HTTP プロトコル（ポート 6970）を使用して TFTP 設定ファイルを要求します。

TFTP 動作の例

エンドポイントをリブートするたびに、エンドポイントは（TFTP を介して）設定ファイルを要求します。設定ファイルの名前は要求するエンドポイントの MAC アドレスに基づいています（たとえば、MAC アドレスが ABCDEF123456 の Cisco Unified IP Phone 7961 の場合、ファイル名は SEPABCDEF123456.cnf.xml となります）。受信した設定ファイルには、電話機で実行するソフトウェアのバージョンと、電話機の登録に使用する Cisco Unified CM サーバのリストが格納されています。エンドポイントは、必要な設定情報を取得し、動作可能にするために TFTP を介して、リンガー ファイル、ソフトキー テンプレート、およびその他のファイルをダウンロードすることもできます。

設定ファイルに、電話機が現在使用しているバージョン番号と異なるバージョン番号のソフトウェア ファイルが含まれている場合、電話機は TFTP サーバから新しいソフトウェア ファイルもダウンロードして、アップグレードします。エンドポイントがソフトウェアをアップグレードするためにダウンロードする必要があるファイルの数は、エンドポイントのタイプと、電話機の現在のソフトウェアと新しいソフトウェアの差分によって異なります。たとえば、Cisco Unified IP Phones 7961、7970、および 7971 は、最悪のケースのソフトウェア アップグレードで 5 つのソフトウェア ファイルをダウンロードします。

TFTP ファイル転送時間

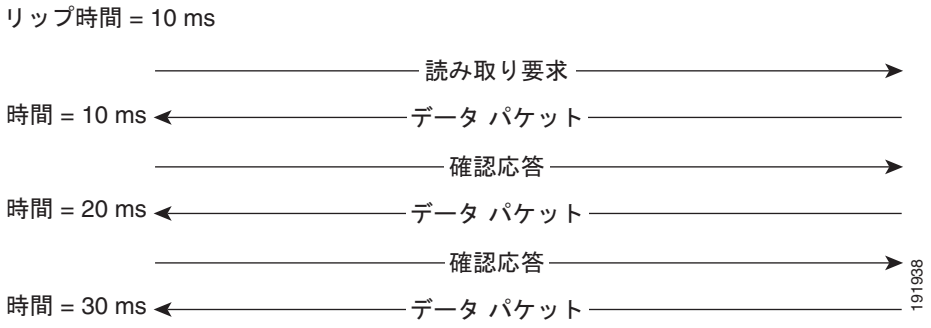
エンドポイントがファイルを要求するたびに、新しい TFTP 転送セッションが確立します。集中型コール処理配置の場合、これらの各転送が完了する時間は、エンドポイントを起動し、動作可能にするためにかかる時間と定期保守時にエンドポイントをアップグレードするためにかかる時間に影響を与えます。TFTP 転送時間は、これらの最終状態に影響を与える唯一の要因ではありませんが、重要なコンポーネントです。

TFTP を介して各ファイルの転送を完了する時間は、ファイル サイズ、再送信が必要な TFTP パケットの割合、およびネットワーク遅延またはラウンドトリップ時間の関数として予測可能です。

一目見ただけでは、ネットワーク帯域幅は前述のステートメントから欠落しているように見えますが、実際には再送信が必要な TFTP パケットの割合を介して含まれています。これは、ファイル転送をサポートするのに十分なネットワーク帯域幅がない場合、パケットはネットワーク インターフェイス キューイング アルゴリズムによってドロップされ、再送信する必要があるためです。

TFTP は User Datagram Protocol（UDP; ユーザ データグラム プロトコル）上で動作します。Transmission Control Protocol（TCP; 伝送制御プロトコル）とは異なり、UDP は信頼性の高いプロトコルではありません。つまり、UDP は本質的にパケット損失を検出する機能を備えていません。言うまでもなく、ファイル転送におけるパケット損失の検出は重要であるため、RFC 1350 は TFTP をロックステップ プロトコルとして規定しています。つまり、TFTP 送信側は 1 つのパケットを送信し、次のパケットを送信する前に応答を待ちます（図 3-8 を参照）。

図 3-8　TFTP パケット転送シーケンスの例

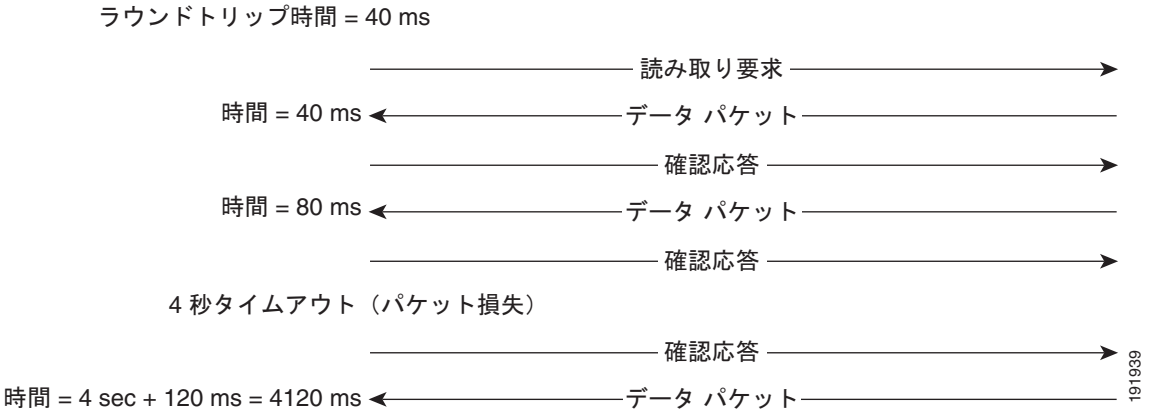


応答がタイムアウト時間（デフォルトでは 4 秒）内に受信されない場合、送信側はデータ パケットまたは確認応答を再送信します。5 回送信されても応答がない場合、TFTP セッションは失敗します。タイムアウト時間は常に同じであり、TCP タイムアウトのように適応できないので、パケット損失は、転送セッションを完了するのにかかる時間を大幅に増加させる可能性があります。

各データ パケット間の遅延は、最短でも、ネットワークのラウンドトリップ時間と同じなので、ネットワーク遅延は TFTP セッションで実現できる最大スループットの係数にもなります。

図 3-9 では、ラウンドトリップ時間が 40 ms に増加し、1 つのパケットが送信中に失われています。エラー率が 12% と高い率である一方、セッションを完了する時間が 30 ms（図 3-8 を参照）から 4160 ms（図 3-9 を参照）に増加しているので、TFTP の遅延とパケット損失の効果が簡単にわかります。

図 3-9　TFTP セッション完了時間におけるパケット損失の効果



次の公式を使用して、TFTP ファイル転送が完了するのにかかる時間を計算します。

FileTransferTime = FileSize * [(RTT + ERR * Timeout) / 512000]

定義：

FileTransferTime は秒単位です。

FileSize はバイト単位です。

RTT はラウンドトリップ時間（ミリ秒単位）です。

ERR はエラー率または失われたパケットの比率です。

Timeout はミリ秒単位です。

512000 =（TFTP パケット サイズ）*（1000 ミリ秒/秒）=
（512 バイト）*（1000 ミリ秒/秒）

表 3-5 と表 3-6 は、この公式を使用して、各種エンドポイント デバイス タイプ、プロトコル、およびネットワーク遅延用のソフトウェア ファイルの転送時間を計算した例を示しています。

表 3-5　SCCP デバイスの TFTP ファイル転送時間

デバイス タイプ（Cisco Unified IP Phone）	ファームウェア サイズ（バイト、100,000 未満の値は切り上げ）	転送完了時間（エラー率 1%）				
		RTT 40 ms	RTT 80 ms	RTT 120 ms	RTT 160 ms	RTT 200 ms
7985	15,000,000	39 分 3 秒	58 分 35 秒	78 分 7 秒	97 分 39 秒	117 分 11 秒
7921	9,700,000	25 分 15 秒	37 分 53 秒	50 分 31 秒	63 分 9 秒	75 分 46 秒
7975	6,300,000	16 分 24 秒	24 分 36 秒	32 分 48 秒	41 分 0 秒	49 分 13 秒
7970 または 7971	6,300,000	16 分 24 秒	24 分 36 秒	32 分 48 秒	41 分 0 秒	49 分 13 秒
7965 または 7945	6,300,000	16 分 24 秒	24 分 36 秒	32 分 48 秒	41 分 0 秒	49 分 13 秒
7962 または 7942	6,200,000	16 分 8 秒	24 分 13 秒	32 分 17 秒	40 分 21 秒	48 分 26 秒
7941 または 7961	6,100,000	15 分 53 秒	23 分 49 秒	31 分 46 秒	39 分 42 秒	47 分 39 秒
7931	6,100,000	15 分 53 秒	23 分 49 秒	31 分 46 秒	39 分 42 秒	47 分 39 秒
7911 または 7906	6,100,000	15 分 53 秒	23 分 49 秒	31 分 46 秒	39 分 42 秒	47 分 39 秒
7935	2,100,000	5 分 28 秒	8 分 12 秒	10 分 56 秒	13 分 40 秒	16 分 24 秒
7920	1,200,000	3 分 7 秒	4 分 41 秒	6 分 15 秒	7 分 48 秒	9 分 22 秒
7936	1,800,000	4 分 41 秒	7 分 1 秒	9 分 22 秒	11 分 43 秒	14 分 3 秒
7940 または 7960	900,000	2 分 20 秒	3 分 30 秒	4 分 41 秒	5 分 51 秒	7 分 1 秒
7910	400,000	1 分 2 秒	1 分 33 秒	2 分 5 秒	2 分 36 秒	3 分 7 秒
7912	400,000	1 分 2 秒	1 分 33 秒	2 分 5 秒	2 分 36 秒	3 分 7 秒
7905	400,000	1 分 2 秒	1 分 33 秒	2 分 5 秒	2 分 36 秒	3 分 7 秒
7902	400,000	1 分 2 秒	1 分 33 秒	2 分 5 秒	2 分 36 秒	3 分 7 秒

表 3-6　SIP デバイスの TFTP ファイル転送時間

デバイス タイプ（Cisco Unified IP Phone）	ファームウェア サイズ（バイト、100,000 未満の値は切り上げ）	転送完了時間（エラー率 1%）				
		RTT 40 ms	RTT 80 ms	RTT 120 ms	RTT 160 ms	RTT 200 ms
7975	6,600,000	17 分 11 秒	25 分 46 秒	34 分 22 秒	42 分 58 秒	51 分 33 秒
7970 または 7971	6,700,000	17 分 26 秒	26 分 10 秒	34 分 53 秒	43 分 37 秒	52 分 20 秒
7965 または 7945	6,600,000	17 分 11 秒	25 分 46 秒	34 分 22 秒	42 分 58 秒	51 分 33 秒
7962 または 7942	6,500,000	16 分 55 秒	25 分 23 秒	33 分 51 秒	42 分 19 秒	50 分 46 秒
7941 または 7961	6,500,000	16 分 55 秒	25 分 23 秒	33 分 51 秒	42 分 19 秒	50 分 46 秒
7911 または 7906	6,400,000	16 分 40 秒	25 分 0 秒	33 分 20 秒	41 分 40 秒	50 分 0 秒
7940 または 7960	900,000	2 分 20 秒	3 分 30 秒	4 分 41 秒	5 分 51 秒	7 分 1 秒
7912	400,000	1 分 2 秒	1 分 33 秒	2 分 5 秒	2 分 36 秒	3 分 7 秒
7905	400,000	1 分 2 秒	1 分 33 秒	2 分 5 秒	2 分 36 秒	3 分 7 秒

表 3-5 と表 3-6 の値は、必要なファームウェア ファイルを電話機にダウンロードするおおよその時間です。これは、電話機を新しいファームウェアにアップグレードし、動作可能になるまでにかかる時間の推定値では*ありません*。

Cisco Unified IP Phone ファームウェア リリース 7.*x* には、新しいファイルのダウンロード時に 10 分のタイムアウトが用意されています。この時間内に転送が完了しない場合、後で転送が正常に完了する場合であっても、電話機はダウンロードを破棄します。この問題が発生した場合は、ローカルの TFTP サーバを使用して、電話機を 8.*x* ファームウェア リリースにアップグレードすることを推奨します。このリリースには、61 分のタイムアウト値が用意されています。

ネットワーク遅延とパケット損失は TFTP 転送時間に上記のような影響を与えるので、ローカルの TFTP サーバは便利です。このローカルの TFTP サーバは、WAN を介したクラスタを使用する配置における Unified CM サブスクライバか、または Cisco サービス統合型ルータ（ISR）などで実行する代替のローカル TFTP Load Server です。最新のエンドポイント（より大きなファームウェア ファイルを必要とする）は、Load Server アドレスを使用して設定できます。これにより、エンドポイントは、中央の TFTP サーバから比較的小さい設定ファイルをダウンロードする一方で、ローカルの TFTP サーバ（Unified CM クラスタの一部ではない）を使用してより大きなソフトウェア ファイルをダウンロードできます。代替のローカル TFTP Load Server をサポートしている Cisco IP Phone の詳細については、「エンドポイント機能の要約」（P.18-53）を参照してください。

（注）　起動時に各電話機で実行される正確な処理と、ダウンロードされるファイルのサイズは、電話機のモデル、電話機に設定されているシグナリング タイプ（SCCP、MGCP、または SIP）、および電話機の以前の状態によって異なります。要求されるファイルは異なりますが、各電話機で実行される一般的なプロセスは同じで、すべての場合で TFTP を使用して適切なファイルが要求され、配送されます。TFTP サーバの配置に関する一般的な推奨事項が、プロトコルや配置する電話機モデルによって変わることはありません。

TFTP サーバの冗長性

オプション 150 を使用すると、最大 2 つの IP アドレスを DHCP スコープの一部として電話機に配布できます。電話機はリスト内の最初のアドレスを試行し、最初の TFTP サーバとの通信を確立できなければ、その次のアドレスを試行します。このアドレス リストには冗長性メカニズムがあるため、電話機は、そのプライマリ TFTP サーバに障害が発生しても、別のサーバから TFTP サービスを取得できます。

TFTP のロード シェアリング

TFTP サーバの順序が異なるリストを別のサブネットに付与して、ロード バランシングを実現することを推奨します。次の例を参考にしてください。

- サブネット 10.1.1.0/24：オプション 150：TFTP1_Primary、TFTP1_Secondary
- サブネット 10.1.2.0/24：オプション 150：TFTP1_Secondary、TFTP1_Primary

通常の動作では、10.1.1.0/24 の電話機は TFTP1_Primary に TFTP サービスを要求し、サブネット 10.1.2.0/24 の電話機は TFTP1_Secondary に TFTP サービスを要求します。TFTP1_Primary に障害が発生した場合、両方のサブネットからの電話機が TFTP1_Secondary に TFTP サービスを要求します。

ロード バランシングは、単一の TFTP サーバがホットスポットになること、つまり、複数のクラスタの電話機すべてが同じサーバを利用してサービスを取得しようとすることを回避します。TFTP ロード バランシングは、Unified CM のアップグレード時など、電話機のソフトウェア ロードが転送される場合に特に重要です。これは、転送されるファイルのサイズと数が増えることで、TFTP サーバにかかる負荷が大きくなるためです。

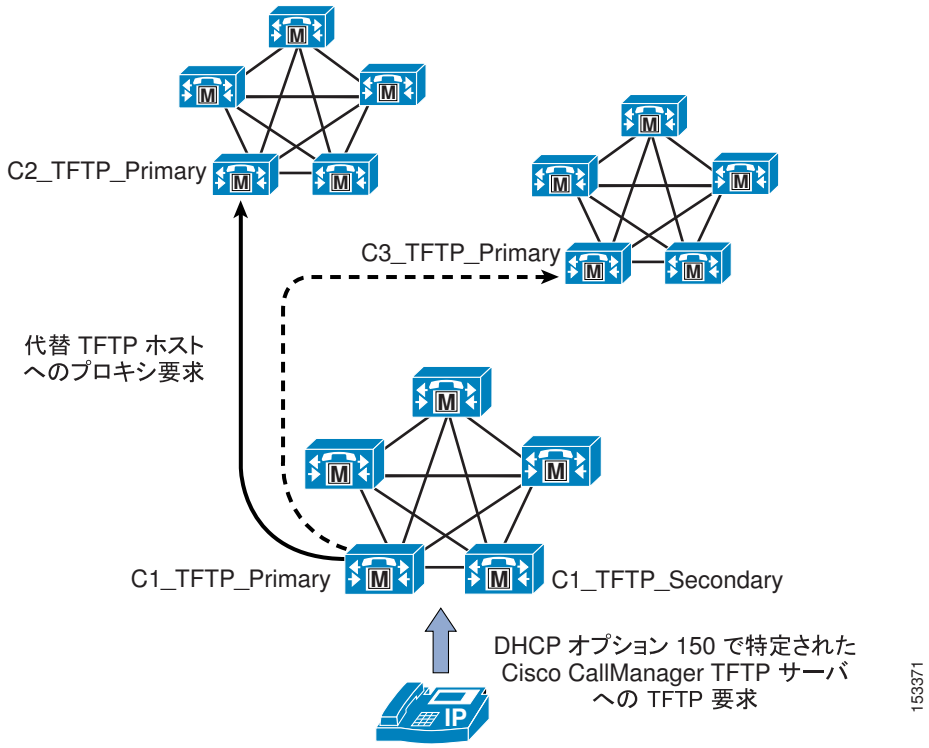
中央集中型 TFTP サービス

マルチクラスタ システムでは、単一のサブネットまたは VLAN に複数のクラスタの電話機を含めることができます。この場合、サブネットまたは VLAN 内のすべての電話機に提供されるアドレスの TFTP サーバは、電話機が属するクラスタに関係なく、各電話機から送信されるファイル転送要求に応答する必要があります。中央集中型 TFTP 配置では、1 つのクラスタに関連付けられている TFTP サーバのセットが、マルチクラスタ システムのすべての電話機に TFTP サービスを提供する必要があります。

このファイル アクセスの単一ポイントを提供するために、各クラスタの TFTP サーバは、中央のプロキシ TFTP サーバ経由でファイルを提供できる必要があります。Cisco Unified CM 5.0 では、中央の TFTP サーバに各クラスタの TFTP サーバをポイントするリダイレクト ロケーションのセットを設定することによって、このプロキシ設定を行います。この設定では、他のクラスタごとに 1 つずつ、中央の TFTP サーバの代替ファイル ロケーションの HOST リダイレクト ステートメントを使用します。中央集中型クラスタの各冗長 TFTP サーバは、各子クラスタの冗長サーバの 1 つをポイントする必要があります。中央集中型サーバが子クラスタの両方の冗長サーバをポイントする必要はありません。各クラスタ内でのファイルの再配布および中央クラスタの冗長サーバ間での電話機のフェールオーバー メカニズムには、高い耐障害性があるからです。

図 3-10 に、このプロセスの動作例を示します。Cluster 3 に登録されている電話機からの要求は、Cluster 1 で設定されている中央集中型 TFTP サーバ（C1_TFTP_Primary）に転送されます。このサーバは、次に、電話機が要求したファイルのコピーによる最初の応答があるまで、設定済みの代替 TFTP サーバのそれぞれに対して照会します。中央集中型セカンダリ TFTP サーバ（C1_TFTP_Secondary）への要求は、要求されたファイルが見つかるか、すべてのサーバから要求されたファイルが存在しないという応答があるまで、プロキシによって別のクラスタのセカンダリ TFTP サーバに送信されます。

図 3-10　　中央集中型 TFTP サーバ



リリースの異なる Unified CM を実行するサーバが含まれる混在環境の中央集中型 TFTP

以前の Unified CM リリースから Unified CM 5.0 以降のリリースに移行するときに、大規模な中央集中型 TFTP 環境では、混合モードでの運用が必要になることがよくあります。Unified CM 5.0 以前では、中央集中型 TFTP サーバは子サーバにファイルを要求せず、すべての子クラスタの TFTP ディレクトリをリモートで中央サーバにマウントし、すべてのローカル ディレクトリとリモート ディレクトリで要求されたファイルを検索していました。移行期間中は、両方のモード（Unified CM 5.0 以前で使用する *リモート マウント*と、Unified CM 5.0 以降のリリースで使用する *プロキシ要求*の混合モード）で動作できる中央集中型 TFTP サーバを提供する必要があります。Unified CM 5.0 以降のリリースに対応するサーバは、混在環境でのファイル システムのリモート マウントをサポートしないため、Cisco Unified CM 4.1(3)SR3a 以降の Windows OS ベースの Unified CM リリースを混合モードの中央集中型 TFTP クラスタとして配置する必要があります。

（注）　Cisco Unified CM Release 4.1(3)SR3a（およびそれ以降の Windows OS プラットフォーム対応の Unified CM リリース）には、混合モードの中央集中型 TFTP 設計をサポートする cTFTP サーバ デーモンへのアップグレードが含まれています。これらのリリースでは、中央集中型 TFTP サーバがリモート マウントとプロキシ要求の両方を、他のクラスタ内の代替 TFTP ファイル サーバに到達する方法としてサポートします。

混合モードの TFTP サーバを設定する場合、HOST プロキシ要求によって Unified CM 5.0 以降のリリースに対応するサーバを指定し、リモート マウント設定プロセスを使用して Unified CM 4.1(3)SR3a 以前の任意のサーバを指定する必要があります。例 3-2 を参照してください（リモート マウント設定の詳細については、次を参照してください）。混合モードをサポートする任意の子クラスタは、リモート マウントとプロキシ クラスタのどちらにも設定できます。

中央集中型 TFTP 設定では、メイン TFTP サーバは、最高のバージョンの Cisco Unified Communications Manager を実行するクラスタ内に存在する必要があります。たとえば、互換性がある Cisco Unified CM 4.*x*（混合モード）クラスタと Unified CM 7.0 クラスタ間で中央集中型 TFTP サーバを使用している場合、中央 TFTP サーバは Cisco Unified CM 7.0 クラスタ内に存在する必要があります。

中央集中型 TFTP サーバが低いバージョンの Cisco Unified Communications Manager を実行するクラスタ内に存在する場合、すべての電話機が、この中央集中型 TFTP サーバから提供されるロケール ファイルを使用します。これらの古いロケール ファイルには、新しくローカライズされた語句がメイン クラスタの TFTP サーバから提供されるロケール ファイルに含まれていないため、高いバージョンの Cisco Unified CM を実行するクラスタに登録された電話機の表示問題を引き起こす可能性があります。

例 3-2　混合モードの TFTP の設定

Unified CM TFTP サーバの [Service Parameters] > [TFTP Server] > [Cisco TFTP (Active) Parameters] で、次のように設定します。

- Parameter Name = パラメータ値
- Alternate Cisco File Server = HOST://10.10.10.1
- Alternate Cisco File Server = C:¥Program Files¥Cisco¥TFTPpath¥TFTP2

リモート マウントの代替 Cisco ファイル サーバ設定の詳細については、次の Web サイトで入手可能な『*Cisco Unified Communications SRND Based on Cisco Unified CallManager 4.x*』を参照してください。

http://www.cisco.com/go/ucsrnd

ネットワーク タイム プロトコル（NTP）

NTP を使用すると、ネットワーク デバイスは、そのクロックをネットワーク タイム サーバまたはネットワーク対応のクロックと同期させることができます。NTP は、ネットワーク内のすべてのデバイスが同じ時刻に設定されていることを保証するうえで重要です。テレフォニー ネットワークのトラブルシューティングまたは管理を行う場合は、ネットワーク全体でデバイス上にあるすべてのエラー ログ、セキュリティ ログ、トレース、およびシステム レポート内のタイムスタンプを同期させることが極めて重要です。この同期により、管理者は、ネットワークのアクティビティと動作を、共通の時系列に基づいて再現できます。課金記録とコール詳細レコード（CDR）でも、正確な同期時刻が必要になります。

Unified CM の NTP 時刻同期

時刻同期は、Unified CM サーバにおいて特に重要です。CDR レコードが正確で、ログ ファイルの同期が取れていることを保証するだけではなく、クラスタ内で将来的に IPSec 機能を有効にしたり、外部エンティティと通信したりするには、正確な時刻源が必要です。

Unified CM は、クラスタ内のすべてのサブスクライバの NTP 時刻を自動的にパブリッシャと同期します。インストール時に、各サブスクライバは自動的に、パブリッシャで実行されている NTP サーバをポイントするように設定されます。パブリッシャはマスター サーバと見なされ、外部サーバと同期するように設定されている場合を除き、内部ハードウェア クロックを基にクラスタに時刻を提供します。クラスタの時刻と外部時刻源を確実に同期させるために、パブリッシャは Stratum-1、Stratum-2、または Stratum-3 NTP サーバをポイントするように設定することを強く推奨します。

Unified CM を Cisco IOS または Linux ベースの NTP サーバと同期させることを推奨します。Windows Time Services を NTP サーバとして使用することは推奨できず、サポート対象にもなっていません。Windows Time Services は、多くの場合、Simple Network Time Protocol（SNTP; 簡易ネットワーク タイム プロトコル）を使用していますが、Linux ベースの CM は SNTP とは正常に同期できないためです。

互換性、精度、およびネットワーク ジッタの問題を回避するために、プライマリ ノードに指定する外部 NTP サーバは、NTP v4（バージョン 4）にしてください。IPv6 アドレッシングを使用している場合は、外部 NTP サーバは、NTP v4 *でなければなりません*。

（注）　NTP.conf ファイルの手動設定はできなくなりました。このファイルに対して行った変更は、自動的にシステム設定で置き換えられます。

Cisco Unified Communications 環境における NTP 時刻同期に関する追加情報については、次の Web サイトで入手可能なホワイト ペーパー『*Cisco IP Telephony Clock Synchronization: Best Practices*』を参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_white_paper0900aecd8037fdb5.shtml

Cisco IOS と CatOS の NTP 時刻同期

時刻同期は、ネットワーク内の他のデバイスにも重要です。Cisco IOS ルータと Catalyst スイッチは、NTP を介してそれぞれの時刻をその他のネットワーク デバイスと同期させるように設定する必要があります。この設定は、デバッグ メッセージ、syslog メッセージ、およびコンソール ログ メッセージにタイムスタンプが適切に付加されることを保証するうえで重要です。ネットワーク全体でデバイスに発生するイベントの明確な時間記録が得られれば、テレフォニー ネットワークの問題に関するトラブルシューティングが簡素化されます。

例 3-3 は、Cisco IOS および CatOS デバイスに対する NTP 時刻同期の設定を示しています。

例 3-3　　Cisco IOS と CatOS の NTP 設定

Cisco IOS の設定：

```
ntp server 64.100.21.254
```

CatOS の設定：

```
set ntp server 64.100.21.254
set ntp client enable
```

ルータとスイッチの NTP 時刻同期が適切に行われるよう保証するには、**clock timezone** コマンド（Cisco IOS の場合）、**set timezone** コマンド（CatOS の場合）、またはその両方を使用して、時間帯を設定することが必要になる場合があります。

WAN インフラストラクチャ

統合されたネットワーク上で Unified Communications を正常に動作させるには、WAN インフラストラクチャを適切に設計することも極めて重要です。インフラストラクチャを適切に設計するには、基本的な設定と設計に関するベスト プラクティスに従って、できるだけ可用性の高い、スループットを保証できる WAN を配置する必要があります。さらに、WAN インフラストラクチャを適切に設計するには、すべての WAN リンク上にエンドツーエンド QoS を配置する必要もあります。次の項では、これらの要件について説明します。

- 「WAN の設計と設定」（P.3-36）
- 「WAN の QoS」（P.3-40）
- 「リソース予約プロトコル（RSVP）」（P.11-18）
- 「帯域幅のプロビジョニング」（P.3-47）

WAN の設計と設定

WAN を適切に設計するには、耐障害性のあるネットワーク リンクを構築し、このリンクが使用不能になる可能性を考える必要があります。耐障害性のある冗長なネットワークを構築するには、慎重に WAN トポロジを選択し、必要な帯域幅をプロビジョニングし、ネットワーク トポロジ内の別のレイヤと同じように WAN インフラストラクチャにアプローチします。次の項では、必要なインフラストラクチャのレイヤとネットワーク サービスについて説明します。

- 「配置上の考慮事項」（P.3-36）
- 「保証帯域幅」（P.3-38）
- 「ベストエフォート型の帯域幅」（P.3-39）

配置上の考慮事項

音声ネットワークの WAN 配置では、ハブアンドスポーク、フル メッシュ構造、または部分メッシュ構造のトポロジを使用できます。ハブアンドスポーク トポロジは、1 つの中央ハブ サイトと、中央ハブ サイトに接続された複数のリモート スポーク サイトで構成されます。このシナリオでは、各リモート（スポーク）サイトは、中央（ハブ）サイトから 1 WAN リンク ホップ離れており、他のすべてのスポーク サイトから 2 WAN リンク ホップ離れています。メッシュ構造のトポロジには複数の WAN リンクが含まれ、サイト間のホップ数は任意です。このシナリオでは、同じサイトに対して複数の異なるパ

スがあり、別のサイトと異なるリンクで通信が行われるサイトがあります。最も単純な例として、他の 2 つのサイトとの WAN リンクを持つ 3 つのサイトが三角形を形成している例があります。この場合、あるサイトから別のサイトへのパスは 2 つあります。

トポロジ非対応コール アドミッション制御を行うには、WAN をハブアンドスポークにするか、MPLS VPN の場合はスポークレス ハブにする必要があります。このトポロジにすると、Unified CM のロケーションまたはゲートキーパーによって提供されるコール アドミッション制御によって、WAN にある任意の 2 つのサイト間で使用可能な帯域幅が正常にトラッキングされます。また、WAN リンクを介して複数のハブアンドスポーク配置を相互接続することもできます。

トポロジ対応コール アドミッション制御は、ハブアンドスポークと任意の WAN トポロジの両方で使用できます。このコール アドミッション制御の形式には、リソース予約プロトコル（RSVP）をサポートする WAN インフラストラクチャの部分が必要です。詳細については、「リソース予約プロトコル（RSVP）」（P.11-18）および「コール アドミッション制御」（P.11-1）を参照してください。

集中型および分散型マルチサイト配置モデルや、これらの配置モデルに対する Multiprotocol Label Switching（MPLS）の影響に関する詳細については、「Unified Communications の配置モデル」（P.5-1）の章を参照してください。

可能であれば、WAN リンクを冗長にして、より高いレベルの耐障害性を実現する必要があります。冗長な WAN リンクを、別のサービス プロバイダーから入手するか、またはネットワーク内の物理的に異なる入力/出力点に配置すると、単一のリンクに障害が発生してもバックアップの帯域幅および接続性を利用できることが保証されます。障害のないシナリオでは、この冗長リンクを使用して、追加の帯域幅を利用し、WAN 内の複数のパスと機器を介してフローごとにトラフィックのロード バランシングを行うことができます。トポロジ非対応コール アドミッション制御では、サイト間で使用できる帯域幅を減少させる障害が発生した場合に、コール アドミッション制御メカニズムがこれらの障害または帯域幅の減少の影響を受けないように、通常、冗長パスを多めにプロビジョニングし、少なめにサブスクライブする必要があります。トポロジ対応コール アドミッション制御では、トポロジの変更の多くを動的に調整でき、使用可能な合計帯域幅を効率的に使用できます。

音声とデータは、LAN で収束される場合とまったく同じように、WAN でも収束される必要があります。QoS プロビジョニングおよびキューイング メカニズムは、一般に、WAN 環境において音声とデータを同じ WAN リンク上で相互運用できることを保証するために使用されます。音声とデータを分離して別々のリンク上で転送すると、多くの場合において問題になることがあります。これは、1 つのリンクで障害が発生すると、一般に、すべてのトラフィックが単一リンクに集中するためです。その結果、トラフィックの各タイプでスループットが減少し、ほとんどの場合において音声品質が低下します。さらに、ネットワーク リンクまたはデバイスを別々に保守すると、最善を尽くしても、トラブルシューティングや管理が困難になります。

WAN リンクでは、障害が発生する可能性や、オーバーサブスクリプションになる可能性があるため、WAN のもう一方の側にあるサイトには、必要に応じて非集中型のリソースを配置することを推奨します。特に、メディア リソース、DHCP サーバ、および音声ゲートウェイのほか、Survivable Remote Site Telephony（SRST）や Cisco Unified Communications Manager Express（Unified CME）などのコール処理アプリケーションは、適宜、サイトの規模やそのサイトにおけるこれらの機能の重要性に応じて、中央以外のサイトに配置される必要があります。音声アプリケーションおよびデバイスを非集中化すると、ネットワーク配置がより複雑になり、企業全体でこれらのリソースを管理する作業もより複雑になり、さらにネットワーク ソリューションの総コストが増加する可能性があることに留意してください。ただし、WAN リンク障害の発生中にリソースが使用可能になるという事実により、これらの要因は軽減される場合もあります。

WAN 環境に音声を配置する場合は、WAN リンクを通過するすべての音声コールに対して低帯域幅の G.729 コーデックを使用することを推奨します。これは、この方法によって、このような低速リンク上で帯域幅が節約されるためです。さらに、MoH などのメディア リソースは、可能であればマルチキャスト トランスポート メカニズムを使用するように設定される必要があります。これは、この方法によって、さらに帯域幅が節約されるためです。

音声に対する QoS 保証のないベストエフォート ネットワークを介してコールが行われる場合は、Internet Low Bit Rate Codec（iLBC）を使用することを検討してください。これにより、フレームが失われる可能性のあるネットワークで、品位のある音声品質の低下と適切なエラー復元特性が可能になります。コーデック タイプとサンプル サイズに基づく帯域幅使用量の詳細については、表 3-9 を参照してください。

IP 音声ネットワークの遅延

International Telecommunication Union（ITU; 国際電気通信連合）の G.114 勧告には、音声ネットワークにおける片方向の遅延は 150 ミリ秒以下でなければならないと明記されています。ネットワーク内に低速 WAN リンクを実装する場合は、この要件に留意することが重要です。片方向の遅延がこの 150 ミリ秒の勧告を超えないように、WAN リンクのトポロジ、テクノロジー、および物理的な距離を考慮する必要があります。片方向の遅延が 150 ミリ秒を超える VoIP ネットワークの実装は、音声コールの品質だけでなく、コールのセットアップ時間およびメディアのカットスルー時間にかかわる問題ももたらします。これは、コールを確立するために、各デバイスとコール処理アプリケーション間で複数のコール シグナリング メッセージを交換する必要があるためです。

保証帯域幅

音声は、一般に、重要なネットワーク アプリケーションと見なされるため、ベアラおよびシグナリング音声トラフィックが常にその宛先に到達することが不可欠となります。このため、専用の保証帯域幅を提供できる WAN トポロジおよびリンク タイプを選択することが重要です。次に示す WAN リンク テクノロジーは、専用の保証帯域幅を提供できます。

- 専用回線
- フレーム リレー
- 非同期転送モード（ATM）
- ATM/フレームリレーのサービス インターワーキング
- Multiprotocol Label Switching（MPLS）
- Cisco 音声およびビデオ対応 IP Security VPN（IPSec V3PN）

これらのリンク テクノロジーは、専用の方式で配置されているか、またはプライベート ネットワークに配置されている場合に、保証トラフィック スループットを提供できます。これらの WAN リンク テクノロジーはいずれも、特定の速度または帯域幅サイズでプロビジョニングできます。また、これらのリンク テクノロジーには、低リンク速度でもネットワーク トラフィックのスループットを保証できる組み込みメカニズムがあります。トラフィック シェーピング、フラグメンテーションとパケット インターリーブ、および Committed Information Rate（CIR; 認定情報レート）などの機能を使用すると、WAN においてパケットがドロップされないこと、すべてのパケットが定期的に WAN リンクにアクセスできること、およびこれらのリンクを通過しようとするすべてのネットワーク トラフィックが十分な帯域幅を使用できることを保証できます。

Dynamic Multipoint VPN（DMVPN）

スポークツースポーク DMVPN ネットワークは、ハブアンドスポーク トポロジと比較して、Cisco Unified Communications に対する利点を提供できます。スポークツースポーク トンネルは、WAN のホップ数と復号化/暗号化段階を削減することで、エンドツーエンドの遅延の低減をもたらします。また、DMVPN は、関連した管理および操作上のオーバーヘッドなしで、ポイントツーポイント トンネルのフル メッシュと同等の簡素化された設定方法を提供します。スポークツースポーク トンネルの使用はハブのトラフィックも削減し、その結果、帯域幅とルータ処理キャパシティを節約できます。ただし、スポークツースポーク DMVPN ネットワークは、スポークハブスポーク パスからスポークツースポーク パスへの RTP パケット ルーティングの転送時に発生する遅延変動（ジッタ）の影響を受けやす

くなっています。この DMVPN パス転送時の遅延における変動は、コールの非常に早い段階で発生し、通常は気が付きません。ただし、遅延の差が 100 ms を超える場合、単一の瞬間的なオーディオのひずみが聞こえる場合があります。

集中型コール処理を使用するマルチサイト DMVPN WAN の配置に関する詳細については、『*Cisco Unified Communications Voice over Spoke-to-Spoke DMVPN Test Results and Recommendations*』を参照してください。このドキュメントは、http://www.cisco.com/go/designzone で入手可能です。

ベストエフォート型の帯域幅

WAN トポロジの中には、専用の保証帯域幅を提供できないために、ネットワーク トラフィックが重要な場合であってもそのトラフィックが宛先に到達することを保証できないものがあります。このようなトポロジでは、音声トラフィックに重大な問題が発生する場合があります。その理由は、保証ネットワーク スループットをプロビジョニングするメカニズムがないためだけでなく、トラフィック シェーピング、パケット フラグメンテーションとインターリーブ、キューイング メカニズム、またはエンドツーエンド QoS を備えていないために、音声などの重要なトラフィックが優先的に処理されることを保証できないためです。

次に示す WAN ネットワーク テクノロジーおよびリンク タイプは、このようなベストエフォート型の帯域幅テクノロジーの例です。

- インターネット
- DSL
- ケーブル
- 衛星
- 無線

ほとんどの場合、これらのリンク タイプはいずれも、重要な音声および音声アプリケーションに必要となる、保証されたネットワーク接続性および帯域幅を提供できません。ただし、これらのテクノロジーは、個人用または在宅勤務者用のネットワーク配置に適している場合があります。これらのトポロジは、可用性の高いネットワーク接続性と、十分なネットワーク スループットを提供できる一方で、長期間にわたって使用不能になる場合や、速度が抑制されるために音声などのリアルタイム アプリケーションでネットワーク スループットが不足する場合、あるいは大量のパケット損失を引き起こすために繰り返し再送信することが必要になる場合があります。言い換えると、これらのリンクとトポロジは、保証帯域幅を提供できません。また、トラフィックをこれらのリンク上で送信する場合は、ベストエフォートで送信されるため、その宛先に到達することが保証されません。このため、企業クラスの音声サービスおよび品質が要求される音声対応のネットワークには、ベストエフォート型の WAN トポロジを*使用しない*ことを推奨します。

（注） DSL およびケーブル テクノロジーの新しい QoS メカニズムの中には、保証帯域幅を提供できるものがあります。ただし、これらのメカニズムは、多くのサービス プロバイダーによって一般的に配置されているものではありません。一般にベストエフォートに基づくネットワークで QoS 保証を提供するサービスの場合、サービス プロバイダーの Service Level Agreement（SLA; サービス レベル契約）で提供される帯域幅および QoS 保証を確認して理解することが重要です。

（注） アップストリームおよびダウンストリームの QoS メカニズムが、ワイヤレス ネットワークにおいてサポートされるようになりました。Voice over Wireless LAN の QoS の詳細については、http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns820/landing_voice_wireless.html で入手可能な『*Voice over Wireless LAN Design Guide*』を参照してください。

WAN の QoS

ネットワークに音声およびビデオのトラフィックを送る場合は、事前に、必要なすべてのアプリケーションに十分な帯域幅があることを確認することが重要です。この帯域幅をプロビジョニングしたら、すべてのインターフェイス上で音声プライオリティ キューイングを実行する必要があります。トラフィックのバーストがバッファをオーバーサブスクリプションにする場合、ジッタとパケット損失を削減するには、このキューイングが必要です。このキューイング要件は、LAN インフラストラクチャの要件とほぼ同じです。

次に、WAN では、一般に、トラフィック シェーピングなどの追加メカニズムを使用して、WAN リンク上で処理能力を超えるトラフィックが送信されないことを保証する必要があります。処理能力を超えるトラフィックが送信されると、パケットがドロップされる場合があります。

最後に、リンク効率化技術を WAN パスに適用できます。たとえば、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）を使用すると、小さな音声パケットが大きなデータ パケットの後に続いてキューに入ることを防止できます。このようにキューに入ると、低速リンク上で許容できない遅延が発生することがあります。

これらの QoS メカニズムの目標は、音声トラフィックの遅延、パケット損失、およびジッタを削減することで、信頼性の高い、高品質の音声を保証することです。表 3-7 は、この目標を実現するために WAN インフラストラクチャで必要となる QoS 機能とツールを示しています。

表 3-7　WAN テクノロジーとリンク速度ごとの Unified Communications サポートに必要な QoS 機能とツール

WAN テクノロジー	リンク速度：56 ～ 768 kbps	リンク速度：768 kbps 以上
専用回線	• MLP（マルチリンク ポイントツーポイント プロトコル） • MLP LFI（リンク フラグメンテーション/インターリーブ） • LLQ（低遅延キューイング） • オプション：cRTP（RTP ヘッダー圧縮）	• LLQ
フレームリレー（FR）	• トラフィック シェーピング • LFI（FRF.12） • LLQ • オプション：cRTP • オプション：Voice-Adaptive Traffic Shaping（VATS） • オプション：Voice-Adaptive Fragmentation（VAF）	• トラフィック シェーピング • LLQ • オプション：VATS
非同期転送モード（ATM）	• TX-ring バッファ変更 • MLP over ATM • MLP LFI • LLQ • オプション：cRTP（MLP が必要）	• TX-ring バッファ変更 • LLQ

表 3-7　WAN テクノロジーとリンク速度ごとの Unified Communications サポートに必要な QoS 機能とツール（続き）

WAN テクノロジー	リンク速度：56 ～ 768 kbps	リンク速度：768 kbps 以上
フレームリレーと ATM のサービス インターワーキング（SIW）	• TX-ring バッファ変更 • MLP over ATM と FR • MLP LFI • LLQ • オプション：cRTP（MLP が必要）	• TX-ring バッファ変更 • MLP over ATM と FR • LLQ
Multiprotocol Label Switching（MPLS）	• インターフェイス テクノロジーに応じて、上記と同じ • 一般に、サービス プロバイダーの仕様に応じて、フローをリマークするにはクラスベースのマーキングが必要	• インターフェイス テクノロジーに応じて、上記と同じ • 一般に、サービス プロバイダーの仕様に応じて、フローをリマークするにはクラスベースのマーキングが必要

次の各項では、音声とデータの両方のトラフィックをサポートするように WAN を設計する場合に、考慮すべき最も重要な機能と手法を説明しています。

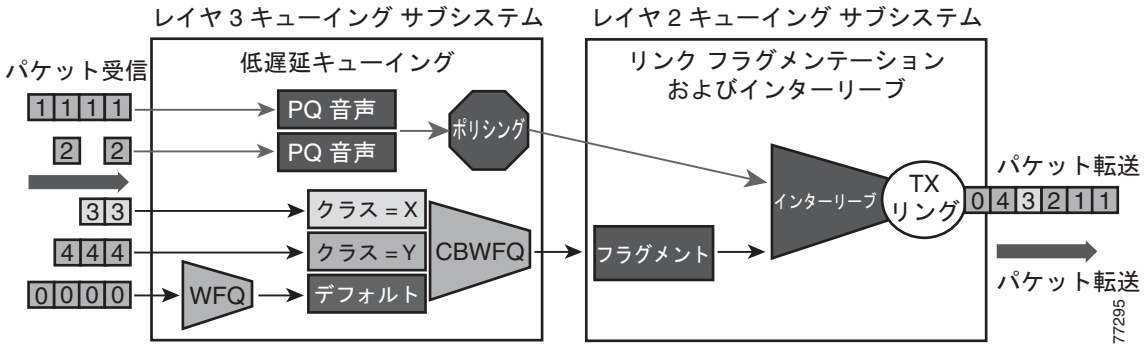
- 「トラフィックの優先順位」（P.3-41）
- 「リンク効率化手法」（P.3-43）
- 「トラフィック シェーピング」（P.3-45）

トラフィックの優先順位

多数の使用可能な優先付け体系の中から選択する場合、関係するトラフィックのタイプと、WAN 上のメディアのタイプが主に考慮すべき要素です。IP WAN を介したマルチサービス トラフィックの場合は、すべてのリンクに対して Low-Latency Queuing（LLQ; 低遅延キューイング）を使用することを推奨します。この方法では、最大 64 のトラフィック クラスをサポートできるほか、たとえば、音声と双方向ビデオに対するプライオリティ キューイング動作、音声制御トラフィックに対する最小帯域幅のクラスベース WFQ、主幹業務のデータに対する追加の最小帯域幅の WFQ、およびその他すべてのトラフィック タイプに対するデフォルトのベストエフォート型キューを指定できます。

図 3-11 は、優先付け体系の例を示しています。

図 3-11　WAN を介した VoIP 用の最適化キューイング



LLQ には、次の優先付けの基準を使用することを推奨します。

- *音声*がプライオリティ キューに入る基準は、Differentiated Services Code Point（DSCP）値 46、または Per-Hop Behavior（PHB）値 EF です。
- *ビデオ会議*トラフィックがプライオリティ キューに入る基準は、DSCP 値 34、または PHB 値 AF41 です。ただし、ビデオ トラフィックはパケット サイズが大きいため、このパケットをプライオリティ キューに入れるのは、768 Kbps を超える速度の WAN リンク上に限定する必要があります。この値に満たないリンク速度では、パケット フラグメンテーションが必要です。ただし、プライオリティ キューに入るパケットはフラグメント化されません。そのため、小さな音声パケットが大きなビデオ パケットの後に続いてキューに入る可能性があります。768 Kbps 以下の速度のリンクでは、ビデオ会議トラフィックは別のクラスベース WFQ（CBWFQ）に入る必要があります。

  （注）　片方向ビデオ トラフィック（ビデオ オンデマンドやライブ ビデオ フィードなどのサービス向けのストリーミング ビデオ アプリケーションによって生成されるトラフィックなど）は、常に CBWFQ 方式を使用する必要があります。これは、このタイプのトラフィックは、双方向ビデオ会議トラフィックよりも遅延許容度がはるかに高いためです。

- WAN リンクが輻輳すると、*音声制御シグナリング* プロトコルが停止する可能性があります。したがって、IP Phone が IP WAN を介してコールできなくなります。そのため、音声制御プロトコル（たとえば、H.323、MGCP、および Skinny Client Control Protocol（SCCP））には、独自のクラスベース WFQ が必要です。このキューに入る基準は、DSCP 値 24 または PHB 値 CS3 です。

  （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）に移行しました。ただし、一部の製品は、引き続きシグナリング トラフィックを DSCP 26（PHB AF31）としてマークします。したがって、コール シグナリング用に AF31 と CS3 の両方を予約することを推奨します。

- 場合によっては、特定のデータ トラフィックで、ベストエフォート型よりも優れた処理が必要になることがあります。このトラフィックは、*ミッションクリティカル データ*と呼ばれ、必要な帯域幅を持つ 1 つ以上のキューに入ります。このクラス内のキューイング方式は、最小帯域幅が割り当てられた First-In-First-Out（FIFO; ファーストインファーストアウト）です。このクラスのトラフィックは、設定された帯域幅限界を超えると、デフォルト キューに入れられます。このキューへの入力基準は、Transmission Control Protocol（TCP）ポート番号、レイヤ 3 アドレス、または DSCP/PHB 値にすることができます。
- 残りの企業トラフィックはすべて、ベストエフォート型処理のデフォルト キューに入れることができます。キーワード **fair** を指定すると、キューイング アルゴリズムは WFQ になります。

Scavenger Class

Scavenger Class は、特定のアプリケーションに対してベストエフォート未満のサービスを提供することを目的としています。このクラスに割り当てられるアプリケーションは、企業の組織的目標にはほとんどまたはまったく貢献せず、本質的にはエンターテイメント志向であることが一般的です。

Scavenger トラフィックを最小帯域幅キューに割り当てることにより、輻輳期間中はこのトラフィックが抑制されて事実上発生しなかったことにされますが、オフピーク時に発生するなどで帯域幅が業務目的で使用されていない場合には、このトラフィックが使用可能になります。

- Scavenger トラフィックは、DSCP CS1 としてマークされる必要があります。
- Scavenger トラフィックは、最小限の設定可能なキューイング サービスに割り当てられる必要があります。たとえば、Cisco IOS では、Scavenger Class に 1% の CBWFQ を割り当てることになります。

リンク効率化手法

次のリンク効率化技術によって、低速 WAN リンクの品質と効率が向上します。

Compressed Real-Time Transport Protocol（cRTP）

cRTP を使用すると、リンク効率化を高めることができます。このプロトコルは、40 バイトの IP ヘッダー、ユーザ データグラム プロトコル（UDP）ヘッダー、および RTP ヘッダーを約 2 ～ 4 バイトに圧縮します。cRTP は、ホップごとに動作します。個々のリンクで cRTP を使用するのは、そのリンクが次の条件を*すべて*満たす場合だけにしてください。

- 音声トラフィックによる負荷が、特定リンク上で 33% を超えている場合。
- リンクが低ビット レート コーデック（たとえば G.729）を使用する場合。
- 他のリアルタイム アプリケーション（たとえば、ビデオ会議）が同じリンクを使用しない場合。

リンクが上記の条件のいずれかを満たさない場合、cRTP は無効であり、そのリンクで使用しないでください。cRTP を使用する前に考慮する必要があるもう一つの重要なパラメータは、ルータの CPU 使用率です。これは、圧縮操作と圧縮解除操作によって悪影響を受けます。

ATM とフレームリレーの Service Inter-Working（SIW; サービス インターワーキング）リンクで cRTP を使用する場合は、Multilink Point-to-Point Protocol（MLP; マルチリンク ポイントツーポイント プロトコル）を使用する必要があります。

cRTP 圧縮は、パケットが出力インターフェイスを通過する前、つまり、LLQ クラスベース キューイングが行われた後の最終段階として行われます。Cisco IOS Release 12.2(2)T からは、cRTP により、*音声*クラスの帯域幅を圧縮パケット値に基づいて設定できる LLQ クラスベース キューイング メカニズムへのフィードバック メカニズムを使用できるようになりました。12.(2)2T よりも前の Cisco IOS リリースでは、このメカニズムは使用されていないため、LLQ は圧縮帯域幅を認識しません。したがって、圧縮が行われないものとして*音声*クラスの帯域幅をプロビジョニングする必要があります。表 3-8 は、512 Kbps リンクで G.729 コーデックを使用して 10 コールに対応する場合の、*音声*クラスの帯域幅の設定における違いの例を示しています。

表 3-8 では、cRTP 以外の G.729 コールの場合が 24 Kbps で、cRTP の G.729 コールの場合が 10 Kbps であることを前提としていることに注意してください。これらの帯域幅の数値は、音声ペイロードと IP/UDP/RTP ヘッダーだけに基づいています。レイヤ 2 ヘッダーの帯域幅は考慮に入れていません。ただし、実際の帯域幅プロビジョニングでは、レイヤ 2 ヘッダーの帯域幅も、WAN リンクで使用されたタイプに基づいて考慮に入れられます。

表 3-8　512 Kbps リンク帯域幅と G.729 コーデックを使用して 10 コールに対応する場合の LLQ 音声クラスの帯域幅要件

Cisco IOS リリース	cRTP が設定されていない場合	cRTP が設定されている場合
12.2(2)T よりも前	240 kbps	240 kbps[1]
12.2(2)T 以降	240 kbps	100 kbps

1. 不要な帯域幅の 140 Kbps は、LLQ *音声*クラスで設定される必要があります。

また、Cisco IOS Release 12.2(13)T からは、Class-Based cRTP 機能を使用して、cRTP を音声クラスの一部として設定できるようになったことにも注意してください。このオプションを使用すると、サービス ポリシーを介してインターフェイスに接続されているクラス内で cRTP を指定できます。この新しい機能により、**show policy interface** コマンドを使用して、圧縮の統計情報や帯域幅の状況を表示できます。このコマンドは、cRTP が IP/RTP ヘッダーを圧縮している事実を踏まえて、インターフェイス サービス ポリシー クラスに対して提供されるレートを確認するときに非常に役立つ場合があります。

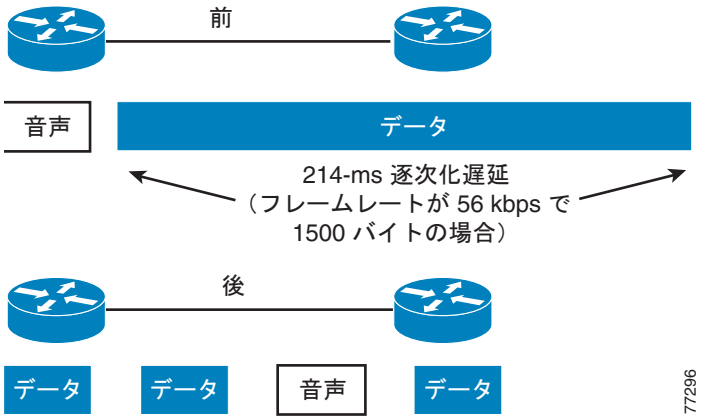
音声およびビデオに対応した IPSec VPN（V3PN）で cRTP を使用する場合の追加の推奨事項については、次の Web サイトで入手可能な V3PN 資料を参照してください。

http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns817/landing_voice_video.html

リンク フラグメンテーション/インターリーブ（LFI）

低速リンク（768 Kbps 未満）の場合、許容できる音声品質を確保するには、LFI メカニズムを使用する必要があります。この手法は、図 3-12 に示されているように、大きなデータ フレームの背後で、音声トラフィックが遅延しないようにして、ジッタを制限します。この目的のための 2 つの手法は、Multilink Point-to-Point Protocol（MLP; マルチリンク ポイントツーポイント プロトコル）LFI（専用回線、ATM、および SIW 用）と、フレームリレー用の FRF.12 です。

図 3-12　　リンク フラグメンテーション/インターリーブ（LFI）



Voice-Adaptive Fragmentation（VAF）

上記の LFI メカニズムのほかに、フレームリレー リンク用の LFI メカニズムには Voice-Adaptive Fragmentation（VAF）もあります。VAF は FRF.12 フレームリレー LFI を使用します。ただし、VAF が設定されている場合、フラグメンテーションが発生するのは、LLQ プライオリティ キューにトラフィックが存在する場合、またはインターフェイス上で H.323 シグナリング パケットが検出された場合だけです。この方法を使用すると、WAN インターフェイス上で音声トラフィックが送信されているときに、大きなパケットがフラグメント化およびインターリーブされることが保証されます。ただし、WAN リンク上に音声トラフィックが存在しない場合は、フラグメント化されていないリンクを介してトラフィックが転送されるため、フラグメンテーションに必要なオーバーヘッドが低減されます。

VAF は、一般に、Voice-Adaptive Traffic Shaping と組み合せて使用されます（「Voice-Adaptive Traffic Shaping（VATS）」（P.3-46）を参照）。VAF はオプションの LFI ツールです。VAF を有効にする場合は注意が必要です。これは、音声アクティビティが検出されるタイミングと LFI メカニズムが連動するタイミングの間に多少の遅延が生じるためです。また、最後の音声パケットが検出されてか

ら、VAF が非アクティブになるまでの間に、設定可能な非アクティブ化タイマー（デフォルトは 30 秒）が期限切れになる必要があります。そのため、この期間は LFI が不必要に発生します。VAF は、Cisco IOS Release 12.2(15)T 以降で使用できます。

トラフィック シェーピング

トラフィック シェーピングは、ATM やフレーム リレーなどの複数アクセスの非ブロードキャスト メディアに必要です。この場合、物理的なアクセス速度は 2 つのエンドポイント間で異なり、複数の支店サイトは、一般に中央サイトの単一ルータ インターフェイスに集約されます。

図 3-13 は、同一 IP WAN 上での音声とデータの転送時にトラフィック シェーピングが必要な主な理由を示しています。

図 3-13　フレームリレーと ATM を使用したトラフィック シェーピング

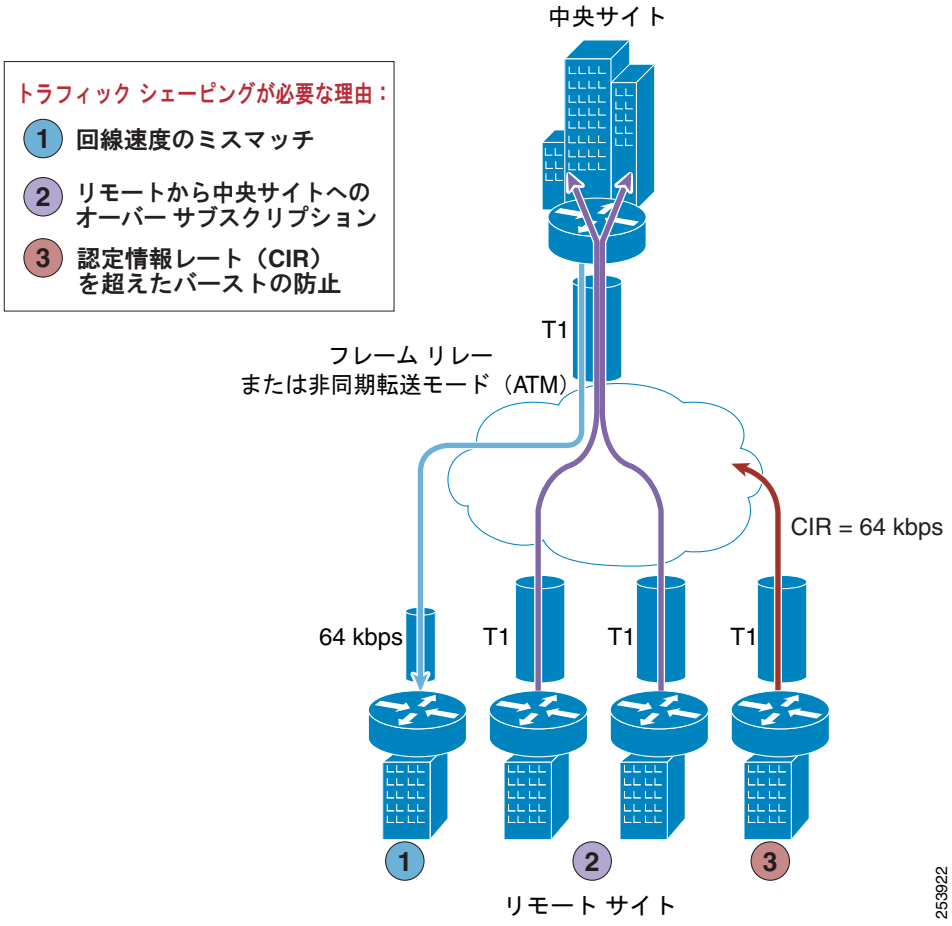


図 3-13 は、次の 3 つのシナリオを示しています。

1. 回線速度のミスマッチ

中央サイトのインターフェイスは、一般に高速インターフェイス（たとえば、T1 以上）ですが、小規模なリモート サイトの支店のインターフェイス回線速度はかなり遅くなります（たとえば、64 Kbps）。データが中央サイトから低速リモート サイトにフル レートで送信される場合、リモート サイトのインターフェイスが輻輳し、その結果、音声品質の低下の原因となるパケットのドロップが発生する可能性があります。

2. 中央サイトとリモート サイト間のリンクのオーバーサブスクリプション

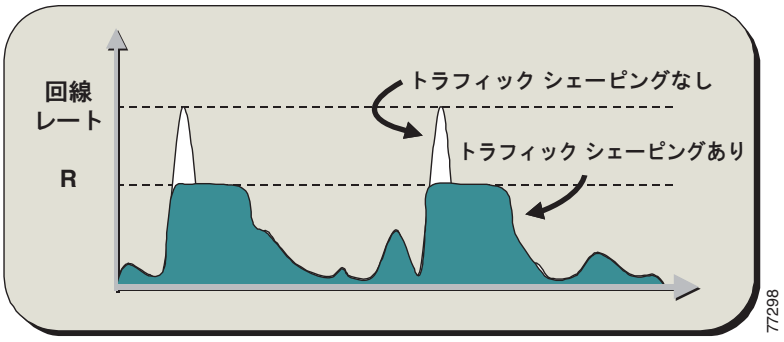
   複数のリモート サイトを 1 つの中央サイトに集約する場合、帯域幅をオーバーサブスクリプションにするのは、フレームリレーまたは ATM ネットワークでは一般的な方法です。たとえば、T1 インターフェイスで WAN に接続するリモート サイトが複数あるにもかかわらず、中央サイトには 1 つの T1 インターフェイスしかない場合があります。この設定により、配置されたネットワークは統計多重化による恩恵を受けますが、中央サイトのルータ インターフェイスが、トラフィックのバースト時に輻輳し、音声品質が低下することがあります。

3. 認定情報レート（CIR）を超えたバースト

   もう 1 つの一般的な設定は、CIR を超えたトラフィック バーストを許可することです。CIR は、サービス プロバイダーが、損失なく、遅延の少ないネットワークを介して転送することを保証したレートです。たとえば、T1 インターフェイスを備えたリモート サイトでは、CIR が 64 Kbps に過ぎない場合があります。64 Kbps 超に相当するトラフィックが WAN を介して送信される場合、プロバイダーは、追加トラフィックに「廃棄適性」のマークを付けます。プロバイダーのネットワークで輻輳が起きた場合、このトラフィックはトラフィック分類に関係なくドロップされるため、音声品質に悪影響を与える可能性があります。

トラフィック シェーピングは、インターフェイスから送出されるトラフィックを、回線レート未満のレートに制限して、WAN の両端で輻輳が起きないようにし、こうした問題を解決します。図 3-14 は、このメカニズムの一般的な例を説明しています。ここで、R は、トラフィック シェーピングが適用される場合のレートです。

図 3-14　　トラフィック シェーピングのメカニズム



Voice-Adaptive Traffic Shaping（VATS）

VATS は、オプションのダイナミック メカニズムで、WAN を介して音声が送信されているかどうかに基づいてさまざまなレートで、フレームリレー Permanent Virtual Circuits（PVC; 相手先固定接続）上のトラフィックをシェーピングします。LLQ 音声プライオリティ キューにトラフィックが存在する場合や、リンク上で H.323 シグナリングが検出された場合は、VATS が連動します。一般に、フレームリレーは、常時、PVC の保証帯域幅または CIR に合せて、トラフィックをシェーピングします。ただし、この PVC では、一般に、CIR を超えた（回線速度までの）バーストが許可されているため、トラフィック シェーピングによって、WAN に存在する可能性のある追加の帯域幅をトラフィックが継続的に使用するようになります。フレームリレー PVC 上で VATS が有効の場合、リンク上に音声トラ

フィックが存在するときは、WAN インターフェイスは CIR でトラフィックを送信できます。ただし、音声が存在しないときは、音声以外のトラフィックが回線速度までバーストして、WAN に存在する可能性がある追加の帯域幅を利用できます。

VATS を Voice-Adaptive Fragmentation（VAF）と組み合せて使用する場合（「リンク フラグメンテーション/インターリーブ（LFI）」（P.3-44）を参照）、インターフェイス上で音声アクティビティが検出されたときは、音声以外のトラフィックはすべてフラグメント化され、トラフィックはすべて WAN リンクの CIR に合せてシェーピングされます。

VAF の場合と同様、VATS をアクティブにすると音声以外のトラフィックに悪影響を与える可能性があるため、VATS を有効にするときは注意してください。リンク上に音声が存在すると、データ アプリケーションのスループットは低下します。これは、アプリケーションが CIR をはるかに下回る速度まで抑制されるためです。この動作の結果、音声以外のトラフィックで、パケット ドロップや遅延が発生する場合があります。さらに、音声トラフィックが検出されなくなってから、トラフィックが回線速度までバーストするまでの間に、非アクティブ化タイマー（デフォルトは 30 秒）が期限切れになる必要があります。VATS を使用する場合は、エンド ユーザの期待を設定し、WAN を介した音声コールが存在するとデータ アプリケーションの速度が定期的に低下することをエンド ユーザに知らせることが重要です。VATS は、Cisco IOS Release 12.2(15)T 以降で使用できます。

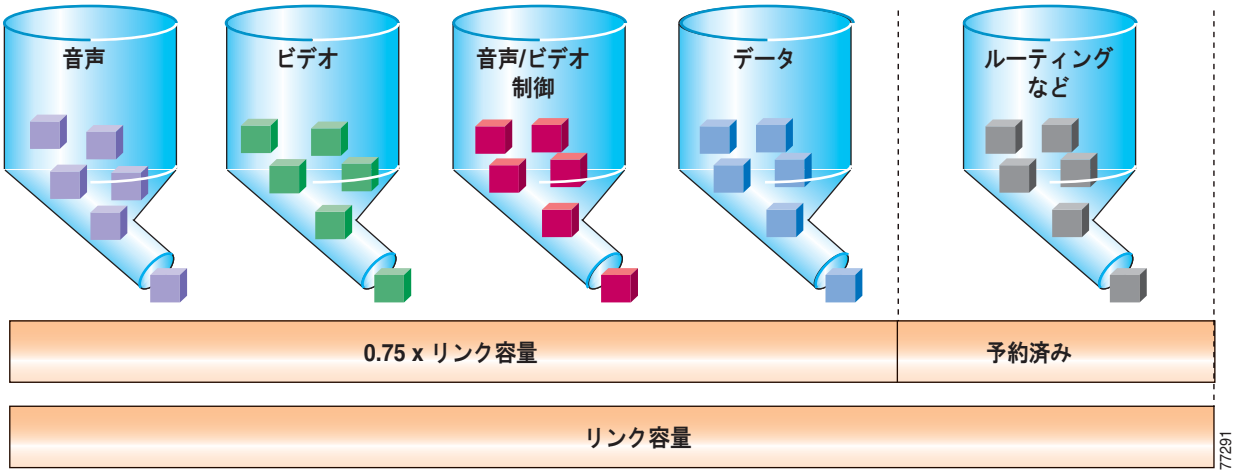
Voice-Adaptive Traffic Shaping 機能とフラグメンテーション機能の詳細、およびそれらの設定方法については、次の Web サイトで入手可能なドキュメントを参照してください。

http://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/ft_vats.html

帯域幅のプロビジョニング

成功する IP ネットワークを設計する主要部分は、ネットワーク帯域幅の適切なプロビジョニングです。主要なアプリケーション（たとえば、音声、映像、およびデータ）ごとの帯域幅必要量を加算すると、必要な帯域幅を計算できます。この合計値は、任意のリンクの最小帯域幅必要量を表します。この値は、そのリンクに使用可能な合計帯域幅の約 75% 以下でなければなりません。この 75% ルールは、ルーティングやレイヤ 2 キープアライブなどのオーバーヘッド トラフィックに、いくらかの帯域幅が必要であることを前提としています。図 3-15 は、こうした帯域幅のプロビジョニング プロセスを示しています。

図 3-15　リンクの帯域幅プロビジョニング



使用可能な合計帯域幅の 75% 以下をデータ、音声、およびビデオに使用することに加え、すべての LLQ プライオリティ キューに対して設定する合計帯域幅は、通常、リンクの合計帯域幅の 33% 以下にする必要があります。使用可能な帯域幅の 33% 超をプライオリティ キュー用にプロビジョニングすると、いくつかの理由で問題となる場合があります。まず、帯域幅の 33% 超を音声用にプロビジョニングすると、CPU 使用率が高くなる場合があります。各音声は毎秒 50 パケットを送信する（20 ms サンプルを使用する）ので、プライオリティ キューに多数のコールをプロビジョニングすると、パケット レートが高いため、CPU レベルが高くなる場合があります。また、プライオリティ キューに複数のタイプのトラフィックをプロビジョニングすると（たとえば、音声とビデオ）、プライオリティ キューは実質的に First-in, First-out（FIFO; ファーストイン ファーストアウト）キューとなるため、QoS を有効にする意味がなくなります。予約するプライオリティ帯域幅の割合を大きくすると、より多くのリンク帯域幅が FIFO となるため、実質的に QoS の効果がなくなります。最後に、使用可能な帯域幅の 33% 超を割り当てると、プロビジョニングされたすべてのデータ キューが実質的に不足状態になる場合があります。単一のコールでもリンク帯域幅の 33% 超を要求する可能性があるため、非常に低速のリンク（192 Kbps 未満）では、リンク帯域幅の 33% 以下をプライオリティ キュー用にプロビジョニングするという推奨事項は、明らかに非現実的となる場合があります。このような場合や、この推奨事項に従うと特定のビジネス ニーズを満たせない場合は、必要に応じて 33% ルールを超えてもかまいません。

トラフィックの観点から見ると、IP テレフォニー コールは次の 2 つの部分から構成されています。

- 実際の音声サンプルが入っている Real-Time Transport Protocol（RTP）パケットから構成される、音声およびビデオ ベアラ ストリーム。
- コールに関係するエンドポイントに応じて、複数のプロトコルのいずれか（たとえば、H.323、MGCP、SCCP、または (J)TAPI）に属するパケットから構成される、呼制御シグナリング。たとえば、呼制御機能は、コールのセットアップ、保持、終了、または転送に使用される機能です。

帯域幅のプロビジョニングには、ベアラ トラフィックだけでなく、呼制御トラフィックも含まれていなければなりません。実際に、マルチサイト WAN 配置では、呼制御トラフィック（およびベアラ ストリーム）は、WAN を通過する必要があるので、そのトラフィックに十分な帯域幅を割り当てないと、悪影響を与える可能性があります。

次の 3 つの項では、トラフィックのタイプについて、帯域幅プロビジョニングの推奨事項を説明します。

- すべてのマルチサイト WAN 配置における音声およびビデオ ベアラ トラフィック（「ベアラ トラフィック用のプロビジョニング」（P.3-48）を参照）
- 集中型コール処理を使用するマルチサイト WAN 配置における呼制御トラフィック（「集中型コール処理を使用した呼制御トラフィック用のプロビジョニング」（P.3-52）を参照）
- 分散型コール処理を使用するマルチサイト WAN 配置における呼制御トラフィック（「分散型コール処理を使用した呼制御トラフィック用のプロビジョニング」（P.3-56）を参照）

ベアラ トラフィック用のプロビジョニング

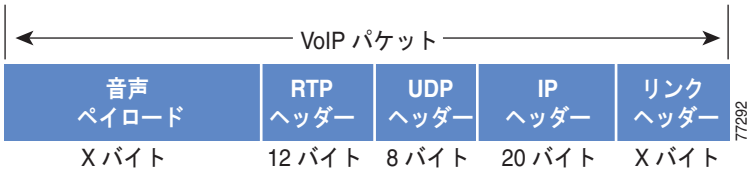
この項では、次のトラフィック タイプの帯域幅プロビジョニングについて説明します。

- 「音声ベアラ トラフィック」（P.3-49）
- 「ビデオ ベアラ トラフィック」（P.3-51）

音声ベアラ トラフィック

図 3-16 に示されているように、VoIP（Voice-over-IP）パケットは、音声ペイロード、IP ヘッダー、ユーザ データグラム プロトコル（UDP）ヘッダー、Real-Time Transport Protocol（RTP）ヘッダー、およびレイヤ 2 リンク ヘッダーから構成されています。Secure Real-Time Transport Protocol（SRTP）暗号化を使用すると、各パケットの音声ペイロードは 4 バイト増加します。リンク ヘッダーの大きさは、使用されるレイヤ 2 メディアによって異なります。

図 3-16　一般的な VoIP パケット



VoIP ストリームによって消費される帯域幅を計算するには、次に示すように、パケットのペイロードとすべてのヘッダーを加算し（ビット単位）、1 秒あたりのパケット レート（デフォルトでは、毎秒 50 パケット）を掛けます。

レイヤ 2 帯域幅（kbps）= [（1 秒あたりのパケット数）*（音声ペイロード *X* バイト + RTP/UDP/IP ヘッダー 40 バイト + レイヤ 2 オーバーヘッド *Y* バイト）* 8 ビット] / 1000

レイヤ 3 帯域幅（kbps）= [（1 秒あたりのパケット数）*（音声ペイロード *X* バイト + RTP/UDP/IP ヘッダー 40 バイト）* 8 ビット] / 1000

1 秒あたりのパケット数 = [1/（サンプリング レート（msec））] * 1000

音声ペイロード（バイト）= [（コーデック ビット ビット レート（kbps））*（サンプリング レート msec）] / 8

表 3-9 は、VoIP フローあたりのレイヤ 3 帯域幅を詳しく記述しています。表 3-9 は、音声ペイロードと IP ヘッダーだけによって消費される帯域幅を示しています。ここでは、パケット レートとして、デフォルトのパケット レートである 50 パケット / 秒（pps）と、暗号化されていないペイロードと暗号化されたペイロードの両方のレートである 33.3 pps を使用しています。表 3-9 には、レイヤ 2 ヘッダーのオーバーヘッドは含まれていません。また、RTP ヘッダー圧縮（cRTP）などの可能な圧縮方式を考慮していません。Unified CM Administration の Service Parameters メニューを使用すると、コーデック サンプリング レートを調整できます。

表 3-9　音声ペイロードと IP ヘッダーだけの帯域幅使用量

コーデック	サンプリング レート	音声ペイロード（バイト数）	1 秒あたりのパケット数	1 会話あたりの帯域幅
G.711 および G.722-64k	20 ms	160	50.0	80.0 kbps
G.711 および G.722-64k（SRTP）	20 ms	164	50.0	81.6 kbps
G.711 および G.722-64k	30 ms	240	33.3	74.7 kbps
G.711 および G.722-64k（SRTP）	30 ms	244	33.3	75.8 kbps
iLBC	20 ms	38	50.0	31.2 kbps
iLBC（SRTP）	20 ms	42	50.0	32.8 kbps
iLBC	30 ms	50	33.3	24.0 kbps

表 3-9　音声ペイロードと IP ヘッダーだけの帯域幅使用量（続き）

コーデック	サンプリング レート	音声ペイロード（バイト数）	1 秒あたりのパケット数	1 会話あたりの帯域幅
iLBC（SRTP）	30 ms	54	33.3	25.1 kbps
G.729A	20 ms	20	50.0	24.0 kbps
G.729A（SRTP）	20 ms	24	50.0	25.6 kbps
G.729A	30 ms	30	33.3	18.7 kbps
G.729A（SRTP）	30 ms	34	33.3	19.8 kbps

より正確な方法でプロビジョニングするには、帯域幅の計算にレイヤ 2 ヘッダーを含めます。表 3-10 は、レイヤ 2 ヘッダーを計算に含めたときの、音声トラフィックによって消費される帯域幅の量を示しています。

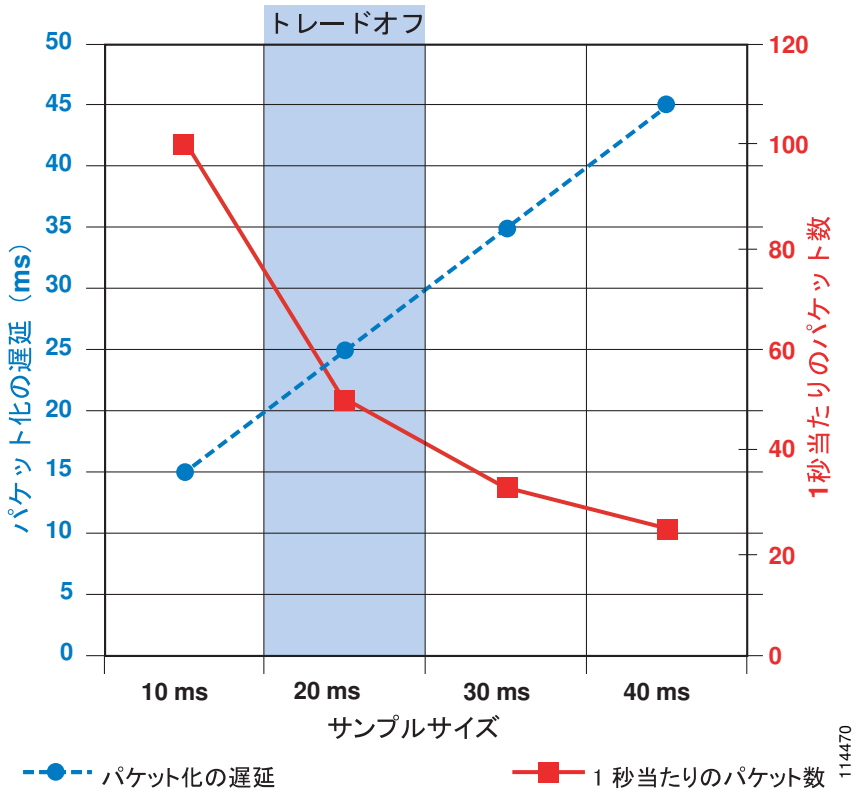
表 3-10　レイヤ 2 ヘッダーが含まれた帯域幅使用量

	ヘッダー タイプとサイズ						
コーデック	イーサネット 14 バイト	PPP 6 バイト	ATM 53 バイトのセルと 48 バイトのペイロード	フレーム リレー 4 バイト	MLPPP 10 バイト	MPLS 4 バイト	WLAN 24 バイト
G.711 および G.722-64k（50.0 pps）	85.6 kbps	82.4 kbps	106.0 kbps	81.6 kbps	84.0 kbps	81.6 kbps	89.6 kbps
G.711 および G.722-64k（SRTP）（50.0 pps）	87.2 kbps	84.0 kbps	106.0 kbps	83.2 kbps	85.6 kbps	83.2 kbps	該当なし
G.711 および G.722-64k（33.3 pps）	78.4 kbps	76.3 kbps	84.8 kbps	75.7 kbps	77.3 kbps	75.7 kbps	81.1 kbps
G.711 および G.722-64k（SRTP）（33.3 pps）	79.5 kbps	77.4 kbps	84.8 kbps	76.8 kbps	78.4 kbps	76.8 kbps	該当なし
iLBC（50.0 pps）	36.8 kbps	33.6 kbps	42.4 kbps	32.8 kbps	35.2 kbps	32.8 kbps	40.8 kbps
iLBC（SRTP）（50.0 pps）	38.4 kbps	35.2 kbps	42.4 kbps	34.4 kbps	36.8 kbps	34.4 kbps	42.4 kbps
iLBC（33.3 pps）	27.7 kbps	25.6 kbps	28.3 kbps	25.0 kbps	26.6 kbps	25.0 kbps	30.4 kbps
iLBC（SRTP）（33.3 pps）	28.8 kbps	26.6 kbps	42.4 kbps	26.1 kbps	27.7 kbps	26.1 kbps	31.5 kbps
G.729A（50.0 pps）	29.6 kbps	26.4 kbps	42.4 kbps	25.6 kbps	28.0 kbps	25.6 kbps	33.6 kbps
G.729A（SRTP）（50.0 pps）	31.2 kbps	28.0 kbps	42.4 kbps	27.2 kbps	29.6 kbps	27.2 kbps	35.2 kbps
G.729A（33.3 pps）	22.4 kbps	20.3 kbps	28.3 kbps	19.7 kbps	21.3 kbps	19.8 kbps	25.1 kbps
G729A（SRTP）（33.3 pps）	23.5 kbps	21.4 kbps	28.3 kbps	20.8 kbps	22.4 kbps	20.8 kbps	26.2 kbps

30 ms を超えるサンプリング レートを設定することは可能ですが、これを行うと、通常、音声品質が非常に低下します。図 3-17 に示されているように、サンプリング サイズが増加すると、1 秒あたりのパケット数が減少するため、デバイスの CPU に与える影響は小さくなります。同様に、サンプル サイズ

が増加すると、1 パケットあたりのペイロードが大きくなるため、IP ヘッダーのオーバーヘッドが低下します。ただし、サンプル サイズが増加すると、パケット化の遅延も増加するため、音声トラフィックのエンドツーエンドの遅延が増加します。サンプル サイズを設定する場合は、パケット化の遅延と 1 秒あたりのパケット数とのトレードオフを考慮する必要があります。このトレードオフが 20 ms で最適化されている場合、30 ms のサンプル サイズでも、1 秒あたりのパケット数に対する遅延の比率は妥当なものになります。しかし、40 ms のサンプル サイズでは、パケット化の遅延が大きくなりすぎます。

図 3-17　音声のサンプル サイズ：1 秒あたりのパケット数とパケット化の遅延との比較



ビデオ ベアラ トラフィック

オーディオの場合、各パケットのサンプル サイズを指定して、パケットあたりのオーバーヘッドの比率を計算することは比較的簡単です。これに対して、ビデオの場合は、ビデオで表されるモーションの量（最後のフレームから変更されるピクセル数）によってペイロードが変わるため、正確なオーバーヘッドの比率を計算することは、ほとんど不可能です。

ビデオの正確なオーバーヘッド率を計算できないという問題を解決するために、パケットが通過するレイヤ 2 メディアのタイプにかかわらず、コール速度に 20% を加算することを推奨します。追加の 20% は、イーサネット、ATM、フレーム リレー、PPP、HDLC、およびその他の転送プロトコル間の差を吸収するための余裕となり、ビデオ トラフィックのバースト性に対するクッションにもなります。

エンドポイントで要求されるコール速度（128 kbps、256 kbps など）はコールの最大バースト速度を表し、クッションとして追加分が含まれていることに注意してください。コールの平均速度は、通常、この値を大幅に下回ります。

呼制御トラフィック用のプロビジョニング

Unified Communications エンドポイントが WAN によって呼制御アプリケーションと分けられている場合、または相互接続された 2 つの Unified Communications システムが WAN によって分けられている場合、これらのエンドポイント間やシステム間の呼制御およびシグナリング トラフィック用にプロビジョニングする必要がある帯域幅の量について、考慮が必要です。ここでは、集中型または分散型のコール処理モデルが配置されている場合の、コール シグナリング トラフィック用の WAN 帯域幅プロビジョニングについて説明します。Unified Communications の集中型および分散型のコール処理配置モデルについては、「Unified Communications の配置モデル」（P.5-1）を参照してください。

集中型コール処理を使用した呼制御トラフィック用のプロビジョニング

集中型コール処理配置では、Unified CM クラスタとアプリケーション（たとえば、ボイスメール）は、中央サイトに置かれ、複数のリモート サイトが IP WAN を介して接続されます。リモート サイトでは、コール処理に中央の Unified CM を使用します。

この配置モデルには、次の考慮事項が適用されます。

- リモート サイトの支店の電話機がコールを発信するたびに、制御トラフィックは、支店内へのコールであっても、IP WAN を通過して、中央サイトの Unified CM に到達します。
- この配置モデルで IP WAN を通過するシグナリング プロトコルは、SCCP（暗号化と非暗号化）、SIP（暗号化と非暗号化）、H.323、MGCP、および CTI-QBE です。すべての制御トラフィックは、中央サイトの Unified CM と、リモート サイトの支店のエンドポイントまたはゲートウェイとの間で交換されます。
- クラスタで RSVP が配置されている場合、中央サイトの Unified CM クラスタとリモート サイトの Cisco RSVP Agent の間の制御トラフィックは、SCCP プロトコルを使用します。

その結果、支店のルータと中央サイトの WAN アグリゲーション ルータとの間で WAN を通過する制御トラフィック用の帯域幅を提供する必要があります。

このシナリオで WAN を通過する制御トラフィックは、次の 2 つのカテゴリに分割できます。

- 休止トラフィック。このトラフィックは、コールのアクティビティに関係なく、支店のエンドポイント（電話機、ゲートウェイ、および Cisco RSVP Agent）と Unified CM との間で定期的に交換されるキープアライブ メッセージから構成されます。このトラフィックはエンドポイント数の関数になります。
- コール関連トラフィック。このトラフィックは、コールのセットアップ、終了、転送などが必要なときに、支店のエンドポイントと、中央サイトの Unified CM との間で交換されるシグナリング メッセージから構成されます。このトラフィックは、エンドポイント数とエンドポイントに関連付けられたコール量の関数になります。

生成される呼制御トラフィックの見積もりをするには、支店の各 IP Phone が発信する、1 時間あたりの平均コール数について推測する必要があります。わかりやすくするために、この項での計算では、電話機あたりの毎時平均コール数を 10 と想定します。

（注）　この平均数が、特定の配置のニーズを満たさない場合、「拡張公式」（P.3-54）に記載されている拡張公式を使用して、推奨帯域幅を計算できます。

上記を前提とし、最初はシグナリングの暗号化が設定されていないリモート サイトの支店の場合を考慮すると、呼制御トラフィックに必要な推奨帯域幅は、次の公式で得られます。

公式 1A：SCCP 制御トラフィックに必要な推奨帯域幅、シグナリングの暗号化なし

帯域幅（bps）= 265 *（支店内の IP Phone とゲートウェイの数）

公式 1B：SIP 制御トラフィックに必要な推奨帯域幅、シグナリングの暗号化なし

帯域幅（bps）= 538 *（支店内の IP Phone とゲートウェイの数）

サイトに SCCP エンドポイントと SIP エンドポイントが混在している場合は、使用する電話機のタイプごとに上記の 2 つの公式を個別に使用し、結果を合計します。

公式 1 やこの項に記載されている他のすべての公式には、25% 過剰プロビジョニング係数が含まれています。制御トラフィックにはバースト性があり、高いアクティビティのピークの後に、アクティビティの低い期間が続きます。このため、制御トラフィック キューに必要な最小の帯域幅だけを割り当てると、アクティビティの高い期間に、バッファリング遅延や、場合によってはパケット ドロップなど、望ましくない影響が現れることがあります。Cisco IOS の Class-Based Weighted Fair Queuing（CBWFQ; クラスベース WFQ）キューに対するデフォルトのキュー項目数は、64 パケットです。このキューに割り当てられた帯域幅によって、そのサービス レートが決まります。設定されている帯域幅が、このタイプのトラフィックによって消費される平均帯域幅になっていることを前提とすると、明らかに、アクティビティが高い期間ではすべての着信パケットをキューから「排出」するのに十分なサービス レートとならないため、パケットはバッファに入れられます。64 パケットの制限に到達した場合、それ以降のパケットはすべて、ベストエフォート型のキューに割り当てられるか、またはドロップされます。したがって、トラフィック パターンの変動を吸収し、一時的なバッファ オーバーランのリスクを最小限に抑えるために、この 25% の過剰プロビジョニング係数を導入することを推奨します。この導入は、キューのサービス レートを増やすことに相当します。

暗号化を設定すると、Unified CM とエンドポイント間で交換されるシグナリング パケットのサイズが増加するため、推奨帯域幅が影響を受けます。次の公式では、シグナリングの暗号化の影響を考慮に入れています。

公式 2A：SCCP 制御トラフィックに必要な推奨帯域幅、シグナリングの暗号化あり

シグナリングの暗号化を使用する場合の帯域幅（bps）= 415 *（支店内の IP Phone とゲートウェイの数）

公式 2B：SIP 制御トラフィックに必要な推奨帯域幅、シグナリングの暗号化あり

シグナリングの暗号化を使用する場合の帯域幅（bps）= 619 *（支店内の IP Phone とゲートウェイの数）

Cisco IOS ルータ上のキューに割り当てることができる最小帯域幅が 8 Kbps であるという事実を考慮すると、支店のさまざまな規模に対する最小帯域幅と推奨帯域幅の値を、表 3-11 のようにまとめることができます。

表 3-11　呼制御トラフィック用の推奨レイヤ 3 帯域幅（シグナリングの暗号化の有無別）

支店の規模（IP Phone とゲートウェイの数）	SCCP 制御トラフィック用の推奨帯域幅（暗号化なし）	SCCP 制御トラフィック用の推奨帯域幅（暗号化あり）	SIP 制御トラフィック用の推奨帯域幅（暗号化なし）	SIP 制御トラフィック用の推奨帯域幅（暗号化あり）
1 ～ 10	8 kbps	8 kbps	8 kbps	8 kbps
20	8 kbps	9 kbps	11 kbps	12 kbps
30	8 kbps	13 kbps	16 kbps	19 kbps
40	11 kbps	17 kbps	22 kbps	25 kbps
50	14 kbps	21 kbps	27 kbps	31 kbps
100	27 kbps	42 kbps	54 kbps	62 kbps
150	40 kbps	62 kbps	81 kbps	93 kbps

（注）　表 3-11 では、電話機あたりの毎時平均コール数を 10 と想定し、RSVP 制御トラフィックを含みません。この表の値に追加する RSVP 関連の帯域幅を判断するには、「RSVP を使用するコールに関する考慮事項」（P.11-38）を参照してください。

（注）　サイト間コールに RSVP ベースのロケーション ポリシーを使用する場合は、表 3-11 の値を増やし、Cisco RSVP Agent の制御トラフィックの分を補正する必要があります。たとえば、コールの 10% が WAN を経由する場合、表 3-11 の値に 1.1 を掛けます。

拡張公式

この項で示されている上記の公式は、電話機 1 台あたりの平均コール レートを毎時 10 コールと想定しています。しかし、コール パターンが大きく異なる場合（たとえば、支店にコール センター エージェントが配置されている場合）、この想定が、実際の配置に該当しない場合があります。こうした場合の呼制御帯域幅必要量を計算するには、次の公式を使用してください。これらの公式には、電話機 1 台あたりの毎時平均コール数を表す追加変数（CH）が含まれています。

公式 3A：支店の SCCP 制御トラフィックに必要な推奨帯域幅、シグナリングの暗号化なし

帯域幅（bps）= (53 + 21 * CH) *（支店内の IP Phone とゲートウェイの数）

公式 3B：支店の SIP 制御トラフィックに必要な推奨帯域幅、シグナリングの暗号化なし

帯域幅（bps）= (138 + 40 * CH) *（支店内の IP Phone とゲートウェイの数）

公式 4A：支店の SCCP 制御トラフィックに必要な推奨帯域幅、シグナリングの暗号化あり

シグナリングの暗号化を使用する場合の帯域幅（bps）=（73.5 + 33.9 * CH）*（支店内の IP Phone とゲートウェイの数）

公式 4B：支店の SIP 制御トラフィックに必要な推奨帯域幅、シグナリングの暗号化あり

シグナリングの暗号化を使用する場合の帯域幅（bps）=（159 + 46 * CH）*（支店内の IP Phone とゲートウェイの数）

（注）　公式 3A と 4A は、デフォルトの SCCP キープアライブ間隔である 30 秒に基づいています。公式 3B と 4B は、デフォルトの SIP キープアライブ間隔である 120 秒に基づいています。

シェアド ライン アピアランスに関する考慮事項

シェアド ライン アピアランスに発信されるコール、またはブロードキャスト ディストリビューション アルゴリズムを使用する回線グループに送信されるコールは、システムが消費する帯域幅に 2 つのネット効果を与えます。

- 設定された回線のすべての電話機が同時に鳴るため、システムの負荷は回線の毎時コール数（CH）よりも大幅に高い CH 値に対応します。その結果、対応する帯域幅の使用量が増加します。WAN 接続されたシェアド ライン機能を配置する場合は、ネットワーク インフラストラクチャの帯域幅プロビジョニングを調整する必要があります。公式 3 および 4 で使用する CH 値を、次の公式に従って増やす必要があります。

  CHS = CHL *（ライン アピアランス数）/（回線数）

  CHS は公式 3 および 4 で使用する時間あたりのシェアド ライン コール数で、CHL は回線の時間あたり平均コール数です。たとえば、5 回線で設定されたサイトで、時間あたりの平均コール数が 6 で、そのうち 2 回線が 4 台の電話機で共有されている場合、次のようになります。

  回線数 = 5

ライン アピアランス数 = (2 回線が 4 台の電話機に出現し、3 回線が 1 台ずつの電話機に出現) = (2 * 4) + 3 = 11 回線が出現

CHL = 6

CHS = 6 * (11 / 5) = 13.2

- 呼び出す各電話機が個別のシグナリング制御ストリームを必要とするため、Unified CM から同じ支店に送信されるパケット量は、呼び出す電話機の数に比例して増加します。Unified CM は 100 Mbps インターフェイスでネットワークに接続されるため、大量のパケットをすぐに生成できますが、キューイング メカニズムがシグナリング トラフィックを処理するまで、このパケットはバッファに入れる必要があります。処理速度は、通常、100 Mbps よりも 2 桁小さい WAN インターフェイスの実効情報転送速度によって制限されます。

  このトラフィックによって、中央サイトの WAN ルータのキュー項目数があふれることがあります。デフォルトでは、Cisco IOS の各トラフィック クラスで使用できるキュー項目数は 64 です。WAN インターフェイスのキューに入れられる前にパケットがドロップされることを防ぐには、シグナリング キューの項目数が、各シェアド ライン型の電話機について少なくとも 1 つの完全なシェアド ライン イベントで発生するすべてのパケットを保持できるサイズであることを確認してください。ドロップされたパケットを再送信することでシステムからの応答時間が損なわれるような競合状態を防ぐには、ドロップの防止が不可欠です。

  そのため、シェアド ライン型の電話機が動作するために必要なパケット量は、次のようになります。

  - SCCP プロトコル：シェアド ライン型の電話機ごとに 13 パケット
  - SIP プロトコル：シェアド ライン型の電話機ごとに 11 パケット

  たとえば、SCCP と、同じ回線を共有する 6 台の電話機を使用する場合、トラフィックのシグナリング クラス用のキュー項目数は 78 以上に調整する必要があります。表 3-12 は、支店サイトでのシェアド ライン アピアランスの量に基づいた推奨されるキュー項目数を示しています。

表 3-12　支店サイトごとの推奨されるキュー項目数

シェアド ライン アピアランスの数	キュー項目数（パケット数）	
	SCCP	SIP
5	65	55
10	130	110
15	195	165
20	260	220
25	325	275

フレーム リレーなどのレイヤ 2 WAN テクノロジーを使用する場合、この調整は、シェアド ライン型の電話機がある支店に対応する回線で行う必要があります。

MPLS などのレイヤ 3 WAN テクノロジーを使用する場合は、単一のシグナリング キューで複数の支店を処理できます。この場合、処理するすべての支店の合計に対して、調整を行う必要があります。

分散型コール処理を使用した呼制御トラフィック用のプロビジョニング

分散型コール処理配置では、IP WAN を介して複数のサイトが接続されます。各サイトには、Unified CM クラスタが含まれ、単一サイト モデルか、集中型コール処理モデルのどちらかを設定できます。サイト間のコール アドミッション制御には、ゲートキーパーを使用できます。

この配置モデルには、次の考慮事項が適用されます。

- WAN を介したコールの発信に使用されるシグナリング プロトコルは、H.323 または SIP です。
- 制御トラフィックは、各サイトの Cisco IOS ゲートキーパーと Unified CM クラスタとの間、および Unified CM クラスタ相互間で交換されます。

したがって、制御トラフィック用の帯域幅は、Unified CM 相互間の WAN リンクだけでなく、各 Unified CM とゲートキーパー間の WAN リンクでもプロビジョニングされなければなりません。トポロジはハブアンドスポークに限定され、一般にゲートキーパーはハブに置かれるので、各サイトを他のサイトに接続する WAN リンクは、通常、ゲートキーパーに接続するリンクと一致します。

WAN を通過する制御トラフィックは、次のカテゴリのいずれかに属します。

- 休止トラフィック。このトラフィックは、各 Unified CM とゲートキーパー間で定期的に交換される登録メッセージから構成されます。
- コール関連トラフィック。このトラフィックは、次の 2 つのタイプのトラフィックから構成されます。
  - コール アドミッション制御トラフィック。コールのセットアップ前とコールの終了後に、Unified CM とコール アドミッション制御デバイス（ゲートキーパー、Cisco RSVP Agent など）との間で交換されます。
  - メディア ストリームに関連付けられたシグナリング トラフィック。コールのセットアップ、終了、転送などが必要なときに、クラスタ間トランクで交換されます。

制御トラフィックの合計数は、任意の時間にセットアップし、終了するコール数によって異なるので、コール パターンとリンク使用状況について、何らかの想定をする必要があります。各スポーク サイトをハブに接続する WAN リンクは、通常、さまざまなタイプのトラフィック（たとえば、データ、音声、およびビデオ）を受け入れるように設定されます。従来型のテレフォニーから類推すると、WAN リンクの中で音声用に設定された部分を、複数の*仮想タイ ライン*と見なすことができます。

平均コール所要時間を 2 分、各仮想タイ ラインの利用率を 100% と想定すると、各タイ ラインの伝送量は毎時 30 コールであると推論できます。この前提により、呼制御トラフィック用の推奨帯域幅を仮想タイ ライン数の関数として表す、次の公式が得られます。

公式 6：仮想タイ ライン数に基づく推奨帯域幅

推奨帯域幅（bps）= 116 *（仮想タイ ライン数）

Cisco IOS ルータ上のキューに割り当て可能な最小帯域幅は、8 Kbps です。つまり 8 Kbps の最小キュー サイズは、*最大 70 の仮想タイ ライン*によって生成される呼制御トラフィックを受け入れることができると推定できます。これは、大部分の大企業での配置に十分な量です。

ワイヤレス LAN インフラストラクチャ

統合されたネットワークの wireless LAN（WLAN; ワイヤレス LAN）部分に Unified Communications を追加する場合は、ワイヤレス LAN インフラストラクチャの設計が重要になります。Cisco Unified Wireless IP Phone が導入されている場合、音声トラフィックは WLAN 上に移るため、そこで既存のデータ トラフィックと合流します。有線 LAN および有線 WAN インフラストラクチャの場合と同様、WLAN に音声を追加するには、基本的な設定と設計に関するベスト プラクティスに従って、可用性の高いネットワークを配置する必要があります。また、WLAN インフラストラクチャを適切に設計するには、ネットワーク全体でエンドツーエンドの音声品質を保証するために、QoS を理解してワイヤレス ネットワーク上に配置する必要もあります。次の項では、これらの要件について説明します。

- 「WLAN の設計と設定」（P.3-57）
- 「WLAN の QoS」（P.3-61）

Voice over Wireless LAN の詳細については、次の Web サイトで入手可能な『*Voice over Wireless LAN Design Guide*』の最新版を参照してください。

http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns820/landing_voice_wireless.html

WLAN の設計と設定

WLAN を適切に設計する場合は、最初に、既存の有線ネットワークが、可用性の高い、耐障害性のある冗長な方式で配置されていることを確認する必要があります。次に、ワイヤレス テクノロジーについて理解する必要があります。最後に、ワイヤレス Access Point（AP; アクセス ポイント）とワイヤレス テレフォニー エンドポイントを効果的な方法で設定および配置すると、柔軟性のある、セキュアで冗長な、拡張性の高いネットワークを構築できます。

次の項では、WLAN インフラストラクチャのレイヤとネットワーク サービスについて説明します。

- 「ワイヤレス インフラストラクチャに関する考慮事項」（P.3-57）
- 「ワイヤレス AP の設定と設計」（P.3-60）

ワイヤレス インフラストラクチャに関する考慮事項

次の項では、WLAN インフラストラクチャを設計するためのガイドラインとベスト プラクティスについて説明します。

- 「VLAN」（P.3-57）
- 「ローミング」（P.3-58）
- 「ワイヤレス チャネル」（P.3-58）
- 「無線の干渉」（P.3-59）
- 「WLAN 上のマルチキャスト」（P.3-60）

VLAN

有線 LAN インフラストラクチャの場合と同様、ワイヤレス LAN に音声を配置する場合は、アクセス レイヤにある 2 つ以上の VLAN を有効にする必要があります。ワイヤレス LAN 環境のアクセス レイヤには、アクセス ポイント（AP）と最初のホップのアクセス スイッチが含まれます。AP とアクセス スイッチ上では、データ トラフィック用のネイティブ VLAN と、音声トラフィック用の Voice VLAN（Cisco IOS の場合）または Auxiliary VLAN（CatOS の場合）を設定する必要があります。この Voice / Auxiliary VLAN は、ネットワークにある他のすべての有線 Voice VLAN とは分離される必要があります。また、有線 LAN 上の音声エンドポイントの場合と同様、ワイヤレス音声エンドポイント

は、RFC 1918 プライベート サブネット アドレスを使用してアドレス指定される必要があります。ワイヤレス インフラストラクチャを配置する場合は、WLAN AP の管理用に独立した管理 VLAN を設定することも推奨します。この管理 VLAN には WLAN アピアランスを設定しないでください。つまり、関連付けられた Service Set Identifier（SSID）を設定することも、WLAN から直接アクセスできるように設定することもしないでください。

ローミング

デバイスがレイヤ 3 で移動する場合、デバイスはネイティブ VLAN の境界を越えて AP から別の AP に移動します。WLAN ネットワーク インフラストラクチャが自律分散型 AP で構成されている場合、Cisco LAN コントローラによって、Cisco Unified Wireless IP Phone は、IP アドレスを保持し、アクティブ コールを維持しながらレイヤ 3 でローミングできます。シームレスなレイヤ 3 ローミングが行われるのは、クライアントが同じモビリティ グループ内でローミングする場合だけです。Cisco LAN コントローラおよびレイヤ 3 ローミングの詳細については、次の Web サイトで入手可能な製品マニュアルを参照してください。

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

Lightweight アクセス ポイント インフラストラクチャにわたるクライアントのシームレスなレイヤ 3 ローミングは、動的インターフェイス トンネリングを使用する WLAN コントローラによって実現されます。WLAN コントローラと VLAN にわたってローミングする Cisco Unified Wireless IP Phone は、同じ SSID を使用する場合、IP アドレスを保持できるので、アクティブ コールを維持できます。

（注）　デュアルバンド WLAN（2.4 GHz と 5 GHz 帯域を装備）では、クライアントが両方の帯域をサポートする場合、同じ SSID によって 802.11b/g と 802.11a 間でローミングできます。ただし、これにより、音声パスにギャップが発生する場合があります。これらのギャップを回避するには、音声帯域を 1 つだけ使用します。

ワイヤレス チャネル

ワイヤレス エンドポイントと AP は、特定のチャネル上で無線を介して通信します。1 つのチャネル上で通信する場合、ワイヤレス エンドポイントは、一般に、他の非オーバーラップ チャネル上で発生するトラフィックと通信を認識しません。

2.4 GHz 802.11b および 802.11g 用のチャネル設定を最適化するには、設定するチャネルの間に 5 チャネル以上の間隔を設定して、チャネル間の干渉やオーバーラップを防止する必要があります。許可されるチャネルが 1 ～ 11 の北米では、チャネル 1、6、および 11 が、AP とワイヤレス エンドポイント デバイスに使用可能な 3 つの非オーバーラップ チャネルです。それに対して、許可されるチャネルが 1 ～ 13 の欧州では、5 チャネルの間隔がある組み合せは複数可能です。日本も許可されるチャネルが 1 ～ 14 なので、5 チャネルの間隔がある組み合せは複数可能です。

5 GHz 802.11a 用のチャネル設定を最適化するには、1 チャネル以上の間隔を設定して、チャネル間の干渉やオーバーラップを防止する必要があります。北米では、次の 20 のオーバーラップのないチャネルを使用できます。36、40、44、48、52、56、60、64、100、104、108、112、116、132、136、140、149、153、157、および 161。欧州では、同じオーバーラップのないチャネルを使用できます。ただし、多くの国はチャネル 40 の使用をサポートしていないので、19 のオーバーラップのないチャネルだけ使用できます。日本では、次の 8 つのオーバーラップのないチャネルだけがサポートされます。36、40、44、48、52、56、60、および 64。より大きなオーバーラップのないチャネルのセットにより、802.11a では、より高密度に配置された WLAN に対応できます。

一部のチャネルでは、レーダー（軍事、衛星、および気象）による干渉を防止するために、802.11a 帯域が Dynamic Frequency Selection（DFS; 動的周波数選択）および Transmit Power Control（TPC; 伝送パワー コントロール）をサポートする必要があることに注意してください。規制により、チャネル 52 ～ 64、100 ～ 116、および 132 ～ 140 が DFS および TPC をサポートする必要があります。TPC

は、これらのチャネル上の伝送が干渉を引き起こすほど強力にならないように制御します。DFC は、チャネルのレーダー パルスをモニタし、レーダー パルスを検出した場合、DFC はチャネル上の伝送を停止して、新しいチャネルに切り替えます。

AP カバレッジは、同じチャネルで設定された AP 間でオーバーラップが発生しない（または最小になる）ように、配置する必要があります。同じチャネルのオーバーラップは、通常、19 dBm の間隔で発生します。ただし、オーバーラップのないチャネルで適切な AP 配置およびカバレッジを行うには、最低限 20% のオーバーラップが必要です。このオーバーラップ量であれば、ワイヤレス エンドポイントが AP カバレッジ セルの間を移動するときにローミングが円滑に行われることが保証されます。オーバーラップが 20% 未満の場合、ローミングに時間がかかり、音質が悪くなることがあります。

高層オフィスビルや病院など、多階の建物にワイヤレス デバイスを配置する場合は、ワイヤレス AP とチャネル カバレッジのプランニングに 3 つめの次元が加わります。802.11 の 2.4 GHz と 5.0 GHz の波形は、いずれもフロア、天井、および壁を通過できます。このため、同一フロア上のオーバーラップ セルまたはチャネルを考慮するだけでなく、隣接フロア間のチャネル オーバーラップを考慮する必要もあります。3 チャネルだけで適切なオーバーラップを実現するには、慎重に 3 次元の計画を立てる必要があります。

（注）　ワイヤレス ネットワークを正しく動作させるには、ワイヤレス インフラストラクチャ内で AP の配置とチャネルの設定を慎重に行う必要があります。このため、運用環境にワイヤレス ネットワークを配置する前に、実地調査を徹底的に行う必要があります。調査では、非オーバーラップ チャネル設定、AP カバレッジ、および必要なデータ レートとトラフィック レートを確認し、不正 AP を排除し、考えられる干渉源の影響を特定して軽減する必要があります。

無線の干渉

ワイヤレス環境に干渉源があると、エンドポイントの接続性やチャネル カバレッジが大幅に制限される可能性があります。また、物体や障害物があると、信号反射やマルチパス歪みが発生する可能性があります。マルチパス歪みが発生するのは、トラフィックまたはシグナリングが送信元から宛先に向かって複数の方向に進む場合です。一般に、トラフィックの一部は、残りの部分よりも先に宛先に到着します。そのため、場合によっては、遅延やビット エラーが発生する可能性があります。マルチパス歪みの影響を軽減するには、干渉源や障害物を排除または削減し、ダイバーシティ アンテナを使用してトラフィックを一度に受信するアンテナが 1 つだけになるようにします。実地調査中に干渉源を特定し、可能であれば排除する必要があります。少なくとも、干渉の影響を軽減するために、AP を適切に配置し、ロケーションに適した指向性の、または無指向性のダイバーシティ無線アンテナを使用する必要があります。

考えられる干渉源には、次のものがあります。

- オーバーラップ チャネル上にある他の AP
- 他の 2.4 GHz アプライアンス（2.4 GHz コードレス電話機、個人用ワイヤレス ネットワーク デバイス、硫黄プラズマ照明システム、電子レンジ、不正 AP および 2.4 GHz 帯域のライセンスフリーで動作する他の WLAN 機器など）
- 金属機器、構造物、およびその他の金属面や反射面（金属 I ビーム、ファイリング キャビネット、機器ラック、ワイヤー メッシュまたは金属壁、防火扉と防火壁、コンクリート、および冷暖房のダクトなど）
- 高出力の電気装置（変圧器、強力電気モーター、冷蔵庫、エレベータ、およびエレベータ機器など）

Bluetooth 対応デバイスは、802.11 b および g デバイスと同じ 2.4 GHz 無線帯域を使用するので、Bluetooth および 802.11 b または g デバイスが相互に干渉し、その結果接続に関する問題が起きる可能性があります。Bluetooth デバイスは 802.11 b および g WLAN 音声デバイスと干渉，妨害を引き起こす潜在的な可能性があるので（その結果，音声品質の低下，登録解除，およびコールセットアップ遅延

を引き起こす）、可能な場合には、すべての WLAN 音声デバイスを、5 GHz 無線帯域を使用する 802.11a に配置することを推奨します。ワイヤレス電話機を 802.11a 無線帯域に配置することで、Bluetooth デバイスによって引き起こされる干渉を回避できます。

WLAN 上のマルチキャスト

設計上、マルチキャストはユニキャストの確認応答レベルを備えていません。802.11 仕様に従って、アクセス ポイントは、次の Delivery Traffic Indicator Message（DTIM）周期に到達するまで、すべてのマルチキャスト パケットをバッファに入れる必要があります。DTIM 周期はビーコン周期の倍数です。ビーコン周期が 100 ms（通常のデフォルト）で DTIM 値が 2 の場合、アクセス ポイントは、バッファに入れられた単一のマルチキャスト パケットを転送する前に、最大 200 ms 待機する必要があります。ビーコン間の周期（DTIM 設定の積としての）は、バッテリ電源式デバイスによって、一時的に省電力モードに移行するために使用されます。この省電力モードは、デバイスがバッテリ電源を節約するのに役立ちます。

WLAN 上のマルチキャストは、管理者がバッテリの寿命要件に対するマルチキャスト トラフィックの品質要件を比較検討しなければならない二重の問題を提起します。第 1 に、マルチキャスト パケットの遅延は、特に、音声などのリアルタイム トラフィックをマルチキャストするアプリケーションに対して、マルチキャスト トラフィックの品質に悪影響を及ぼします。マルチキャスト トラフィックの遅延を制限するには、通常、DTIM 周期を 1 の値に設定して、マルチキャスト パケットがバッファに入れられる時間が、マルチキャスト トラフィックの配信で感知できる遅延を排除するために十分な低さになるようにする必要があります。ただし、DTIM 周期を 1 の値に設定することで、バッテリ電源式 WLAN デバイスが省電力モードに移行できる時間が短縮され、その結果、バッテリの寿命が短くなります。バッテリ電源を節約し、バッテリの寿命を長くするには、通常、DTIM 周期を 2 以上の値に設定する必要があります。

マルチキャスト アプリケーションまたはトラフィックが存在しない WLAN ネットワークでは、DTIM 周期を 2 以上の値に設定する必要があります。マルチキャスト アプリケーションが存在する WLAN ネットワークでは、可能な場合は常に、DTIM 周期を 2 の値に設定する必要があります。ただし、マルチキャスト トラフィックの品質が低下する場合、または許容できない遅延が発生する場合は、DTIM 値を 1 に下げる必要があります。DTIM 値が 1 に設定されている場合、管理者は、バッテリ駆動式デバイスのバッテリ寿命が大幅に短縮されることに注意する必要があります。

ワイヤレス ネットワーク上でマルチキャスト アプリケーションを有効にする前に、これらのアプリケーションをテストして、パフォーマンスや動作が許容できるレベルにあることを確認するよう推奨します。

マルチキャスト トラフィックを使用する場合の追加の考慮事項については、「メディア リソース」（P.17-1）を参照してください。

ワイヤレス AP の設定と設計

エンド ユーザに高品質の音声が提供されるように、ワイヤレス ネットワークが音声トラフィックを処理することを保証するには、AP を適切に選択、配置、および設定することが不可欠となります。

AP の選択

ワイヤレス音声用のアクセス ポイントの配置に関する推奨事項については、http://www.cisco.com/en/US/products/ps5678/Products_Sub_Category_Home.html にあるマニュアルを参照してください。

AP の配置

音声配置用に Cisco アクセス ポイント（AP）を使用するときは、いかなる場合も、15 ～ 25 を超えるデバイスを、単一の 802.11b または 802.11b/g AP に関連付けないことを推奨します。802.11a または 802.11a/g AP では、45 ～ 50 を超えるデバイスを、単一の AP に関連付けないことを推奨します。これらの数は、使用プロファイルおよび使用可能なデータ レートによって異なります。AP 上のデバイスの

数は、各デバイスがメディアにアクセスできる期間に影響します。デバイスの数が増加すると、トラフィックの競合も増加します。上記に指定された数を越えるデバイスを関連付けると、AP のパフォーマンスが低下し、関連付けられたデバイスの応答時間が遅くなる可能性があります。

限定された数のデバイスだけが単一の AP に関連付けられることを保証するメカニズムはありませんが、システム管理者は、定期的なサイト調査を行い、ユーザとデバイスのトラフィック パターンを分析することによって、デバイスと AP の割合を管理できます。追加のデバイスおよびユーザを特定の領域でネットワークに追加した場合は、追加のサイト調査を行い、ネットワークにアクセスする必要があるエンドポイントの数に対応するために追加の AP が必要かどうかを判断する必要があります。

AP の設定

ワイヤレス音声を配置する場合は、特定の AP 設定に関する次の要件に従います。

- Address Resolution Protocol（ARP; アドレス解決プロトコル）キャッシングを有効にする

  AP には ARP キャッシングが必要です。これは、ARP キャッシングを使用すると、AP がワイヤレス エンドポイント デバイスの ARP 要求に応答する際に、省電力モードまたはアイドル モードを終了するようエンドポイントに要求する必要がなくなるためです。この機能により、ワイヤレス エンドポイント デバイスのバッテリ寿命が長くなります。

- AP 上のダイナミック伝送パワー コントロール（DTPC）を有効にする

  これにより、AP 上の伝送パワーと音声エンドポイント上の伝送パワーの一致が保証されます。伝送パワーの一致により、片方向オーディオ トラフィックの可能性を排除できます。音声エンドポイントは、関連付けられた AP の Limit Client Power（mW）設定に基づいて伝送パワーを調整します。

- AP 上に設定されている各 VLAN に Service Set Identifier（SSID）を割り当てる

  SSID を使用すると、エンドポイントで、トラフィックの送受信に使用するワイヤレス VLAN を選択できます。このワイヤレス VLAN と SSID は、有線 VLAN にマッピングされます。音声エンドポイントでは、このマッピングにより、プライオリティ キューイング処理が行われること、および有線ネットワーク上の Voice VLAN にアクセスできることが保証されます。

- AP 上で **QoS Element for Wireless Phones** を有効にする

  この機能を使用すると、AP がビーコンで QoS Basic Service Set（QBSS）情報要素を提供することが保証されます。QBSS 要素は、AP でのチャネル使用率の推計を示します。また、QBSS 要素を使用することにより、Cisco ワイヤレス音声デバイスは、ローミングに関する決定を下し、負荷が高すぎる場合にコール試行を拒否できます。Cisco IOS Release 12.3(7)JA から、AP はビーコンで 802.11e Clear Channel Assessment（CCA）QBSS も提供するようになりました。CCA ベースの QBSS 値は、実際のチャネル使用率を反映したものになります。

- AP 上で 2 つの QoS ポリシーを設定して、VLAN とインターフェイスに割り当てる

  音声ポリシーとデータ ポリシーに各 VLAN のデフォルトの分類を設定することで、音声トラフィックがプライオリティ キューイング処理されることを保証します（詳細については、「インターフェイス キューイング」（P.3-62）を参照してください）。

WLAN の QoS

LAN および WAN 有線ネットワーク インフラストラクチャで高品質の音声を保証するために QoS が必要であるのと同様、ワイヤレス LAN インフラストラクチャでも QoS が必要です。データ トラフィックにはバースト性があり、音声などのリアルタイム トラフィックはパケット損失や遅延の影響を受けやすいため、ワイヤレス LAN バッファを管理し、無線の衝突を制限し、パケット損失、遅延、および遅延変動を最小限に抑えるには、QoS ツールが必要です。

ただし、ほとんどの有線ネットワークとは異なり、ワイヤレス ネットワークは共有メディアです。また、ワイヤレス エンドポイントにはトラフィックを送受信するための専用帯域幅がありません。ワイヤレス エンドポイントでは、トラフィックを 802.1p CoS、DSCP、および PHB でマークできますが、ワイヤレス ネットワークには共有性があるため、このエンドポイントでは、アドミッション制御とネットワーク アクセスが制限されます。

ワイヤレス QoS には、次の主要な設定領域があります。

- 「トラフィック分類」（P.3-62）
- 「インターフェイス キューイング」（P.3-62）
- 「帯域幅のプロビジョニング」（P.3-63）

トラフィック分類

有線ネットワーク インフラストラクチャの場合と同様、できるだけネットワークのエッジの近くで適切なワイヤレス トラフィックを分類またはマークすることが重要です。トラフィック マーキングは、有線およびワイヤレス ネットワーク全体でキューイング方式の入力基準となるため、マーキングはできるだけワイヤレス エンドポイントで行われる必要があります。ワイヤレス ネットワーク デバイスによるマーキングまたは分類は、有線ネットワーク デバイスの場合（表 3-3 を参照）と同じである必要があります。

Cisco Wireless IP Phone は、有線ネットワークのトラフィック分類ガイドラインに従って、音声メディア トラフィックまたは RTP トラフィックを DSCP 46（または PHB EF）でマークし、音声シグナリング トラフィック（SCCP）を DSCP 24（または PHB CS3）でマークします。このトラフィックをマークしたら、ネットワーク全体でプライオリティ処理およびキューイング、またはベストエフォート型よりも優れた処理およびキューイングを行うことができます。ワイヤレス音声デバイスはすべて、この方法でトラフィックをマークできる必要があります。ワイヤレス ネットワーク上の他のトラフィックはすべて、ベストエフォート型としてマークされるか、有線ネットワークのマーキング ガイドラインで規定されているいくつかの中間分類を使用してマークされる必要があります。

インターフェイス キューイング

マーキングが行われたら、有線ネットワークの AP およびデバイスが QoS キューイングを実行できるようにする必要があります。これにより、音声のトラフィック タイプに別のキューが割り当てられるため、このトラフィックがワイヤレス LAN を通過するときにドロップまたは遅延する可能性が低くなります。ワイヤレス ネットワーク上のキューイングは、アップストリームとダウンストリームの 2 つの方向で行われます。アップストリーム キューイングは、ワイヤレス エンドポイントから AP に向かって移動するトラフィックと、AP から有線ネットワークに向かって移動するトラフィックを対象とします。ダウンストリーム キューイングは、有線ネットワークから AP に向かって移動するトラフィックと、AP からワイヤレス エンドポイントに向かって移動するトラフィックを対象とします。

アップストリーム キューイングでは、Wi-Fi Multimedia（WMM）をサポートするデバイスは、プライオリティ キューイングなどのキューイング メカニズムを利用できます。

ダウンストリーム QoS に関しては、Cisco AP は現在、ワイヤレス クライアントに送信されているダウンストリーム トラフィックに対して最大 8 つのキューを割り当てることができます。これらのキューへの入力基準は、DSCP、Access Control List（ACL; アクセス コントロール リスト）、および VLAN などの要素の数に基づいて設定できます。8 つのキューが使用可能ですが、ワイヤレス音声を配置する場合は 2 つのキューだけを使用することを推奨します。音声メディアとシグナリング トラフィックはすべて、最高レベルのプライオリティ キューに入り、他のトラフィックはすべて、ベストエフォート型キューに入る必要があります。これにより、音声トラフィックが最適にキューイング処理されることが保証されます。

この 2 つのキューを自律分散型 AP に対して設定するには、AP 上に 2 つの QoS ポリシーを作成します。1 つめのポリシーには Voice という名前を付け、VLAN のすべてのパケットに対するデフォルトの分類として **Voice < 10 ms Latency (6)** サービス クラスを設定します。2 つめのポリシーには Data という名前を付け、VLAN のすべてのパケットに対するデフォルトの分類として **Best Effort (0)** サービス クラスを設定します。次に、Data ポリシーをデータ VLAN の着信および発信無線インターフェイスに割り当て、Voice ポリシーを Voice VLAN の着信および発信無線インターフェイスに割り当てます。QoS ポリシーを VLAN レベルで適用すると、AP が着信または発信するすべてのパケットを検査して、パケットに適用する必要があるキューイングのタイプを判別することはなくなります。

Lightweight AP では、WLAN コントローラは、同じキューイング ポリシーを提供できる組み込み QoS プロファイルを備えています。音声 VLAN または音声トラフィックは、音声キューにプライオリティ キューイングを設定する、**Platinum** ポリシーを使用するように設定されます。データ VLAN またはデータ トラフィックは、データ キューにベストエフォート型キューイングを設定する、**Silver** ポリシーを使用するように設定されます。次に、これらのポリシーは、VLAN に基づいて着信および発信無線インターフェイスに割り当てられます。

上記のように設定すると、ダウンストリーム方向のすべての音声メディアおよびシグナリングがプライオリティ キューイング処理されることが保証されます。

帯域幅のプロビジョニング

シスコでは、ワイヤレス音声ネットワークのテストに基づいて、802.11b クライアントを持つデータ レート 11 Mbps の 802.11b 専用 AP では、最大 7 つのアクティブな G.711 音声ストリームまたは 8 つの G.729 音声ストリームをサポートできることを確認しています。AP レートが 11 Mbps より低く設定されている場合、各 AP のコール キャパシティが低下します。

54 Mbps のデータ レートの 802.11a では、アクティブな音声ストリームの最大数は AP ごとに 14 ～ 18 に増加します。

54 Mbps のデータ レートの 802.11g 環境の場合、理論上のアクティブ音声ストリームの最大数も、AP あたり 14 ～ 18 に増加します。ただし、大部分の 802.11g 環境は、802.11b クライアント（したがって、11 Mbps のデータレート）および 802.11g クライアントを含む混在環境なので、AP ごとに 8 ～ 12 のアクティブな音声ストリームが含まれ、通常、キャパシティは大幅に低下します。

（注） 同じ AP に関連付けられた 2 台の電話機間のコールは、2 つのアクティブ音声ストリームとしてカウントされます。

これらの制限を超えないようにするには、いくつかのコール アドミッション制御の形式が必要になります。Cisco AP およびワイヤレス音声クライアントには、コール アドミッション制御に使用される 2 つのメカニズムがあります。

- QoS Basic Service Set（QBSS）

  QBSS はビーコン情報要素であり、この情報要素により、AP はワイヤレス IP 電話機にチャネル使用率情報を送信します。この QBSS 値は、ワイヤレス電話機が他の AP にローミングするかどうかを判別するのに役立ちます。QBSS 値が低いと、その AP がローミング先として適切な候補であることを示し、QBSS 値が高いと、デバイスがその AP にローミングするべきでないことを示しています。この QBSS 情報は便利ですが、コールが適切な QoS を保持することを保障するものではなく、またコールを処理するのに十分な帯域幅が存在することを保証するものではないため、真のコール アドミッション制御メカニズムではありません。Cisco Unified Wireless IP Phone が、高い QBSS を持つ AP に関連付けられている場合、AP は、コールのセットアップを拒否し、発信側のデバイスに Network Busy メッセージを送信することにより、コールが開始または受信されるのを防止します。しかし、ワイヤレス IP Phone と別のエンドポイントの間でコールがセットアップされた後は、電話機が、高い QBSS を持つ AP にローミングして関連付けを行うことができ、それによりその AP で使用可能な帯域幅のオーバーサブスクリプションが発生する場合があります。

- Wi-Fi Multimedia Traffic Specification（WMM TSPEC）

  WMM TSPEC は QoS メカニズムであり、このメカニズムによって、WLAN クライアントはその帯域幅と QoS 要件を通知して、AP がその要件に対応できるようにします。クライアントが電話を掛けようと準備する場合、クライアントは TSPEC を示す Add Traffic Stream（ADDTS）メッセージを，関連付けられた AP に送信します。次に、AP は、帯域幅とプライオリティ処理が使用できるかどうかに応じて、ADDTS 要求を受け入れるかまたは拒否します。コールが拒否された場合、電話機は Network Busy メッセージを受信します。ローミング中、TSPEC をサポートしている通話中のクライアントは、ADDTS メッセージを新しい AP にアソシエーション プロセス の一部として送信して、プライオリティ処理に使用可能な帯域幅を確保します。十分な帯域幅がない場合、ローミングは、隣接する AP が使用可能であれば、それにロードバランスされます。

Cisco Unified Wireless IP Phone 7921G および 7925G は、QBSS と TSPEC の両方をサポートしています（TSPEC は QBSS より優先されます）。したがって、Cisco Unified Wireless IP Phone 7921G または 7925G でのコール アドミッション制御は、TSPEC を使用する場合、より正確になり、AP のコール キャパシティを超過する可能性を排除できます。

（注）　Cisco IOS Release 12.3(7)JA から、AP は 802.11e CCA ベースの QBSS を送信するようになりました。これらの QBSS 値は、特定の AP の実際のチャネル使用率を表します。

QBSS 情報要素が AP から送信されるのは、AP 上で **QoS Element for Wireless Phones** が有効になっている場合だけです（「ワイヤレス AP の設定と設計」（P.3-60）を参照）。

Service Advertisement Framework（SAF）

Cisco Service Advertisement Framework（SAF）を使用すると、ネットワーク アプリケーションで IP ネットワーク内のネットワーク サービスに関する情報をアドバタイズしたり検出したりできます。SAF は、次の機能コンポーネントおよびプロトコルで構成されています。

- SAF クライアントは、サービスに関する情報をアドバタイズしたり消費したりします。
- SAF フォワーダは、SAF サービスの可用性情報を配布したり維持したりします。
- SAF クライアント プロトコルは、SAF クライアントと SAF フォワーダ間で使用されます。
- SAF フォワーダ プロトコルは、SAF フォワーダ間で使用されます。

アドバタイズされたサービスの特性は、SAF フォワーダのネットワークにとって重要ではありません。SAF フォワーダ プロトコルは、サービスの可用性に関する情報を、SAF ネットワークに登録されている SAF クライアント アプリケーションに動的に配布するように設計されています。

SAF でアドバタイズできるサービス

理論上は、どのサービスでも SAF を介してアドバタイズできます。SAF を使用する最も重要なサービスは、Cisco Unified Communications の Call Control Discovery（CCD; コール制御ディスカバリ）です。CCD は SAF を使用して、Cisco Unified CM、Unified CME などの呼制御エージェントによってホストされる内部 Directory Number（DN; ディレクトリ番号）の可用性に関する情報を配布および維持します。また、CCD は、これらの内部ディレクトリ番号に公衆網から到達できるようにする対応した番号プレフィックスも配布します（「To PSTN」プレフィックス）。

SAF の動的な特性、およびコール エージェントがホストする DN 範囲と To PSTN プレフィックスの可用性を SAF ネットワーク内の他のコール エージェントにアドバタイズできることにより、静的でより労働集約的な他のダイヤル プラン配布方式を大幅に上回るメリットを提供します。SAF CCD の詳細については、「Service Advertisement Framework のコール制御ディスカバリを使用したコール ルーティングおよびダイヤル プラン配信」（P.5-66）を参照してください。

SAF ネットワーク

SAF ネットワークには、次の項で説明するように、多数の機能コンポーネントが含まれています。

SAF フォワーダ、SAF クライアント、および非 SAF ネットワーク

Cisco SAF ネットワークでは、サービス情報は、サービスに関する知識を効率的に配布して検出を容易にする特定の機能を想定した SAF 対応ノードのネットワークを介して配布されます。Cisco SAF ネットワーク ノードは、次の 2 つの機能的役割に分類されます。

- SAF フォワーダ
- SAF クライアント

Cisco SAF ネットワークを設定するには、SAF フォワーダと SAF クライアントの両方を設定する必要があります。Cisco SAF が備えている柔軟性により、必要に応じて、Cisco SAF フォワーダおよび Cisco SAF クライアントとして動作するように単一のエッジ ルータを設定できます。

SAF フォワーダをサポートしているプラットフォームは、次のとおりです。

- Cisco IOS Release 15.0(1)M を搭載した Cisco Integrated Services Routers（ISR; サービス統合型ルータ）、ISR Generation 2（ISR G2）、および 7200 シリーズ ルータ（http://wwwin.cisco.com/ios/release/15mt を参照）
- Cisco IOS Release 12.2(33)SRE を搭載した Cisco 7600 シリーズ ルータ
- Cisco IOS Release 12.2XE 2.5.0 (RLS5) を搭載した Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ

SAF クライアントをサポートしているプラットフォームは、次のとおりです。

- Cisco IOS Release 15.0(1)M を搭載した Cisco Integrated Services Routers（ISR; サービス統合型ルータ）および ISR Generation 2（ISR G2）（http://wwwin.cisco.com/ios/release/15mt を参照）
- Cisco Unified Communications Manager 8.0(1) 以降のバージョン

Cisco SAF フォワーダ

SAF フォワーダは Cisco IOS ルータ上で稼動します。Cisco SAF フォワーダは、Cisco SAF クライアントによってアドバタイズされたサービスを受信し、SAF フォワーダのネットワークを通じてサービスを確実に配布して、Cisco SAF クライアントがサービスを使用できるようにします。

Cisco SAF フォワーダは IP マルチキャストを使用して、LAN 上の他の Cisco SAF フォワーダを自動的に検出し、ピアとして通信します。IP マルチキャストをサポートしていないネットワークでは、SAF フォワーダは、SAF ネイバーとの間にユニキャストのポイントツーポイントの隣接関係を構築することで、ピアとして静的に接続できます。

ネットワーク内で SAF を有効にするために必要なことは、ルータのサブセットを SAF フォワーダとして設定することだけです。SAF フォワーダ間にピア関係が作成されると、SAF フォワーダ間で交換される TCP/IP ベースの SAF メッセージは、どの IP ネットワークでも通過できるようになります。非 SAF ルータと SAF ルータのネットワークでは、任意の IP ルーティング プロトコルを実行できます。

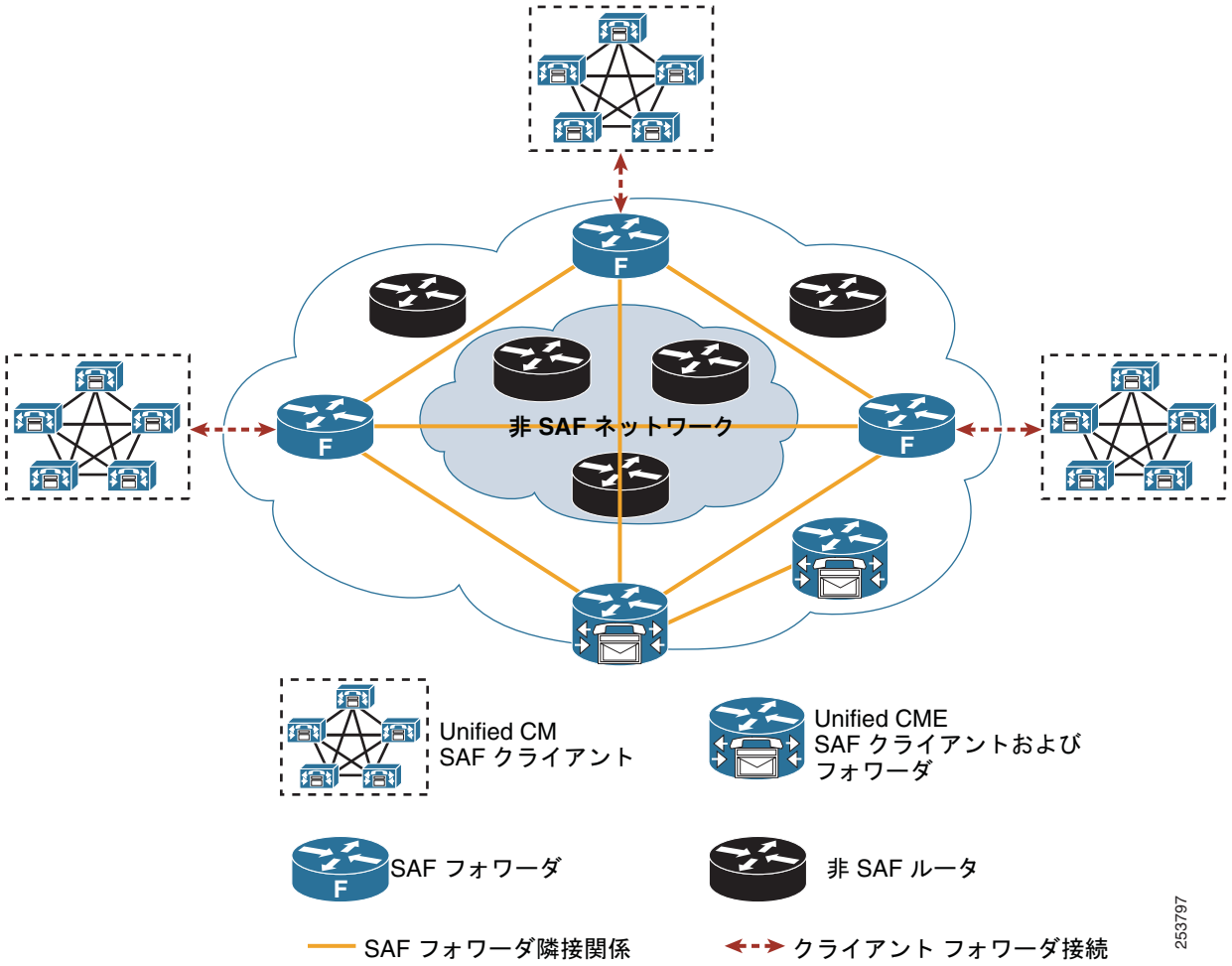
SAF Forwarder Protocol（SAF-FP; SAF フォワーダ プロトコル）は、IP ルーティング プロトコルではなく、「サービス」ルーティング プロトコルです。SAF フォワーダ プロトコルは、サービスに関する情報を IP ネットワークでルーティングします。SAF-FP は、EIGRP テクノロジーに基づくものであり、歴史的に EIGRP ベースの IP ルーティング用に開発されてきた機能の多くを利用して、サービス情報の配布にこの機能を適用します。

SAF フォワーダ プロトコルには、次の特性があります。

- DUAL アルゴリズムおよびスプリット ホライズン ルールを使用して、ルーティング ループが発生しないようにする。
- 定期的なブロードキャストを送信しないで、変更が発生した場合にだけ更新を送信する。
- キープアライブ メカニズムを使用して、ピア SAF フォワーダの可用性を追跡する。
- スケーラブルであり、SAF フォワーダでの障害発生時に迅速なコンバージェンスを提供する。
- SAF ピア（ネイバー）認証方式を提供する。

Cisco SAF フォワーダは、Cisco SAF クライアントと SAF ネットワーク間の関係の基礎を提供します。Cisco SAF フォワーダはネットワーク内の任意の場所に設置できますが、通常はネットワークの端、つまり境界に配置します（図 3-18 を参照）。クライアント/フォワーダの関係は、アドバタイズされる各サービスの状態を維持するために使用されます。クライアントがサービスを削除するか、またはフォワーダ ノードから切り離した場合、ノードは、使用できなくなったサービスについて SAF ネットワークに通知します。SAF フォワーダ ノードが他のフォワーダ ノードからアドバタイズメントを受信すると、アドバタイズメント全体のコピーを作成してから、他の SAF ピアに転送します。

図 3-18　SAF クライアント、SAF フォワーダ、および非 SAF ネットワーク間の隣接関係



Cisco SAF クライアントの概要

Cisco SAF クライアントは、サービスの作成者（サービスを SAF ネットワークにアドバタイズする）、サービスの消費者（SAF ネットワークの 1 つ以上のサービスを要求する）、またはその両方になることができます。SAF クライアントは、次の 3 つの基本機能を実行します。

- SAF ネットワークへの登録
- サービスのパブリッシュ
- サービスへのサブスクライブ

SAF クライアントは、次の 2 つの形式を使用します（図 3-19 を参照）。

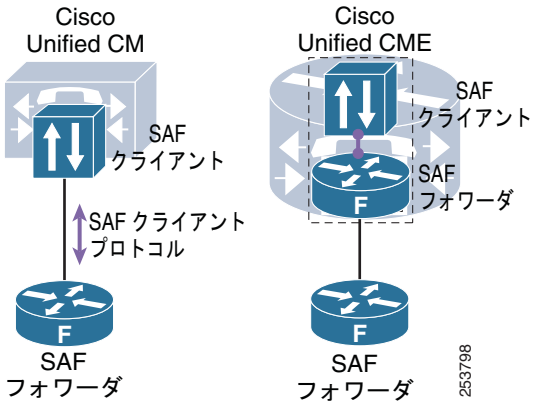
- 内部 SAF クライアント

  内部 SAF クライアントは、SAF フォワーダと同じ Cisco IOS プラットフォームに配置されます。クライアント/フォワーダ接続は、インターネット Application Programming Interface（API; アプリケーション プログラミング インターフェイス）を介して確立されます。Cisco Unified Communications Manager Express（Unified CME）など、Cisco IOS に配置されている呼制御アプリケーションは、内部 SAF クライアントを使用して、共存する内部 SAF フォワーダに接続できます。

- 外部 SAF クライアント

  外部 SAF クライアントは Cisco IOS 内には配置されず、SAF Client Protocol（SAF-CP; SAF クライアント プロトコル）を使用して Cisco IOS ベースの SAF フォワーダと通信します。Cisco Unified CM によって使用される SAF クライアントなどの外部 Cisco SAF クライアントは、設定済みの IP アドレスおよびポート番号を使用して Cisco SAF フォワーダへの TCP/IP 接続を開始します。

図 3-19　　外部および内部 SAF クライアントと SAF フォワーダ



クライアントとフォワーダ間の接続が確立されると、Cisco SAF クライアントは Cisco SAF フォワーダに登録メッセージを送信します。この登録メッセージは、ハンドル（「クライアント ラベル」と呼ばれる）を使用して、Cisco SAF フォワーダに接続されている他のすべての Cisco SAF クライアントから、その Cisco SAF クライアントを一意に識別します。Cisco SAF クライアントが SAF フォワーダへの登録を完了すると、SAF ネットワークにサービスをアドバタイズ（パブリッシュ）したり、SAF ネットワークのサービスを要求（サブスクライブ）したりできるようになります。

サービスをアドバタイズする場合、Cisco SAF クライアントは、提供されるサービスの詳細を含むアドバタイズメントを Cisco SAF フォワーダにパブリッシュ（送信）します。Cisco SAF クライアントは、それぞれに異なるサービスをアドバタイズする複数のパブリッシュ要求を送信できます。Cisco SAF フォワーダは、Cisco SAF クライアントによってパブリッシュされたすべてのサービスをアドバタイズします。

サービスを要求する場合、Cisco SAF クライアントはサブスクライブ要求をフォワーダに送信します。サブスクライブ要求には、Cisco SAF クライアントの目的のサービス セットを表すフィルタが含まれています。この要求に応えて、Cisco SAF フォワーダは、フィルタに一致する現在のサービス セットを一連の通知要求で Cisco SAF クライアントに送信します。フロー制御を提供するために複数の通知要求が送信されるため、Cisco SAF クライアントは、Cisco SAF フォワーダが次の要求を送信する前に、それぞれの通知要求に応答する必要があります。パブリッシュ要求と同様に、Cisco SAF クライアントは、それぞれに異なるフィルタが含まれた複数のサブスクライブ要求を生成できます。また、Cisco SAF クライアントは、既存のサブスクリプションの 1 つを削除するサブスクライブ解除要求も生成できます。

Cisco 外部 SAF クライアントおよび SAF フォワーダとの相互作用

クライアント/フォワーダ認証

外部 SAF クライアントと SAF フォワーダ間での TCP/IP 接続の確立時に、ユーザ名およびパスワードを含む共有秘密キーが認証に使用されます。ユーザ名は、共有秘密キーとして使用するパスワードを決定するためのインデックスとして使用されます。Cisco SAF クライアントは要求を送信するときに、そのユーザ名、実際のメッセージ内容、およびパスワードの MD5 ハッシュを含む属性を送信します。Cisco SAF フォワーダは要求を受信すると、ユーザ名属性を探し、そのユーザ名属性を使用してパスワードのローカル コピーにアクセスします。続いて、ローカルに格納されているパスワードの MD5 ハッシュを計算します。パスワードが一致すると、Cisco SAF クライアントは認証され、接続が続行されます。ただし、Cisco SAF フォワーダが要求を拒否することもあります。

クライアント/フォワーダ キープアライブ

SAF クライアントが SAF ネットワークにサービスをパブリッシュすると、Cisco SAF フォワーダはキープアライブ メカニズムを使用して、Cisco SAF クライアントのステータスを追跡します。Cisco SAF フォワーダおよび Cisco SAF クライアントは、登録時にキープアライブ タイマー値を交換します。Cisco SAF フォワーダは、キープアライブ タイマー値と等しい時間内に Cisco SAF クライアントからの要求が確認されなかった場合、Cisco SAF クライアントで障害が発生したと見なします。Cisco SAF クライアントは、要求間の間隔がこの値を超えないようにします。Cisco SAF クライアントに送信するデータがない場合は、タイマーをリフレッシュする登録メッセージを生成します。

Cisco SAF クライアントで障害が発生したことを Cisco SAF フォワーダが検出すると、その Cisco SAF クライアントの代わりに、アドバタイズされたサービスをネットワークから削除して、Cisco SAF クライアントが確立したすべてのサブスクリプションを抹消します。Cisco SAF クライアントを手動で登録解除して、Cisco SAF フォワーダにすべてのサービスおよびサブスクリプションを適切に削除させることができます。

SAF フォワーダの配置オプション

Unified Communications ネットワークで SAF を有効にするには、1 つ以上の SAF フォワーダを Unified Communications ネットワークに追加する必要があります。Unified CME などの Cisco IOS 呼制御アプリケーションの場合、SAF クライアントとフォワーダをルータ上に共存させて、SAF ネットワーク内の他の SAF フォワーダとの相互接続に使用できます。Unified CM など、外部 SAF クライアントを使用する非 IOS の呼制御アプリケーションは、Unified Communications ネットワーク内に設定されている Cisco IOS SAF フォワーダに接続する必要があります。呼制御アプリケーションと共存しない SAF フォワーダは、ネットワーク内の任意の場所に配置できます。これらのフォワーダの数および場所は、SAF ネットワーク内で必要な復元性および冗長性の程度に大きく依存します。冗長性を提供するには、2 つ以上の SAF フォワーダが必要です（図 3-20 を参照）。SAF ネットワークにさらに SAF フォワーダを追加すると、Unified CM クラスタの各グループに、追加の冗長性およびローカルの SAF フォワーダ リソースを提供できます（図 3-21 を参照）。Cisco ISR および 7200 シリーズ ルータで稼動している Cisco IOS Release 15.0(1) 用の初期バージョンの SAF では、最大 50 台のクライアントを単一の SAF フォワーダに接続できます。

図 3-20　2 つの専用 SAF フォワーダと 2 つの Unified CME SAF フォワーダを使用した SAF ネットワーク

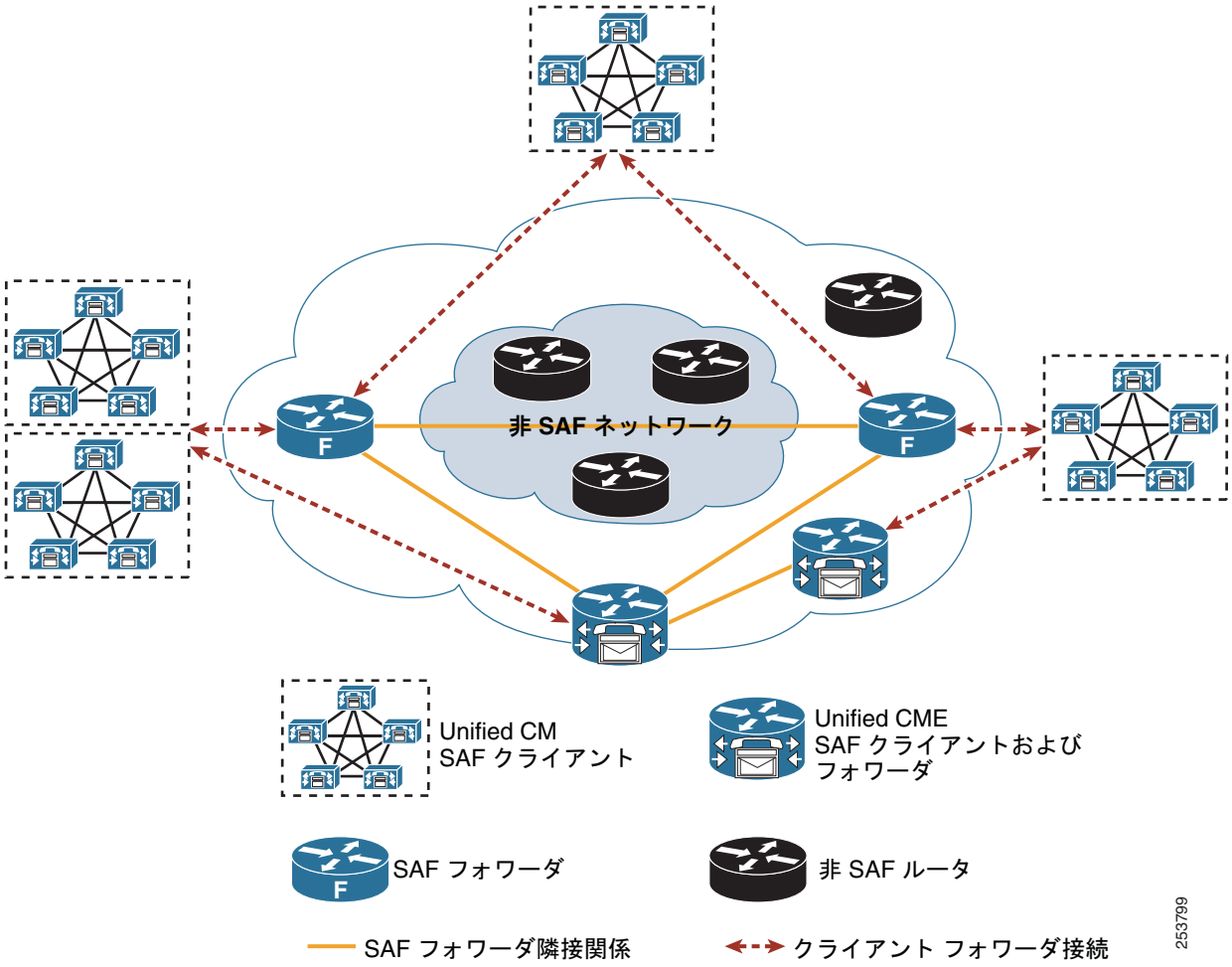
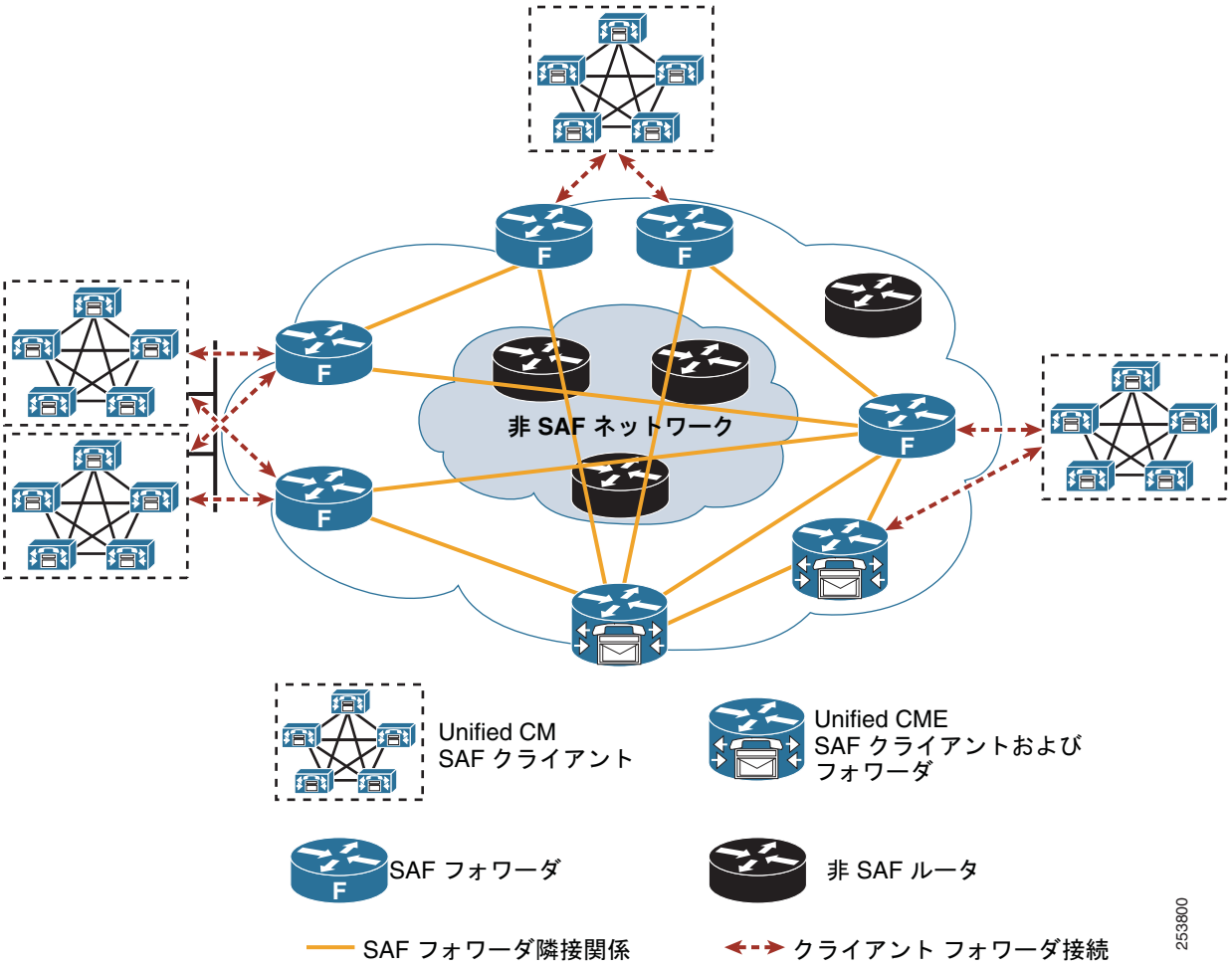


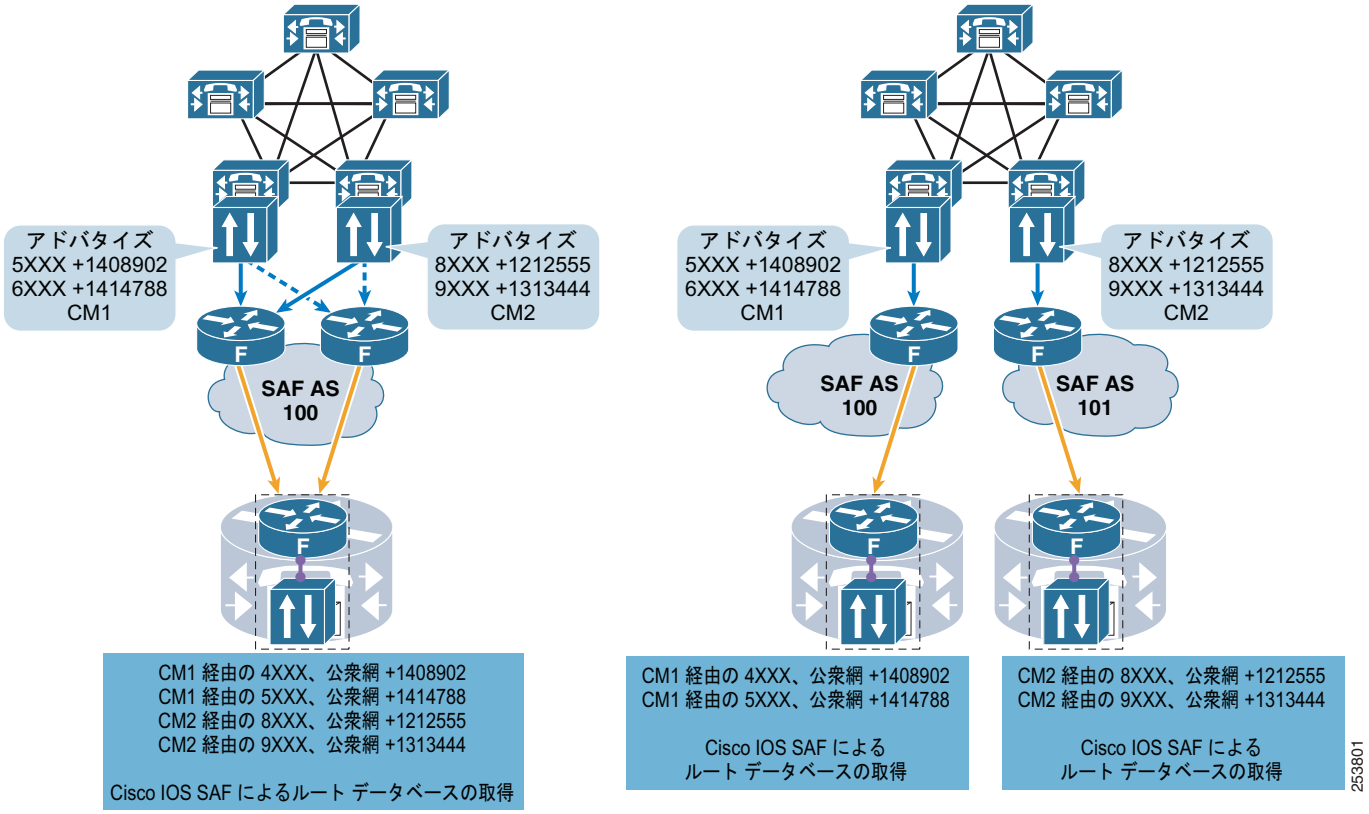
図 3-21　複数の冗長専用 SAF フォワーダと 2 つの Unified CME SAF フォワーダを使用した SAF ネットワーク



SAF 自律システム

IP ルーティング プロトコルと同様に、SAF は Autonomous System（AS; 自律システム）の概念を使用して、SAF ネットワークとその SAF ネットワーク内の共通 SAF フォワーダの境界を定義します（図 3-22 を参照）。大部分の SAF 展開では単一の SAF AS だけが必要ですが、場合によっては（SAF サービスの分離が必要な場合など）、複数の SAF AS を展開することもあります。外部 SAF クライアントは、それぞれに単一の SAF AS に接続してパブリッシュできます。Unified CM クラスタに複数の外部 SAF クライアントを配置している場合、クラスタは複数の SAF AS にサービスをパブリッシュして、各 AS からアドバタイズメントを受信できます。内部 SAF クライアントは、任意の数の Cisco IOS 共存 SAF AS に対してパブリッシュおよびサブスクライブを実行できます。SAF AS 間の SAF サービスの再配送は、現在は使用できません。

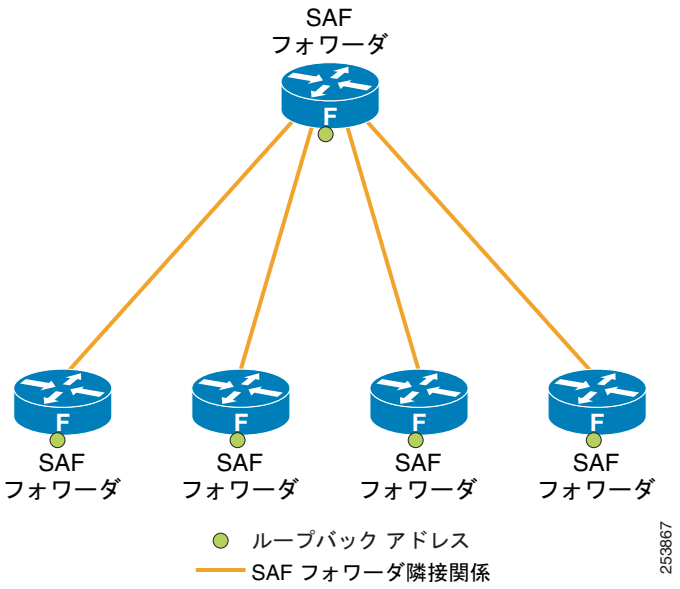
図 3-22　SAF 自律システム



SAF フォワーダのループバック アドレスおよびスプリット ホライズン

図 3-23 のように、ループバック アドレスを SAF フォワーダの設定で使用すると、スプリット ホライズン ルールが有効になり、セントラル SAF フォワーダはスポーク フォワーダ間でアドバタイズメントを転送しません。セントラル SAF フォワーダがスポーク フォワーダ間でアドバタイズメントを転送できるようにするには（これによって SAF ピアのフル メッシュを設定する必要をなくすには）、セントラル SAF フォワーダのループバック インターフェイスで **no split horizon** コマンドを使用します。

図 3-23　SAF およびスプリット ホライズン



Cisco IOS SAF 設定の詳細については、次の Web サイトで入手可能な『*Cisco IOS Service Advertisement Framework Configuration Guide*』を参照してください。

http://www.cisco.com/en/US/docs/ios/saf/configuration/guide/15_0/saf_15_0_book.html