ICE メディアパスの最適化

ICE メディアパスの最適化

X12.5 から、Interactive Connectivity Establishment （ICE）Media Path Optimization がサポートされます。この機能により、MRA エンドポイントのメディアパスが最適化され、MRA に登録されたエンドポイントがエンドポイント間でメディアを直接渡すことができるため、WAN と Expressway サーバーをバイパスできます。

この機能は、ICE プロトコル（RFC 5245）を使用します。ICE に関する背景情報は、https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-maintenance-guides-list.html にある『*Cisco Expressway* 管理者ガイド』の「*ICE* と *TURN* サービスについて」項を参照してください。

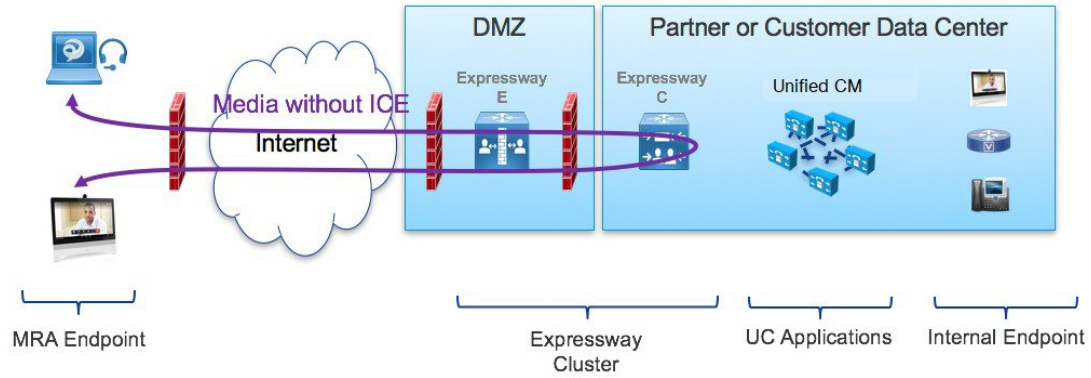
ICE の仕組み

Cisco Expressway X12.5 以前は、ICE は ICE エンドポイントの 1 つとして Cisco Expressway-C B2BUA のみサポートされていました。B2BUA がエンドポイントとして機能する場合、ICE 候補はエンドポイントと B2BUA の間でネゴシエートされます。したがって、メディアは常に Cisco Expressway-E と Cisco Expressway-C を介してトラバースします。

次の図は、メディアパスを最適化するために ICE を使用しない MRA コールを示しています。メディアは、Cisco Expressway-E と Cisco Expressway-C の両方を通過します。

ICE メディアパスの最適化

図 *1 : ICE* メディアパス最適化を使用しない *MRA* コールフロー



Cisco Expressway X12.5 で導入された ICE Media Path Optimization を使用すると、各エンドポイントは、SIP シグナリングをトラバースするゾーンを介して、ICE 候補を他のエンドポイントに渡すことができます。その結果、エンドポイントは ICE プロトコルを使用して、メディアの最適なパスをネゴシエートします。最適なパスは、次のいずれかです。

- **ホストアドレス**—NAT デバイスの背後にあるエンドポイントのホスト IP アドレスを表します。
- **サーバー再帰アドレス**—NAT デバイス上のエンドポイントのパブリックにアクセス可能なアドレスを表します。
- **リレーアドレス**—TURN サーバーで構成されたエンドポイントのリレーアドレスを表します。

すべての ICE コールでは、最初にメディアが Cisco Expressway-E と Cisco Expressway-C を通過し、ネゴシエートされた ICE 候補タイプに応じてメディアパスを切り替えます。これにより、エンドポイントが ICE に対応していない場合でも、 Cisco Expressway は、従来のトラバーサルパスを使用して、中断することなくメディアを渡すことができます。

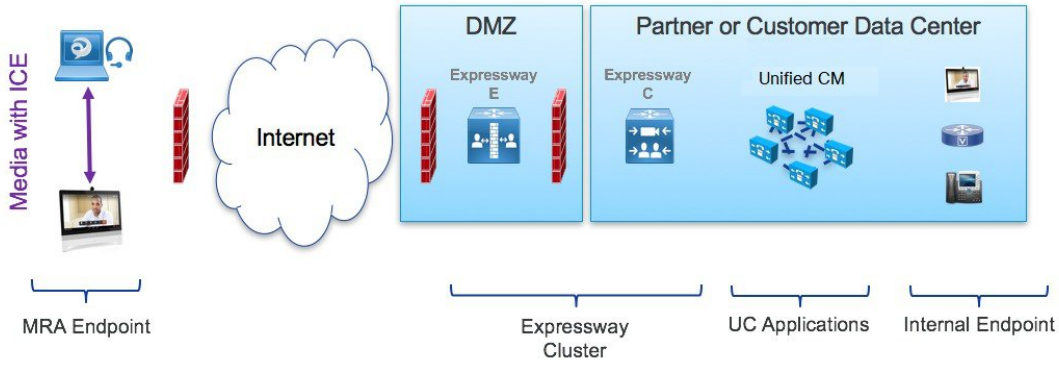
次のセクションでは、3 つの ICE 候補のそれぞれの MRA メディアパスを示します。

ホストアドレスを使用した ICE での MRA コールフロー

次の図は、メディアパスを確立するためにホストアドレスが使用される ICE を使用した MRA コールを示しています。エンドポイントは、ファイアウォールのない同じネットワーク内に存在するため、メディアはホストアドレスを使用してエンドポイント間を直接通過します。

ICE メディアパスの最適化

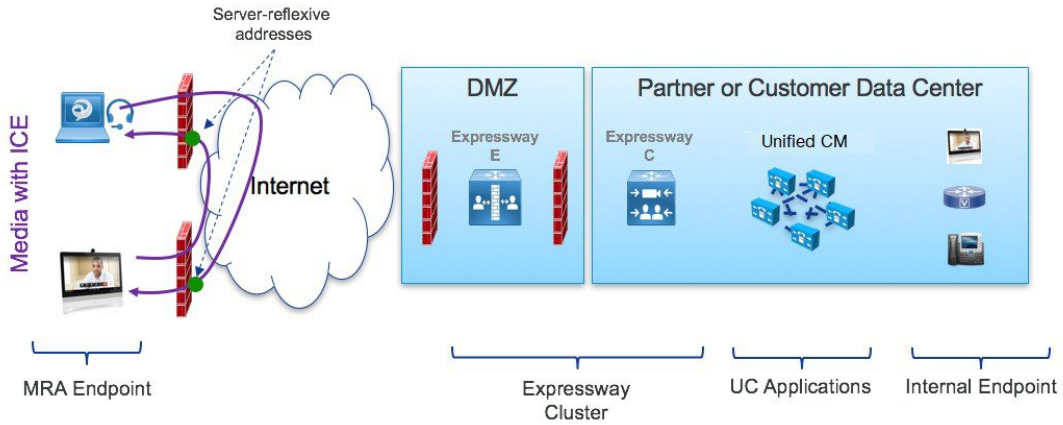
図 *2*:ホストアドレスを使用した *ICE* での *MRA* コールフロー



サーバー再帰アドレスを使用した ICE での MRA コールフロー

次の図は、両方のエンドポイントが異なるファイアウォールの背後にあるため、ホストアドレスが使用されないようになっている ICE を使用した MRA コールを示しています。代わりに、エンドポイントが異なるファイアウォールの背後にあるため、メディアはサーバー再帰アドレスを使用してエンドポイント間を通過します。

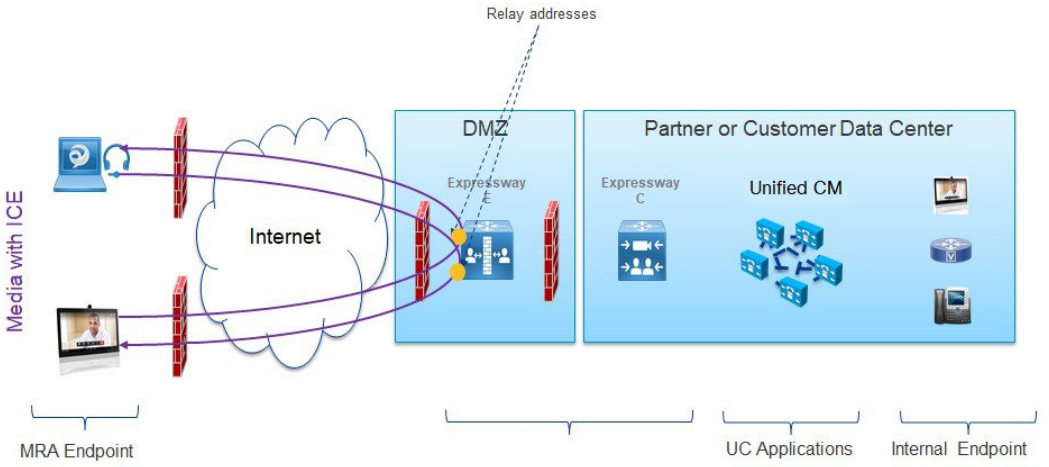
図 *3*:サーバー再帰アドレスを使用した *ICE* での *MRA* コールフロー



リレーアドレスを使用した ICE での MRA コールフロー

対称 NAT を使用した展開など、ホストとサーバー再帰アドレスが正常にネゴシエートできない場合、エンドポイントは ICE 最適化メディアパスとして TURN リレーを利用できます。次の図は、エンドポイントが Cisco Expressway TURN サーバーのリレーアドレスを使用してエンドポイント間でメディアを送信する、ICE を使用した MRA コールを示しています。

図 *4*: リレーアドレスを使用した *ICE* での *MRA* コールフロー

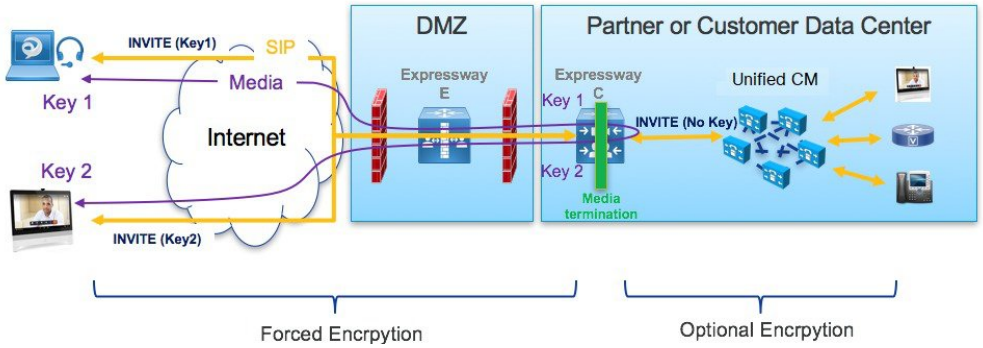


Expressway-C と Unified CM 間のシグナリングパスの暗号化

セキュリティと暗号化は、エンドポイント間の直接メッセージングを検討する際の重要な要素です。MRA エンドポイントはインターネット経由でシグナリングとメディアを送信しているため、暗号化モードでの動作が強制されます。通常の MRA モード（ICE なし）では、エンドポイントと Expressway-C の間では常に暗号化が必要ですが、Expressway-C と Unified CM の間ではオプションです。これが可能な理由は、内部レッグが暗号化されていない場合、Expressway-C がメディアストリームを終了してパケットを復号化できるためです。

次の図は、暗号化が MRA エンドポイントと Expressway-C の間で強制され、内部ネットワークではオプションである、ICE パススルーを使用しない暗号化を示しています。MRA コールでは、各レッグで異なる暗号化キー（キー 1 とキー 2）が交換され、Expressway-C は 2 つのレッグ間のメディアを復号化して再暗号化します。内部レッグが暗号化されていない場合、Unified CM への招待にキーは必要ありません。

図 *5*: *ICE* パススルーを使用しない暗号化

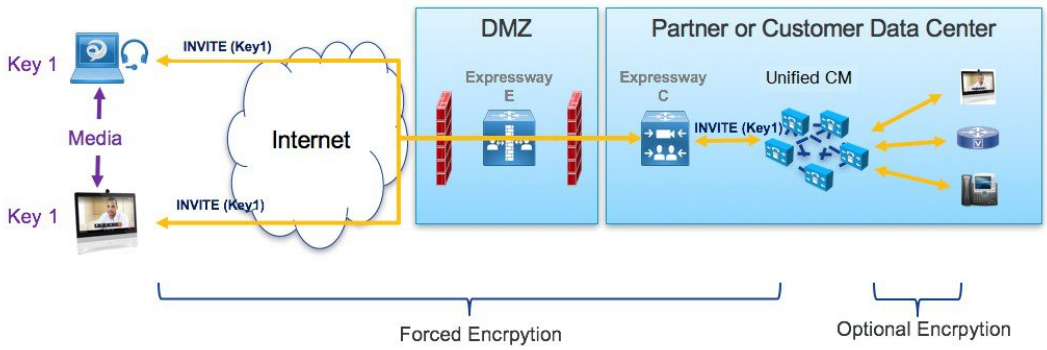


ただし、ICE パススルーモードでは、メディアパケットが Expressway-C 経由ではなく直接相互に送信されるため、エンドポイントはエンドツーエンドで暗号キーを交換できる必要があります。暗号キーが SIP メッセージに含まれる場合は常に、キーを保護するためにメッセージを

TLS 経由で送信する必要があります。暗号キーをエンドツーエンドで送信するには、SIP シグナリングパスをエンドツーエンドで暗号化する必要があるため、Expressway-C と Unified CM の間の内部レッグを暗号化する必要があります。シグナリングパスが暗号化されていない場合、暗号キーはコールセットアップ中にドロップされます。

次の図は、Expressway-C と Unified CM の間のシグナリングレッグも暗号化される ICE パススルーで必要な暗号化を示しています。

図 *6 : ICS* パススルーによる暗号化



サポートされるコンポーネント

Cisco Expressway ベースの展開

現在、ICE メディアパス最適化のサポートは MRA 展開にのみ存在します。次のサービス展開ではテストもサポートもされていません。

- Cisco Webex ハイブリッドサービス
- Jabber Guest
- Collaboration Meeting Room（CMR）クラウド
- ビジネス間コール

HCS 展開

ICE パススルーを使用して、次の HCS 展開タイプで MRA コールのメディアパスを最適化できます。

- HCS 共有アーキテクチャ
- HCS 専用サーバーと HCS 専用インスタンス
- お客様所有のコラボレーション アーキテクチャ

（注） HCS コンタクトセンターは ICE パススルーをサポートしていません。

サポートされるコンポーネント

ICE メディアパスの最適化は、次のコンポーネントでサポートされています。

- HCS 11.5 以降（HCS 展開用）
- Cisco Unified Communications Manager（Unified CM）11.5 以降
- Cisco Expressway-C および Cisco Expressway-E X12.5 以降

サポートされるエンドポイント

MRA に登録されていて、ICE メディアパスの最適化が有効になっている場合、次の ICE 対応エンドポイントは、メディアを相互に直接送信できます。

- Cisco Jabber クライアント、バージョン 12.5 以降、Unified Communications Manager 12.5 以降の使用が前提
- Cisco IP Conference Phone 7832、バージョン 12.5(1) 以降
- Cisco IP Phone 7800 シリーズ（MRA 互換モデルのみ）、バージョン 12.5(1) 以降
- Cisco IP Phone 8800 シリーズ（MRA 互換モデルのみ）、バージョン 12.5(1) 以降
- Cisco TelePresence DX、MX、SX シリーズ、CE バージョン 9.6.1 以降

ICE メディアパスの最適化の前提条件

ICE メディアパス最適化を使用して MRA エンドポイントを展開する場合、次の Cisco Unified Communications Manager の前提条件が存在します。

セキュアモードが Unified CM で実行されている必要がある

次のセキュアモードのいずれかが Cisco Unified Communications Manager で実行されていることが必須です。

- **SIP OAuth モード**は、それをサポートするエンドポイントに推奨されます。SIP OAuth モードは、以下に対してサポートされています。
  - Unified CM リリース 12.5(x) 以降の Cisco Jabber または Webex クライアント
  - Unified CM Release 14 以降の Cisco IP Phone 7800 または 8800 シリーズ
- ICE を使用して MRA 経由で SIP OAuth モードを展開していて、エンドポイントが SIP OAuth モードをサポートしていない場合は、**混合モード**を有効にする必要があります。こ

れには、サポートされていない Cisco IP Phone または TelePresence デバイスが含まれます。SIP OAuth モードを有効にしていない場合、または 12.5(x) 以前の Unified CM リリースを実行している場合は、Cisco Jabber クライアントにも混合モードが必要です。

混合モードを有効にするには、パブリッシャノードで `utils ctl set-cluster mixed-mode` CLI コマンドを実行します。

TLS 暗号化を含む電話セキュリティプロファイル

ICE メディアパス最適化を使用するすべての MRA エンドポイントは、TLS で暗号化された電話セキュリティプロファイルに関連付ける必要があります。電話セキュリティプロファイルには、次を設定する必要があります。

- **[デバイスセキュリティモード（Device Security Mode）]** を **[暗号化（Encrypted）]** にする
- **[転送タイプ（Transport Type）]** を **[TLS]** にする
- **[OAuth認証を有効化（Enable OAuth Authentication）]** をオンにする（SIP OAuth モードを使用している場合）ー確認済み

さらに、Unified CM で混合モードが有効になっている場合、電話セキュリティプロファイル名は FQDN の形式である必要があります。

構成

SIP OAuth モードの構成方法については、「*Cisco Unified Communications Manager* 用構成ガイド」の「SIP OAuth モード」章を参照してください。

混合モードと TLS 暗号化電話セキュリティプロファイルの構成方法については、「*Cisco Unified Communications Manager* 用セキュリティガイド」を参照してください。

ICE メディアパス最適化のタスクフロー

次のタスクを実行して、MRA 展開用に ICE メディアパスの最適化を構成します。

手順

	コマンドまたはアクション	目的
ステップ 1	ICE 設定の構成 （8 ページ）	Unified CM で、MRA エンドポイントに適用できる ICE 設定を構成します。
ステップ 2	サーバー証明書のインストール （9 ページ）	Expressway-C で、適切なサーバー証明書と信頼できる CA 証明書をインストールします。
ステップ 3	CEtcp ネイバーゾーンを CEtls ネイバーゾーンに変更する （9 ページ）	Expressway-C で、既存の CEtcp ネイバーゾーンを CEtls ネイバーゾーンに変更します。

	コマンドまたはアクション	目的
ステップ 4	ICE パススルーサポート用 UC トラバーサルゾーンの設定 （10 ページ）	Expressway-C で、MRA の UC トラバーサルゾーンを設定します。
ステップ 5	ICE パススルーサポート用 UC ネイバーゾーンの設定 （10 ページ）	Expressway-C で、MRA の UC ネイバーゾーンを設定します。
ステップ 6	CLI を使用して Cisco Expressway ゾーンで ICE パススルーを構成する （11 ページ）	Expressway-C で、UC および CEtls ネイバーゾーンの ICE メディアパス最適化を設定します。
ステップ 7	Cisco Expressway-E を TURN サーバーとして設定 （11 ページ）	Expressway-E で、TURN リレーサービスを設定します。

ICE 設定の構成

Cisco Unified Communications Manager で、共通電話プロファイル内で ICE 設定を構成します。これは、プロファイルを使用する MRA 電話のグループに適用できます。

（注） 共通電話プロファイルを使用する代わりに、ICE設定は、製品固有の構成レイアウトの一部として、以下の [Unified CM] 設定画面のいずれかで適用できます。矛盾する構成が存在する場合、以下の優先順位によって、どの構成が電話機に適用されるかが決まります。

1. 電話機の構成—電話機ごとに ICE 設定を構成します。
2. 共通電話プロファイル—プロファイルを使用する電話機のグループに適用される ICE 設定を構成します。
3. 企業電話構成—これらの設定を使用する電話機にクラスタ全体に適用される ICE 設定を構成します。

使用する設定画面に関係なく、デフォルトでは ICE が**有効**になっており、**ホスト**がデフォルトの候補として使用され、サーバーの再帰アドレッシングも**有効**になっています。ただし、Expressway-E リレー TURN サービスを使用するには、これらのいずれかのウィンドウの ICE 設定で Expressway-E サーバーを指定する必要があります。

ステップ 1 Cisco Unified CM Administration で、**[デバイス（Device）] > [デバイス設定（Device Settings）] > [共有電話プロファイル（Common Phone Profile）]**の順に選択します。

ステップ 2 次のいずれかを実行します。

- 新しいプロファイルを作成するには、[新規追加（Add New）] をクリックします。
- **[検索（Find）]** をクリックし、既存のプロファイルを選択します。たとえば、デフォルトで新しい電話機に割り当てられるデフォルトの標準共通電話プロファイルなどです。

ステップ 3 **Interactive Connectivity Establishment（ICE）**で、次の ICE 設定を構成します。

- **ICE**—これが [有効（Enabled）] になっていることを確認します。
- **デフォルトの候補タイプ**ー**[ホスト（Host）]** が推奨値です。
- **サーバー再帰アドレス**—**[有効（Enabled）]** に設定されていることを確認します。
- **プライマリ TURN サーバーホスト名または IP アドレス**ーExpressway-E ノードの FQDN を入力して、プライマリ TURN サーバーとして機能させます。
- **セカンダリ TURN サーバーホスト名または IP アドレス**—Expressway-E ノードの FQDN を入力して、セカンダリ TURN サーバーとして機能させます。
- **TURN サーバー転送タイプ**—**[自動（Auto）]** が推奨値です。
- **TURN サーバーユーザー名**—Expressway-E サーバーにアクセスできるユーザー名を入力します。
- **TURN サーバーパスワード**—Expressway-E にアクセスするユーザーのパスワードを入力します。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 プロファイルを電話機に適用するには、次の手順を実行します。

a) **[デバイス（Device）]** > **[電話機（Phone）]** の順に選択します。
b) **[検索（Find）]** をクリックし、プロファイルを適用する電話機を選択します。
c) 作成する**共通電話プロファイル**を選択します。
d) [保存（Save）] をクリックします。

サーバー証明書のインストール

ここでは、サーバー証明書のインストール手順を説明します。

ステップ 1 サーバー証明書の新しい証明書署名要求を生成します（**[メンテナンス（Maintenance）]** > **[セキュリティ（Security）]** > **[サーバー証明書（Server Certificate）]**）。

詳細については、『Expressway 構成ガイド』ページの『*Cisco Expressway* 証明書作成と使用導入ガイド』を参照してください。

ステップ 2 証明書署名要求生成中、Subject Alternate Names（SAN）のエンドポイントに関連付ける電話機セキュリティプロファイルの名前を含めます。

詳細については、Expressway サーバーの証明書署名要求要件を参照してください。

ステップ 3 Cisco Expressway-C の信頼された証明機関から署名されたサーバー証明書をインストールします。

この証明書により、電話セキュリティ プロファイルを使用するエンドポイントは、 Cisco Expressway-C と Unified CM 間の TLS 接続を介して登録できます。

CEtcp ネイバーゾーンを CEtls ネイバーゾーンに変更する

Cisco Expressway-C で、MRA 用にすでに構成されている 既存の CEtcp ネイバーゾーンを CEtls ネイバーゾーンに変更します。

始める前に

Unified CM が次の有効になっている次のいずれかのモードでセキュアモードになっているかを確認します。

- 混合モード
- SIP OAuth モード

ステップ 1 **[構成（Configuration）] > [Unified Communications] > [Unified CMサーバー（Unified CM servers）]** の順に選択します。

ステップ 2 検出済みの Unified CM サーバーを選択し、**[サーバーを更新（Refresh Servers）]** をクリックして構成を更新します。

ステップ 3 Unified CM 状態が *TLS: Active* と表示されているかを確認します。

CEtcp ネイバーゾーンがまだ作成されていない場合は、Unified CM サーバーを追加してから、サーバーを更新する必要があります。「Unified CM クラスタの追加」に進みます。

Unified CM クラスタがセキュアモードの場合、Cisco Expressway-C は構成不可の CEtls ネイバーゾーンをそれ自体と検出した Unified CM ノードの間で自動生成します。詳細については、自動生成されたゾーンと検索ルールを参照してください。

ICE パススルーサポート用 UC トラバーサルゾーンの設定

この手順では、ICE パススルーをサポートするために UC トラバーサルゾーンを設定する方法について説明します。

ステップ 1 Cisco Expressway-C で、**[構成（Configuration）] > [ゾーン（Zones）] > [ゾーン（Zones）]**の順に選択します。

ステップ 2 Cisco Expressway-E への Unified Communications ゾーンを選択します。

ステップ 3 SIP ペインで、**[ICEパススルーサポート（ICE Passthrough support）]** をオンに設定し、**[ICEサポート（ICE Support）]**をオフに設定します。

（注） ICE パススルーサポートは、ICE サポートより優先されます。ベスト プラクティスとして、ICE パススルー サポートをオンにして ICE サポートをオフにすることをお勧めします。

ICE パススルーサポート用 UC ネイバーゾーンの設定

この手順では、ICE パススルーをサポートするために UC ネイバーゾーンを設定する方法について説明します。

ステップ 1 Cisco Expressway-C で、**[構成（Configuration）] > [Unified Communications] > [Unified CMサーバー（Unified CM servers）]** の順に選択します。

ステップ 2 サーバを選択します。

ステップ 3 Unified CM サーバルックアップペインで**[ICEパススルーサポート（ICE Passthrough support）]** をオンにします。

CLI を使用して Cisco Expressway ゾーンで ICE パススルーを構成する

Cisco Expressway の ICE パススルーオプションは、ゾーンごとにセットアップします。各 Unified CM トラバーサル クライアント ゾーンおよび CEtls ネイバー ゾーンで ICE パススルーを有効にする必要があります。

Web インターフェイスの代わりに CLI を使用して、ICE パススルーのゾーンを構成できます。

ステップ 1 **[構成（Configuration）] > [ゾーン（Zones）]** の順に選択し、Cisco Expressway-E への Unified CM トラバーサルゾーンをクリックします。

ステップ 2 URL で、ゾーンの ID をメモします。たとえば、次の URL では、4 がゾーン ID です。

```
https://expressway.example.com/editzone?id=4
```

ステップ 3 CEtls ネイバーゾーンに対して手順 1 と 2 を繰り返します。

ステップ 4 管理者として Cisco Expressway-C の CLI にログインします。

ステップ 5 次のコマンドを実行して、Unified CM トラバーサル クライアント ゾーンで ICE パススルーを有効にします。

```
xConfiguration Zones Zone <Unified Communication Traversal client zone ID> TraversalClient SIP Media
 ICEPassThrough Support: On
```

ステップ 6 次のコマンドを実行して、CEtls ネイバーゾーンで ICE パススルーを有効にします。

```
xConfiguration Zones Zone <CEtls Neighbor zone ID> Neighbor SIP Media ICEPassThrough Support: On
```

Cisco Expressway-E を TURN サーバーとして設定

TURN サーバーが実行されている Cisco Expressway-E サーバーを使用して、リレーアドレスを検索し、サーバー再帰アドレスを取得できます。これは、通常 MRA に使用するクラスタの Cisco Expressway-E ですが、Cisco Expressway-E サーバーである必要はありません。準拠している TURN サーバーを使用できます。

次の手順は、Cisco Expressway-E TURN サーバーで必要な構成をまとめたものです。

ステップ 1 次の設定で TURN サーバー（**[構成（Configuration）] > [トラバーサル（Traversal）] > [TURN]**）を構成します

- **TURN サービス**：オンに設定。
- **TCP 443 TURN サービス**：オフに設定。
- **TURN ポート多重化**：オフに設定。このオプションは、大規模システムのみ利用できます。
- **TURN リクエストポート**：デフォルト値を使用。中小規模のシステムの場合、デフォルトポートは 3478 です。大規模システムの場合、デフォルトポート範囲は 3478 から 3483 です。

  （注） 大規模システムの **[TURNリクエストポート（TURN request port）]** フィールドは、**[TURN ポート多重化（TURN port multiplexing）]** がオンに設定されている場合のみ利用できます。

- **TURN リクエストポート範囲開始**：デフォルト値を使用。
- **TURNリクエストポート範囲終了**：デフォルト値を使用。

  （注） **TURN リクエストポート範囲開始**と **TURN リクエストポート範囲終了**オプションは、大規模システムの **[TURNポート多重化（TURN port multiplexing）]** がオフに設定されている場合のみ使用できます。

- **委任されたログインチェック**：デフォルト値を使用。
- **認証レルム**：デフォルト値を使用。デフォルト値は TANDBERG です。
- **メディアポート範囲開始**：デフォルト値を使用。デフォルト値は 24000 です。
- **メディアポート範囲終了**：デフォルト値を使用。デフォルト値は 29999 です。

ステップ 2 TURN クライアントが TURN サーバーで認証するためのログイン情報（**[構成（Configuration）] > [認証（Authentication）] > [デバイス（Device）] > [ローカルデータベース（Local database）]**）を構成します。

ステップ 3 [保存（Save）] をクリックします。

ステップ 4 TURN サーバーステータスが **[TURNサーバーステータス（TURN server status）]** で *[アクティブ（Active）]* に変更されたか確認します。

Cisco Expressway-E での TURN サービスの構成手順については、https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html の『*Cisco Expressway* 管理者ガイド』の「*TURN* サービスの構成」項を参照してください。

ICE パススルーメトリックの使用

このセクションでは、 Cisco Expressway で ICE パススルーのメトリックを使用する方法について説明します。

- Cisco Expressway-C で ICE パススルー メトリックを表示する
- collectd デーモンを使用してメトリクスを収集する
- 通話履歴で通話タイプを表示
- 帯域幅操作

Expressway-C で ICE パススルーメトリックを表示

Expressway-C では、完了した ICE パススルーコールのメトリックデータを表示できます。ICE パススルーコールをルーティングするように構成されているサーバーごとに、さまざまなメトリックを使用できます。値は 24 時間ごとに更新されます。

図 *7:* メトリクスの例

ICE Passthrough metrics

Metrics	
Peer	127.0.0.1
Start time	2018-10-22 20:43:45
End time	2018-10-23 20:43:45
B2BUA connected calls	4
Calls with optimized ICE media paths	2
% of calls with optimized ICE media paths	50%
Call types	
Host to host	100%
Host to server reflexive	0%
Host to relay	0%
Server reflexive to server reflexive	0%
Server reflexive to relay	0%
Relay to relay	0%
Advanced	
Calls with required Expressway ICE configuration	100%
Calls attempted with offered ICE candidates	100%
Calls with ICE candidates offered by one endpoint	0%
Calls without ICE candidates	0%
Calls with non-optimized media paths	50%
Calls with ICE candidates offered but without required Expressway ICE configuration	0%

- **[ピア（Peer）]** フィールドには、各ノードの IP アドレスまたはホスト名が表示されます。
- 最新の 24 時間間隔のデータが表示されます。
- 各ピアアドレスは、そのノードの履歴に移動するリンクです。
- 間隔の開始時刻は、最新のサーバー再起動の時刻を反映しています。
- 各列には、個別のクラスタの情報が表示されます。

ステップ 1 Expressway-C で、**[ステータス（Status）]** > **[ICEパススルーメトリック（ICE Passthrough metrics）]** の順に選択します。

このページは、これらのセクションで構成されています。

- **メトリクス**：各ピアのメトリクスが表示される時間間隔。この間隔で、B2BUA 接続されたコールの数、ICE コールの数、および B2BUA コールの合計に対する ICE の割合。N/A 値は、この 24 時間の間隔中に ICE コールが処理されなかった場合に発生します。
- **コールタイプ**：各コールタイプに対して、各コールタイプで発信された ICE コールの割合。
- **詳細**：トラブルシューティングに役立つその他のメトリック。

ステップ 2 フィールドの詳細な説明を表示するには、フィールド名の横にある **i** アイコンをクリックします。

ステップ 3 並べ替えるには、列名をクリックしてから、**上**矢印または**下**矢印をクリックして、その列でデータを並べ替えます。

ステップ 4 **[CSV にエクスポート（Export to CSV）]** をクリックして、表示しているページの値のスプレッドシートを作成します。

ステップ 5 クラスタの IP アドレスまたはホスト名をクリックして、そのクラスタの値の履歴を示す **[ICE コールメトリック履歴（ICE Call Metrics History）]** ページを表示します。

- 各列には個別のパラメータが表示されます。
- 各行には、異なる間隔の値が表示され、最新のものが最初に表示されます。
- 各値は、パーセンテージではなくローバリューです。
- このページには、最大 60 件のレコード（つまり、最新の 24 時間間隔で 60 件）を表示できます。

collectd デーモンを使用したメトリック収集

ICE パススルーコールのメトリックを表示する代わりに、*collectd* デーモンを使用してメトリックを収集できます。収集のためのサーバーのセットアップに関する詳細は、『Expressway の保持および運用ガイド』の『*Cisco Expressway* 有用性ガイド』の「「システム メトリック コレクションの導入」」項を参照してください。

通話履歴で通話タイプを表示

ICE パススルーコールの場合、コールタイプはコール履歴に表示されます。

ステップ 1 Cisco Expressway-C で、**[ステータス（Status）]** > **[コール（Calls）]** > **[履歴（History）]** の順に選択します。

ステップ 2 次のアクションのいずれかを選択します。

- **[開始時刻（Start Time）]** 列の値をクリックすると、通話詳細記録（CDR）が表示されます。

- **[アクション（Actions）]** 列でビューをクリックします。

ステップ 3 **[ICEパススルーコールタイプ（ICE Passthrough call type）]** フィールドの値を検証します。

次の値を使用できます。

- *none*—最適化されたメディアパスがコールに使用されていないことを示します。 Cisco Expressway B2BUA を使用してコールが処理され、接続されます。
- *host_to_host*—コール用に最適化されたメディアパスが、エンドポイントのホストアドレスを使用して確立されたことを示します。
- *host_to_srvrflx*—コール用に最適化されたメディアパスがエンドポイントのいずれかのホストアドレスおよびサーバー再帰アドレスの間で確立されたことを示します。
- *host_to_relay*—コール用に最適化されたメディアパスが別のエンドポイントの TURN リレーアドレスの間で確立されたことを示します。
- *srvrflx_to_srvrflx*—コール用に最適化されたメディアパスがエンドポイントのサーバー再帰アドレスを使用して確立されたことを示します。
- *srvrflx_to_relay*—コール用に最適化されたメディアパスがエンドポイントのいずれかのサーバー再帰アドレスと別のエンドポイントの TURN リレーアドレスの間で確立されたことを示します。
- *relay_to_relay*—コール用に最適化されたメディアパスがエンドポイントのリレーアドレスを使用して確立されたことを示します。

ステップ 4 （任意） B2BUA コールレッグの詳細を確認するには、**[コールコンポーネント（Call components）]** セクションで、B2BUA タイプを表示されているコールレッグを選択します。

帯域幅操作

ICE がネゴシエートされると、メディアが Cisco Expressway に移動し、メディア帯域幅が減少します。**[状態（Status）]** > **[帯域幅（Bandwidth）]** > **[リンク（Links）]** ページに現在の帯域幅が表示されていて、ICE が使用されている場合、現在の使用量の合計は、より少ない使用率を表しています。

（注） 帯域幅の使用量には、TURN サーバーが使用する帯域幅は含まれません。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。