コラボレーション エッジ

改訂日：2019 年 2 月 19 日

この章では、コラボレーション ネットワーク境界におけるサービスへのアクセスを定義する一連のサーバとゲートウェイを含むコラボレーション エッジ推奨アーキテクチャについて説明します。コラボレーション エッジ推奨アーキテクチャは、インターネットや PSTN などのパブリック ネットワークへのアクセスを提供します。

コラボレーション エッジの詳細なアーキテクチャーの説明のあとに、インターネット アクセス用の Cisco Expressway と PSTN アクセス用の Cisco Unified Border Element の展開方法に関する展開の概要セクションが続きます。また、コラボレーション エッジのハイ アベイラビリティー、コラボレーション エッジのセキュリティー、およびコラボレーション エッジ ソリューションのスケーリングについても取り上げます。さらに、コラボレーション エッジの展開プロセスに関するセクションでは、Cisco Expressway、Cisco Unified Border Element、および Cisco 音声ゲートウェイの展開方法に関する詳細情報を提供します。

この章の新規情報とは

C：表 4-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

C：表 4-1　　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所	改訂日
細部の訂正および変更	この章の各項で説明	2019 年 1 月 23 日
モバイルおよびリモート アクセス制御	モバイルおよびリモート アクセス（C：4-28 ページ） モバイルおよびリモート アクセスを展開する（C：4-45 ページ）	2017 年 8 月 30 日

コア コンポーネント

コラボレーション エッジ アーキテクチャのコア コンポーネントを以下に示します。

- Cisco Expressway-C と Expressway-E：音声とビデオのインターネット接続とファイアウォール トラバーサル用
- Cisco Unified Border Element：IP トランク経由の音声 PSTN 接続用
- PSTN 音声ゲートウェイ：直接音声 PSTN 接続用

主なメリット

- 実装されているテクノロジーや使用されているパブリック ネットワークに関係なく、顧客やパートナーに接続します。
- 回復力のある、柔軟で拡張可能なアーキテクチャを提供します。
- ハードウェア クライアントとソフトウェア クライアントがパブリック ネットワーク（インターネットや PSTN）にアクセスできるようにします。
- Cisco Mobile クライアント、リモート クライアント、およびエンドポイントにコラボレーション サービスへのセキュアな VPN レス アクセスを提供します。

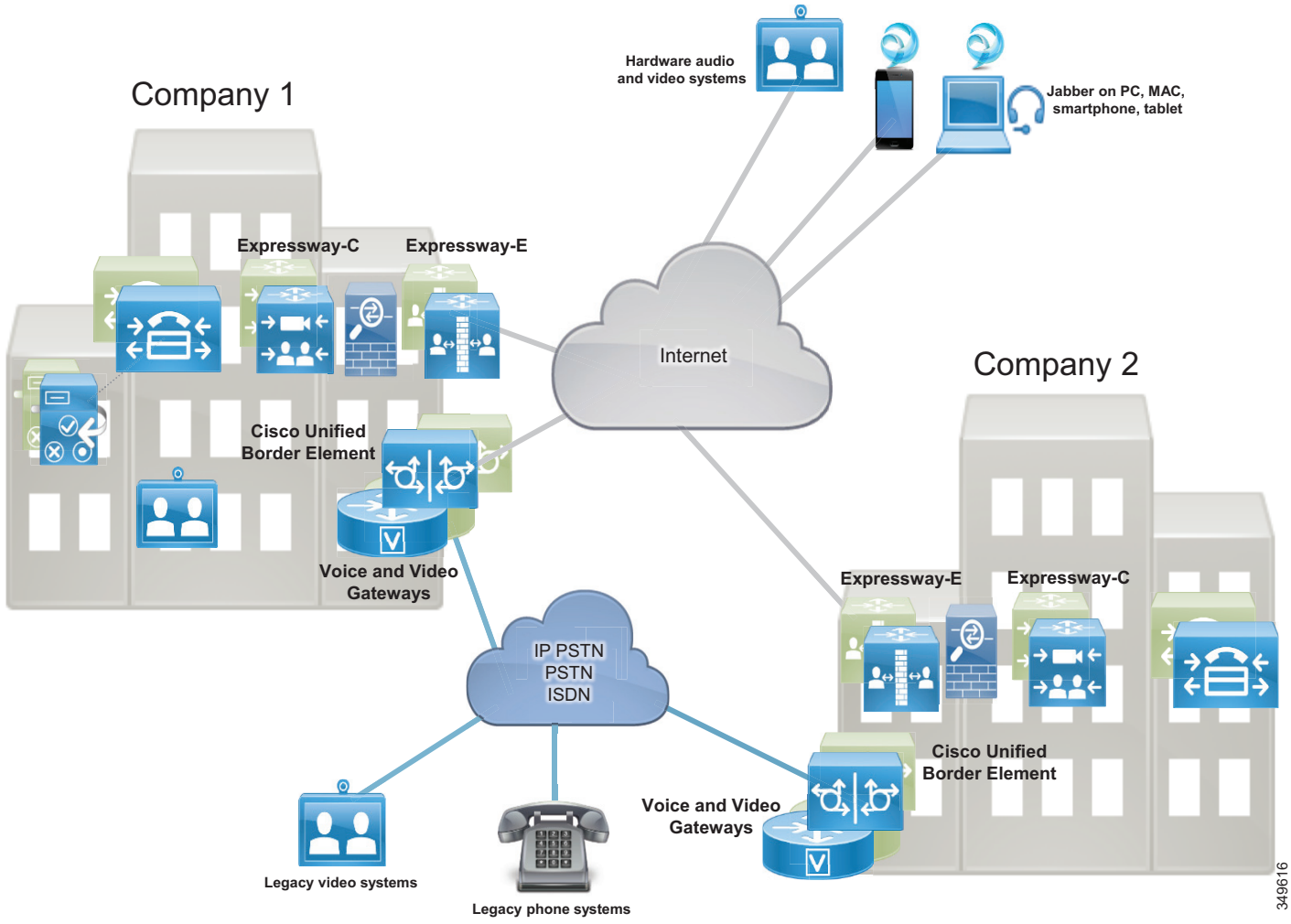
アーキテクチャー

コラボレーション エッジのアーキテクチャは、2 つの主要なネットワーク（インターネットと PSTN）とインターフェイス接続します。

インターネット接続は、VPN レス モバイル & リモート アクセス（MRA）と Business-to-Business（B2B）コミュニケーションを可能にします。これらのサービスを使用すれば、Jabber ユーザとハードウェア エンドポイントは、組織のネットワーク境界の外側にある企業コラボレーション サービスに安全にアクセスして、外部組織との Business-to-Business（B2B）音声およびビデオ通信を実現できます。

Cisco Expressway-C と Expressway-E は、ファイアウォール境界を横断しなければならないほとんどのケースでペアとして展開する必要があります。Expressway-C を内部ネットワークに、Expressway-E を緩衝地帯（DMZ）に配置することによって、ファイアウォールの両側でファイアウォール トラバーサル機能を有効にします。加えて、Expressway-C と Expressway-E をそれぞれクラスタ化することができます（C：図 4-1 を参照）。ほとんどの場合、横断するファイアウォール境界はインターネット接続ですが、個人所有デバイス持ち込み（BYOD）接続用の別個の企業 WiFi ネットワークである場合もあります。

C：図 4-1　　アーキテクチャの概要



PSTN 接続は、通信事業者ネットワークとの音声およびビデオ通信を可能にします。また、PSTN 接続は次のような方法で実現できます。

- 通信事業者への IP トランク経由。通常は音声専用サービス用。この接続は、Cisco Integrated Services Router（ISR）または Cisco Aggregation Services Router（ASR）上の Cisco Unified Border Element（CUBE）によって提供されます。Cisco Unified Border Element は、通信事業者のネットワークが企業ネットワークと通信するセントラル サイトに展開する必要があります。
- 音声ゲートウェイ経由。ゲートウェイには、Cisco Integrated Services Routers（ISR）などのさまざまなルータプラットフォーム上のアナログインターフェイスと ISDN インターフェイスが含まれます。このマニュアルでは、ISDN 音声インターフェイスのみを取り上げます。音声ゲートウェイは、PSTN 接続が必要なサイトでローカルに展開する必要があります。

ビデオ コール用のインターネット通信（Expressway）と音声専用コール用の IP PSTN 接続（CUBE）の展開に関連したコストを削減できます。ただし、IP ネットワークの信頼性は徐々に向上していますが、ネットワークの接続性の問題でリモート サイトから集中型 IP PSTN サービスにアクセスできない場合があることに注意する必要があります。このようなサイトで日常業務が PSTN 接続に大きく依存している場合は、集中型アクセス用のバックアップとしてローカル PSTN 接続の使用をお勧めします。

PSTN に関する推奨事項を以下に示します。

- PSTN を一元管理します。これにより、運用コストと経費が削減されます。
- 日常業務の実行を PSTN に大きく依存しているサイト専用のローカル PSTN 接続を設置します。このような場合は、ISDN チャネル数を削減する必要があります。これは、中央の PSTN アクセスが使用できない状況でしか ISDN チャネルが使用されないためです。これにより、ハードウェア コストが削減され、管理が簡素化され、資金の節約につながります。

上記の考察に基づくと、音声用に PSTN への IP トランク接続、ビデオ用にローカル PSTN ブレークアウトをバックアップとして使用したインターネットを使用することにより、大半の接続要件を満たすことになります。

Cisco Collaboration エッジには、ユーザが次のオプションにアクセスできるシナリオが含まれます。

- テレワーカやモバイル接続用のモバイル & リモート アクセス（MRA）
- 組織間の Business-to-Business（B2B）ビデオ通信
- 携帯電話用と固定電話へのアクセス用の PSTN

これらのシナリオでは、会社にいるユーザもインターネット上の社内ユーザも、まるで会社の中にいるかのように PSTN 音声コールと Business-to-Business（B2B）コミュニケーションにアクセスできます。ほとんどのケースで、保留、転送、会議などのサービスも使用できます。誰が誰に電話するかに関係なく、コラボレーション エッジ ソリューションは、モバイル & リモート アクセス、Business-to-Business（B2B）、PSTN 音声、およびビデオ サービス間の相互接続を可能にします。

インターネット アクセスに関する Expressway-C と Expressway-E の役割

インターネットを使用したコラボレーション サービスは、人気が高く、既存のレガシー ISDN ビデオ システムがどんどん置き換えられています。インターネット ベースのコラボレーション サービスに使用されている 2 つの主なプロトコルは SIP と H.323 です。

また、インターネットは、リモート ユーザとモバイル ユーザを、バーチャル プライベート ネットワーク（VPN）を使用せずに、音声、ビデオ、IM と Presence、およびコンテンツ共有サービスに接続するためにも使用されます。

モバイル & リモート アクセスだけでなく、Business-to-Business（B2B）サービスも、同じ Expressway-C と Expressway-E のソリューション ペアの一部として有効にできます。Expressway-C は社内ネットワーク内に展開されるのに対して、Expressway-E は DMZ 内に展開されます。

Expressway-C と Expressway-E のペアは次の機能を実行します。

- インターワーキング：音声、ビデオ、およびコンテンツ共有用の H.323 / SIP 間コールを相互接続する機能。
- 境界通信サービス：Expressway-C は社内ネットワーク内に配置されますが、Expressway-E はエンタープライズ DMZ 内に配置され、企業ネットワークとインターネット間の通信サービス専用の接続点を提供します。
- セキュリティ：モバイル & リモート アクセスと Business-to-Business（B2B）コミュニケーションの両方に認証と暗号化を提供する機能。

モバイル & リモート アクセス、および Business-to-Business（B2B）コールは Expressway-E と Expressway-C をフロースルーして、コール シグナリングとメディアの両方だけでなく、その他のコラボレーション データ フロー（XMPP や HTTP を含む）も処理されます。

モバイルおよびリモート アクセス

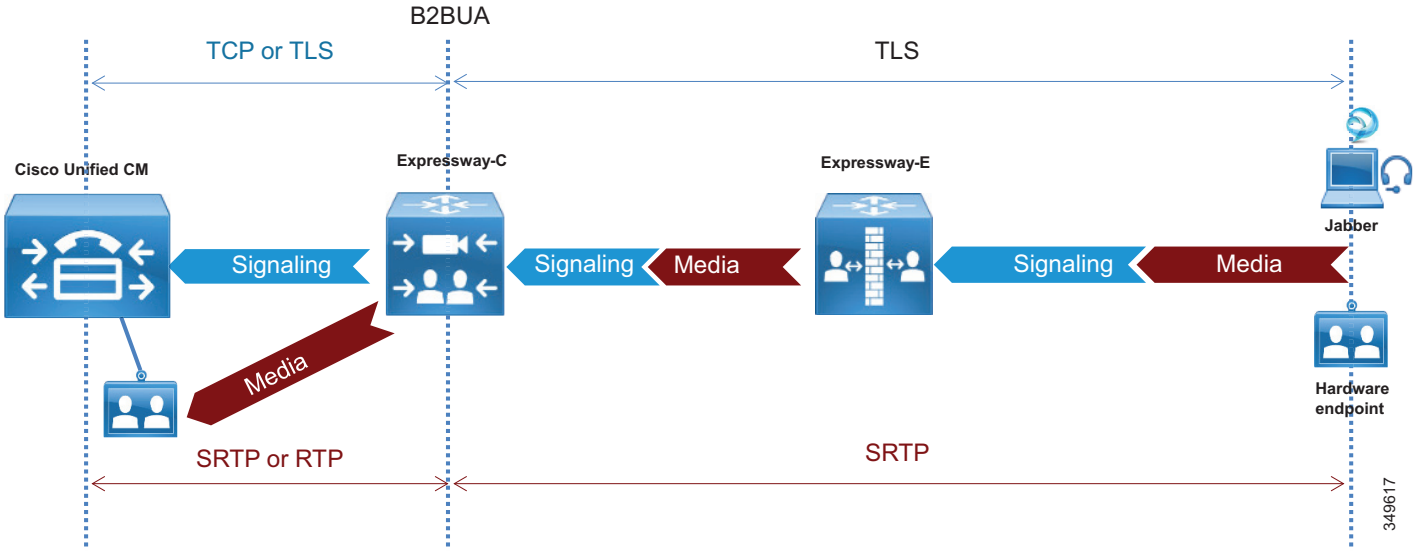
Cisco Expressway ソリューションのモバイル & リモート アクセス機能は、逆プロキシ ファイアウォール トラバーサル接続を提供します。これにより、リモート ユーザとそのデバイスが企業のコラボレーション アプリケーションおよびサービスにアクセスして利用できます。

C：図 4-2 に示すように、Cisco Expressway ソリューションには、2 つの主なコンポーネント（Expressway-E ノードと Expressway-C ノード）が含まれています。この 2 つのコンポーネントは、Cisco Unified Communications Manager（Unified CM）と連携して、セキュアなモバイル & リモート アクセスを可能にします。Expressway-E ノードは、モバイル & リモート デバイスにセキュアなエッジ インターフェイスを提供します。

Expressway-C は、Expressway-E ノードとのセキュアな接続を構築します。Expressway-C ノードは、Unified CM へのプロキシ登録を提供し、リモート セキュア エンドポイント登録を可能にします。Expressway-C ノードには、メディア終端機能を提供するバックツーバック ユーザ エージェント（B2BUA）が含まれます。

C：図 4-2 に、すべてのモバイル & リモート アクセス コールのシグナリングとメディアの両方が Expressway-C と Expressway-E を行き来する様子を示します。

C：図 4-2　　Expressway 上の B2BUA とコール レッグ

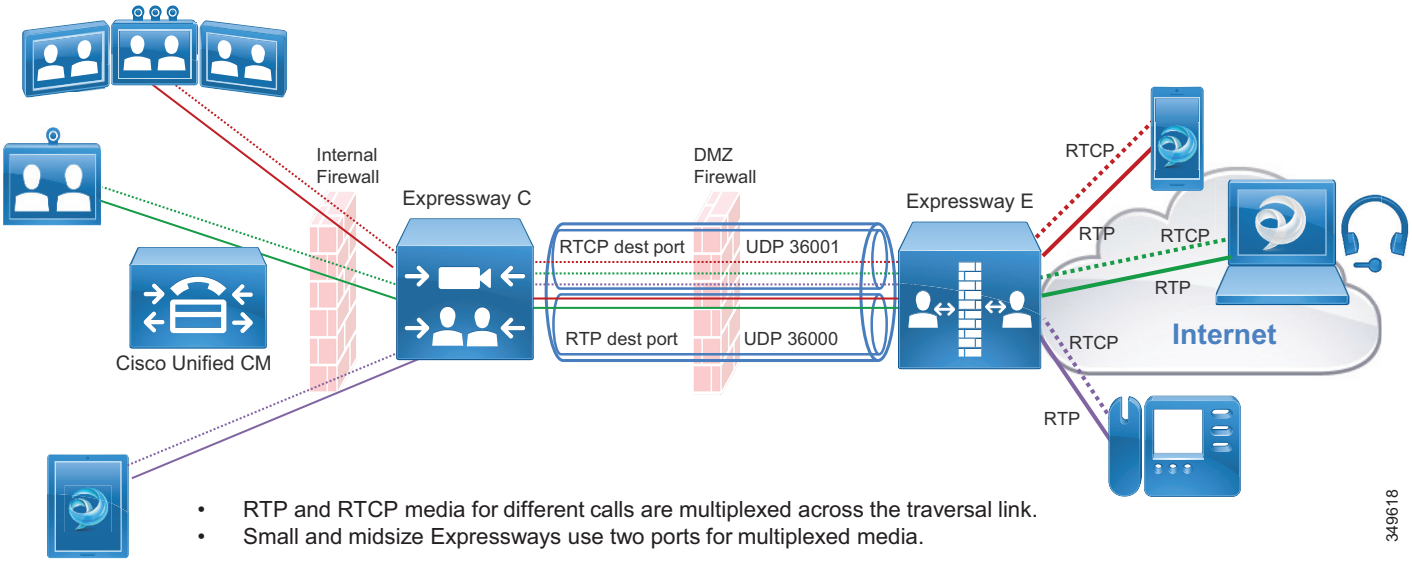


Business-to-Business（B2B）コミュニケーション

Expressway-C と Expressway-E は、連携してインターネット経由の Business-to-Business（B2B）コミュニケーション用のコア コンポーネントであるファイアウォール トラバーサル ソリューションを形成するように設計されています。

Expressway-C は、企業ネットワークの内部（信頼された側）に配置され、Expressway-E へのセキュアで信頼できる各種の標準規格に準拠した接続手段を提供する役割を果たします。また、その背後にあるすべてのデバイスへのトラバーサル クライアントとしての機能を果たします。このソリューションは、アウトバウンド通信用に開かれた少数のポートにすべてのメディアを多重化することによって、大量のメディア ポートを使用するデバイスの問題を解決します。また、Expressway-C から Expressway-E までのトラバーサル ゾーンに関するキープアライブを送信することによって、社内から社外への認証された信頼できる接続を実現します。また、すべてのインターネット通信に対して一括窓口を提供することで、セキュリティ リスクを最小化します。（C：図 4-3 を参照）。

C：図 4-3　　Expressway-C の多重化とキープアライブ



SIP、H.323、XMPP などのリアルタイムや準リアルタイムの通信プロトコルでは、ファイアウォールの背後に設置されたデバイスとの通信ニーズは解決されません。このようなプロトコルを使用した典型的な通信には、シグナリングとメディア内にデバイス IP アドレスが含まれており、それぞれが TCP パケットと UDP パケットのペイロードになります。これらのデバイスが、内部的にルーティング可能な同じネットワーク上に存在する場合は、相互に直接通信することができます。TCP パケットのペイロードで伝送されるシグナリング IP アドレスは送信デバイスに戻すルーティングが可能であり、その逆もできます。ただし、送信デバイスがパブリックまたはネットワーク エッジ ファイアウォールの背後の別のネットワーク上に存在する場合は、2 つの問題が発生します。1 つ目の問題は、受信デバイスが、パケットの復号化後に、ペイロードで伝送された内部 IP アドレスに応答することです。この IP アドレスは、通常、ルーティング不可能な RFC 1918 アドレスであり、絶対に返信先に到達しません。発生する 2 つ目の問題は、返信先 IP アドレスがルーティング可能であっても、メディア（RTP/UDP）が外部ファイアウォールによってブロックされることです。このことは、Business-to-Business（B2B）コミュニケーションと、モバイル & リモート アクセスの通信の両方に当てはまります。

Expressway-E は DMZ 内のネットワーク エッジに配置されます。これは、標準の相互運用性を維持しながら、SIP、H323、および XMPP に関するシグナリングとメディアの両方のルーティング問題を解決する役割を果たします。さらに、ネットワーク内部のエンドポイント、デバイス、およびアプリケーション サーバの代わりにメディアとシグナリングを処理するために該当するヘッダーと IP アドレスを変更します。

インスタント メッセージおよびプレゼンス フェデレーション

インスタント メッセージおよびプレゼンス フェデレーションは、ある組織のユーザがチャットやプレゼンス ステータス情報に関する XMPP トラフィックをその組織の外部ファイアウォール経由で別の組織のユーザとやり取りできるようにします。

以前のシスコ アーキテクチャでは、シスコ適応型セキュリティ アプライアンス（ASA）ファイアウォールを使用して、外部ファイアウォール経由で内部の IM and Presence サーバに直接アクセスするために受信ポートを開くことができました。SIP フェデレーションでは、引き続きこのソリューションが推奨されています。

XMPP フェデレーションでは、XMPP トラフィックを外部の宛先とやり取りするための信頼できるセキュアなファイアウォール トラバーサル ソリューションとして同じ Expressway-C と Expressway-E のペア アーキテクチャを使用します。Expressway-E は、XMPP 用のセキュアな DMZ ベースのターミネーション ポイントをインターネットに提供します。Expressway-C は、ファイアウォール トラバーサル用に Expressway-E への TLS ベースの認証されたセキュア接続を提供するので、ファイアウォール上でポートを開く必要がありません。

また、Expressway-C は、IM と Presence サーバへの AXL API 接続も提供します。AXL API は、Expressway-E から収集された XMPP サーバ間情報を IM と Presence データベースに送信します。これにより、ファイアウォール上で他のポートを開くことなく、Expressway-E 経由で他の組織へのフェデレーション接続を開始するのに必要な接続情報が IM と Presence サーバに提供されます。XMPP フェデレーションでは、音声とビデオのエスカレーションが可能です。同じ組織で、XMPP フェデレーションと SIP フェデレーションの両方を同時に実装することができます。

PSTN アクセス

ここでは、Cisco Unified Border Element をセッション ボーダー コントローラ（SBC）として使用した PSTN アクセス用のアーキテクチャについて説明します。

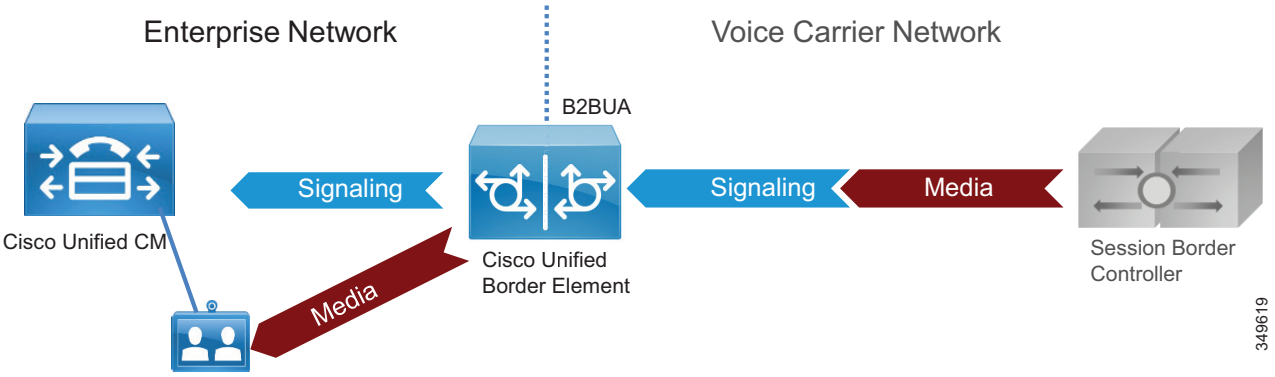
Cisco Unified Border Element の役割

従来の PSTN 接続の代わりに通信事業者への IP トランクを使用した音声接続は人気が高まっており、徐々に既存の TDM ベースの PSTN アクセスに取って代わろうとしています。SIP はプロバイダー ネットワークに接続するためのアクセス プロトコルとして広く使用されており、今日では、多くの通信事業者が音声専用サービスを Cisco Unified Border Element などのセッション ボーダー コントローラ経由で PSTN に提供しています。セッション ボーダー コントローラは、SIP バックツーバック ユーザ エージェント（B2BUA）であり、各コールの音声メディアと SIP シグナリングの両方が Cisco Unified Border Element を通過するフロースルー モードでよく使用されます（C：図 4-4 を参照）。

Cisco Unified Border Element は、さまざまな Cisco ルータおよびゲートウェイ上で利用可能なライセンス供与された Cisco IOS アプリケーションであり、通信事業者のボーダー エレメントへの SIP トランク経由で PSTN に接続するための推奨プラットフォームです。

また、Cisco Unified Border Element は、Cisco Unified Communications Manager（Unified CM）に基づくエンタープライズ音声ネットワークを SIP トランク サービス経由で通信事業者に接続して相互運用できるようにします。さらに、Cisco Unified Border Element は、シグナリング ストリームとメディア ストリームの両方を終端処理して再発信することにより、IP ネットワーク間のセキュアなボーダー相互接続サービスを提供します。Cisco Unified Border Element を使用しているお客様は、現在のネットワーク サービスを縮小して、ネットワーク アーキテクチャを簡略化し、機能強化中のネットワークをコラボレーション サービスに位置付けることができます。

C：図 4-4　　B2BUA としての Cisco Unified Border Element



Cisco Unified Border Element は、エンタープライズ ネットワークと通信事業者ネットワークの間で次の機能を実行します。

- セッション制御：SIP セッションに対して、柔軟なトランク ルーティング、コール アドミッション制御、復元力、およびコール アカウンティングを提供する機能。
- インターワーキング：音声用のメディア トランスコーディング サービスと、SIP の遅延オファーと早期オファー間の相互運用性を提供する機能。
- 境界設定：2 つのネットワーク間のアドレス変換用とポート変換用に別々の境界ポイントとして機能し、トラブルシューティングを容易にする機能。
- セキュリティ：ネットワーク間のリアルタイム トラフィックをインテリジェントに許可または禁止し、アプリケーションの必要に応じてリアルタイム トラフィックを暗号化する機能。

音声ゲートウェイの役割

集中型 PSTN アクセスが使用できない場合は、TDM ゲートウェイを使用して PSTN に接続することをお勧めします。Cisco では、適切なインターフェイスカード（低密度デジタル（BRI）、高密度デジタル（T1、E1、および T3）、およびアナログ（FXS、FXO、および E&M）の各インターフェイス）が有効になっているサービス統合型ルータ（ISR）上で PSTN へのアナログ接続とデジタル接続を可能にするさまざまな TDM ゲートウェイを提供しています。

音声ゲートウェイの詳細については、次に提供される Cisco サービス統合型ルータのドキュメンテーションを参照してください。

https://www.cisco.com/c/en/us/products/routers/branch-routers/index.html

展開の概要

ここでは、インターネット接続用の Cisco Expressway と PSTN アクセス用の Cisco Unified Border Element の展開方法について説明します。

インタネット接続用の Expressway の展開

Cisco Collaboration エッジ アーキテクチャの標準展開には、企業のコラボレーション サービスに対するセキュアなモバイルデバイスおよびリモート VPN レス アクセス用の 1 つ以上の Expressway-C と Expressway-E のペアの展開が含まれます。

復元力を高めるためには、Expressway-C と Expressway-E の両方をクラスタ内に展開する必要があります。クラスタごとのサーバ数は、Unified CM に対する同時プロキシ化登録の数と同時コールの数によって異なります。前者の数には Expressway 経由で Unified CM に登録するモバイル ユーザとリモート ユーザの数が数えられるのに対して、後者の数には Business-to-Business（B2B）とモバイル & リモート アクセス（MRA）の同時コールの数が数えられます（詳細については、サイジングの章を参照してください）。

このサービスは、Jabber クライアント、特定の IP フォン モデル、および TC または CE ソフトウェアを実行している Cisco TelePresence System エンドポイントに提供されます。しばしば、地理的範囲とスケーリングのために複数のペアの Expressway-C と Expressway-E が展開され、これにより、コラボレーション サービスの複数のインスタンスへのアクセスが可能になります。インターネット サービス プロバイダーからのさまざまなメトリックに基づいてリモート クライアントおよびエンドポイント アクセスのバランスを取るため、GeoDNS を使用する必要があります。

この同じ Expressway を Business-to-Business（B2B）コミュニケーションに利用することもできます。コールの量が Expressway クラスタの容量を超える場合は、Business-to-Business（B2B）サービスと MRA サービスを別々のボックスに分割する必要があります（詳細については、サイジングの章を参照してください）。

Expressway が両方のサービスに使用されている場合は、Unified CM がインターネット上のユニファイド ビジネス コミュニケーション アクセス用の SIP トランク経由で Expressway-C に接続されます。Expressway-C は、ネットワークの信頼された側に配置され、セキュアなファイアウォール トラバーサル サービスを Expressway-E に提供します。

エンタープライズ セキュリティ ポリシーに基づいて、さまざまな展開モデルを実装できます。このマニュアルでは、デュアル インターフェイスを備えた DMZ 展開を中心に説明します。これは、この展開が最も一般的でセキュアな展開モデルだからです。その他の展開モデルについては、『*Cisco Expressway Basic Configuration Deployment Guide*』の最新版を参照してください。

Expressway-C と Expressway-E は、ファイアウォール トラバーサル機能を提供します。ファイアウォール トラバーサルは次のように動作します。

1. Expressway-E はエンタープライズ DMZ 内に設置されたトラバーサル サーバです。Expressway-C は企業ネットワーク内部に設置されたトラバーサル クライアントです。
2. Expressway-C は、セキュアなログイン クレデンシャルを使用して、ファイアウォールを通って Expressway-E 上の特定のポートに至るトラバーサル アウトバウンド接続を開始します。ファイアウォールがほとんどの場合の動作と同様にアウトバウンド接続を許可している場合は、企業のファイアウォールで追加のポートを開く必要はありません。ポートの詳細については、『*Cisco Expressway IP Port Usage for Firewall Traversal*』に関するドキュメントの最新版を参照してください。

   モバイル & リモート アクセスには、Unified Communications トラバーサル ゾーンと呼ばれる別のトラバーサル ゾーンが必要です。Unified Communications トラバーサル ゾーンは SIP と連動し、TLS およびメディア暗号化を必要とします。一方、Business-to-Business（B2B）トラバーサル ゾーンは SIP と H.323 を音声とビデオのシグナリング プロトコルとして許可します。Unified Communications トラバーサル ゾーンは、IM and Presence サーバへの接続とプロビジョニング目的で使用される XMPP と HTTPs も許可します。

3。 接続が確立されると、Expressway-C がキープアライブ パケットを定期的に Expressway-E に送信して接続を維持します。

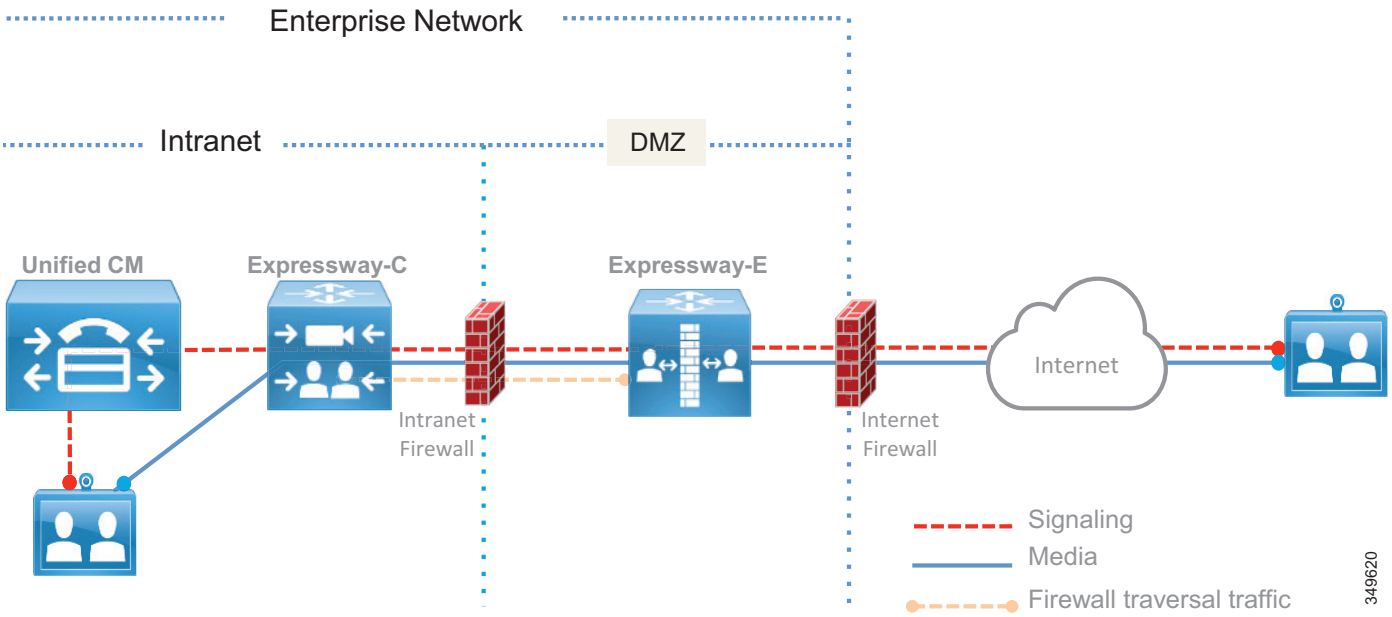
4。 Expressway-E がコールやその他のコラボレーション サービス要求を受け取ると、着信要求を Expressway-C に発行します。

5。 その後で、Expressway-C がその要求を Unified CM またはその他のコラボレーション サービス アプリケーションにルーティングします。

6。 接続が確立され、アプリケーション トラフィック（音声メディアとビデオ メディアを含む）が既存のトラバーサル接続経由で安全にファイアウォールを通過します。

ファイアウォール トラバーサルが機能するためには、Expressway-C 上でトラバーサル クライアント ゾーンを設定し、Expressway-E 上でトラバーサル サーバ ゾーンを設定する必要があります。C：図 4-5 に、ファイアウォール トラバーサル プロセスの概要を示します。

C：図 4-5　　Expressway-C と Expressway-E のファイアウォール トラバーサル プロセス



Expressway-E の展開ではシングル LAN インターフェイスまたはデュアル LAN インターフェイスのどちらも使用できますが、デュアル インターフェイスの使用をお勧めします。デュアルインターフェイス展開シナリオでは、Expressway-E が次の 2 つのファイアウォール間の DMZ 内に配置されます。インターネット ファイアウォールはインターネット向けの NAT サービスを提供し、イントラネット ファイアウォールは企業信頼ネットワークへのアクセスを提供します。

Expressway-E は次の 2 つの LAN インターフェイスを備えています。1 つはインターネット ファイアウォール向け（*外部インターフェイス*とも呼ばれる）で、もう 1 つはイントラネット ファイアウォール向け（*内部インターフェイス*とも呼ばれる）です。

外部インターフェイスにパブリック IP アドレスを割り当てる必要はありません。これは、NAT によってアドレスを静的に変換できるためです。この場合は、NAT で使用されるパブリック IP アドレスを Expressway-E 上の「静的 NAT アドレス」として設定する必要があります。

Expressway-C には、モバイル / リモート アクセスおよび Business-to-Business（B2B）コールを終端する B2BUA が組み込まれています。それぞれのモバイル / リモート アクセス コールに B2BUA のインスタンスが 1 つ必要です。暗号化の設定に応じて、それぞれの Business-to-Business（B2B）コールに B2BUA のインスタンスが 1 つ必要な場合があります。Expressway-E には、Business-to-Business（B2B）コールを終端する B2BUA が組み込まれています。Expressway-C と Expressway-E には、Microsoft や H.323/SIP プロトコル インターワーキングなどのさまざまなサービスに専用の B2BUA も組み込まれています。

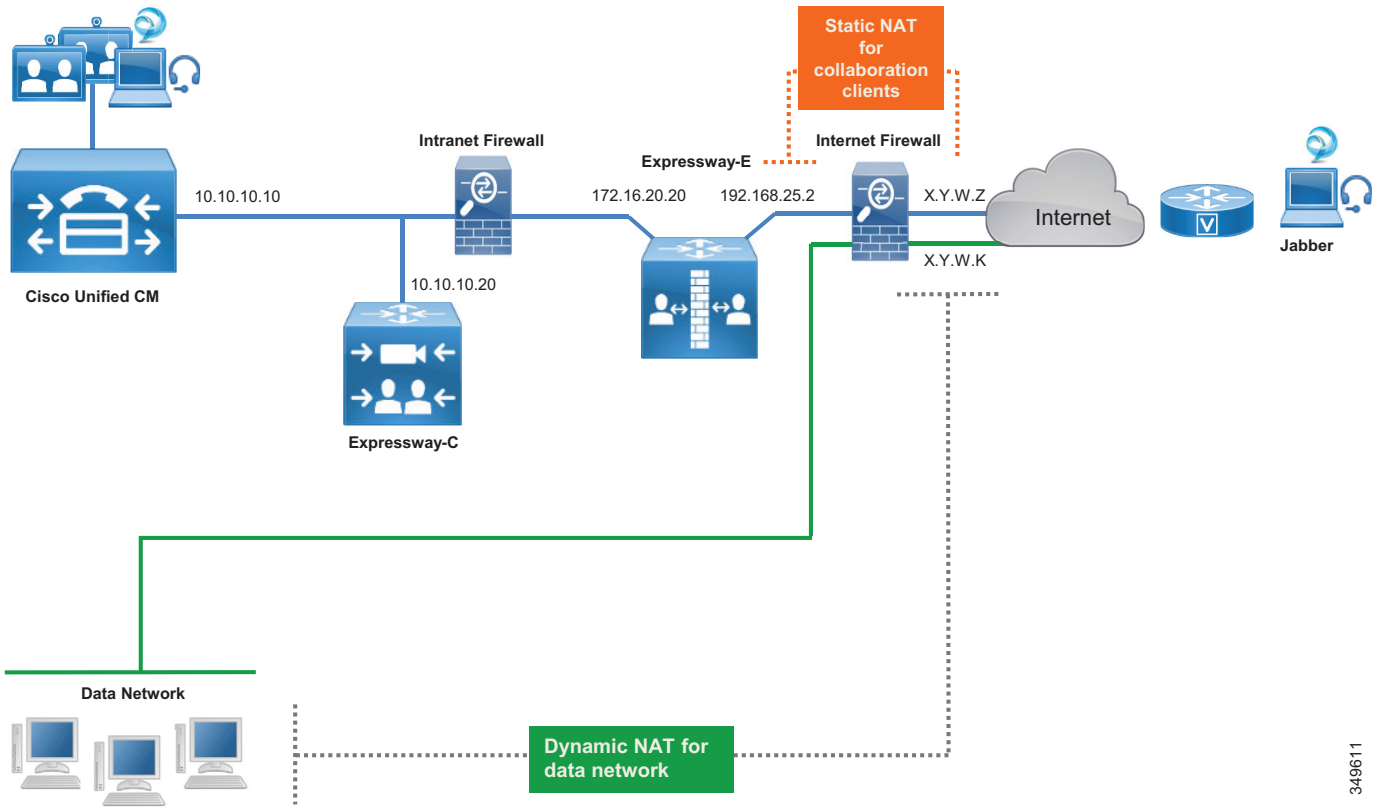
B2BUA は、コラボレーション アプリケーション トラフィックを終端します。インターネットから Expressway-E 経由の Expressway-C への接続はモバイルおよびリモート アクセス用に常に暗号化されますが、Expressway-C と Unified Communications Manager エンドポイントの間の接続は設定に応じて暗号化できる場合とできない場合があります。Business-to-Business（B2B）コミュニケーション用のインターネットからの接続は、設定および会社の方針に従って暗号化される場合とされない場合があります。このマニュアルでは、インターネットと Expressway-C の間でモバイルおよびリモート アクセス用の暗号化が実行されるが、Expressway-C と内部バックエンド サーバおよびクライアントの間の通信は暗号化されずに送信されるシナリオを中心に説明します。これは単なる 1 つのオプションです。Cisco Unified Communications Manager が混在モード用に設定されている場合は、Expressway-C と Cisco Unified Communications Manager の間でもモバイルおよびリモート アクセス接続を暗号化するように設定できます。Business-to-Business（B2B）暗号化機能については、後述のコラボレーション エッジのセキュリティーに関するセクションで説明します。

Expressway-C は、モバイルおよびリモート アクセス クライアントまたはデバイスの Unified CM への登録をプロキシします。Unified CM では、それらが Expressway-C の IP アドレスで登録されたデバイスとして一覧表示されます。

C：図 4-6 に、前述した展開を示します。関連する IP アドレスが図に示されています。場所やインターネット サービス プロバイダーによって異なるパブリック IP アドレスが数字ではなく文字で表現されています。

Expressway-E は 2 つのインターフェイスを備えています。内部インターフェイスの IP アドレスは 172.16.20.20 で、外部インターフェイスの IP アドレスは 192.168.25.2 です。外部インターフェイスの IP アドレスは静的に X.Y.W.Z に変換されます。このアドレスは Expressway-E 上でも設定されます。Expressway-E が INVITE を送信すると、独自のアドレスを使用するのではなく、変換されたインターフェイス アドレスに設定された IP アドレスを使用して Session Description Protocol（SDP）メッセージが作成されるため、着信側はプライベート アドレスではなくルーティング可能なパブリック アドレスを使用できます。

C：図 4-6　　インターネット ファイアウォール上の NAT インターフェイス



インターネット上のエンドポイントが Expressway 経由で Unified CM やその他のコラボレーション アプリケーションに接続すると、ローカル顧客宅内機器（CPE）によってその IP アドレスが最初にパブリック IP アドレスに変換されます。Expressway-E では、ソース IP アドレスが Expressway-E の内部 IP LAN インターフェイスのアドレスに置き換えられます。パケットが Expressway-C に到着すると、Expressway-C はパケットをコラボレーション サービス アプリケーションに転送する前に、パケットのソース IP アドレスを独自の IP アドレスに置き換えます。

もう一方の方向では、内部エンドポイントからのトラフィックが Expressway を通ってインターネットに入ると、その送信元 IP アドレスが Expressway-E 外部 LAN インターフェイス アドレスに置き換えられ、その後、インターネット ファイアウォール上の NAT によって静的に変換されます。データ デバイスの送信元 IP アドレスは、インターネット ファイアウォールの別のインターフェイスを使用して X.Y.W.K に動的に変換されます。

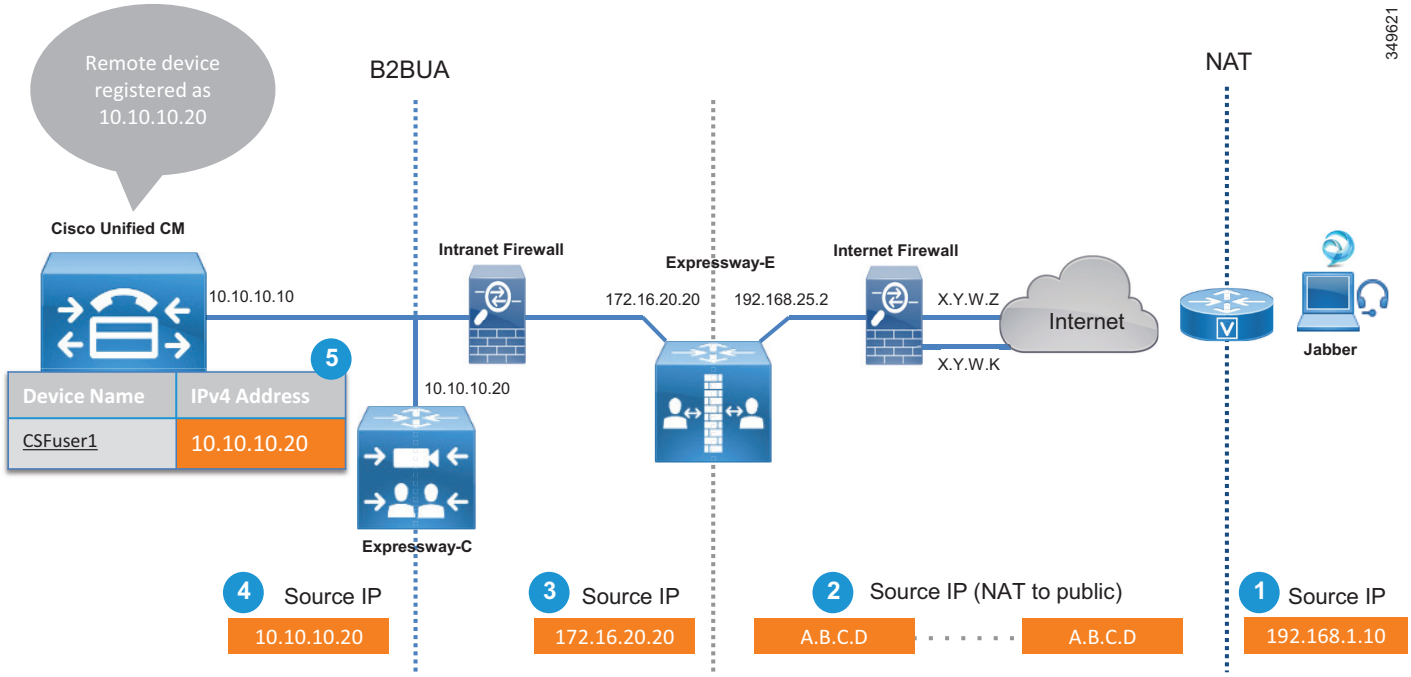
データと Jabber やブラウザなどの通信アプリケーションを使用する PC では、Jabber アプリケーション アドレスは NAT によって静的に変換され、ブラウザ アプリケーション アドレスは NAT によって動的に変換されます。

ファイアウォール内でスタティック NAT 変換が実行される場合でも、パケットの送信元 IP アドレスは転送中に次のように変換されます。パケットが Expressway-C から Expressway-E に到達すると Expressway-C の IP アドレスに変換され、パケットが Expressway-E からファイアウォールに到達すると Expressway-E の IP アドレスに変換されます。ファイアウォールでは、パケットが NAT によって静的に変換されてからインターネットに送信されます。

モバイルおよびリモート アクセス

コール制御サービスの場合は、C：図 4-7 に示すように、Expressway-C プロキシが独自の IP アドレスを使用してエンドポイントを Unified CM に登録します。この動作は、共有回線や複数回線などのサービスがモバイルおよびリモート アクセスで設定されている場合には変化することがあります。

C：図 4-7　　パケットの性質から見た NAT



C：図 4-7 に示すアドレス変換プロセスは次のステップで構成されます。

1. エンドポイントにパブリック IP アドレスが割り当てられていない場合は、インターネットへのアクセスを提供するルータでエンドポイントの送信元 IP アドレスが NAT によって（192.168.1.10 から A.B.C.D に）変換されます。
2. パケットが Expressway-E に到着します。
3. Expressway-E が独自の内部 LAN インターフェイス アドレスを使用して Expressway-C にパケットを送信します（A.B.C.D から 172.16.20.20 に）。
4. Expressway-C がそのパケットを受け取って、接続を終了します。また、独自の IP アドレスを使用して、Unified CM 向けの別の接続を再発信します（172.16.20.20 から 10.10.10.20 に）。
5. エンドポイントが Expressway-C の IP アドレス（10.10.10.20）を使用して Unified CM に登録されます。

Expressway-C の IP アドレスを使用してデバイスを Unified CM に登録する場合は、次のような固有のメリットが得られます。たとえば、リモート デバイスが企業ネットワークに直接接続されていない場合にビデオ帯域幅を制限し、リモート デバイスがオンプレミスの場合にはビデオ帯域幅に別の値を割り当てたりできます。ここでは説明しませんが、この方法は Unified CM 上のモビリティ機能を使用して簡単に実現できます。このモビリティ機能は、IP アドレス範囲に基づく特定のポリシーの定義を可能にします。

エンドポイントがインターネット経由で登録された場合は、Cisco Collaboration アーキテクチャでリモートから管理することはできません。これは、エンドポイントの IP アドレスが動的に変換され、ファイアウォールの背後に配置されるためです。リモート管理が必要な場合は、エンドポイントを VPN 経由で展開してください。ただしエンドポイント アップグレードは例外で、エンドポイントがファイアウォールの背後にある場合でも、リモートでこれを実施できます。

VPN Technologies はこのアーキテクチャの一部ではありませんが、必要に応じて追加することができます。

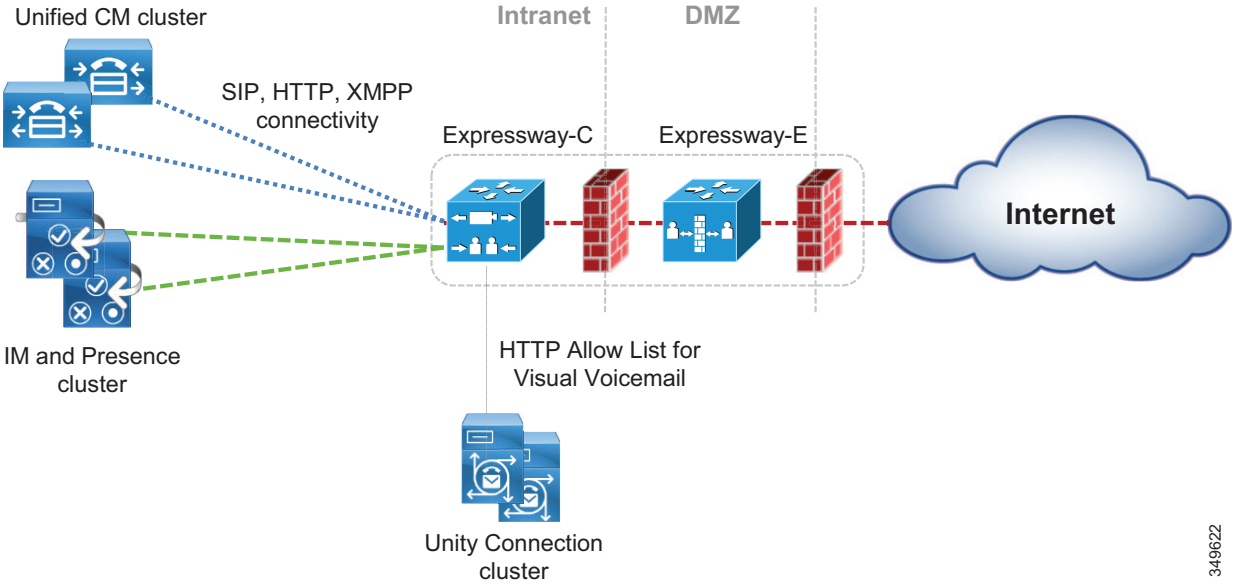
Expressway-E と Expressway-C 上でモバイルおよびリモート アクセスを有効にする必要があります。そうすれば、Unified CM and IM and Presence パブリッシャ ノードの DNS 名を指定することによって、Unified CM and IM and Presence クラスタを検出するように Expressway-C を設定できます。

DMZ 内に展開された Expressway-E は、モバイル & リモート アクセス サービスを使用する Jabber クライアントと TelePresence エンドポイントに信頼できるエントリ ポイントを提供します。

Expressway-C は、HTTPs、SIP、および XMPP を使用して、Unified CM クラスタ、IM と Presence クラスタ、および Cisco Unity Connection に接続します（C：図 4-8 を参照）。

さらに、Jabber が HTTP 経由で特定のサーバに接続しなければならない場合が数多くあります。たとえば、ビジュアル ボイスメール、Jabber 更新サーバ、カスタム HTML タブおよびアイコン、ディレクトリ フォト ホストなどです。このようなケースでは、Jabber が Unified CM を経由せずに直接これらのサーバに接続します。Expressway-C は Jabber クライアントが接続を許可されたサーバを示す HTTP 許可リストを必要とします。

C：図 4-8　　Unified CM、IM と Presence サービス、および Unity Connection への Expressway 接続



C：表 4-2 に、モバイル & リモート アクセスのために Expressway によって使用されるプロトコルの概要を示します。

C：表 4-2　モバイル & リモート アクセス用の Expressway プロトコル

プロトコル	セキュリティ	サービス
SIP	TLS	セッションの確立：登録や招待など
HTTPS	TLS	ログイン、プロビジョニング、設定、連絡先検索、ビジュアル ボイスメール
XMPP	TLS	インスタント メッセージ、プレゼンス
RTP	SRTP	音声、ビデオ、コンテンツ共有、高度なコントロール

Jabber または TelePresence エンドポイント ユーザがログインするときには、完全修飾名（user1@ent-pa.com など）を指定します。クライアントが次の特定の SRV レコードをパブリック DNS サーバにクエリします。

- _cisco-uds._tcp.ent-pa.com：企業 DNS サーバ上でのみ設定されます。
- _collab-edge._tls.ent-pa.com：パブリック DNS サーバ上でのみ設定され、Expressway-E クラスタのパブリック インターフェイスに解決されます。このレコードは常に TLS を示していることに注意してください。

クライアントがインターネット経由で接続されている場合は、パブリック DNS サーバから _cisco-uds に関する応答が返されませんが、クライアントは _collab-edge SRV レコードに関する応答を受け取ります。

その後で、DNS サーバが Expressway-E に関する A レコード（または Expressway-E がクラスタ化されている場合は複数のレコード）をクライアントに送信します。クライアントが Expressway-E の DNS 名を認識したら、プロビジョニングと登録の手順を開始できます。

プロビジョニングは HTTPs を使用して実行されるのに対して、登録では SIP と XMPP が使用されます。

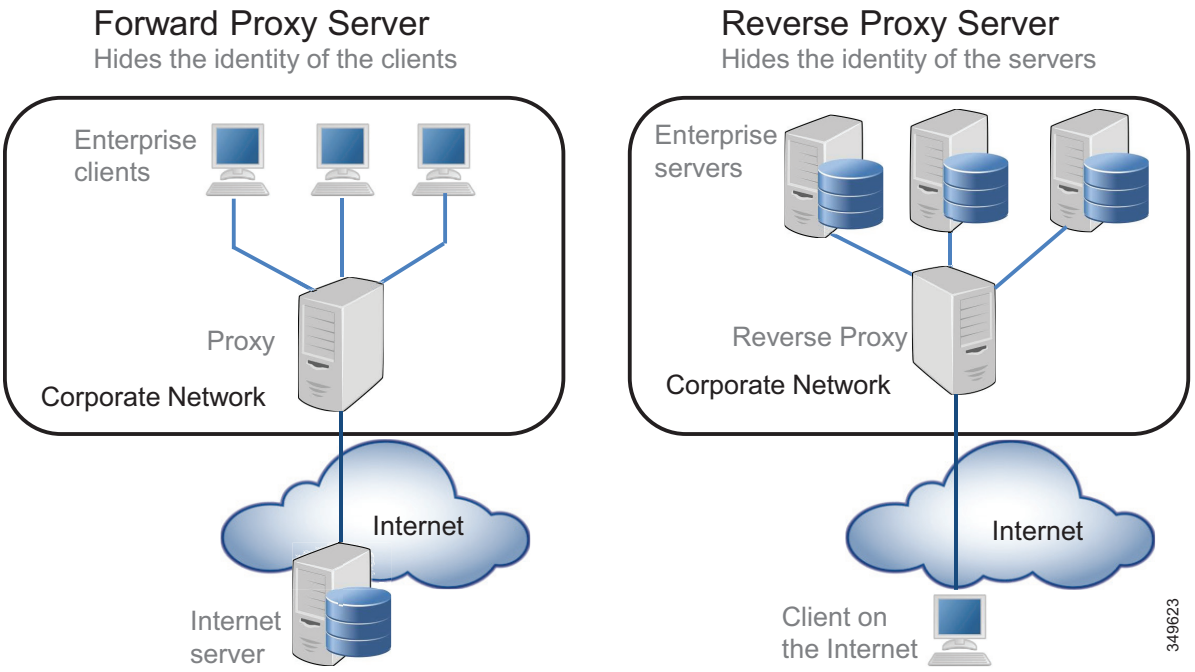
Expressway-C は、プロビジョニング プロセスを管理するための HTTPs 逆プロキシ サーバ機能を備えています。逆プロキシは、*プロキシ サーバ*とも呼ばれる最も一般的な転送プロキシ サーバの逆です。

C：図 4-9 に示すように、転送プロキシ サーバはインターネット サーバへの接続時にクライアント詳細を隠すことによってオンプレミス クライアントに関するサービス情報を提供するのに対して、逆プロキシ サーバはオンプレミス サーバ情報を隠すことによってオフプレミス クライアントに関する情報を提供します。転送プロキシ経由でインターネット サーバに接続している社内ネットワーク内のクライアントは接続先のサーバの ID は知っていますが、サーバはクライアントの ID を知りません。

一方、逆プロキシ経由で接続しているインターネット上のクライアントは、逆プロキシ サーバ経由で接続しているためオンプレミス サーバの ID を知りませんが、オンプレミス サーバは接続先のクライアントの ID を知っています。その後、この情報は、オンプレミス サーバから発信されたかのようにクライアントに戻されます。

Expressway-C は、Cisco Unified CM、IM と Presence、Unity Connection などのコラボレーション アプリケーション サーバの代わりに、プロビジョニング、登録、およびサービスの詳細をインターネット上のクライアントに提供する逆プロキシ機能を備えています。

C：図 4-9　　フォワード プロキシ サーバとリバース プロキシ サーバ



ビジュアル ボイスメール、Jabber 更新サーバ、カスタム HTML タブおよびアイコン、ディレクトリ フォト ホストなどのサービスに対して、Expressway-C は HTTP サービス用のアクセス リストの一種である *HTTP 許可リスト*でこれらのサービスが指定されている場合にこれらの接続を許可することにも留意してください。

プロビジョニングと登録は、クライアント、Expressway-C、Expressway-E、Unified CM、および IM と Presence サーバが関与する多段階プロセスです。

クライアントがコラボレーション エッジ経由で登録する場合に関係する主なステップの概要を以下に示します。

1. プロビジョニングは、クライアントから発行された **get_edge_config** 要求で開始されます。次に例を示します。

   https://expressway_e.ent-pa.com:8443/ZeW50LXBhLmNvbQ/get_edge_config?service_name=_cisco-uds&service_name=_cuplogin

   この要求と一緒に、クライアントはユーザのクレデンシャル（たとえば、ユーザ名「user1」とパスワード「user1」）を送信します。クエリは Expressway-E に送信されてから、Expressway-C に転送されます。

2. Expressway-C が Unified CM に対する UDS クエリを実行して user1 のホーム クラスタを特定します。これはマルチクラスタ シナリオでは必須です。

   GET cucm.ent-pa.com:8443/cucm-uds/clusterUser?username=user1

3. ホーム クラスタが見つかると、Expressway-C に応答が送信されます。この応答には、クラスタ内のすべてのサーバが含まれています。

4。 Expressway-C がクライアントの代わりに user1 に関する次のクエリを発行することによって、ホーム クラスタにプロビジョニング情報を問い合わせます。

GET /cucm-uds/user/user1/devices はデバイス割り当てリストを取得します。

GET /cucm-uds/servers はクラスタのサーバ リストを取得します。

GET /cucm-uds/user/user1 は user1 のユーザ設定と回線設定を取得します。

クエリに対する応答で、TFTP サーバも返されます。

以降のクエリ（**http://us_cucm1.ent-pa.com:6972/SPDefault.cnf.xml** など）は HTTP 経由の TFTP クエリです。こうして、プロビジョニング プロセスが UDS と TFTP サーバに対するクエリによって実行されます。これらのクエリの結果として、プロビジョニング情報がクライアントに転送され、クライアントは登録プロセスを開始することができます。

登録プロセスは次の 2 つのアクションで構成されます。

1。 Expressway-C 上の XCP ルータ機能を介して実行される IM と Presence ログイン。XCP ルータは Expressway-C 上の IM と Presence クラスタに問い合わせて、ユーザの設定場所である IM と Presence クラスタを見つけ、Jabber クライアントが IM と Presence サービスにログインできます。

2。 SIP REGISTER メッセージを使用した Unified CM 登録：Expressway SIP プロキシ機能によってプロキシされます。

Business-to-Business（B2B）コミュニケーション

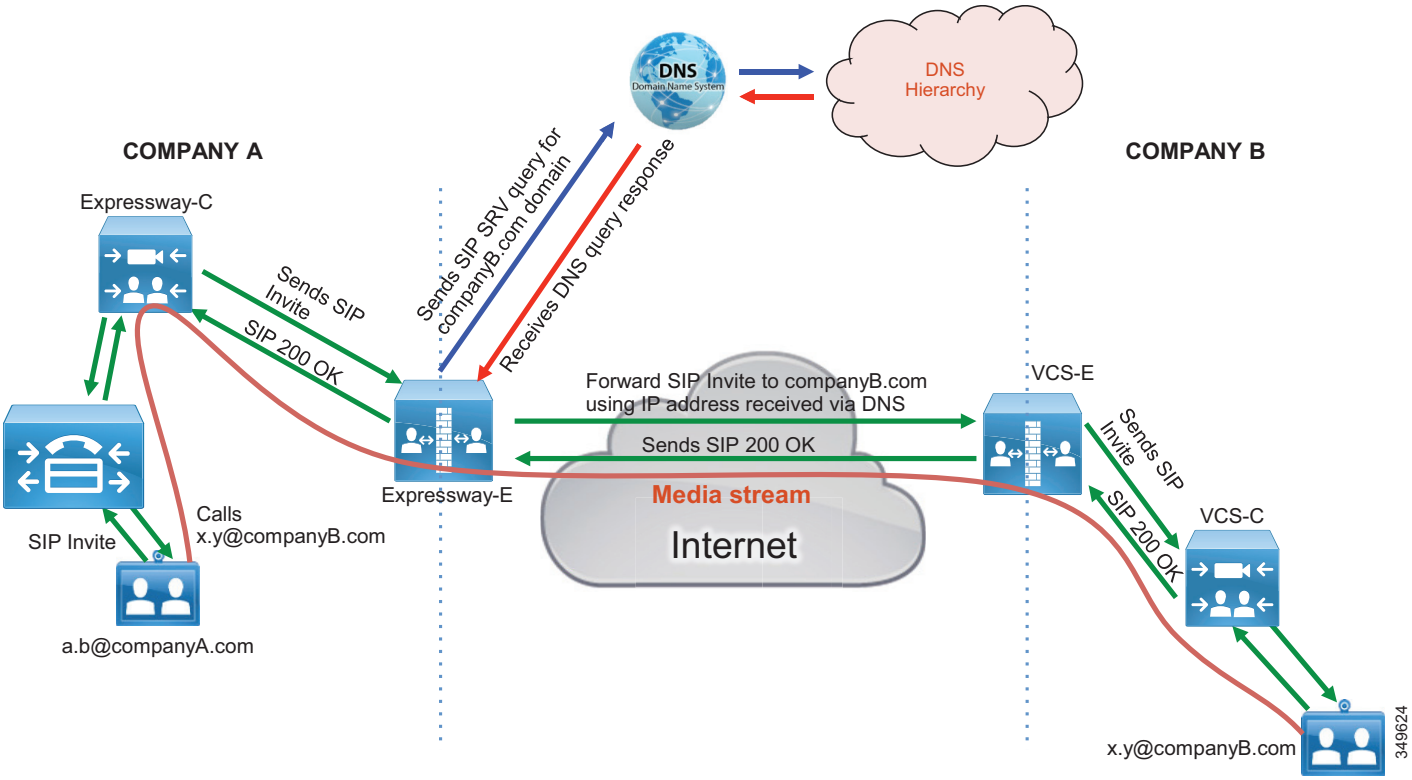
Business-to-Business（B2B）コミュニケーションには、URI ルーティングの目的でリモート組織のドメインを検索できる機能が必要です。これは、Expressway-E 上で DNS ゾーンを作成することによって実行されます。SIP と H.323 の両方がデフォルトで設定されます。これにより、Expressway-E は、自動的に、開始コールで使用されていない別のプロトコルを使用して DNS クエリを再発行できます。そのため、このコールは成功する可能性が高くなります。Expressway-C と Expressway-E は、コールを開始するために使用されたプロトコルを使用しますが、Expressway 上で SIP/H.323 間ゲートウェイ インターワーキングが有効になっている場合は自動的に別のプロトコルを使用しようとします。

Expressway-E の場合、SIP/H.323 間のインターワーキングは [オン（On）] に設定する必要があります。これにより、コールが H.323 コールとして受信された場合に、Expressway-E がそのコールを SIP に接続し、Unified CM への残りのコール レッグにネイティブ SIP を使用できます。同様に、H.323 システムへの発信コールは、Expressway-E に到達して H.323 に接続されるまで SIP コールを維持します。

インターネット経由で Business-to-Business（B2B）コミュニケーションを受信するには、外部 SIP レコードと H.323 DNS レコードが必要です。これらのレコードを使用すれば、他の組織は URI のドメインをそのコール サービスを提供している Expressway-E に解決できます。シスコの検証済みデザインには、Business-to-Business（B2B）コミュニケーション用の SIP レコード、SIPS SRV レコード、および H.323/H.225 SRV レコードが含まれています。RAS に使用される SRV レコードは、登録用のゲートキーパーを見つけるためにエンドポイントで使用されるレコードであり、Expressway-E ではこれが必要ありません。

C：図 4-10 は URI のドメインを解決する DNS プロセスを示し、C：例 4-1 は SRV 検索の例を示し、C：表 4-3 は Business-to-Business（B2B）コール シナリオに使用される DNS SRV レコードを示しています。

C：図 4-10　　DNS を使用した URI ダイヤリング



C：例 4-1　　ent-pa.com ドメインの SRV レコードの例

```
>nslookup
set type=srv
_sips._tcp.ent-pa.com

Non-authoritative answer:
_sips._tcp.ent-pa.com  SRV service location
    priority = 1
    weight   = 10
    port     = 5061
    srv hostname = expe.ent-pa.com.
```

C：表 4-3　　Business-to-Business（B2B）DSN SRV レコード

コール タイプ	SRV レコード	ポート	プロトコル
SIP Business-to-Business（B2B）	_sips._tcp.ent-pa.com	5061	TLS
	_sip._tcp.ent-pa.com	5060	TCP
	_sip._udp.ent-pa.com	5060	UDP
H.323 Business-to-Business（B2B）	_h323ls._udp.ent-pa.com	1719	RAS
	_h323cs._tcp.ent-pa.com	1720	H.225

Expressway-E 上の DNS ゾーンの設定方法については、『*Cisco Expressway Basic Configuration Deployment Guide*』の最新版を参照してください。

Business-to-Business（B2B）コールの IP ベース ダイヤリング

IP ベース ダイヤリングは、H.323 エンドポイントを使ってダイヤルする場合のほとんどのシナリオで使用されるよく知られた機能です。Cisco Collaboration Architecture では、SIP URI を使用するため、IP ベース ダイヤリングは必要ありません。ただし、コールの発着信に IP アドレスしか使用できない他の組織のエンドポイントと対話する場合は、Cisco Collaboration Architecture で着信コールと発信コールの両方に IP ベース ダイヤリングを使用できます。

アウトバウンド コール

アウトバウンド IP ダイヤリングは Expressway-E と Expressway-C ではサポートされますが、Cisco Unified Communications Manager では完全なネイティブ サポートはありません。ただし、後述するように、IP ベース ダイヤリングを使用するように Unified CM をセットアップすることができます。

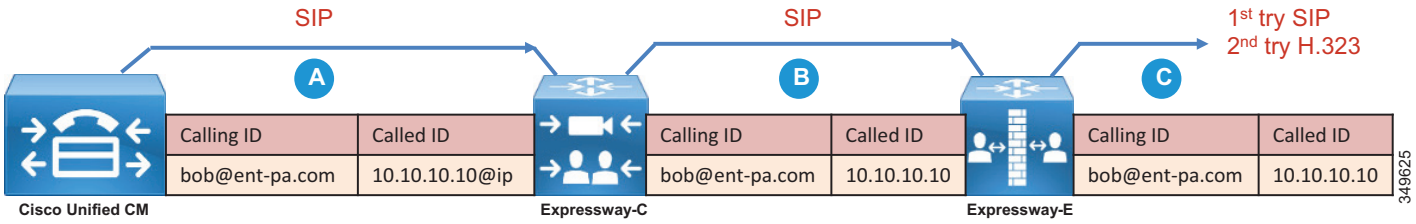
IP アドレス単独でダイヤルする代わりに、Cisco Unified CM 上のユーザは、10.10.10.10@ip のように SIP URI ベースの IP アドレスにダイヤルすることができます。ここで、「@ip」は、リテラルで、「external」、「offsite」、またはその他の意味のある単語に置き換えることができます。

Unified CM は、「ip」架空ドメインを Expressway-C にルーティングするように設定された SIP ルート パターンに一致します。Expressway-C はドメイン「@ip」を除外して、そのコールを（IP アドレス ダイヤリング用に設定されている）Expressway-E に送信します。

Expressway -E 上の不明な IP アドレス宛てのコールは [直接（Direct）] に設定する必要があります。コール制御が展開されていない場合は IP ベース アドレス ダイヤリングのほとんどが H.323 エンドポイントで設定されるため、Expressway-E は H.323 コールをパブリック IP アドレスにあるエンドポイントに直接送信できます。C：図 4-11 に示すように、コールは Expressway-E 上で接続されるまで SIP コールを維持します。

IP アドレス ダイヤリングを提供するための他のオプションがあります。1 つのオプションは、IP アドレス フィールドに使用される "." を記号 "*" に置き換えることです（例：
"10*10*10*10"）。Cisco Unified Communications Manager がそれをルート パターンに照らして照合し、Expressway が正規表現（regex）検索ルールを使用して "*" を "." に置き換えます。

C：図 4-11　　アウトバウンド IP ベース ダイヤリングの例



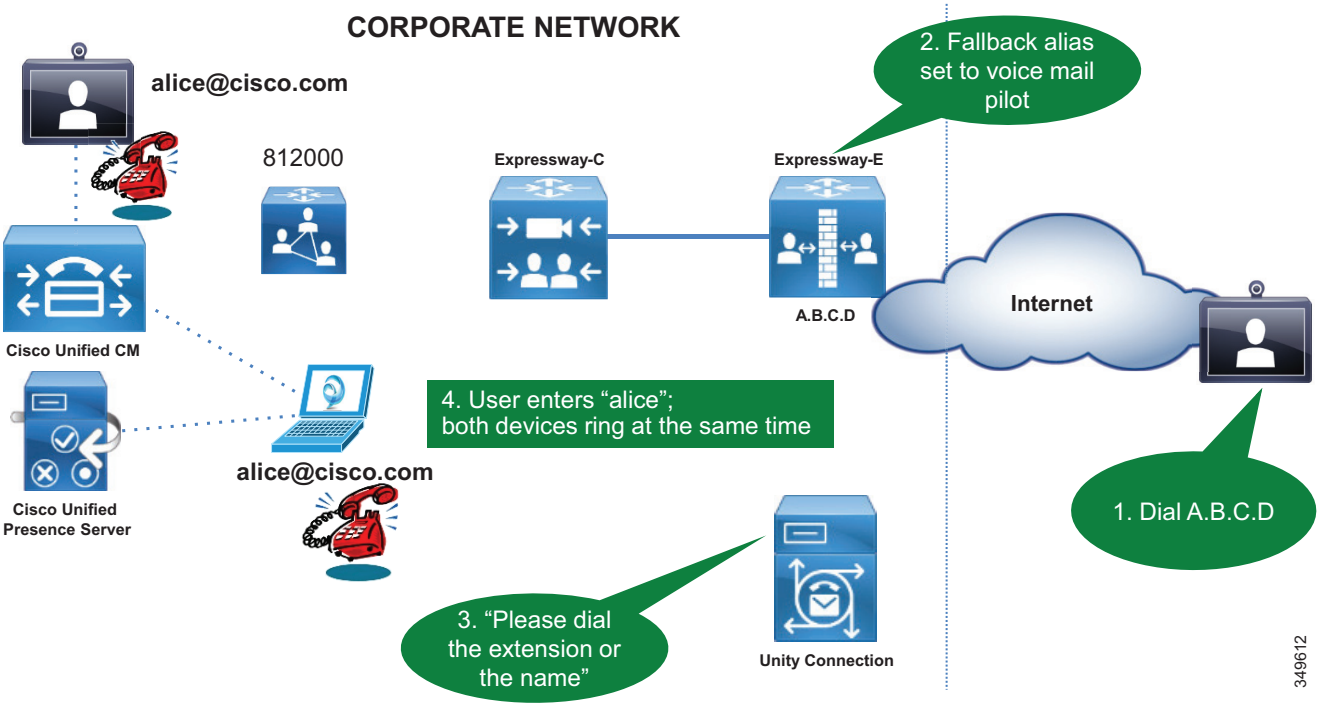
着信コール

IP ベースの着信コールは、Expressway-E で設定されたフォールバック エイリアスを使用します。インターネット上のユーザが Expressway-E 外部 LAN インターフェイスの IP アドレスにダイヤルすると、Expressway-E がそのコールを受信して、フォールバック エイリアスで設定されたエイリアスにコールを送ります。たとえば、コールを会議番号 80044123 または会議エイリアス meet@ent-pa.com に送信するようフォールバック エイリアスが設定されている場合、着信コールはそのような会議を担当する Cisco Meeting Server に送信されます。

IP アドレスとフォールバック エイリアス間の静的マッピングが制限されている場合は、フォールバック エイリアスを Cisco Unity Connection のパイロット番号に設定できます。この方法では、Unity Connection 自動応答機能を使用して、DTMF 経由で、または、Unity Connection でサポート可能な場合は音声認識によって、最終宛先を指定できます。

Unity Connection が Expressway-E の IP アドレスにダイヤルする外部エンドポイントの自動応答機能として使用されている場合は、Unity Connection の Unified CM トランク設定で [再ルーティング用コーリングサーチスペース（Rerouting Calling Search Space）] に設定することを忘れないでください。C：図 4-12 に、セットアップを示します。

C：図 4-12　　インバウンド IP ベース ダイヤリングの例



Expressway 経由の外部 XMPP フェデレーションの展開

XMPP フェデレーションは、モバイル & リモート アクセスと同じタイプのトラバーサル接続（Unified Communications トラバーサル）を利用します。XMPP フェデレーションはスタンドアロン サービスとして展開できます。また、同じ Unified Communications トラバーサル リンクを利用するモバイル & リモート アクセスと一緒に、同じ Expressway-C と Expressway-E のペア上に展開することもできます。

インスタント メッセージおよびプレゼンス フェデレーションを展開するには、次の標準作業を実行します。

1。 フェデレーション用のメールアドレスを検証します。

Expressway 経由の XMPP フェデレーションは、メールアドレスから XMPP アドレスへの変換をサポートしていません。メールアドレスから Jabber ID への変換は、IM と Presence サーバ フェデレーション モデルの機能です。この機能は、ユーザ エクスペリエンスを向上させ、電子メール URI 表記と JID URI 表記が異なる場合に XMPP フェデレーションに関する通信を簡

略化するためによく使用されます。Expressway 経由で XMPP フェデレーションを展開する場合は、ユーザ エクスペリエンスの向上と通信の簡略化という同じ目的が適用されます。IM と Presence ドメインは電子メール ドメインと同じドメインに設定することをお勧めします。また、UserID、メールアドレス表記、および Jabber ID に対して LDAP sAMaccount 名を使用することもお勧めします。コラボレーション アーキテクチャ全体では、反復可能でスケーラブルな URI 表記に関する包括的で一貫した戦略を策定することをお勧めします。

2. IM と Presence サービスが稼働可能で、XMPP フェデレーションがオフになっていることを確認してください。

   IM と Presence サーバ上の XMPP フェデレーションは、Expressway 上で設定されたフェデレーションと競合しないようにするため、オフにする必要があります。

3. サーバ証明書要件を解決します。

   Expressway-C および Expressway-E 用の証明書をセットアップする時期を事前に計画します。XMPP フェデレーションの一部としてチャット ノード エイリアスを使用する予定の場合は、チャット ノード エイリアス FQDN を証明書のサブジェクト代替名（SAN）フィールドに含める必要があります。これを事前に行うことによって、新しい証明書を生成する必要がなくなるだけでなく、Expressway-E 上での公開証明書に対する経費の増加が抑えられます。Expressway のセキュリティと証明書の詳細については、セキュリティーの章を参照してください。

4. Expressway-C 上で XMPP フェデレーション用のローカル ドメインを設定します。

5. Expressway-E を XMPP フェデレーションとセキュリティ用に設定します。

   このステップによって、フェデレーションと、外部フェデレーションに必要なセキュリティ レベルが有効になります。認証は必須であり、ダイヤルバック シークレット経由でセットアップされます。TLS 経由の通信保護が推奨設定です。許可または拒否する外部ドメインと外部チャット ノード エイリアスの承認もこのセクションで設定されます。

6. フェデレーテッド ドメインとチャット ノード エイリアス用の XMPP サーバを DNS ルックアップまたは静的ルートを使用してどのように配置するかを設定します。

   Expressway シリーズは、DNS SRV レコード経由のフェデレーションと静的ルート経由のフェデレーションをサポートしています。静的ルートは、DNS クエリを実行せずに外部ドメインに到達するパスを定義します。パブリック XMPP SRV レコードは、フェデレーションをサポートする外部ドメインを解決するために使用されます。これらのレコードは、オープン フェデレーション モデルを展開するときに、他の組織があなたの組織に到達するために必要です。

7. 正しいファイアウォール ポートが開いていることを確認します。

8. XMPP フェデレーションのステータスをチェックします。

SIP トランク経由の PSTN 音声接続用の Cisco Unified Border Element の展開

Cisco Unified Border Element は、PSTN 集中型アクセスに推奨されているセッション ボーダー コントローラです。これは、企業ネットワークと通信事業者ネットワークの間に境界ポイントとして展開されます。外部インターフェース経由の IP PSTN へのアクセスと、内部インターフェイス経由の企業ネットワークへのアクセスを提供します。集中型 PSTN サービスを有効にするため、企業ネットワークが通信事業者のネットワークに接続されている場所に展開する必要があります。

すべてのリモート サイトが中央の PSTN 接続を利用するため、Cisco Unified Border Element は高い冗長性を備えている必要があります。PSTN 中央サービスが使用できない場合は、ローカル PSTN アクセスを備えたオフィスだけが外部コールを発信できます。そのため、Cisco Unified Border Element をペアで展開して冗長性を確保することをお勧めします。

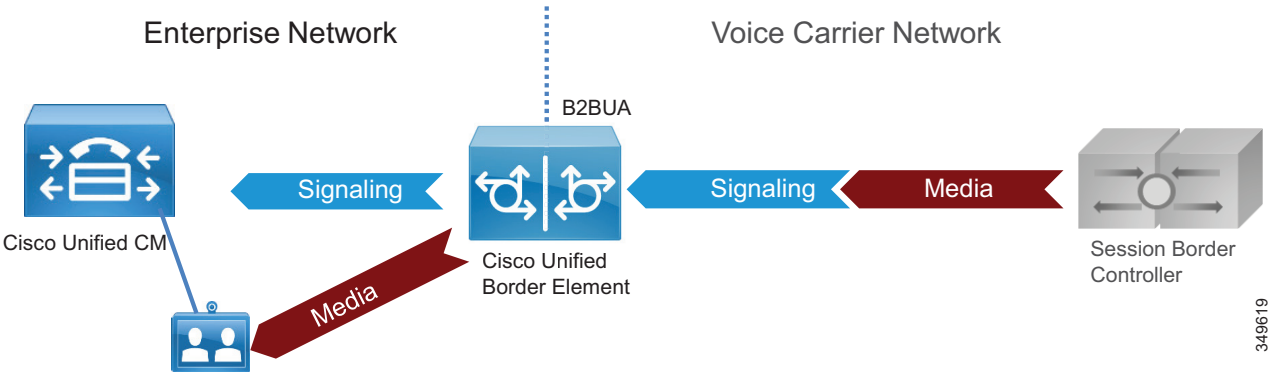
Unified Border Element は、Cisco IOS サービス統合型ルータ（ISR）プラットフォームとアグリゲーション サービス ルータ（ASR）プラットフォーム上でサポートされる Cisco IOS フィーチャ セットです。正しいプラットフォームの選択方法については、サイジング の章を参照してください。

Cisco Unified Border Element は、Unified CM からのセッションを終了して通信事業者ネットワークに向けて再発信する、または、その逆を実行するセッション ボーダー コントローラです。インターネット上で公開される Expressway-E とは対照的に、Cisco Unified Border Element はプライベート ネットワーク（社内ネットワークと通信事業者のネットワーク）間に展開されることに注意してください。通信事業者の視点では、集中型 PSTN へのトラフィックが Cisco Unified Border Element の外部インターフェイスから開始されます。企業の視点では、通信事業者からのトラフィックが Cisco Unified Border Element の内部インターフェイスから開始されます。この意味で、Cisco Unified Border Element はトポロジ隠蔽を実行しています。

Cisco Unified Border Element の展開は Expressway のそれとは異なります。前者は通信事業者ネットワーク（プライベートな管理および保護されたネットワーク）へのアクセスを提供するのに対して、後者はインターネットへのアクセスを提供します。そのため、Cisco Unified Border Element の展開では DMZ が必要ありません。

C：図 4-13 に示すように、この推奨アーキテクチャでは、Unified Border Element が、通信事業者ネットワークに対する WAN インターフェイスと企業ネットワークに対する LAN インターフェイスを備えています。

C：図 4-13　　IP PSTN アーキテクチャ

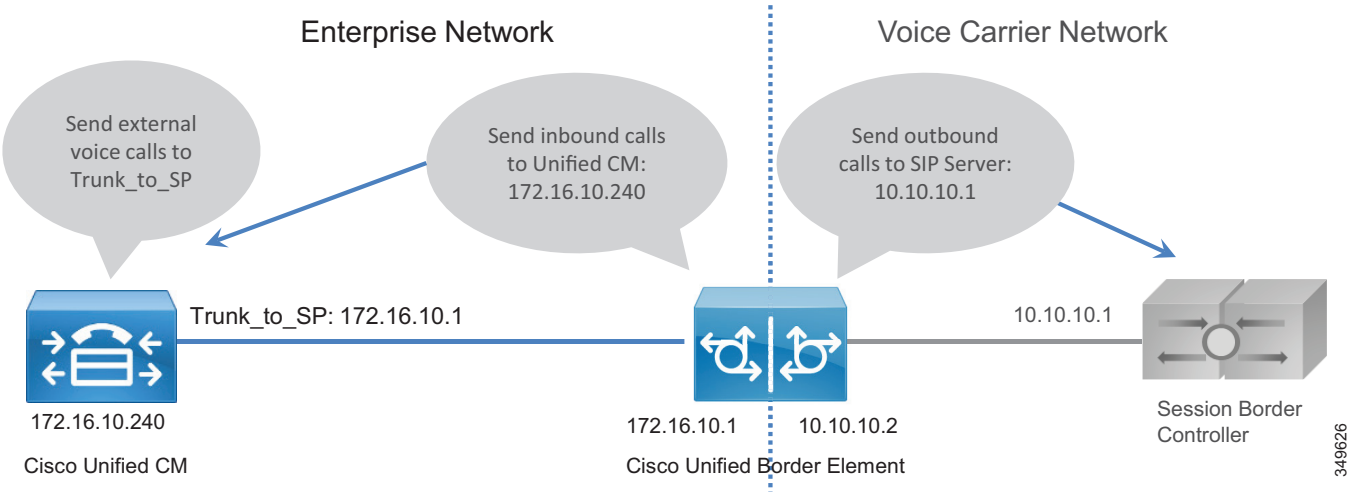


Cisco Unified Border Element は次の機能を実行します。

- C：図 4-14 に示すアドレス変換とポート変換を含むトポロジ隠蔽。Unified CM からのすべてのトラフィックが Unified Border Element 内部インターフェイスに送信され、通信事業者ソフトスイッチからのすべてのトラフィックが Unified Border Element 外部インターフェイスに送信されます。これらの間の直接接続は存在しません。C：図 4-14 に、Cisco Unified CM 上のトランキング設定と Unified Border Element 上の音声ルートの詳細を示します。
- 遅延オファーから早期オファーへの変換とその逆変換
- メディア インターワーキング：インバンドおよびアウトオブバンド DTMF サポート、DTMF 変換、FAX パススルーおよび T.38 FAX リレー、音量およびゲイン制御
- コール アドミッション制御（CAC）：CAC は、CPU、メモリ、コール到着スパイク検出などのリソース消費に基づいて Unified Border Element によって実行できます。CAC はインターフェイス レベルでまたはグローバルに実装できます。Unified CM 上で設定される CAC はロケーションベースですが、Unified Border Element 上で設定される CAC はリソースベースです。Unified Border Element のオーバーサブスクリプションを避ける目的、およびセキュリティ上の理由から、リソースベースの CAC を推奨します（コラボレーション エッジのセキュリティーに関するセクションを参照）。

- RTP/SRTP 間インターワーキング、SIP 不正パケットの検出、非ダイアログ RTP パケットの破棄、SIP リスニング ポートの設定、ダイジェスト認証、同時コール数制限、コール レート制限、電話料金の詐欺行為からの保護、および複数のシグナリングとメディアの暗号化オプションを含むセキュリティ機能
- 保留、転送、および会議を含む通話中補足サービス
- PPI/PAI/ プライバシーおよび RPID：通信事業者との ID ヘッダー インターワーキング
- 複数の通信事業者からの SIP トランクに対する同時接続
- マルチキャスト保留音（MoH）からユニキャスト MoH への変換
- 課金統計情報と呼詳細レコード（CDR）の収集

C：図 4-14　　Cisco Unified Border Element のトランキングに関する留意点



PSTN ゲートウェイ

レガシー PSTN ゲートウェイは、サイトごとに独自の PSTN 接続が割り当てられる分散アーキテクチャで展開されます。集中型 PSTN アクセスには Cisco Unified Border Element の使用をお勧めしますが、日常業務の実行を外部コールに大きく依存しているサイトのバックアップとして PSTN ゲートウェイを使用することもできます。

この場合は、同時 ISDN チャネル数が集中型 PSTN への同時コール数を大きく下回る可能性があります。これは、それらがバックアップ シナリオでしか使用されないためです。たとえば、通常の状況で集中型 PSTN への 30 本の同時コールが許容される場合は、バックアップ シナリオでしか使用されないバックアップ ISDN ゲートウェイを 2 つの BRI チャネルだけをサポートする規模に設定できます。

シスコ音声ゲートウェイは以下をサポートしています。

- DTMF リレー機能
- 補足サービス サポート：補足サービスは、保留、転送、会議などの基本的なテレフォニー機能です。
- FAX パススルーと T.38 FAX リレー

PSTN ゲートウェイはさまざまなプロトコル（SCCP、MGCP、H.323、SIP）をサポートしています。SIP は、Cisco Collaboration ソリューション全体と調和しているうえ、新しい音声製品やビデオ製品に選択されたプロトコルであるため、お勧めのプロトコルです。

音声ゲートウェイ機能は、適切な PVDM とサービス モジュールまたはカードが実装されたすべての Cisco ISR 上で有効になっています。

コラボレーション エッジのハイ アベイラビリティー

ハイ アベイラビリティは、コラボレーション システムの設計と展開における重要な側面です。コラボレーション エッジによって、冗長性、ロード シェアリング、およびコール ライセンス共有が実現されます。

Expressway-C と Expressway-E のハイ アベイラビリティ

Expressway-C と Expressway-E はクラスタで展開することをお勧めします。クラスタごとに最大 6 つの Expressway ノードと最大 N+2 の物理冗長性を設定できます。クラスタ内のすべてのノードがアクティブです。クラスタ設定の詳細については、『*Cisco Expressway Cluster Creation and Maintenance Deployment Guide*』の最新版を参照してください。

Expressway クラスタは設定の冗長性を提供します。クラスタ内で設定される最初のノードは*パブリッシャ*で、その他のすべてのノードは*サブスクライバ*です。設定はパブリッシャ内で実行され、自動的に他のノードにレプリケートされます。

Expressway クラスタは、コール ライセンス共有と回復力を提供します。すべてのリッチ メディア セッションがクラスタ内のノード間で等しく共有されます。コール ライセンスはノードごとに設定されたライセンスによって供与されます。

次のルールが Expressway クラスタリングに適用されます。

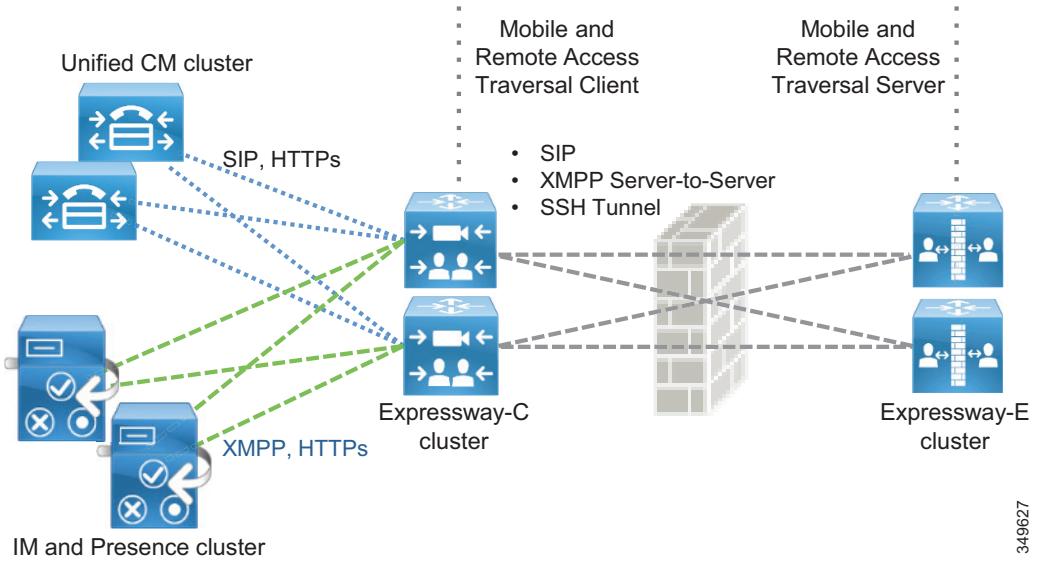
- Expressway-C ノード タイプと Expressway-E ノード タイプを同じクラスタ内に混在させることはできません。
- クラスタ内のすべてのノードで、ゾーン、認証、およびコール ポリシーの設定を同じにする必要があります。
- 設定の変更はマスター ノードでのみ行う必要があり、この変更によってレプリケーション時にクラスタ内の他のピア上の設定が上書きされます。
- あるノードが使用できなくなった場合は、そのノードがクラスタに供与していたライセンスが 2 週間後に使用できなくなります。
- Expressway-C クラスタと Expressway-E クラスタには同じ数のノードを展開します。
- クラスタ全体に同じ OVA テンプレートを展開します。
- クラスタ内のすべてのノードは、他のすべてのクラスタ ノードへの最大ラウンドトリップ時間を 30 ms 以内にする必要があります。したがって、WAN 経由のクラスタリングは遅延の制約があるためお勧めできません。
- 同じクラスタ内のすべてのノードに対して同じクラスタ事前共有キーを使用する必要があります。
- データベース レプリケーションのために、クラスタ内のすべてのノードで H.323 を有効にする必要があります。同時に、インターネットから送られてくる H.323 コールもブロックする必要がある場合は、外部 LAN インターフェイス上の H.323 トラフィックをドロップするファイアウォール ルールを使って Expressway-E を設定できます。

- 同じ Expressway-C と Expressway-E のペアでモバイル & リモート アクセスと Business-to-Business（B2B）コミュニケーションが有効になっている場合は、Unified CM と Expressway-C 間の SIP トランク上で使用されている SIP ポート番号をデフォルトの 5060 または 5061 から変更する必要があります。
- DNS SRV レコードは、クラスタに対して使用可能にする必要があり、クラスタのノードごとに A レコードまたは AAAA レコードを含む必要があります。

Expressway-C は内部ネットワークに、Expressway-E は DMZ にそれぞれ展開されるため、モバイルおよびリモート アクセス用のユニファイド コミュニケーション トラバーサル ゾーンを介して Expressway-C と Expressway-E を接続する必要があります。Business-to-Business（B2B）コールには別個のトラバーサル ゾーンが必要です。このゾーンでは Expressway-C 用のトラバーサル クライアント ゾーンと Expressway-E 用のトラバーサル サーバ ゾーンの名前が保持されます。トラバーサル サーバ、トラバーサル クライアント、およびユニファイド コミュニケーション トラバーサル ゾーンには、Expressway-C と Expressway-E のすべてのノードが含まれているので、いずれかのノードに到達できない場合は代わりにクラスタの別のノードに到達します。

C：図 4-15 に示すように、Expressway-C が Cisco Unified CM、IM and Presence、および Unity Connection の各クラスタのすべてのサーバに接続するため、接続パス全体でハイ アベイラビリティと冗長性が確保されます。

C：図 4-15　　Expressway サービス接続



C：図 4-15 に、Unified Communications トラバーサル ゾーンとモバイル & リモート アクセスに組み込まれているハイ アベイラビリティを示します。ただし、次の説明は、Unified Communications トラバーサル ゾーンと標準の（クライアントとサーバ）トラバーサル ゾーンの両方に適用されます。

Expressway-C 上に設定されたトラバーサル クライアント ゾーンには、対応する Expressway-E クラスタのすべてのクラスタ ノードの完全修飾ドメイン名を含める必要があります。同様に、トラバーサル サーバ ゾーンはすべての Expressway-C クラスタ ノードに接続する必要があります。これは、Expressway-C 証明書のサブジェクトの別名に Expressway-C クラスタ ノードの FQDN を含め、**TLS 検証サブジェクト名**を Expressway-C クラスタの FQDN と同一に設定することによって実現されます。これにより、トラバーサル ゾーン全体にクラスタ ノードのメッシュ構成が形成され、最後のクラスタ ノードが使用不能になるまでトラバーサル ゾーンのハイ アベイラビリティが維持されます。

Expressway-C はトランク経由で Unified CM に接続して、Business-to-Business（B2B）の着信コールと発信コールをルーティングします。Unified CM は Expressway-C へのトランキングも行います。ハイ アベイラビリティを維持するために、各 Expressway-C クラスタ ノードの完全修飾ドメイン名を Unified CM 上のトランク設定に列挙する必要があります。逆に、Unified CM クラスタの各メンバーの完全修飾ドメイン名（FQDN）を Expressway-C のネイバー ゾーン プロファイルに列挙する必要があります。

ここでも、メッシュ状のトランク構成が形成されます。Unified CM は、SIP Options Ping 経由でトランク設定内のノードのステータスをチェックします。あるノードが使用できなくなると、Unified CM はそのノードを運用停止にして、そのノードに対するコールをルーティングしなくなります。Expressway-C も SIP OPTIONS Ping 経由で Unified CM からのトランクのステータスをチェックします。コールは、アクティブかつ使用可能として示されているノードにのみルーティングされます。これにより、トランク設定の両側にハイ アベイラビリティが提供されます。

DNS SRV レコードは、インバウンド Business-to-Business（B2B）トラフィックに対する Expressway-E の可用性を高めることができます。高可用性を確保するためには、クラスタ内のすべてのノードを SRV レコード内に同じ優先度と同じ重要度で列挙する必要があります。これにより、すべてのノードを DNS クエリで返すことができます。DNS SRV レコードは、クライアントがルックアップに費やす時間を最小にするために役立ちます。これは、SRV レコード内に列挙されたすべてのノードを DNS 応答に含めることができるためです。通常は、遠端サーバまたは遠端エンドポイントが DNS 応答をキャッシュし、応答が受信されるまで DNS クエリで返されたすべてのノードを試します。これにより、コールが成功する確率が高まります。

さらに、Expressway クラスタは、クラスタ全体でのリッチ メディア ライセンス共有をサポートします。クラスタからノードが削除された場合は、そのコール ライセンスの共有が次の 2 週間だけ継続されます。どの Expressway も、その物理能力を上回るライセンスを保持することはできても、その物理能力を上回る Rich Media ライセンスを処理することはできません。

Cisco Unified Border Element のハイ アベイラビリティ

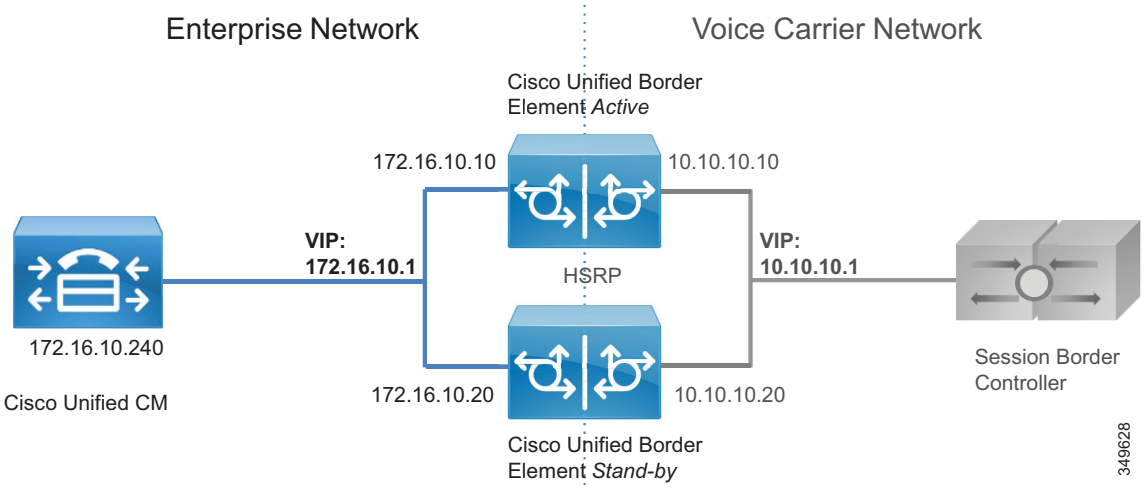
Cisco Unified Border Element のハイ アベイラビリティは複数の方法で実現できます。推奨アーキテクチャでは、コールの保存によるボックスツーボックス冗長性をお勧めします。これは、Unified Border Element で障害が発生した場合にシグナリングとメディアの両方のコールの保存が実施されるためです。

Unified Border Element サーバは、次のアクティブ / スタンバイ モデルのペアで展開されます。アクティブ Unified Border Element がダウンすると、スタンバイ Unified Border Element が起動され、すべてのアクティブ セッションが移行されます。これにより、シグナリングとメディアの両方のハイ アベイラビリティが提供されます（C：図 4-16 を参照）。

Hot Standby Routing Protocol（HSRP）テクノロジーは、1 つのルータの可用性に頼らずに、ネットワーク上のホストからの IP トラフィックをルーティングすることによって、ネットワークのハイ アベイラビリティを実現します。ルータのグループで HSRP を使用して、アクティブ ルータとスタンバイ ルータを選択します HSRP は内部と外部の両方のインターフェイスをモニタします。インターフェイスのいずれかがダウンした場合は、デバイス全体がダウンしたと見なされ、スタンバイ デバイスがアクティブになってアクティブ ルータの役割を引き継ぎます。

ボックスツーボックス冗長性は、HSRP プロトコルを使用してルータの HSRP アクティブ / スタンバイ ペアを形成します。アクティブ サーバとスタンバイ サーバは、同じ仮想 IP アドレスを共有し、ステータス メッセージを継続的に交換します。C：図 4-16 に示すように、Unified Border Element セッション情報がルータのアクティブ / スタンバイ ペア全体で共有されます。ここで、172.16.0.1 と 10.10.10.10 は Cisco Unified Border Element ペアの仮想 IP アドレスです。これにより、アクティブ ルータが予定どおりにまたは予定外の理由で稼働停止状態になった場合に、すぐにスタンバイ ルータがすべての Unified Border Element コール処理の役割を引き継ぐことができます。

C：図 4-16　Cisco Unified Border Element のボックスツーボックス冗長性



音声ゲートウェイのハイ アベイラビリティー

PSTN ゲートウェイは、物理インターフェイスを介して直接 PSTN ネットワークに接続します。ゲートウェイがダウンすると、PSTN とのすべての通信がクリアされます。HSRP などのメカニズムは、このケースではメリットがありませんが、通信事業者向けの IP トランク経由の PSTN アクセスのケースではメリットがあります。ゲートウェイ相互接続を使用した集中型 PSTN が展開される場合もありますが、Unified Border Element と違って、TDM ベースの PSTN ゲートウェイ展開は基本的に分散型です。また、PSTN 音声ゲートウェイは Unified Border Element ほど多くのコール量を管理できません。PSTN の特性上、このシナリオではメディア保存ができません。

ただし、同じ Unified CM ルート グループ内の複数のゲートウェイをコールがロード バランシングされるように設定することによって、シグナリング回復力を提供できます。グループ内のゲートウェイのいずれかがダウンすると、すべてのコールが破棄されますが、残りの使用可能なゲートウェイのいずれかを使用して新しいコールが確立されます。

コラボレーション エッジのセキュリティー

ここでは、コラボレーション エッジでのセキュリティの実装方法について説明します。

Expressway-C と Expressway-E のセキュリティー

Expressway-C と Expressway-E 上のセキュリティは、ネットワーク レベルとアプリケーション レベルでさらに分割することができます。ネットワーク レベルのセキュリティにはファイア ウォール ルールや侵入からの保護などの機能が含まれるのに対して、アプリケーション レベルのセキュリティには認可、認証、および暗号化が含まれます。

ネットワーク レベル保護

Expressway-C と Expressway-E のネットワーク レベル保護は、2 つの主なコンポーネント（ファイアウォール ルールと侵入防御）で構成されます。

ファイアウォール ルールは次の機能を有効にします。

- トラフィックを許可または拒否する送信元 IP アドレスのサブネットを指定します。
- 拒否対象のトラフィックを破棄または拒否するかを選択します。
- SSH や HTTP/HTTPS などの既知のサービスを設定する、または、トランスポート プロトコルとポート範囲に基づいてカスタマイズされたルールを指定します。
- Expressway-E 上の LAN 1 インターフェイスと LAN 2 インターフェイスで別々のルールを設定します。

悪意のあるトラフィックを検出およびブロックし、辞書ベースでの不正ログイン攻撃から Expressway を保護するためには、自動侵入保護機能を使用する必要があります。

自動化された侵入保護は、システム ログ ファイルを解析して、SIP、SSH、Web/HTTPS などの特定のサービス カテゴリへのアクセスの連続的な失敗を検出することによって機能します。指定された時間内の失敗回数が設定されたしきい値を超えた場合は、送信元ホスト IP アドレス（侵入者）と宛先ポートが、指定された期間ブロックされます。その期間が過ぎると、自動的にホスト アドレスのブロックが解除されるため、一時的に設定が間違っていた正規のホストがロックアウトされなくなります。

モバイルおよびリモート アクセス

モバイルおよびリモート アクセスでは、インターネット上のクライアントと Expressway-C の間の設定オプションは TLS、SRTP、HTTPS、および XMPP だけです。クライアントと Expressway-C の間のすべてのトラフィックが常に暗号化されます。

Unified CM と Expressway-C の間の接続は設定に応じて、暗号化と認証が行われます。Unified CM が混合モードの場合は、メディアとシグナリングのエンドツーエンド暗号化をお勧めします。

Cisco Unified CM と Expressway-C の間のセキュアな通信にはセキュリティ証明書が必要です。証明書はサーバとクライアントのアイデンティティを提供し、Expressway-C、Expressway-E、Unified CM、および Unified CM IM and Presence Service に証明書を展開する必要があります。推奨される設定は、認証局（CA）を使用して証明書に署名することです。

CA はプライベートにもパブリックにもできます。プライベート CA 展開にはコスト効率が高いというメリットがありますが、この証明書は組織内部でしか有効ではありません。パブリック CA はセキュリティを向上させ、すべての組織から信頼されます。そのため、異なる組織間の通信に広く利用されています。

コストを削減するために、Expressway-C 証明書が社外で認定されていない内部 CA によって署名されている場合があります。この場合は、Expressway-C と Expressway-E の接続を確立するために、内部 CA 証明書を Expressway-E の信頼された CA 証明書リストに含めることが重要です。Expressway-E 証明書は、パブリック CA によって署名される必要があります。

C：表 4-4 に、証明書展開に対するパブリック アプローチとプライベート アプローチの概要を示します。証明書の詳細については、セキュリティーの章を参照してください。

C：表 4-4　　パブリック証明機関、プライベート証明機関、および証明書

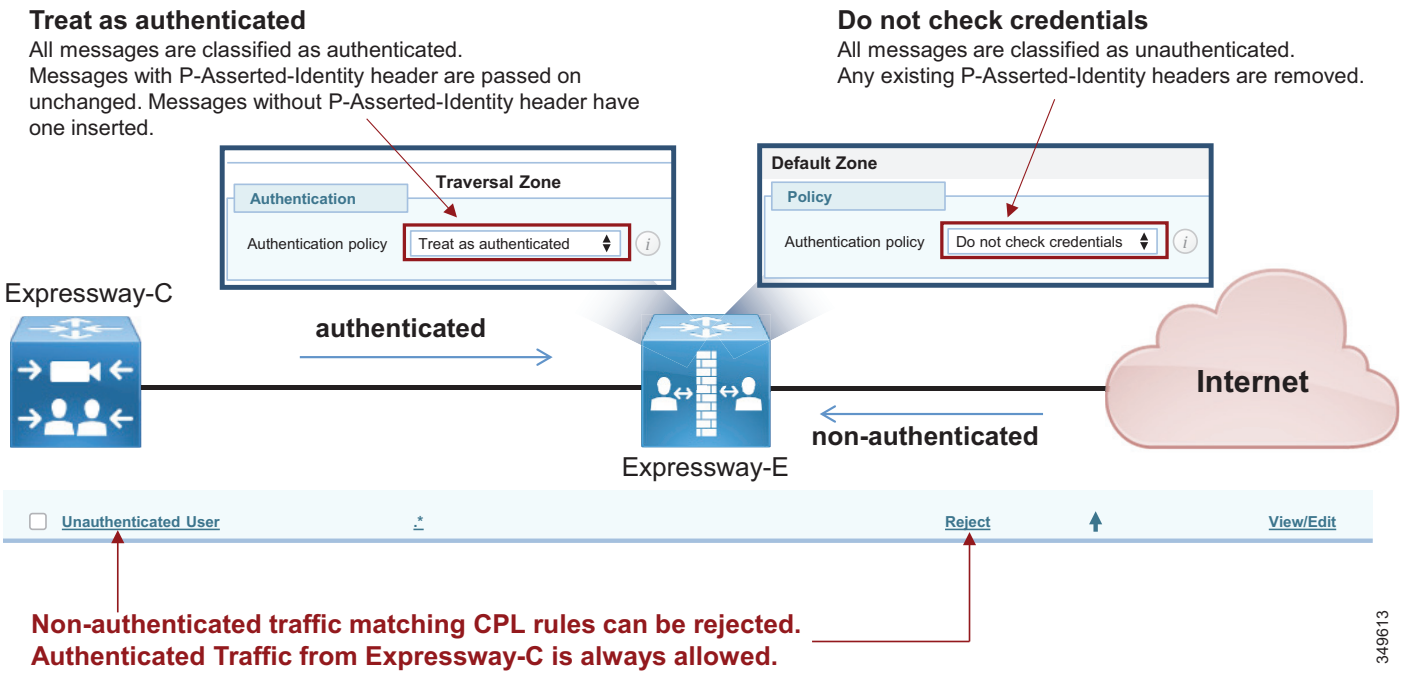
	Unified CM	IM and Presence Service	Expressway-C	Expressway-E
証明書の署名者	内部 CA	内部 CA	内部 CA	パブリック CA
信頼リストへの掲載	内部 CA 証明書	内部 CA 証明書	内部 CA 証明書とパブリック CA 証明書	内部 CA 証明書とパブリック CA 証明書

Business-to-Business（B2B）コミュニケーション

Business-to-Business（B2B）コミュニケーションの保護には、認証、暗号化、および認可が含まれます。Business-to-Business（B2B）コミュニケーションでは、デフォルトで、認証されたトラバーサル リンクが使用されます。また、トラバーサル リンクは、Expressway-C と Expressway-E の間の相互認証される Transport Layer Security（MTLS）接続によって検証される公開キー インフラストラクチャ（PKI）の利点を活用できます。Business-to-Business（B2B）トラバーサル リンクがモバイルおよびリモート アクセスと同じ Expressway-C および Expressway-E インフラストラクチャに展開される場合は、トラバーサル ゾーンが Expressway-C クラスタ ノードと Expressway-E クラスタ ノードの IP アドレスではなく FQDN を使用することを確認してください。これにより、各サーバの証明書を使用して、提示された証明書をトラバーサル接続に対して信頼された証明書に照らして検証するのが容易になります。

着信コールは認証済みか未認証かによって区別できます。この区別は、保護されたリソースへのアクセスの承認に使用できます。コール認証の設定は、ゾーン設定レベルで実施されます。例として、Expressway-E デフォルト ゾーン認証ポリシーを「クレデンシャルを確認しない」に設定できます。これにより、C：図 4-17 に示すように、不明なリモート Business-to-Business（B2B）コールが未認証としてマークされます。

C：図 4-17　　コール認証



これらのコールでは、PSTN などの保護されたリソースへのアクセスを制限する必要があります。これは、Call Processing Language（CPL）ルールをゲートウェイ アクセスに使用されるプレフィクスへのアクセスをブロックする正規表現を使用して設定することによって実現されます

例として、範囲 80XXXXXX の一連のデバイスだけにコールが許可され、外部のインターネット宛先からの +E.164 番号、ゲートウェイ アクセス、その他のサービス（ここでは 0 と 9 で示す）が禁止されている企業を想定します。この場合、ルールは C：表 4-5 に示すように設定できます。

C：表 4-5　　拒否ベースのポリシーの例

ソース タイプ	[接続先（Destination）]	アクション
デフォルト ゾーン	8 [1-9] \ d{6} @ent-pa¥ com	却下
デフォルト ゾーン	[09]\d*@ent-pa\.com	却下
デフォルト ゾーン	\+\d*@ent-pa\.com	却下
デフォルト ゾーン	.*@ent-pa\.com	許可
デフォルト ゾーン	.*	却下

ルールは、トップダウンで照合されます。C：表 4-5 のルールの例では、次の場合にコールが拒否されます。

- 宛先が 8 で始まり、その後に 1 ～ 9 の 1 桁の数字、さらに 6 桁、さらに会社のドメインが続く。
- 宛先が 0 または 9 で始まり、その後に任意の桁数、さらに会社のドメインが続く。
- 宛先が +E.164 番号に一致し、その後に会社のドメインが続く。

C：表 4-5 の最初の 3 つのルールによって拒否されなかったコールは、宛先に会社のドメインが含まれていれば、4 番目のルールによって許可されます。

その他の宛先は、C：表 4-5 の最後のルール（"deny all"）によって拒否されます。これには、ドメインが指定されていないコールが含まれます。

要件と推奨事項

- Business-to-Business（B2B）トラバーサル クライアント ゾーンとトラバーサル サーバ ゾーンで H.323 をオフにします。これにより、Expressway-C と Expressway-E の間のすべてのトラフィックが確実に暗号化されます。コールがトラバーサル サーバ ゾーンに送信される前（インバウンド コールの場合）およびインターネットに送信される前（アウト バウンド コールの場合）に、H.323 インターワーキングが Expressway-E 上で実行されます。
- Business-to-Business（B2B）トラバーサル ゾーンのトラバーサル クライアント側（Expressway-C）のメディア暗号化を**ベスト エフォート**に設定します。Expressway-E Business-to-Business（B2B）トラバーサル サーバ、デフォルト ゾーン、および Business-to-Business（B2B）DNS ゾーンに、同じメディア暗号化設定（**ベスト エフォート**）を使用します。これは、SIP コールの暗号化が常に Expressway-C 上で実施されることを意味します。リモート システムで暗号化がサポートされない場合は、Expressway-C が非暗号化コールをセットアップします。強力な暗号化ポリシーが必要な場合は、メディア暗号化を**強制暗号化**に設定します。この場合、ベスト エフォートの場合と同様にコールが暗号化されます。違いは、リモート システムで暗号化がサポートされない場合に、非暗号化フォールバックなしでコールが終了することです。
- Unified CM と Expressway-C 間の SIP トランクのシグナリング暗号化には TLS を使用します。

モバイルおよびリモート アクセス シナリオと Business-to-Business（B2B）コール シナリオでの証明書の設定：

- 証明書に関する一般的な要件として、Expressway-C と Expressway-E の完全修飾 DNS 名（FQDN）が証明書のホスト名と一致する必要があります。
- Business-to-Business（B2B）コミュニケーションには、証明書に関する他の要件はありませんが、モバイル / リモート アクセス（MRA）には追加の要件があります。Expressway でのモバイルおよびリモート アクセス用の証明書のセットアップ方法について、詳しくはセキュリティーの章を参照してください。

Cisco Unified Border Element のセキュリティー

インターネット接続とは異なり、IP トランク経由の PSTN 接続は、通信事業者から提供されたプライベート ネットワークを介して配信されます。つまり、この接続は制御されたネットワークです。したがって、インターネット エッジ用に展開されたセキュリティは、IP PSTN アクセス用に展開されたセキュリティとは異なります。Cisco Unified Border Element と通信事業者間にはファイアウォールが存在しません。ただし、特定のケースでは、企業と電気通信プロバイダーでエンタープライズ DMZ を使用する必要があります。

通信事業者と企業ネットワークの間では、通常、トラフィックが暗号化されずに送信されます。会社のポリシーによって、内部のエンタープライズ トラフィックを暗号化できる場合とできない場合があります。このようなケースでは、Unified Border Element で TLS/TCP 変換と SRTP/RTP 変換を実行できます。複数のゲートウェイが展開されている場合は、内部 CA を使用して Unified Border Element 証明書に署名することをお勧めします。

Unified Border Element はファイアウォールなしで展開されるため、さまざまなレイヤで保護されます。たとえば、通信事業者のセッション ボーダー コントロールのみに PSTN 側からのコールの開始を許可し、Unified CM のみに内部ネットワーク側からのコールの開始を許可するアクセス コントロール リストを作成できます。

Unified Border Element は、電話料金の詐欺行為やテレフォニー サービス拒否（TDoS）攻撃からも保護されます。ラージ パケット到着率は、CPU、メモリ、帯域利用率、およびコール到着スパイク検出に基づくコール アドミッション制御メカニズムを通して削減することもできます。

音声ゲートウェイのセキュリティ

PSTN ゲートウェイは、顧客ネットワークに 1 つのインターフェイス、PSTN 上に 2 つ目のインターフェイスを備えています。これらのインターフェイスは社内ネットワーク内に展開され、インターネットからは到達できません。PSTN は本質的にセキュアなので、ゲートウェイを保護するための特定のツールは存在しません。ただし、インターネットにアクセス可能なルータ上にゲートウェイが展開されている場合は例外です。この場合は、ゲートウェイ上の Cisco IOS 機能を使用してファイアウォールと侵入防御を実行できます。その他の場合は、ゲートウェイを保護するために必要な特定のツール（サービス拒否（DoS）攻撃からの保護など）はありません。

ただし、エンドポイントからゲートウェイへのメディアを常に暗号化することをお勧めします。このようなケースでは、ゲートウェイで TLS と SRTP が使用されます。この場合は、CA 署名証明書を使用することをお勧めします。

コラボレーション エッジ ソリューションのスケーリング

展開されたコラボレーション エッジ クラスタの数は、コール制御クラスタの数ではなく、インターネットへの接続ポイントの数に左右されます。複数の Unified CM および IM and Presence クラスタと、複数の TelePresence Conductor クラスタを使用しているお客様は、単一のインターネット接続ポイントが設置されていれば、単一のインターネット エッジを所有していることになります。通信事業者が PSTN ネットワークへの接続ポイントを複数提供している場合は、同じ環境に複数の PSTN 外線が設置されている可能性があります。

インターネット エッジ ソリューションのスケーリング

複数のインターネット エッジが展開されている場合は、コラボレーション トラフィックを最も近いインターネット エッジに送信するためのルーティング ルールを正しく設定することが重要です。

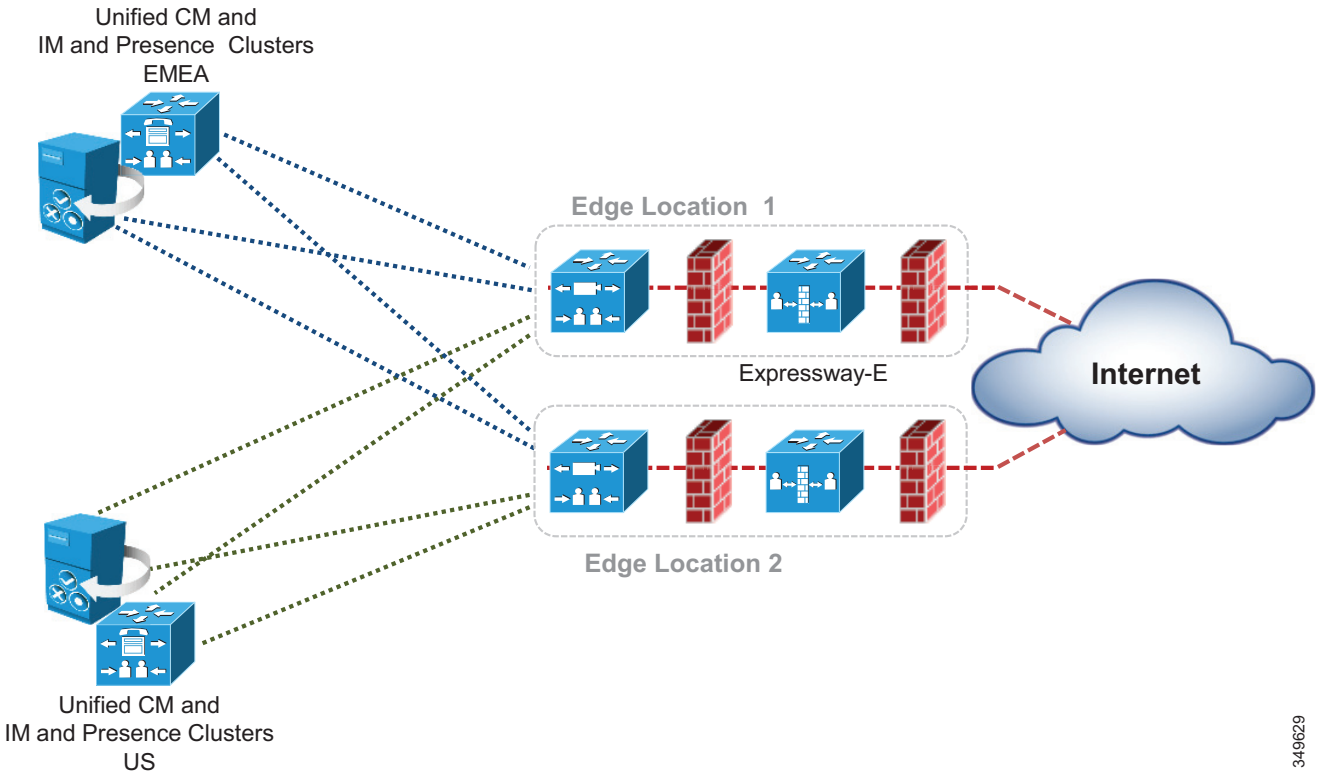
モバイルおよびリモート アクセス

複数の Unified CM および IM and Presence クラスタが展開されている場合は、すべての Expressway-C がすべての Unified CM クラスタを検出する必要があります。Expressway-C が一部のクラスタしか検出しない場合は、検出されたクラスタに属しているユーザに関する登録しかプロキシできません。

Expressway-C でまだ未検出の Unified CM and IM and Presence クラスタに属するクライアントから登録要求が発行された場合、そのクライアントはログインできません。この理由で、C：図 4-18 に示すように、ユーザのモビリティが有効になっている場合に各 Expressway-C がすべての Unified CM and IM and Presence クラスタを検出することが重要です。

加えて、いくつかの Unified CM and IM and Presence クラスタが同じ SIP ドメインを共有している場合は、Unified CM クラスタで ILS を有効にすることが重要です。ILS 機能は、各 Unified CM クラスタに同じネットワーク内の他のクラスタを認識させ、特定のユーザがどのクラスタ（つまりホーム）に属するかを Expressway-C に示すことができます。そのためには、Unified CM ユーザ ページ設定で [ホーム クラスタ（home cluster）] 設定が有効になっている（チェックボックスがオンになっている）必要があります。

C：図 4-18　　複数の Unified CM および IM and Presence クラスタのサービス検出



複数のインターネット エッジが展開されている場合は、着信要求の負荷がそれらの間でどのように分散されるかを理解することが重要です。インターネット エッジが同じデータセンターまたは同じエリアに展開されている場合は、DNS SRV レベルでロード バランシングを実行できます。たとえば、企業ネットワークにモバイル & リモート アクセス用の 3 つのインターネット エッジが含まれており、それぞれが 2 つの Expressway-E ノードと Expressway-C ノードのクラスタで構成されている場合は、**_collab-edge._tls.ent-pa.com** に 6 つすべての Expressway-E レコードが同じ優先度と重要度で追加されます。これにより、登録とコールがさまざまな Expressway-E クラスタと Expressway-C クラスタに均等に分配されます。

モバイル & リモート アクセス接続エンドポイントが特定の Expressway クラスタ ペアを介して登録されると、クライアントが切断されるか、クライアントのスイッチがオフにされるまで接続されたままになります。

ただし、Expressway クラスタが地理的地域全体に展開されている場合は、エンドポイントが確実に最も近い Expressway-E クラスタを使用するようにするため、DNS SRV の優先度と重要度のレコードに加えて何らかのインテリジェント メカニズムが必要になります。

たとえば、ある企業が 2 つの Expressway クラスタを使用しており、1 つは米国（US）に、もう 1 つはヨーロッパ（EMEA）に設置されている場合、US に住んでいるユーザは US 内の Expressway-E クラスタに転送され、ヨーロッパに住んでいるユーザはヨーロッパ内の Expressway-E クラスタに転送されるのが理想的です。これは、GeoDNS サービスを実装することによって容易に実現できます。GeoDNS サービスはコスト効率が高く、設定が簡単です。GeoDNS を使用すれば、位置（IP アドレス ルーティング）や最小遅延などの複数のポリシーに基づいてトラフィックをルーティングできます。

次に、GeoDNS サービス用の DNS を設定する例を示します。

- DNS SRV レコード用の GeoDNS 設定
- CNAME エイリアス用の GeoDNS の設定

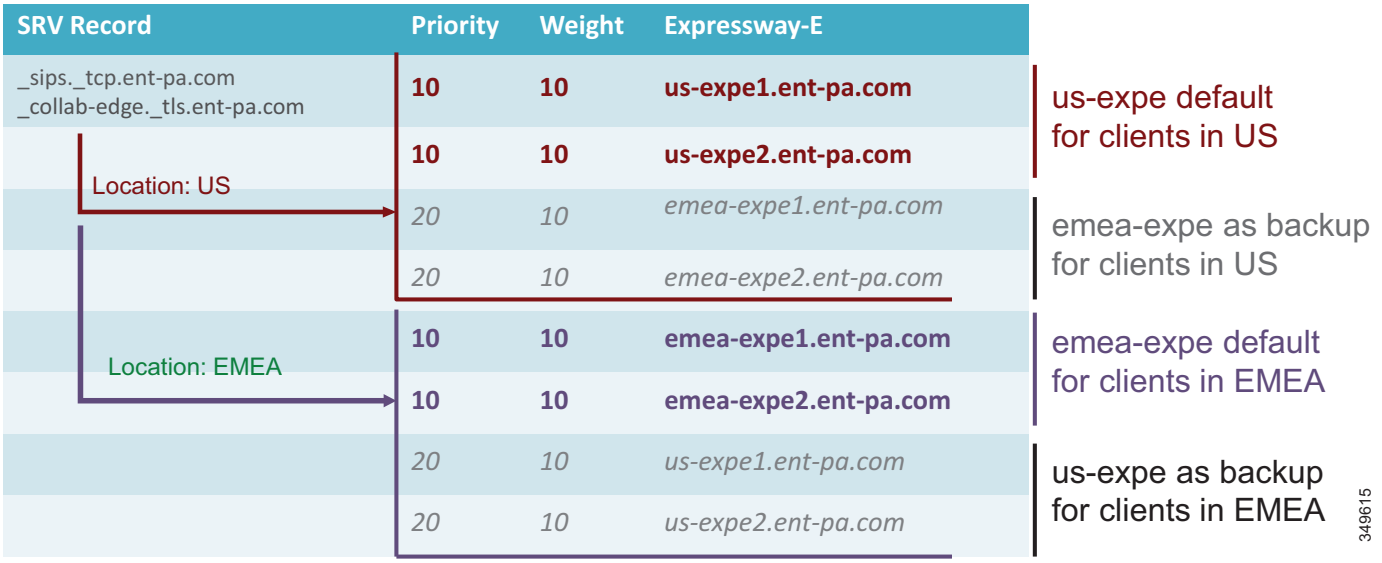
DNS SRV レコード用の GeoDNS 設定

最初のシナリオ例では、2 つのインターネット エッジ Expressway クラスタが米国と欧州に 1 つずつ展開され、それぞれが 2 つの Expressway-C および Expressway-E サーバで構成されます。発信側エンドポイントとヨーロッパ エッジの間で測定された遅延が、エンドポイントと米国エッジの間の遅延を下回っている場合、またはエンドポイント IP アドレスが欧州の範囲に一致する場合、設定されたポリシー（遅延または IP アドレス）に基づいてエンドポイントがヨーロッパ エッジに転送されて登録されます。

一部の GeoDNS プロバイダーは、SRV レコードで GeoDNS サービスをサポートしていますが、多くのプロバイダーは CNAME または A レコードに対してのみ GeoDNS を許可しています。設定をシンプルにしてトラブルシューティングを容易にするために、SRV レコードで GeoDNS サービスを実装することをお勧めします。SRV レコードの GeoDNS 設定を C：図 4-19 に示します。

発信者が米国にいる場合は、コールが米国クラスタに送信されますが、米国クラスタがダウンしている場合はコールが EMEA クラスタに送信されます。この設定は任意の DNS SRV レコードに対して機能するので、Business-to-Business（B2B）シナリオだけでなく、モバイルおよびリモート アクセス シナリオにも対応できます。また、これにより、C：図 4-19 に示すように地理的冗長性も確保されます。

C：図 4-19　　DNS SRV レコード用の GeoDNS 設定例



このシナリオでは、モバイルおよびリモート アクセス (または Business-to-Business コール) の SRV レコードに、特定の場所に対応するタグが付加されます。この SRV レコードはその場所の Expressway-E ピアに解決され、さらに低い優先度でバックアップ場所の Expressway-E ピアに解決されます。これにより、何らかの理由で米国エンドポイントが米国 Expressway クラスタを使用できない場合は、EMEA 内の Expressway-E クラスタにリダイレクトされます。逆もまた同じです。

地理的冗長性は Jabber クライアントとハードウェア クライアントの両方で機能します。ただし、Jabber ユーザがほぼ毎日ログオンとログオフを行うのに対して、ハードウェア クライアントは同じエッジに接続されることが多い点に注意してください。この設定がハードウェア エン

ドポイントにも提供される場合、地理的バックアップの発生後に一旦オフにしてオンに戻さない限り、元の Expressway-E クラスタをホームとして再設定できません。Jabber ではログアウトがより頻繁に発生するため、これは問題とはなりません。

CNAME エイリアス用の GeoDNS の設定

一部の Geo DNS プロバイダーは、DNS SRV レコードに適用される GeoDNS サービスをサポートしませんが、代わりに CNAME または A レコードに適用される GeoDNS サービスをサポートする場合があります。CNAME はそのリソースの実際の A レコードに解決されるエイリアスで、これは DNS SRV 実装において最も一般的な DNS レコードです。すべてのケースで機能する普遍的な設定を提供することはできませんが、この特定のシナリオに対処するための推奨事項をいくつか紹介します。

SRV レコードではなく CNAME レコードに関してのみ GeoDNS サービスを指定することを GeoDNS プロバイダーが許可している場合、以下の例は、CNAME のみが GeoDNS サービスでサポートされる場合の GeoDNS の設定方法を示しています。このシナリオでは、DNS SRV レコードが CNAME レコードに解決され、さらに A レコードに解決されます。CNAME レコードに地理的場所を割り当てることができます。たとえば、米国の Expressway-E クラスタと EMEA における別の Expressway-E クラスタを考えてください。Business-to-Business コール用に SIP TLS の SRV レコード **_sips._tcp.ent pa.com** または **_sip._tcp.ent pa.com** が設定されています。このレコードは、CNAME レコード **alias1.ent pa.com** に解決されます。

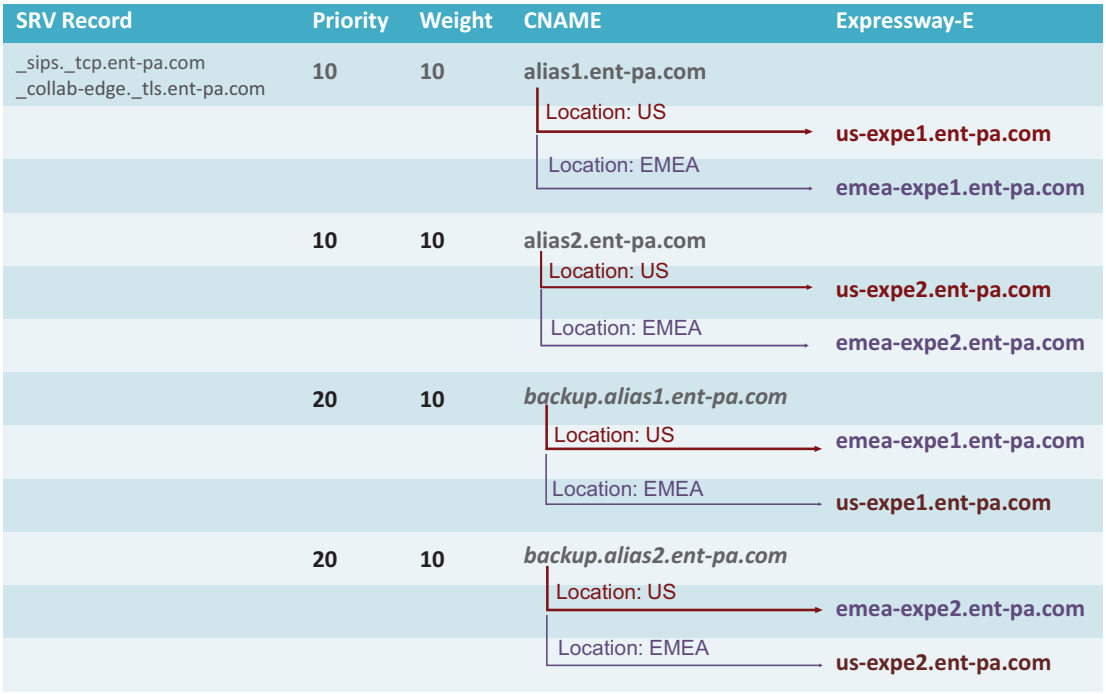
GeoDNS 設定に基づいて、レコードがアクティブになっているリージョンを識別するラベルが CNAME レコードに適用されます。この場合の CNAME 解決は、最も高い優先度（この例では 10）を持つ米国用の A レコード 1 つと EMEA 用の別の A レコードになります。これにより、両方のリージョンのクラスタの最初のピアが解決されます。

2 番目の CNAME レコードは、優先度が最も高い米国および EMEA クラスタの 2 番目のピアに解決されます。クラスタのすべてのピアが含まれるようになるまで、これを繰り返す必要があります。

地理的冗長性を確保するには、バックアップ CNAME エイリアスを作成する必要があります。C：図 4-20 の例では、**backup-alias1.ent-pa.com** が米国ユーザ用の最初の EMEA Expressway ピアと EMEA ユーザ用の米国 Expressway ピアに解決されるため、両方のリージョンの地理的冗長性が確保されます。クラスタのすべてのピアが含まれるようになるまで、このバックアップ エイリアス プロセスを繰り返す必要があります。これらのバックアップ レコードは、DSN SRV が低優先度（この例では 20）に設定されているので、最初のものが応答しない場合にのみ使用されます。

C：図 4-20 は、CNAME レコードに適用される GeoDNS サービスの DNS レコード構造を示しています。

C：図 4-20　　CNAME と地理的冗長性を伴う Geo DNS の DNS レコード構造



Business-to-Business（B2B）コミュニケーション

Business-to-Business（B2B）コミュニケーションの拡張性は、複数の Expressway-C クラスタと Expressway-E クラスタを同じ物理位置にまたは地理的に分散して追加することによって解決できます。

複数の Expressway-C と Expressway-E のペアが展開されている場合は、Unified CM が発信コールを発信側エンドポイントに最も近いエッジ サーバに転送できるため、内部 WAN トラフィックが最低限に抑えられます。加えて、複数のエッジ クライアントが利用されている場合は、Expressway-C が Unified CM クラスタを使用してメッシュ状のトランク構成を形成する必要があります。これにより、地理的に見つけたトラバーサルがいっぱいになった場合または使用できない場合に、追加のアウトバウンド トラバーサル パスを許可することで拡張性と復元力が高まります。

大規模展開では、モバイル & リモート アクセスから分離した Expressway-C と Expressway-E のペア上で Business-to-Business（B2B）コミュニケーションをホストした方が適切な場合があります。これにより、サーバ リソースを外部インターネット通信専用にすることができます。

着信コールに関する留意点

DNS SRV レコードは、SIP と H.323 ent-pa.com ドメインに対して承認された Expressway-E クラスタを特定するために使用されます。重要度と優先度が同じ SRV レコードは、Expressway-E クラスタ ノード全体でコールのバランスを取るために使用されます。

地理的に分散した複数の Expressway-E クラスタ全体で着信コールをスケーリングする場合は、トラフィックのロード バランシングが主要課題になります。Expressway-C と Expressway-E は SIP または H.323 トラフィックのロード バランシングをサポートしません。そのため、DNS クエリに対する応答のロード バランシングがソリューションの重要なスケーリング手段になります。

モバイル & リモート アクセス サービスと同様に、GeoDNS は同じクエリに対する別々の DNS 応答を送信するために使用されます。ネットワーク遅延や地理的位置などのさまざまなメトリックを使用して、DNS 応答で正しい Expressway-E クラスタを指定する必要があります。

GeoDNS は、お客様が選択したメトリックに基づいて、接続先の他のサーバまたはエンドポイントに最適なエッジ Expressway-E を提供する非常に優れた手段です。この場合の応答は、通常、クエリの発行元のサーバに物理的に最も近いエッジに基づいて行われます。このメカニズムは、SRV レコードが異なることを除いて、前述したメカニズムと同じです。たとえば、SIP TLS の SRV レコードは _sips._tcp.ent-pa.com になります。C：図 4-20 は、GeoDNS サービスのセットアップに使用できます。ここで、_collab-edge._tls.ent-pa.com は _sips._tcp.ent-pa.com に置き換えられます。

別のソリューションとしては、宛先のエンドポイントまたはデバイスに最も近いエッジを返すように設計します。この場合は、宛先エンドポイントの位置を検索または確認して、該当するエッジを返す必要があります。このソリューションのメリットは、最短の内部パスをエンドポイントに提供することによって顧客ネットワーク上の帯域幅の使用が最小限に抑えられることです。

これを実現するには、着信側エンドポイントが別のリージョンに属している場合にそのリージョンの Expressway-E にコールを転送するよう Expressway-E を設定できます。

たとえば、EMEA 内の 2 つの Expressway-C クラスタと Expressway-E クラスタと、APJC 内の別の 2 つの Expressway-C クラスタと Expressway-E クラスタについて考えます。EMEA 内の Expressway-C トランク上の Unified CM インバウンド コーリング サーチ スペースには、EMEA 電話機のパーティションは含まれますが、APJC 電話機のパーティションは含まれません。同様に、APJC 内の Expressway-C トランク上のインバウンド コーリング サーチ スペースには、APJC 電話機のパーティションは含まれますが、EMEA 電話機のパーティションは含まれません。EMEA 内のインターネット上のユーザが APJC にある企業エンドポイントにコールした場合は、そのコールが DNS から EMEA Expressway-E クラスタ（Business-to-Business コールのデフォルト）に送信されます。EMEA Expressway-E と Expressway-C はそのコールを宛先に送信しようとしますが、Expressway-C トランクのインバウンド コーリング サーチ スペースがそのコールをブロックします。次に EMEA Expressway-E はそのコールを APJC Expressway E に転送します。今回はコールが宛先に配信されます。これは、APJC Expressway-C のインバウンド コーリング サーチ スペースに APJC エンドポイントのパーティションが含まれているためです。

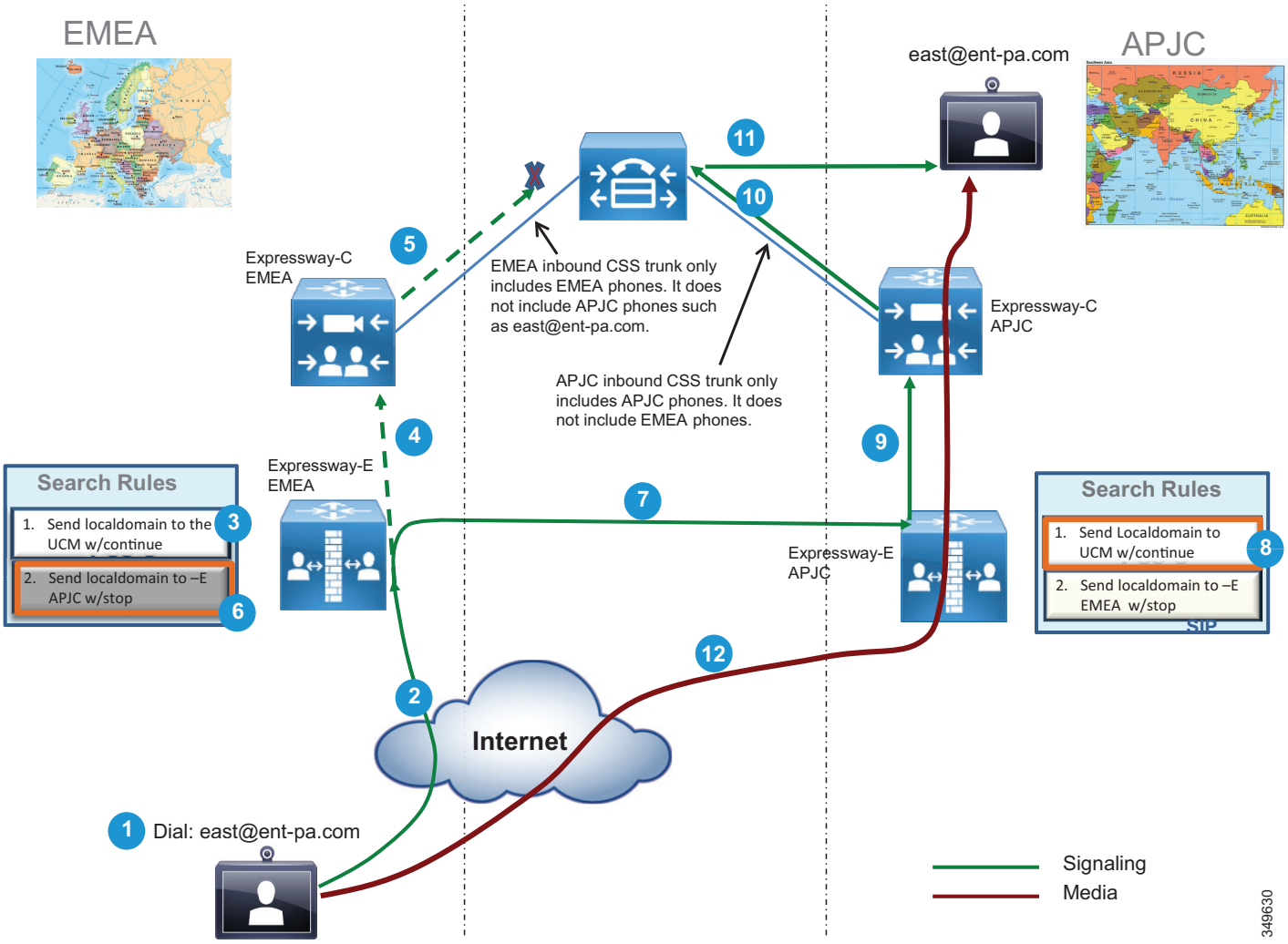
EMEA 内の Expressway-E がシグナリングとメディアのパスからそれ自体を削除できるようにするには、Expressway-E EMEA クラスタ上に TCP/TLS 変換または RTP/SRTP 変換が確実に存在しないようにし、すべての Expressway-C と Expressway-E でコール シグナリング最適化パラメータが確実に [オン（on）] に設定することが重要です。

これは確定的プロセスではないため、Expressway エッジが 3 つ以上の場合は、検索メカニズムに時間がかかりすぎることがあります。したがって、この設定は Expressway エッジが 2 つ以下の場合にお勧めします。

3 つ以上のエッジにスケールするには、Directory Expressway と呼ばれる別のアーキテクチャを展開できます。Directory Expressway アーキテクチャは、プリファード アーキテクチャに含まれません。

C：図 4-21 に、宛先エンドポイントに最も近いエッジの選択を可能にする Expressway エッジ設計を示します。

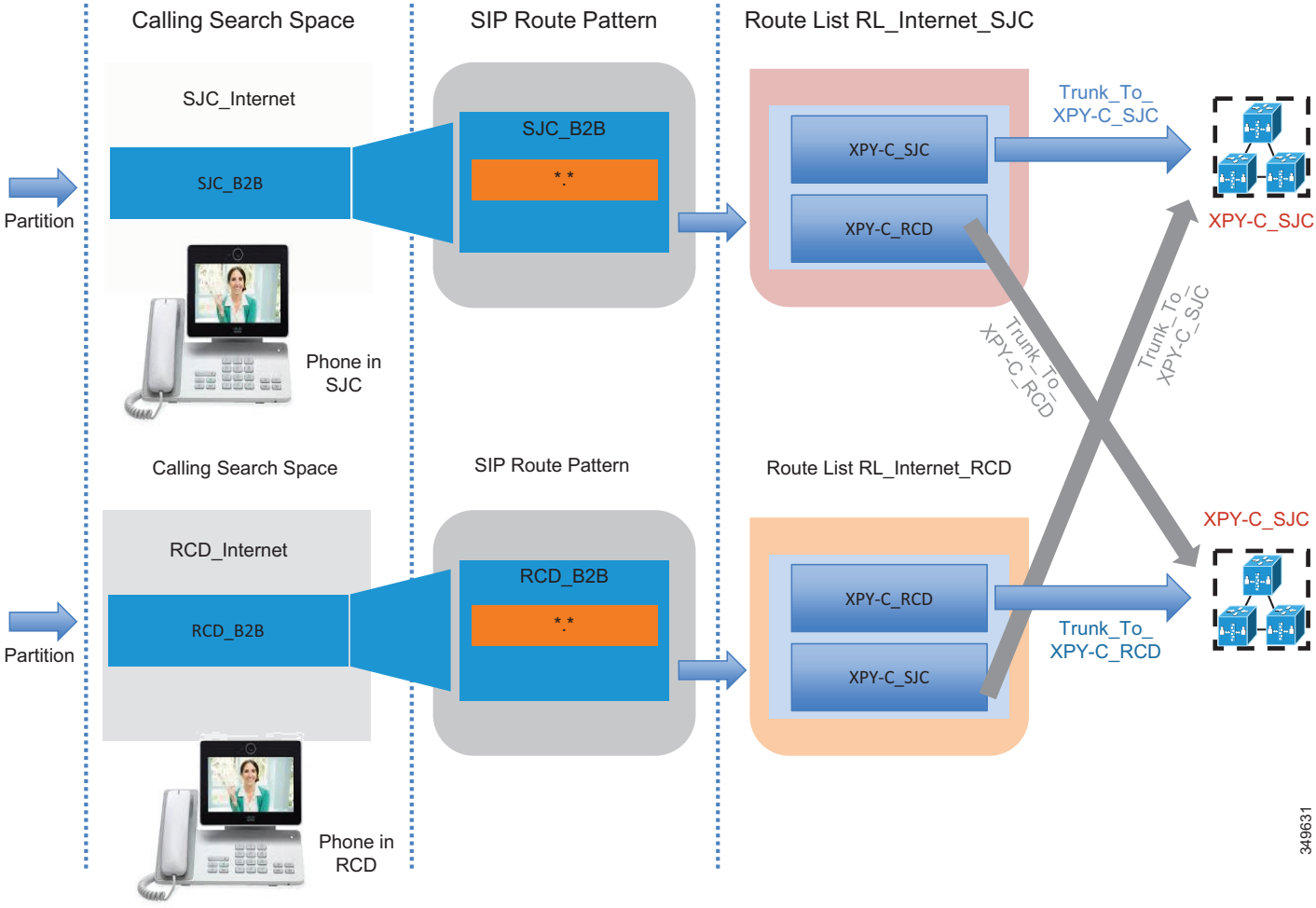
C：図 4-21　　宛先に最も近い Expressway クラスタの選択



発信コールに関する留意点

発信コールは発信側のエンドポイントに最も近い Expressway-C に転送する必要があります。これは、コーリング サーチ スペースやパーティションなどの Cisco Unified CM メカニズムを使用して実現できます。C：図 4-22 に、Unified CM の設定を示します。

C：図 4-22　Unified CM で設定するパーティションとコーリング サーチ スペース



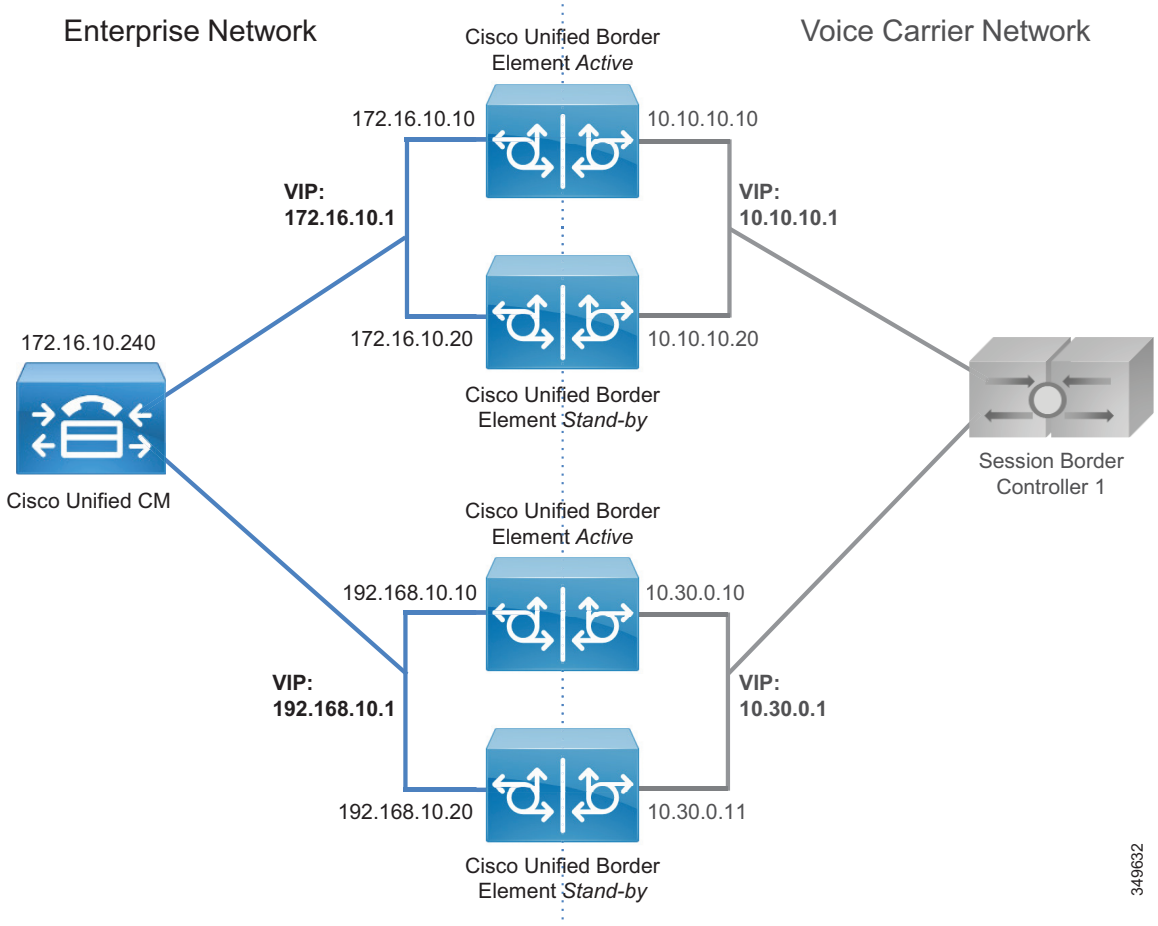
Unified CM ローカル ルート グループ機能は、複数のサイトが複数の Expressway-C クラスタにアクセスする場合にこのソリューションのスケーリングに役立ちます。このメカニズムは、ISDN ゲートウェイや Cisco Unified Border Element 上でも適用されます。詳細については、次のセクションで説明します。設定の詳細は、Cisco Unified Border Element や音声ゲートウェイにも当てはまるため、次の 2 つのセクションで説明します。

Cisco Unified Border Element のスケーリング

プラットフォームあたりのセッション容量については、サイジングの章を参照してください。

複数のデータセンターを展開している場合は、それぞれのデータセンターに Cisco Unified Border Element を展開することができます。この構成はさまざまな用途に使用されます。たとえば、C：図 4-23 に示すようなディザスタ リカバリ アーキテクチャが必要な場合があります。

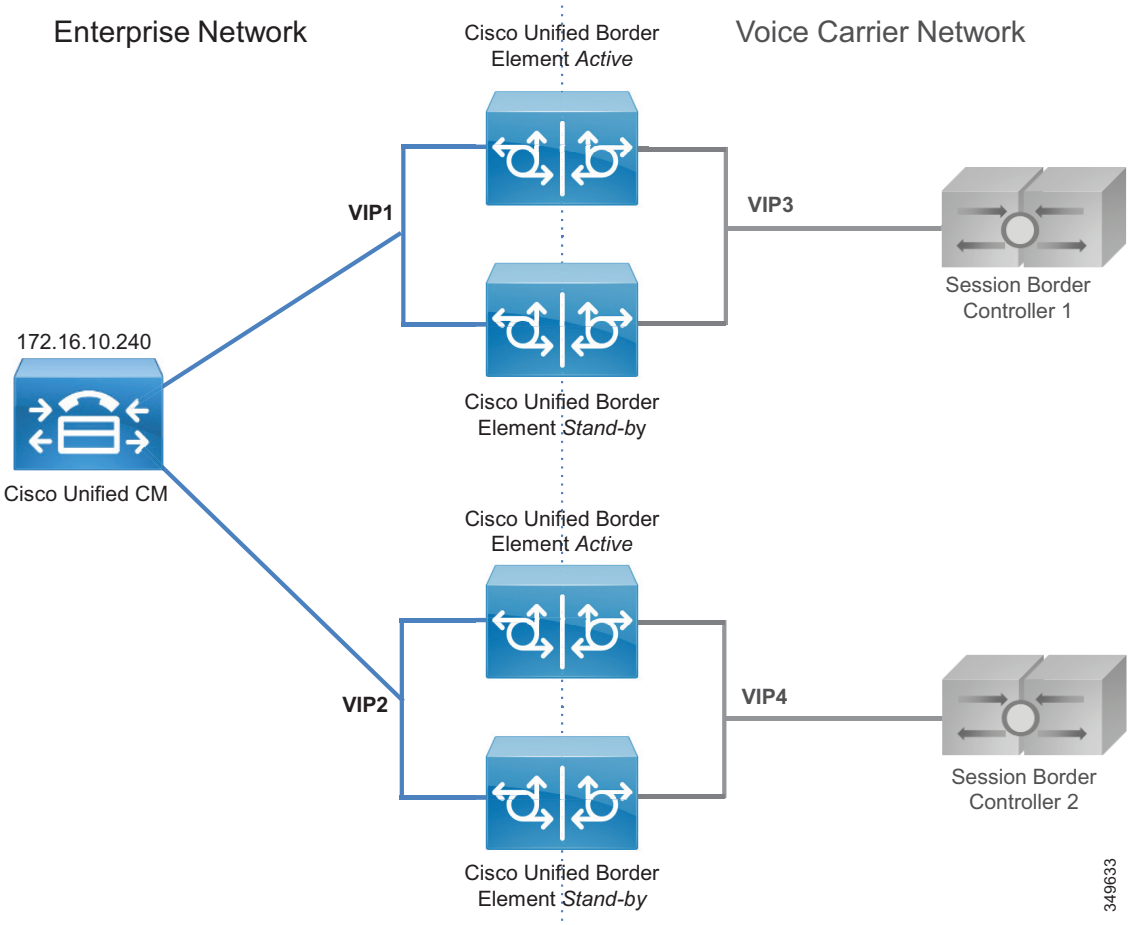
C：図 4-23　　複数の Cisco Unified Border Element



Unified Border Element へのすべてのトランクを同じルート グループ内に含めることができます。これにより、データセンター間にロード バランシングが実現します。データセンター内のアクティブ ルータが故障した場合は、アクティブ コールが保存されます。あるデータセンターが到達不能になった場合、コール要求は残りのデータセンターに送信されます。この場合は、アクティブ コールが破棄されるため、ユーザは手動で回復する必要があります。

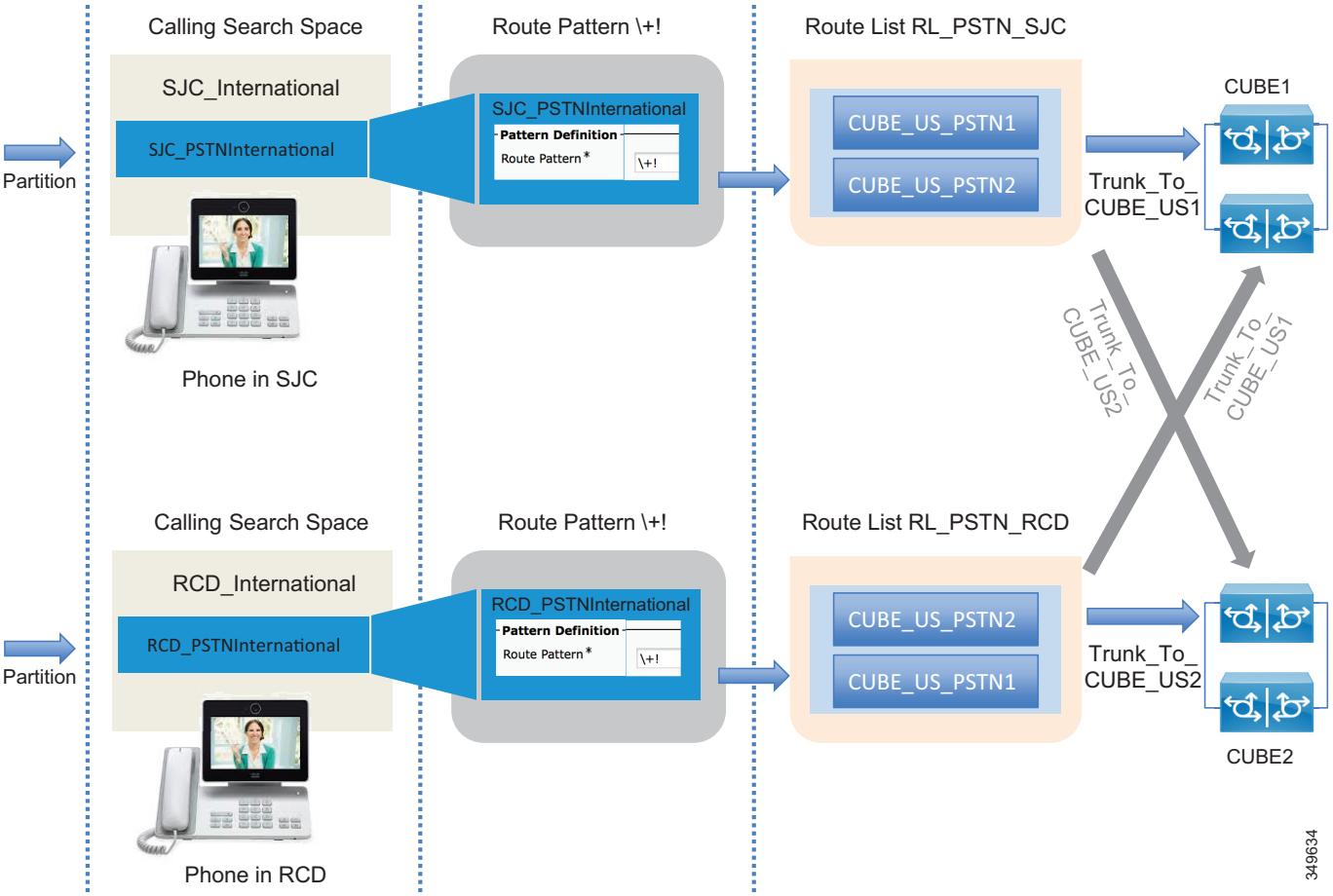
C：図 4-24 に示すように、企業音声ネットワークが広範囲に広がっている場合は、通信事業者からの複数のセッション ボーダー コントローラ（SBC）が使用されます。通信事業者の推奨事項に基づいて、SBC ごとに Cisco Unified Border Element が展開される場合があります。

C：図 4-24　　別々の SBC に接続された複数の Cisco Unified Border Element



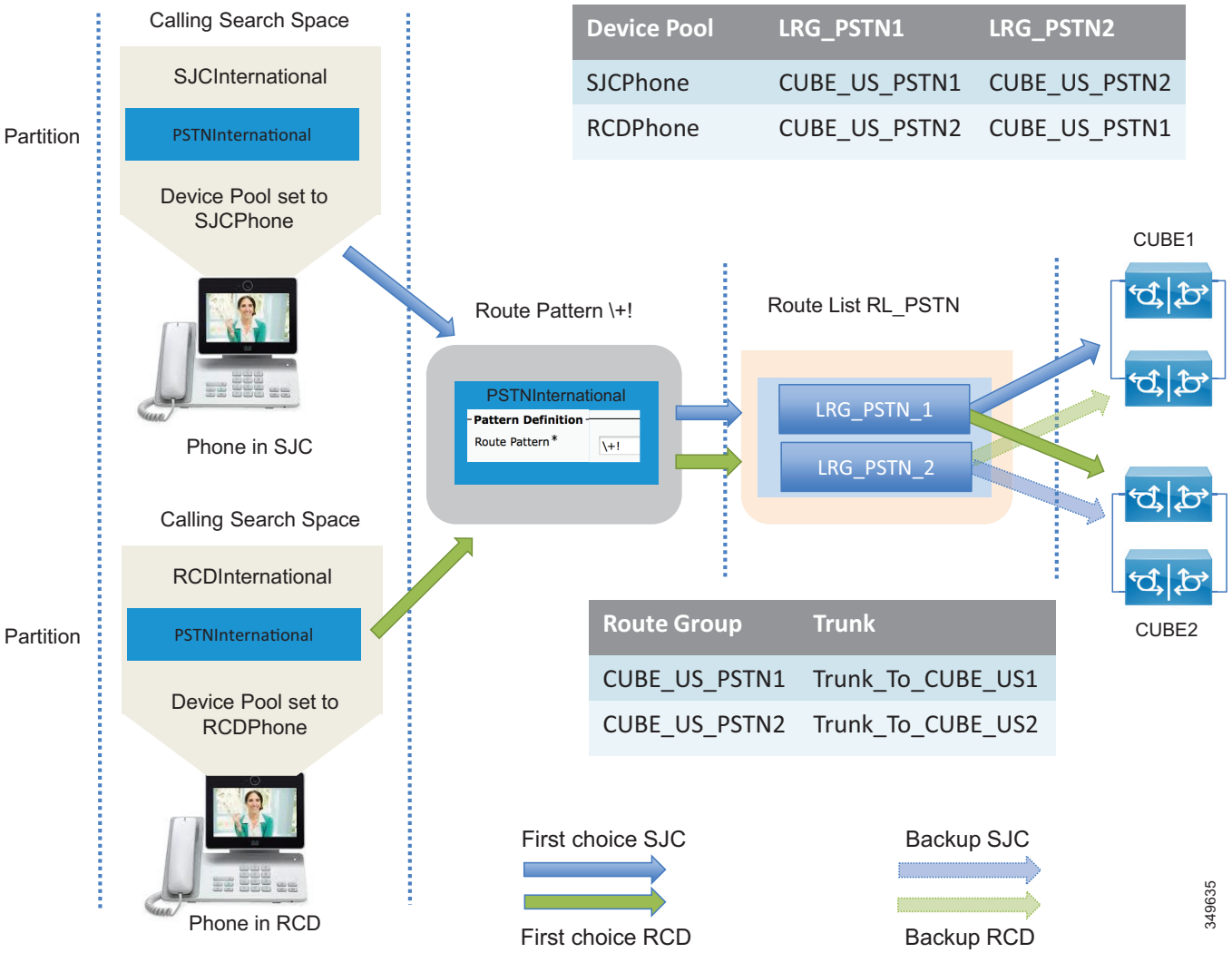
たとえば、US ですでに展開済みのものに加えて、別の Unified Border Element が必要になったとします。Trunk_to_CUBE_US2 という名前の新しいトランクを追加します。C：図 4-25 に、コーリング サーチ スペースとルート パターン間の標準の一対一マッピングに基づく設定を示します。この設定は、Unified Border Elements の数が増えるにつれて、Unified CM リソースに対する影響が大きくなるため、いくつかの制限があります。この設定を C：図 4-25 に示します。C：図 4-26 に示すローカル ルート グループ アプローチと比較してみてください。

C：図 4-25　Cisco Unified Border Element 接続用の Unified CM の設定



同じルート パターン \+! がすべての物理宛先分繰り返され、別々のパーティションに配置されます。元のパーティション PSTNInternational を SJC_PSTNInternational と RCD_PSTNInternational の 2 つに分割する必要があります。ルート パターン \+! を削除して、新しく作成された 2 つのパーティションに移動する必要があります。このアプローチは、サイト数があまり多くない（3 つ以下の）場合に機能します。さらに優れたアプローチは、C：図 4-26 に示すローカル ルート グループの概念を使用したアプローチです。

C：図 4-26　ローカル ルート グループ アプローチを使用した Cisco Unified Border Element 接続用の Unified CM の設定



この場合、デバイス プール SCJPhone の LRG_PSTN1 はルート グループ CUBE_US_PSTN1 と同じに設定されるのに対して、デバイス プール RCDPhone の LRG_PSTN1 はルート グループ CUBE_US_PSTN2 と同一に設定されます。LRG_PSTN2 は、SJC 電話機では CUBE_US_PSTN2 と同じに設定され、RCD 電話機では CUBE_US_PSTN1 と同一に設定されます。このアプローチをお勧めする理由は、新しいパーティションやルート パターンが必要ないうえ、C：図 4-25 に示すアプローチよりはるかにスケーラブルなことです。

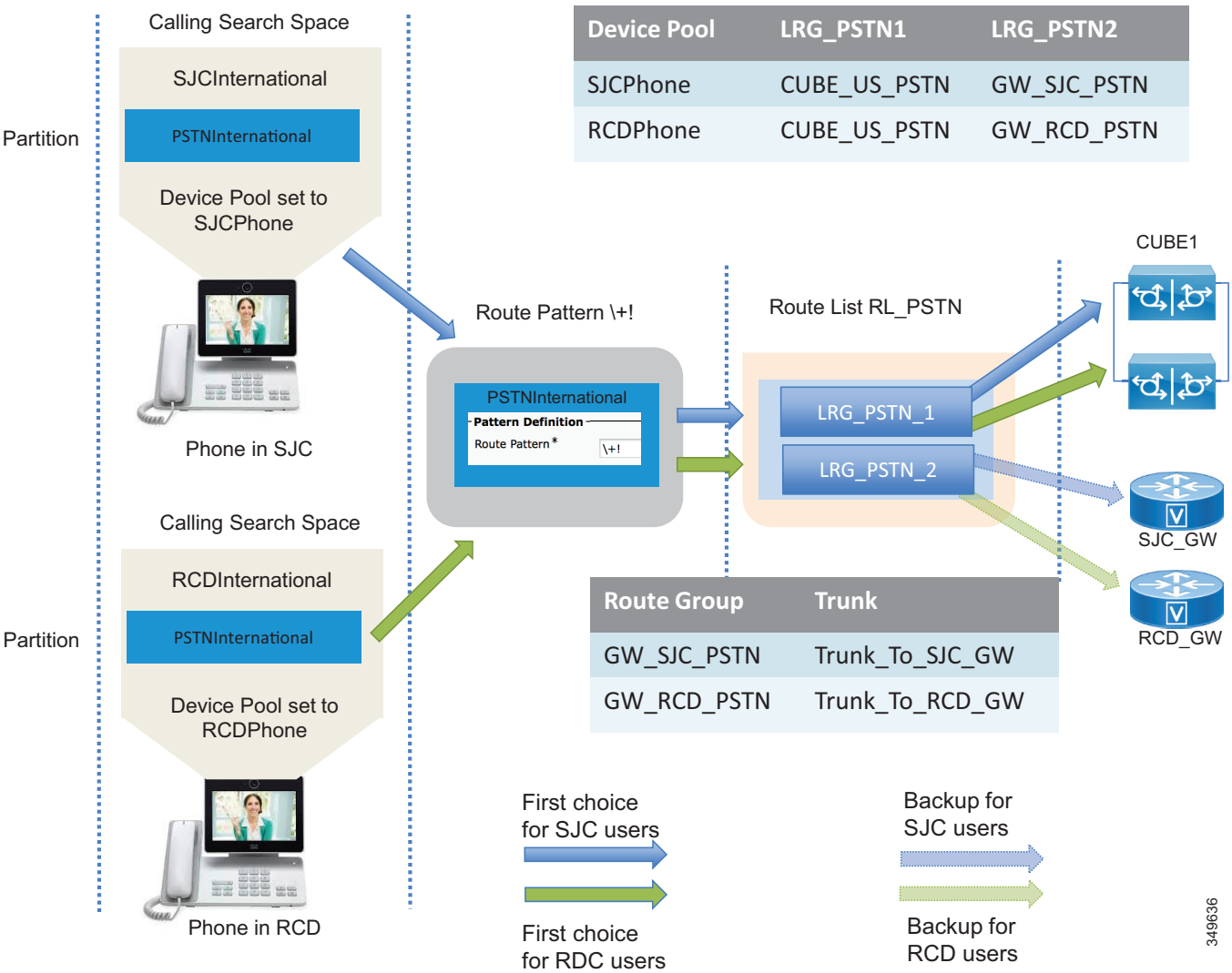
PSTN ソリューションのスケーリング

ローカル PSTN アクセスを提供する分散ゲートウェイは、支店に展開され、バックアップ サービスとして使用されます。

支店の数が多い場合は、Unified CM 内のルート グループとルート リスト設定の構造がうまくスケーリングしません。この展開では、PSTN へのルート パターンをサイトごとにレプリケートする必要のないローカル ルート グループ機能の使用をお勧めします。

以前のセクションで説明した設定は、このシナリオをカバーするため容易に対応できます。必要なことは、C：図 4-27 に示すように、デバイス プロファイル LRG_PSTN1 をルート グループ CUBE_US_PSTN に割り当て、LRG_PSTN2 をそのデバイス プール用のローカル ゲートウェイに対応するルート グループに割り当てることです。

C：図 4-27　ローカル ゲートウェイを使用した集中型 PSTN アクセスに関する設定



コラボレーション エッジの展開プロセス

ここでは、コラボレーション エッジの展開プロセスの概要について説明します。すべての展開ですべてのアクセス手段が必要なわけではないため、コラボレーション エッジの各コンポーネントは個別に取り扱われます。たとえば、ある会社は PSTN しか所有していないが、別の会社が、特定のローカル サイトで IP PSTN のローカル バックアップとして PSTN を使用し、インターネット エッジを展開している場合があります。

コラボレーション エッジ コンポーネントは次の順序で展開する必要があります。

- Expressway-C と Expressway-E を展開する
- Cisco Unified Border Element を展開する
- Cisco Voice Gateway を展開する

Expressway-C と Expressway-E を展開する

このセクションでは、Expressway-C と Expressway-E をインストールして展開するのに必要なタスクの概要を示します。このタスクを次の順序で実行する必要があります。

1. Expressway-C と Expressway-E の OVA テンプレートをダウンロードして展開し、Expressway ソフトウェアをインストールします。アプライアンス モデルが使用されている場合、OVA テンプレートと Expressway ソフトウェアをダウンロードしてインストールする必要はありません。
2. DNS と NTP を含むネットワークのインターフェイスと設定、およびシステムのホスト名とドメイン名を構成します。Expressway-E は 2 つの LAN インターフェイスを備えています。外部インターフェイスの IP アドレスを静的に変換しなければならない場合は、変換後のインターフェイスの IP アドレスを設定する必要があります。Expressway-E はペイロード参照内のパブリック IP アドレスを使用します。2 つの LAN インターフェイスを備えた Expressway-E 用のスタティック ルーティングを設定します。Expressway-C インタ フェースが Expressway-E とは別のネットワーク上に存在し、Expressway-C インターフェイスが NAT によって変換されない場合は、スタティック ルーティングが必要です。これにより、Expressway-C が Expressway-E と同じネットワークに存在するかのように表されます。単一の Expressway-E インターフェイスもサポートされますが、このプリファード アーキテクチャのドキュメントでは説明しません。
3. クラスタリングを設定します。

モバイルおよびリモート アクセスを展開する

1. Unified Communications モードを [モバイルおよびリモート アクセス（Mobile and remote access）] に設定することによって、モバイルおよびリモート アクセスを有効にします。
2. ユニファイド コミュニケーション モードを [モバイルおよびリモート アクセス（Mobile and remote access）] に設定した後、Expressway-C 上で、C：表 4-6 に示すように [MRA アクセス制御（MRA Access Control）] 設定を指定します。

C：表 4-6　Expressway-C モバイルおよびリモート アクセス（MRA）のアクセス制御設定

パラメータ	設定	説明
認証パス（Authentication path）	UCM/LDAP 基本認証	MRA 接続エンドポイントの認証パスを決定します。SSO を使用している場合は、他の設定のいずれかを選択します。
OAuth トークンによる承認（更新あり）（Authorize by OAuth token with refresh）	オン	Jabber MRA 接続に関する OAuth 2 認証フローを有効にします。
ユーザ クレデンシャルによる承認（Authorize by user credential）	オン	ハードウェア エンドポイント MRA 接続の認証を有効にします。
内部認証の可用性の確認（Check for internal authentication availability）	いいえ（No）	ホーム クラスタ認証モードを問い合わせないようにシステムを設定します。この展開内のすべてのクラスタが同じ認証方式を使用します。

3。 モバイルおよびリモート アクセスが有効にするドメインを選択します。[Unified CM 上の SIP 登録およびプロビジョニング（SIP registration and provisioning on Unified CM）]、[Unified CM 上の IM and Presence サービス（IM and Presence service on Unified CM）]、および [会社間フェデレーションの場合の XMPP フェデレーション（XMPP federation if inter-company federation）] をオンにします。

4。 Expressway-C と Expressway-E に CA 証明書をアップロードします。[TLS 検証モード（TLS verify mode）] が [オン（on）]（推奨）になっている場合は、Unified CM クラスタと IM and Presence クラスタを検出するためにこの証明書が必要です。このように、Expressway-C は、証明書をチェックすることによって、クラスタ サーバのアイデンティティを検証します。

5。 各クラスタのパブリッシャを設定することによって、Unified CM サーバと IM and Presence サーバを検出します。

6。 Expressway-C と Expressway-E の両方に証明書をインストールします。どちらのタイプの Expressway ノードも、その後 CA によって署名される、証明書署名要求（CSR）を生成できます。内部 CA を使用している場合は、CSR をその CA で署名する必要があります。Expressway-C 証明書を内部 CA によって署名することができますが、Expressway-E ではパブリック CA によって署名される証明書が必要です。その後で、署名した証明書を Expressway-C と Expressway-E にアップロードする必要があります。

7。 Expressway-C と Expressway-E の間の Unified Communication トラバーサル ゾーンを設定して、Cisco Unified CM へのプロキシ登録を許可します。

8。 すべてが正しくセットアップされていることを確認するために、Unified Communications のステータスをチェックします。

注
- この設定によって、モバイルおよびリモート アクセスが有効になります。Business-to-Business（B2B）では追加の設定が必要です。
- 上記設定は、Expressway-C と Expressway-E 上だけで完結します。
- これらのステップは、Unified CM への TCP/RTP 接続（TLS/SRTP は表示されていない）の場合に必要です

Business-to-Business（B2B）コミュニケーションを展開する

ここでは、Business-to-Business（B2B）コミュニケーションのセットアップに必要な追加のステップの概要について説明します。

1. Expressway-C と Expressway-E の両方で NTP、DNS、およびシステム名を含む基本的なレイヤ 3 設定を構成します。
2. Expressway-E 上でトラフィック ルーティングに必要な IP ルートを含む NAT 設定をセットアップします。
3. Expressway-E を DMZ に配置する前に、外部ファイアウォールが Expressway-E 宛てのすべてのトラフィックをブロックするように設定されていることを確認します。
4. Expressway-C と Expressway-E の両方のローカルまたはリモート認証を含む管理アクセス ポリシーを設定します。
5. 該当する DNS サーバ内の DNS A レコードを各サーバの FQDN が解決できるように設定します。
6. Expressway-C からのトラバーサル クライアント接続を認証する目的で Expressway-E 内のローカル認証クレデンシャルをセットアップします。
7. Expressway-E 上で SIP 専用のトラバーサル サーバ ゾーンをセットアップします。
8. Expressway-E 上のインターワーキングを [オン（On）] に設定します。これにより、Expressway-E で H.323 コールを送受信して、それらをネットワークのエッジで SIP に接続できるようになるため、企業内部で単一のプロトコルが維持されます。
9. Expressway-C 上で SIP 専用のトラバーサル クライアント ゾーンをセットアップします。
10. Expressway-E の FQDN を使用してトラバーサル リンクを有効にして PKI の使用を可能にします。
11. 外部 DNS ゾーンを Business-to-Business（B2B）コミュニケーションのアウトバウンド ドメイン解決用に設定します。
12. Expressway-E 上でビデオ、音声、IP PSTN ゲートウェイなどの保護されたリソースへのアクセスを制限する基本的な CPL ルールを導入します。
13. Expressway-C と Expressway-E が権限を与えられたドメインをセットアップします。
14. Expressway-C と Expressway-E 上で事前検索変換、検索ルール、DNS 検索ルール、および外部 IP アドレス ルーティングを使用してダイヤル プランをセットアップします。
15. Expressway-C 上で Unified CM までの SIP ネイバー ゾーンを設定します。
16. Unified CM 上の SIP トランクが Expressway-C と通信するように設定します。

Cisco Unified Border Element を展開する

ここでは、ボックスツーボックス冗長性を備えた Cisco Unified Border Element を展開するためのプロセスの概要について説明します。ボックスツーボックス冗長性は両方の Unified Border Element ルータ上で設定する必要があり、設定内容は両方とも同じです。アクティブ Unified Border Element から スタンバイ Unified Border Element に設定をコピーして貼り付けることができます。

1. ネットワーク設定（アクティブ Unified Border Element とスタンバイ Unified Border Element の両方の 2 つのイーサネット インターフェイス（LAN 向けと WAN 向け）と IP ルーティング）を構成します。

2。 両方のルータ上の Unified Border Element を SIP 間コール、FAX のリレーまたはパススルー、プライバシー ヘッダーとしての発信元 ID 処理、およびアーリーオファーの強制に対して有効にします。Unified CM がベスト エフォートアーリーオファー専用に設定されているため、Unified Border Element 上でこの機能を有効にすることをお勧めします。新しい展開ではアーリーオファーのみがエンドポイントから送信されますが、代わりにディレイドオファーが送信される旧式のシスコ デバイスが関与している場合もあります。このマニュアルではこのようなケースを取り上げませんが、Cisco Unified Border Element 上でアーリーオファーを強制することをお勧めします。

3。 ボックスツーボックス冗長性を有効にして、アクティブ ルータとスタンバイ ルータの LAN インターフェイスと WAN インターフェイスの両方で HSRP をグローバルに設定します。

4。 音声コーデック優先順位を設定します（音声コーデックがネゴシエート可能であり、Unified CM または通信事業者ソフト スイッチによって強制されない場合）。

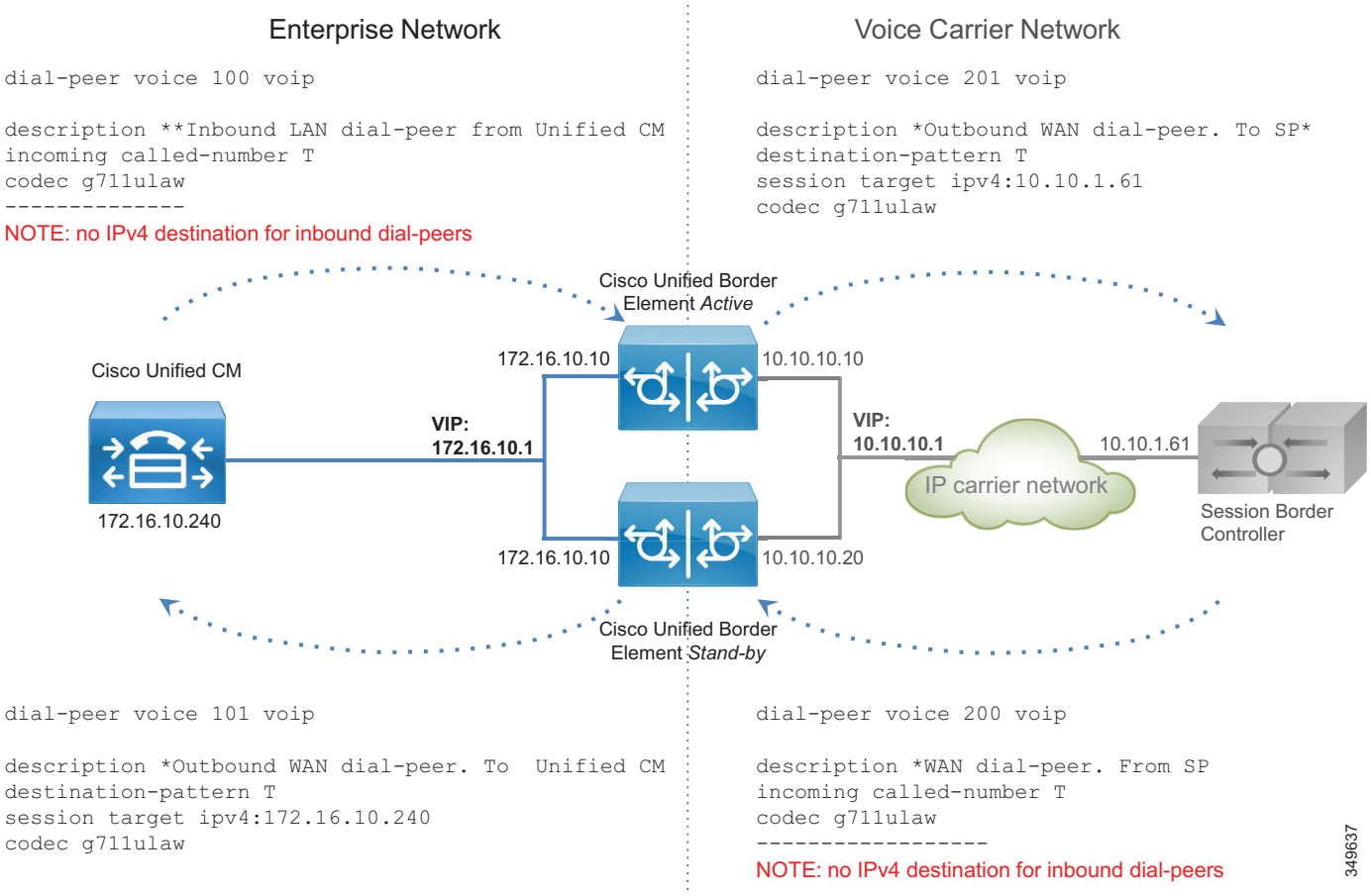
5。 保留音を設定します。

6。 ダイヤルピアを設定します。ダイヤルピアはコール レッグに関連付けられており、インバウンドまたはアウトバウンドで照合できます。たとえば、Unified CM からの着信コールはインバウンド ダイヤルピア（着信コール レッグに対応する）によって照合されます。別のコール レッグが電気通信業者のセッション ボーダー コントローラ（SBC）宛てに Cisco Unified Border Element（CUBE）によって生成され、別のダイヤル ピアに対して照合されます。同じダイヤル ピアでインバウンド コールまたはアウトバウンド コールを照合できますが、各ダイヤル ピアで特定のコール レッグを照合することをお勧めします。この提案に従うと、次の 4 種類のダイヤルピアが用意されます。Unified CM から CUBE へのインバウンド ダイヤルピア、CUBE から SBC へのアウトバウンド ダイヤルピア、SBC から CUBE へのインバウンド ダイヤルピア、および CUBE から Unified CM へのアウトバウンド ダイヤルピア。ダイヤルピアは、発信側または着信側の番号またはパターンに照らして照合できます。また、ダイヤルピアは、単一のコーデックを強制することも、ステップ 4 で設定したコーデックのリストをネゴシエートすることもできます。**incoming called-number** コマンドはダイヤルピア インバウンドのみを作成します。

   インバウンド ダイヤルピアにはターゲットが関連付けられませんが、アウトバウンド ダイヤルピアには Unified CM または通信事業者の SBC がターゲットとして定義されます。

   外部宛先へのコールは汎用パターンと一致するため、Unified Border Element 上のダイヤルピア設定がエラーの原因になる場合があります。たとえば、C：図 4-28 では、発信コールがダイヤルピア 201 と 101 の両方と一致するため、ルーティングが正しく機能しません。

C：図 4-28　Cisco Unified Border Element 上でのインバウンド ダイヤルピアとアウトバウンド ダイヤルピアの設定



C：図 4-29 の変数 T は任意の長さの任意の数値文字列を表します。これは、Unified CM からのコールが世界中の任意の宛先に送信される可能性があるためです。最も近い一致が役に立つ場合もありますが、Unified Border Element が一元管理されており、複数の場所にサービスを提供している場合は、「宛先パターン」設定内で可能性のあるすべての宛先を列挙するのは実用的ではありません。この制限を克服し、ルーティング プロセスを簡略化して応答性を高めるために、次の追加の設定を実行します。

a。 アウトバウンド ダイヤルピア内のサーバ グループ：サーバ グループがダイヤルピア内の宛先として設定され、ラウンドロビン アルゴリズムが選択されている場合は、Unified Border Element は複数のサーバで負荷を共有します。

```
voice class server-group 1
    ipv4 172.16.10.240
    ipv4 172.16.10.241
    ipv4 172.16.10.242
    ipv4 172.16.10.243
    ipv4 172.16.10.244
    hunt-scheme round-robin
```

b。 SIP Out-of-Dialog OPTIONS Ping：サーバが稼働中の ping 間隔やサーバがダウン中の間隔（この例ではそれぞれ 30 秒と 60 秒に設定）などのさまざまなパラメータを設定できます。

```
voice class sip-options-keepalive 171
    transport tcp
    sip-profile 100
    down-interval 30
    up-interval 60
    retry 5
    description Target Unified CM
```

この方法では、Unified CM へのアウトバウンド ダイヤルピアが次のようになります。

```
dial-peer voice 101 voip
    description *Outbound WAN dial-peer. ToUnified CM
    destination-pattern T
    session protocol sipv2
    session server-group 1
    voice-class sip options-keepalive profile 171
    codec g711ulaw
```

c。 通信事業者への発信コール レッグがアウトバウンド ダイヤルピアによって照合されます。

```
dial-peer voice 201 voip
description *Outbound WAN dial-peer. To SP*
destination-pattern T
session target ipv4:10.10.1.61
 codec g711ulaw
```

d。 先行する「*」は、発信コール（Unified Border Element から見れば着信コール）で Unified CM から送信されます。これにより、ルータはコールの方向を識別できます。この記号はコールが IP PSTN に到達する前に除去する必要があります。また、設定されたダイヤル プランに基づいて、発信者番号を 「+」を使って正規化する必要があります。ルール 2 は「+」を前に付加し、発信者番号に適用されますが、ルール 1 は先行する「*」を「+」に置き換えます。これらのルールは着信者番号にも適用されます。そのため、着信者番号用と発信者番号用の 2 つのルールを作成できます。ただし、着信者番号は常に最初のルールと照合され、発信者番号は常に 2 つ目のルールと照合されるため、単一の音声トランスレーション ルールを使用できます。これは、インバウンド ダイヤルピア上で設定されます。

発信コール レッグ（ダイヤルピア）は **dpg** コマンド経由でインバウンド ダイヤルピアにバインドされるため、「*」が先行するコールが受信された場合は、SBC に対向しているダイヤルピアに送信され、Cisco Unified CM 向けのダイヤルピアには送信されません。

```
voice class dpg 201
    dial-peer 201

voice translation-rule 2
    ??? 1 /^\*/ /+/
    ???2 // /+/
voice translation-profile SIPtoE164
    translate called 2
    translate calling 2
dial-peer voice 100 voip
    translation-profile outgoing SIPtoE164
    incoming called-number *T
destination dpg 201
    codec g711
```

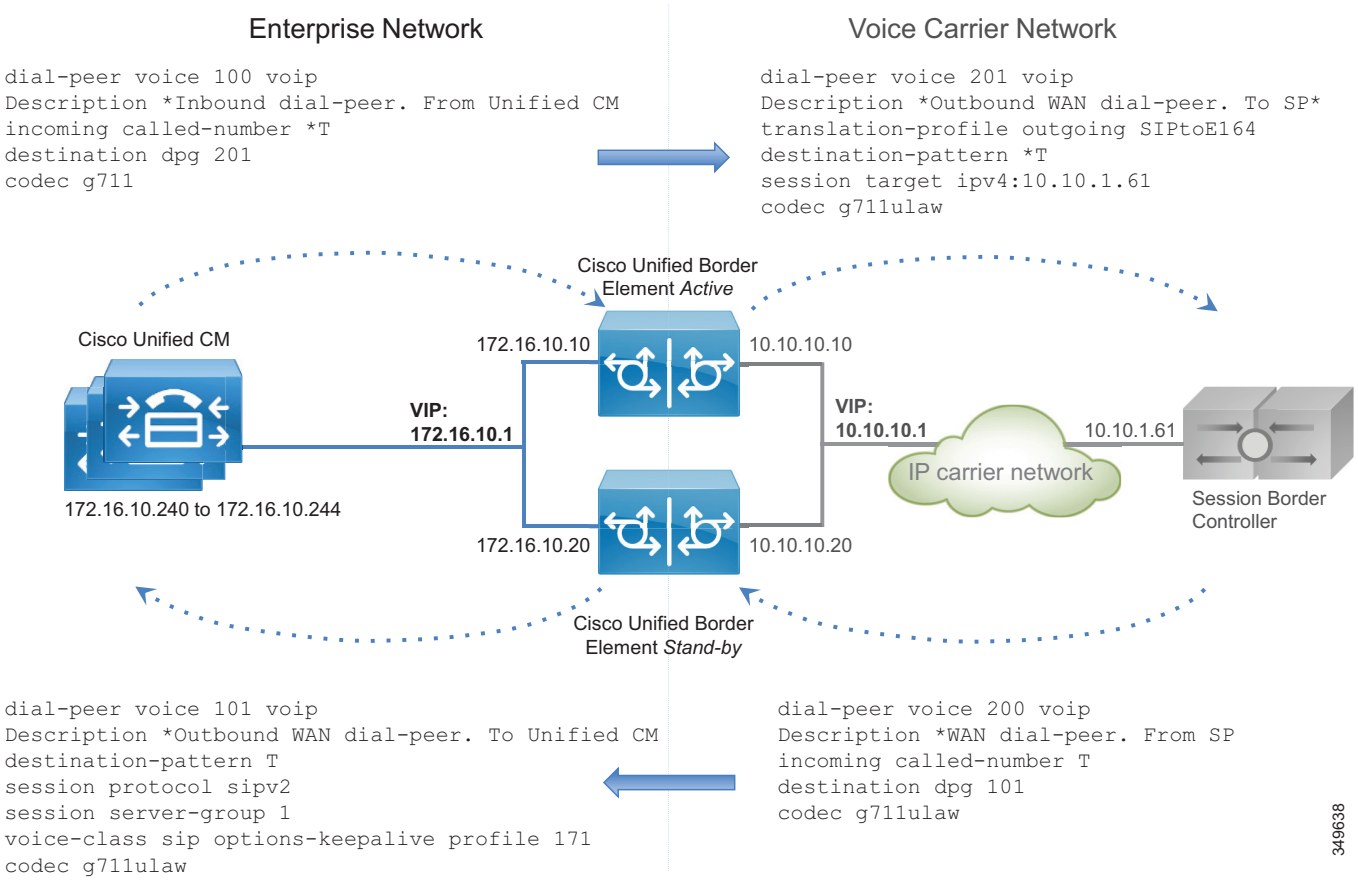
ダイヤルピア 200 はダイヤルピア 101 にもバインドする必要があります。

```
voice class dpg 101
    dial-peer 101

dial-peer voice 200 voip
    description *WAN dial-peer. From SP
    incoming called-number T
    destination dpg 101
    codec g711ulaw
```

C：図 4-29 でこれについて説明します。

C：図 4-29　　Cisco Unified Border Element のダイヤルピア設定



コール レッグが Unified CM から到着した場合は、「*」が先行する Unified Border Element にヒットするため、ダイヤルピア 100 と一致します。その後で、このコールは、インバウンド ダイヤルピア宛先としてアウトバウンド ダイヤルピア グループを使用してダイヤルピア 200 に送信されます。ダイヤルピア 200 は先行する「*」を除外し、そのコールを PSTN に送信します。この機能を使用しない場合は、ダイヤルピア 201 も一致するため、ルーティング エラーが発生することに注意してください。

コール レッグが SBC から到着した場合は、ダイヤルピア 201、101、および 200 と一致する可能性があります。ただし、「着信者番号」の方が「宛先パターン」より優先されるため、ダイヤルピア 200 が一致します。また、ダイヤルピア 200 がダイヤルピア 101 にリンクされているため、コールは正しく宛先にルーティングされます。

7。 必要に応じて、トランスコーディングを設定します。トランスコーディングには専用のハードウェア リソース（DSP）が必要なことを覚えておいてください。

Unified CM 上で次の設定作業を実行します。

1。 コール制御の章で指定されているように、各 Unified Border Element にベスト エフォート早期オファー トランクを設定します。

2。 ルート グループ CUBE_US_PSTN を設定し、メンバーとして Unified Border Element トランクを追加します。

3。 ローカル ルート グループ LRG_PSTN1 を設定します。

4。 デフォルト ローカル ルート グループとルート グループ LRG_PSTN1 を含むルート リストを設定します。

5。 デバイス プールごとに、LRG_PSTN1 を CUBE_US_PSTN に設定します。

Cisco Voice Gateway を展開する

PSTN インターフェイスは Cisco ISR ルータや ASR ルータなどのさまざまなルータで使用できます。PSTN インターフェイスには、アナログ、BRI、および PRI ISDN 音声カードが含まれます。アナログ インターフェイスは、ほとんど、FAX マシンとアナログ電話機に接続するために使用されます。

ISDN 音声インターフェイスを備えた PSTN ゲートウェイを設定するには、次の作業を実行します。

1。 ルータ上でネットワーク設定とルーティングを構成します。

2。 ISDN インターフェイスをアクティブ化します。

3。 通信事業者の要件に基づいて、ユーザ側の ISDN パラメータ、スイッチタイプ、フレーミング、および回線コードを設定します。

4。 ダイヤルピアを設定します。

ダイヤルピア ロジックは IP PSTN や Unified Border Element 用のものと同じですが、この場合は、「voip」ダイヤルピアに加えて、音声ゲートウェイには PSTN 向けの「pots」ダイヤルピアもあります。

FAX マシンなどのアナログ装置が存在する場合は、アナログ インターフェイスを介してルータに接続できます。

ルータがアナログ FAX 相互接続専用に使用されていて、PSTN インターフェイスが別のルータに接続されている場合は、T.38 FAX リレーを設定できます。これは、特に PSTN ゲートウェイへのパスが WAN をトラバースする場合に、このリレーがより高い復元力を示すためです。

ダイヤルピア設定は IP PSTN や Unified Border Element の設定と異なります。ゲートウェイは特定の場所に展開され、その場所の電話機を制御するため、パターン宛先は +14085554XXX のようによく見る形式になります。

一方、着信 PSTN コールのアドレスはプラン、タイプ、および番号で構成されます。プランとタイプは SIP でサポートされておらず、通信事業者に基づくため、コールは別のプランとタイプを使用してゲートウェイに到達する可能性があります。たとえば、ドイツの同じエリア コード 6100 内のトランク上の E.164 宛先 4961007739764 へのコールの場合は、出力 ISDN SETUP メッセージ内の着信者番号（プラン / タイプ / 番号）が ISDN/national/61007739764、ISDN/subscriber/7739764、または unknown/unknown/061007739764 として送信されます。

プラン / タイプに基づいて番号が変化するため、ダイヤルピアが一致しない場合があります。そのため、プラン / タイプを unknown/unknown に強制する必要があります。この方法では、完全な E164 番号が宛先に開示されます。ダイヤルピア構造は、コール制御の章で詳しく説明されており、ここでは一貫性を保つために参照されています。

アウトバウンド ダイヤルピアの場合は、次のルールによって、発信者番号がプラン「unknown」とタイプ「unknown」に変換され、着信者番号が先行する「*」を使って +E.164 番号に変換されます。

```
voice translation-rule 1
       rule 1 /^\*/ // type any unknown plan any unknown
       rule 2 // // type any unknown plan any unknown
voice translation-profile ISDNunknown
       translate called 1
translate calling 1
dial-peer voice 1 pots
       translation-profile outgoing ISDNunknown
```

インバウンド ダイヤルピアの場合は、発信者情報にタイプが 「national」の 10 桁の数字が含まれていれば（および米国を示す国番号「1」が含まれていなければ）、コールは「+1」が先行する +E.164 番号に正しく変換されます。「unknown」の場合は、以降のルールが一致しません。

着信者番号が海外の宛先から送られてきたため国番号が含まれており、E.164 形式だった場合は、ルール 2 によって先行する「+」が付加されます。

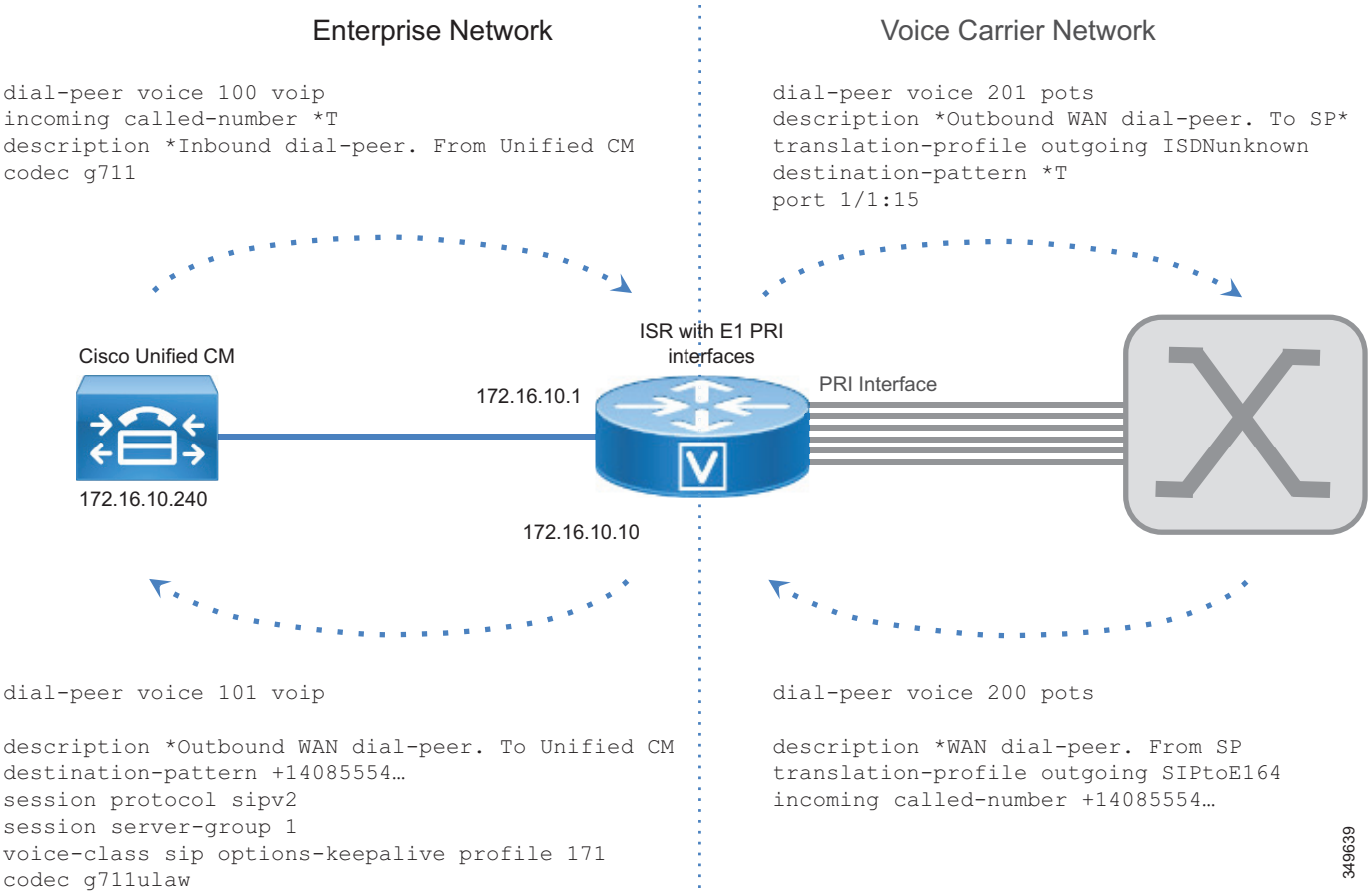
ただし、ISDN セットアップはホップバイホップのため、タイプが「national」のコールはそれほど多くないことが予想されます。これは、最近のスイッチが強制的にタイプを「national」にしているためです。いずれの場合も、次のルールによって、発信者番号と着信者番号が正しく正規化されます。

```
voice translation-rule 3
    rule 1 /^\(.+\)$/ /+1\1/ type national unknown plan any unknown
    rule 2 /^\(.+\)$/ /+\1/ type international unknown plan any unknown
voice translation-profile ISDNtoE164
    translate called 3
    translate calling 3

dial-peer voice 1 pots
    translation-profile incoming ISDNtoE164
```

C：図 4-30 に、G.711 のダイヤルピア設定と E1 PRI インターフェイスを示します。

C：図 4-30　　音声ゲートウェイのダイヤルピア設定



Unified CM 上で次の設定作業を実行します。

1. 各ゲートウェイのベスト エフォート早期オファー トランク（Trunk_to_SiteID_GW、SiteID は場所を識別する変数）を設定します。
2. ルート グループ LRG_PSTN1 を設定して、メンバーとしてゲートウェイ トランクを含めます。
3. ローカル ルート グループ LRG_PSTN1 を設定します。
4. デフォルト ローカル ルート グループと LRG_PSTN1 を含むルート リストを設定します。
5. デバイス プールごとに、LRG_PSTN1 を Trunk_to_SiteID_GW に設定します。この設定では、推奨されているように、サイトごとにデバイス プール SiteIDPhone が存在することを想定しています。

ローカル ルート グループ設定を使用することによって、PSTN アクセスの認識が容易になります。たとえば、Unified Border Element を PSTN への集中型アクセスに使用し、ローカル PSTN 接続をバックアップとして使用することができます。この場合は、デバイス プールによって Unified Border Element ルート グループが LRG_PSTN1 に指定され、LRG_PSTN2 にローカル ゲートウェイへのトランク（Trunk_to_SiteID_GW）が含まれます。