CHAPTER 3

ネットワーク インフラストラクチャ

この章では、企業の環境で IP テレフォニー 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デバイスの役割を示し、表 3-1 では、それらの役割のサポートに必要な機能を示しています。

IP テレフォニーは、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、厳しい要件を課します。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。

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

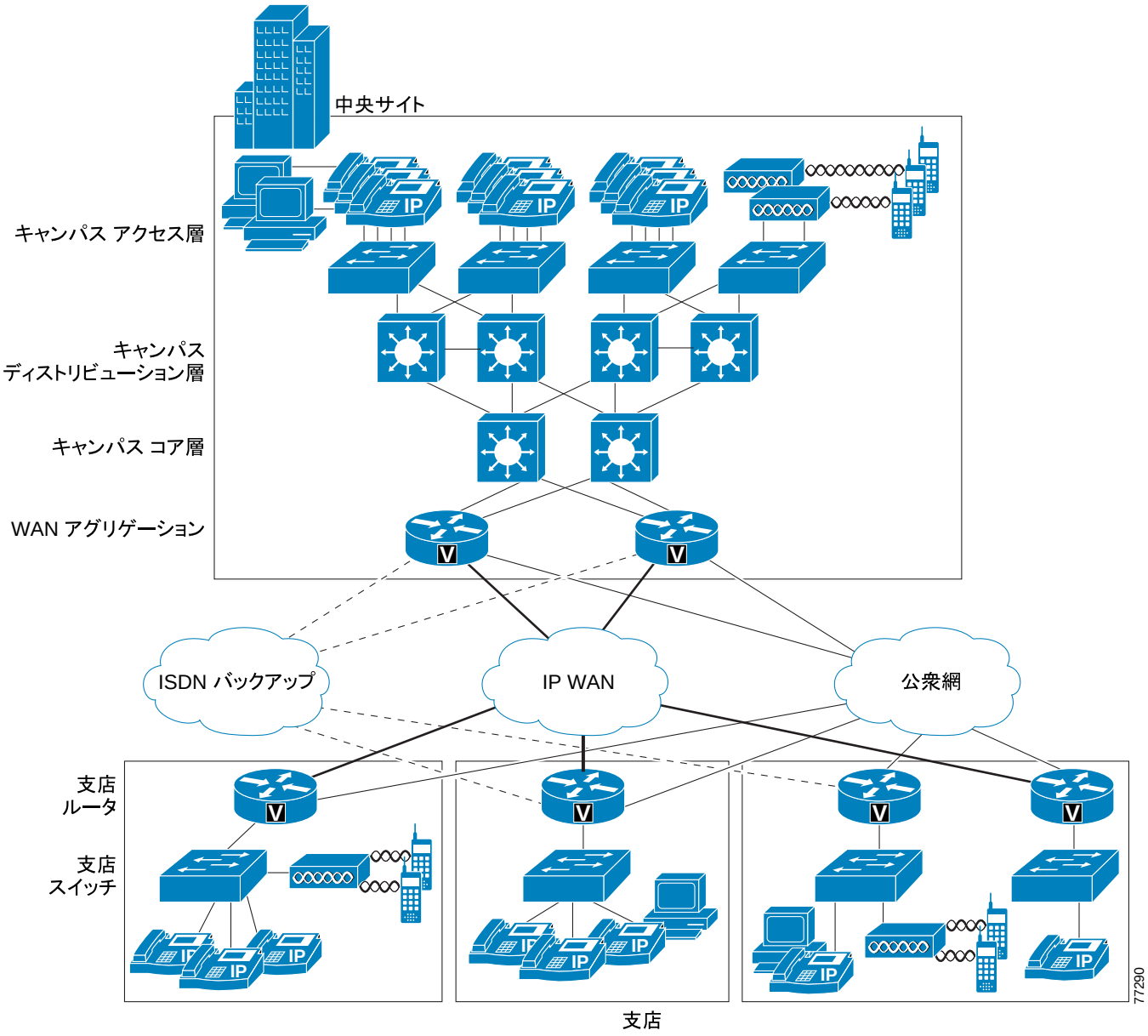


表 3-1　ネットワーク インフラストラクチャ内の役割に必要な機能

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 • 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 • LFI（Link Fragmentation and Interleaving） • リンク効率 • 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 • リンク効率 • 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 • 複数キュー サポート • 802.1p および 802.1Q

LAN インフラストラクチャ

統合されたネットワーク上で IP テレフォニー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きわめて重要です。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。

高可用性のための 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たら、追加のネットワーク機能を提供する、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。

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

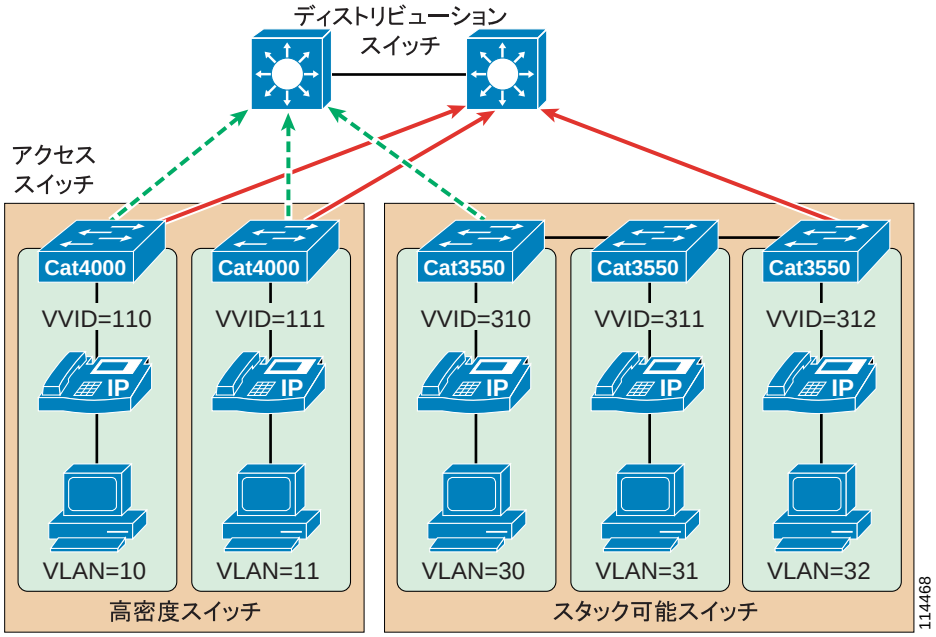
http://www.cisco.com/warp/public/cc/so/neso/lnso/cpso/gcnd_wp.pdf

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（複数可）からワイヤリング クローゼット スイッチまでです。

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、VLAN が存在するアクセス レイヤ スイッチは 1 つのみ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。アクセス レイヤ スイッチに RSTP、MISTP、またはその両方が設定可能で、実際に設定されている場合は、トポロジ上のループについて考慮する必要がありません。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 ほどに制限することをお勧めします。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。一般的なアクセス レイヤ スイッチには、スタック可能な Cisco Catalyst 2950、3500XL、3550、および 3750 のほか、より大規模で高密度な Catalyst 4000 および 6000 スイッチがあります。

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お勧めします。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 を分離することをお勧めします。

- 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必要があります。

- QoS 信頼性境界の音声デバイスへの拡張

  音声デバイスの信頼性境界を拡張することなく、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 デバイスに拡張することができます。

- 悪質なネットワーク攻撃からの保護

  VLAN アクセス制御、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、DoS 攻撃（サービス拒絶攻撃）、およびデータ デバイスがパケット タギングを介してプライオリティ 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お勧めします）
- 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（これらの機能が必要になるのは、SoftPhone 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 IP テレフォニー 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 のフォールト トレランス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）には転送されなくなります。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高可用性を提供することが保証されます。Catalyst 2950、3550、または 3750 など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のみに流れている場所を検出し、サービスを落として、リンクします。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。

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。また、このレイヤは LAN におけるレイヤ 2 からレイヤ 3 への最初のトラバーサルとなります。ディストリビューション レイヤ スイッチには、一般に、レイヤ 3 対応の Catalyst 4000 および 6000 スイッチと、より小規模な配置向けの Catalyst 3750 があります。

ディストリビューション レイヤでは、冗長性を確保して高可用性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。

ホットスタンバイ ルータ プロトコル（HSRP）

すべてのルータが冗長になっていること、および障害発生時に別のルータが処理を引き継げることを保証するには、ディストリビューション レイヤで HSRP も有効にする必要があります。HSRP の設定には、次のコマンドを含める必要があります。

- standby track

  standby track コマンドは、HSRP で特定のインターフェイス（複数可）をモニタリングすることを示します。インターフェイスがダウンした場合は、そのルータの HSRP プライオリティが低下し、別のデバイスへのフェールオーバーが発生します。このコマンドは、**standby preempt** コマンドと組み合せて使用されます。

- standby preempt

  このコマンドを使用すると、スタンバイ グループにおいて、HSRP が設定されたデバイスの中で特定のデバイスのプライオリティが最も高くなったときに、そのデバイスが HSRP スタンバイ アドレスのアクティブ レイヤ 3 ルータとして処理を引き継ぐことが保証されます。

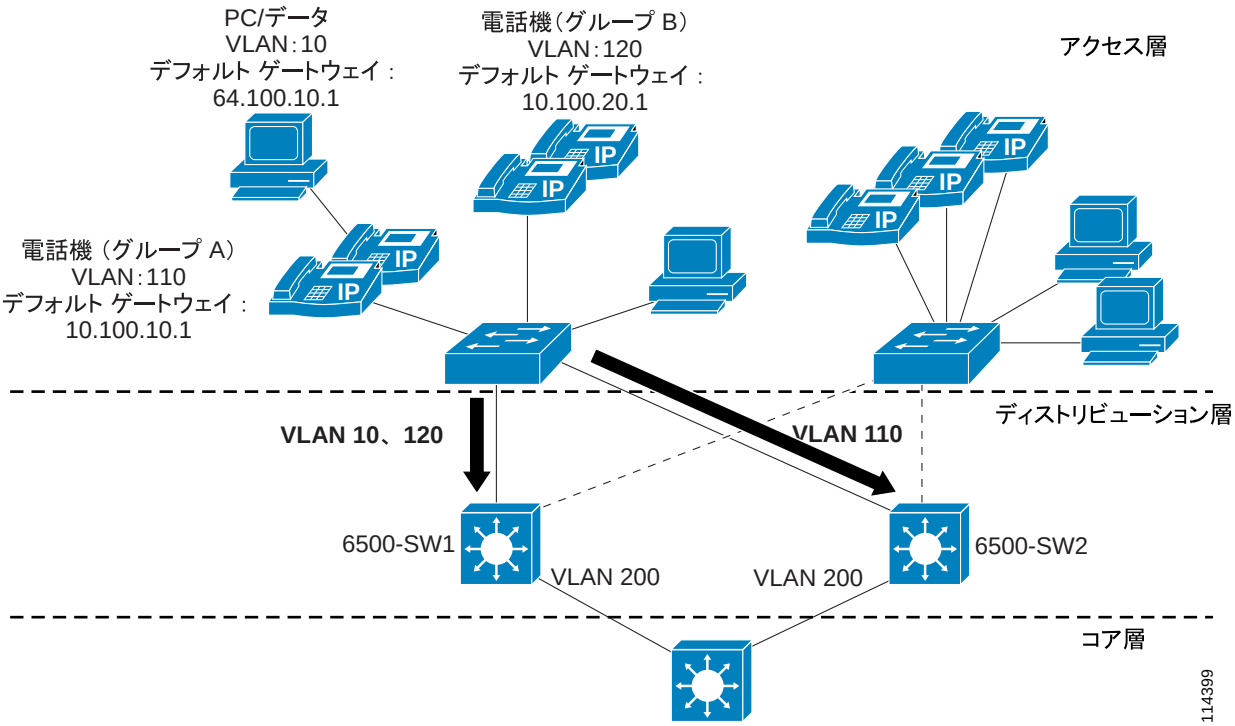
また、HSRP には、両方の HSRP ルータ間でトラフィックをロード バランシングするように設定する必要があります。ロード バランシングを行うには、アクティブ HSRP ルータである各 HSRP デバイスを 1 つの VLAN またはインターフェイス用に設定し、スタンバイ ルータを別の VLAN またはインターフェイス用に設定します。両方の HSRP デバイスにアクティブ VLAN とスタンバイ VLAN を均等に分散させると、ロード バランシングが保証されます。1 つの VLAN 上のデバイスは、アクティブ HSRP デバイスをそのデフォルト ゲートウェイとして使用し、別の VLAN 上のデバイスは、同じ HSRP デバイスを、もう一方の HSRP デバイスに障害が発生した場合にのみスタンバイ デフォルト ゲートウェイとして使用します。このタイプの設定では、すべてのネットワーク トラフィックが単一のアクティブ ルータに送信されることが防止されるため、その他の HSRP デバイスへロード バランシングされるようになります。

図 3-3 は、HSRP 対応のネットワークの例を示しています。この図では、2 つの Catalyst 6500 スイッチ（6500-SW1 と 6500-SW2）に複数の VLAN インターフェイスが設定されています。ネットワーク内にリンク障害がないことを前提とすると、6500-SW1 は、VLAN 110（Group A の電話機の Voice VLAN）に対応するスタンバイ HSRP ルータであり、VLAN 10（データ VLAN）および VLAN 120（Group B の電話機の Voice VLAN）に対応するアクティブ HSRP ルータになっています。6500-SW2 は、その逆に設定されています。つまり、VLAN 110 に対応するアクティブ HSRP ルータであり、VLAN 10 および VLAN 120 に対応するスタンバイ HSRP ルータになっています。両方のスイッチは、設定どおり、アクティブに使用されています。両者にすべてのレイヤ 2 VLAN を均等に分散させると、負荷を両者に分散させることができます。また、各スイッチは、そのローカル VLAN 200 インターフェイスをトラックするように設定されており、VLAN 200 にリンク障害が発生した場合は、もう一方のスイッチがプリエンプション処理し、すべての VLAN に対応するアクティブ ルータとなります。同様に、一方のスイッチに障害が発生した場合は、もう一方のスイッチが 3 つの VLAN すべてのトラフィックを処理します。

図 3-3 のアクセス レイヤにある PC と電話機には、各 HSRP グループの HSRP アドレスに対応したデフォルト ゲートウェイが設定されています。Voice VLAN 110 および 120 のデバイスは、デフォルト ゲートウェイとして 10.100.10.1 と 10.100.20.1 をそれぞれ指しています。これらのデフォルト ゲートウェイは、両方のスイッチにある VLAN 110 および 120 インターフェイスの HSRP アドレスに対応しています。データ VLAN 10 のデバイスは、デフォルト ゲートウェイとして 64.100.10.1 を指しています。このデフォルト ゲートウェイは、両方のスイッチにある VLAN 10 インターフェイスの HSRP アドレスに対応しています。アクセス レイヤからディストリビューション レイヤに流

れるトラフィックは 2 つのスイッチに分散されます（障害がない場合）が、リターン パスでの分散を保証するメカニズムはありません。コア レイヤから戻ってアクセス レイヤに向かうトラフィックは、最短および最小コストの、またはそのどちらかのルーテッド パスに沿って流れます。

図 3-3　standby preempt と standby track を使用した HSRP ネットワーク設定の例



例 3-1 および例 3-2 は、図 3-3 に示されている 2 つの Catalyst 6500 スイッチの設定を示しています。

例 3-1　6500-SW1 の設定

```
interface Vlan 10
 description Data VLAN 10
 ip address 64.100.10.11 255.255.255.0
 standby preempt
 standby ip 64.100.10.1
 standby track Vlan 200

interface Vlan110
 description Voice VLAN 110
 ip address 10.100.10.11 255.255.255.0
 standby preempt
 standby ip 10.100.10.1
 standby track Vlan 200
 standby priority 95

interface Vlan120
 description Voice VLAN 120
 ip address 10.100.20.11 255.255.255.0
 standby preempt
 standby ip 10.100.20.1
 standby track Vlan 200
```

例 3-2　6500-SW2 の設定

```
interface Vlan 10
 description Data VLAN 10
 ip address 64.100.10.12 255.255.255.0
 standby preempt
 standby ip 64.100.10.1
 standby track Vlan 200
 standby priority 95

interface Vlan110
 description Voice VLAN 110
 ip address 10.100.10.12 255.255.255.0
 standby preempt
 standby ip 10.100.10.1
 standby track Vlan 200

interface Vlan120
 description Voice VLAN 120
 ip address 10.100.20.11 255.255.255.0
 standby preempt
 standby ip 10.100.20.1
 standby track Vlan 200
 standby priority 95
```

障害発生時に HSRP が収束する速さは、HSRP の Hello タイマーとホールド タイマーの設定によって異なります。デフォルトでは、これらのタイマーは 3 秒と 10 秒にそれぞれ設定されています。この設定は、Hello パケットが HSRP スタンバイ グループのデバイス間で 3 秒ごとに送信されること、および Hello パケットが 10 秒間受信されないとスタンバイ デバイスがアクティブになることを意味します。これらのタイマー設定値を低くすると、フェールオーバーまたはプリエンプション処理を高速化できます。ただし、CPU 使用率の増加やスタンバイ状態の不要なフラッピングを避けるため、Hello タイマーを 1 秒未満に設定することや、ホールド タイマーを 4 秒未満に設定することはしないでください。HSRP トラッキング メカニズムを使用している場合、トラッキングしているリンクに障害が発生したときは、Hello タイマーやホールド タイマーに関係なく、ただちにフェールオーバーまたはプリエンプション処理が行われます。

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、およびフォールト トレランスを保証するには、ディストリビューション レイヤで、Open Shortest Path First（OSPF）や Enhanced Interior Gateway Routing Protocol（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お勧めします。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。レイヤ 3 対応の Catalyst 6000 スイッチは、一般的なコア レイヤ デバイスであり、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。

コア レイヤにおいても、高可用性を保証するために、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スーパーバイザ エンジン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。

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合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 CallManager クラスタ サーバは、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、コンファレンス ブリッジ、DSP またはトランスコーダ ファーム、およびメディア 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ます。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 Cisco CallManager 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お勧めします。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すみます。

ネットワーク サービス

可用性が高く、耐障害性のあるマルチレイヤ キャンパス ネットワークの構築が完了したら、DNS、DHCP、TFTP、および NTP などのネットワーク サービスを配置できます。

ドメイン ネーム システム（DNS）

DNS を使用すると、ホスト名をネットワーク（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、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 アドレスを受信することができます。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。

ただし、DNS を利用することは問題となる場合があります。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、Cisco CallManager と IP テレフォニー エンドポイント間の通信には DNS を利用しないでください。

ホスト名の代わりに IP アドレスを使用するように、Cisco CallManager、ゲートウェイ、およびエンドポイント デバイスを設定します。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お勧め *できません*。同様に、HOSTS ファイルを設定することもお勧めできません。これは、何千ものエンドポイントおよびサーバを含む大規模な IP テレフォニー ネットワークでは、このファイルの管理に膨大な時間がかかり、非効率的になる場合があるためです。IP テレフォニー ネットワークから DNS 設定を排除すれば、テレフォニー デバイスおよびアプリケーションは DNS サーバを利用する必要がなくなります。

ただし、LMHOSTS ファイルを設定する必要はあります。このファイルは、サーバのホスト名または NetBios 名を IP アドレスに解決またはマッピングするメカニズムを備えています。LMHOSTS ファイルには、サーバ名とそれに対応する IP アドレスのリストを含める必要があります。クラスタ内のすべてのサーバに関するエントリと、**127.0.0.1 localhost** を持つエントリ（ループバック エントリ）を含める必要があります。このファイルをクラスタ内のすべてのサーバにコピーする必要があります。LMHOSTS ファイルは、ディレクトリ パス C:\WINNT\system32\drivers\etc に配置します。例 3-3 は、6 つのサーバを含むクラスタの一般的な LMHOSTS ファイルを示しています。

例 3-3　LMHOSTS ファイル

```
127.0.0.1       localhost       !The local host entry
64.101.1.7      ccm1-hq-1
64.101.2.7      ccm1-hq-2
64.101.1.8      ccm1-hq-3
64.101.2.8      ccm1-hq-4
64.101.1.21     ccm1-moh-1
64.101.2.21     ccm1-moh-2
```

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、テレフォニー ネットワーク内での IP Phone と Cisco CallManager 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 テレフォニー障害回復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）　クラスタ内の DNS 名が解決されるのは、システムの初期化時（つまり、サーバのブートアップ時）のみです。結果として、クラスタ内のサーバが、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。

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 テレフォニー 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 テレフォニー ネットワーク デバイスに設定情報を提供することができます。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識別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 つ目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）ことを強くお勧めします。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、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、Cisco CallManager システムが 3 つの別々のサイトで WAN を介してクラスタ化されている場合は、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。ただし、設定ファイルが変更された場合、パブリッシャはクラスタ内の各 TFTP サーバにデータベースの新しいコピーを送信する必要があります。このようにデータベースを伝搬すると、パブリッシャの CPU リソースが消費されるため、クラスタ内に 3 つ以上の TFTP サーバが配置されている場合はパフォーマンスが低下することがあります。

DHCP、スタンドアロン サーバと共存サーバの比較

一般に、DHCP は、スタンドアロン サーバ上で動作するように設定される必要があります。これは、多数のデバイスが DHCP 設定を要求すると、CPU とメモリの使用率が増加し、サーバのパフォーマンスに影響を及ぼす場合があるためです。したがって、Cisco CallManager サーバ上では DHCP を実行しないでください。たとえば、クラスタに登録されているデバイスが 1,000 以下の小規模な Cisco CallManager 配置であれば、Cisco CallManager サーバ上で DHCP を実行してもかまいません。ただし、サーバの CPU 負荷が高くなる場合は、DHCP をスタンドアロン サーバに移行する必要があります。クラスタに登録されているデバイスが 1,000 を超える場合、DHCP はスタンドアロン サーバ上で実行される必要があります。

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）ことをお勧めします。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、ラップトップや無線テレフォニー 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 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、Cisco CallManager 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最長で 4 日後に、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することができます。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、各支店で設定を更新する作業が発生します（詳細については、P.3-14 の「DHCP のネットワーク配置」を参照）。

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 Cisco CallManager 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支店テレフォニー 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 サービスを提供することができます。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** 設定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 Cisco CallManager 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 サービスを提供することができます。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 3-4 は、Cisco IOS DHCP サーバの基本的な設定コマンドを示しています。

例 3-4　Cisco IOS DHCP サーバの設定コマンド

```
service dhcp                                !Activate DHCP Service on the IOS Device

ip dhcp excluded-address <ip-address>|<ip-address-low> <ip-address-high>
                                            !  Specify an IP Address or IP Address Range
to
                                            !  be excluded from the DHCP pool

ip dhcp pool <dhcp-pool name>               !Specify DHCP pool name
   network <ip-subnet> <mask>               !Specify DHCP pool IP subnet and mask
   default-router <default-gateway-ip>      !Specify the Default-gateway
   option 150 ip <tftp-server-ip-1> ...     !Specify TFTP servers (up to four) -
                                            ! IP phones use only the first two addresses
in
                                            ! the array.
```

Trivial File Transfer Protocol（TFTP）

Cisco CallManager システムにおいて、エンドポイント（SCCP プロトコルを実行する IP Phone など）は、TFTP プロセスを利用して設定情報を取得します。エンドポイントは、要求元の MAC アドレスに基づいた名前の設定ファイルを要求します（たとえば、IP Phone の MAC アドレスが ABCDEF123456 の場合、ファイル名は SEPABCDEF123456.cnf.xml となります）。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、電話機を登録する Cisco CallManager サーバのリストが含まれています。

設定ファイルにおいて、電話機が現在使用しているものと異なるソフトウェア ファイルを実行するように指示されている場合、電話機は新しいバージョンのソフトウェアを TFTP サーバに要求します。電話機はこのプロセスを、ソフトウェア アップグレードのたびに行います。

集中型コール処理配置では、リモート電話機は、支店の WAN リンクを介して設定ファイルと電話機のソフトウェアをダウンロードする必要があります。定期保守において新しいソフトウェアをダウンロードする場合、ダウンロード時間は、アップグレードが必要な電話機の数、ファイル サイズ、および WAN リンクの帯域幅とトラフィック使用率による関数となります。

たとえば、Cisco CallManager Release 3.3(3)SR1 では、電話機の設定ファイルのサイズは約 2,700 バイトで、Cisco IP Phone 7960 用のデフォルトのソフトウェア ロード（P00305000101.bin）は 396,804 バイトです。支店において 256 Kbps の WAN 帯域幅を使用してソフトウェアをダウンロードする場合、1 台の電話機でアップグレード時に新しいソフトウェアをダウンロードするには、約 12 秒かかります。その同じ支店にある 10 台の電話機で新しいソフトウェアが必要な場合、ダウンロード プロセスには約 2 分かかります。

マルチクラスタ キャンパス 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。したがって、この中央の TFTP サーバは、他のクラスタによって作成および管理されるファイルにアクセスできる必要があります。

このファイルにアクセスできるようにするには、各クラスタの TFTP サーバを、中央の TFTP サーバのドライブ上で設定ファイルを作成および管理するように設定する必要があります。設定を実行するには、各 TFTP サーバ（中央の TFTP サーバを除く）の設定で代替ファイル ロケーション エントリを使用します。

Cisco CallManager Release 3.2 以降を使用する場合、Cisco TFTP サーバは、デフォルトで、IP Phone の設定ファイルを RAM にキャッシュします。中央の TFTP サーバに書き込むファイルについては、ファイル キャッシングを無効（オフ）にする必要があります。無効にするには、中央の TFTP サーバに書き込むように設定された TFTP サーバごとに、次のサービス パラメータを指示通りに設定します。

- Enable Caching of Configuration Files：**False**（必須）
- Enable Caching of Constant and Bin Files at Startup：**False**（推奨）

TFTP サーバは、サーバ上にないファイル（別のクラスタの TFTP サーバによって作成および管理される設定ファイルなど）の要求を受信すると、代替ファイル ロケーションのリスト内でそのファイルを検索します。中央の TFTP サーバは、他のクラスタに関連付けられたサブディレクトリまで検索するように設定される必要があります。

例 3-5　代替 TFTP ファイル ロケーション

大規模なキャンパス システムを配置する場合は、3 つのクラスタを使用します。各クラスタには TFTP サーバを含めます。Cluster1 に対応する TFTP サーバの TFTP1 は、キャンパスの中央 TFTP サーバとして設定します。それ以外のクラスタと TFTP サーバの名前は、順に、Cluster2 に対応するものを TFTP2 に、Cluster3 に対応するものを TFTP3 にします。すべてのサブネットでは、DHCP スコープがオプション 150 として TFTP1 の IP アドレスを提供します。

最初に、TFTP2 と TFTP3 が、それぞれの設定ファイルを TFTP1 のドライブに書き込むように設定します。それぞれの書き込み先は、次に示す別々のサブディレクトリとします。

- TFTP2 の代替ファイル ロケーションの設定：\\TFTP1_IP\Program Files\Cisco\TFTPpath\TFTP2
- TFTP3 の代替ファイル ロケーションの設定：\\TFTP1_IP\Program Files\Cisco\TFTPpath\TFTP3

次に、TFTP1 が代替ファイル ロケーションを検索するように設定します。設定方法は次のとおりです。

- 代替ファイル ロケーション 1：c:\Program Files\Cisco\TFTPpath\TFTP2
- 代替ファイル ロケーション 2：c:\Program Files\Cisco\TFTPpath\TFTP3

（注） この例では、TFTP1_IP は TFTP1 の IP アドレスを表しています。また、TFTP1 では、TFTP2 と TFTP3 用に Windows NT サブディレクトリを手動で作成する必要があります。

TFTP サーバで代替ファイル ロケーションを指定する場合は、Universal Naming Convention（UNC; 汎用命名規則）パス（形式は \\<*IP アドレス*>\< *フォルダへのフル パス*>）を使用することをお勧めします。デフォルト以外の NT「共有」を作成することや、DNS 名を使用することはお勧め *できません*。また、すべてのクラスタが、Cisco TFTP サービス用の適切なログイン ID、パスワード、およびセキュリティ特権（ワークグループ、ドメイン、またはディレクトリベース）を処理することを確認します。

さらに、大規模なキャンパス配置では、Maximum Serving Count サービス パラメータを、次のように調整します。専用 TFTP サーバの推奨値は、シングル プロセッサ システムの場合が 1,500 で、デュアルプロセッサ システムの場合が 3,000 です。デュアルプロセッサ システムが Windows 2000 Advanced Server を実行している場合、サービス数は最大 5,000 にすることができます。

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することができます。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。

図 3-4 に示されているように、クラスタ内に 2 つの TFTP サーバを設定できます。各サーバでは、同じ設定ファイルのリストを別々に作成および管理できます。マルチクラスタ配置では、各クラスタに、プライマリとセカンダリの 2 つの TFTP サーバを設定できます。プライマリ TFTP サーバは、中央のプライマリ TFTP サーバにファイルを書き込むように設定できます。同様に、セカンダリ TFTP サーバでは、中央のセカンダリ TFTP サーバにファイルを書き込むように設定できます。この設定により、冗長性を保証するように設定された TFTP サーバに関する 2 つの別々のグループ（プライマリとセカンダリ）が作成されます。各グループには、中央サーバとして機能するメンバーが設定されます。

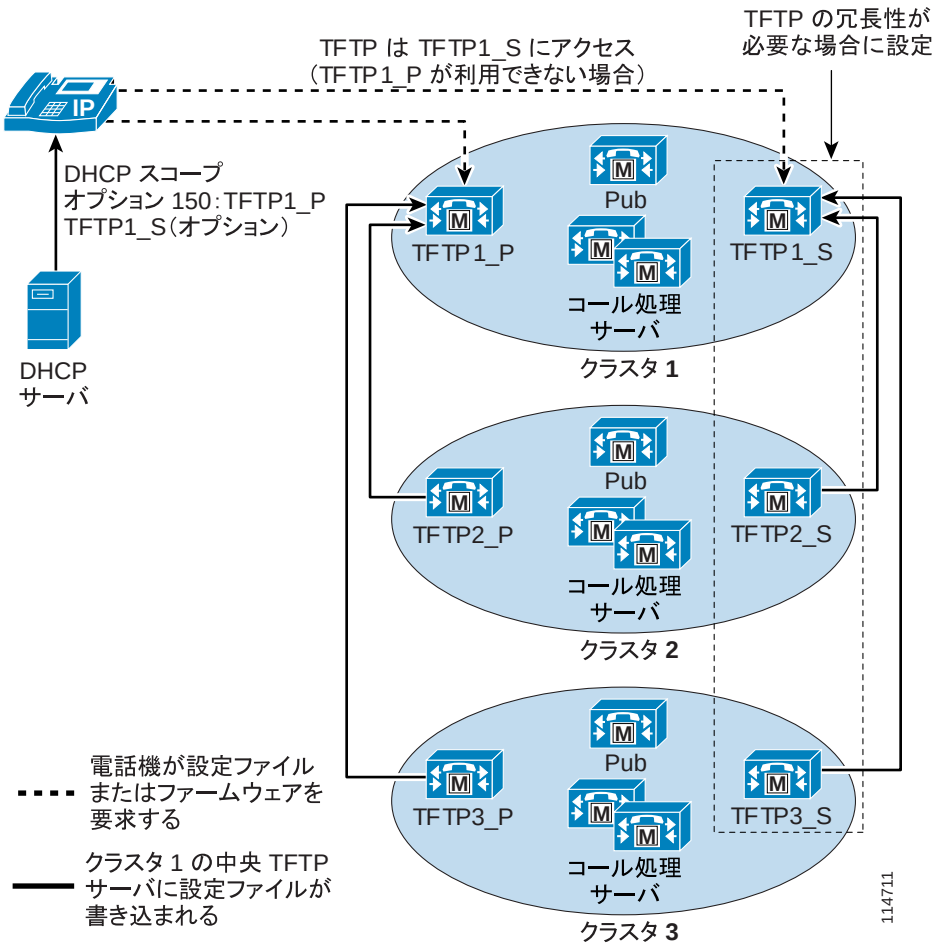
例 3-6　TFTP サーバの冗長性

例 3-5 で説明した事例に対して TFTP の冗長性を追加する場合は、各クラスタに 2 つの TFTP サーバを設定します。すべてのプライマリ TFTP サーバは、その設定ファイルを TFTP1_P に書き込むように設定し、すべてのセカンダリ TFTP サーバは、その設定ファイルを TFTP1_S に書き込むように設定します。次を参照してください。

- TFTP2_P の代替ファイル ロケーションの設定：\\TFTP1_P\Program Files\Cisco\TFTPpath\TFTP2
- TFTP3_P の代替ファイル ロケーションの設定：\\TFTP1_P\Program Files\Cisco\TFTPpath\TFTP3
- TFTP2_S の代替ファイル ロケーションの設定：\\TFTP1_S\Program Files\Cisco\TFTPpath\TFTP2
- TFTP3_S の代替ファイル ロケーションの設定：\\TFTP1_S\Program Files\Cisco\TFTPpath\TFTP3

TFTP1_P と TFTP1_S はどちらも、例 3-5 で説明したように、代替ファイル ロケーションのリストを検索するように設定する必要があります。

図 3-4　すべてのクラスタの中央 TFTP サーバに関する TFTP サーバの冗長性



TFTP のロード シェアリング

前の項では、一度に 1 つの TFTP サーバを使用して複数のクラスタの電話機にサービスを提供する方法について説明しました。ここで示すアプローチでは、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お勧めします。次の例を参考にしてください。

- サブネット 10.1.1.0/24 の場合：オプション 150：TFTP1_P、TFTP1_S
- サブネット 10.1.2.0/24 の場合：オプション 150：TFTP1_S、TFTP1_P

通常動作では、サブネット 10.1.1.0/24 の電話機は TFTP1_P 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_S に TFTP サービスを要求します。TFTP1_P に障害が発生した場合、両方のサブネットの電話機は TFTP1_S 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、Cisco CallManager 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。

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上で重要です。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きわめて重要です。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。

Cisco CallManager の NTP 時刻同期

時刻同期は、Cisco CallManager サーバにおいて特に重要です。次の手順を実行して、ネットワーク内のすべての Cisco CallManager 上で自動 NTP 時刻同期を設定する必要があります。

ステップ 1　NTP.conf ファイルを設定します。

NTP.conf ファイルは C:\WINNT\ ディレクトリにあります。ファイルには、時刻について照会できる 1 つ以上の NTP タイム サーバのリストを設定する必要があります。また、ファイルは、ローカル LAN セグメントの NTP ブロードキャストを介して NTP タイム サーバのアップデートを受信するように設定する必要もあります。Cisco CallManager でブロードキャスト メッセージを介して時刻を受信するために使用できる、ブロードキャスト対応の NTP タイム サーバが必要です。例 3-7 は、NTP.conf ファイルを設定する 2 つの方法を示しています。

ステップ 2　NTP Service がブートアップ時に自動的に開始するように設定します。

各 Cisco CallManager サーバにおいて、Microsoft Windows のサービス アプリケーションで、NTP Service がシステムのブートアップ時に自動的に開始するように設定します。

ステップ 3　各 Cisco CallManager サーバにおいて、サービス アプリケーションを使用して NTP Service を開始または再開します。

（注）　NTP Service が Cisco CallManager サーバ上の Microsoft サービス コントロール パネル アプリケーションに表示されない場合は、C:\Program Files\Cisco\Xntp>**install.bat** を実行して手動でインストールします。

例 3-7　NTP.conf 設定ファイル

```
server 64.100.21.254
server 64.200.40.10
driftfile %windir%\ntp.drift
```

または

```
broadcastclient
driftfile %windir%\ntp.drift
```

例 3-7 で参照されている driftfile は、NTP タイム サーバから受信された NTP メッセージ内の情報に基づいて、NTP Service を介して自動的にアップデートされます。

（注）　デフォルトでは、NTP サーバと NTP クライアント間のクロック オフセットまたは調整幅が 1,000 秒より大きい場合、NTP のアップデートは行われません。このデフォルト動作を調整するには、**tinker panic** < *秒数* > コマンドを NTP.conf ファイルに追加します。秒数には、許容できる時間差を指定します。この値を 0 に設定すると、panic 機能が無効になり、任意の値のクロック オフセットが受け入れられます。

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上で重要です。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 3-8 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 3-8　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。

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信できます。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 Uninterrupted 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信す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。

Cisco PoE は、データ接続に使用されるペア線を介して供給されます（ピン 1、2、3、および 6）。既存のアクセス スイッチ ポートがインライン パワーに対応していない場合は、パワー パッチパネルを使用して、ケーブル上に電力を供給することができます（この場合は、4、5、7、および 8 ピンが使用されます）。また、配置要件によっては、パワー インジェクタを使用することもできます。

注意　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場合、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。現時点で 802.3af に準拠しているのは、一部のアクセス スイッチおよび電話機のみです。将来的には、すべての電話機とスイッチが 802.3af PoE をサポートする予定です。Catalyst 6500、4500、および 3750 は、現在、802.3af をサポートしています。802.3af PoE 標準をサポートする Cisco IP Phone については、P.17-34 の「エンドポイント機能の要約」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 IP Phone（Cisco 7970、7960、7940、および 7910+SW IP Phone）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 IP Phone（Cisco 7902、7905、および 7910 IP Phone）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 イーサネットのみがサポートされ、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 IP Phone（Cisco 7970、7960、7940、7910+SW、および 7912 IP Phone）は、10Mb 半二重にネゴシエートできるよう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 7912 IP Phone 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 組のみです。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。

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、非準拠に起因する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お勧めします。

IBM ケーブリングの使用に関する詳細については、次の Web サイトで入手可能な製品情報『*Shielded Twisted-Pair Cabling Support for Cisco Fast Ethernet Products*』を参照してください。

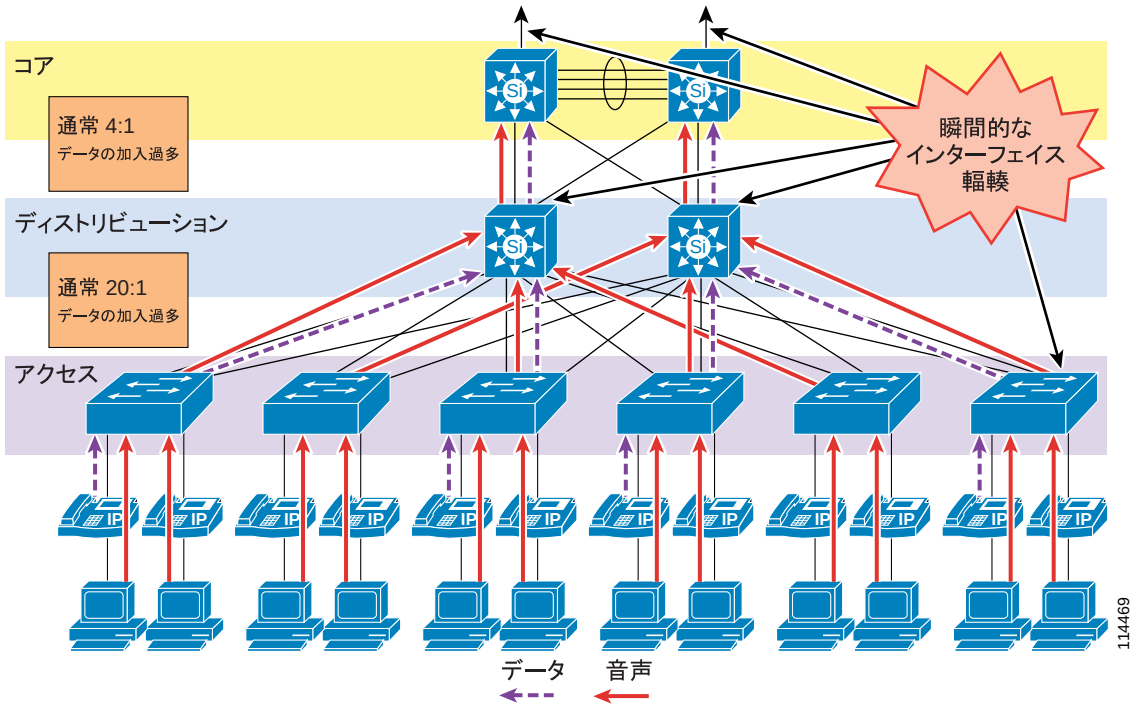
http://www.cisco.com

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 3-5 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 3-5　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かどうかが一定していない地点は、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.3-24）
- インターフェイス キューイング（P.3-25）
- 帯域幅のプロビジョニング（P.3-25）
- 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.3-25）

トラフィック分類

できるだけネットワークの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須部分でした。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。IP Phone は、その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 3-2 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 フローを分類でき、実際に分類する必要があります。

表 3-2 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 3-2　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

トラフィックのタイプ	レイヤ 2 サービス クラス（CoS）	レイヤ 3 IP 優先順位	レイヤ 3 Differentiated Services Code Point（DSCP）	レイヤ 3 Per-Hop Behavior（PHB）
音声 Real-Time Transport Protocol（RTP）	5	5	46	EF
音声制御シグナリング[1]	3	3	24	CS3
ビデオ会議	4	4	34	AF41
データ	0、1、2	0、1、2	10 ～ 22	BE ～ AF23

1. 音声制御シグナリング 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する予定ですが、多くの製品は、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お勧めします。

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お勧めします。Cisco Catalyst 6000、4000、3750、35XX、および 2950 スイッチはすべて、ポートごとに 2 つ以上の出力キューをサポートします。

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 リンク上に定常状態の輻輳がないように、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は異なります。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）とファースト 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の保護対象となるトラフィック 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、および支店で 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 環境にはより大量の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、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 IP テレフォニー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きわめて重要です。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 の設計と設定に関するベスト プラクティス

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

音声ネットワークに関する WAN 配置では、ハブアンドスポーク トポロジに従う必要があります。このトポロジは、中央のハブ サイトと、中央のハブ サイトに接続された複数のリモート スポーク サイトを持ちます。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。このトポロジにすると、中央サイトの Cisco CallManager 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。

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、第 2 章「IP テレフォニー配置モデル」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。

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お勧めします。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 CallManager Express（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お勧めします。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。

最後に、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。

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。

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*ことをお勧めします。

（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。しかし、これらのメカニズムは、サービス プロバイダーによって配置されることが一般的ではないため、依然としてこれらのサービスは大幅なオーバーサブスクリプションになります。

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、リンク効率技術を WAN パスに適用できます。たとえば、Link Fragmentation and Interleaving（LFI）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、およびジッタを低減することによって、信頼できる高品質の音声を保証することにあります。表 3-3 は、WAN インフラストラクチャをこの目標に導くために必要な QoS 機能およびツールを示しています。

表 3-3　WAN テクノロジーとリンク速度ごとの IP テレフォニー 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 kbps ～ 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（Link Fragmentation and Interleaving） • LLQ（低遅延キューイング） • オプション :cRTP（Compressed Real-Time Transport Protocol）	• 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
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

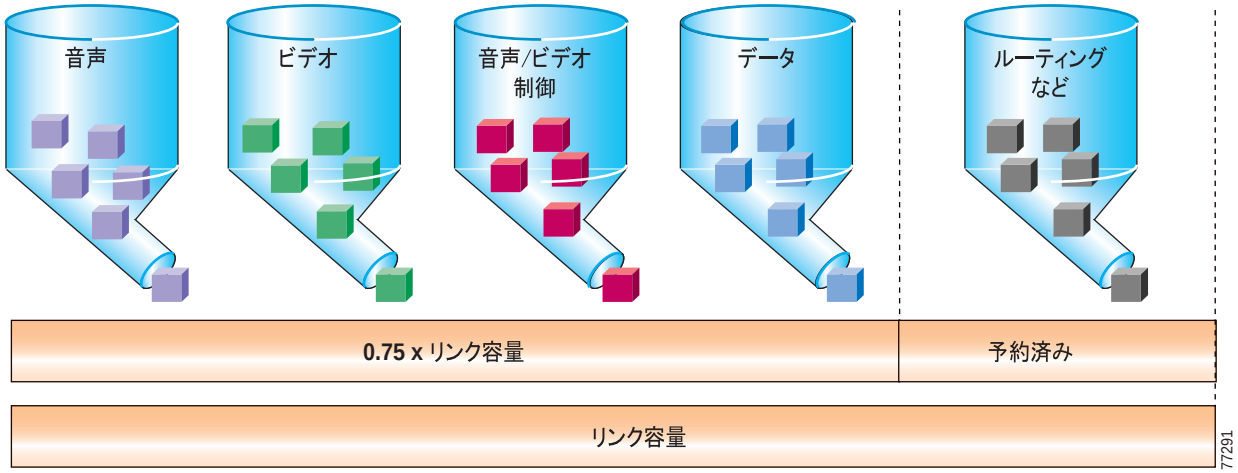
次の 4 つの項では、音声とデータの両方のトラフィックをサポートするように WAN を設計する場合に、考慮すべき最も重要な機能と手法を説明しています。

- 帯域幅のプロビジョニング（P.3-31）
- トラフィックの優先順位（P.3-37）
- リンク効率手法（P.3-40）
- トラフィック シェーピング（P.3-40）

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 3-6 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 3-6　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 RTP（Real-Time Transport Protocol）パケットから構成される、音声キャリア 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、コール制御信号。たとえば、コール制御機能は、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、音声ストリーム トラフィックだけでなく、コール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、コール制御トラフィック（および音声ストリーム）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。

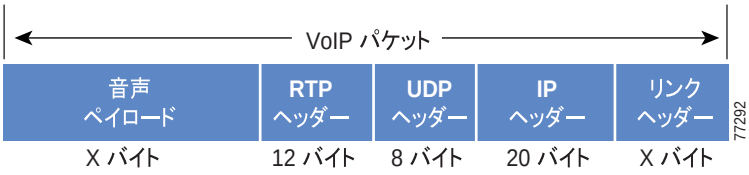
次の 3 つの項では、次のタイプのトラフィックについて、帯域幅プロビジョニングの推奨事項を説明します。

- すべてのマルチサイト WAN 配置における音声ベアラ トラフィック（P.3-32 の「音声ベアラ トラフィック用のプロビジョニング」を参照）
- 集中型コール処理を使用するマルチサイト WAN 配置におけるコール制御トラフィック（P.3-34 の「集中型コール処理を使用したコール制御トラフィック用のプロビジョニング」を参照）
- 分散型コール処理を使用するマルチサイト WAN 配置におけるコール制御トラフィック（P.3-36 の「分散型コール処理を使用したコール制御トラフィック用のプロビジョニング」を参照）

音声ベアラ トラフィック用のプロビジョニング

図 3-7 に示されているように、VoIP（Voice-over-IP）パケットは、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。デフォルトのパケット レート 20 ms では、VoIP パケットには、G.711 の場合は 160 バイトのペイロードがあり、G.729 の場合は 20 バイトのペイロードがあります。SRTP（Secure Real-Time Transport Protocol）暗号化を使用すると、各パケットのペイロードは 4 バイト増加します。デフォルトのパケット レート 20 ms では、SRTP VoIP パケットには、G.711 の場合は 164 バイトのペイロードがあり、G.729 の場合は 24 バイトのペイロードがあります。IP ヘッダーは 20 バイト、UDP ヘッダーは 8 バイト、RTP ヘッダーは 12 バイトです。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 3-7　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、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 秒当たりのパケット レート（デフォルトでは、毎秒 50 パケット）を掛けます。表 3-4 では、デフォルトのパケット レートである毎秒 50 パケット（pps）での VoIP フロー当たりの帯域幅を詳しく記述しています。表 3-4 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、Compressed Real-Time Transport Protocol（cRTP）などの可能な圧縮方式を考慮していません。Cisco CallManager Administration の Service Parameters メニューを使用すると、パケット レートを調整できます。

表 3-4 は、音声ペイロードと IP ヘッダーのみ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 3-4　音声ペイロードと IP ヘッダーのみの帯域幅使用量

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 秒当たりの パケット数	1 会話当たりの 帯域幅
G.711	20 ms	160	50.0	80.0 kbps
G.711（SRTP）	20 ms	164	50.0	81.6 kbps
G.711	30 ms	240	33.3	74.7 kbps
G.711（SRTP）	30 ms	244	33.3	75.8 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

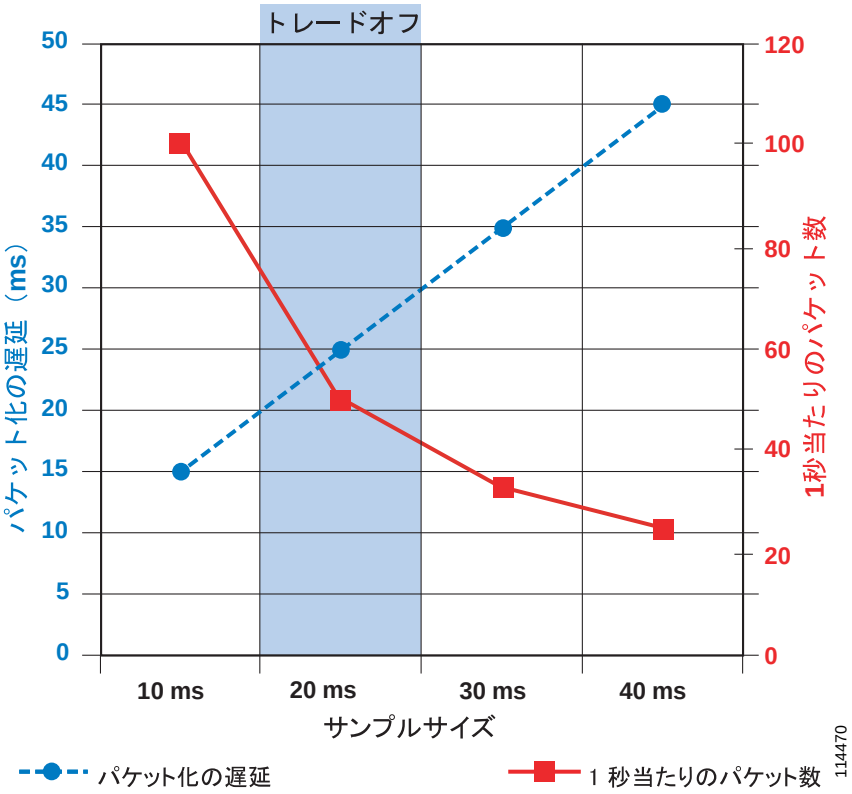
より正確な方法でプロビジョニングするには、帯域幅の計算にレイヤ 2 ヘッダーを含めます。表 3-5 は、レイヤ 2 ヘッダーを計算に含めたときの、音声トラフィックによって消費される帯域幅の量を示しています。

表 3-5　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（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（SRTP）（50.0 pps）	87.2 kbps	84.0 kbps	106.0 kbps	83.2 kbps	85.6 kbps	83.2 kbps	適用対象外
G.711（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（SRTP）（33.3 pps）	79.5 kbps	77.4 kbps	84.8 kbps	76.8 kbps	78.4 kbps	76.8 kbps	適用対象外
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	適用対象外
G.729A（33.3 pps）	22.4 kbps	20.3 kbps	28.3 kbps	19.7 kbps	21.3 kbps	19.7 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	適用対象外

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 3-8 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 秒当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 パケット当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 秒当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 秒当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 3-8　音声のサンプル サイズ：1 秒当たりのパケット数とパケット化の遅延との比較



集中型コール処理を使用したコール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、Cisco CallManager 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 サイトは 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 Cisco CallManager 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 Cisco CallManager 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）、H.323、MGCP、および TAPI です。すべての制御トラフィックは、中央サイトの Cisco CallManager 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。

その結果、制御トラフィック用の帯域幅を提供しなければならない領域は、支店のルータと、中央サイトの WAN アグリゲーション ルータとの間にあります。

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、電話機のアクティビティに関係なく、支店の IP Phone と Cisco CallManager 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。
- 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 IP Phone および / またはゲートウェイと、中央サイトの Cisco CallManager 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。

したがって、生成されるコール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 時間当たりの平均コール数について推測する必要があります。分かりやすくするために、この項での計算では、電話機当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、P.3-36 の「拡張公式」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、コール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 1：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 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 パターンの変更を吸収し、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、過剰プロビジョニング係数を導入することをお勧めします。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、Cisco CallManager 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 2：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）

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 3-6 のようにまとめることができます。

表 3-6　コール制御トラフィック用の推奨帯域幅（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）	制御トラフィック用の推奨帯域幅（暗号化なし）	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
20	8 kbps	9 kbps
30	8 kbps	13 kbps
40	11 kbps	17 kbps
50	14 kbps	21 kbps
60	16 kbps	25 kbps
70	19 kbps	29 kbps
80	21 kbps	33 kbps
90	24 kbps	38 kbps

表 3-6　コール制御トラフィック用の推奨帯域幅（シグナリングの暗号化の有無別）（続き）

支店の規模（IP Phone とゲートウェイの数）	制御トラフィック用の推奨帯域幅（暗号化なし）	制御トラフィック用の推奨帯域幅（暗号化あり）
100	27 kbps	42 kbps
110	29 kbps	46 kbps
120	32 kbps	50 kbps
130	35 kbps	54 kbps
140	37 kbps	58 kbps
150	40 kbps	62 kbps

（注）　表 3-6 の値は、レイヤ 3 帯域幅を示しています。WAN リンクをプロビジョニングする場合、使用するレイヤ 2 テクノロジーに応じて、これらの数値にレイヤ 2 オーバーヘッドを加算する必要があります。

拡張公式

この項で示されている上記の公式は、電話機 1 台当たりの平均コール 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。こうした場合のコール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 台当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 3：支店の推奨帯域幅、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 4：リモート サイトの支店の推奨帯域幅、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）

分散型コール処理を使用したコール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、Cisco CallManager 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 Cisco CallManager クラスタとの間、および Cisco CallManager 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、Cisco CallManager 相互間の WAN リンクだけでなく、各 Cisco CallManager 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。

- 静止トラフィック。このトラフィックは、各 Cisco CallManager 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、Cisco CallManager とゲートキーパー間で交換される。
  - H.225 または H.245 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、2 つの Cisco CallManager 間で交換される。

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、なん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することができます。この前提により、コール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 5: 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）

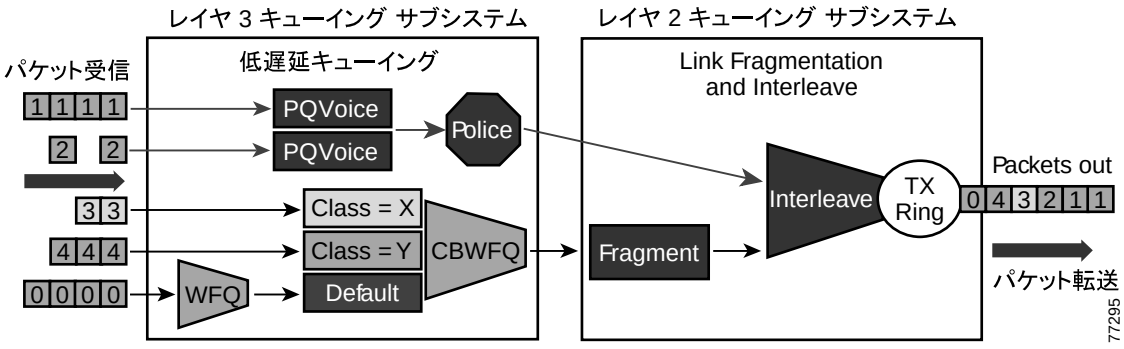
Cisco IOS ルータ上のキューに割り当て可能な最小帯域幅は、8 Kbps です。つまり 8 Kbps の最小キュー サイズは、*最大 70 の仮想タイ ライン*によって生成されるコール制御トラフィックを受け入れることができると推定できます。これは、大部分の大企業での配置に十分な量です。

トラフィックの優先順位

多数の使用可能な優先順位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）を使用することをお勧めします。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 3-9 は、優先順位体系の例を示しています。

図 3-9　WAN を介した VoIP 用の最適化キューイング



LLQ には、次の優先順位の基準を使用することをお勧めします。

- *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* プロトコルを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）に変更し始めています。ただし、多くの製品は、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、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お勧めします。

- 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、必要量の帯域幅を持つ 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 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。

リンク効率手法

次のリンク効率技術によって、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全部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 利用率です。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サービス インターワーキング（SIW）リンクで cRTP を使用する場合は、マルチリンク ポイントツーポイント プロトコル（MLP）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)2T 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 メカニズムからフィードバック 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 3-7 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 3-7 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 ヘッダーのみに基づいています。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 3-7　512 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 Release	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 を指定することができます。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することができます。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。

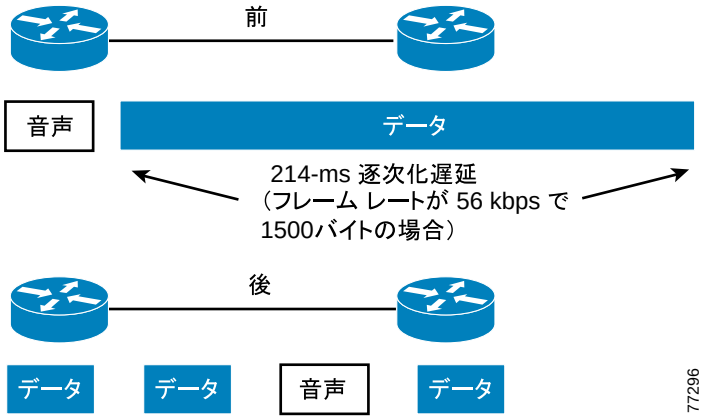
音声およびビデオに対応した IPSec VPN（V3PN）で cRTP を使用する場合の追加の推奨事項については、次の Web サイトで入手可能な V3PN 資料を参照してください。

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

LFI（Link Fragmentation and Interleaving）

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 3-10 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、マルチリンク ポイントツーポイント プロトコル（MLP）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 3-10　LFI（Link Fragmentation and Interleaving）



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のみです。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（P.3-42 の「Voice-Adaptive Traffic Shaping（VATS）」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、一般に集約されて、中央サイトの単一ルータ インターフェイスになります。

図 3-11 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 3-11　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

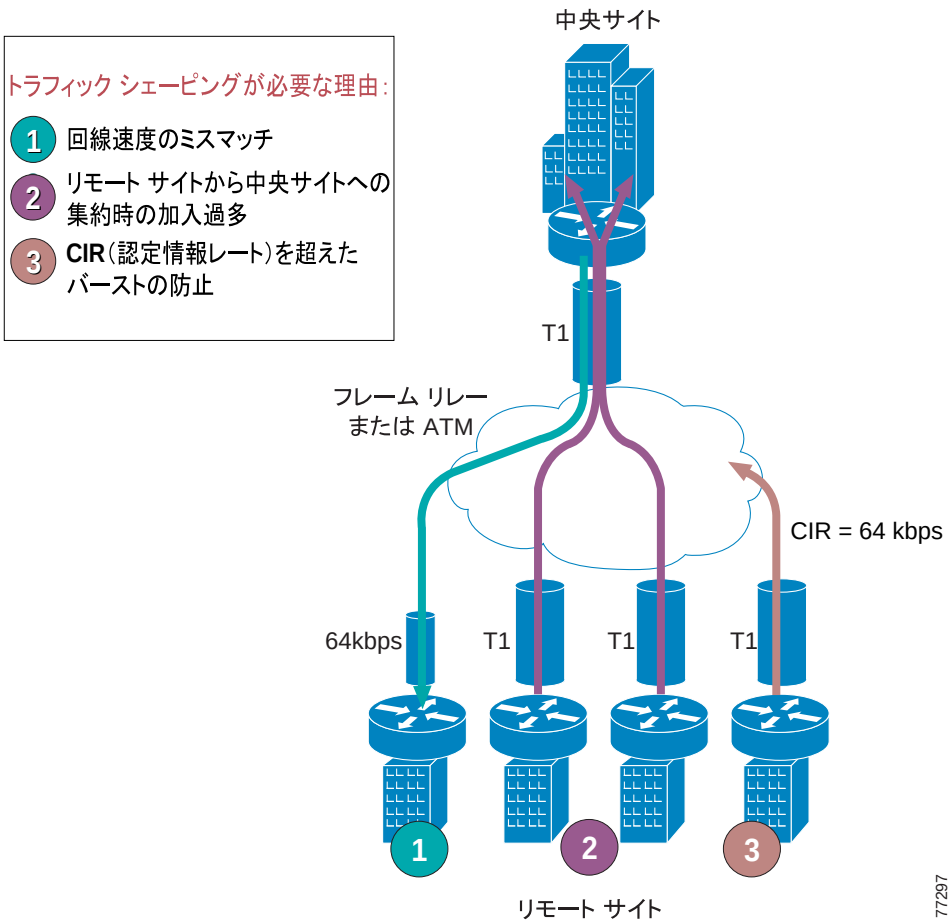


図 3-11 は、次の 3 つのシナリオを示しています。

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、音声パフォーマンスが低下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

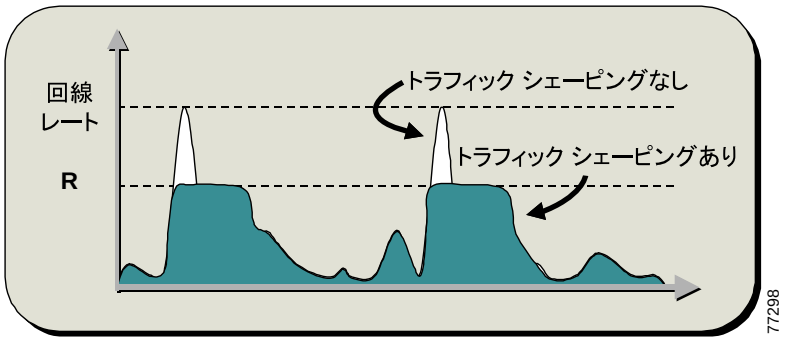
   複数のリモート サイトを 1 つの中央サイトに集約する場合、帯域幅をオーバーサブスクリプションにするのは、フレームリレーまたは ATM ネットワークでは一般的な方法です。たとえば、T1 インターフェイスで WAN に接続するリモート サイトが複数あるにもかかわらず、中央サイトには 1 つの T1 インターフェイスしかない場合があります。この設定により、配置されたネットワークは統計多重化による恩恵を受けますが、中央サイトのルータ インターフェイスが、トラフィックのバースト時に輻輳し、音声品質が低下することがあります。

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 3-12 は、このメカニズムを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 3-12　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（P.3-39 の「LFI（Link Fragmentation and Interleaving）」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つつ、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/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ft_vats.htm

無線 LAN インフラストラクチャ

統合されたネットワークの無線 LAN（WLAN）部分に IP テレフォニーを追加する場合は、無線 LAN インフラストラクチャの設計が重要になります。Cisco 無線 IP Phone 7920 などの無線 IP テレフォニー エンドポイントが追加されている場合、音声トラフィックは WLAN 上に移動しているため、そこで既存のデータ トラフィックと共にコンバージされます。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 を理解して無線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 の設計の詳細については、次の Web サイトで入手可能な『*Cisco Wireless LAN SRND*』のガイドを参照してください。

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

Cisco 7920 無線 IP Phone の詳細については、次の Web サイトで入手可能な『*Cisco Wireless IP Phone 7920 Design and Deployment Guide*』を参照してください。

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

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、無線テクノロジーについて理解する必要があります。最後に、無線アクセス ポイント（AP）と無線テレフォニー 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。

無線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

有線 LAN インフラストラクチャの場合と同様、無線 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。無線 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、無線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。無線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 を設定することもお勧めします。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

無線インフラストラクチャでは、無線エンドポイントのローミングについて考慮することも非常に重要です。無線デバイスがレイヤ 2 で移動する場合、デバイスはその IP アドレスとネットワーク設定を保持します。このため、ローミングは、きわめて迅速に（100 ～ 400 ms で）行われる場合があります。ローミングで必要になるのは、Cisco LEAP または Extensible Authentication Protocol（EAP）を使用する場合の再認証と、エンドポイントが移動したことを示すために前回の AP と新しい AP の間で Inter-Access Point Protocol（IAPP）メッセージを受け渡しすることです。レイヤ 2 ローミングは、一般に、エンドユーザに負荷を感じさせません。

デバイスがレイヤ 3 で移動する場合、デバイスは AP から別の AP に移動し、サブネットの境界を越えます。新しい Cisco Catalyst 6500 シリーズ ワイヤレス LAN サービス モジュール（WLSM）のリリースにより、Cisco 7920 無線 IP Phone では、スタティック WEP の使用中に、コールが存続可能なレイヤ 3 ローミングがサポートされるようになりました。Cisco Centralized Key Management（Cisco CKM）を使用すると、Cisco 7920 IP Phone は、LEAP の使用中に完全なレイヤ 3 モビリティを実現できます。Cisco WLSM の詳細については、次の Web サイトで入手可能な製品資料を参照してください。

http://www.cisco.com

（注）　Cisco Catalyst 4000 シリーズ スイッチをディストリビューション レイヤでレイヤ 3 デバイスとして使用する場合は、少なくとも、Supervisor Engine 2+（SUP2+）モジュールまたは Supervisor Engine 3（SUP3）モジュールが必要です。Supervisor Engine 1 または 2（SUP1 または SUP2）モジュールを使用すると、ローミング遅延が発生する場合があります。Cisco Catalyst 2948G、2948G-GE-TX、2980G、2980G-A、および 4912 スイッチも、ローミング遅延を引き起こすことがわかっています。これらのスイッチを無線音声ネットワークで使用することはお勧めできません。

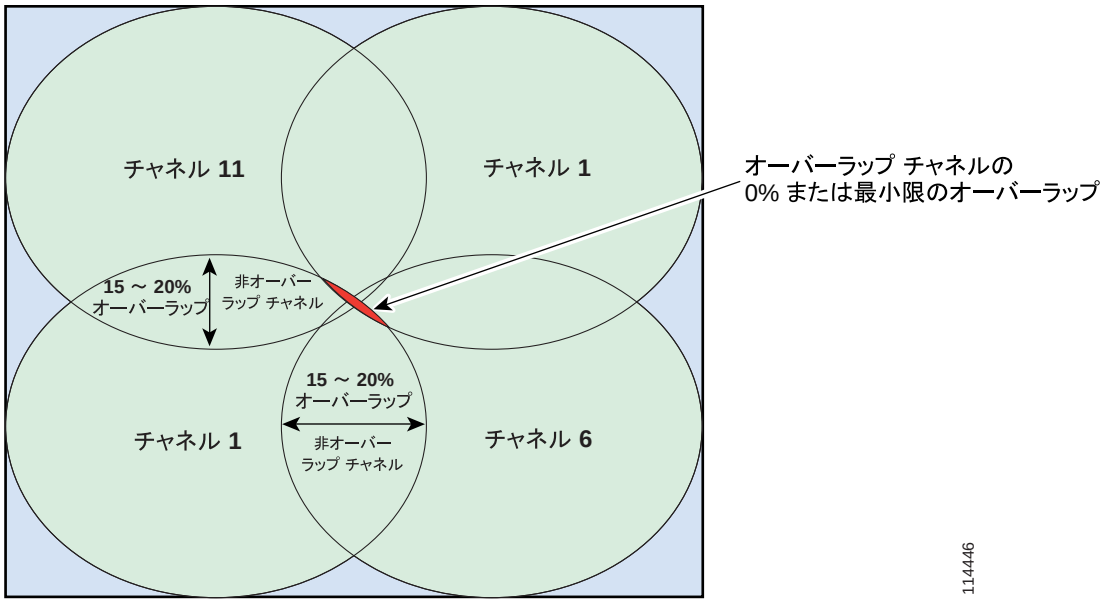
無線チャネル

無線エンドポイントと 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、無線エンドポイントは、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 用のチャネル設定を最適化するには、5 チャネル広げて、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、チャネル 1、6、および 11 が、AP と無線エンドポイント 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。欧州では、802.11b に使用可能な非オーバーラップ チャネルは、1 と 6 のほか、11、12、または 13 のいずれかです。日本では、これらのチャネルは、1 と 6 のほか、11、12、13、または 14 のいずれかです。

AP カバレッジは、同じチャネルに設定された AP 間で発生するオーバーラップが最小またはゼロになるように配置される必要があります（図 3-13 の Channel 1 を参照）。ただし、*非オーバーラップ* チャネル（北米では 1、6、および 11）上で適切な AP 配置およびカバレッジを実現するには、15 ～ 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、無線エンドポイントが AP

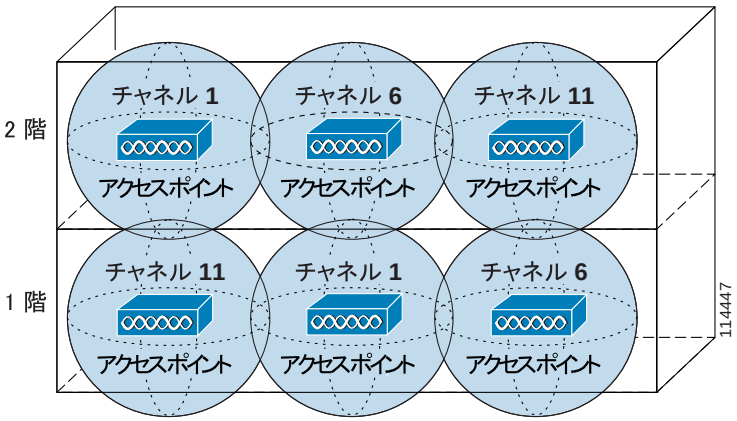
カバレッジ セルの間を移動するときにローミングが円滑に行われることが保証されます。オーバーラップが 15 ～ 20% を下回ると、ローミング時間が遅くなり、音声品質が低下する場合があります。一方、オーバーラップが 15 ～ 20% を超えると、ローミングが頻繁に、または常時行われる場合があります。図 3-13 は、オーバーラップ チャネルと非オーバーラップ チャネルの両方に適切な AP オーバーラップを示しています。

図 3-13　無線 802.11b チャネルのオーバーラップ



高層オフィスビルや病院など、多階の建物に無線デバイスを配置する場合は、無線 AP とチャネル カバレッジのプランニングに 3 つ目の次元が加わります。802.11b の 2.4 GHz 波形は、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 チャネルのみを使用する場合、適切なオーバーラップを実現する唯一の方法は、3 次元のプランニングを慎重に行うことです。図 3-14 は、802.11b 無線カバレッジを 3 次元の側面で考慮した場合の、チャネル オーバーラップの可能性を示しています。

図 3-14　無線 802.11b チャネルのオーバーラップに関する考慮事項（3 次元の場合）



（注）　無線ネットワークを正しく動作させるには、無線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、運用環境に無線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、不良 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

無線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、個人用無線ネットワーク デバイス、硫黄プラズマ照明システム、電子レンジ、不良 AP、および 2.4 GHz 帯域のライセンスフリー動作を利用する他の 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）

WLAN 上のマルチキャスト

音声デバイスを含む WLAN 上でマルチキャスト トラフィックを転送することはお勧めできません。その理由は、次のとおりです。

- AP に関連付けられたデバイスが省電力モードになると、マルチキャスト パケットが AP 上でバッファに入れられるため。

  Cisco 無線 IP Phone 7920 などのデバイスが省電力モードになると、AP 上ですべてのマルチキャスト パケットがバッファに入れられます。この状態は、このデバイスが次にアクティブになるまで続きます。このバッファリングによりパケット遅延が発生し、AP に関連付けられたすべてのデバイスが、省電力モードでない場合も含めて影響を受けます。この状況は、Music On Hold やストリーミング ビデオなどのリアルタイム マルチキャスト アプリケーションで重大な問題となる場合があります。

- WLAN 上のマルチキャスト パケットは応答されないため、損失や破損が起きても再送信されません。

  AP と無線エンドポイントのデバイスは、リンク レイヤ上で応答を使用して、信頼性の高い配信を保証します。パケットが受信されない場合や応答されない場合、パケットは再送信されます。この再送信は、WLAN 上のマルチキャスト トラフィックには行われません。無線ネットワークでは有線ネットワークよりもビット エラーの発生頻度が高いため、この再送信が行われない場合は、有線 LAN よりも多くのパケットが損失します。

無線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お勧めします。

無線 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、無線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

無線音声を配置する場合は、次の AP を選択することをお勧めします。

- Aironet 350 シリーズ AP
- Aironet 1100 シリーズ AP
- Aironet 1200 シリーズ AP

これらの AP には、Cisco IOS Release 12.2(13)JA3 以降を使用する必要があります。無線音声を配置する場合、VxWorks オペレーティング システムを AP に使用することはお勧め *できません*。これは、VxWorks には新しい機能が追加されていませんが、音声の配置にはそれらの新しい機能の一部が必要となるためです。

AP の配置

Cisco アクセス ポイント（AP）を配置するときは、いかなる場合も、単一の AP に 15 ～ 25 を超えるデバイスを関連付けないでください。この数は、使用プロファイル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。1 つの AP に 15 ～ 25 を超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。

AP の設定

無線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 が無線エンドポイント 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、無線エンドポイント デバイスのバッテリ寿命が長くなります。

- AP と無線音声エンドポイントの伝送パワーを一致させる

  可能であれば、AP と音声エンドポイントの伝送パワーを一致させる必要があります。AP と音声エンドポイントの伝送パワーを一致させると、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。伝送パワーが AP によって異なる場合は、すべての音声エンドポイントの伝送パワーを、伝送パワーが最も高い AP に一致するように設定する必要があります。

  （注）　Cisco 7920 無線 IP Phone のファームウェアのバージョン 1.0(8) より、電話機は、Dynamic Transmit Power Control（DTPC）機能を利用して、その伝送パワーを現在の AP の Limit Client Power（mW）に基づいて自動的に調整するようになりました。

- データ レートを 11 Mbps に設定する

  最大 11 Mbps のデータ レートを設定すると、音声デバイスのスループットの最適レベルと、AP ごとのアクティブ コールの最大数が保証されます。

- RF チャネルの選択を手動で設定する（**Search for Least Congested Channel** オプションは使用 *しないでください*）

  無線ネットワーク チャネルを制御し、チャネル オーバーラップを排除するには、そのロケーションに基づいて、AP ごとにチャネル数を手動で設定することが重要です。

- 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無線 VLAN を選択できます。この無線 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 無線音声デバイスは、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することができます。

- 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、P.3-50 の「インターフェイス キューイング」を参照）。

無線セキュリティ

無線インフラストラクチャでは、セキュリティについて考慮することも重要です。無線電話機などの無線エンドポイントは、次のセキュリティ メカニズムのいずれかを使用して、無線ネットワークに接続することができます。

- Cisco LEAP

  Cisco LEAP は、ネットワークに対して認証するためのユーザ名とパスワードを、無線エンドポイントに要求します。この認証が行われると、動的な鍵が生成され、無線デバイスとの間で送受信されるトラフィックが暗号化されます。この方法には、Cisco Secure Access Control Server（ACS）など、EAP 準拠の Remote Authentication Dial-In User Service（RADIUS）認証サーバが必要です。このサーバは、無線デバイスを認証するためのユーザ データベースにアクセスします。Cisco LEAP は、Voice VLAN へのアクセスに対して最高レベルのセキュリティを要求するため、無線音声での使用に推奨されるセキュリティ メカニズムです。

- スタティック Wire Equivalent Privacy（WEP）

  スタティック WEP では、静的に設定された 40 ビットまたは 128 ビットの文字の鍵を、無線エンドポイントと AP の間で交換する必要があります。鍵が一致すると、無線デバイスはネットワークにアクセスできます。WEP 暗号化アルゴリズムには既知の脆弱性があることに注意してください。この脆弱性に加え、静的な鍵の設定と保守が複雑であることもあって、このセキュリティ メカニズムは、多くの場合に不適切となることがあります。

- Open 認証

  この方法では、認証は要求されず、無線エンドポイント デバッグと無線ネットワークの間を移動するトラフィックはセキュリティで保護されません。この方法では、無線デバイスに、無線デバイスの接続先となる無線 VLAN 用の適切な SSID を設定するだけで済みます。この方法を無線音声に使用することは原則としてお勧めできません。これは、Voice VLAN へのアクセスに対して認証が要求されず、音声トラフィックが暗号化されないためです。

Cisco LEAP 認証と ACS 配置モデル

これまで説明したように、Cisco LEAP は、ネットワークおよび Voice VLAN へのアクセスに対して最もセキュアで堅牢なメカニズムを提供するため、無線デバイス認証（特に音声デバイス）に最適な方法です。EAP 準拠の RADIUS サーバが必要となるため、Cisco Secure ACS for Windows Server Version 3.1 以降の使用をお勧めします。

無線認証および暗号化用に Cisco LEAP を配置する場合は、ネットワーク内の ACS の配置を慎重に検討して、次の ACS 配置モデルのいずれかを選択します。

- 集中型 ACS

  ACS サーバ（複数可）は、ネットワーク内の中央に配置され、ネットワーク内のすべての無線デバイスおよびユーザを認証するために使用されます。

- リモート ACS

  リモート ロケーションが低速リンクまたは輻輳した WAN リンクを介して中央サイトから分離しているネットワークでは、ACS サーバをリモート サイトに配置し、リモート無線デバイスまたはユーザをこのサーバでローカルに認証することができます。その結果、WAN リンクを介して集中型 ACS で認証する場合の遅延がなくなります。

- Cisco AP 上のローカルおよびフォールバック RADIUS サーバ

  リモート ロケーションが低速 WAN リンクを介して中央サイトから分離しているネットワークでは、ローカルの無線デバイスがローカル Cisco IOS AP に対して認証できます。Cisco IOS Release 12.2(11)JA 以降を実行する AP では、外部 ACS を利用しないでローカルに Cisco LEAP ユーザおよびデバイスを認証できます。この機能では、単一の AP で最大 50 ユーザをサポートできます。この機能は、中央またはローカル ACS の代わりに使用することも、WAN または ACS に障害が発生してリモート サイトのユーザがローカル ACS または中央サイトの ACS にアクセスできなくなった場合に使用することもできます。

ACS の配置モデルを選択する場合は、認証サービスを冗長にして、無線デバイスがネットワークへのアクセスを試みるときに ACS が単一障害点にならないようにする必要があります。このため、各 ACS サーバはそのデータベースをセカンダリ サーバに複製する必要があります。さらに、WAN に障害が発生しても引き続きリモートの無線デバイスが認証できることを保証するため、リモート サイトにローカルの ACS サーバまたは AP の RADIUS サーバを配置することをお勧めします。

ACS サーバの配置に加え、ACS サーバに関連するユーザ データベースのロケーションの影響を考慮することも重要です。ACS サーバはユーザ データベースにアクセスして無線デバイスを認証する必要があるため、ユーザ データベースのロケーションは、認証に要する時間に影響を与えます。ユーザ データベースがネットワーク上の Microsoft Active Directory（AD）サーバである場合、ACS は AD サーバに認証要求を送信し、応答を待つ必要があります。ネットワークへの認証を試みる無線音声エンドポイントへの応答時間が最小になることを保証するには、ACS サーバ上でローカルにユーザを定義することをお勧めします。リモート データベースは、応答時間が不明であるため、認証時間に悪影響を与える場合があります。

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、無線 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、無線 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、無線ネットワークは共有メディアです。また、無線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。無線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、無線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。

無線 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.3-50）
- インターフェイス キューイング（P.3-50）
- 帯域幅のプロビジョニング（P.3-51）

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無線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、有線および無線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無線エンドポイントで行われる必要があります。無線ネットワーク 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 3-2 を参照）と同じである必要があります。

Cisco 無線 IP Phone 7920 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 26（または PHB AF31）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。無線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。無線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無線 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。無線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、無線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 から無線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。

残念ながら、無線ネットワークで使用できるアップストリーム キューイングはほとんどありません。Cisco 無線 IP Phone 7920 などの無線デバイスは、パケットがデバイスを通過するときにアップストリームのキューイングを行えますが、無線ネットワークは共有メディアであるため、無線 LAN 上のすべてのクライアントでキューイングを行うようにするメカニズムは用意されていません。したがって、音声メディア パケットは無線エンドポイントを通過するときにプライオリティ処理される場合がありますが、このパケットは、他の無線デバイスが送信を試みている可能性のある他のすべてのパケットと競合することになります。このため、無線クライアントを AP ごとに 15 ～ 25 以下に抑えるというガイドラインに従うことがきわめて重要になります。このガイドラインの上限を超えると、音声パケットの遅延やジッタが増加する場合があります。

ダウンストリーム QoS に関しては、Cisco AP は現在、無線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、無線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お勧めします。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 つ目のポリシーには **voice** という名前を付け、**Default Classification for all packets on the Vlan** として **Voice <10 ms Latency (6)** サービス クラスを設定します。2 つ目のポリシーには **data** という名前を付け、**Default Classification for all packets on the Vlan** 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。この設定にすると、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

帯域幅の適切なプロビジョニングも、無線ネットワーキングに対する QoS 要件の 1 つです。帯域幅のプロビジョニングでは、有線ネットワークと無線ネットワーク間の帯域幅や、AP で処理できる同時音声コールの数が対象となります。無線 AP は、一般に、アクセス レイヤ スイッチ ポートへの 100 Mbps リンクを介して有線ネットワークに接続されます。AP 上の入力イーサネット ポートは 100 Mbps のトラフィックを受信できますが、802.11b 無線ネットワークの最大スループットは 11 Mbps です。無線メディアの半二重性と無線ヘッダーのオーバーヘッドを考慮すると、802.11b 無線ネットワークの実質的なスループットは、約 7 Mbps となります。このように有線ネットワークと無線ネットワーク間のスループットは一致しないため、ネットワーク内でトラフィック バーストが発生すると、パケットがドロップする場合があります。

トラフィック バーストによって過剰なトラフィックが AP に送信されることを許可しても、結局は AP でドロップされるため、代わりに、レート制限または規制によってこのトラフィックを無線ネットワークで処理できるレートに抑えることをお勧めします。AP で過剰なトラフィックをドロップさせると、AP での CPU 使用率と輻輳が増加します。代わりに、有線アクセス レイヤ スイッチと無線 AP 間のリンク上でトラフィック レートを 7 Mbps に制限すると、トラフィックがアクセス レイヤ スイッチでドロップされることが保証されるため、AP の負荷がなくなります。AP に送信されるトラフィックのレート制限の詳細については、P.17-31 の「Cisco 無線 IP Phone 7920」の項にある QoS の推奨事項を参照してください。無線ネットワークの配置によっては、実質的なスループットが 7 Mbps を下回ることがあります。特に、単一の AP に関連付けられたデバイスの数が推奨値より多い場合に該当します。

シスコでは、無線音声ネットワークのテストに基づいて、単一の無線 AP で最大 7 つの G.711 音声コールまたは最大 8 つの G.729 音声コールをサポートできることを確認しています。これらの制限を超えると、音声品質が低下し、場合によっては音声コールがドロップされます。音声トラフィックの無線帯域幅をプロビジョニングするのに最適なコール アドミッション制御のメカニズムまたは方式はありませんが、Cisco 7920 無線 IP Phone では、ネットワーク上の AP から受信するチャネル使用率の情報に基づいた、コール アドミッション制御または帯域幅プロビジョニングの簡易バージョンを使用できます。この情報は、QoS Basic Service Set（QBSS）を含むビーコンを介して、AP から電話機に送信できます。QBSS は、その AP による RF チャネルの使用率の推計を示します。QBSS 要素の値が大きいほど、チャネル使用率が高くなり、チャネルと AP が追加の無線音声デバイスに対して十分な帯域幅を提供できる可能性が低くなります。QBSS 要素の値が 45 以上の場合、無線 IP Phone によって試行されるコールはすべて拒否され、「Network Busy」メッセージ、ファースト ビジー音、またはその両方が示されます。また、無線 IP Phone は、そのローミング アルゴリズムで QBSS 要素を検討し、QBSS 要素が 45 以上のビーコンを送信する AP には移動しません。

（注）　QBSS 値は、特定の AP におけるチャネル使用率の推計にすぎません。実際のチャネル使用率は、示された値よりもはるかに高い場合があります。このため、上限の 7 または 8 コールにすでに到達していても、引き続きその AP 上で無線音声デバイスから音声コールを発信できる場合があります。その場合は、コールがドロップされたり、音声品質が低下したりします。

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のみです（P.3-47 の「無線 AP の設定と設計」を参照）。