PSTN フォールバック

PSTN フォールバック機能は IP ネットワーク内の輻輳をモニタし、コールを公衆電話交換網（PSTN）にリダイレクトするか、またはネットワーク輻輳に基づいてコールを拒否します。この機能ではまた、ICMP ping メカニズムを使用してネットワーク接続の損失を検出した後、コールを再ルーティングすることもできます。フォールバック サブシステムには、さまざまな宛先の Calculated Planning Impairment Factor（ICPIF）または遅延や損失の値を保持するネットワーク トラフィック キャッシュがあります。既知の宛先への新しい各コールは許可されるのをプローブ上で待つ必要がなく、通常、その値は以前のコールからキャッシュされるため、パフォーマンスが向上します。

ICPIF では、音声パスに沿った機器ごとの劣化係数を計算した後、それらを累計して合計の劣化値を取得します。詳細については、国際電気通信連合（ITU）標準の G.113 を参照してください。ITU では、ノイズ、遅延、エコーなどの劣化のタイプに値が割り当てられます。

機能情報

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

プラットフォームのサポートおよびソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、Cisco IOS および Catalyst OS ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

内容

このマニュアルの構成は、次のとおりです。

PSTN フォールバックに関する情報

ここでは、PSTN フォールバック機能に関する次の情報を提供します。

サービス保証エージェント

サービス保証エージェント（SAA）は、設定された IP アドレスの遅延、ジッター、およびパケット損失情報を提供するためのネットワーク輻輳分析メカニズムです。SAA は、ユーザ データグラム プロトコル（UDP）上で定義されたクライアント/サーバ プロトコルに基づいています。UDP は、IP プロトコル スタックのコネクションレス トランスポート層プロトコルです。UDP は、確認応答や配信保証なしでデータグラムを交換する単純なプロトコルです。エラー処理と再送信は、他のプロトコルで処理する必要があります。SAA プローブ パケットは、オーディオ UDP ポート範囲の上端からランダムに選択されたポート上に出力されます。

SAA プローブが収集する情報は、フォールバック キャッシュ内に保存される ICPIF または遅延や損失の値を計算するために使用されます。これらの値は、キャッシュが期限切れになるか、またはオーバーフローするまでこのキャッシュ内に残ります。エントリが期限切れになるまで、プローブはその特定の宛先に定期的に送信されます。この時間間隔はユーザが設定できます。

この機能拡張を使用すると、ネットワーク拒否（失われたパケットや、送信に時間がかかりすぎるパケットなど）の原因を示すコードを設定することもできます。49 のデフォルトの原因コードは、Quality of Service が使用できないことを示すメッセージ **qos-unavail** を表示します。

（注） Cisco IOS ソフトウェアの Cisco SAA 機能は以前、Response Time Reporter（RTR）と呼ばれていました。「PSTN フォールバックの設定方法」の項では、コマンドライン インターフェイスが引き続き RTR プローブ（現在では実際には SAA プローブ）を設定するためのキーワード **rtr** を使用していることに注意してください。

PSTN フォールバックのアプリケーション

PSTN フォールバック機能および機能拡張には、次の利点があります。

- コールのセットアップ時にデータ ネットワークが輻輳状態になっているときは、コールを自動的に再ルーティングします。
- サービス プロバイダーが、コール アドミッション時に Voice over IP（VoIP）ユーザに会話の品質に関する妥当な保証を提供できるようにします。
- 設定された IP アドレスの遅延、ジッター、およびパケット損失情報を提供します。
- 以前のコールのコール値をキャッシュします。新しいコールは、許可される前にプローブ結果を待つ必要がありません。
- コール拒否のタイプを示すユーザ設定可能な原因コードを表示できるようにします。

PSTN フォールバックの制限

PSTN フォールバック機能には、次の制限があります。

- ネットワーク輻輳を検出しても、PSTN フォールバック機能は既存のコールに対して何も行いません。後続のコールに影響を与えるだけです。
- システム当たりに許可される ICPIF または遅延や損失の値は 1 つだけです。
- 新しい IP 宛先への最初のコールでは、わずかな追加コール設定の遅延が予想されます。

注意 ゲートウェイ内で **call fallback active** を設定すると、コールの送信先の他の（ターゲット）ゲートウェイに対する SAA ジッター プローブが作成されます。call fallback active が正しく動作するには、そのターゲット ゲートウェイの設定に **rtr responder** コマンド（12.3(14)T よりも前の Cisco IOS Release）または **ip sla monitor responder** コマンド（Cisco IOS Release 12.3(14)T 以降）が含まれている必要があります。各ターゲット ゲートウェイの設定にこれらのコマンドのいずれかが含まれていない場合は、そのターゲット ゲートウェイへのコールが失敗します。

PSTN フォールバックの設定方法

ここでは、次の手順について説明します（各手順は任意または必須のどちらかとして示されています）。

- SAA プローブに MD5 認証を使用するコール フォールバックの設定（必須）
- 代替ダイヤル ピアへのフォールバックを使用しない宛先モニタリングの設定（任意）
- コール フォールバックのキャッシュ パラメータの設定（任意）
- コール フォールバックのジッター プローブ パラメータの設定（任意）
- コール フォールバックのプローブ タイムアウトと重みパラメータの設定（任意）
- コール フォールバックのしきい値パラメータの設定（任意）
- コール フォールバックの待機タイムアウトの設定（任意）
- VoIP 代替パス フォールバック SNMP トラップの設定（任意）
- IP 宛先をモニタするための ICMP ping の設定（任意）

SAA プローブに MD5 認証を使用するコール フォールバックの設定

SAA プローブに MD5 認証を使用するようにコール フォールバックを設定するには、次のコマンドを使用します。

手順の概要

1. **enable**
2. **config terminal**
3. **call fallback active**
4. **call fallback key-chain** *name-of-chain*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**call fallback active** **例：** `Router(config)# call fallback active`	ネットワーク輻輳が発生した場合の代替ダイヤルピアへの PSTN フォールバック機能をイネーブルにします。
ステップ 4	**call fallback key-chain** *name-of-chain* **例：** `Router(config)# call fallback key-chain sample`	サービス保証エージェント（SAA）プローブを送受信するのためのメッセージ ダイジェスト アルゴリズム 5（MD5）認証の使用を指定します。

代替ダイヤル ピアへのフォールバックを使用しない宛先モニタリングの設定

代替ダイヤル ピアへのフォールバックを使用しない宛先モニタリングを設定するには、次のコマンドを使用します。

手順の概要

1. **enable**
2. **config terminal**
3. **call fallback monitor**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**call fallback monitor** **例：** `Router(config)# call fallback monitor`	代替ダイヤル ピアへのフォールバックを使用しない宛先モニタリングをイネーブルにします。

コール フォールバックのキャッシュ パラメータの設定

コール フォールバックのキャッシュ パラメータを設定するには、次のコマンドを使用します。

手順の概要

1. **enable**
2. **config terminal**
3. **call fallback cache-size** *number*
4. **call fallback cache-timeout** *seconds*
5. **clear call fallback cache** [*ip-address*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**call fallback cache-size** *number* **例：** `Router(config)# call fallback cache-size 5`	コール フォールバックのキャッシュ サイズを指定します。
ステップ 4	**call fallback cache-timeout** *seconds* **例：** `Router(config)# call fallback cache-timeout 300`	キャッシュ エントリが消去されるまでの時間（秒単位）を指定します。デフォルト値：600。
ステップ 5	**clear call fallback cache** [*ip-address*] **例：** `Router(config)# clear call fallback cache 10.1.1.1`	キャッシュ内のすべての IP アドレスまたは特定の IP アドレスの現在の ICPIF 推定値をクリアします。

コール フォールバックのジッター プローブ パラメータの設定

コール フォールバックのジッター プローブ パラメータを設定するには、次のコマンドを使用します。

手順の概要

1. **enable**
2. **config terminal**
3. **call fallback jitter-probe num-packets** *number-of-packets*
4. **call fallback jitter-probe precedence** *precedence*
   または
   call fallback jitter-probe dscp *dscp-number*
5. **call fallback jitter-probe priority-queue**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**call fallback jitter-probe num-packets** *number-of-packets* **例：** `Router(config)# call fallback jitter-probe num-packets 10`	ジッターのパケット数を指定します。デフォルトは 15 です。

	コマンドまたはアクション	目的

ステップ 4	**call fallback jitter-probe precedence** *precedence*
	または
	call fallback jitter-probe dscp *dscp-number*
	
	例：
	`Router(config)# call fallback jitter-probe precedence 2`
	または
	`Router(config)# call fallback jitter-probe dscp 2`
		ジッター プローブ送信の処理を指定します。デフォルトは 2 です。
		ジッター プローブ送信の DiffServ コード ポイント（dscp）パケットを指定します。
		（注） **call fallback jitter-probe precedence** コマンドは、**call fallback jitter-probe dscp** コマンドと互いに排他的です。ルータ上でイネーブルにできるのは、これらのコマンドのうちの 1 つだけです。通常は、**call fallback jitter-probe precedence** コマンドがイネーブルになっています。**call fallback jitter-probe dscp** コマンドが設定されている場合は、precedence 値が DSCP 値で置き換えられます。DSCP をディセーブルにして、デフォルトのジッター プローブ precedence 値を復元するには、**no call fallback jitter-probe dscp** コマンドを使用します。

ステップ 5	**call fallback jitter-probe priority-queue** **例：** `Router(config)# call fallback jitter-probe priority-queue`	ジッター プローブのキューにプライオリティを割り当てます。

コール フォールバックのプローブ タイムアウトと重みパラメータの設定

コール フォールバックのプローブ タイムアウトと重みパラメータを設定するには、次のコマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **call fallback probe-timeout** *seconds*
4. **call fallback instantaneous-value-weight** *weight*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**call fallback probe-timeout** *seconds* **例：** `Router(config)# call fallback probe-timeout 20`	SAA プローブのタイムアウト（秒単位）を設定します。デフォルトは 30 です。
ステップ 4	**call fallback instantaneous-value-weight** *percent* **例：** `Router(config)# call fallback instantaneous-value-weight 50`	コール要求のために、キャッシュ内に登録されている最後の 2 つのプローブの平均を取るようにコール フォールバック サブシステムを設定します。 • *percent*：パーセンテージで表された、瞬時値の重み。範囲：0 ～ 100。デフォルトは 66 です。

コール フォールバックのしきい値パラメータの設定

コール フォールバックのしきい値パラメータを設定するには、次のコマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **call fallback threshold delay** *delay-value* **loss** *loss-value*
   または
   call fallback threshold icpif *threshold-value*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	**call fallback threshold delay** *delay-value* **loss** *loss-value*
	または
	call fallback threshold icpif *threshold-value*
	
	例：
	`Router(config)# call fallback threshold delay 100 loss 150`
	または
	`Router(config)# call fallback threshold icpif 100`
		パケット遅延や損失の値を使用するようにフォールバックのしきい値を指定します。デフォルト設定はありません。
		（注） **call fallback threshold delay loss** コマンドで設定される遅延の量が、**call fallback wait-timeout** コマンドで設定された待ち時間の値の量の半分を超えないようにしてください。そうしないと、しきい値の遅延が正しく機能しません。**call fallback wait-timeout** コマンドのデフォルト値は 300 ミリ秒に設定されているため、**call fallback threshold delay loss** コマンドでは最大 150 ミリ秒の遅延を設定できます。これより高いしきい値を設定したい場合は、**call fallback wait-timeout** コマンドを使用して、待ち時間の遅延をデフォルト値（300 ミリ秒）から増やす必要があります。
		
		ネットワーク トラフィックに Calculated Planning Impairment Factor（ICPIF）のしきい値を使用するようにフォールバックのしきい値を指定します。

コール フォールバックの待機タイムアウトの設定

コール フォールバックの待機タイムアウト パラメータを設定するには、次のコマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **call fallback wait-timeout** *milliseconds*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**call fallback wait-timeout** *milliseconds* **例：** `Router(config)# call fallback wait-timeout 200`	プローブへの応答の待機タイムアウト間隔（ミリ秒）を設定します。デフォルトは 300 ミリ秒です。 **（注）** **call fallback wait-timeout** コマンドで設定される待ち時間の期間が、常に **call fallback threshold delay loss** コマンドで設定されたしきい値の遅延時間の量の 2 倍以上になるようにしてください。そうしないと、プローブが失敗します。 **call fallback threshold delay loss** コマンドで設定される遅延が一方向の遅延に対応するのに対して、**call fallback wait-timeout** コマンドで設定される待ち時間の期間はラウンドトリップ遅延に対応します。しきい値の遅延時間は、待ち時間の値の半分に設定してください。

VoIP 代替パス フォールバック SNMP トラップの設定

VoIP 代替パス フォールバック SNMP トラップ機能によって、簡易ネットワーク管理プロトコル（SNMP）トラップの生成機能が追加されます。この機能は、ネットワークの状態が設定済みのしきい値を満たすことができなかったためにフォールバック サブシステムによってコールがリダイレクトまたは拒否されたときに、SNMP 通知トラップを提供するために、フォールバック サブシステムの上に構築されます。SNMP トラップは、コールが公衆電話交換網（PSTN）または代替 IP ポートにリダイレクトされた場合にのみトリガーすることによって、コール ステータスに関する不必要なメッセージで管理システムにフラッディングを引き起こすことなく VoIP 管理ステータス MIB 情報を提供します。

コールは、WAN 接続の損失、遅延、パケット損失、ジッターなどのネットワークの問題のために拒否される場合があります。このリリースでは、この機能は H.323 での VoIP シグナリング プロトコルのみをサポートします。

この機能は、発信側ゲートウェイと終端側ゲートウェイで設定する必要があります。SNMP トラップ パラメータを設定するには、次のコマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **call fallback active**
4. **snmp-server enable traps voice fallback**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**call fallback active** **例：** `Router(config)# call fallback active`	ネットワーク輻輳が発生した場合の代替ダイヤルピアへの PSTN フォールバック機能をイネーブルにします。
ステップ 4	**snmp-server enable traps voice fallback** **例：** `Router(config)# snmp-server enable traps voice fallback`	SNMP トラップ パラメータを設定します。

次の作業

終端側の音声ゲートウェイで **rtr responder** コマンドを設定します。終端側ゲートウェイで **rtr responder** がイネーブルになっている場合は、発信側ゲートウェイがネットワークの状態を確認するために終端側ゲートウェイに Response Time Report（RTR）プローブを送信すると、終端側ゲートウェイはそのプローブ要求に応答します。

コール フォールバックのマップ パラメータの設定

call fallback map コマンド オプションは、ターゲット ネットワークの集約/統合モードを提供します。たとえば、4 台の個別の音声ゲートウェイ ルータが個別の LAN-to-WAN アクセス ルータを経由してリモート LAN 上でまとめて接続されている場合は、map オプションを使用すると、1 台のリモート WAN アクセス ルータに 1 つのプローブを送信できます（4 台の音声ゲートウェイ ルータの IP アドレ

スごとに個別のプローブを保持する必要はありません)。リモート アクセス ルータと音声ゲートウェイ ルータは同じリモート LAN 上でまとめて接続されているため、アクセス ルータへのプローブにより、個別の音声ゲートウェイ ルータへのプローブに対する同様の結果が返されます。

コール フォールバックのマップ パラメータを設定するには、次のコマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **call fallback map** *map* **target** *ip-address* **address-list** *ip-address1 ip-address2 ... ip-address7*
   または
   call fallback map *map* **target** *ip-address subnet ip-network netmask*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**call fallback map** *map* **target** *ip-address* **address-list** *ip-address1 ip-address2 ... ip-address7* または **call fallback map** *map* **target** *ip-address subnet ip-network netmask*	ルータの背後に位置する複数の宛先ピアへの距離の（IP アドレスごとの）キャッシュ テーブルを保持するコール フォールバック ルータを指定します。 • *map*：フォールバック マップ。範囲は 1 ～ 16 です。デフォルトはありません。 • **target** *ip-address*：ターゲット IP アドレス。 • *ip-address1 ip-address2 ... ip-address7*：キャッシュ テーブル内に保持されている IP アドレスを一覧表示します。IP アドレスの最大数は 7 です。 ルータの背後に位置する複数の宛先ピアへの距離の（サブネット アドレスごとの）キャッシュ テーブルを保持するコール フォールバック ルータを指定します。

IP 宛先をモニタするための ICMP ping の設定

この機能は、RTR をサポートしていない可能性のある VoIP ネットワーク内の IP 宛先をモニタするためにイネーブルにされます。このモニタリングは ICMP ping と呼ばれます。RTR または ICMP ping に基づき、結果によってダイヤルピアの動作状態が変更されます。また、この項で説明する設定では、VoIP ダイヤルピアの下に設定されている次のセッション ターゲットのモニタリングに対するサポートも提供されます。

- DNS
- IP バージョン 4
- SIP サーバ
- enum

IP 宛先に ping を実行するためのコール フォールバックのモニタ プローブを設定するには、次の作業のいずれかを完了します。

- call fallback icmp-ping コマンドと monitor probe コマンドのダイヤル ピア設定
- call fallback icmp-ping コマンドのグローバル設定
- busyout monitor probe icmp-ping コマンドの音声ポート設定
- busyout monitor probe icmp-ping コマンドの音声クラス設定

call fallback icmp-ping コマンドと monitor probe コマンドのダイヤル ピア設定

ICMP ping を使用して IP 宛先をモニタするためのダイヤルピア パラメータを設定するには、この作業を完了します。この設定は、VoIP ダイヤル ピアにのみ適用されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* **voip**
4. **call fallback** [**icmp-ping** | **rtr**]
5. **monitor probe** {**icmp-ping** | **rtr**} [*ip address*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**dial-peer voice tag voip** **例：** `Router(config)# dial-peer voice 10 voip`	ダイヤル ピア コンフィギュレーション モードを開始し、音声カプセル化の方式を指定して、特定のダイヤル ピアを定義します。 *tag*：特定のダイヤル ピアを定義する番号。範囲は 1 ～ 2147483647 です。

	コマンドまたはアクション	目的
ステップ 4	**call fallback** [**icmp-ping** | **rtr**] **例**： `Router(config-dial-peer)# call fallback icmp-ping`	IP 宛先への ping のためのダイヤルピア パラメータを設定します。 • **icmp-ping** : ICMP ping を使用して IP 宛先をモニタします。 • **rtr** : RTR プローブを使用してセッション ターゲットをモニタし、ダイヤル ピアのステータスを更新します。RTR プローブがデフォルトです。 **（注）** この **call fallback icmp-ping** コマンドが入力されない場合は、グローバル設定内の **call fallback active** コマンドが測定に使用されます。この **call fallback icmp-ping** コマンドが入力された場合は、これらの値によってグローバル設定が上書きされます。 **monitor probe icmp-ping** コマンドを使用するには、これらの 2 コマンドのどちらかが有効になっている必要があります。どちらの **call fallback** コマンドも有効でない場合は、**monitor probe icmp-ping** コマンドが正しく動作しません。
ステップ 5	**monitor probe** {**icmp-ping** | **rtr**} [*ip address*] **例**： `Router(config-dial-peer)# monitor probe icmp-ping`	プローブの結果に基づいて、ダイヤルピアのステータス変更をイネーブルにします。 • **icmp-ping** : プローブのための方法として ICMP ping を使用します。 • **rtr** : プローブのための方法として RTR を使用します。 *ip address* : プローブされる宛先の IP アドレス。IP アドレスが指定されない場合は、セッション ターゲットから IP アドレスが読み取られます。

call fallback icmp-ping コマンドのグローバル設定

ICMP ping を使用して IP 宛先をモニタするためのグローバル パラメータを設定するには、この作業を完了します。

手順の概要

1. **enable**
2. **configure terminal**
3. **call fallback active** [**icmp-ping** | **rtr**]
4. **call fallback icmp-ping** [**count** *number*] [**codec** *type*] | **size** *number*] **interval** *number* [**loss** *number*] [**timeout** *value*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**call fallback active** [**icmp-ping** | **rtr**] **例：** `Router(config)# call fallback active icmp-ping`	IP 宛先への ping のためのグローバル パラメータを設定します。 • **icmp-ping** : ICMP ping を使用して IP 宛先をモニタします。 • **rtr** : RTR プローブを使用して IP 宛先をモニタします。RTR プローブがデフォルトです。 **（注）** **call fallback icmp-ping** コマンドを使用するには、その前に **call fallback active icmp-ping** コマンドが入力される必要があります。このコマンドを最初に入力しないと、**call fallback icmp ping** コマンドが正しく動作しません。
ステップ 4	**call fallback icmp-ping** [**count** *number*] [**codec** *type*] | **size** *bytes*] **interval** *seconds* [**loss** *number*] [**timeout** *milliseconds*] **例：** `Router(config)# call fallback icmp ping codec g729 interval 10 loss 10`	ICMP ping のパラメータを設定します。 • **count** : 宛先 IP アドレスに送信される ping パケットの数。デフォルトは 5 です。 • **codec** : ping パケットのサイズを決定するためのコーデック タイプ。 • *type* : 受け入れ可能なコーデック タイプは、**g711a**、**g711u**、**g729**、および **g729b** です。 • **size** : ping パケットのサイズ（バイト単位）。デフォルトは 32 です。 • **interval** : ping パケット セット間の時間（秒単位）。デフォルトは 5 です。この値は、**timeout** 値より大きい値にしてください。 • **loss** : パーセンテージで表された、しきい値のパケット損失。デフォルトは 20 です。 • **timeout** : エコー パケットのタイムアウト（ミリ秒）。デフォルトは 500 です。

busyout monitor probe icmp-ping コマンドの音声ポート設定

ICMP ping を使用して IP 宛先をモニタするための音声ポート パラメータを設定するには、この作業を完了します。

手順の概要

1. **enable**
2. **configure terminal**
3. **voice-port** *slot*/*port*
4. **busyout monitor probe icmp-ping** *ip address* [**codec** *type* | **size** *bytes*] [**loss** *percent*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**voice-port** *slot*/*port* **例：** `Router(config)# voice-port 1/0`	音声ポート コンフィギュレーション モードを開始し、設定パラメータを有効にするスロットとポートを識別します。 **（注）** このコマンドの構文は、プラットフォームによって異なります。詳細については、『*Cisco IOS Voice Command Reference*』を参照してください。
ステップ 4	**busyout monitor probe icmp-ping** *ip address* [**codec** *type*	**size** *bytes*] [**loss** *percent*] **例：** `Router(config-voiceport)# busyout monitor probe 10.1.1.1 g711u loss 10 delay 2000`	音声ポート設定の下でのモニタリングのための ICMP ping のパラメータを指定します。 • *ip address*：ping の送信先の宛先の IP アドレス。 • **codec**：（任意）ping パケットのサイズを決定するためのコーデック タイプ。 • *type*：受け入れ可能なコーデック タイプは、**g711a**、**g711u**、**g729**、および **g729b** です。 • **size**：（任意）ping パケットのサイズ（バイト単位）。デフォルトは 32 です。 **loss**：（任意）パーセンテージで表された、しきい値のパケット損失。デフォルトは 20 です。

busyout monitor probe icmp-ping コマンドの音声クラス設定

ICMP ping を使用して IP 宛先をモニタするための音声クラス パラメータを設定するには、この作業を完了します。

手順の概要

1. **enable**
2. **configure terminal**
3. **voice class busyout** *tag*
4. **busyout monitor probe icmp-ping** *ip address* [**codec** *type* | **size** *bytes*] [**loss** *percent*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**voice class busyout** *tag* **例：** `Router(config)# voice class busyout 10`	ローカル ボイス ビジーアウト機能のための音声クラスを作成します。 *tag*：1 つの音声クラスに割り当てられた一意の識別番号。範囲は 1 ～ 10000 です。
ステップ 4	**busyout monitor probe icmp-ping** *ip address* [**codec** *type*	**size** *bytes*] [**loss** *percent*] **例：** `Router(config-class)# busyout monitor probe icmp-ping 10.1.1.1 codec g729b size 32`	音声ポートの下でのモニタリングのための ICMP ping のパラメータを設定します。 • *ip address*：ping の送信先の宛先の IP アドレス。 • **codec**：（任意）ping パケットのサイズを決定するためのコーデック タイプ。 • *type*：受け入れ可能なコーデック タイプは、**g711a**、**g711u**、**g729**、および **g729b** です。 • **size**：（任意）ping パケットのサイズ（バイト単位）。デフォルトは 32 です。 • **loss**：（任意）パーセンテージで表された、しきい値のパケット損失。デフォルトは 20 です。

PSTN フォールバック機能を確認およびモニタする方法

ここでは、次の項目について説明します。

PSTN フォールバック設定の確認

この項にある **show** コマンドを使用すると、PSTN コールバック機能の動作を確認するための統計情報および設定パラメータを表示できます。

- **show running-config**：新機能が設定されているかどうかを確認するために、現在実行されているコンフィギュレーション ファイルの内容を表示します。
- **show call history voice**：音声コールのコール履歴テーブルを表示し、コール フォールバック、コール遅延、およびコール損失パラメータを確認します。
- **show call fallback cache**：コール フォールバック キャッシュ内のすべての IP アドレスの現在の Calculated Planning Impairment Factor（ICPIF）推定値を表示します。
- **show call fallback config**：現在の設定を表示します。
- **show call fallback stats**：コール フォールバックの統計情報を表示します。

PSTN フォールバックのモニタリングおよびメンテナンス

PSTN フォールバック機能をモニタおよびメンテナンスするには、次のコマンドを使用します。

- **clear call fallback cache**：キャッシュ内のすべての IP アドレスの現在の ICPIF 推定値をクリアします。
- **clear call fallback stats**：コール フォールバックの統計情報をクリアします。
- **debug call fallback detail**：VoIP コール フォールバックの詳細を表示します。
- **debug call fallback probes**：音声フォールバック プローブの詳細を表示します。
- **test call fallback probe** *ip-address*：特定の IP アドレスへのプローブをテストし、ICPIF SAA 値を表示します。
- **debug snmp packets**：ルータによって送受信されたすべての簡易ネットワーク管理プロトコル（SNMP）パケットに関する情報を表示します。

次の作業

「IP 宛先をモニタするための ICMP ping の設定」では、SAA/RTR プローブ結果の不具合（ICPIF、ジッター、損失など）のため、または ICMP ping テストの失敗のためにダイヤルピアが一時的にディセーブルになるメカニズムについて説明します。この状態が発生した場合は、代替ルートを表す代替ダイヤルピアを検索するために、通常の代替ダイヤルピア選択プロセス（ハンティング）がトリガーされます。

グローバル設定の **voice hunt** コマンドは、初期のダイヤルピア パスが失敗した理由を説明している特定の原因コードに基づいて、ハンティングが発生しているかどうか（引き続き代替ダイヤルピアの一致を検索または「ハント」するかどうか）を制御します。ハンティングは通常、原因コードがネットワー

ク輻輳を示している場合は適していますが、障害の原因コードが着信側のユーザが実際にビジー状態にあることを示している場合は通常不適切です。着信側のユーザに到達するための代替パスが取得された場合でも、ユーザが実際にビジー状態にあると、そのユーザはどのパスが使用されるかには関係なくビジー状態になります。

voice hunt コマンドの詳細については、『*Cisco IOS Voice Command Reference*』を参照してください。