CHAPTER 7

Cisco IPICS の配置モデル

この章では、Cisco IPICS の配置モデルについて説明します。これらのモデルは、Cisco IPICS の配置を設計する際に参考として利用できます。

この章では、次のトピックについて取り上げます。

単一サイト モデル

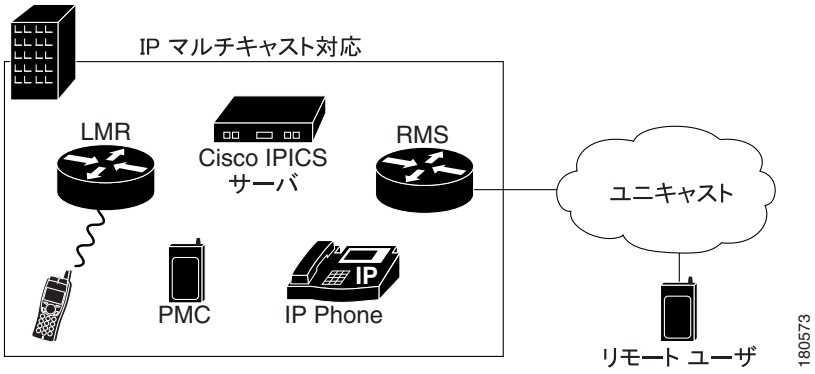
Cisco IPICS の単一サイト モデルは、単一のマルチキャスト ドメインに配置する状況を表しています。Cisco IPICS のコンポーネントはマルチキャスト対応の 1 つのサイトまたはキャンパスに配置され、IP WAN 上で Cisco IPICS マルチキャスト サービスは提供されません。一般的に、LAN または MAN に対しては単一サイト モデルを配置し、サイト内のマルチキャスト音声トラフィックを伝送します。LAN を越えた先または MAN からのコールは、Cisco IPICS のリモート機能を使用して、SIP ベースのユニキャスト コールを通じて Cisco IPICS ドメインに接続します。

単一サイト モデルの設計上の特長は、次のとおりです。

- Cisco IPICS サーバ
- RMS
- PMC
- Cisco Unified IP Phone
- LMR ゲートウェイ（オプション）
- PIM sparse モードを使用するマルチキャスト対応ネットワーク
- 会議およびトランスコーディングのための RMS デジタル シグナル プロセッサ（DSP）リソース

図 7-1 に、Cisco IPICS の単一サイト モデルを示します。

図 7-1　単一サイト モデル



単一サイト モデルの利点

統合されたネットワーク ソリューションの単一インフラストラクチャには、コスト上の大きな利点があります。また、このソリューションの Cisco IPICS では、企業の IP ベース アプリケーションを利用できるようになります。単一サイトの配置では、サイトを完全に独立させることも可能です。IP WAN に依存しないため、WAN の障害または帯域幅不足によって Cisco IPICS のサービスや機能が失われることがありません。

単一サイト モデルのベスト プラクティス

Cisco IPICS の単一サイト モデルを実装する場合は、次のガイドラインに従ってください。

- 可用性の高い、耐障害性のあるインフラストラクチャを用意します。Cisco IPICS をインストールするには、安定したインフラストラクチャであることが重要です。このようなインフラストラクチャは、必要に応じてマルチサイト配置に変更することも容易です。
- すべてのローカル エンドポイントで G.711 コーデックを使用します。このコーディックの使用により、トランスコーディングで DSP リソースを消費することがなくなります。
- 高可用性、電話機用の接続オプション（インライン パワー）、QoS メカニズム、マルチキャスト、およびセキュリティ用の推奨ネットワーク インフラストラクチャを実装しています（詳細については、第 4 章「Cisco IPICS のインフラストラクチャに関する検討事項」を参照してください）。

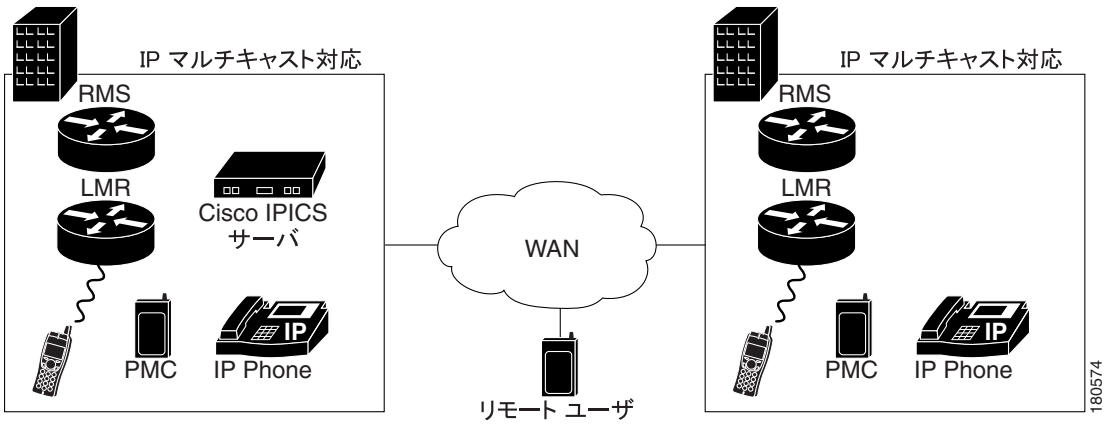
マルチサイト モデル

Cisco IPICS マルチサイト モデルは、単一の Cisco IPICS サーバから構成されています。この Cisco IPICS サーバは、2 つまたはそれ以上のサイトにサービスを提供し、IP WAN を使用してサイト間でマルチキャスト IP 音声トラフィックを転送します。また、IP WAN は、中央サイトとリモート サイト間のコール制御信号も伝送します。

サイト間では、マルチキャストを有効にすることができますが、マルチキャストは必須ではありません。マルチキャスト対応の WAN で接続されたマルチサイトは、マルチキャスト ドメインが 1 つしかないため、実質的には変型トポロジの単一サイト モデルです。マルチサイト モデル配置において主な差異となるのは、コア ネットワークの接続が、Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）を採用したサービス プロバイダー ネットワークであるかどうかです。これに該当する場合は、マルチキャスト VPN を使用した MPLS が配置され、サイト間に単一のマルチキャスト ドメインが構築されます。サイト間にネイティブ マルチキャスト サポートがないマルチサイトの場合は、サイト間に Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）を利用したマルチキャストまたは M1:U12:M2 のいずれかを導入します。サイト間に IPSec VPN を設定して、サイト間トラフィックを保護することもできます。

図 7-2 は、中央サイトに Cisco IPICS サーバがあり、すべてのサイトが IP WAN で接続される典型的な Cisco IPICS マルチサイト配置を示しています。

図 7-2　マルチサイト モデル



マルチサイト モデルにおける IP WAN の接続オプションには、次のものがあります。

- 専用回線
- フレームリレー
- 非同期転送モード（ATM）
- ATM とフレームリレーのサービス インターワーキング（SIW）
- MPLS バーチャル プライベート ネットワーク
- 音声およびビデオ対応 IP Security Protocol VPN（IPSec VPN（V3PN））

WAN エッジに置かれているルータには、プライオリティ キューイングやトラフィック シェーピングなどの Quality of Service（QoS）メカニズムが装備されていて、WAN の帯域幅が恒常的に不足している場合に、データ トラフィックから音声トラフィックを保護しています。

この項では、次のトピックについて取り上げます。

- マルチキャスト VPN を使用した MPLS（P. 7-4）
- マルチキャスト アイランド（P. 7-11）

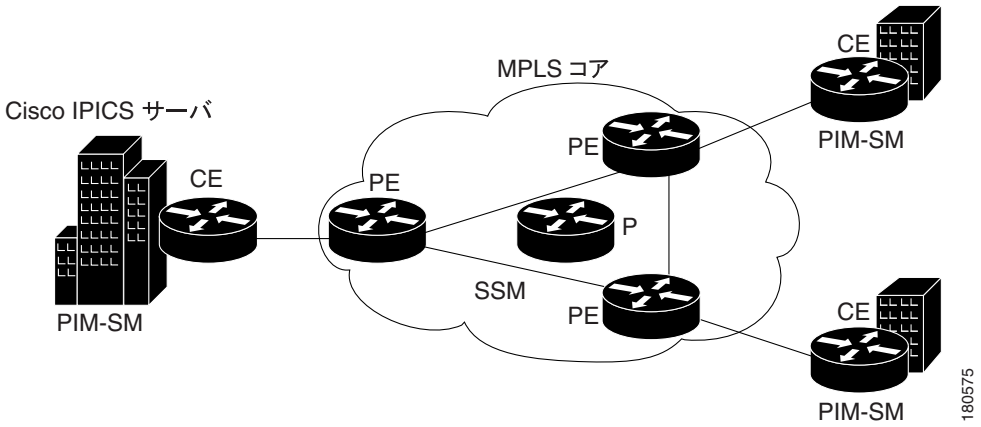
マルチキャスト VPN を使用した MPLS

MPLS は、MPLS VPN ではネイティブ マルチキャストをサポートしていません。この項では、MPLS コアを越えてマルチキャストを使用可能にする技術について説明します。ここでは、ユニキャスト MPLS コアと VPN が設定済みで正常に動作していること、および読者が IP マルチキャストと MPLS を理解していることを前提とします。これらのトピックの詳細については、次の URL で入手可能なマニュアルを参照してください。

http://www.cisco.com/en/US/products/ps6552/products_ios_technology_home.html

図 7-3 に、この項で扱うトポロジを示します。

図 7-3　マルチキャスト VPN を使用した MPLS



MPLS の用語

MPLS では、次の用語が使用されます。

- カスタマー エッジ ルータ（CE）：ネットワークの末端にあり、1 つ以上の プロバイダー エッジ（PE）ルータへのインターフェイスを備えているルータ。
- データ マルチキャスト ディストリビューション ツリー（MDT）：ネットワーク内にアクティブな送信元が存在する場合に、動的に作成されるツリー。別の PE ルータの背後にあるアクティブな受信者に送信されます。データ MDT の接続先となるのは、アクティブな送信元（またはアクティブな送信元からのトラフィックの受信側）を持つ CE ルータに接続された PE ルータ、またはアクティブな送信元（またはトラフィックの受信側）に直接接続された PE ルータだけです。
- デフォルト MDT：マルチキャスト バーチャル プライベート ネットワーク（MVPN）設定によって作成されるツリー。デフォルト MDT は、カスタマー コントロール プレーンと低レートのデータ プレーンのトラフィックに使用されます。このツリーは、マルチキャスト VPN ルーティングおよび転送（MVRF）を使用して、特定のマルチキャスト ドメイン（MD）内にあるすべての PE ルータを接続します。それぞれの顧客ネットワーク内にアクティブな送信元がある場合、すべての MD 内に 1 つずつデフォルト MD が存在します。
- LEAF：マルチキャスト データの受信者を記述します。送信元はルートと見なされ、宛先はリーフです。
- マルチキャスト ドメイン（MD）：マルチキャスト トラフィックを交換できる MVRF の集合。
- マルチキャスト VPN ルーティングおよび転送（MVRF）：MPLS コアの向こう側にマルチキャスト トラフィックを転送する方法を決定するために、PE ルータで使用されます。

- プロバイダー ルータ（P）：プロバイダー ネットワークのコアにあり、他の P ルータおよび他の PE ルータへのインターフェイスだけを備えたルータ。
- プロバイダー エッジ ルータ（PE）：プロバイダー ネットワークの末端にあり、他の P ルータおよび PE ルータ、および 1 台以上の CE ルータへのインターフェイスを備えたルータ。
- PIM-SSM：PIM 送信元固定マルチキャスト

MVPN の基本概念

MVPN を理解するには、次の基本概念を押さえておくことが重要です。

- サービス プロバイダーは、自社固有の IP マルチキャスト ドメイン（P ネットワーク）を持った IP ネットワークを保有します。
- MVPN を利用する顧客は、それぞれ固有の IP マルチキャスト ドメイン（C ネットワーク）を持った IP ネットワークを保有します。
- サービス プロバイダーの MVPN ネットワークは、顧客の IP マルチキャスト データをリモートの顧客サイトに転送します。転送を実行するために、サービス プロバイダーは自社の PE で顧客のトラフィック（C パケット）を P パケットの内部にカプセル化します。カプセル化された P パケットは、P ネットワーク内のネイティブ マルチキャストとしてリモートの PE サイトに転送されます。
- カプセル化された P パケットを転送するプロセスの実行中、P ネットワークは C ネットワークのトラフィックについてまったく情報を持っていません。PE は、両方のネットワークに参加するデバイスです（1 つの PE に対して複数の顧客ネットワークが存在する場合もあります）。

VPN マルチキャスト ルーティング

MVPN ネットワークの PE ルータは、複数のルーティング テーブルを保持します。1 つのグローバル ユニキャスト / マルチキャスト ルーティング テーブル、および直接接続された各 MVRF のユニキャスト / マルチキャスト ルーティング テーブルがあります。

マルチキャスト ドメインは、VPN からのマルチキャスト パケットを、コア内でルーティングされるマルチキャスト パケットの中にカプセル化するという原理に基づいています。コア ネットワーク内でマルチキャストが使用されるため、コア内に PIM を設定する必要があります。MVPN のプロバイダー コアの内部では、PIM-SM、PIM-SSM、PIM-BIDIR がサポートされます。PIM-BIDIR はどのプラットフォームでもサポートされるわけではないため、プロバイダー コア内で推奨される PIM オプションは、PIM-SM または PIM-SSM です。MVPN の内部では、PIM-SM、PIM-SSM、PIM-BIDIR、および PIM-DENSE-MODE がサポートされます。MVPN は、マルチキャスト ディストリビューション ツリー（MDT）を利用します。MDT は PE ルータを送信元としており、マルチキャスト宛先アドレスを持っています。同じ MVPN のサイトを保持している PE ルータは、デフォルト MDT の送信元となり、デフォルト MDT に参加して、このツリー上でトラフィックを受信します。

また、デフォルト MDT は常時オンのツリーであり、PIM 制御トラフィック、dense モード トラフィック、および rp ツリー (*, G) トラフィックを伝送します。同じデフォルト MDT を使用して設定されている PE ルータは、すべてこのトラフィックを受信します。

データ MDT はオンデマンドで作成されるツリーであり、当該のトラフィックを必要とする受信者がいる PE ルータだけが参加します。データ MDT は、トラフィック レートしきい値、または送信元グループ ペアのいずれかに基づいて作成できます。デフォルト MDT では、MVPN を構成するすべての VPN ルーティングおよび転送（VRF）が同じグループ アドレスを持っている必要があります。PIM-SSM が使用されている場合、複数のデータ MDT が同じグループ アドレスを持つことがあります。PIM-SM が使用されている場合、データ MDT はそれぞれ別のグループ アドレスを持っている必要があります。これは、アドレスが同じである場合、PE ルータが不要なトラフィックを受信する可能性があるためです。

MVPN のためのプロバイダー ネットワークの設定

この項では、プロバイダー ネットワークを MVPN 用に設定する方法の例を示します。

ここでは、図 7-3 に示したトポロジを取り上げ、プロバイダー ネットワークで MVPN を使用できるようにするための手順を説明します。この手順では、顧客 VPN は「ipics」と呼ばれています。

手順

ステップ 1　プロバイダー ネットワークの PIM モードを選択します。

シスコでは、コアのプロトコルには PIM-SSM をお勧めします。送信元検出のアトリビュートを使用した、追加の送信元検出 BGP 設定が必要ありません。MDT グループ アドレスを持つ MDT の送信元のアドバタイズには、Route Distinguisher（RD; ルート識別子）タイプが使用されます。PIM-SM は最も広く普及しているマルチキャスト プロトコルであり、適用対象が分散している場合と集中している場合のいずれにも使用されます。PIM SSM は、PIM SM に基づいています。初期共有ツリーがなく、以降の最短パス ツリーへのカットオーバーもないため、PIM SSM と PIM SM のどちらもデフォルト MDT での運用に適しています。

すべての関連ハードウェアで双方向 PIM サポートが使用可能になった場合、デフォルト MDT には双方向 PIM をお勧めします。データ MDT には、PIM SM または PIM SSM が適しています。PIM SM よりも PIM SSM のほうが配置は簡単です。ランデブー ポイントが不要であり、プロバイダー ネットワークは既知の安定したマルチキャスト デバイスのグループです。シスコでは、プロバイダーのコア配置には PIM SSM を使用することをお勧めします。この設定例では、コアに PIM-SSM を使用します。

ステップ 2　プロバイダー ネットワークの内部で使用される VPN グループ アドレスを選択します。

デフォルト PIM-SSM の範囲は 232/8 です。ただし、このアドレス範囲はインターネットでのグローバルな使用のために設計されたものです。プライベート ドメインの内部で使用する場合は、この管理スコープ マルチキャスト範囲の外側にあるアドレスを使用します（これは、RFC 2365 で推奨されています）。プライベート アドレス範囲を使用することで、境界ルータ上でのフィルタリングが単純になります。シスコでは、239.232/16 を使用することをお勧めします。この範囲のアドレスは、プライベート アドレスであることが簡単に分かり、2 番目のオクテットに 232 が使用されているので、SSM アドレスであることもすぐに分かるためです。このマニュアルで説明する設計では、この範囲をデフォルト MDT とデータ MDT に割り振ります（データ MDT については、P.7-5 の「VPN マルチキャスト ルーティング」で説明しています）。デフォルト MDT では 239.232.0.0 ～ 239.232.0.255 を使用し、データ MDT では 239.232.1.0 ～ 239.232.1.255 を使用します。このアドレス範囲では、PE ルータ 1 台あたり最大で 255 の MVRF をサポートできます。

ステップ 3　プロバイダー ネットワークを PIM-SSM 用に設定します。

次のコマンドを使用して、基本的な PIM-SSM サービスを有効にします。

- すべての P ルータおよび PE ルータについて、次のコマンドをグローバルに設定します。

```
ip multicast-routing
ip pim ssm range multicast_ssm_range
ip access-list standard multicast_ssm_range
 permit 239.232.0.0 0.0.1.255
```

- コアに直接接続されるすべての P インターフェイスと PE インターフェイスについて、次のコマンドを設定します。

```
ip pim sparse-mode
```

- 各 PE ルータで、BGP セッションの送信元となるために使用されるループバック インターフェイスに対して次のコマンドを設定します。

```
ip pim sparse-mode
```

ステップ 4　VRF の MDT を設定します。

- VRF のマルチキャスト ルーティングを設定するには、VRF ipics で使用されるすべての PE ルータについて次のコマンドを設定します。

```
ip vrf ipics
mdt default 239.232.0.0
```

- この VRF でマルチキャスト ルーティングを有効にするには、次のコマンドを設定します。

```
ip multicast-routing vrf ipics
```

ステップ 5　VPN 内部の PIM モードを設定します。

VPN 内部の PIM モードは、VPN の顧客がどのタイプの PIM を使用するかに応じて異なります。シスコは、auto-rp または Bootstrap Router（BSR; ブートストラップ ルータ）を通じて、VPN 内部で使用されているグループ モードの自動検出を提供しています。検出のための追加設定は不要です。また、PE ルータを VPN 内部の RP として設定すると、プロバイダーが顧客に RP を提供することもできます。この項で説明するトポロジでは、VPN の顧客が RP サービスを提供し、PE ルータが auto-rp を通じて group-to-rendezvous point（RP）マッピングを自動的にラーニングします。

PE-CE インターフェイスは、すべて sparce-dense-mode に設定します。この設定によって、auto-rp または BSR メッセージのいずれかが受信および転送され、PE が VPN 内部の group-to-rendezvous point（RP）をラーニングできるようになります。このように設定するには、インターフェイスに直接接続するすべての顧客について、次のコマンドを設定します。

```
ip pim sparse-mode
```

MVPN のためのプロバイダー ネットワークの確認

P.7-6 の「MVPN のためのプロバイダー ネットワークの設定」で説明した設定を完了した後は、設定内容が正しいことを次の手順に従って確認します。

手順

ステップ 1　BGP アップデートを確認します。

BGP は、SSM が使用されている場合は送信元検出に対応します。この機能は BGP-MDT アップデートと呼ばれます。すべての BGP-MDT アップデートが PE ルータで正しく受信されたことを確認するには、次のいずれかの操作を行います。

- **show ip pim mdt bgp** コマンドを使用します。

```
PE1#show ip pim mdt bgp
Peer (Route Distinguisher + IPv4)            Next Hop
  MDT group 239.232.0.0
   2:65019:1:10.32.73.248                    10.32.73.248 (PE-2 Loopback)
   2:65019:1:10.32.73.250                    10.32.73.250 (PE-3 Loopback)
```

2:65019:1 は、このアップデートに関連付けられている RD タイプ（2）および RD（65019:1）を示しています。

以降に出力されているのは、BGP セッションの送信元となるために使用されるアドレスです。

- **show ip bgp vpnv4 all** コマンドを使用します。

```
PE1#show ip bgp vpnv4 all
BGP table version is 204, local router ID is 10.32.73.247
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 65019:1 (default for vrf ipics)
*>i10.32.72.48/28   10.32.73.248             0    100      0 ?
... (output omitted)
Route Distinguisher: 2:65019:1
*> 10.32.73.247/32  0.0.0.0                                0 ?
*>i10.32.73.248/32  10.32.73.248             0    100      0 ?
*>i10.32.73.250/32  10.32.73.250             0    100      0 ?
```

ステップ 2　グローバル mroute テーブルを確認します。

show ip mroute mdt-group-address コマンドを使用して、各 PE ルータの (Source, Group) エントリが存在することを確認します。PIM-SSM が使用されているため、送信元は BGP セッションの送信元となるために使用されるループバック アドレスであり、グループは、設定されている MDT アドレスです。トラフィックが発生していない場合は、デフォルト MDT エントリだけが示されます。

```
PE1#show ip mroute 239.232.0.0
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report, Z - Multicast Tunnel
       Y - Joined MDT-data group, y - Sending to MDT-data group
Outgoing interface flags: H - Hardware switched
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode

(10.32.73.247, 239.232.0.0), 1w0d/00:03:26, flags: sTZ
  Incoming interface: Loopback0, RPF nbr 0.0.0.0
  Outgoing interface list:
    FastEthernet0/0, Forward/Sparse, 1w0d/00:02:47

(10.32.73.248, 239.232.0.0), 1w0d/00:02:56, flags: sTIZ
  Incoming interface: FastEthernet0/0, RPF nbr 10.32.73.2
  Outgoing interface list:
    MVRF ipics, Forward/Sparse, 1w0d/00:01:30

(10.32.73.250, 239.232.0.0), 1w0d/00:02:55, flags: sTIZ
  Incoming interface: FastEthernet0/0, RPF nbr 10.32.73.2
  Outgoing interface list:
    MVRF ipics, Forward/Sparse, 1w0d/00:01:29
```

各 (S, G) エントリに対して s フラグが設定されていることを確認します。s フラグは、このグループが ssm モードで使用されていることを示します。z フラグが設定されていることを確認します。z フラグは、この PE ルータがマルチキャスト トンネルのリーフであることを示します。ルータは、マルチキャスト トンネルのリーフである場合、基本的にはこのトラフィックの受信者であるため、ルータは追加の検索を実行して、このトラフィックの転送先となる MVRF を特定する必要があります。リモート PE の (S, G) エントリに I フラグが設定されていることを確認します。このフラグは、自身が SSM グループに参加していることをルータが認識していることを示します。これは、IGMPv3 ホストが当該の特定チャネルへの参加を要求したような状態になります。

ステップ 3　グローバル テーブル内の PIM ネイバーを確認します。

すべての PE ルータおよび P ルータについて **show ip pim neighbors** コマンドを使用して、PIM ネイバーがグローバル テーブル内に適切に設定されていることを確認します。

```
PE1#show ip pim neighbor
PIM Neighbor Table
Neighbor          Interface                Uptime/Expires    Ver   DR
Address                                                            Prio/Mode
10.32.73.2        FastEthernet0/0          1w4d/00:01:21     v2    1 / DR
10.32.73.70       Serial0/2                1w4d/00:01:29     v2    1 / S
```

ステップ 4　VPN 内部の PIM ネイバーを確認します。

すべての PE ルータについて **show ip pim vrf ipics neighbors** コマンドを使用し、CE ルータが PIM ネイバーとして示されること、およびリモート PE ルータがトンネル上の PIM ネイバーとして示されることを確認します。

```
PE1#show ip pim vrf ipics neighbor
PIM Neighbor Table
Neighbor          Interface                Uptime/Expires    Ver   DR
Address                                                            Prio/Mode
10.32.73.66       Serial0/0                1w3d/00:01:18     v2    1 / S
10.32.73.248      Tunnel0                  3d17h/00:01:43    v2    1 / S
10.32.73.250      Tunnel0                  1w0d/00:01:42     v2    1 / DR S
```

ステップ 5　VPN の group-to-rendezvous point（RP）マッピングを確認します。

メインの顧客サイトは、VPN 内部で auto-rp を使用するように設定されています。VPN IPICS は、マルチキャスト範囲 239.192.21.64 ～ 79 をチャネルおよび VTG 用に使用します。

```
ip pim send-rp-announce Loopback0 scope 16 group-list multicast_range
ip pim send-rp-discovery scope 16
ip access-list standard multicast_range
 permit 239.192.21.64 0.0.0.15
```

show ip pim vrf ipics rp mapping コマンドを使用して、PE ルータが group-to--rendezvous point（RP）マッピング情報を VPN から正しくラーニングしたことを確認します。

```
PE1#show ip pim vrf ipics rp map
PIM Group-to-RP Mappings

Group(s) 239.192.21.64/28
  RP 10.32.72.248 (?), v2v1
    Info source: 10.32.73.62 (?), elected via Auto-RP
         Uptime: 1w3d, expires: 00:02:54
```

この出力は、PE ルータが group-to-rendezvous point（RP）を正しくラーニングし、この情報が VPN 内部で使用されることを示しています。デフォルト MDT は、マルチキャスト複製が実行されるプロバイダー ネットワークのコアにあるすべての PE ルータに到達します。デフォルト MDT だけが設定されている場合は、PE ルータがトラフィックの受信を必要としているかどうかにかかわらず、すべての PE ルータにこのトラフィックが到達します。

トラフィック転送の最適化：データ MDT

データ MDT は、トラフィックの転送を最適化するために設計されたものです。データ MDT は、オンデマンドで作成されるマルチキャスト ツリーです。データ MDT の作成基準は、トラフィック負荷のしきい値（Kbps 単位）、または VPN 内の特定の送信元を指定したアクセス リストです。データ MDT を作成するのは、自身のサイトに送信元が接続されている PE だけです。データ MDT の条件を設定する必要はありません。ただし、VPN 内部の各 (S, G) に対して条件が設定されていなくても、データ MDT は作成されます。このデータ MDT は、ルータのリソースを必要とします。したがって、送信元が存在するという理由だけではデータ MDT を作成しないことをお勧めします。非ゼロのしきい値を使用することをお勧めします。この値にすると、アクティブな送信元がある場合に限り、データ MDT の作成が開始されるためです。マルチキャスト VPN ルーティングおよび転送（MVRF）エントリの最大数は、256 です。

VRF のデータ MDT を設定するには、P.7-6 の「MVPN のためのプロバイダー ネットワークの設定」のステップ 2 で説明したいずれかの範囲を使用します。VRF ごとに、最大で 256 のアドレスを使用できます。この制限はプロトコルによる制約ではなく、実装時に選択したものです。SSM が使用されるため、データ MDT のアドレス範囲は、同じ VPN のすべての PE ルータで同一です。データ MDT に使用されるアドレスの数を指定するには、次のコマンドのように逆マスクを使用します。

```
ip vrf ipics
 mdt data 239.232.1.0 0.0.0.255 threshold 1
```

データ MDT の正常動作の確認

データ MDT は、グローバル テーブルに mroute エントリを作成します。また、送信側および受信側 PE ルータの機能を確認するコマンドもあります。データ MDT の動作を確認するには、設定済みのしきい値を超えるマルチキャスト トラフィックがサイト間に存在している必要があります。データ MDT をテストする簡単な方法は、あるサイトのマルチキャスト グループに静的に参加して、そのグループを別のサイトから ping することです。次に例を示します。

CE1

```
interface Loopback0
 ip address 10.32.72.248 255.255.255.255
 ip pim sparse-mode
 ip igmp join-group 239.192.21.68
```

CE2

```
ping 239.192.21.68 size 500 repeat 100
```

データ MDT の動作を確認するには、次の手順を実行します。

ステップ 1　送信側 PE ルータを確認します。

show ip pim vrf ipics mdt send コマンドを送信側 PE ルータ（PE2）で使用して、データ MDT の設定を確認します。

```
PE2#show ip pim vrf ipics mdt send
MDT-data send list for VRF: ipics
  (source, group)                  MDT-data group      ref_count
  (10.32.72.244, 239.192.21.68)    239.232.1.0         1
  (10.32.73.74, 239.192.21.68)     239.232.1.1         1
```

ステップ 2　受信側 PE ルータを確認します。

show ip pim vrf ipics mdt receive detail コマンドを受信側 PE ルータ（PE1）で使用して、このルータがデータ MDT 上で受信していることを確認します。

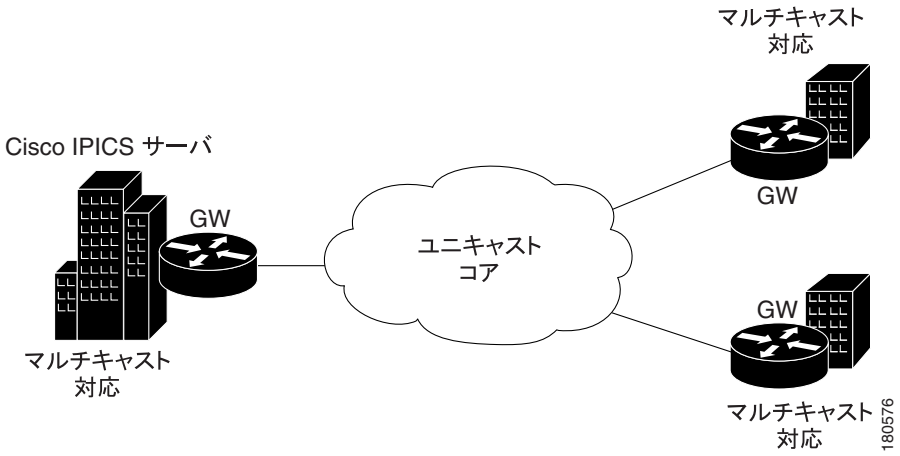
```
PE1#show ip pim vrf ipics mdt receive

Joined MDT-data [group : source] for VRF: ipics
 [239.232.1.0 : 10.32.73.248] ref_count: 1
 [239.232.1.1 : 10.32.73.248] ref_count: 1
```

すべてが正しく設定されている場合は、この時点で VPN IPICS 内のサイトが MVPN を使用してマルチキャスト トラフィックを伝送でき、すべてのサイトが同じマルチキャスト ドメインに所属します。したがって、Cisco IPICS サーバ上のすべてのチャネルとユーザを同じロケーションを使用して設定できます。

マルチキャスト アイランド

マルチキャスト アイランドとは、マルチキャストが使用可能になっているサイトです。ユニキャストのみの接続で相互に接続された複数のマルチキャスト アイランドで、マルチサイト配置を構成することができます。図 7-4 を参照してください。

図 7-4　マルチキャスト アイランド



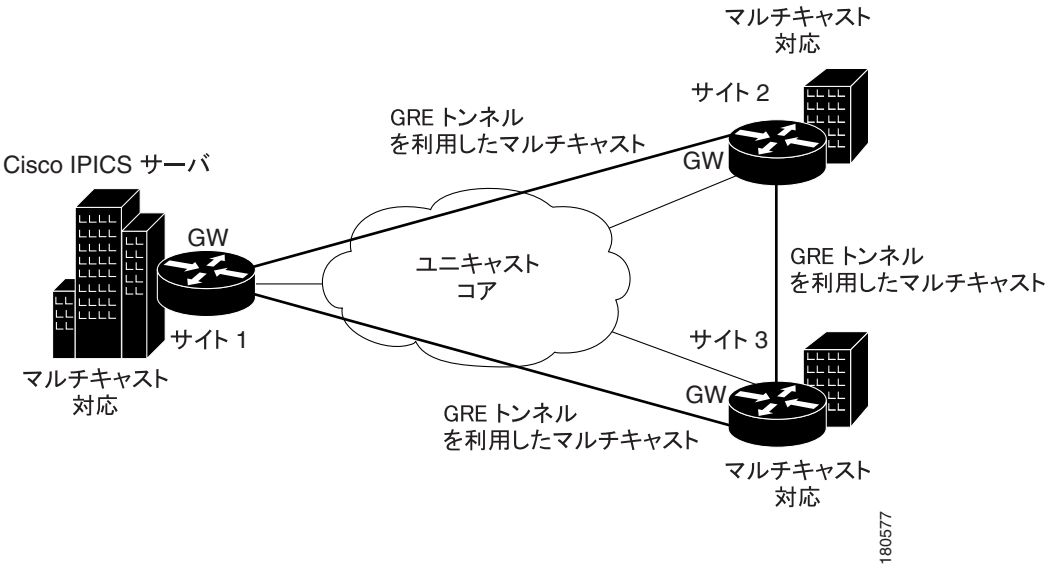
次のいずれかの方法を使用することで、アイランド間にマルチキャスト サポートを提供できます。

- GRE を利用したマルチキャスト（P. 7-12）
- M1:U12:M2 接続トランク（P. 7-14）

GRE を利用したマルチキャスト

この項では、GRE を利用したマルチキャストを設定する方法の概要を示します。図 7-5 は、GRE を利用したマルチキャストを導入した Cisco IPICS 配置を示しています。

図 7-5　GRE トンネルを利用したマルチキャスト



トンネルは、サイト 1 のゲートウェイとサイト 2 のゲートウェイの間に設定します。このトンネルは、それぞれのゲートウェイの loopback0 インターフェイスを送信元としています。トンネル インターフェイスに対して **ip pim sparse-dense mode** コマンドを設定し、ゲートウェイ ルータ上でマルチキャスト ルーティングを有効にします。トンネル インターフェイスに対して sparse-dense モードを設定することで、グループの RP 設定に応じて、sparse モードまたは dense モードのパケットをトンネル上で転送できるようになります。

次の例は、GRE を利用したマルチキャストをサイト 1 とサイト 2 の間に実装するために必要な設定を示しています。サイト 1 とサイト 3、およびサイト 2 とサイト 3 の間でも、同じ方法を使用します。

```
interface loopback 0
 ip address 1.1.1.1 255.255.255.255

interface Tunnel0
 ip address 192.168.3.1 255.255.255.252
 ip pim sparse-mode
 tunnel source Loopback0
 tunnel destination 2.2.2.2
```

サイト 2

```
ip multicast-routing

interface loopback 0
 ip address 2.2.2.2 255.255.255.255

interface Tunnel0
 ip address 192.168.3.2 255.255.255.252
 ip pim sparse-mode
 tunnel source Loopback0
 tunnel destination 1.1.1.1
```

トンネル上で PIM sparse モードを設定する場合は、必ず次のガイドラインに従ってください。

- 共有ツリー (*, G) 上を RP から流れるマルチキャスト トラフィックの RPF 確認を正しく実行するには、RP アドレスに対して、トンネル インターフェイスをポイントする **ip mroute rp-address nexthop** コマンドを設定します。

  たとえば、サイト 1 に RP（RP アドレス 10.1.1.254）があるとします。この場合、サイト 2 のゲートウェイの mroute は **ip mroute 10.1.1.254 255.255.255.255 tunnel 0** コマンドになります。このコマンドによって、共有ツリー上を流れるトラフィックの RPF 確認が正しく実行されます。
- 最短パス ツリー（SPT）上を流れるマルチキャスト (S, G) トラフィックの RPF 確認を正しく実行するには、マルチキャスト送信元に対して、各ゲートウェイ ルータ上のトンネル インターフェイスをポイントする **ip mroute source-address nexthop** コマンドを設定します。

  この場合、SPT トラフィックがトンネル インターフェイス上を流れるときは、**ip mroute 10.1.1.0 255.255.255.0 tunnel 0** コマンドをサイト 2 ゲートウェイ上で設定し、**ip mroute 10.1.2.0 255.255.255.0 tunnel 0** コマンドをサイト 1 ゲートウェイ上で設定します。この設定によって、Tu0 インターフェイス上の着信マルチキャスト パケットの RPF 確認が正しく実行されるようになります。

GRE を利用したマルチキャストを使用する場合の帯域幅の考慮事項

Cisco IPICS は、G.711 コーデックと G.729 コーデックのどちらでも動作します。表 7-1 に、ユニキャスト接続トランク上での音声コールの帯域幅要件を示します。この帯域幅は、使用されるコーデック、ペイロードのサイズ、および cRTP と VAD のいずれかまたは両方が設定されるかどうかに基づいて決まります。

表 7-1　ユニキャスト接続トランクでの帯域幅に関する考慮事項

圧縮技術	ペイロードのサイズ（バイト数）	フル レートの帯域幅（Kbps）	cRTP 使用時の帯域幅（Kbps）	VAD 使用時の帯域幅（Kbps）	cRTP と VAD 使用時の帯域幅（Kbps）
G.711	240	76	66	50	43
G.711	160	83	68	54	44
G.729	40	17.2	9.6	11.2	6.3
G.729	29	26.4	11.2	17.2	7.3

トンネルを通過するときの帯域幅消費は、サイト間で通信中のアクティブなチャネル、VTG、PMC ユーザの数によって決まります。

トンネル通過時の帯域幅を計算する方法の例として、次の場合を取り上げます。

ケース 1：サイト 1 とサイト 2 にアクティブなチャネルが存在

サイト 1 内のすべてのユーザが 1 つのチャネルを使用し、サイト 2 内のすべてのユーザが別のチャネルを使用しています。トンネルを通過するマルチキャスト音声フローはありません。

ケース 2：サイト 1 のアクティブなチャネルに n 人のユーザ、サイト 2 のアクティブなチャネルに m 人のユーザ

次の例の「コール帯域幅」は、表 4-2 の帯域幅値です。

帯域幅 1 = コール帯域幅 * n（サイト 1 からサイト 2 へのフロー）

帯域幅 2 = コール帯域幅 * m（サイト 2 からサイト 1 へのフロー）

合計帯域幅 = 帯域幅 1 + 帯域幅 2

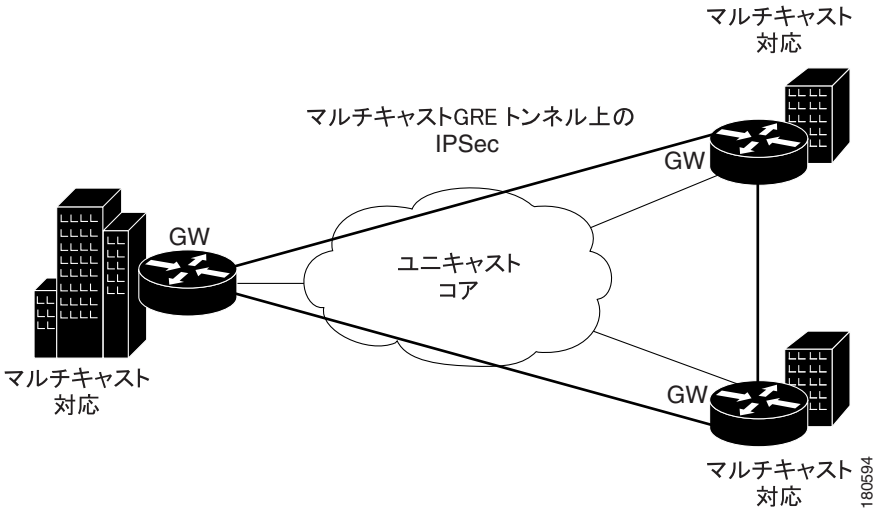
（「コール帯域幅」は表 3-1 の値）

アクティブなチャネルの数、チャネルごとのアクティブなユーザの数、およびチャネルが複数のサイトに広がっているかどうかによっては、帯域幅の使用率が重要な意味を持ちます。

IPSec VPN

マルチキャスト GRE トンネル上に IPSec VPN を実装できます。図 7-6 を参照してください。

図 7-6　マルチキャスト GRE トンネル上での IPSec

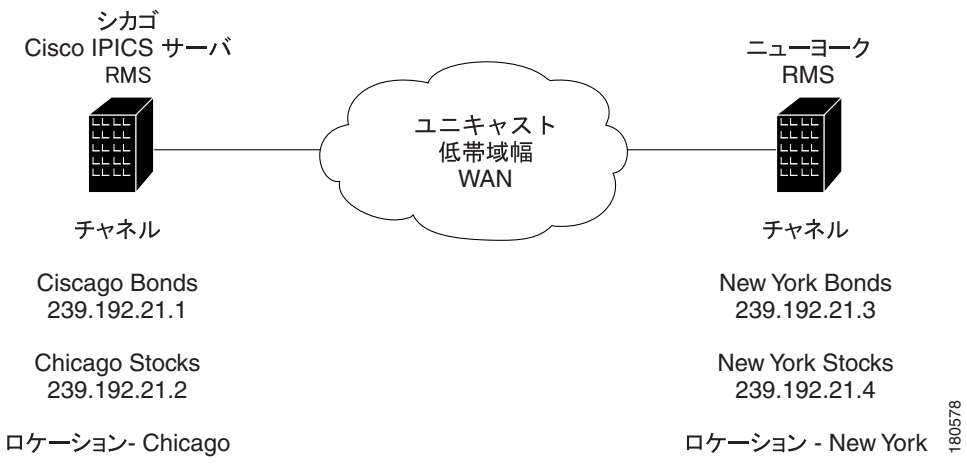


GRE トンネル上に IPSec を設定する方法は、数多くあります。適切なシスコ マニュアルを参照してください。

M1:U12:M2 接続トランク

M1:U12:M2 接続トランクは、リアルタイムのマルチキャスト音声トラフィックを Cisco IPICS アイランド間で伝送する場合に、GRE トンネルを利用したマルチキャストの代替となる手段です。たとえば、図 7-7 に示した状況について考えます。

図 7-7　ユニキャストのみのサイト間接続



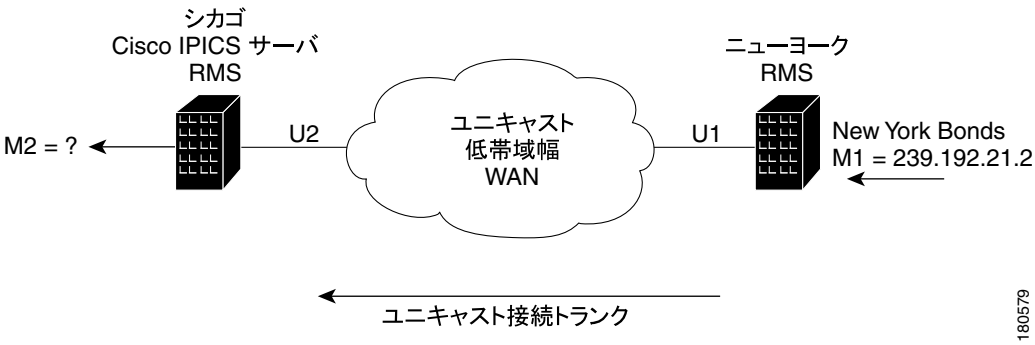
この例では、Stocks and Bonds Company 社がシカゴとニューヨークにオフィスを構えています。各ロケーションに対して、Cisco IPICS サーバ上に 2 つのチャネルが設定されています。シカゴとニューヨークの間にマルチキャスト サポートが存在しないため、このシナリオでは、それぞれに別のマルチキャスト ドメインを設定し、独自の RP を配置する必要があります。Cisco IPICS サーバ上に設定されるロケーションは、2 つのマルチキャスト ドメイン Chicago と New York を表しています。シカゴのチャネルおよび RMS はロケーション Chicago を使用して設定し、ニューヨークのチャネルおよび RMS はロケーション New York を使用して設定する必要があります。

シカゴにいるユーザは、Chicago Bonds チャネルまたは Chicago Stocks チャネルを使用して互いに通信できます。ニューヨークにいるユーザは、New York Bonds チャネルまたは New York Stocks チャネルを使用して互いに通信できます。

Chicago Stocks および Chicago Bonds は VTG 内に配置できます。これらのチャネルは両方ともロケーションが Chicago であるため、Cisco IPICS サーバは、シカゴの RMS を使用してこれらのチャネルを混合します。同様に、New York Stocks および New York Bonds も VTG 内に配置できます。これらのチャネルは両方ともロケーションが New York であるため、Cisco IPICS サーバは、ニューヨークの RMS を使用してこれらのチャネルを混合します。

ドメイン間 VTG は設定できません。VTG のロケーションは、自動的に All になります。このロケーションは、VTG 内のすべてのチャネルとユーザが同じマルチキャスト ドメイン内にあることを前提としています。この制限事項は、図 7-8 に示すように、M1:U12:M2 接続トランクを使用することで回避できます。

図 7-8　M1:U12:M2 接続トランク



この例では、Chicago Bonds と New York Bonds で構成される VTG が必要だとします。M1:U12:M2 接続トランクが New York Bonds チャネルからのマルチキャスト トラフィック（M1）をユニキャスト アドレス（U1）にマッピングして、このトラフィックをユニキャスト VoIP ネットワークを通じて伝送します。Chicago RMS が受信するユニキャスト トラフィックは、マルチキャスト アドレス M2 にマッピングされます。M2 マルチキャスト アドレスはシカゴの New York Bonds プロキシ チャネルに割り当てられ、Chicago Bonds チャネルを持つ VTG に配置されます。M2 には、Chicago マルチキャスト ドメイン内の有効なマルチキャスト アドレスが割り当てられている必要があります。競合を避けるため、マルチキャスト プールの一部であるアドレスや、他のチャネルで使用されるアドレスは使用しないでください。

ほとんどの配置には、チャネルで使用するために確保されたアドレス範囲があります。次の範囲リストは、一般的な割り当て方を示しています。

239.192.21.1 ～ 16：チャネル アドレス

239.192.21.17 ～ 32：VTG アドレス

また、次のアドレスが割り当てられているとします。

239.192.21.1：Chicago Bonds

239.192.21.2：Chicago Stocks

239.192.21.3：New York Bonds

239.192.21.4：New York Stocks

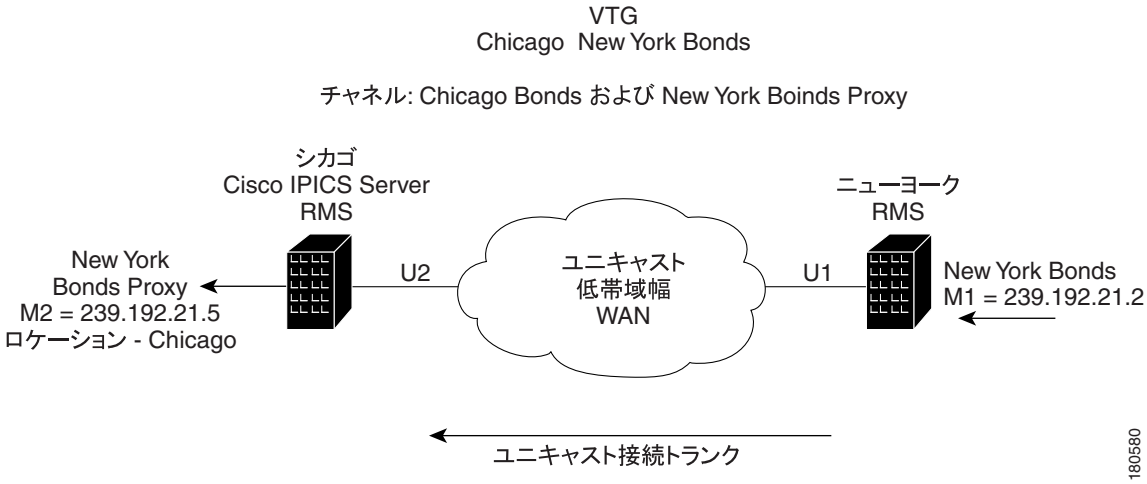
ここで、次のフリー アドレスである 239.192.21.5 が M2 に使用されているとします。VTG は、チャネル、ユーザ、またはこの両方を包含することができます。作成される VTG には Chicago Bonds チャネルが含まれていますが、New York Bonds を表すチャネルも含まれている必要があります。New York Bonds チャネルはこの VTG に配置できません。このチャネルは、Chicago の RMS から到達できるマルチキャストではないためです。したがって、ロケーション Chicago には New York Bonds チャネルを表すプロキシ チャネルが必要です。

New York Bonds プロキシ

239.192.21.5：ロケーション Chicago

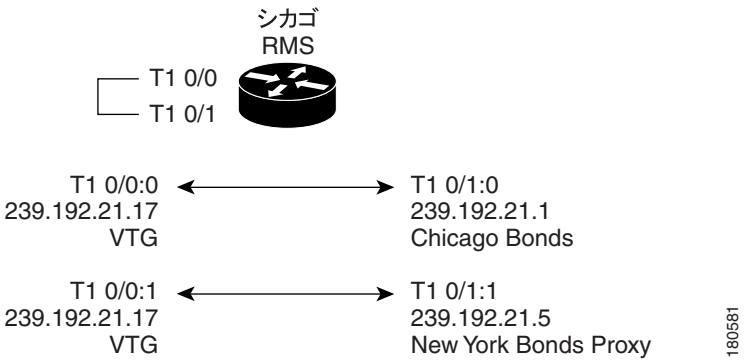
図 7-9 に、Chicago で New York Bonds チャネルのプロキシを設定する方法を示します。

図 7-9　プロキシ チャネル



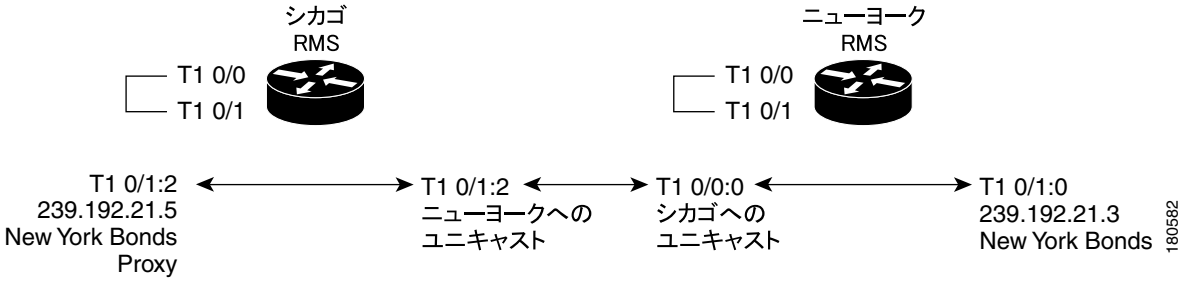
Chicago New York Bonds という VTG が Cisco IPICS サーバで作成される場合、この TG には Chicago Bonds と New York Bonds Proxy という 2 つのチャネルが含まれます。Cisco IPICS サーバはシカゴの RMS を設定して（どちらのチャネルもロケーションは Chicago）、2 つのチャネルをこの VTG に混合します。Cisco IPICS で、この VTG にマルチキャスト アドレス 239.192.21.17 を使用しているとします。チャネルを VTG に混合し、VTG をチャネルに混合するには、シカゴの RMS に DS0 のペアが 2 つ必要です。図 7-10 は、Cisco IPICS サーバが VTG「Chicago New York Bonds」のために実行するシカゴ RMS の設定を示しています。この RMS 設定は、2 チャネルの VTG における標準的なものです。

図 7-10　Cisco IPICS サーバが実行する VTG 設定



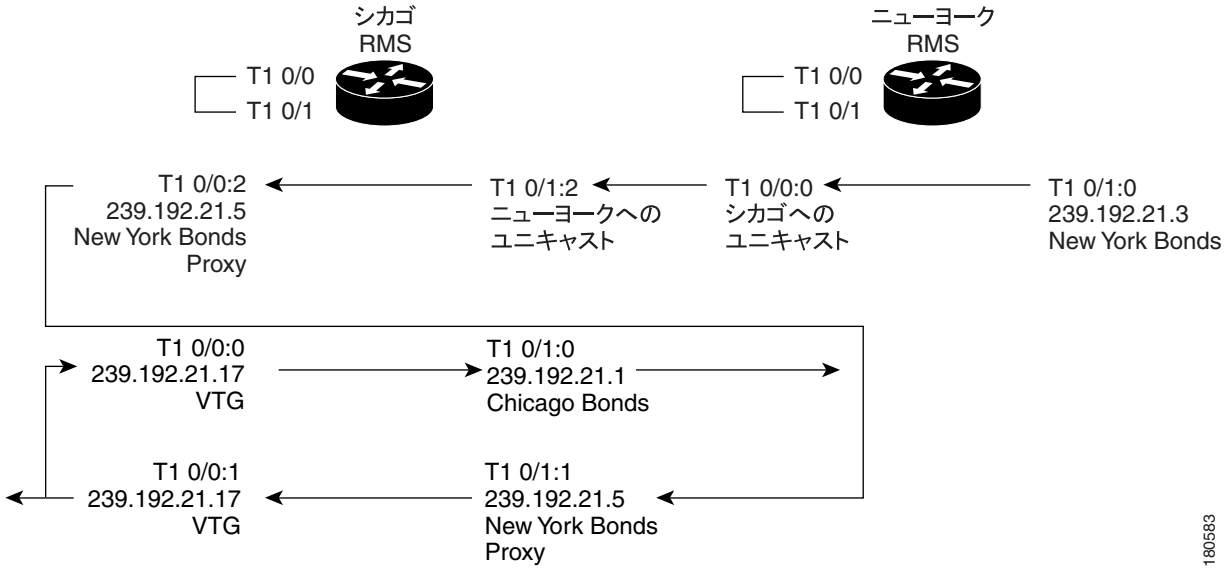
M1:U12:M2 接続トランクを実装するには、RMS を手動で設定する必要があります。この設定が必要になるのは、トラフィックを New York Bonds から VTG に、および VTG から New York Bonds に伝送するためです。図 7-11 を参照してください。

図 7-11　M1:U12:M2 トランクの設定



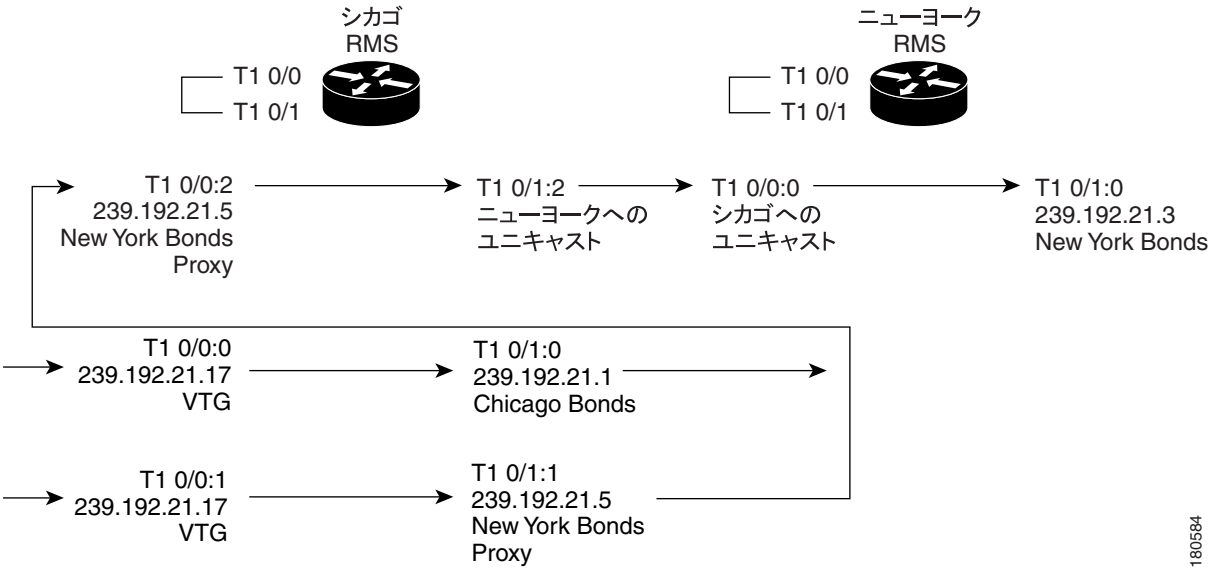
ニューヨークから VTG へのトラフィック フローを図 7-12 に示します。この例では、PMC、Cisco Unified IP Phone、LMR ゲートウェイに接続されている無線のいずれかを使用して、ニューヨークにいるユーザが New York Bonds チャネル上で発言します。宛先アドレスは、チャネルが Cisco IPICS サーバで設定されたときにチャネルに割り当てられたマルチキャスト アドレスです。このトラフィックは、ニューヨークの RMS に到達すると、接続トランクを通じてユニキャストとしてシカゴの RMS に送信されます。シカゴの RMS は、このニューヨークからのユニキャスト トラフィックを New York Bonds Proxy チャネルにマッピングします。このチャネルは VTG にマッピングされ、VTG は Chicago Bonds チャネルにマッピングされます。VTG チャネルまたは Chicago Bonds チャネルのいずれかを聞いているすべてのユーザが、トラフィックを受信します。

図 7-12　New York Bonds から VTG および Chicago Bonds



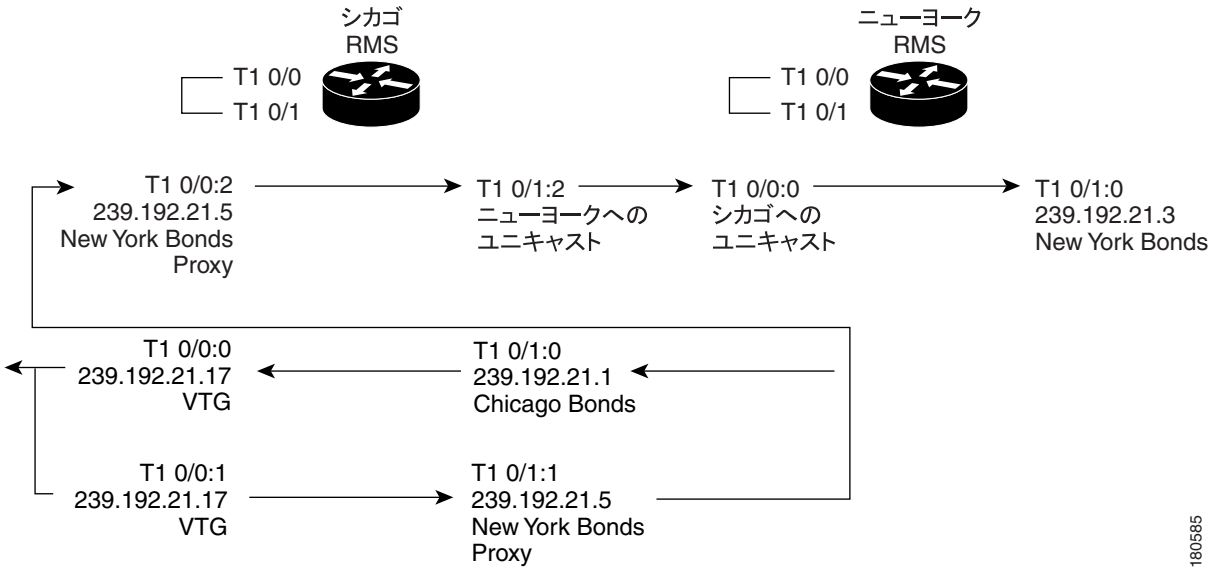
VTG から New York Bonds へのトラフィック フローを図 7-13 に示します。この例では、シカゴのユーザが VTG チャネルで発言すると、トラフィックがマルチキャスト グループ 239.192.21.17 に送信されます。このトラフィックは、シカゴの RMS に到達すると New York Bonds Proxy チャネルと Chicago Bonds チャネルの両方に混合されます。New York Bonds Proxy チャネルにマッピングされたトラフィックは、接続トランクを通じてユニキャストとしてニューヨークに送信され、ニューヨークで New York Bonds チャネルに混合されます。

図 7-13　VTG から Chicago Bonds および New York Bonds



Chicago Bonds から New York Bonds へのトラフィック フローを図 7-14 に示します。

図 7-14　Chicago Bonds から VTG および New York Bonds



トラフィックが VTG（図 7-13）と Chicago Bonds（図 7-14）のどちらから到達するかは、VTG の設定によって異なります。VTG は、チャネル、ユーザ、またはこの両方を包含することができます。VTG がチャネルだけ（Chicago Bonds と New York Bonds Proxy）を使用して作成されている場合、シカゴにいるユーザの PMC または Cisco Unified IP Phone には VTG チャネルが表示されません。また、Chicago Bonds チャネル上のシカゴのユーザ、および New York Bonds チャネル上のニューヨークのユーザは、自分が VTG に入っていることを知りません。シカゴのユーザは Chicago Bonds チャネルで送受信を実行し、ニューヨークのユーザは New York Bonds チャネルで送受信を実行します。VTG チャネルとの間で送受信される唯一のトラフィックは、シカゴの RMS への内部トラフィックです。

Chicago Bonds チャネルに関連付けられているユーザが VTG にも配置されている場合、そのユーザの PMC または Cisco Unified IP Phone には VTG が表示されます。このユーザは、Chicago Bonds チャネルまたは VTG チャネルのいずれかをアクティブにすることができます。VTG チャネルをアクティブにした場合、トラフィックは VTG のマルチキャスト アドレスに送信され、シカゴの RMS の Chicago Bonds チャネルと New York Bonds Proxy チャネルに混合されます。New York Bonds に関連付けられているユーザを VTG に配置することはできません。ユーザはロケーション New York にいて、VTG はシカゴの RMS に混合されるためです。

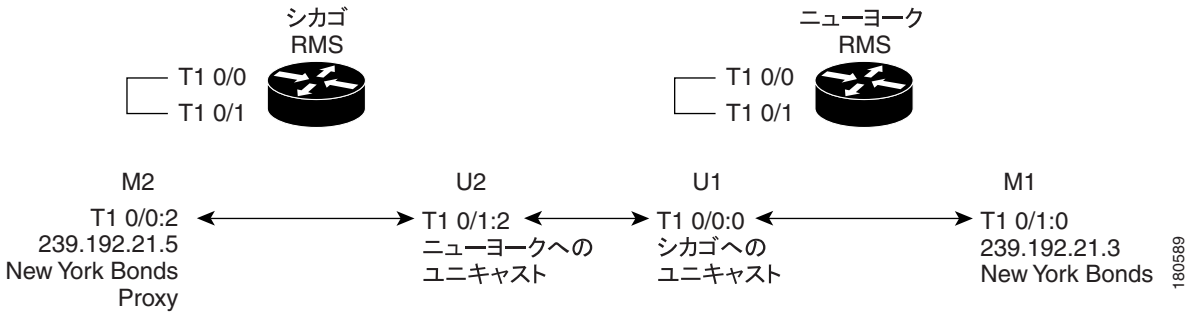
このソリューションは対称的です。ロケーション New York と New York Bonds チャネルで Chicago Bonds Proxy を使用して、VTG を作成することもできます。この場合、Cisco IPICS はシカゴの RMS ではなくニューヨークの RMS を使用し、動作はここで示した例とまったく同一になります。

ユニキャスト接続トランクの設定

この項では、ユニキャスト接続トランクに必要な手動での RMS 設定について説明し、M1:U12:M2 による、シカゴとニューヨークの Stocks and Bonds 社のシナリオを実現します。

図 7-15 に、シカゴとニューヨーク間で設定が必要になるユニキャスト接続トランクのコンポーネントを示します。

図 7-15　ユニキャスト接続トランクのコンポーネント



（LMR、PMC、または Cisco Unified IP Phone から）ダイヤルされる番号が存在しないため、内部でダイヤルされ、VoIP ダイヤル ピアと一致するかどうかが確認される番号を **connection trunk digits** コマンドを使用して生成します。この **connection trunk** コマンドによって、RMS ルータ間に永続的な VoIP コールも確立されます。以降の設定例では、RMS 上の T1 リソースを使用し、T1 ポートは次のように設定されているものとします。

```
controller T1 0/0
 framing esf
 clock source internal
 linecode b8zs
 cablelength short 133
 ds0-group 0 timeslots 24 type e&m-lmr
 ds0-group 1 timeslots 1 type e&m-lmr
 …
 ds0-group 23 timeslots 23 type e&m-lmr
```

RMS 上の T1 リソースを使用する場合は、接続トランクに使用される DS0 を使用しないように Cisco IPICS を設定する必要があります。

次の設定例では、RMS T1 ループバックの DS0 リソース 0/0 および 0/1 を使用します。このため、音声ポートを明示的にブロックして、Cisco IPICS サーバがこれらの音声ポートを動的に割り当てることを防止する必要があります。DS0 をブロックするには、Cisco IPICS Administration Console を使用して、シカゴ RMS のポート 0/0:2 とニューヨーク RMS のポート 0/0:0 を無効にします（手順については、『*Cisco IPICS Server Administration Guide, Release 2.1(1)*』の「Viewing and Configuring Loopbacks」の項を参照してください）。DS0 が Reserved 状態の場合、RMS は DS0 を動的に割り当てません。

（注） RMS を手動で設定する前に、RMS DS0 リソースが無効になっていることを確認してください。無効になっていないと、RMS によって手動設定が上書きされる場合があります。

次の表は、シカゴ RMS およびニューヨーク RMS コンポーネント内にある、接続トランクの U1 と U2 部分を設定するために必要な手動設定を示しています。Session Target フィールドでは、RMS 名を RMS Loopback0 の IP アドレスに置き換えます。

シカゴ ユニキャスト U2	ニューヨーク ユニキャスト U1
voice-port 0/1:2 timeouts call-disconnect 3 voice-class permanent 1 connection trunk 1000 answer mode dial-peer voice 1 voip destination-pattern 1000 session target ipv4:New York RMS (U2) codec g729r8 bytes 20 (Default) voice-class permanent 1 ip qos dscp cs5 media dial-peer voice 2 pots destination-pattern 2000 port 0/1:2	voice-port 0/0:0 timeouts call-disconnect 3 voice-class permanent 1 connection trunk 2000 dial-peer voice 1 voip destination-pattern 2000 session target ipv4:Chicago RMS (U1) codec g729r8 bytes 20 (Default) voice-class permanent 1 ip qos dscp cs5 media dial-peer voice 2 pots destination-pattern 1000 port 0/0:0

次の表は、ニューヨーク RMS の音声ポートとダイヤル ピア エントリを設定して M1:U12:M2 接続トランクの M1 部分を使用可能にするために必要となる、手動コマンドを示しています。

ニューヨークのマルチキャスト音声ポート	ニューヨークのマルチキャスト ダイヤル ピア M1
voice-port 0/1:0 voice-class permanent 1 auto-cut-through lmr m-lead audio-gate-in lmr e-lead voice no echo-cancel enable no comfort-noise timeouts call-disconnect 3 timing hookflash-in 0 timing hangover 40 connection trunk 2001	dial-peer voice 3 voip destination-pattern 2001 session protocol multicast session target ipv4:239.192.21.3:21000 (New York Bonds M1) codec g711ulaw voice-class permanent 1

次の表は、シカゴ RMS の音声ポートとダイヤル ピア エントリを設定して M1:U12:M2 接続トランクの M2 部分を使用可能にするために必要となる、手動コマンドを示しています。

シカゴのマルチキャスト音声ポート	シカゴのマルチキャスト ダイヤル ピア M2
voice-port 0/0:2 voice-class permanent 1 auto-cut-through lmr m-lead audio-gate-in lmr e-lead voice no echo-cancel enable no comfort-noise timeouts call-disconnect 3 timing hookflash-in 0 timing hangover 40 connection trunk 1001	dial-peer voice 3 voip destination-pattern 1001 session protocol multicast session target ipv4:239.192.21.5:21000 (New York Bonds Proxy M2) codec g711ulaw voice-class permanent 1

接続トランクの確認

次の出力は、接続トランクのステータスを調べるために RMS で使用できる Cisco IOS コマンドを示しています。この出力例では、使用されるダイヤル ピアが表示され、トランク接続が接続（connected）状態であることが示されています。

```
New York#show voice call status
CallID CID   ccVdb      Port      DSP/Ch Called # Codec    Dial-peers
0xF    11F0  0x6772A350 0/0:0.24  0/13:1 2000     g729r8   2/1
0x11   11F3  0x67729198 0/1:0.24  0/13:3 2001     g711ulaw 0/3
2 active calls found

Chicago#show voice call summary | i TRUNKED
0/1:2.24     g729r8      y S_CONNECT          S_TRUNKED
0/0:2:0.24   g711ulaw    y S_CONNECT         S_TRUNKED
```

ユニキャスト接続トランクでの帯域幅に関する考慮事項

Hoot & Holler 混合アルゴリズムについては、第 2 章「Cisco IPICS のコンポーネントに関する検討事項」で説明しています。帯域幅に関する考慮事項については、第 4 章「Cisco IPICS のインフラストラクチャに関する検討事項」で説明しています。1 つのユニキャスト接続トランクで必要となる帯域幅を調べるには、1 つの音声ストリームにおける帯域幅要件を表 4-2 で確認してください。

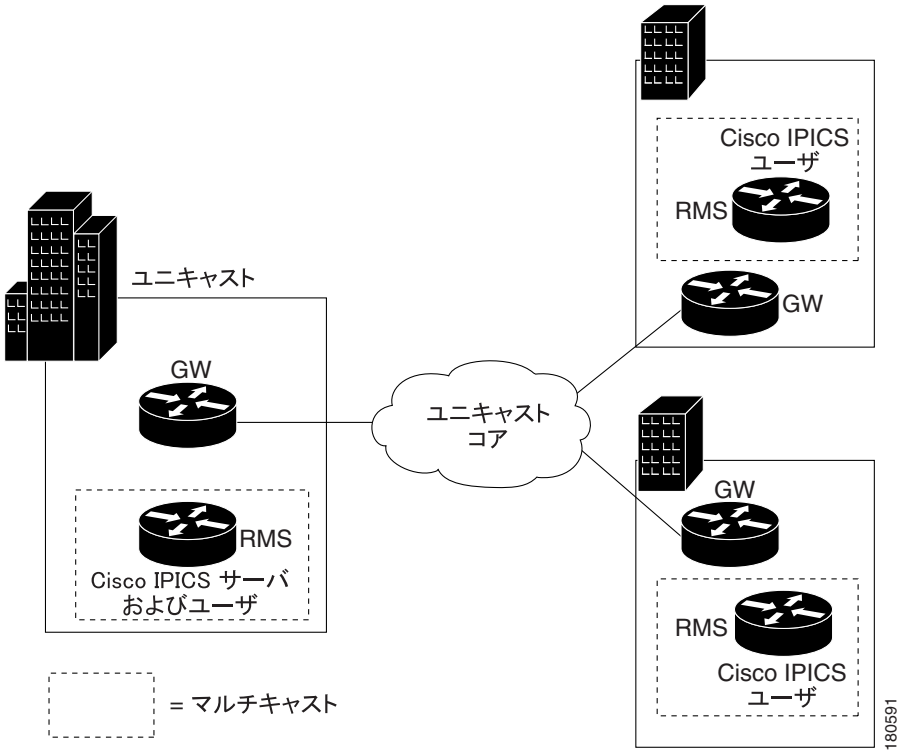
たとえば、G.729 コーデック、20 バイトのペイロード サイズ、cRTP と VAD を使用する場合は、7.3 Kbps が必要です。

この計算値は、1 つの接続トランクで使用される帯域幅です。複数の接続トランクを使用する場合は、この数値をトランクの数で乗算します。

マルチキャスト特異点

マルチキャスト特異点は、特殊な構成のマルチキャスト アイランド シナリオです。サイト間で、マルチキャスト ルーティングが有効になっていません。サイト内では、Cisco IPICS 固有のデバイス（RMS、LMR ゲートウェイ、PMC、Cisco Unified IP Phone）上だけでマルチキャストが有効になっています。これらの Cisco IPICS デバイスは、マルチキャスト特異点では図 7-16 に示した配置になります。

図 7-16　マルチキャスト特異点



これらのマルチキャスト特異点は、GRE トンネルを利用したマルチキャスト（図 7-17 を参照）または M1:U12:M2 接続トランク（図 7-18 を参照）を使用して互いに接続できます。

図 7-17　GRE トンネルを利用したマルチキャスト特異点

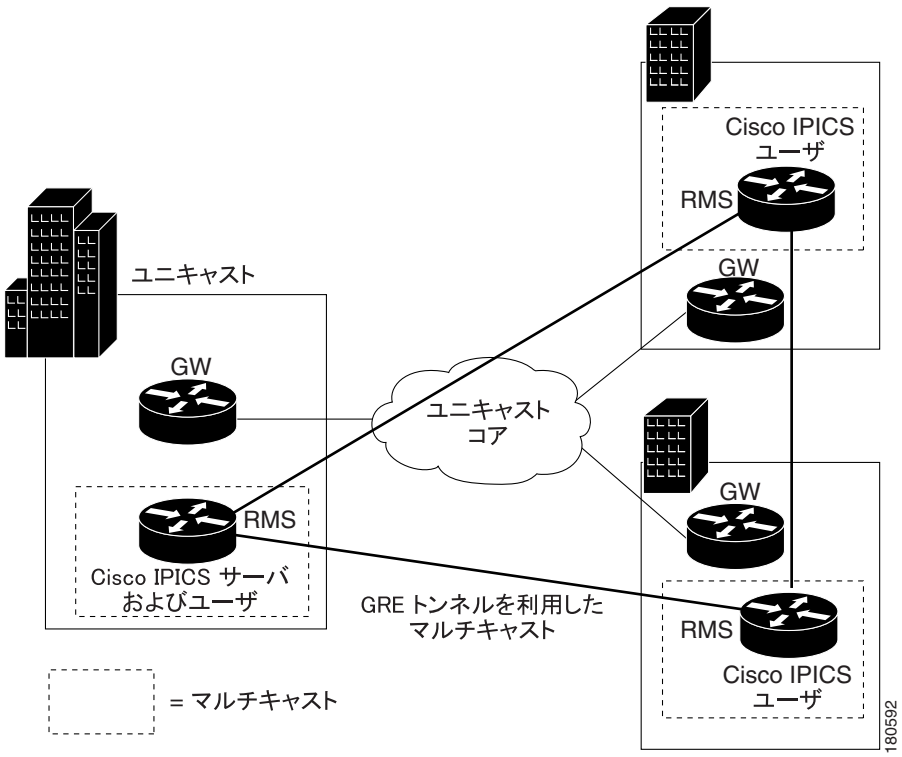
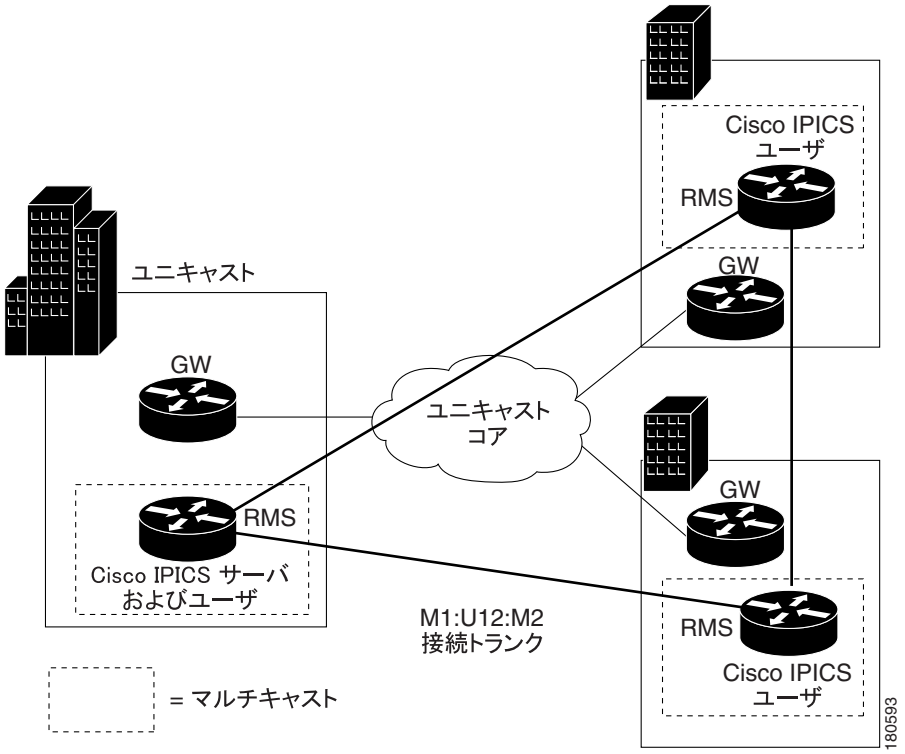


図 7-18　M1:U12:M2 接続トランクを利用したマルチキャスト特異点



GRE トンネルを利用したマルチキャストの設定は、マルチキャスト アイランド シナリオの場合と同一です。ただし、トンネルはゲートウェイ ルータ間ではなく RMS ルータ間に設定する必要があります。ゲートウェイ ルータではマルチキャストを使用できないためです。

M1:U12:M2 接続トランクの設定は、マルチキャスト アイランド シナリオの場合と同一です。どちらの場合も、トランクは RMS ルータ間に設定する必要があります。

マルチキャスト特異点は、次の規則に従っている必要があります。

1. RMS および LMR ゲートウェイは、すべてマルチキャスト特異点の内側に配置されている必要があります。つまり、これらのデバイスは、直接接続されたマルチキャスト対応 LAN 上にある必要があります。
2. マルチキャスト特異点の内側にいるユーザは、すべてマルチキャスト対応ゾーン内にいるため、PMC または Cisco Unified IP Phone を使用できます。
3. マルチキャスト特異点の外側にいるユーザは、リモート ロケーションを使用して接続している場合、PMC を使用できます。
4. Cisco Unified IP Phone はマルチキャストしかサポートしていないため、マルチキャスト特異点の外側にいるユーザは Cisco Unified IP Phone を使用できません。

複数のマルチキャスト特異点を同一サイト内に配置し、それぞれを GRE トンネルを利用したマルチキャストを使用して接続することができます。このソリューションを採用するかどうかは、組織のポリシーによって決まります。