



H.323 のサポート

現在、SBC は、SIP だけでなく、H.323 もサポートしています。これにより、複数のベンダーのマルチメディア製品およびアプリケーションの相互運用が可能となり、また、ユーザは互換性を気にすることなく通信できます。

H.323 は、Local Area Network (LAN; ローカル エリア ネットワーク)、Wide Area Network (WAN)、インターネットなどのパケット交換網におけるマルチメディア通信の国際標準です。これは 1996 年、International Communications Union (ITU) により初めて定義されました。最新版は、H.323 パージョン 5 (2003) です。

H.323 サポートの機能履歴

リリース	変更内容
リリース 3.5.0	この機能は、Cisco XR 12000 シリーズ ルータで導入されました。
リリース 3.5.1	H.323 プライバシー機能が導入されました。

内容

このモジュールの構成は次のとおりです。

- [「H.323 サポートの前提条件」\(P.79\)](#)
- [「H.323 サポートの制約事項」\(P.80\)](#)
- [「H.323 サポートに関する情報」\(P.80\)](#)
- [「H.323 機能の設定」\(P.95\)](#)
- [「その他の関連資料」\(P.103\)](#)

H.323 サポートの前提条件

- この機能を使用するには、H.323 に関連する ITU 標準、ゲートキーパー、およびゲートウェイに関する基本的な理解を必要とします。ゲートウェイは、Public Switched Telephone Network (PSTN; 公衆電話回線網) と H.323 ネットワークの間のエッジルーティングを決定します。ゲートキーパーは、複数のゲートウェイを論理的ゾーンにグループ化し、ゾーン間でコールルーティングを行います。

H.323 サポートの制約事項

H.323 サポートの制約事項については、この章、およびこのマニュアルのその他の H.323 に関連する章で、機能ごとに列挙してあります。

H.323 サポートに関する情報

H.323 はプロトコルおよびドキュメントの集合であり、これには標準 H.323、H.225.0、H.245、H.450 シリーズおよび H.460 シリーズのドキュメントが含まれます。これは、データ コラボレーションおよびファイル転送に使用される T.120 をサポートしています。標準 H.323 システムには、H.323 のすべてのコンポーネントが必要であるわけではありません。たとえば、ナンバー ポータビリティについて記述した H.460.2 は、通常、企業のビデオ会議システムでは使用されません。

H.323 は、Voice over Internet Protocol (VoIP)、および IP ベースのビデオ会議で使用され、Session Initiation Protocol (SIP) と同様の役割を果たします。H.323 は、IP 以外のパケット交換網で動作する場合もありますが、開発当初から主に IP ネットワークで動作するように設計されています。ほとんどのユーザは H.323 プロトコルに規定されているマルチポイント機能を活用していませんが、H.323 はマルチポイントの音声およびビデオ会議機能を使用できるように設計されています。

H.323 は機能的には SIP より進んでいますが、柔軟性の面では SIP に劣ります。現在、SIP の定義は明確ではありませんが、スケーラビリティに優れ、インターネットアプリケーションを統合しやすくなっています。SIP 同様、H.323 も世界中のネットワークにおける音声およびビデオ転送で世界市場をリードし、毎月、膨大な量の音声トラフィックを運んでいます。SBC は SIP と H.323 の両方をサポートしています。これにより、複数のベンダーが提供するマルチメディア製品およびアプリケーションの相互運用を可能にし、ユーザが互換性を気にすることなく通信できるようになります。

SBC でサポートされる H.323 の機能

サポート対象の次の H.323 機能については、このガイドの他の該当箇所で個別に説明されていたり、Q.931/H.225 標準プロトコルの一部として記述されていたりします。

- H.323/SIP インターワーキング（「[H.323-SIP インターワーキング](#)」の章を参照）：SIP/H.323 コールおよびメディア シグナリングの定義済みサブセットのインターワーキングです。
- シグナリング ピアの DNS コンフィギュレーション：この機能を使用すると、adjacency-signal-peer のコンフィギュレーションで IP アドレスの代わりにドメイン名を使用できます。
- ハンティング（「[SBC ポリシーの実装](#)」の章の「ハンティング」を参照）：障害時に SBC が他のルートまたは宛先隣接をハントできるようになります。とは、ルートを再試行することを意味します。
- 基本的な会議パススルー（この機能は Q.931/H.225 パススルーの一部です）：conferenceID および conferenceGoal のパススルーです。会議は、コール マネージャなどのサードパーティ製機器によって制御されます。SBC により、会議は、会議に関連するすべての情報をパススルーできるようになります。
- H.450 パススルー（この機能は Q.931/H.225 パススルーの一部です）：コール レッグ間の H.450 エレメントのパススルーです。

この章では、サポート対象の次の H.323 機能について説明します。

- [H.245 個別制御チャネル](#)
- [H.245 パススルー](#)

- スロー スタート メディア リレー
- T.38 ファクス リレー
- DTMF インターワーキング
- トランスコーディング
- RAS テクノロジー プレフィックス
- ユーザ プロトコル タイマーの制御
- T.38 ファクス リレー
- Q.931/H.225 パススルー
- H.323 プライバシー

H.245 個別制御チャンネル

H.323 プロシージャでは、SBC は TCP 経由で個別に H.245 制御チャンネルをセットアップする必要があります。この機能により、トンネル型 H.245 サポートが補完され、ユーザはトンネリングを使用するかどうかを制御できるようになります。

SBC は、この新機能によって H.323 同士のコールを実行し、2 つのコール レッグは異なる H.245 トランスポート メカニズムのネゴシエーションを実行できるようになります。コール レッグは、H.245 個別制御チャンネルを使用するかどうかをそれぞれ独自に決定します。

SBC は、次のいずれかのケースで必要とされた場合だけ、H.245 個別制御チャンネルをセットアップします。

- SBC が startH245 Facility を受信した場合
- SBC が H.245 メッセージを送信する必要があるが、トンネリングが使用できない場合

トンネリングが使用可能であるときに SBC が H.245 個別制御チャンネルを要求することはありません。ただし、「disable tunneling」 CLI コマンドが設定されている場合を除きます（後の「[H.245 個別制御チャンネルの設定](#)」を参照）。ピアが h245Address を提供しているという理由だけで、SBC が H.245 アドレスに接続することはありません。

SBC は、必要になるまで H.245 アドレス ユニットの提供せず、次の処理を実行します。

- 可能であれば、SBC は代わりにピアへ接続します。
- 可能ではない場合、SBC は startH245 Facility に自身の H.245 アドレスを提供し、10 秒間、ピアの接続を待ちます。この制限時間は設定できません。

H.323 v2 以降、Facility reason として startH245 がサポートされたため、この機能はすべてのピア デバイスでサポートされると考えられます。ピアが H.245 接続を要求したときに、この接続が存在しなかった場合、相手側は startH245 Facility を使用して、SBC に接続を促す必要があります。

可能な H.245 転送（トンネル型または個別）が存在せず、SBC により H.245 メッセージを送信しなければならない場合、このコールは終了します。

provisionalRespToH245Tunnelling を受信すると、SBC は個別に H.245 を指向する前に待機し、最終的なトンネリング結果を判断します。この時点で H.245 メッセージはキューに入れられ、H.245 転送が可能になると送信されます。

H.245 接続で競争が発生したときには、SBC はこの競争に負けた場合だけ切断します。SBC が勝った場合は、相手側が切断する必要があります。競争は、接続アドレス/ポートではなく、リッスンアドレス/ポートを比較することにより、解決されます。

複数のコールが 1 つの接続を共有している場合、コール スコープ、または接続スコープでバックプレッシャをかけます。したがって、コール レッグ B が何らかの理由で H.245 メッセージを転送できない場合、コール レッグ A の接続はピアに対して TCP バックプレッシャをかけます。コール レッグ A が H.245 トンネリングを実行し、その他のコールと Q.931 TCP 接続を共有した場合、その他のコールでもピアにバックプレッシャがかかるようになります。

SBC は、関連するソケットを閉じて、コールと同じポイントで H.245 個別接続を切断します。

H.245 個別制御チャネルに対する制約事項

- SBC は、H.323-H.323 コールにおいてピア間またはピアと DBE との間に直接 H.245 TCP 接続をセットアップさせるようなモデルをサポートしていません。
- 隣接単位またはコール単位で H.245 転送ステータスを一覧表示するための表示コマンドは用意されていません。
- H.245 セキュリティはサポートされていません。

H.245 パススルー

メディア バイパスでは、H.245 コンテンツは変更されずに 2 つの H.323 コール レッグ間を通過します (メディア バイパスの詳細については、「SBC 隣接の実装」の「メディア ルーティングへの隣接の影響」を参照してください)。パススルーは、H.245 メッセージがトンネル型 H.245 転送経路で受信されたか、H.245 個別制御チャネル経路で受信されたかに関係なく発生します。また、H.323 コール レッグが両方とも同じ H.245 転送メカニズムを使用している必要はありません。この機能では、通過する H.245 コンテンツを変更せずに、2 個の H.323 デバイスの間に SBC を挿入することができます。

これが可能なのは、エンドポイント間で H.245 メッセージが不透明にパススルーされるためです。Fast Start の要求および応答は、H.245 本体と同様にパススルーされます。SBC により検査されるメッセージは、ファスト スタートおよび論理チャネル シグナリングのメッセージだけです。これらは、コールで使用される帯域幅を獲得するために使用されます。

H.245 パススルーの制約事項

- 特定のメッセージまたはメッセージ要素のパススルーをブロックする設定はこの機能には含まれません。このような設定は別に用意されています。
- メディア バイパス コールでは、課金レコードに SDP は表示されません。
- SBC は、すべてのシグナリング トラフィックに対する一般的なレート制限を除いて、パススルーされる H.245 トラフィックのレート制限をサポートしていません。

スロー スタート メディア リレー

SBC は、単方向 H.245 チャネルのメディア リレー (DBE によるメディア パススルー) をサポートしています。H.245 コーデック タイプは、DBE プログラミング、トランスコーダ プログラミング、および課金を目的として、セッション記述プロトコル (SDP) に変換されます。これはコーデック マッピング テーブルを使用して実行されます (後の「T.38 ファクス リレー」を参照)。SDP マッピングがないコーデック タイプを処理する場合、SBE はベストエフォート方式で試行し、可能な最良の SDP 一致を探します。

2 個の H.323 デバイス間に SBC を挿入しても、H.245 の機能には影響はありません（「H.245 パススルー」を参照）。たとえば、SBC は、メディア リレー コール の H.245 チャネルの論理チャネル番号を変更しません。分散 DBE モデルでは、DBE で必要なメディアの停止を確立するために、H.248 信号が使用されます。

SBC は、次のような H.245 プロシージャを使用してメディアの再ネゴシエーションをサポートします

- fax upspeed : エンドポイントは低ビット レートの音声コーデックから G.711 に切り替えます。
- TCS=0 : 一方のエンドポイントが他方に対し、一時的にすべてのチャネルをクローズするように働きかけます。

T.38 ファクスへの切り替えについては、後述の「T.38 ファクス リレー」を参照してください。

スロー スタート メディア リレーの制約事項

- SBC は、ファスト スタートと Open Logical Channel Close (OLC) のいずれでも、双方向 H.245 チャネルをサポートしていません。
- 異なるタイプの UserInputIndication 間では、DTMF インターワーキングはサポートされていません。
- DTMF インターワーキングを制御するユーザ コンフィギュレーションはありません。DTMF インターワーキングは機能ネゴシエーションによってだけトリガーされます。
- 特定のコーデックのセットアップをブロックする手段も、未知のコーデックを無視する手段もありません。上記のベストエフォート型の機能が常にイネーブルになります。
- SBC では、マルチポイント機能はサポートされていません。

コーデック マッピング

次に示すコーデック マッピングは、H.245 コーデックを SDP として表すために SBC によって使用されます。その目的は次のとおりです。

- 課金レコード（メディア リレーだけ）
- DBE プログラミング（メディア リレーだけ）
- 帯域幅割り当て（メディア リレーおよびメディア バイパス）この帯域幅は、SDP に基づいて計算されます。H.245 から直接計算されることはありません。

H.245 コーデック	表示
g711Alaw64k	PCMA/8000
g711Ulaw64k	PCMU/8000
g722_64k	G722/8000
g7231	G723.1/80
g728	G728/8000
g729	G729/8000
g729AnnexA	G729/8000
g729wAnnexB	G729/8000
g729AnnexAwAnnexB	G729/8000
gsmHalfRate	GSM-HR/8000

H.245 コーデック	表示
gsmFullRate	GSM/8000
その他すべてのオーディオ コーデック	PCMU/8000 (デフォルト コーデック)
T.38	「T.38 ファクス リレー」 を参照してください。

次の点に注意してください。

- SBC は、メディア リレーでもメディア バイパスでも、T.38 を除く H.245 のビデオおよびデータ コーデックをサポートしません。
- H.323/SIP インターワーキングのためにサポートされているコーデックの範囲はさらに小さくなります (詳細は、「[H.323-SIP インターワーキング](#)」の章を参照)。

DTMF インターワーキング

ユーザ要求の転送には、Dual-Tone Multi-Frequency (DTMF) トーンが使用されます。システムによって、サポートされている DTMF の形式は異なる可能性があります。SBC はこれらのシステムの間で、DTMF インターワーキングをイネーブルにします。

たとえば、標準に準拠しない H.323 デバイスの一部では、英数字 `UserInputIndication` の最小公分母はサポートされていません。このようなデバイスが DTMF 信号を送信できるのは、RFC2833 telephony イベントを通じて、またはインバンド メディア データとしてだけです。一方、`UserInputIndication` をサポートして、RFC2833 telephony イベントはサポートしないデバイスもあります。

このような 2 つのデバイスがバックツーバックで配置された場合、インバンド メディア データと同様に DTMF トーンを送信するという選択肢しかありません。これらのデバイスの上に SBC を配置すると、両者の間の SBC インターワーキングにより、両側ともサポート対象の信号方式を使用して (一方は `UserInputIndication`、もう一方は RFC 2833)、DTMF を送信できます。

この機能を使用するためには、コールの特定の側 (RFC 2833 だけのデバイスに面している側) で RFC 2833 DTMF の代行受信と挿入をイネーブルにするように SBE が DBE をプログラムする必要があります。その後、SBE と DBE は協力して、H.245 制御チャネルと RTP ストリームの間で DTMF シグナリングを転送します。

DTMF インターワーキングでは、`TerminalCapabilitySet` を通じてネゴシエーションが行われます。したがって、SBC は英数字と RFC 2833 の両方式をサポートしていることをアダプタイズするために、`TerminalCapabilitySet` を送出できなければなりません。

この項で説明する新機能は、既存のすべての H.323 DTMF インターワーキング機能に代わるものです。H.323 コールは、英数字 `UserInputIndication` と RFC2833 の間の DTMF インターワーキングをサポートする必要があります。この場合は、SBE は DBE と連携して RTP での DTMF 挿入および代行受信を実行します。

DTMF インターワーキングでは、手動設定ではなく、`TerminalCapabilitySet` を通じてネゴシエーションが行われます。そのため、SBC は通過時に必要に応じて `TerminalCapabilitySet` を送出することにより、英数字と RFC2833 の両方式をサポートしていることを必ずアダプタイズする必要があります (ただし、TCS=0 の場合は例外です)。

DTMF インターワーキングの制約事項

- DTMF インターワーキングでは、英数字 `UserInputIndication` メソッドだけがサポートされます。
- SBE は、ピアが任意の形式の `UserInputCapability` をアダプタイズし、英数字 DTMF を送受信できると想定します。

- 手動設定では DTMF インターワーキングは強制できません。
- インバンド オーディオ データとしての DTMF の検出と挿入はいずれもサポートされていません。

トランスコーディング

この機能は、H.323 スロー スタート コールを追加できるようにするためのトランスコーディング サポートへのアップデートです。SBC はスロー スタート コールのトランスコーディングをサポートしています。これにより、通常なら相互に通信できないようなコーデックの異なるエンドポイント間での通信が可能で、バックツーバック配置の 2 つの H.323 エンドポイントには、相互に受け入れ可能な共通のコーデックがない場合もあります。

典型的な例としては、一方が帯域幅制限や管理ポリシーなどを理由に狭帯域幅のコーデック（たとえば G.729）を要求し、もう一方は G.711 だけをサポートしているといった場合が考えられます。たとえば、発信側が g711alaw を使用し、着信側が G.729 annex B を使用している場合、SBC は g711alaw コーデックを G.729 annex B コーデックに変換して、この 2 者間の通信を可能にします。SBC は、コーデックのネゴシエーションが必要であることを検出すると、Cisco MGX 8880 スイッチの VISM をメディア ゲートウェイとして使用してトランスコーディングを実行します。MGX 8880 トランスコーダとともに、エンドポイント間に SBC を配置すれば、こうしたコールを成功させることができます。

以前のリリースでサポートされていたのは、ファスト スタートだけのトランスコーディング バージョンでした。この機能は現在、TerminalCapabilitySet からトリガーされるトランスコーディングの実装に置き換えられています。

トランスコーディングに関する制約事項

- トランスコーダを使用するかどうかは各コールに 1 回決定され、エンドポイントがアップデートされた TerminalCapabilitySets (TCS=0 を含む) を発行しても変更されません。
- トランスコーディングが必要な場合、SBC はコールに対称コーデックを強制します。
- ファスト スタート コールではトランスコーディングは呼び出されません。適切なチャンネルがない場合、エンドポイントは、トランスコーディングを呼び出すことのできる時点でスロー スタートに廃棄する必要があります。
- トランスコーディング用にサポートされているコーデックは G.711 と G.729 だけです。これらのコーデックとの動作がテストされているトランスコーダは Cisco MGX 8880 スイッチだけです。

RAS テクノロジー プレフィックス

テクノロジー プレフィックスは、オプションの H.323 標準ベース機能です。ゲートウェイやゲートキーパーでサポートされ、H.323 VoIP ネットワーク内で、より柔軟なコール ルーティングを可能にします。ゲートキーパーはテクノロジー プレフィックスを使用して同じタイプのエンドポイントをグループにまとめます。テクノロジー プレフィックスは、ゲートウェイのタイプ、クラス、またはプールの識別にも使用されます。この機能によって、隣接ごとに RAS テクノロジー プレフィックスを設定し、ゲートキーパーにこのプレフィックスを登録できるようになります。

現在、H.323 隣接には、オプションとして、1 ~ 32 桁のダイヤル番号からなる単一のテクノロジー プレフィックスを設定できるようになっています。これは、次に示す RRQ フィールドで、ゲートキーパーにテクノロジー プレフィックスを発行します。

```
terminalType.gateway.protocol.voice.supportedPrefixes.
```

既存の隣接設定と同様、このフィールドは、隣接が接続されている間に変更できません。この機能は、着信番号のディジットの追加と削除に対する既存の SBC のサポートと連携して機能します（「SBC ポリシーの実装」の章の「番号操作」を参照）。

RAS テクノロジー プレフィックスの制約事項

- この機能では、たとえば、ゲートキーパーへのプレフィックス AliasAddresses の登録のようなゾーンプレフィックスはサポートされていません。

ユーザ プロトコル タイマーの制御

H.323 標準では、各種メッセージについて、タイマー、タイムアウト、およびリトライ回数が推奨されています。これらは固定値ではなく、範囲で表されています。これらの値を定義する機能は、異なるデバイス間のインターワーキングに役立ちます。現在、H.323 タイマーとリトライ回数は、グローバルレベルおよび隣接単位でユーザによる設定が可能です。タイマーは秒単位で設定します。

設定可能な Q.931/H.225 タイマーは次のとおりです。

- Q.931/H.225 セットアップ タイマー T303
- Q.931/H.225 確立タイマー T301
- Q.931/H.225 着信コール設定処理タイマー T310

設定可能な RAS タイムアウトおよびリトライ回数は次のとおりです

- GRQ
- RRQ
- URQ
- ARQ
- BRQ
- DRQ
- LRQ

RAS RRQ TTL およびキープアライブ時間（ライトウェイト RRQ 動作を制御）は設定可能です。これら 2 つの設定値は相互に関連しています。特定の隣接に安全でない値を設定すると、SBE は値をデフォルトに戻します。

隣接リトライ タイマーは設定可能であり、なんらかの理由で隣接が失敗した場合の自動隣接接続再試行に使用できます。

次のタイマーはハードコードされています。

- TCP シャットダウン タイムアウト：TCP 接続のグレースフルクローズ時に、リモート クローズのために許容される時間。この時間が経過すると強制クローズとなります。ハードコードされている値は 1 秒です。
- TCP 接続タイムアウト：リモートピアへの TCP 接続試行を停止するまでの許容時間。ハードコードされている値は 1 秒です。

制約事項

- 隣接接続中にタイマー値またはリトライ回数を変更できます。ただし、進行中のタイマーのトランザクションやゲートキーパーのトランザクションは影響されません。

- すべての RAS タイムアウトを一度に設定できるファシリティはありません。
- H.245 タイマーは、インターワーキングの場合にだけ機能するため、ここでは取り上げません。
- 次の Q.931/H.225 タイマーの設定は SBC ではサポートされていません。
 - Q.931/H.225 オーバーラップ送信タイマー T302
 - Q.931/H.225 オーバーラップ受信タイマー T304
 - Q.931/H.225 状態タイマー T322。
- 次の RAS タイマーの設定は SBC ではサポートされていません。
 - IRQ
 - IRR
 - RAI
 - SCI

T.38 ファクス リレー

この機能は、T.38 fax のメディア リレーに対するサポートを提供します。サポートされる機能は次のとおりです。

- ファクスだけと、ファクスおよび音声のコール
- 音声から T.38 fax への切り替え
- UDPTL を経由する T.38 リレーのみ、および単方向 H.245 チャンネルのみ。

T.38 H.245 - SDP マッピング

T.38 H.245 - SDP マッピングを次に示します。

```
DataApplicationCapability
application
  t38fax
    t38FaxProtocol          m=image 40000 {udptl | tcp} t38
    t38FaxProfile
      fillBitRemoval        a=T38FaxFillBitRemoval
      transcodingJBIG       a=T38FaxTranscodingJBIG
      transcodingMMR        a=T38FaxTranscodingMMR
      version                a=T38FaxVersion:<digits>
      t38FaxRateManagement a=T38FaxRateManagement:{localTCF | transferredTCF}
      t38FaxUdpOptions OPTIONAL
      t38FaxMaxBuffer       a=T38FaxMaxBuffer:<digits>
      t38FaxMaxDatagram     a=T38FaxMaxDatagram:<digits>
      t38FaxUdpEC           a=T38FaxUdpEC:{t38UDPFEC | t38UDPRedundancy}
      t38FaxTcpOptions OPTIONAL
      t38TCPBidirectionalMode [no mapping]
    maxBitRate              a=T38maxBitRate:<digits> (UDP only)
```

メディア リレー機能に必要なパラメータは、ポートとピーク ビット レートだけです。上の例では、これらのパラメータが強調表示されています。したがって、T.38 fax 機能があると、次のように SDP が DBE に送信されます。

```
m=image <remote T.38 port> udptl t38
a=T38maxBitRate:14400
```

インターワーキングの場合には、完全なマッピングを行う必要があります。ただし、これはこのリリースではサポートされません。

H.245 モード要求

音声から fax コールへの切り替えは、RequestMode の交換によって処理されます。H.323-H.323 コールでは、この交換は DBE シグナリングなしにコール レッグ間で透過的にパススルーされます。これにより、エンドポイントは T.38 チャンネルとのオーディオの置換を調整できます。

RAS 最大ビット レート

SBC は、H.323v5 標準に従い、ゲートキーパーとの間で同意した最大ビット レートに関して UDP のカウントを行います。TCP はカウントしません。

H.323 Annex D/T.38 Annex B 相互運用性

T.38 Annex B は、H.323 Annex D のファスト スタート専用（非 H.245）バージョンです。SBC は、Annex B ノードとの相互運用をサポートしていません。

制約事項

- RAS メッセージで SupportedProtocols の「t38FaxAnnexbOnly」フィールドをアダプタイズするように SBC を設定することはできません。SBC はこのフィールドを受信しても無視します。
- TCP や SRTP のトランスポートはサポートされません。
- 双方向 H.245 チャンネル シグナリングはサポートされていません。

Q.931/H.225 パススルー

これは、2 つの H.323 コール レッグ間で Q.931/H.225 のメッセージ要素がパススルーされるようにする機能です。ここでは、Q.931/H.225 メッセージでパススルーできる部分を示した、SBC の「ベース パススルー プロファイル」について説明します。

ベース パススルー プロファイルでは、次の表記法が使用されています。

- このマニュアルには、Q.931/H.225 メッセージの ASN.1 構文が複製されます。
- 次のタグは ASN.1 サブツリーに付加されます。これらは、パススルーの動作を表します。
 - P : 「パススルー」。このサブツリーは、コール レッグ間を不透明に（わからないように）通過します。
 - P* : 「プライバシーに影響するパススルー」。「P」と同様ですが、このサブツリーのパススルーでは、エンドポイントについての情報やリモートの電話番号が明らかになる可能性があります。
 - B : 「ブロック」。このサブツリーは、SBC によって無条件にブロックされ、含まれている情報はすべて失われます。
 - SBC。このサブツリーは SBC によって操作されます。通常、SBC 独自の値に置換されます。

Call Proceeding のパススルー

Call Proceeding メッセージがパススルーされることはありません。ただし、このメッセージのフィールドは抽出されて、アップストリーム コール ログの Progress または Facility に挿入されます。

- Progress が使用されるのは、Call Proceeding に progress インジケータが含まれている場合です。
- その他の場合には、Facility が使用されます。

サポート対象外のメッセージ

次に示す Q.931 メッセージは SBC ではサポートされていません。これは、H.323 で禁止されているため、または対応する機能を現在 SBC がサポートしていないためです。

- Status, Status Enquiry
- SetupAck
- Information
- Notify
- userInformation

プライバシー

CAC ポリシーのプライバシーがイネーブルに設定されているアウトバウンド コール レッグでは、「P*」（プライバシーを含むパススルー）とマークされているサブツリーは自動的にブロックされます。この自動ブロックを設定によって無効にすることはできません。したがって、このフィールドをパススルーさせるためには、プライバシーをディセーブルに設定するしかありません。

プロトコル バージョンの設定

SBC は、メッセージをパススルーする際に、発信メッセージのバージョンを、元のプロトコル メッセージで受信された値よりも低い独自の ASN.1 値に設定します。

Q.931/H.225 ベース パススルー プロファイル

Q931Message	
protocolDiscriminator	SBC
callReferenceValue	SBC
message	
setup	
sendingComplete	P
bearerCapability	P
facility	P
progressIndicator	P
progressIndicator31	P
notificationIndicator	P
display	P*
keypadFacility	P
signal	P
callingPartyNumber	SBC
callingPartySubaddress	B
calledPartyNumber	SBC
calledPartySubaddress	B
redirectingNumber	P*
userUser	

```

h323-uu-pdu
h323-message-body
  setup
    protocolIdentifier      SBC
    h245Address             SBC
    sourceAddress           SBC
    sourceInfo              SBC
    destinationAddress      SBC
    destCallSignalAddress   SBC
    destExtraCallInfo       B
    destExtraCRV            B
    activeMC                 P
    conferenceID             P
    conferenceGoal           P
    callServices             P
    callType                 B
    sourceCallSignalAddress SBC
    remoteExtensionAddress  B
    callIdentifier           P
    h245SecurityCapability  B
    tokens                   B
    cryptoTokens            B
    fastStart                SBC
    mediaWaitForConnect     P
    canOverlapSend          B
    endpointIdentifier       P*
    multipleCalls            SBC
    maintainConnection       SBC
    connectionParameters    P
    language                 P
    presentationIndicator   SBC
    screeningIndicator       SBC
    serviceControl           P
    symmetricOperationRequired P
    capacity                 B
    circuitInfo              SBC
    desiredProtocols         B
    neededFeatures           B
    desiredFeatures          B
    supportedFeatures        B
    parallelH245Control      B
    additionalSourceAddresses B
  nonStandardData          P
  h4501SupplementaryService P
  h245Tunneling            SBC
  h245Control               SBC
  nonStandardControl       P
  callLinkage               P
  tunnelledSignallingMessage P
  provisionalRespToH245Tunneling SBC
  stimulusControl           P
  genericData               P
  user-data                 P
callProceeding
  bearerCapability          P
  facility                  P
  progressIndicator         SBC
  progressIndicator31       SBC
  notificationIndicator     P
  display                   P
  userUser
    h323-uu-pdu
      h323-message-body
        callProceeding

```

protocolIdentifier	SBC
destinationInfo	P*
h245Address	SBC
callIdentifier	P
h245SecurityMode	B
tokens	B
cryptoTokens	B
fastStart	SBC
multipleCalls	SBC
maintainConnection	SBC
fastConnectRefused	SBC
featureSet	B
nonStandardData	P
h4501SupplementaryService	P
h245Tunneling	SBC
h245Control	SBC
nonStandardControl	P
callLinkage	P
tunnelledSignallingMessage	P
provisionalRespToH245Tunneling	SBC
stimulusControl	P
genericData	P
user-data	P
alerting	
bearerCapability	P
facility	P
progressIndicator	SBC
progressIndicator31	SBC
notificationIndicator	P
display	P*
signal	P
userUser	
h323-uu-pdu	
h323-message-body	
alerting	
protocolIdentifier	SBC
destinationInfo	P*
h245Address	SBC
callIdentifier	P
h245SecurityMode	B
tokens	B
cryptoTokens	B
fastStart	SBC
multipleCalls	SBC
maintainConnection	SBC
alertingAddress	P*
presentationIndicator	SBC
screeningIndicator	SBC
fastConnectRefused	SBC
serviceControl	P
capacity	B
featureSet	B
nonStandardData	P
h4501SupplementaryService	P
h245Tunneling	SBC
h245Control	SBC
nonStandardControl	P
callLinkage	P
tunnelledSignallingMessage	P
provisionalRespToH245Tunneling	SBC
stimulusControl	P
genericData	P
user-data	P
connect	

bearerCapability	P
facility	P
progressIndicator	SBC
progressIndicator31	SBC
notificationIndicator	P
display	P*
dateTime	P
connectedNumber	P*
connectedSubaddress	P*
userUser	
h323-uu-pdu	
h323-message-body	
connect	
protocolIdentifier	SBC
h245Address	SBC
destinationInfo	P*
conferenceID	P
callIdentifier	P
h245SecurityMode	B
tokens	B
cryptoTokens	B
fastStart	SBC
multipleCalls	SBC
maintainConnection	SBC
language	P
connectedAddress	P*
presentationIndicator	SBC
screeningIndicator	SBC
fastConnectRefused	SBC
serviceControl	P
capacity	B
featureSet	B
nonStandardData	P
h4501SupplementaryService	P
h245Tunneling	SBC
h245Control	SBC
nonStandardControl	P
callLinkage	P
tunnelledSignallingMessage	P
provisionalRespToH245Tunneling	SBC
stimulusControl	P
genericData	P
user-data	P
progress	
bearerCapability	P
cause	P
facility	P
progressIndicator	SBC
progressIndicator31	SBC
notificationIndicator	P
display	P*
userUser	
h323-uu-pdu	
h323-message-body	
progress	
protocolIdentifier	SBC
destinationInfo	SBC
h245Address	SBC
callIdentifier	P
h245SecurityMode	B
tokens	B
cryptoTokens	B
fastStart	SBC
multipleCalls	SBC

maintainConnection	SBC
fastConnectRefused	SBC
nonStandardData	P
h4501SupplementaryService	P
h245Tunneling	SBC
h245Control	SBC
nonStandardControl	P
callLinkage	P
tunnelledSignallingMessage	P
provisionalRespToH245Tunneling	SBC
stimulusControl	P
genericData	P
user-data	P
releaseComplete	
cause	SBC
facility	P
notificationIndicator	P
display	P*
signal	P
userUser	
h323-uu-pdu	
h323-message-body	
connect	
protocolIdentifier	SBC
reason	SBC
callIdentifier	P
tokens	B
cryptoTokens	B
busyAddress	P*
presentationIndicator	SBC
screeningIndicator	SBC
capacity	B
serviceControl	P
featureSet	B
nonStandardData	P
h4501SupplementaryService	P
h245Tunneling	SBC
h245Control	SBC
nonStandardControl	P
callLinkage	P
tunnelledSignallingMessage	P
provisionalRespToH245Tunneling	SBC
stimulusControl	P
genericData	P
user-data	
facility	
facility	P
notificationIndicator	P
display	P*
callingPartyNumber	P*
calledPartyNumber	P*
userUser	
h323-uu-pdu	
h323-message-body	
facility	
protocolIdentifier	SBC
alternativeAddress	B
alternativeAliasAddress	P
conferenceID	P
reason	P
callIdentifier	P
destExtraCallInfo	P
remoteExtensionAddress	P
tokens	B

cryptoTokens	B
conferences	P
h245Address	SBC
fastStart	SBC
multipleCalls	SBC
maintainConnection	SBC
fastConnectRefused	SBC
serviceControl	P
circuitInfo	B
featureSet	B
destinationInfo	P*
h245SecurityMode	B
empty	
nonStandardData	P
h4501SupplementaryService	P
h245Tunneling	SBC
h245Control	SBC
nonStandardControl	P
callLinkage	P
tunnelledSignallingMessage	P
provisionalRespToH245Tunneling	SBC
stimulusControl	P
genericData	P
user-data	P

制約事項

- Q.931/H.225 からのメッセージ エLEMENTのうち、この項に記載されていないものはパススルーできません。
- セキュリティ トークンのパススルーはサポートされていません。

H.323 プライバシー

H.323 プライバシー機能を使用すると、Q.931/H.225 メッセージに隠れている ID を呼び出すことができます。この機能が実装されている場合、SBC は、リモートの発信側または着信側についての情報を示す Q.931/H.225 メッセージ エLEMENTを除去してから、エンドポイントに渡します。



(注)

プライバシーに影響する Q.931/H.225 メッセージ エLEMENTは、H.323 パススルー プロファイルに定義されています。

SBC がメッセージにプライバシー サービスを適用するのは、ユーザからのプライバシー要求がメッセージに含まれている場合、または SBC に対する CAC ポリシーで発信側または着信側単位でプライバシーをイネーブルにするように設定されている場合です。ただし、プライバシーの設定フィールドがデフォルト値に設定されている場合には、SBC はそのメッセージにプライバシー サービスを適用せずに次のコール レッグにメッセージを転送します。H.323 プライバシー サービスを隣接単位で提供するように SBC を設定することもできます。

SBC は、H.323 プライバシー サービスを提供する際に次のルールを適用します。

- プライベート情報を見逃すように H.323 隣接が設定されている場合、着信メッセージがプライバシー サービスを要求していても、また CAC ポリシーでプライバシーがイネーブルに設定されていても、SBC はプライバシー サービスを適用しません。

- H.323 隣接はプライベート情報を見逃すように設定されていないが、CAC ポリシーはプライバシーをイネーブルにするように設定されている場合、SBC は発信メッセージにプライバシー サービスを適用します。
- 着信メッセージによりプライバシー サービスが要求されているが、CAC ポリシーでは、プライバシーをイネーブルにするように設定されていない場合、プライバシー サービスを適用するように隣接が設定されていれば、SBC はこのサービスを適用します。
- CAC ポリシーと隣接のどちらも、プライバシー サービスを適用するように設定されていないときに、着信メッセージによりプライバシー サービスが要求された場合、SBC はプライバシー サービスを適用せず、プライベート情報のパススルーを許可します。

制限事項

- SBC は、H.245 メッセージ、および RAS メッセージに H.323 プライバシー サービスを適用しません。
- 現在、着信側のプライバシーに関する CAC ポリシーは、`connectedNumber` がある場合に限り、「接続時」に H.323 シグナリング スタックに対して使用できます。したがって、`connectedNumber` がない場合、コールの接続前または接続後にパススルーされる Q.931 プロトコル メッセージに着信側のプライバシー サービスは適用されません。この制限のため、SBC はプライバシー サービス要求を適用せずに、Q.931 Alerting、Q.931Progress、および Q.931 Release Complete の各メッセージを転送します。
- インターワーキング コールの場合、SBC は、CAC ポリシーに基づくプライバシー要求だけを適用します。

H.323 機能の設定

H.245 個別制御チャネルの設定

このコマンドを使用すると、隣接単位でトンネリングをディセーブルにできます。この機能は、トンネリングによって混乱するような既存デバイスとの相互運用に役立ちます。このコマンドは、着信コールと発信コールの両方を制御します。

手順の概要

1. `configure`
2. `sbc service-name`
3. `sbc`
4. `adjacency h323 adjacency-name`
5. `h245 tunnel disable`
6. `commit`
7. `exit`

手順の詳細

	コマンドまたはアクション	目的
ステップ1	<code>configure</code> 例: RP/0/0/CPU0:router# configure	グローバル コンフィギュレーション モードをイネーブルにします。
ステップ2	<code>sbc service-name</code> 例: RP/0/0/CPU0:router(config)# sbc mysbc	SBC サービスのモードを開始します。 <i>service-name</i> 引数を使用して、SBC の名前を定義します。
ステップ3	<code>sbe</code> 例: RP/0/0/CPU0:router(config-sbc)# sbe	SBC の Signaling Border Element (SBE) 機能のモードを開始します。
ステップ4	<code>adjacency h323 adjacency-name</code> 例: RP/0/0/CPU0:router(config-sbc-sbe)# adjacency h323 2651XM-5	SBE H.323 隣接のモードを開始します。 <i>adjacency-name</i> 引数を使用して、H.323 隣接の名前を定義します。
ステップ5	<code>h245 tunnel disable</code> 例: RP/0/0/CPU0:router(config-sbc-sbe-adj-h323)# h245 tunnel disable	隣接単位でトンネリングをディセーブルにします。これにより、トンネリングによって混乱させられた既存デバイスとの相互運用が容易になります。このコマンドは、着信コールと発信コールの両方を制御します。 デフォルトでは、トンネリングはイネーブルに設定されています。
ステップ6	<code>commit</code> 例: RP/0/0/CPU0:router(config-sbc-sbe-adj-h323)# commit	設定変更を保存します。実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、 commit コマンドを使用します。
ステップ7	<code>exit</code> 例: RP/0/0/CPU0:router(config-sbc-sbe-adj-h323)# exit	メディア アドレス モードを終了し、DBE モードに戻ります。

RAS テクノロジー プレフィックスの設定

この機能によって、隣接ごとに RAS テクノロジー プレフィックスを設定し、ゲートキーパーにこのプレフィックスを登録できるようになります。RAS テクノロジー プレフィックスは 1 ~ 32 桁のダイヤル番号から構成されます。

手順の概要

1. `configure`
2. `sbc service-name`

3. **sbe**
4. **adjacency h323 adjacency-name**
5. **tech-prefix tech-prefix**
6. **commit**
7. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ1	configure 例： RP/0/0/CPU0:router# configure	グローバル コンフィギュレーション モードをイネーブルにします。
ステップ2	sbc service-name 例： RP/0/0/CPU0:router(config)# sbc mysbc	SBC サービスのモードを開始します。 <i>service-name</i> 引数を使用して、SBC の名前を定義します。
ステップ3	sbe 例： RP/0/0/CPU0:router(config-sbc)# sbe	SBC の Signaling Border Element (SBE) 機能のモードを開始します。
ステップ4	adjacency h323 adjacency-name 例： RP/0/0/CPU0:router(config-sbc-sbe)# adjacency h323 2651XM-5	SBE H.323 隣接のモードを開始します。 <i>adjacency-name</i> 引数を使用して、H.323 隣接の名前を定義します。
ステップ5	tech-prefix tech-prefix 例： RP/0/0/CPU0:router(config-sbc-sbe-adj-h323)# tech-prefix 32#	隣接ごとに RAS テクノロジー プレフィックスを設定し、ゲートキーパーにこのプレフィックスを登録します。RAS テクノロジー プレフィックスは 1 ～ 32 桁のダイヤル番号と、それに続くシャープ (#) 記号から構成されます。 デフォルトではテクノロジー プレフィックスは設定されていません。
ステップ6	commit 例： RP/0/0/CPU0:router(config-sbc-sbe-adj-h323)# commit	設定変更を保存します。実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、 commit コマンドを使用します。
ステップ7	exit 例： RP/0/0/CPU0:router(config-sbc-sbe-adj-h323)# exit	メディア アドレス モードを終了し、DBE モードに戻ります。

ユーザ プロトコル タイマー制御の設定

手順の概要

1. `configure`
2. `sbc service-name`
3. `sbe`
4. `h323 | adjacency h323 adjacency-name`
5. `adjacency timeout`
6. `h225 timeout`
7. `ras retry`
8. `ras rrq ttl`
9. `ras rrq keepalive`
10. `ras timeout`
11. `commit`
12. `exit`
13. `show services sbc sbc-name sbe h323 timers`

手順の詳細

	コマンドまたはアクション	目的
ステップ1	<code>configure</code> 例： RP/0/0/CPU0:router# <code>configure</code>	グローバル コンフィギュレーション モードをイネーブルにします。
ステップ2	<code>sbc service-name</code> 例： RP/0/0/CPU0:router(config)# <code>sbc mysbc</code>	SBC サービスのモードを開始します。 <code>service-name</code> 引数を使用して、SBC の名前を定義します。
ステップ3	<code>sbe</code> 例： RP/0/0/CPU0:router(config-sbc)# <code>sbe</code>	SBC の Signaling Border Element (SBE) 機能のモードを開始します。
ステップ4	<code>h323 adjacency h323 adjacency-name</code> 例： RP/0/0/CPU0:router(config-sbc-sbe)# <code>adjacency h323 2651XM-5</code>	全 H.323 隣接または特定の H.323 隣接のいずれかのモードを開始します。 <code>adjacency-name</code> 引数を使用して、H.323 隣接の名前を定義します。
ステップ5	<code>adjacency timeout</code> 例： RP/0/0/CPU0:router(config-sbc-sbe-adj-h323)# <code>adjacency timeout 10000</code>	接続障害が発生した場合に、SBC がリモート シグナリング ピアへの再接続と、そのピアからのキープアライブ メッセージの受信を続ける時間をミリ秒単位で定義します。 値の範囲は 10000 ~ 30000 です。

コマンドまたはアクション	目的
<p>ステップ6 <code>h225 timeout [establishment timeout value proceeding timeout value setup timeout value</code></p> <p>例: RP/0/0/CPU0:router(config-sbc-sbe-adj-h323)# h225 timeout establishment 250000</p>	<p>H.225 メッセージの受信待ち時間を定義します。</p> <ul style="list-style-type: none"> • establishment timeout value : h225 establishment ステートのタイムアウト値 (ミリ秒単位)。デフォルト値は 180000 です。値の範囲は 30000 ~ 300000 です。 • proceeding timeout value : h225 proceeding ステートのタイムアウト値 (ミリ秒単位)。10000。値の範囲は 1000 ~ 30000 です。 • setup timeout value : h225 setup のタイムアウト値 (ミリ秒単位)。デフォルト値は 4000 です。値の範囲は 1000 ~ 30000 です。
<p>ステップ7 <code>ras retry [arq brq drq grq rrq urq] retry count</code></p> <p>例: RP/0/0/CPU0:router(config-sbc-sbe-adj-h323)# ras retry arq 2 ras retry brq 2 ras retry drq 2 ras retry rrq 2 ras retry urq 2</p>	<p>RAS メッセージの送信に失敗した場合のメッセージ再送信試行回数を定義します。</p> <ul style="list-style-type: none"> • arq retry count : ARQ トランザクションの再試行回数。 • brq retry count : BRQ トランザクションの再試行回数。 • drq retry count : DRQ トランザクションの再試行回数。 • grq retry count : GRQ トランザクションの再試行回数。 • rrq retry count : RRQ トランザクションの再試行回数。 • urq retry count : URQ トランザクションの再試行回数。 <p>値の範囲は 0 ~ 30 です。</p>
<p>ステップ8 <code>ras rrq ttl</code></p> <p>例: RP/0/0/CPU0:router(config-sbc-sbe-adj-h323)# ras rrq ttl 100</p>	<p>登録要求 (RRQ) メッセージの存続可能時間 (TTL) をミリ秒単位で定義します。</p> <p>デフォルト値は 60 です。値の範囲は 16 ~ 300 です。</p>
<p>ステップ9 <code>ras rrq keepalive</code></p> <p>例: RP/0/0/CPU0:router(config-sbc-sbe-adj-h323)# ras rrq keepalive 100000</p>	<p>登録要求 (RRQ) キープアライブ メッセージの時間をミリ秒単位で定義します。</p> <p>デフォルト値は 45000 です。値の範囲は 15000 ~ 150000 です。</p>

	コマンドまたはアクション	目的
ステップ 10	<pre> ras timeout [arq brq drq grq rrq urq] timeout 例: RP/0/0/CPU0:router(config-sbc-sbe-adj-h323)# ras timeout arq 1000 ras timeout brq 1000 ras timeout drq 1000 ras timeout grq 1000 ras timeout rrq 1000 ras timeout urq 1000 </pre>	<p>すべての RAS メッセージで共通に使用されるタイムアウト値をミリ秒単位で定義します。</p> <ul style="list-style-type: none"> • arq timeout : ARQ トランザクションのタイムアウト値。 • brq timeout : BRQ トランザクションのタイムアウト値。 • drq timeout : DRQ トランザクションのタイムアウト値。 • grq timeout : GRQ トランザクションのタイムアウト値。 • rrq timeout : RRQ トランザクションのタイムアウト値。 • urq timeout : URQ トランザクションのタイムアウト値。 <p>デフォルトは 5000 です。値の範囲は 1000 ~ 45000 です。</p>
ステップ 11	<pre> commit 例: RP/0/0/CPU0:router(config-sbc-sbe-adj-h323)# commit </pre>	<p>設定変更を保存します。実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、commit コマンドを使用します。</p>
ステップ 12	<pre> exit 例: RP/0/0/CPU0:router(config-sbc-sbe-adj-h323)# exit </pre>	<p>H.323 グローバル モード、または指定された隣接モードを終了します。</p>
ステップ 13	<pre> show services sbc service-name sbe h323 timers 例: RP/0/0/CPU0:router# show services sbc mysbc sbe h323 timers </pre>	<p>すべての H.323 タイマーの値を表示します。</p>

H.323 プライバシーの設定

この機能により、SBC は、アウトバウンド メッセージに H.323 プライバシー サービスを適用することができます。

手順の概要

1. **configure**
2. **sbc service-name**
3. **sbe**
4. **adjacency h323 adjacency-name**

5. `allow private info`
6. `privacy restrict outbound`
7. `commit`
8. `exit`

手順の詳細

	コマンドまたはアクション	目的
ステップ1	<code>configure</code> 例： RP/0/0/CPU0:router# <code>configure</code>	グローバル コンフィギュレーション モードをイネーブルにします。
ステップ2	<code>sbc service-name</code> 例： RP/0/0/CPU0:router(config)# <code>sbc mysbcb</code>	SBC サービスのモードを開始します。 <i>service-name</i> 引数を使用して、SBC の名前を定義します。
ステップ3	<code>sbe</code> 例： RP/0/0/CPU0:router(config-sbc)# <code>sbe</code>	SBC の Signaling Border Element (SBE) 機能のモードを開始します。
ステップ4	<code>adjacency h323 adjacency-name</code> 例： RP/0/0/CPU0:router(config-sbc-sbe)# <code>adjacency h323 2651XM-5</code>	SBE H.323 隣接のモードを開始します。 <i>adjacency-name</i> 引数を使用して、H.323 隣接の名前を定義します。
ステップ5	<code>allow private info</code> 例： RP/0/0/CPU0:router(config-sbc-sbe-adj-h323)# <code>allow private info</code>	プライバシー サービスを適用するように CAC ポリシーが設定されていても、またユーザがプライバシー サービスを要求していても、隣接が送信するメッセージのプライベート情報を見逃すように H.323 隣接を設定します。隣接によるプライベート情報の送信を見逃すことを止めるように H.323 隣接を設定するには、このコマンドの no 形式を使用します。
ステップ6	<code>privacy restrict outbound</code> 例： RP/0/0/CPU0:router(config-sbc-sbe-adj-h323)# <code>privacy restrict outbound</code>	ユーザがプライバシー サービスを要求した場合に、アウトバウンドメッセージにプライバシー制限を適用するように H.323 隣接を設定します。隣接によるプライベート情報メッセージの送信を見逃すように H.323 隣接を設定するには、このコマンドの no 形式を使用します。

	コマンドまたはアクション	目的
ステップ7	<code>commit</code> 例: RP/0/0/CPU0:router(config-sbc-sbe-adj-h323)# commit	設定変更を保存します。実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、 commit コマンドを使用します。
ステップ8	<code>exit</code> 例: RP/0/0/CPU0:router(config-sbc-sbe-adj-h323)# exit	SBE H.323 グローバル モード、または指定された隣接モードを終了します。

H.245 個別制御チャネル、および RAS テクノロジー プレフィックス : 例

```
configure
sbc mysbc
sbe
adjacency h323 h323-fxs-1b
signaling-address ipv4 88.110.128.13
signaling-port 1720
remote-address ipv4 10.0.0.0/8
signaling-peer 10.124.2.2
signaling-peer-port 1720
account h323-fxs-1b
tech-prefix 2#
h245-tunnel disable
attach
commit
exit
```

ユーザ プロトコル タイマー制御の設定 : 例

```
configure
sbc mysbc
sbe
adjacency h323 abcd
adjacency timeout 10000
h225 timeout establishment 40000
adjacency timeout 10000?
h225 timeout ?
  establishment h225 establishment state timeout value.
  proceeding h225 proceeding state timeout value.
  setup h225 setup timeout value.
h225 timeout proceeding 30000
h225 timeout setup 30000
ras ?
  retry RAS retry configuration.
  rrq RRQ (Registration Request) configuration.
  timeout RAS timeout configuration.
ras retry ?
  arq Retry count for an ARQ transaction.
  brq Retry count for an BRQ transaction.
  drq Retry count for an DRQ transaction.
  grq Retry count for an GRQ transaction.
```



```

    rrq  Retry count for an RRQ transaction.
    urq  Retry count for an URQ transaction.
ras retry arq 2
ras retry brq 2
ras retry drq 2
ras retry rrq 2
ras retry urq 2
ras rrq ?
    keepalive  Rate for keepalive msgs to refresh an H323 adjacency registration.
    ttl        TTL (time to live) value for an RRQ request.
ras rrq keepalive ?
    <15000-150000>  Keepalive refresh time in milliseconds - default: 45000 ras rrq
keepalive 15000
ras rrq ttl ?
    <16-300>  TTL value in seconds - default: 60
ras rrq ttl 30
adjacency timeout 30000
ras timeout ?
    arq  Timeout value for an ARQ transaction.
    brq  Timeout value for an BRQ transaction.
    drq  Timeout value for an DRQ transaction.
    grq  Timeout value for an GRQ transaction.
    rrq  Timeout value for an RRQ transaction.
    urq  Timeout value for an URQ transaction.
ras timeout arq ?
    <1000-45000>  Timeout value in milliseconds - default: 5000
ras timeout arq 1000
ras timeout brq 1000
ras timeout drq 1000
ras timeout grq 1000
ras timeout rrq 1000
ras timeout urq 1000

```

その他の関連資料

次の各項では、H.323 サポートの設定に関連する参考資料を示します。

関連資料

関連項目	マニュアル タイトル
Cisco IOS XR マスター コマンド リファレンス	『Cisco IOS XR Master Commands List』
Cisco IOS XR SBC インターフェイス コンフィギュレーション コマンド	『Cisco IOS XR Session Border Controller Command Reference』
Cisco IOS XR ソフトウェアを使用するルータを初回に起動し設定するための情報	『Cisco IOS XR Getting Started Guide』
Cisco IOS XR コマンド モード	『Cisco IOS XR Command Mode Reference』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	<p>Cisco IOS XR ソフトウェアを使用して MIB の場所を特定してダウンロードするには、次の URL にある Cisco MIB Locator を使用して、[Cisco Access Products] メニューからプラットフォームを選択します。</p> <p>http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</p>

RFC

RFC	タイトル
RFC 2833	『RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals』

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポート Web サイトでは、製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクなどの、数千ページに及ぶ技術情報が検索可能です。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html