CHAPTER 11

診断の実行

この章では、Cisco Prime Provisioning 6.3 での Diagnostics アプリケーションについて説明します。

概要

この項では、Cisco Prime Provisioning Diagnostics アプリケーションの概要について説明します。

この章の構成は、次のとおりです。

診断の概要

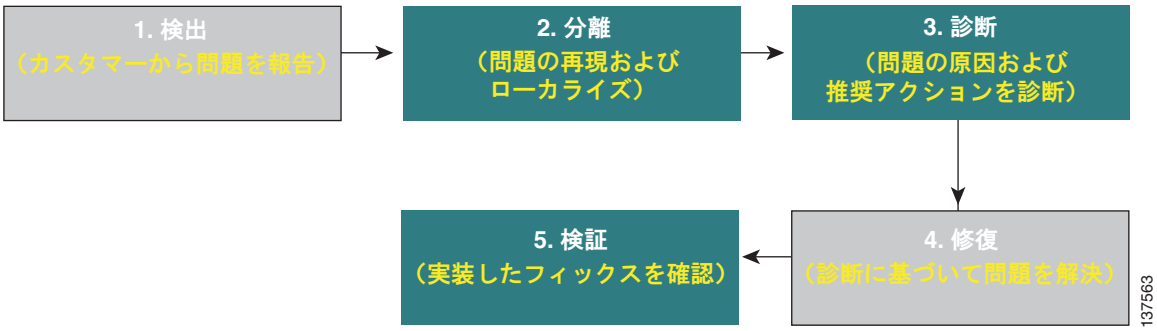
Diagnostics はワークフローに基づいた自動ネットワーク管理アプリケーションで、マルチプロトコル ラベル スイッチング（MPLS）VPN の問題をトラブルシューティングおよび診断します。Diagnostics は、MPLS に関連するネットワーク停止の診断に要する時間を削減するための機能を提供します。多くの場合、時間単位から分単位に短縮されます。診断は、ネットワーク障害シナリオに基づいて、MPLS のアクセス、エッジ、およびコアの各ネットワーク間で実行されます。サービス プロバイダーおよび企業の「自己導入」の、両方の MPLS VPN ネットワークに同様に適用できます。Network Operations Center（NOC; ネットワーク オペレーション センター）は技術者をサポートします。本製品以降は、第 2 次および第 3 次のサポートも受けることができるようになりました。Diagnostics は、オプションで、Prime Provisioning MPLS VPN プロビジョニング コンポーネントと統合できます。MPLS VPN の中核となる問題を診断するには、Label-Switched Path（LSP; ラベルスイッチド パス）ping および LSP traceroute など、MPLS のオペレーションおよびメンテナンス（OAM）機能をサポートする Cisco IOS ソフトウェア リリースおよび IOS XR ソフトウェア リリースが必要です。

障害の発見やトラブルシューティングを効果的に行うため、次の 5 つのステップを踏みます。

1. 検知
2. 分離
3. 診断
4. 修復
5. 確認

Diagnostics は、エンド カスタマーが VPN サービスを使用して問題をレポートするような、反応的な状況をサポートすることを目的として設計されています。これは、基本的に、図 11-1 の「診断」のステップに該当します。ルータ デバイスに加えられた変更を徹底して自ら管理し、それを行うための社内手順を定めているプロバイダーが多いため、「修復」機能はサポートされません。

図 11-1　　反応的な障害ライフサイクル



（注）　ステップ 2、3、および 5 は Diagnostics によって実行されます。ステップ 1 と 4 は手動で実行する必要があります。

Diagnostics では、「分離」、「診断」、および「検証」のステップを重点的に扱います。ネットワークでの障害の分離および診断、障害の発生したデバイスの特定、適切なデバイス ステータスのチェック、および障害発生の考えられる理由を特定するための設定を行うための貴重な機能を提供します。また、Diagnostics は、デバイス設定に加えた変更によって問題が解決されたことを検証するため、テストを再実行する機能も提供します。

この機能は、Prime Provisioning のその他のモジュール（VPN プロビジョニングや Traffic Engineering Management など）に依存せず、単独で使用できます。また、その他の Prime Provisioning モジュールが一部またはすべて使用されている Prime Provisioning インストールでも使用できます。MPLS VPN プロビジョニング機能が使用された場合は、カスタマー データおよび VPN データをトラブルシューティングの開始点として使用し、どのエンドポイント（カスタマー エッジ デバイスなど）間の接続をテストするかを特定できます。

Diagnostics はトラブルシューティングだけでなく、VPN ポストプロビジョニング チェックにも使用できます。VPN を展開した後、手動でまたは Prime Provisioning VPN プロビジョニング機能を使用して接続テストを実行し、VPN が正常にプロビジョニングされているかどうかを検証できます。

（注）　Diagnostics では、基礎となる設定またはルーティングのトラブルシューティング中の変更がサポートされません。Diagnostics の実行中にオペレータまたはルータのコントロール プレーンにより加えられた変更は、いずれも実行される実際のトラブルシューティングには反映されません。このような変更が加えられた場合、Diagnostics で正しい障害シナリオや観察の結果が得られるとは限りません。

前提となる知識

Diagnostics は、MPLS VPN について最低限の知識を持ったユーザによる使用を前提として設計されています。Diagnostics の MPLS VPN 接続性検証テストは、MPLS VPN についてほとんど、またはまったく知らないユーザでも実行できます。また、必要に応じてテスト結果をエクスポートし、MPLS VPN に詳しいエンジニアに解釈してもらうこともできます。ただし、MPLS VPN はもともと複雑であ

るため、RFC 2547 に従って MPLS VPN について習熟し、Diagnostics の利点を最大限に生かすことを推奨します。特に、RFC 2547 アークテクチャ、トポロジ、制御、およびデータ プレーンの知識は、アプリケーションを最大限に利用する方法を理解し、結果を解釈するうえで役立ちます。

Diagnostics は現在、IETF RFC 4379 準拠のラベル スイッチド パス（LSP）ping および LSP traceroute を使用するシスコ デバイスおよびネットワークを診断します。Diagnostics は、Cisco IOS で使用可能な先行のドラフト（ドラフト 3）も継続してサポートしています。ネットワーク内のすべてのデバイスで、一貫した LSP ping および traceroute のドラフトを使用する必要があります。

推奨文献：

- 『MPLS and VPN Architectures』Ivan Pepelnjak、Jim Guichard（Cisco Press）
- 『Troubleshooting Virtual Private Networks』Mark Lewis（Cisco Press）
- LSP ping/trace RFC：http://www.ietf.org/rfc/rfc4379.txt
- RFC 2547：http://www.ietf.org/rfc/rfc2547.txt?number=2547
- RFC 4379：http://www.ietf.org/rfc/rfc4379.txt?number=4379
- MPLS Embedded Management：LSP Ping/Traceroute and AToM VCCV: http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/gslsppt.html

サポートされているハードウェア、IOS、および IOS XR バージョン

サポートされているプロバイダー（P）およびプロバイダー エッジ（PE）ネットワーク デバイスのタイプおよび関連する Cisco IOS および IOS XR バージョンの詳細については、*『Cisco Prime Provisioning 6.3 Installation Guide』*を参照してください。

（注） その他のデバイス タイプ、IOS、および IOS XR バージョンのサポートが、パッチ リリースで追加される場合があります。最新のパッチ リリースとサポートされているデバイス タイプ、IOS、および IOS VR バージョンの詳細については、Cisco.com を参照してください。

「Prime Provisioning サービスの設定」（P.3-6）で説明されているデバイス タイプ、IOS、および IOS XR バージョンは、MPLS ラベル スイッチド パス（LSP）の ping および traceroute 機能をサポートしています。この機能は、Diagnostics のトラブルシューティングに必要です。すべての P および PE デバイスがサポートされているデバイス タイプ、IOS、および IOS XR バージョンのリストに準拠していれば、Diagnostics はアクセス回線、MPLS VPN、および MPLS コアの問題をトラブルシューティングできます。Diagnostics は、他社製品などのその他のデバイス タイプ、IOS、および IOS XR バージョンにも対応できます。ただし、ネットワーク内にこのリストに準拠していない P または PE デバイスが含まれている場合、完全な診断ができない場合があります。表 11-1 に、可能性のあるシナリオとその結果を示します。

表 11-1　ハードウェア、IOS、および IOS XR のバージョン コンプライアンス

シナリオ	結果
すべての P および PE デバイスが、サポートされているシスコ製ハードウェア、IOS、および IOS XR バージョンに準拠している。	MPLS VPN 接続性検証テストは、アクセス回線、MPLS VPN、および MPLS コアの問題を正しくトラブルシューティングします。
すべての PE デバイスが、サポートされているシスコ製ハードウェア、IOS、および IOS XR バージョンに準拠している。1 台または複数の P デバイスが、サポートされているシスコ製ハードウェア、IOS、および IOS XR バージョンに準拠していない（他社製品など）。	MPLS VPN 接続性検証テストは、アクセス回線および MPLS VPN の問題を正しくトラブルシューティングしますが、MPLS コアの問題のトラブルシューティングは完了できない場合があります。

表 11-1　ハードウェア、IOS、および IOS XR のバージョン コンプライアンス （続き）

シナリオ	結果
PE デバイスが、サポートしていない IOS および IOS XR バージョンを実行しているシスコ製ハードウェアであり、MPLS LSP ping および traceroute 機能をサポートしていない。	MPLS VPN 接続性検証テストは、アクセス回線および MPLS VPN の問題を正常にトラブルシューティングできる *可能性はあります*。MPLS VPN 接続性検証テストは、MPLS コアのトラブルシューティングを実行できません。
PE デバイスがシスコ製以外のハードウェアである。	MPLS VPN 接続性検証テストは実行できません。

Diagnostics は、すべてのベンダーの管理対象および管理対象外の CE ルータをサポートしています。CE デバイスについては、デバイス タイプ、IOS、または IOS XR バージョンの要件はありません。

Diagnostics は、MPLS LSP ping および traceroute 機能をサポートしている他のデバイス タイプ、IOS および IOS XR バージョンで動作できます。この機能をサポートしているデバイス タイプ、IOS、および IOS XR のバージョンの詳細については、Cisco Feature Navigator を使用してください。http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp を参照してください。

（注）　PE デバイスが、サポートされていない IOS または IOS XR バージョン（MPLS ping および traceroute 機能を実装していないもの）を実行している場合は、アクセス回線および VPN エッジのトラブルシューティングは実行されますが、MPLS コアのトラブルシューティングはできません。このシナリオでは、コアの障害は PE デバイス上のラベル転送情報ベース（LFIB）不一致としてレポートされます。LFIB 不一致はコア障害の症状ですが、コアはトラブルシューティングできないため、実際のコア障害は診断できません。

IPv6

Internet Assigned Numbers Authority（IANA）が管理する IPv4 アドレス フリー プールが残り少なくなってきています。シスコは、この事態に対応するため、IPv6 アドレス指定を採用しています。

Diagnostics は、IPv4 と IPv6 の両方のアドレスを持つデバイスの、設定および選択をサポートしています。Diagnostics は、接続回線が次のような状態の MPLS VPN サービスをトラブルシューティングできます。

- IPv6 アドレス指定を使用する場合
- デュアルスタックの IPv4/IPv6 アドレス指定を使用する場合

デュアルスタックは、同じインターフェイス上に IPv4 と IPv6 の両方を共存させるための技術です。インターネット上には、永久ではないものの、今後長年にわたって IPv6 と IPv4 ノードが混在します。このため、IPv4 ノードを大規模に展開している企業では、IPv4 から IPv6 への移行を成功させることがとても重要です。たとえば、単一のインターフェイスを、IPv4 アドレスと IPv6 アドレスの両方を持つように設定できます。「デュアルスタック」と呼ばれるあらゆる要素（プロバイダー エッジやカスタマー エッジ ルータなど）は、IPv4 だけでなく、IPv6 アドレス指定およびルーティング プロトコルも実行します。

（注）　Diagnostics は、グローバル ユニキャスト IPv6 アドレスのみをサポートします。グローバル ユニキャスト アドレスの機能は、131.107.1.100 のような IPv4 ユニキャスト アドレスと類似しています。つまり、これらのアドレスは、従来型の、公的にルーティング可能なアドレスであると言えます。グローバル ユニキャスト アドレスには、グローバル ルーティング プレフィックス、サブネット ID、およびインターフェイス ID が含まれます。

表 11-2　一般的なユニキャスト アドレス構造

フィールド	ネットワーク プレフィックス	サブネット	インターフェイス ID
Bits	48	16	64

（注）　Diagnostics では、接続回線エンドポイントが IPv6 と IPv6 の場合、IPv4 と IPv4 の場合のいずれにおいてもテストを起動できます。両方のアドレス指定を混在させることはできません。

IPv6 アドレスでテストを開始する場合の詳細については、「Diagnostics 接続テストの概要」（P.11-14）を参照してください。

診断機能

Diagnostics のトラブルシューティングおよび診断は、次の 4 つのドメインをサポートしています。

- アクセス回線：アクセス回線のトラブルシューティングには、ATM、フレーム リレー、およびイーサネットのルーティング プロトコルの基本的なトラブルシューティング、レイヤ 1 およびレイヤ 3 の基本的なトラブルシューティング、およびレイヤ 2 の高度なトラブルシューティングが含まれます。
- MPLS VPN：MPLS VPN のトラブルシューティングは、RFC2547 に基づいて MPLS/MP-BGP VPN をサポートしています。サポートされているトポロジは、ハブ アンド スポーク、セントラル サービス、フル メッシュ、およびイントラネットまたはエクストラネット VPN です。
- MPLS コア：MPLS コアのトラブルシューティングは、データ プレーンおよびコントロール プレーンのトラブルシューティングをサポートしています。この機能は、MPLS 運用管理および保守（OAM）がサポートされている Cisco IOS または Cisco IOS XR バージョンを実行するすべての MPLS コアおよびエッジ デバイス（検出されたすべての MPLS トラフィック エンジニアリング トンネルのトラブルシューティングを含む）用として用意されています。MPLS OAM がサポートされている Cisco IOS、および Cisco IOS XR のバージョンの詳細については、「サポートされているハードウェア、IOS、および IOS XR バージョン」（P.11-3）を参照してください。

（注）　Diagnostics では、コア内のルーティング プロトコル（ただし IGP プロトコルが OSPF の場合はファースト ホップおよび PE-P-PE トポロジでの OSPF 障害を除く）、コア内の IP 接続性、および相互自律システム（AS）または Carrier-Supporting-Carrier（CsC）の一部のバリエーション（特に LSP が存在しない相互 AS オプション B および CsC）はトラブルシューティングされません。

スタートアップ ガイド

この項では、シスコの Prime Provisioning 診断の使用を開始する方法について説明します。

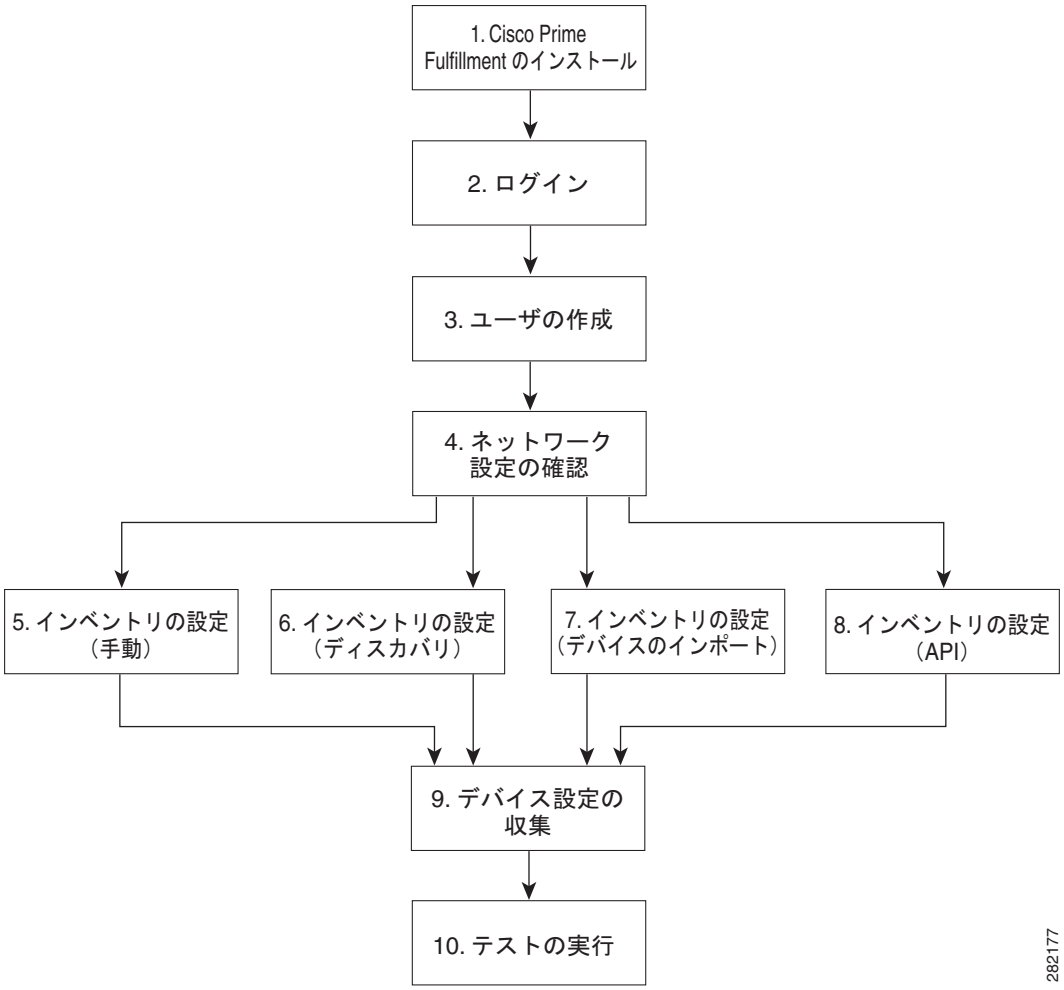
次の事項について説明します。

- 「ユーザ ロール」（P.11-7）

- 「ユーザ ロール」（P.11-7）
- 「ユーザの作成」（P.11-7）
- 「ネットワーク設定」（P.11-7）
- 「インベントリの設定」（P.11-9）

図 11-2 に、Diagnostics の使用を開始する際のワークフローを示します。

図 11-2　Diagnostics の概要



6. ユーザの作成：ユーザを作成し、Diagnostics ユーザ ロールを割り当てます。「ユーザ ロール」（P.11-7）、および「ユーザの作成」（P.11-7）を参照してください。
7. ネットワーク設定の確認：Diagnostics に必要な設定が、すべてのネットワーク デバイスで行われていることを確認します。「ネットワーク設定」（P.11-7）を参照してください。
8. インベントリの設定（手動）：必要な Prime Provisioning インベントリ オブジェクトを手動で作成します。「インベントリの設定」（P.11-9）を参照してください。
9. インベントリの設定（ディスカバリ）：Prime Provisioning ディスカバリを使用して、必要な Prime Provisioning インベントリ オブジェクトを作成します。「インベントリの設定」（P.11-9）を参照してください。

10. インベントリの設定（デバイス インポート）：インベントリ マネージャのデバイス インポート機能を使用して、必要な Prime Provisioning インベントリ オブジェクトを作成します。「インベントリの設定」（P.11-9）を参照してください。
11. インベントリの設定（API）：必要なインベントリ オブジェクトを Prime Provisioning API によって作成します。「インベントリの設定」（P.11-9）を参照してください。
12. デバイス設定の収集：インターフェイス設定を含むデバイス設定を収集し、Prime Provisioning インベントリに追加します。Prime Provisioning インベントリを実際のデバイス設定と定期的に同期するように、スケジュール タスクを設定できます。「デバイス設定の収集」（P.11-12）を参照してください。
13. テストの実行：MPLS VPN 接続性検証テストを設定して実行します。「MPLS VPN 接続性検証テストの実行」（P.11-18）を参照してください。

ユーザ ロール

Prime Provisioning ユーザが使用できる機能は、割り当てられているユーザ ロールによって決まります。ユーザ ロールによって、デバイスの作成と削除やデバイス設定の収集、MPLS VPN 接続性検証テストの実行を行うこともできます。

Diagnostics 機能を使用するには、実行する権利が与えられる接続性テストのタイプに応じて、次の定義済み Diagnostics ロールの 1 つ以上が割り当てられている必要があります。

1. MplsDiagnosticsRole：2 つの CE 間で MPLS VPN 接続性テストを実行できます。
2. MplsDiagnosticsPeToAttachedCeTestRole：PE と接続された CE との間で MPLS VPN 接続性テストを実行できます。
3. MplsDiagnosticsCetoPeAcrossCoreTestRole：MPLS コアをまたぐ CE および PE 間で MPLS VPN 接続性テストを実行できます。
4. MplsDiagnosticsPetoPeInVrfTestRole：2 つの PE 間で MPLS VPN 接続性テストを実行できます。
5. MplsDiagnosticsPeToPeCoreTestRole：2 つの PE 間でコア MPLS VPN 接続性テストを実行できます。

（注）　すべての Diagnostics ロールで、デバイスの作成と削除やデバイス設定の収集、MPLS VPN 接続性検証テストの実行を行うことができます。

ユーザの作成

Prime Provisioning ユーザの作成方法については、*『Cisco Prime Provisioning 6.3 Administration Guide』*を参照してください。

ネットワーク設定

この項では、ネットワークのトラブルシューティングを Diagnostics で行うために必要なネットワーク設定を説明します。

MPLS IP 存続可能時間伝搬

MPLS IP 存続可能時間（TTL）伝搬は、シスコ デバイスではデフォルトでイネーブルになっています。Diagnostics では、MPLS IP TTL 伝搬が MPLS コア内でイネーブルになっている必要があります。MPLS IP TTL 伝搬がイネーブルになっていない場合、Diagnostics は MPLS コア内で問題のトラブルシューティングを実行できません。その状態でも、アクセス回線の問題、または MPLS コアのエッジにおける問題のトラブルシューティングは可能です。

Cisco IOS では、IOS コマンドの **no mpls ttl-propagate forward** を使用すると、MPLS コアに転送されるパケットの MPLS IP TTL 伝搬をディセーブルにできます。このコマンドでは、MPLS コアに転送されるパケットの TTL 伝搬が停止されますが、MPLS コア内部から送信されるパケットの TTL 伝搬は許可されます。Diagnostics は、この状況で正しく機能します。

Cisco IOS コマンドの **no mpls ip propagate-ttl** を使用して、または Cisco IOS XR コマンドの **mpls ip-ttl-propagate disable** を使用して TTL 伝搬をディセーブルにしている場合は、すべての TTL 伝搬がディセーブルになるため、Diagnostics は MPLS ネットワークをトラブルシューティングできません。

（注）　トラブルシューティング対象に選択したデバイスと、同じネットワークの一部であるデバイスに対して、タイムスタンプをディセーブルにする必要があります。

MPLS LSP ping/traceroute のリビジョン

Diagnostics は、バージョン 3 の IETF LSP ping ドラフト（draft-ietf-mpls-lsp-ping-03.txt）に基づいて、IOS MPLS LSP ping/traceroute 実装をサポートします。それよりも後のバージョンの IETF LSP ping ドラフトはサポートされません。最新の IOS バージョン（12.4(6)T を含む）および IOS XR は、以降のバージョンの IETF LSP ping ドラフト /RFC 4379 を実装しています。これらの IOS または IOS XR バージョンで Diagnostics を使用するには、バージョン 3 の IETF LSP ping ドラフトを使用するように IOS または IOS XR を設定する必要があります。そのためには、IOS または IOS XR グローバル コンフィギュレーション モードで **mpls oam** コマンドに続けて **echo revision 3** コマンドを入力する必要があります。必要に応じて、コアのすべてのルータが同じバージョンの IEFT LSP ping ドラフトまたは RFC を使用していることを確認します。

ポイントツーポイント アクセス回線リンクでの 31 ビット プレフィックス

IPv4 アドレッシングを使用するアクセス回線リンクに対して、Diagnostics は、31 ビット プレフィックスで設定されたアクセス回線リンクによるトラブルシューティングをサポートします。ただし、各クラスフル ネットワークに対して、Diagnostics は可能性のある 2 つの 31 ビット プレフィックス設定によるトラブルシューティングをサポートしません。その 2 つとは、クラスフル ネットワーク アドレスまたはネットワーク ブロードキャスト アドレスをホスト アドレスとして使用するサブネットです。たとえば、クラス A ネットワーク 10.0.0.0 において、IP アドレス 10.0.0.0 と 10.0.0.1 をホスト アドレスとして使用する 31 ビット プレフィックス サブネット、および IP アドレス 10.255.255.254 と 10.255.255.255 をホスト アドレスとして使用するサブネットはサポートされません。これらの範囲の間にあるすべてのサブネットはサポートされます。

サポートされていない 31 ビット プレフィックス サブネットを使用して Diagnostics テストが設定された場合は、テストは実行されず、サポートされていない 31 ビット プレフィックス設定であることを通知するメッセージが表示されます。このような状況では、このリンクを手動でトラブルシューティングするか、リンクを再設定してサポートされるサブネット設定を使用する必要があります。

インベントリの設定

Diagnostics は、他の Prime Provisioning モジュールにまったく依存することなく使用できます。ただし、使用する前に、Prime Provisioning リポジトリに多数のオブジェクトを入力する必要があります。最低でも、これにはプロバイダー、プロバイダー リージョン、デバイスおよび PE デバイス オブジェクトが含まれます。これらの各オブジェクトのロールについて、以下で説明します。

- プロバイダー：一般的にプロバイダーとは、ネットワーク サービスをカスタマーに提供するサービス プロバイダーまたは大企業です。プロバイダーは、特定のプロバイダーを表した論理インベントリ オブジェクトです。
- プロバイダー リージョン：プロバイダー リージョンは、1 つのボーダー ゲートウェイ プロトコル（BGP）自律システム内のプロバイダー エッジ ルータ（PE）のグループであると見なされます。プロバイダー リージョンを定義する主な目的は、プロバイダーがヨーロッパ、アジア太平洋などの広い地域で一意の IP アドレス プールを使用できるようにすることです。
- デバイス：Prime Provisioning のデバイスは、ネットワーク内の物理デバイスを論理的に表したものです。Prime Provisioning が管理するすべてのネットワーク要素は、システム内でデバイスとして定義する必要があります。
- PE デバイス：PE デバイスは、特定のプロバイダー リージョンに関連付けられたプロバイダー エッジ（PE）またはプロバイダー（P）ルータを論理的に表したものです。PE デバイスは最初にデバイスとして追加してから、そこに PE デバイス タイプを割り当てる必要があります。

MPLS ネットワークのすべてのプロバイダー エッジ（PE）およびプロバイダー（P）ルータを Prime Provisioning インベントリに追加する必要があります。各プロバイダー エッジ ルータはデバイスとして作成してから、ロール タイプ N-PE（ネットワーク方向の PE）を割り当てた PE デバイスとする必要があります。各プロバイダー デバイスはデバイスとして作成してから、ロール タイプ P（プロバイダー）を割り当てた PE デバイスとする必要があります。Prime Provisioning インベントリへの顧客宅内装置（CPE）デバイスの追加はオプションです。

（注） デバイスがプロバイダー デバイスおよびプロバイダー エッジ デバイスの両方として動作する場合は、そのデバイスを、ロール タイプ N-PE（ネットワーク方向の PE）を割り当てた PE デバイスとして作成する必要があります。

多くの MPLS VPN ネットワークがルータ リフレクタを使用します。ルータ リフレクタを Prime Provisioning インベントリに追加することを推奨します。ルータ リフレクタはデバイスとして追加してから、ロール タイプが P の PE デバイスとして追加する必要があります。ルータ リフレクタを Prime Provisioning インベントリに追加することにより、Diagnostics は、このデバイスを含む潜在的な障害を識別できます。

（注） その他の Prime Provisioning の機能を使用して MPLS ネットワークを管理している場合は、必要なインベントリ オブジェクトの多くがすでに存在している可能性があります。たとえば、Prime Provisioning MPLS VPN 機能を使用している場合に、必要なプロバイダー、プロバイダー リージョン、およびプロバイダー エッジ デバイスはすでに存在することがあります。その場合は、プロバイダー デバイスのみを追加する必要があります。

必要なインベントリ オブジェクトを作成するための、多数のオプションがあります。これらのオブジェクトは Prime Provisioning GUI により手動で作成することも、Prime Provisioning Discovery 機能、インベントリ マネージャのデバイス インポート機能、あるいは Prime Provisioning API を利用するサードパーティの Operations Support System（OSS）クライアント プログラムを使用して作成することもできます。これらのオプションについては、それぞれ次の項を参照してください。

- 「手動作成」（P.11-10）

- 「Discovery」（P.11-10）
- 「インベントリ マネージャ デバイスのインポート」（P.11-11）
- 「Prime Provisioning API」（P.11-12）
- 「Prime Provisioning API」（P.11-12）

（注）　デバイスの作成時に、デバイス アクセス情報（ログインおよびパスワード）が、物理デバイスに設定されている情報と一致している必要があります。

手動作成

手動作成では、必要な設定を Prime Provisioning グラフィカル ユーザ インターフェイス（GUI）により入力することで、オブジェクトを Prime Provisioning リポジトリに追加できます。オブジェクトの手動作成は、Prime Provisioning リポジトリに追加するオブジェクト数が少ない場合に推奨されます。オブジェクトの手動作成の手順を次に示します。

1. プロバイダーを作成します。
2. プロバイダー リージョンを作成します。
3. デバイスを作成します。
4. インターフェイス設定などのデバイス設定を収集します
5. PE デバイスを作成し、プロバイダー デバイスおよびプロバイダー エッジ デバイスのロールを割り当てます。

（注）　Provider（P; プロバイダー）デバイスおよびプロバイダー エッジ（PE）デバイスは、いずれも適切な PE ロール タイプが割り当てられた PE デバイス オブジェクトとして Prime Provisioning リポジトリに追加する必要があります。プロバイダー デバイスおよびプロバイダー エッジ デバイスに割り当てる必要のある PE ロール タイプの詳細については、「インベントリの設定」（P.11-9）を参照してください。Prime Provisioning サーバおよびデバイス間で使用するトランスポート メカニズムを選択する場合、Cisco CNS Configuration Engine は Diagnostics に必要なコマンドをサポートしないため、MDE と組み合わせて使用できません。Cisco CNS Configuration Engine を Diagnostics と使用しようとすると、Diagnostics はデバイスに接続できないと間違って報告します。

プロバイダー、プロバイダー リージョン、デバイス、および PE デバイス オブジェクトを手動で作成する方法については、「リソースの設定」（P.2-42）を参照してください。

デバイスを手動作成する場合は、対象のデバイスのインターフェイス設定も追加する必要があります。

インターフェイス設定は、デバイス作成時に手動で追加することも、タスク マネージャの Collect Configuration タスクを使用して追加することもできます。タスク マネージャの Collect Configuration タスクの実行方法の詳細については、「デバイス設定の収集」（P.11-12）を参照してください。Collect Configuration タスクを使用することを推奨します。

Discovery

Discovery では、XML ファイルに最低限のデバイスおよびトポロジ情報を設定することにより、ネットワークのデバイスを Prime Provisioning リポジトリに追加できます。次に、Discovery プロセスはこれらのデバイスを照会し、必要なデバイスおよびトポロジ情報を Prime Provisioning リポジトリに入力します。リポジトリに追加するオブジェクト数が多い場合は、Discovery の使用を推奨します。

Prime Provisioning Discovery には、デバイスを検出するための方法として CDP とデバイス / トポロジの 2 つが用意されています。デバイス検出を実行する前に、Discovery に必要な XML コンフィギュレーション ファイルを作成することが必要です。デバイスを検出する方法の詳細については、付録 E「インベントリ - ディスカバリ」を参照してください。

（注）　Provider（P; プロバイダー）デバイスおよびプロバイダー エッジ（PE）デバイスは、いずれも適切な PE ロール タイプが割り当てられた PE デバイス オブジェクトとして Prime Provisioning リポジトリに追加する必要があります。プロバイダー デバイスおよびプロバイダー エッジ デバイスに割り当てる必要のある PE ロール タイプの詳細については、「インベントリの設定」（P.11-9）を参照してください。

（注）　Discovery の完了後に、検出されたすべてのデバイスに対してタスク マネージャの Collect Configuration タスクを実行する必要があります。Collect Configuration タスクを実行しないと、Diagnostics は検出されたデバイスにログインして、トラブルシューティングを実行できません。タスク マネージャの Collect Configuration タスクの実行方法の詳細については、「デバイス設定の収集」（P.11-12）を参照してください。

インベントリ マネージャ デバイスのインポート

インベントリ マネージャのデバイス インポート機能を使用すると、デバイスの Cisco IOS 実行コンフィギュレーションを含むファイルから Prime Provisioning リポジトリに複数のデバイスをインポートできます。リポジトリに追加するオブジェクト数が多い場合は、インベントリ マネージャのデバイス インポート機能の使用を推奨します。デバイスをインポートする方法の詳細については、付録 E「インベントリ - ディスカバリ」を参照してください。

プロバイダー（P）およびプロバイダー エッジ（PE）デバイスをインポートする前に、必要なプロバイダーおよびプロバイダー リージョン オブジェクトを作成する必要があります。プロバイダーおよびプロバイダー リージョンオブジェクトを手動で作成する方法については、付録 E「インベントリ - ディスカバリ」を参照してください。

デバイスをインポートするときは、Cisco IOS 実行コンフィギュレーションを含むファイルがあるディレクトリを指定する必要があります。ファイル名は指定しないでください。ファイルは、Prime Provisioning サーバからアクセスできるファイル システムのディレクトリに存在する必要があります。

（注）　Provider（P; プロバイダー）デバイスおよびプロバイダー エッジ（PE）デバイスは、いずれも適切な PE ロール タイプが割り当てられた PE デバイス オブジェクトとして Prime Provisioning リポジトリに追加する必要があります。プロバイダー デバイスおよびプロバイダー エッジ デバイスに割り当てる必要のある PE ロール タイプの詳細については、「インベントリの設定」（P.11-9）を参照してください。

（注）　イネーブル シークレット パスワードは、Cisco IOS 実行コンフィギュレーションに追加される前に暗号化されます。その結果、デバイス インポート機能は、Prime Provisioning リポジトリにインポートするデバイスに対してイネーブル シークレット パスワードを設定できません。インポートするデバイスにイネーブル シークレット パスワードが設定されている場合は、Prime Provisioning リポジトリでこれらのデバイスに手動でイネーブル パスワードを設定する必要があります。イネーブル シークレット パスワードとイネーブル パスワードの両方がデバイスに設定されている場合、インベントリ マネージャのデバイス インポート機能は Prime Provisioning リポジトリに追加するデバイスにイネーブル パ

スワードを使用します。このパスワードは正しいイネーブル シークレット パスワードで上書きする必要があります。Prime Provisioning リポジトリのデバイスのイネーブル パスワードは、デバイスのインポート中にも、デバイスのインポート後にも設定できます。

（注）　デバイス インポートの完了後に、インポートされたすべてのデバイスに対してタスク マネージャの Collect Configuration タスクを実行する必要があります。Collect Configuration タスクを実行しないと、Diagnostics はインポートされたデバイスにログインして、トラブルシューティングを実行できません。タスク マネージャの Collect Configuration タスクの実行方法の詳細については、「デバイス設定の収集」（P.11-12）を参照してください。

Prime Provisioning API

Prime Provisioning アプリケーション プログラム インターフェイス（API）は、Prime Provisioning システムに接続するために Operations Support System（OSS）クライアント プログラムを使用することができます。Prime Provisioning API は、Prime Provisioning サーバからデータの挿入、取得、更新、および削除を行うためのメカニズムを提供します。API を使用して、必要なプロバイダー、プロバイダー リージョン、デバイスおよび PE デバイス オブジェクトを追加できます。

（注）　Prime Provisioning API は Diagnostics に標準には含まれておらず、別途購入できます。

Prime Provisioning API の使用方法の詳細については、*『Cisco Prime Provisioning 6.3 API Programmer Guide』*および *『Cisco Prime Provisioning API 6.3 Programmer Reference』*を参照してください。

デバイス設定の収集

タスク マネージャの Collect Configuration タスクを使用して、Prime Provisioning リポジトリのデバイスにインターフェイス設定を追加することを推奨します。タスク マネージャの Collect Configuration タスクはネットワークの物理デバイスに接続し、ルータからデバイス情報（インターフェイス設定を含む）を収集して、その情報を Prime Provisioning リポジトリに入力します。

タスク マネージャの Collect Configuration タスクを使用してデバイス インターフェイスの設定を追加する方法の詳細については、「タスク マネージャ」（P.10-25）を参照してください。

デバイス設定と Prime Provisioning リポジトリの同期

（注）　診断の精度は最新のデバイス情報に依存します。デバイス設定に何らかの変更を加えた後および定期的に、デバイス設定を物理デバイスと再同期することを推奨します。これにより、Prime Provisioning インベントリに保持されているデバイス設定がネットワークの物理デバイスと一致します。

タスク マネージャのスケジュール タスクを使用して、デバイス設定を最新に保つことを推奨します。Collect Configuration と Collect Configuration from File のどちらでも使用できます。タスク マネージャの Collect Configuration スケジュール タスクの作成方法の詳細については、「タスク マネージャ」（P.10-25）を参照してください。MPLS ネットワークの PE および P ルータは、すべてがタスク マネージャのスケジュール タスク Collect Configuration を使用してその設定を収集する必要があります。タスク マネージャの Collect Configuration タスクでは、インターフェイス設定およびその他のデバイス

属性の詳細が収集されます。タスク マネージャの Collect Configuration タスクの実行スケジュール間隔は、ネットワークに対する設定変更の頻度に依存します。タスク マネージャの Collect Configuration タスクを各 P および PE ルータで毎日実行することを推奨します。

Cisco MPLS Diagnostics Expert の使用

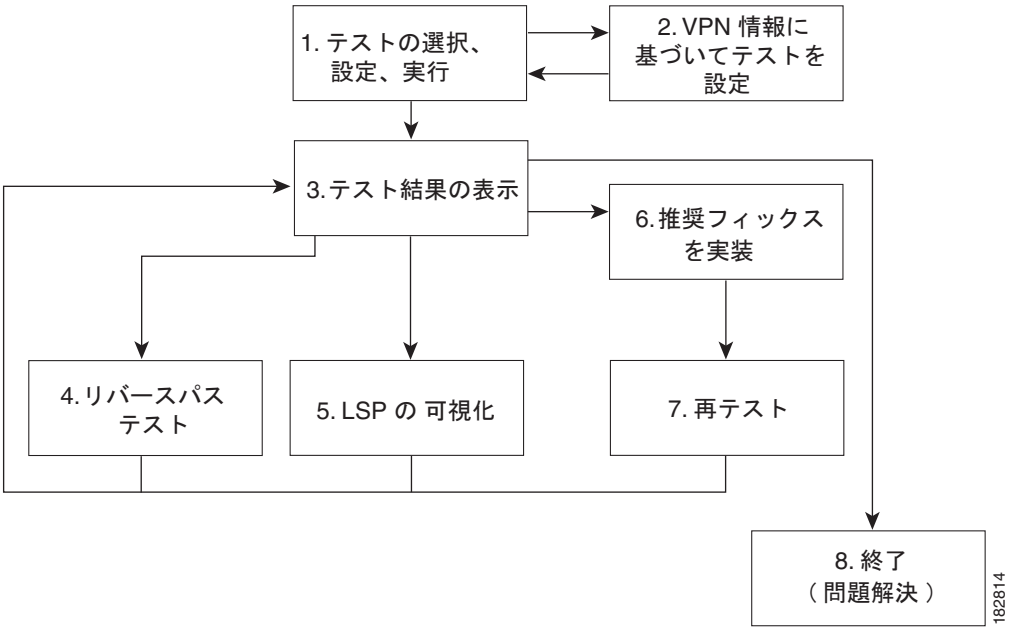
この項では、Diagnostics を使用する方法について説明します。

次の事項について説明します。

- 「Diagnostics 接続テストの概要」（P.11-14）
- 「MPLS VPN 接続性検証テストの実行」（P.11-18）
- 「[Progress] ウィンドウ」（P.11-39）
- 「テスト結果の解釈」（P.11-39）
- 「高度なトラブルシューティング オプション」（P.11-45）
- 「トンネル チェックのオフ：他社製 P ルータを使用したネットワークの場合」（P.11-48）

図 11-3 に、Diagnostics を使用する場合のワークフローを示します。

図 11-3　Diagnostics 使用ワークフロー



1. テストの選択、設定、および実行：MPLS VPN 接続性検証テストを設定して実行します。「MPLS VPN 接続性検証テストの実行」（P.11-18）を参照してください。
2. VPN 情報によるテストの設定：オプションで、VPN 情報を使用して MPLS VPN 接続性検証テストを設定します。これは、Prime Provisioning VPN プロビジョニング機能を使用してネットワーク内に VPN をプロビジョニングした場合にのみ可能です。「カスタマー VRF 情報を使用した設定」（P.11-29）および「カスタマー VPN/VRF 情報を使用した設定」（P.11-31）を参照してください。
3. テスト結果の表示：MPLS VPN 接続性検証テストの結果を、テスト ログを含めて表示します。「テスト結果の解釈」（P.11-39）を参照してください。
4. リバース パス テスト：高度なトラブルシューティングであるリバース パス テストを実行します。「リバース パス テスト」（P.11-46）を参照してください。
5. LSP 可視化：高度なトラブルシューティングである LSP 可視化を実行します。「LSP 可視化」（P.11-46）を参照してください。
6. 推奨フィックスの実装：テスト結果の推奨に従ってフィックスを実装します。
7. 再テスト：MPLS VPN 接続性検証テストを再実行します。通常、実装したフィックスを確認するために実行します。

Diagnostics 接続テストの概要

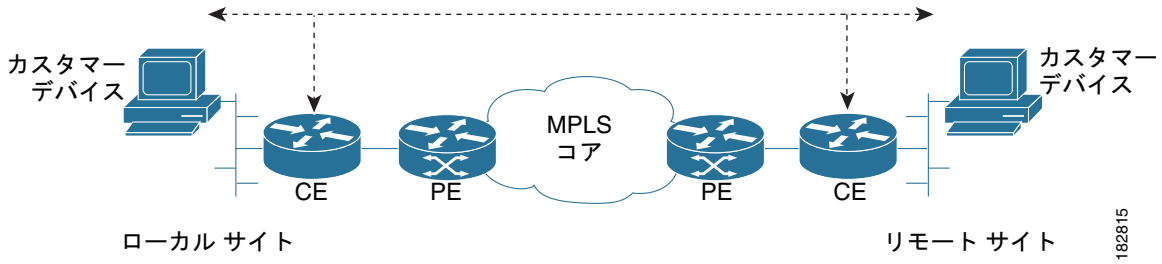
接続性テストは、CE - CE 間ネットワーク全体のサブセクションのトラブルシューティングを目的としています。次の接続性テストが用意されています。

1. L3VPN - CE to CE：2 つの CE 間の MPLS VPN 接続性をチェックします。「L3VPN - CE to CE 接続性テスト」（P.11-14）を参照してください。
2. L3VPN - PE to attached CE：PE と、接続されている CE の間の MPLS VPN 接続性をチェックします。「L3VPN - PE to attached CE 接続性テスト」（P.11-15）を参照してください。
3. L3VPN - CE to PE across Core：MPLS コアをまたがる CE と PE 間の MPLS VPN 接続性をチェックします。「L3VPN - CE to PE across Core 接続性テスト」（P.11-16）を参照してください。
4. L3VPN - PE to PE in VRF：2 つの PE 間の MPLS VPN 接続性をチェックします。「L3VPN - PE to PE in VRF 接続性テスト」（P.11-17）を参照してください。
5. MPLS - PE to PE：2 つの PE 間の MPLS コア接続性をチェックします。「L3VPN - PE to PE 接続テスト」（P.11-17）を参照してください。

L3VPN - CE to CE 接続性テスト

L3VPN - CE to CE テスト（図 11-4）は、2 つの CE 間またはカスタマー デバイス IP アドレスが既知のカスタマー デバイス間の MPLS VPN 接続性をチェックします。

図 11-4　L3VPN - CE to CE 接続性テスト



この場合、Diagnostics はコア、エッジ、および接続回線のトラブルシューティングを実行します。

IPv6 トラブルシューティング

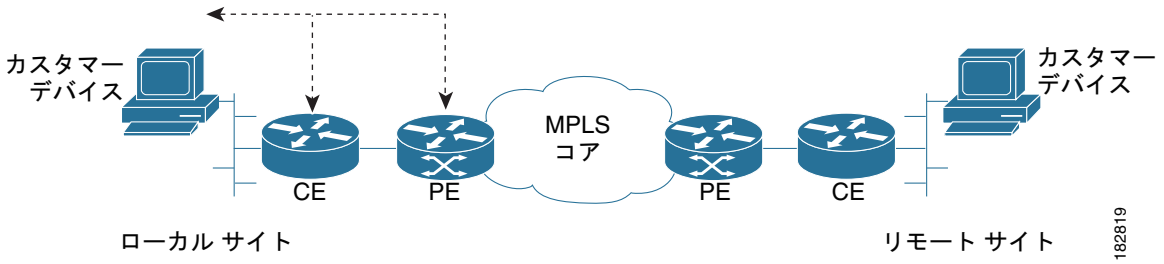
L3VPN - CE to CE テストでは、次のすべての条件が満たされている場合に、IPv6 セグメントのトラブルシューティングを起動します。

- インターフェイス選択画面でグローバル ユニキャスト IPv6 アドレスが入力された行を選択した、または指定したローカルおよびリモート PE アクセス回線インターフェイスがグローバル ユニキャスト IPv6 アドレスを持っている、またはデータベースでインターフェイスの詳細情報を使用できない場合。
- ローカルサイトおよびリモートサイトに指定した CE アクセス回線インターフェイス IP アドレスの両方がグローバル ユニキャスト IPv6 アドレスの場合。
- オプションで、ローカル サイトおよびリモート サイトの両方またはいずれか一方に指定したカスタマー デバイス IP アドレスがグローバル ユニキャスト IPv6 アドレスの場合。

L3VPN - PE to attached CE 接続性テスト

L3VPN - PE to attached CE 接続テスト（図 11-5）は、PE とローカルに接続された CE 間の VPN 接続性テストを実行します。この場合、Diagnostics はエッジおよび接続回線のトラブルシューティングを実行します。

図 11-5　L3VPN - PE to attached CE 接続性テスト



L3VPN - PE to attached CE 接続性テストは、逆の方向には実行できません。

接続の問題は、多くの場合ローカルの接続回線に原因があります。利用できない可能のあるリモートサイトの PE および CE の詳細を必要とせずに、ローカルの接続回線を単独でテストできます。

L3VPN - PE to attached CE 接続性テストによって、VRF 対応 IP SLA プローブで報告されるものと同じ接続回線の接続断を診断できます。この通知には、Diagnostics で対応するアクセス回線の接続性テストを設定するために必要な、すべての情報が含まれています。

IPv6 トラブルシューティング

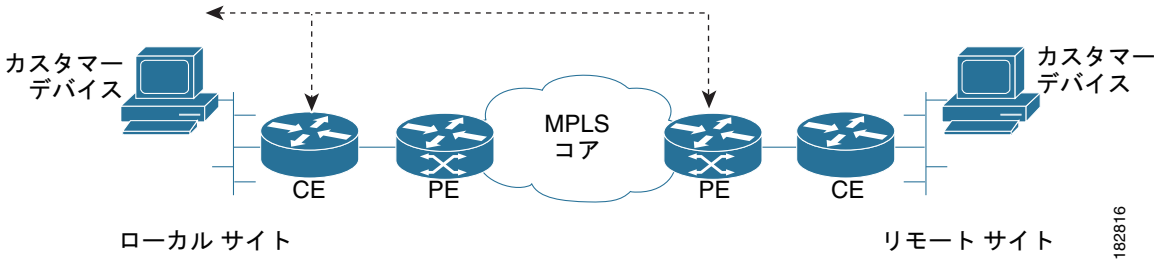
L3VPN - PE to attached CE テストでは、次のすべての条件が満たされている場合に、IPv6 セグメントのトラブルシューティングを起動します。

- インターフェイス選択画面でグローバル ユニキャスト IPv6 アドレスが入力された行を選択した、または指定した PE アクセス回線インターフェイスがグローバル ユニキャスト IPv6 アドレスを持っている、またはデータベースでインターフェイスの詳細情報を使用できない場合。
- 指定した CE アクセス回線インターフェイス IP アドレスがグローバル ユニキャスト IPv6 アドレスの場合。
- オプションで、指定したカスタマー デバイス IP アドレスがグローバル ユニキャスト IPv6 アドレスの場合。

L3VPN - CE to PE across Core 接続性テスト

L3VPN - CE to PE across Core 接続性テスト（図 11-6）は、MPLS コアをまたいだ、CE またはカスタマーデバイス（カスタマー デバイス IP アドレスが既知のもの）と PE 間の MPLS VPN 接続性をチェックします。

図 11-6　L3VPN - CE to PE across Core 接続性テスト



この場合、Diagnostics はコア、両方のエッジ、および接続回線のトラブルシューティングを実行します。

IPv6 トラブルシューティング

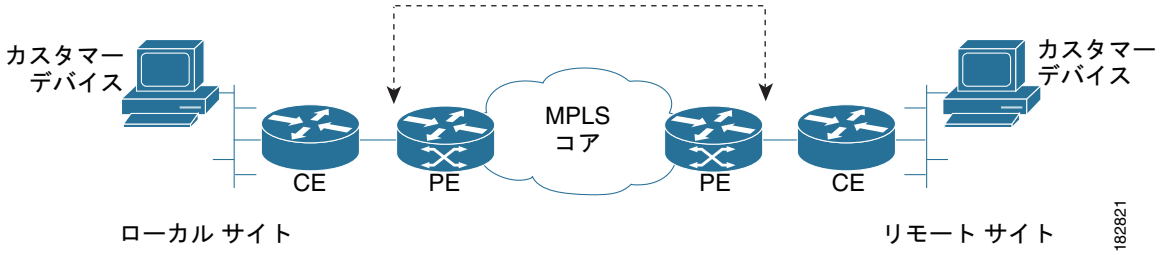
L3VPN - CE to PE across Core テストでは、次のすべての条件が満たされている場合に、IPv6 セグメントのトラブルシューティングを起動します。

- インターフェイス選択画面でグローバル ユニキャスト IPv6 アドレスが入力された行を選択した、または指定した PE アクセス回線インターフェイスがグローバル ユニキャスト IPv6 アドレスを持っている、またはデータベースでインターフェイスの詳細情報を使用できない場合。
- 指定した CE アクセス回線インターフェイス IP アドレスがグローバル ユニキャスト IPv6 アドレスの場合。
- オプションで、指定したカスタマー デバイス IP アドレスがグローバル ユニキャスト IPv6 アドレスの場合。
- 選択または指定された PE アクセス回線インターフェイスにグローバル ユニキャスト IPv6 アドレスがあるか、インターフェイス詳細がデータベースにない場合。

L3VPN - PE to PE in VRF 接続性テスト

VRF 接続性テストの L3VPN - PE to PE（図 11-7）は、2 つの PE 間の MPLS 接続性をチェックします。Diagnostics はコアおよび両側のエッジのトラブルシューティングを実行します。

図 11-7　　L3VPN - PE to PE in VRF 接続性テスト



組織によっては、コアまたはエッジ ネットワークをプロビジョニングしても、すぐには CE を割り当てないことがあります。L3VPN - PE to PE in VRF 接続性テストを使用すると、段階的にネットワークを展開してテストできます。また、このテスト オプションでは高い柔軟性も提供され、CE 情報の準備ができていないときにエッジまたはコア ネットワーク セグメントをテストできます。

さらに、L3VPN - PE to PE in VRF 接続性テストによって、VRF 対応 IP SLA プローブで報告されるものと同じ短距離（PE からリモート PE）VPN 接続断も診断できます。この通知には、Diagnostics で対応するエッジの接続性テストを設定するために必要な、すべての情報が含まれています。

IPv6 トラブルシューティング

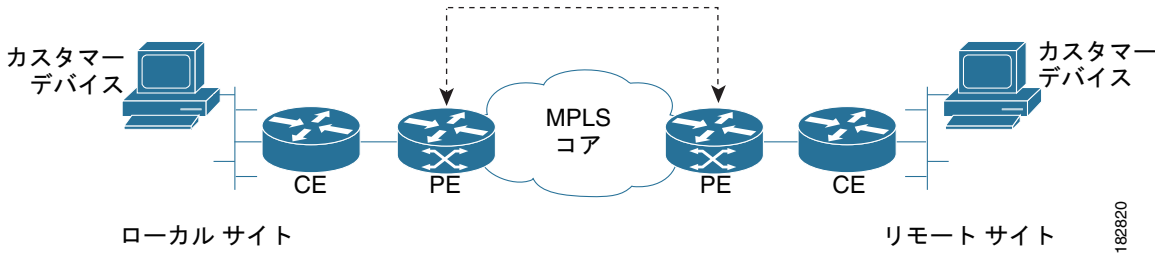
L3VPN - PE to PE in VRF テストでは、次のすべての条件が満たされている場合に、IPv6 セグメントのトラブルシューティングを起動します。

- グローバル ユニキャスト IPv6 アドレスを持つローカル サイト PE アクセス回線インターフェイスまたはリモート サイト PE アクセス回線インターフェイスのいずれかを、インターフェイス選択画面で選択する必要がある場合。
- インターフェイス選択画面でグローバル ユニキャスト IPv6 アドレスが入力された行を選択した、または指定したローカル PE アクセス回線インターフェイスがグローバル ユニキャスト IPv6 アドレスしか持っていない場合。
- インターフェイス選択画面でグローバル ユニキャスト IPv6 アドレスが入力された行を選択した、または指定したリモート PE アクセス回線インターフェイス IP アドレスがグローバル ユニキャスト IPv6 アドレスしか持っていない場合。

L3VPN - PE to PE 接続テスト

L3VPN - PE to PE コア接続性テスト（図 11-8）は、2 つの PE 間の MPLS 接続性をチェックします。

図 11-8　　L3VPN - PE to PE コア接続性テスト



L3VPN - PE to PE コア テストは、CE インターフェイスへのアクセスがブロックされている場合（たとえばアクセス リストの使用によるもの）または組織内の異なるグループが、それぞれ別のネットワーク セグメントについて責任を負っている場合を対象にしています。たとえば、Core グループの P に問題があるが、完全な CE-CE または PE-PE テストを実行するためのエンド カスタマーのコンテキストがない場合が該当します。

L3VPN - PE to PE コア テストによって、MPLS 対応 PE 間の接続性をテストする IP SLA ヘルス モニタ プローブで報告されるものと同じコア接続断を診断できます。この通知には、Diagnostics で対応するコアの接続性テストを設定するために必要な、すべての情報が含まれています。

IPv6 トラブルシューティング

コア内の L3VPN - PE to PE テストの場合、このテスト タイプは IPv4 アドレスのみを使用するため、IPv6 トラブルシューティングは開始できません。

MPLS VPN 接続性検証テストの実行

この項では、MPLS VPN 接続性検証テストの実行方法について説明します。ここでは、次の項目について説明します。

- 「[MPLS Diagnostics Expert Feature Selection] ウィンドウを開く」（P.11-18）
- 「L3VPN - CE to CE テストの選択、設定および実行」（P.11-19）
- 「L3VPN - PE to attached CE テストの選択、設定および実行」（P.11-32）
- 「L3VPN - CE to PE across Core テストの選択、設定、および実行」（P.11-33）
- 「L3VPN - PE to PE テストの選択、設定および実行」（P.11-34）
- 「MPLS - PE to PE テストの選択、設定および実行」（P.11-35）

（注）　IOS XR バージョン 3.8.0 以降のデバイスで実行される各コマンドでは、出力の最初の行に、Diagnostics が処理できなかったデバイスの現在のタイムスタンプが表示されます。XR デバイスのタイムスタンプを無効にするには、テストを起動する前に、*timestamp disable* コマンドを使用する必要があります。

[MPLS Diagnostics Expert Feature Selection] ウィンドウを開く

（注）　同じクライアント マシンで並行して複数の MPLS VPN 接続性検証テストを実行する場合は、各テストを異なる HTTP セッションで実行する必要があります。そのためには、コマンドライン、またはデスクトップのブラウザのアイコン、または [Start] メニューから起動した個別のブラウザで各テストを実行します。同じブラウザ ウィンドウの別のタブ、または既存のブラウザ ウィンドウから起動したブラウザ ウィンドウで、複数のテストを並行して実行しないでください。

ステップ 1　Prime Provisioning にログインします。ログイン方法の詳細については、*『Cisco Prime Provisioning 6.3 Installation Guide』* を参照してください（「**Installing and Logging Into Prime Provisioning**」>「**Logging In for the First Time**」）。

Prime Provisioning のホーム ウィンドウが表示されます。

ステップ 2　[Diagnostics] タブをクリックします。

[MPLS Diagnostics Expert Feature Selection] ウィンドウが表示され、使用できる MPLS VPN 接続性検証テスト タイプが示されます。

（注）　また、少なくとも 1 つの Diagnostics ユーザ ロールが割り当てられていることを確認する必要があります。「ユーザ ロール」（P.11-7）を参照してください。

（注）　使用できるテスト タイプは、割り当てられているユーザ ロールによって決まります。ユーザ ロールは、テスト タイプごとに定義する必要があります。テスト タイプにアクセスできない場合、そのテスト タイプは [MPLS Diagnostics Expert Feature Selection] ウィンドウに表示されません。詳細については、「ユーザ ロール」（P.11-7）を参照してください。

L3VPN - CE to CE テストの選択、設定および実行

この項では、L3VPN - CE to CE テスト タイプを選択、設定、および実行する方法の詳細について説明します。

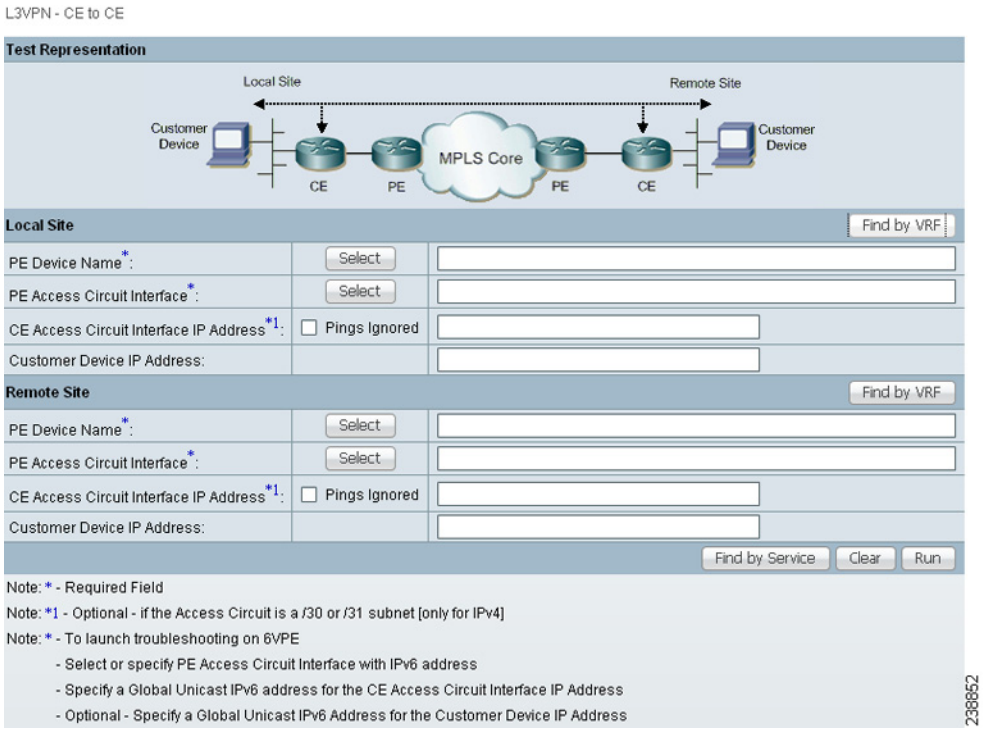
ステップ 1　[Diagnostics] メニューから、[L3VPN - CE to CE] テスト タイプを選択します。

ステップ 2　[L3VPN - CE to CE] 接続性検証テスト タイプをクリックします。

L3VPN - CE to CE 接続性検証テスト タイプの詳細については、「L3VPN - CE to CE 接続性テスト」（P.11-14）を参照してください。[L3VPN - CE to CE] ウィンドウが表示され、L3VPN - CE to CE テスト タイプに対応する入力ウィンドウが表示されます。

ヒント　使用できるテスト タイプごとに独自の入力ウィンドウがあり、異なるパラメータのセットを必要とします。たとえば、L3VPN - CE to CE テストにはローカル サイトとリモート サイトの両方の情報が必要で、L3VPN - PE to attached CE テストのテスト設定ウィンドウではローカル サイトの詳細だけが要求されます。

図 11-9　L3VPN - CE to CE テスト タイプ



[L3VPN - CE to CE] ウィンドウを使用して、実行する接続性テストを設定できます。

このウィンドウには、次のコンポーネントが表示されます。

- ネットワーク図
- ローカル サイト設定領域
- リモート サイト設定領域

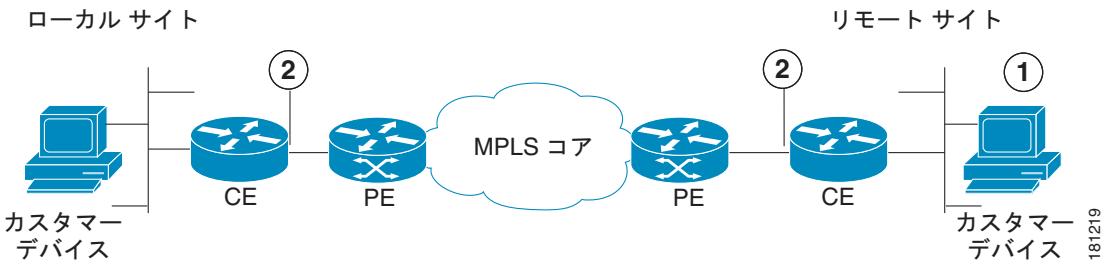
ネットワーク図は、テストを設定するために入力する必要がある情報のコンテキストを提供する静的なイメージです。

MPLS VPN 接続性検証は、VPN 内にある 2 つのサイト間の接続性をテストします。テストを通じて、これらのサイトはローカル サイトおよびリモート サイトと呼ばれます。接続性の問題は、特定のサイトの視点から報告または検出されることが予想されます。通常は、この特定のサイトをローカル サイトとして使用し、このサイトからテストを実行します。ただし、これは必須ではありません。接続性は両方向でテストできるため、どちらのサイトもローカル サイトまたはリモート サイトとして使用できます。

L3 VPN 接続性テストの範囲（図 11-10 を参照）は、サイトごとに変更できます。サイトごとに、そのサイト内にあるカスタマー デバイスへの接続性（図 11-10 の *1*）、または CE アクセス回線インターフェイスへの接続性（図 11-10 の *2*）をテストできます。テスト範囲は、指定した設定によって決まります。

カスタマー デバイスの IP アドレスが既知の場合は、そのデバイスへの接続性検証テストを実行することを推奨します。カスタマー デバイスの IP アドレスが未知の場合は、サイトの CE までの接続性検証テストを実行できます。

図 11-10　テスト範囲



1. カスタマー デバイス。
2. CE アクセス回線インターフェイス。

カスタマー サイトのサブネットワーク内にあるデバイスへの接続性をテストするには、[Customer Device IP Address] フィールドにデバイスの IP アドレスを入力します。デフォルトでは、サイトの必須フィールドだけを指定した場合、CE アクセス回線インターフェイスへのテストが実行されます。

（注） 必須フィールドは、[L3VPN - CE to CE Diagnostics - Test Setup] ウィンドウに、青いアスタリスクで示されています。すべての必須フィールドに有効な情報が入力されるまでは、次に進めません。

（注） /30 または /31 アドレッシングが使用されている場合は、[CE Access Circuit Interface IP Address] フィールドは Diagnostics により自動的に入力されます。

Cisco IOS および Cisco IOS XR アクセス コントロール リスト（ACL）により、さまざまな基準に基づいて選択したトラフィックがブロックされるようにできます。カスタマー デバイスまたは CE インターフェイスへの MPLS VPN 接続性検証テストを実行したときに、CE 上で設定されている ACL が原因で、矛盾した結果が報告される場合があります。可能な場合、MPLS VPN 接続性検証テストは、CE デバイス上で設定されている ACL によってトラフィックがブロックされたことを報告します。ただし ACL の設定によっては、CE デバイス上で設定されている ACL によってトラフィックがブロックされたことを識別できない場合があります。場合によっては、MPLS VPN 接続性検証テストでアクセス回線の障害または不明な障害が報告されることがあります。トラフィックが CE でブロックされている疑いがある場合は、そのサイトの [Pings Ignored] チェックボックスをオンにしてください。このようにすると、Diagnostics はトラブルシューティング時にブロッキング アクセス ACL を考慮し、見つかった問題についてより正確な診断が返されます。

（注） サイトの [Pings Ignored] チェックボックスをオンにした場合は、CE IP アドレスとオプションで [Customer Device IP Address] フィールドを使用して、PE デバイスでトラブルシューティングおよび設定チェックが実行されます。

ステップ 3　必要に応じて [L3VPN - CE to CE] ウィンドウのフィールドを設定します。

表 11-3 には、[L3VPN - CE to CE] ウィンドウのフィールド説明が表示されています。

（注） 表示されるフィールドは、選択したテスト タイプによって異なります。たとえば、CE to CE テストにはローカル サイトとリモート サイトの両方の情報が必要で、PE to attached CE テストのテスト設定ウィンドウではローカル サイトの詳細だけが要求されます。

（注）　テストを設定する別の方法として、カスタマー VPN 情報を使用する方法があります。詳細については、「カスタマー VPN/VRF 情報を使用した設定」（P.11-31）を参照してください。

表 11-3　[L3VPN - CE to CE Diagnostics - Test Setupp] ウィンドウのフィールドの説明

フィールド	有効なテストタイプ	説明
Find by VRF	All	[Find by VRF] ボタンをクリックして、VRF 検索を使用して特定される PE ホスト名または PE インターフェイスの詳細を使用するテストを設定します。（「カスタマー VRF 情報を使用した設定」（P.11-29）を参照）。
PE Device Name	All	[PE Device Name] フィールドにサイトの PE デバイス名を入力するか、[Select] ボタンをクリックしてサイトの PE デバイス名を選択します。 （注）　[Select] ボタンをクリックすると、[Select PE Device] ウィンドウが開きます。（「PE デバイスの選択」（P.11-25）を参照してください）。 デバイス名は、デバイスの完全修飾ホスト名およびドメイン名です。たとえば、router1.cisco.com とします。ただし、ドメイン名はオプションであるため、多くの場合デバイス名はデバイスのホスト名です。たとえば、router1 とします。 指定するデバイス名は、ロール タイプが N-PE の PE デバイスのデバイス名と一致する必要があります。

表 11-3　[L3VPN - CE to CE Diagnostics - Test Setupp] ウィンドウのフィールドの説明 （続き）

フィールド	有効なテスト タイプ	説明
LSP Endpoint Loopback IP Address	L3VPN - PE to PE コアのみ	BGP ネクスト ホップがピア PE の BGP ルータ ID と異なる場合は、BGP ネクスト ホップを入力します。ループバック IP アドレスを入力するか、IP アドレスに解決されるループバック名を入力できます。 コアをテストするときは、ローカル PE からリモート PE に MPLS OAM ping およびトレースが実行されます。この ping の宛先によって、ローカル PE のルーティング情報に基づいて LSP が選択されます。 カスタマー トラフィックは、カスタマー ルートの BGP ネクスト ホップ アドレスを宛先として使用し、LSP を選択します。Diagnostics がテストする IP プレフィックスがカスタマー トラフィックで使用される BGP ネクスト ホップ アドレスと一致していることを確認してください。これによって、Diagnostics はカスタマー トラフィックが経由する LSP と同じ LSP をテストするようになります。 L3VPN - PE to PE コア テストの場合、Diagnostics はカスタマー ルート情報を持っていません。そのため、Diagnostics は BGP ネクスト ホップを識別できず、ping の宛先の選択はネクスト ホップではなくリモート PE の BGP ルータ ID に基づきます。 ネットワーク設定によっては、このルータ ID がカスタマー トラフィックで使用されるネクスト ホップと一致せず、不正な LSP がテストされる（または、どの LSP もテストされない）ことがあります。 これは、次のような場合に発生します。 • BGP ルータ ID が、LSP が割り当てられていないループバックのアドレスである。 • BGP ルータ ID がループバックのアドレスでない。 • カスタマーが複数の定義済み LSP を持っており、カスタマー トラフィックはルータ ID により与えられた LSP 以外の LSP を使用している。 • カスタマーが複数の定義済み LSP を持っており、カスタマー トラフィックがルートマップに基づいて LSP を切り替える。 上記の場合は、正しい BGP ネクスト ホップを指定する必要があります。 **（注）** LSP エンドポイント ループバック IP アドレスを指定することで、Diagnostics は MPLS コアにある複数の LSP でコアの障害をテストおよび検出できるようになります。 詳細については、「MPLS - PE to PE テストへの LSP エンドポイント ループバック IP アドレスの設定」（P.11-36）を参照してください。
PE Access Circuit Interface	L3VPN - CE to CE L3VPN - PE to attached CE L3VPN - CE to PE across Core L3VPN - PE to PE in VRF	[PE Access Circuit Interface] フィールドに PE アクセス回線インターフェイスのインターフェイス名を入力するか、[Select] ボタンをクリックして PE アクセス回線インターフェイスを選択します。 **（注）** [Select] ボタンをクリックすると [Select Device Interface] ウィンドウが開きます（「PE アクセス回線インターフェイスの選択」（P.11-25）を参照）。 PE アクセス回線インターフェイスを選択するには、有効な PE デバイス名を指定しておく必要があります。指定されたインターフェイスは、サイトの CE に接続されているアクセス回線インターフェイスになっている必要があります。指定されたインターフェイス名は、デバイスのインターフェイスと一致する必要がありますが、必ずしも Prime Provisioning デバイス インベントリに存在する必要はありません。

表 11-3　[L3VPN - CE to CE Diagnostics - Test Setupp] ウィンドウのフィールドの説明 （続き）

フィールド	有効なテスト タイプ	説明
CE Access Circuit Interface IP Address	L3VPN - CE to CE L3VPN PE to attached CE L3VPN - CE to PE across Core	ローカル サイトの CE アクセス回線インターフェイスの IP アドレスを入力します。これは、指定された PE に接続されているアクセス回線インターフェイスにする必要があります。 IPv4 アドレッシングと /30 サブネット マスク（255.255.255.252）または /31 サブネット マスク（255.255.255.254）を使用して設定された PE アクセス回線インターフェイスが選択された場合、その /30 または /31 サブネットで残っているホスト アドレスが [CE Access Circuit Interface IP Address] フィールドに自動的に入力されます。/31 マスク（255.255.255.254）サブネット マスクで設定されている PE アクセス回線インターフェイスを手動で入力した場合、CE アクセス回線インターフェイス IP アドレスの取得は、テストの開始後でないと試行されません。この場合、[CE Access Circuit Interface IP Address] フィールドは [OK] ボタンをクリックするまで自動入力されません。 PE アクセス回線インターフェイスが IP アンナンバードを使用している場合、または CE アクセス回線インターフェイスが別のサブネットにある場合、正しい CE アクセス回線インターフェイス IP アドレスを取得できません。 このテストは、管理対象および管理対象外のシスコ製 CE デバイスおよび他社製 CE デバイスをサポートしています。
Pings Ignored	L3VPN - CE to CE L3VPN - PE to attached CE L3VPN - CE to PE across Core	このチェックボックスをオンにして、プロバイダー コア ネットワークから発信された ping およびトレース ルート パケットを無視する ACL が CE で設定されていることを指定します。
Customer Device IP Address	L3VPN - CE to CE L3VPN - PE to attached CE L3VPN - CE to PE across Core	ローカル サイト カスタマー ネットワーク上のカスタマー デバイス IP アドレスを入力します。カスタマー デバイスの IP アドレスを入力すると、このデバイスへの接続性テストが実行されます。
Find by Service	All	[Populate using VPN/VRF] ウィンドウを開くには、[Find by Service] ボタンをクリックします。[Populate using VPN/VRF] ウィンドウでは、カスタマー VPN/VRF 情報を使用してテストを設定できます（「カスタマー VPN/VRF 情報を使用した設定」（P.11-31）を参照）。
[OK] ボタン	All	[OK] をクリックして、テストを実行します。
[Clear] ボタン	All	[Clear] をクリックして、ウィンドウのすべてのフィールドをリセットします。

ステップ 4　すべての必須フィールドに入力したら、[OK] をクリックしてテストを実行します。

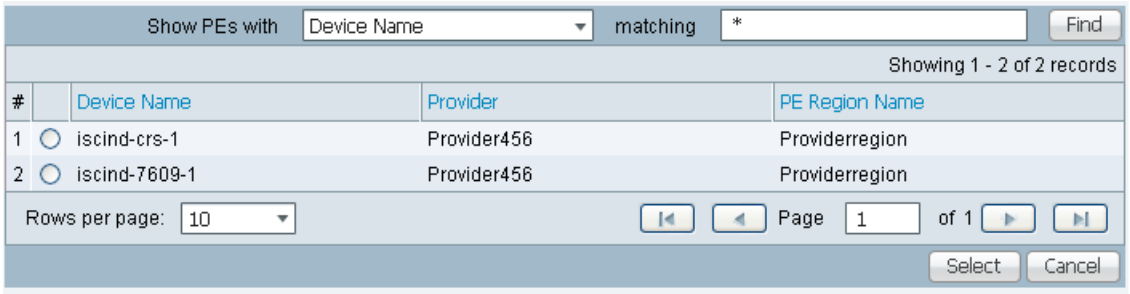
[Progress] ウィンドウが表示されます。「[Progress] ウィンドウ」（P.11-39）を参照してください。

PE デバイスの選択

（ローカルまたはリモートの [PE Device Name] の）[Select] ボタンをクリックすると、[Select PE Device] ウィンドウ（図 11-11 を参照）が開き、ローカルまたはリモート サイト PE を選択できます。[Select PE Device] ウィンドウには、インベントリで使用できるすべての PE デバイスを含むテーブルが表示されます。

（注）　Diagnostics デバイス セレクタのデフォルト値を設定できます。図 11-11 を参照してください。設定可能な値は、[Device Name]、[Provider]、および [PE Region Name] です。

図 11-11　[Select PE Device] ウィンドウ

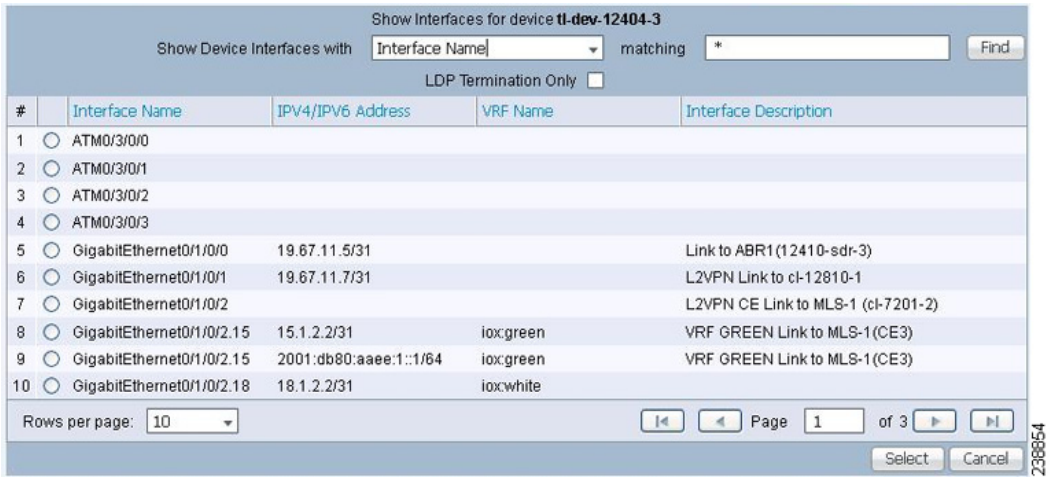


（注）　PE 表に表示されるすべての PE 属性について、ワイルドカードを使用した文字列検索を実行できます。Prime Provisioning インベントリからローカルまたはリモート サイトの PE を選択すると、ローカルまたはリモートの [PE Device Name] フィールドに入力されたすべての値が上書きされます（図 11-9 を参照）。この検索機能は、大量の PE がある大規模なネットワークで便利です。

PE アクセス回線インターフェイスの選択

（ローカルまたはリモートの [PE Access Circuit Interface] の）[Select] ボタンをクリックすると、[Select Device Interface] ウィンドウ（図 11-12 を参照）が開き、インターフェイス名を選択できます。[Select Device Interface] ウィンドウには、選択されたローカルまたはリモート PE デバイスのすべてのインターフェイスを含むテーブルが表示されます。

図 11-12　[Select Device Interface] ウィンドウ



表に表示されるすべての属性について、ワイルドカードを使用した文字列検索を実行できます。Prime Provisioning インベントリからローカルまたはリモートの PE アクセス回線インターフェイスを選択すると、ローカルまたはリモートの [PE Access Circuit Interface] フィールドに入力されたすべての値が上書きされます（図 11-9 を参照）。

表 11-4 に、[Select Device Interface] ウィンドウのフィールドの説明を示します。

ワンポイントアドバイス

[Show Device Interfaces with] ドロップダウン ボックスと [matching] フィールドを使用して、最初に適切な検索パターンを入力します（図 11-12 を参照）。これによって、大規模なネットワークで発生する、大きくて時間がかかる余分な検索をせずに済みます。表 11-4 に、[Select Device Interface] ウィンドウのフィールドの説明を示します。

表 11-4　[Select Device Interface] ウィンドウのフィールドの説明

フィールド	説明
Show Device Interfaces with	[Show Devices with] ドロップダウン ボックスを使用して、検索結果を調整できます。ドロップダウン メニューから [Interface Name]、[IPV4 Address]、[IPV6 Address]、[VRF Name]、または [Interface Description] を選択して、検索結果を調整するカテゴリを選択します。
matching（オプション フィールド）	[Show Devices with] ドロップダウン ボックスで選択したカテゴリ内の検索を調整するための情報を、[matching] フィールドに入力します。部分文字列としてテキストを入力します。ワイルドカードもサポートされます。
LDP Termination Only	[LDP Termination Only] チェックボックスは、LDP 終端ループバック インターフェイスの選択が必要な場合に、LDP 終端ループバック インターフェイスをフィルタリングするために使用します。このチェックボックスは、オフのままにします。
Find	[Find] をクリックして、[Select Device Interface] ウィンドウで設定した情報を使用して検索を実行します。

表 11-4　[Select Device Interface] ウィンドウのフィールドの説明 （続き）

フィールド	説明
Interface Name	検索の実行後、見つかったインターフェイスのリストが表示されます。[Interface Name] カラムのヘッダーをクリックすると、インターフェイス名のリストがソートされます。
IPV4/IPV6 Address	検索の実行後、見つかった IPV4/IPV6 アドレスのリストが表示されます。[IPV4/IPV6 Address] カラムのヘッダーをクリックすると、IPV4/IPV6 アドレスのリストがソートされます。 IPV6 アドレスを選択するには、既存のリストから選択するか、手動で入力します。
VRF Name	検索の実行後、見つかった VRF 名のリストが表示されます。[VRF Name] カラムのヘッダーをクリックすると、VRF 名のリストがソートされます。
Interface Description	検索の実行後、見つかったインターフェイスの説明のリストが表示されます。[Interface Description] カラムのヘッダーをクリックすると、インターフェイスの説明のリストがソートされます。
Row per page	表に表示される行の行数が表示されます。テーブルの行を選択するには、対応するオプション ボタンをクリックします。
Select	[Select] をクリックして、テーブルでの選択を確認します。テーブルで選択した値が [PE Access Circuit Interface] フィールドに入力された状態で、[L3VPN - CE to CE Diagnostics] ウィンドウが表示されます。
Cancel	[Cancel] をクリックすると、[Select Device for VRF Search] ウィンドウが閉じます。

ヒント　[Interface Description] を使用して、カスタマー接続の詳細を記述することを推奨します。Diagnostics では、[Interface Description] の検索ができます（カスタマー回線 ID など）。詳細については、「L3VPN - CE to PE across Core テストの選択、設定、および実行」（P.11-33）および「L3VPN - PE to PE テストの選択、設定および実行」（P.11-34）を参照してください。

IOS マルチリンク アクセス回線インターフェイス間のテスト

Diagnostics では、Cisco IOS マルチリンク アクセス回線インターフェイスをまたがるトラブルシューティングがサポートされます。トラブルシューティングは、マルチリンク バンドル インターフェイスでのみ実行されます。個別のバンドル リンクのトラブルシューティング、またはマルチリンク固有のトラブルシューティングは実行されません。次のマルチリンク技術がサポートされます。

- マルチリンク PPP over Frame Relay（マルチリンク グループ インターフェイス設定）
- マルチリンク PPP over Frame Relay（仮想テンプレート インターフェイス設定）
- マルチリンク PPP over ATM（マルチリンク グループ インターフェイス設定）
- マルチリンク PPP over ATM（仮想テンプレート インターフェイス設定）
- シリアル上のマルチリンク PPP
- マルチリンク フレームリレー

（注）　マルチリンクは Cisco IOS でのみサポートされ、Cisco IOS XR ではサポートされません。

（注）　マルチリンク アクセス回線インターフェイスでは、レイヤ 2 フレーム リレー、ATM、およびイーサネットのトラブルシューティングは実行されません。

各マルチリンク バンドルには、関連付けられている多数のインターフェイスがあります。マルチリンク アクセス回線で MPLS VPN 接続性検証テストを設定するときは、正しいインターフェイスを [MPLS VPN Test Configuration] ウィンドウの [PE Access Circuit Interface] フィールドに入力する必要があります。入力する必要があるインターフェイスは、使用するマルチリンク設定に応じて異なります。表 11-5 で、[PE Access Circuit Interface] フィールドに入力する必要があるインターフェイスについてマルチリンク技術ごとに説明します。

表 11-5　マルチリンク インターフェイス

マルチリンク技術	PE アクセス回線インターフェイス
ML-PPPoFR（マルチリンク グループ）	マルチリンク バンドルを表すマルチリンク インターフェイス。
ML-PPPoFR（Virtual-Template）	マルチリンク バンドルを表す仮想アクセス インターフェイス。
ML-PPPoATM（マルチリンク グループ）	マルチリンク バンドルを表すマルチリンク インターフェイス。
ML-PPPoATM（Virtual-Template）	マルチリンク バンドルを表す仮想アクセス インターフェイス。
ML-PPPoSerial	マルチリンク バンドルを表すマルチリンク インターフェイス。
ML-FR	仮想回線を設定しているフレーム リレー インターフェイス。これは、Multilink Frame Relay（MFR; マルチリンク フレーム リレー）インターフェイスまたは MFR インターフェイスのフレーム リレー サブインターフェイスの場合があります。

マルチリンク フレーム リレー（MFR）を除き、マルチリンク バンドルを表すインターフェイスを [PE Access Circuit Interface] フィールドに入力する必要があります。マルチリンク フレーム リレーの場合は、フレーム リレー インターフェイス、または仮想回線が設定されているサブインターフェイスを入力する必要があります。これは、MFR インターフェイスまたは MFR インターフェイスのサブインターフェイスの場合があります。いずれの場合も、[PE Access Circuit Interface] フィールドに入力されたインターフェイスには IP アドレスと VRF が必要で、アップ/アップ状態になっている必要があります。

PE デバイスの有効なマルチリンク バンドル インターフェイスを判別するには、**show ppp multilink** または **show frame-relay multilink** IOS コマンドを使用します。PE デバイスにアクティブなマルチリンク バンドルがない場合、設定済みマルチリンク バンドルがないか、設定済みマルチリンク バンドルのすべてのバンドル リンクがダウン/ダウン状態になっている可能性があります。

（注）　仮想アクセス インターフェイスは、動的に作成されて、割り当てられます。仮想アクセス インターフェイスが属するマルチリンク バンドルと、その役割は、インターフェイスの状態が変化するに従って変化することがあります。そのため、仮想アクセス インターフェイスは Prime Provisioning/Diagnostics リポジトリに保存されません。仮想アクセス インターフェイスを使用して VPN 接続性検証テストを設定するときは、手動でインターフェイス名を [MPLS VPN Test Configuration] ウィンドウの [PE Access Circuit Interface] フィールドに入力する必要があります。[Interface Selection] ポップアップ ダイアログボックスから仮想アクセス インターフェイスを選択することはできません。

カスタマー VRF 情報を使用した設定

[MPLS VPN Connectivity Verification] ウィンドウに情報を入力するときは、PE ホスト名または PE インターフェイスの詳細を入力する必要があります。場合によっては、PE ホスト名または PE インターフェイスの詳細がわからないことがあります。ただし、この情報は対応する既知の VRF 名によって識別できます。対応する VRF 名は、VRF 検索を使用して識別できます。

（注） VRF 名でインターフェイスを検索するには、あらかじめ Prime Provisioning タスク マネージャの Collect Configuration タスクを実行し、VRF 名を Prime Provisioning にアップロードしておく必要があります。VRF 検索は、最後に実行した Collect Configuration タスク内の情報に基づきます。タスク マネージャの Collect Configuration タスクの実行方法の詳細については、「デバイス設定の収集」（P.11-12）を参照してください。

ステップ 1　[MPLS VPN Connectivity Verification] ウィンドウの [Find by VRF] ボタンをクリックします。

[Select Device for VRF Search] ウィンドウが表示されます。

（注） [Select Device for VRF Search] ウィンドウに表示されるフィールドは、PE データ フィールドに入力されているかどうかにかかわらず、最初は空です。

ステップ 2　[Select Device for VRF Search] ウィンドウに表示されるフィールドを設定します。

表 11-6 に、[Select Device for VRF Search] ウィンドウのフィールドの説明を示します。

ワンポイントアドバイス まず、該当する検索パターンを入力します。これによって、大規模なネットワークで発生する、大きくて時間がかかる余分な検索をせずに済みます。VRF 名のパターンを入力し、[Find] ボタンをクリックします。たとえば、*t** と入力して [Find] をクリックすると、文字 *t* で始まるすべての VRF のリストが表示されます。[Show Devices with] ドロップダウン ボックスから選択し、[matching] フィールドに情報を入力して [Find] をクリックすると、結果リストをさらにフィルタリングできます。表 11-6 に、[Select Device for VRF Search] ウィンドウのフィールドの説明を示します。

表 11-6　[Select Device for VRF Search] ウィンドウのフィールドの説明

フィールド	説明
VRF Search String	検索する VRF 名の文字列を入力します。部分文字列として VRF 名の文字列を入力します。ワイルドカードもサポートされます。
Show Devices with	[Show Devices with] ドロップダウン ボックスを使用して、検索結果を調整できます。ドロップダウン メニューから [Device Name]、[Interface Name]、[IPV4 Address]、[IPV6 Address]、または [Interface Description] を選択して、検索結果を調整するカテゴリを選択します。
matching（オプション フィールド）	[Show Devices with] ドロップダウン ボックスで選択したカテゴリ内の検索を調整するための情報を、[matching] フィールドに入力します。部分文字列としてテキストを入力します。ワイルドカードもサポートされます。
Find	[Find] をクリックして、[Select Device for VRF Search] ウィンドウで設定した情報を使用して VRF 検索を実行します。

表 11-6　[Select Device for VRF Search] ウィンドウのフィールドの説明 （続き）

フィールド	説明
Device Name	検索の実行後、見つかったデバイス名のリストが表示されます。[Device Name] カラムのヘッダーをクリックすると、デバイス名のリストがソートされます。
Interface Name	検索の実行後、見つかったインターフェイスのリストが表示されます。[Interface Name] カラムのヘッダーをクリックすると、インターフェイス名のリストがソートされます。
IPV4/IPV6 Address	検索の実行後、見つかった IPV4/IPV6 アドレスのリストが表示されます。[IPV4/IPV6 Address] カラムのヘッダーをクリックすると、IPV4/IPV6 アドレスのリストがソートされます。 IPV6 アドレスを選択するには、既存のリストから選択するか、手動で入力します。
VRF Name	検索の実行後、見つかった VRF 名のリストが表示されます。[VRF Name] カラムのヘッダーをクリックすると、VRF 名のリストがソートされます。
Interface Description	検索の実行後、見つかったインターフェイスの説明のリストが表示されます。[Interface Description] カラムのヘッダーをクリックすると、インターフェイスの説明のリストがソートされます。
Rows per page	表に表示される行の行数が表示されます。テーブルの行を選択するには、対応するオプション ボタンをクリックします。
Select	[Select] をクリックして、テーブルでの選択を確認します。テーブルで選択した値が [PE Device Name] および [PE Access Circuit Interface] フィールドに入力された状態で、[L3VPN - CE to CE Diagnostics - Test Setup] ウィンドウが表示されます。
Cancel	[Cancel] をクリックすると、[Select Device for VRF Search] ウィンドウが閉じます。

ステップ 3　[Find] をクリックして、検索を開始します。

[Select Device for VRF Search] ウィンドウに表示されるテーブルに、検索結果が入力されます。

ヒント　各カラムに表示されている情報をソートするには、カラム見出しをクリックします。

ヒント　[VRF Name] および [Interface Description] カラムの情報を表示するため、必要に応じてテーブルの幅が自動的に拡大されます。テーブルの幅が拡大された場合は、水平方向のスクロールバーを使用してウィンドウの右側にスクロールします。

ステップ 4　（任意）[Show Devices with] ドロップダウン ボックスおよび [matching] フィールドを設定して、検索結果を調整します。

[Find] をクリックして、検索結果でテーブルを更新します。

ステップ 5　オプション ボタンをクリックして、必要な PE デバイス名とインターフェイス名を選択します。

ステップ 6　[Select] をクリックします。

[Select Device for VRF Search] ウィンドウが閉じます。選択した値が [PE Device Name] および [PE Access Circuit Interface] フィールドに入力された状態で、[L3VPN - CE to CE Diagnostics - Test Setup] ウィンドウが表示されます。

カスタマー VPN/VRF 情報を使用した設定

Diagnostics は、他の Prime Provisioning 機能から独立して、スタンドアロンで使用できます。ただし、Prime Provisioning VPN/VRF プロビジョニング機能を使用してネットワーク内で VPN/VRF をプロビジョニングしている場合は、MPLS VPN 接続性検証テストを設定する代替手段として、カスタマーおよび VPN/VRF に関連付けられているこのプロビジョニング情報を使用できます。デバイス固有の設定を指定するのではなく、カスタマー、VPN/VRF、ローカル サイト、およびリモート サイトを指定します。必要なすべてのテスト設定は、この情報から取得されます。

（注） カスタマー VPN/VRF 情報を使用して MPLS VPN 接続性検証テストを設定するオプションは、Prime Provisioning VPN/VRF プロビジョニング機能を使用してネットワーク内で VPN/VRF をプロビジョニングしている場合にのみ使用できます。

ステップ 1　[L3VPN - CE to CE Diagnostics - Test Setup] ウィンドウの [Find by Service] ボタンをクリックします。

[Populate using VPN/VRF] ウィンドウが表示されます。

ステップ 2　[Populate using VPN/VRF] ウィンドウに表示されるフィールドを設定します。

表 11-7 に、[Populate using VPN/VRF] ウィンドウのフィールドの説明を示します。

表 11-7　[Populate using VPN/VRF] ウィンドウのフィールドの説明

フィールド	説明
カスタマーの詳細	
Customer Name	[Select] ボタンをクリックして、[Select Customer] ポップアップ ウィンドウからカスタマーを選択します。
VPN/VRF Name	[Select] ボタンをクリックして、[VPN/VRF name] ポップアップ ウィンドウから VPN/VRF 名を選択します。 **（注）** カスタマー名を選択してからでないと、VPN/VRF 名は選択できません。
サイトの詳細	
Local Site	[Select] ボタンをクリックして、[Local Site] ポップアップ ウィンドウからローカル サイトを選択します。 **（注）** カスタマー名および VPN/VRF 名を選択してからでないと、ローカル サイトは選択できません。
Remote Site	[Select] ボタンをクリックして、[Remote Site] ポップアップ ウィンドウからリモート サイトを選択します。 **（注）** カスタマー名および VPN/VRF 名を選択してからでないと、リモート サイトを選択できません。 **（注）** [Remote Site] フィールドは、PE to attached CE テスト タイプでは使用できません。

ステップ 3　[OK] をクリックします。

[L3VPN - CE to CE Diagnostics - Test Setup] ウィンドウが再表示されます。[Populate using VPN/VRF] ウィンドウで指定したカスタマー VPN/VRF 情報に基づいて、必要なフィールドが入力されます。

（注）　カスタマー デバイスをテストする場合は、ローカルまたはリモート サイトの [Customer Device IP Address] フィールドに IP アドレスを入力できます。

（注）　自動入力された [L3VPN - CE to CE Diagnostics - Test Setup] ウィンドウの任意のフィールドを編集できます。

ステップ 4　[L3VPN - CE to CE Diagnostics - Test Setup] ウィンドウの [OK] をクリックして、テストを実行します。

[Progress] ウィンドウが表示されます（「[Progress] ウィンドウ」（P.11-39）を参照）。

VPN トポロジ

デフォルトで、MPLS VPN 接続性検証テストでは、ローカル サイトとリモート サイトはフル メッシュ VPN トポロジで接続され、これらのサイトは直接通信できると見なされます。テストするサイトがフル メッシュ以外の VPN トポロジで接続されている場合、MPLS VPN 接続性検証テストに必要な設定が異なる場合があります。この場合、テストから誤った結果が得られることがあります。そのため、テスト結果を解釈するときには注意が必要です。サポートされる各 VPN トポロジで必要な設定の詳細、およびテスト結果の解釈方法については、「VPN トポロジ」（P.11-51）を参照してください。

L3VPN - PE to attached CE テストの選択、設定および実行

この項では、L3VPN - PE to attached CE テスト タイプを選択、設定、および実行する方法の詳細について説明します。

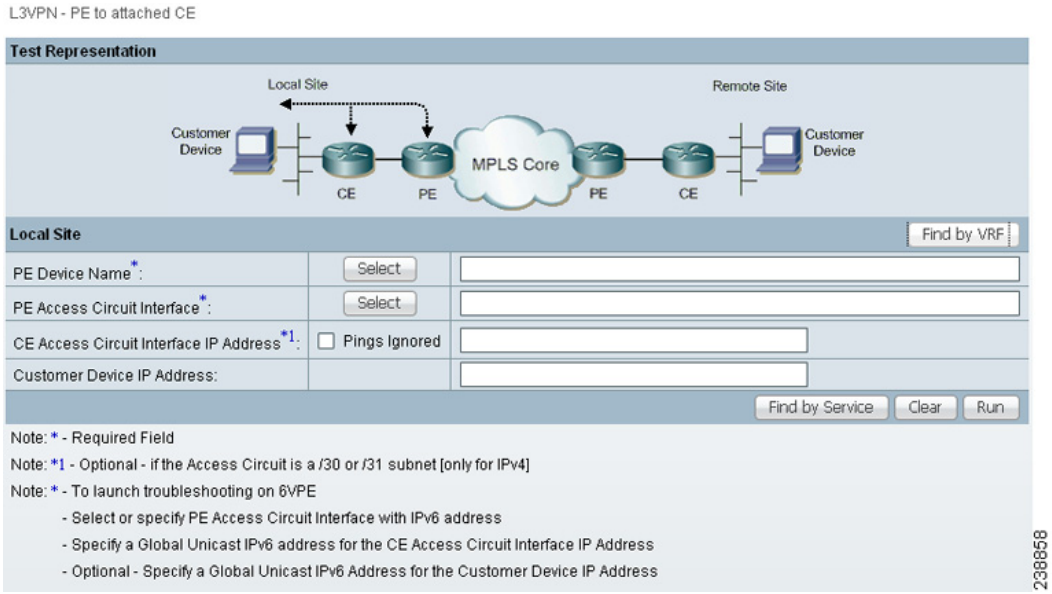
ステップ 1　[Diagnostics] メニューから、[L3VPN - PE to Attached CE] テスト タイプを選択します。

ステップ 2　[L3VPN - PE to attached CE] 接続性検証テスト タイプをクリックします。

PE to attached CE 接続性検証テスト タイプの詳細については、「L3VPN - PE to attached CE 接続性テスト」（P.11-15）を参照してください。

[MPLS VPN Connectivity Verification Configuration] ウィンドウ（図 11-13 を参照）が表示され、PE to attached CE テスト タイプに対応したフィールドが表示されます。[MPLS VPN Connectivity Verification Configuration] ウィンドウで、実行する接続性テストを設定できます。

図 11-13　L3VPN - PE to Attached CE テスト タイプ



[L3VPN - PE to Attached CE] ウィンドウには、次のコンポーネントが表示されます。

- ネットワーク図
- ローカル サイト設定領域

  これらのコンポーネントおよびテスト範囲については、「L3VPN - CE to CE テストの選択、設定および実行」（P.11-19）に詳しい説明があります。

ステップ 3　必要に応じて [L3VPN - PE to Attached CE] ウィンドウのフィールドを設定します。

表 11-3（P.11-22）に、L3VPN - PE to attached CE テスト タイプに対応するフィールドの説明を示します。

ステップ 4　すべての必須フィールドに入力したら、[OK] をクリックしてテストを実行します。[Progress] ウィンドウが表示されます。「[Progress] ウィンドウ」（P.11-39）を参照してください。

L3VPN - CE to PE across Core テストの選択、設定、および実行

この項では、L3VPN - CE to PE across Core テスト タイプを選択、設定、および実行する方法の詳細について説明します。

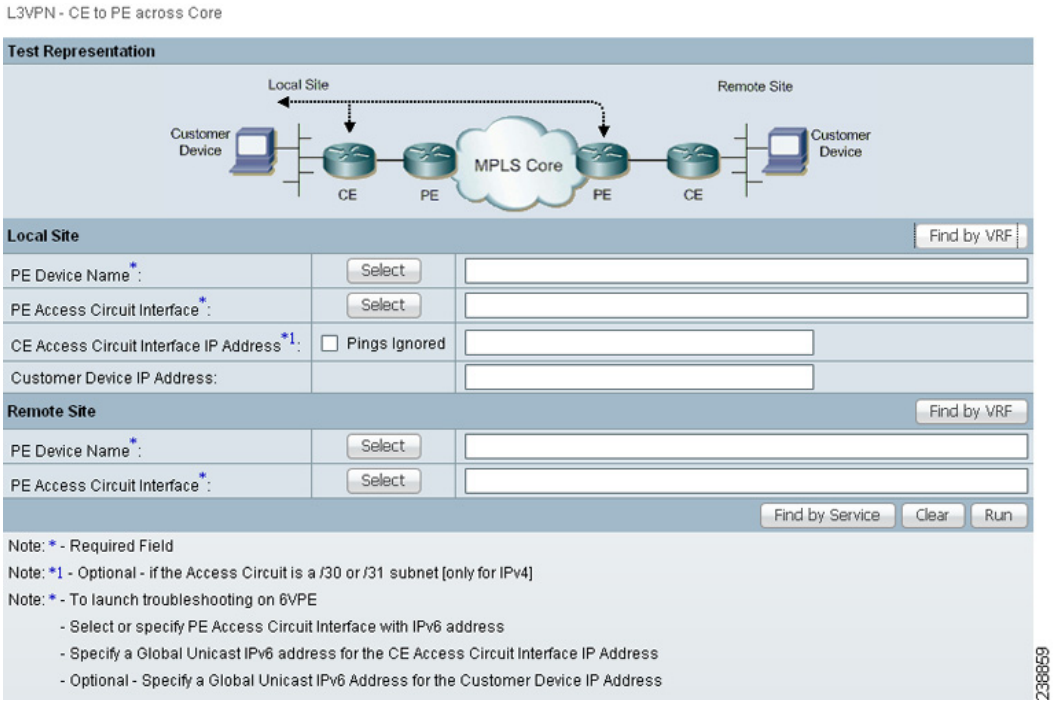
ステップ 1　[Diagnostics] メニューから、[L3VPN - CE to PE across Core] テスト タイプを選択します。

ステップ 2　[L3VPN - CE to PE across Core] 接続性検証テスト タイプをクリックします。

[L3VPN - CE to PE across core] 接続性検証テスト タイプの詳細については、「L3VPN - CE to PE across Core 接続性テスト」（P.11-16）を参照してください。

[L3VPN - CE to PE Across MPLS Core Diagnostics - Test Setup] ウィンドウ（図 11-14 を参照）が表示され、L3VPN - CE to PE across Core テスト タイプに対応したフィールドが表示されます。[L3VPN - CE to PE Across MPLS Core Diagnostics - Test Setup] ウィンドウで、実行する接続性テストを設定できます。

図 11-14　L3VPN - CE to PE across Core テスト タイプ



[L3VPN - CE to PE Across Core] ウィンドウには、次のコンポーネントが表示されます。

- ネットワーク図
- ローカル サイト設定領域
- リモート サイト設定領域

これらのコンポーネントおよびテスト範囲については、「L3VPN - CE to CE テストの選択、設定および実行」（P.11-19）に詳しい説明があります。

ステップ 3　必要に応じて [L3VPN - CE to PE across Core] ウィンドウのフィールドを設定します。

表 11-3（P.11-22）に、L3VPN - CE to PE across core テスト タイプに対応するフィールドの説明を示します。

ステップ 4　すべての必須フィールドに入力したら、[OK] をクリックしてテストを実行します。

[Progress] ウィンドウが表示されます。「[Progress] ウィンドウ」（P.11-39）を参照してください。

L3VPN - PE to PE テストの選択、設定および実行

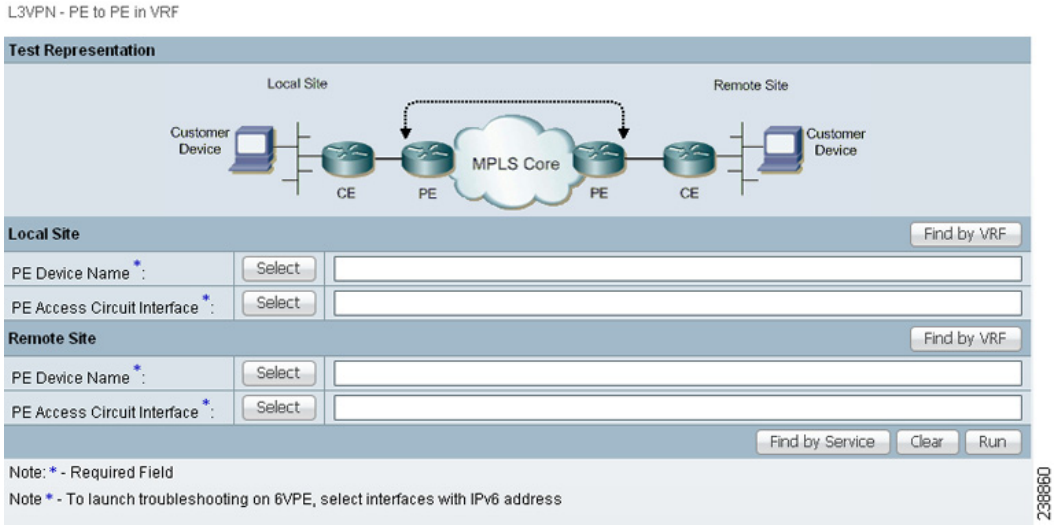
この項では、L3VPN - PE to PE テスト タイプを選択、設定、および実行する方法の詳細について説明します。

ステップ 1　[Diagnostics] メニューから、[L3VPN - PE to PE] テスト タイプを選択します。

L3VPN- PE to PE in VRF 接続性検証テスト タイプの詳細については、「L3VPN - PE to PE in VRF 接続性テスト」（P.11-17）を参照してください。

[L3VPN- PE to PE in VRF Diagnostics - Test Setup] ウィンドウ（図 11-15 を参照）が表示され、L3VPN - PE to PE in VRF テスト タイプに対応したフィールドが表示されます。[L3VPN- PE to PE in VRF Diagnostics - Test Setup] ウィンドウで、実行する接続性テストを設定できます。

図 11-15　　L3VPN - PE to PE テスト タイプ



[L3VPN - PE to PE in VRF Diagnostics - Test Setup] ウィンドウには、次のコンポーネントが表示されます。

- ネットワーク図
- ローカル サイト設定領域
- リモート サイト設定領域

これらのコンポーネントおよびテスト範囲については、「L3VPN - CE to CE テストの選択、設定および実行」（P.11-19）に詳しい説明があります。

ステップ 2　必要に応じて [L3VPN - PE to PE in VRF Diagnostics - Test Setup] ウィンドウのフィールドを設定します。

表 11-3（P.11-22）に、L3VPN - PE to PE in VRF テスト タイプに対応するフィールドの説明を示します。

ステップ 3　すべての必須フィールドに入力したら、[OK] をクリックしてテストを実行します。

[Progress] ウィンドウが表示されます。「[Progress] ウィンドウ」（P.11-39）を参照してください。

MPLS - PE to PE テストの選択、設定および実行

この項では、L3VPN - PE to PE（コア）テスト タイプを選択、設定、および実行する方法の詳細について説明します。

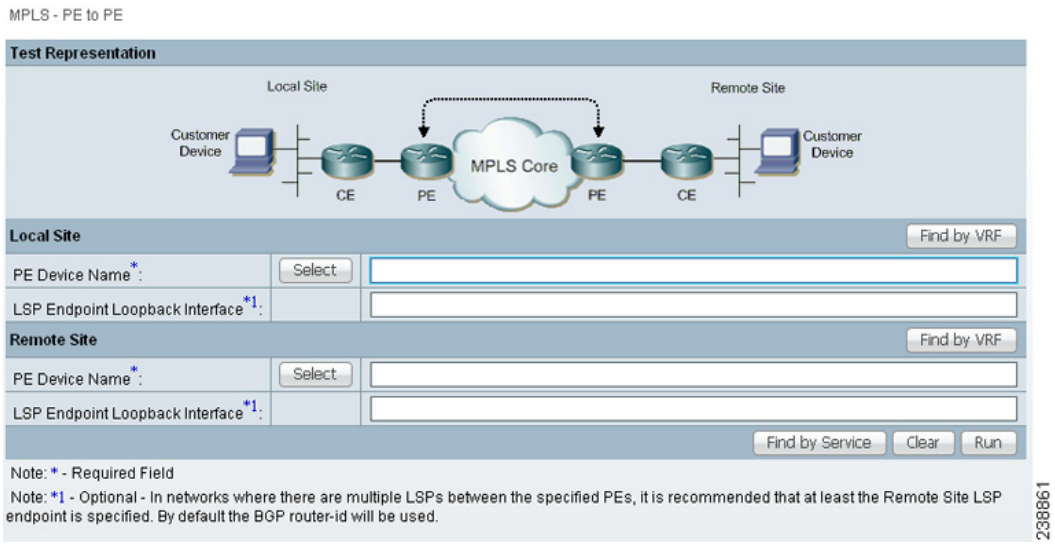
ステップ 1　[Diagnostics] メニューから、[MPLS - PE to PE] テスト タイプを選択します。

ステップ 2　[MPLS - PE to PE] 接続性検証テスト タイプをクリックします。

PE to PE 接続性検証テスト タイプの詳細については、「L3VPN - PE to PE 接続テスト」（P.11-17）を参照してください。

[MPLS - PE to PE] ウィンドウ（図 11-16 を参照）が表示され、MPLS - PE to PE テスト タイプに対応したフィールドが表示されます。[MPLS - PE to PE] ウィンドウを使用して、実行する接続性テストを設定できます。

図 11-16　MPLS - PE to PE テスト タイプ



[MPLS - PE to PE] ウィンドウには、次のコンポーネントが表示されます。

- ネットワーク図
- ローカル サイト設定領域
- リモート サイト設定領域

これらのコンポーネントおよびテスト範囲については、「L3VPN - CE to CE テストの選択、設定および実行」（P.11-19）に詳しい説明があります。

ステップ 3　必要に応じて [MPLS - PE to PE] ウィンドウのフィールドを設定します。

表 11-3（P.11-22）に、L3VPN - PE to PE テスト タイプに対応するフィールドの説明を示します。

ステップ 4　すべての必須フィールドに入力したら、[OK] をクリックしてテストを実行します。

[Progress] ウィンドウが表示されます。「[Progress] ウィンドウ」（P.11-39）を参照してください。

MPLS - PE to PE テストへの LSP エンドポイント ループバック IP アドレスの設定

この項では、MPLS - PE to PE テスト タイプで LSP エンドポイント ループバック インターフェイスおよび IP アドレスを設定する方法の詳細について説明します。

リモート LSP エンドポイント ループバック IP アドレス

L3 VPN カスタマー トラフィックは、カスタマー ルートの BGP ネクスト ホップ アドレスを使用して LSP を選択します。コアをテストするときは、ローカル PE からリモート PE に MPLS OAM ping およびトレースが実行されます。トラフィックが経由するものと同じ LSP を Diagnostics でテストするには、Diagnostics がテストする IP プレフィックスがカスタマー ルートの BGP ネクスト ホップ アドレスになるようにします。

PE to PE コア テスト タイプでは、Diagnostics はカスタマー ルート情報を持っていません。そのため、Diagnostics は BGP ネクスト ホップを識別できません。デフォルトで、Diagnostics は ping およびトレースの宛先をネクスト ホップではなくリモート PE の BGP ルータ ID に基づいて選択します。複数のコアがある、複数のループバック アドレスが制御トラフィックおよびデータ プレーン トラフィックに使用されるなど一部のネットワーク設定では、この BGP ルータ ID がカスタマー トラフィックで使用されるネクスト ホップと一致せず、不正な LSP がテストされる（または、どの LSP もテストされない）ことがあります。

ローカル LSP エンドポイント ループバック IP アドレス

進行方向で実行したテストで問題を検出できなかった場合は、MPLS - PE to PE テスト タイプで逆方向のテストを実行できます。ローカル LSP エンドポイント ループバック IP アドレスを設定すると、逆方向のテストを実行するときに、正しい LSP が選択されます。

LSP エンドポイント ループバック IP アドレスを指定する場合

次の場合に、LSP エンドポイント ループバック IP アドレスを指定します。

- BGP ルータ ID が、LSP が割り当てられていないループバックのアドレスである。
- BGP ルータ ID がループバックのアドレスでない。
- 複数の LSP が定義されており、トラフィックはルータ ID により与えられた LSP 以外の LSP を使用している。
- 複数の定義済み LSP があり、トラフィックがルートマップに基づいて LSP を切り替える。

（注） リモート LSP エンドポイントを指定するときは、正しい BGP ネクスト ホップを指定する必要があります。

図 11-17 に、[LSP Endpoint Loopback IP Address] フィールドの使用方法を表したネットワーク トポロジの例を示します。このネットワーク トポロジの例には 3 つの論理 MPLS コアが存在し、一部の PE BGP ルータ ID はループバック インターフェイスに関連付けられていません。さらに、2 つの CE は、別々のコアにデュアルホーム接続されています。

図 11-17　ネットワーク トポロジの例

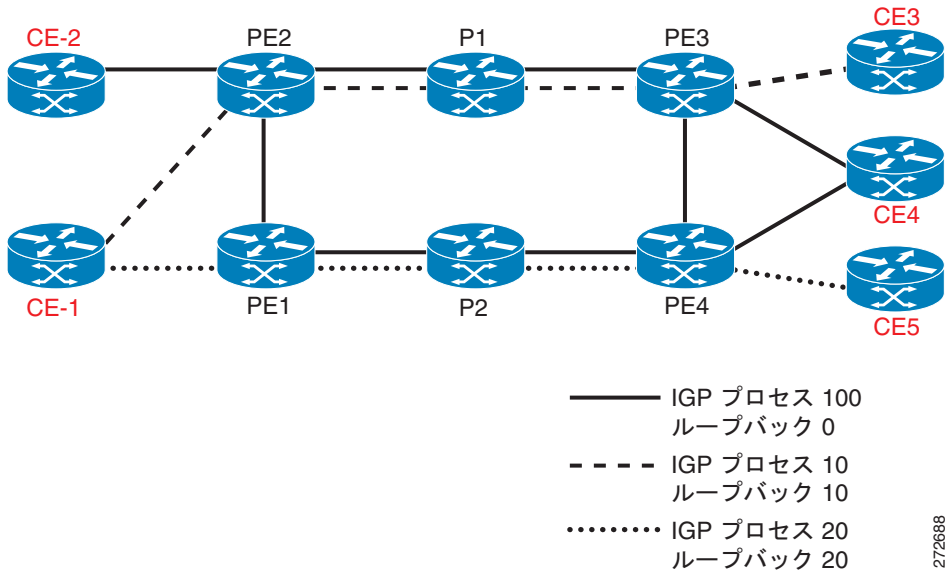


表 11-8 に、図 11-17 に示されているネットワーク トポロジの例に関連する IP アドレッシング情報を示します。

表 11-8　IP アドレス指定

PE	BGP ルータ ID	ループバック 0	ループバック 10	ループバック 20
PE2	1.1.1.1	1.1.1.1	N/A	20.20.20.1
PE3	1.1.1.3	1.1.1.3	N/A	20.20.20.3
PE1	50.50.50.1	1.1.1.6	10. 10.10.1	N/A
PE4	50.50.50.3	1.1.1.8	10. 10.10.3	N/A

表 11-9 に、各 LSP をテストするときにリモート LSP エンドポイント IP アドレスとして使用できる IP アドレスを示します。

表 11-9　各 LSP のテストに必要な入力

テスト対象の LSP	対象 CE	リモート サイトの PE	リモート エンドポイント
実線	CE-2	PE2	ネクスト ホップが BGP ルータ ID のため、必要ありません。
実線	CE-4	PE4	1.1.1.8（ループバック 0）
実線	CE-4	PE3	ネクスト ホップが BGP ルータ ID のため、必要ありません。
点線	CE-1	PE2	20.20.20.1（ループバック 20）
点線	CE-3	PE3	20.20.20.3（ループバック 20）
破線	CE-1	PE1	10. 10.10.1（ループバック 10）
破線	CE-5	PE4	10. 10.10.3（ループバック 10）

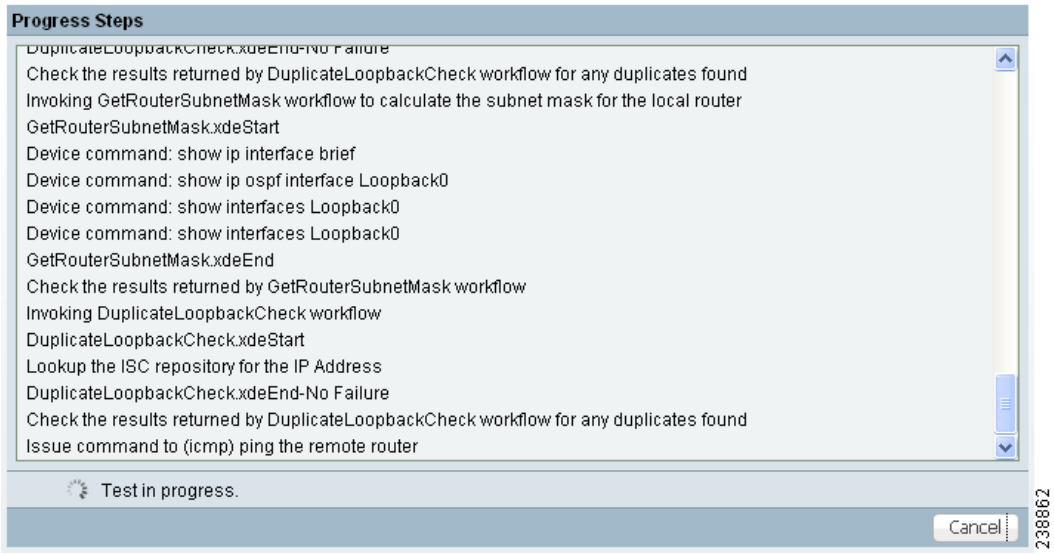
[Progress] ウィンドウ

テストの実行中に、[Progress] ウィンドウ（図 11-18 を参照）が表示されます。

（注）　MPLS VPN 接続性検証テストの実行時間は、場合によって異なります。ネットワークのサイズ、選択したテスト タイプ、接続性の問題が識別されたかどうか、および、この接続性の問題の性質によっては、テストの完了までにしばらく時間がかかることがあります。

[Progress] ウィンドウには、完了した各ステップに関する 1 行のテキストによるサマリーと、現在実行中のステップが表示されます。

図 11-18　[Progress] ウィンドウ



必要な場合、[Cancel] ボタンをクリックするとテストがキャンセルされます。[Cancel] をクリックすると、テストを本当にキャンセルするかどうかの確認を求められます。確認すると、現在のステップが完了し次第、テストがキャンセルされます。現在のステップでデバイス間のやり取りが行われている場合は、それが完了してからテストがキャンセルされます。キャンセルを実行すると、[Test Results] ウィンドウが表示され、テストをキャンセルしたことが表示されます。テスト ログには、完了したステップすべてが表示されます。

テストが完了すると、[Test Results] ウィンドウが表示されます。詳細については、「テスト結果の解釈」（P.11-39）を参照してください。

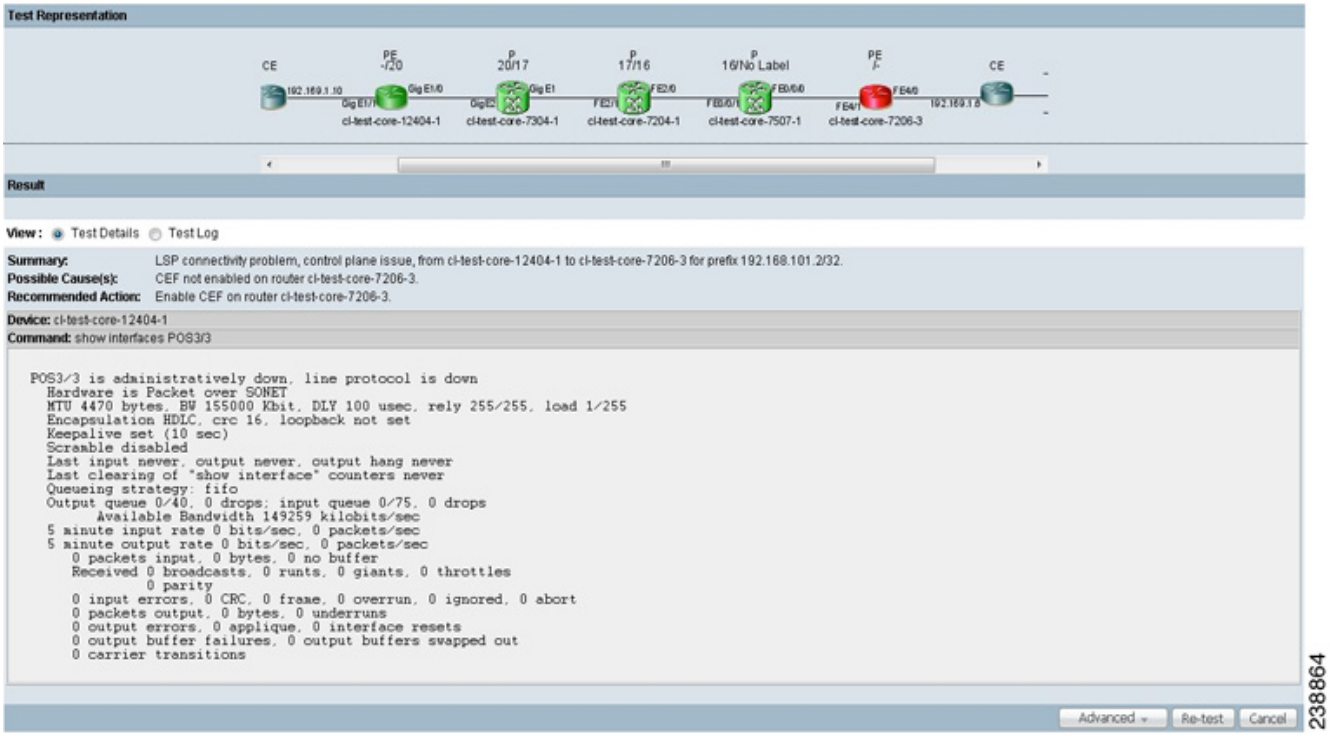
テスト結果の解釈

この項では、テスト結果の解釈方法について説明します。ここでは、次の項目について説明します。

- 「データ パス」（P.11-41）
- 「Test Details」（P.11-43）
- 「Test Log」（P.11-44）
- 「Export」（P.11-45）

MPLS VPN 接続性検証テストが完了すると、[Test Results] ウィンドウが表示されます（図 11-19 を参照）。

図 11-19　障害固有の追加情報が表示された [Test Results] ウィンドウ



[Test Result] ウィンドウには、見つかった問題の場所、原因、推奨されるアクション、観察結果、および実行された自動トラブルシューティングと診断ステップの詳細が表示されます。また、[Test Result] ウィンドウから、必要に応じて高度なトラブルシューティング オプションを起動できます（表 11-10 を参照）。

[Test Results] ウィンドウは、次のコンポーネントで構成されています。

表 11-10　[Test Results] ウィンドウのフィールドの説明

フィールド / ボタン	説明
Data path	「データ パス」（P.11-41）を参照してください。
Test Details	「Test Details」（P.11-43）を参照してください。
Test Log	「Test Log」（P.11-44）を参照してください。
[Export] ボタン	[Test Log] オプション ボタンを選択すると、[Export] ボタンが表示されます。「Export」（P.11-45）を参照してください。
[Advanced] ボタン	高度なトラブルシューティングを起動するには、[Advanced] ボタンをクリックします。「高度なトラブルシューティング オプション」（P.11-45）を参照してください。このボタンで使用できるオプションは、テスト結果およびテスト タイプに応じて動的に設定されます。

表 11-10　[Test Results] ウィンドウのフィールドの説明 （続き）

フィールド/ボタン	説明
[Re-test] ボタン	既存の設定を使用して再度接続性テストを実行するには、[Re-test] ボタンをクリックします。実装したフィックスを確認するために使用できます。
[Cancel] ボタン	現在のテストをキャンセルして [Test Configuration] ウィンドウに戻るには、[Cancel] ボタンをクリックします。キャンセルの確認は求められません。

テストしたパスに複数の障害がある場合、報告される障害は、Diagnostics が実行するトラブルシューティングの順序によって決まります。CE to CE 接続性テスト タイプの場合、Diagnostics トラブルシューティングは次の順序で実行されます。

1. アクセス回線（ローカルおよびリモート）。
2. MPLS Traffic Engineered（TE）トンネル。
3. MPLS コア。
4. MPLS VPN エッジ。

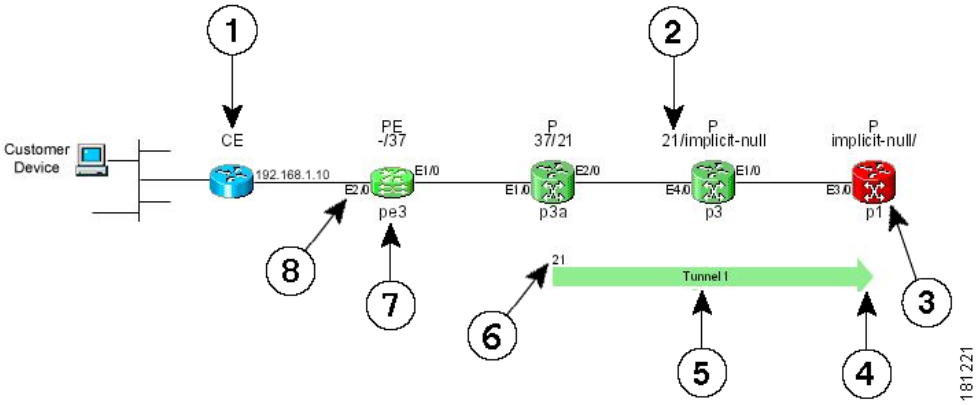
その他のテスト タイプも同じ順序でトラブルシューティングを実行しますが、すべてのステップを実行するわけではありません。

（注）　[Test Result] ウィンドウには、最初に見つかった障害の詳細が表示されます。複数の障害が存在する場合は、現在の障害を修復してテストを再実行しないと、後続の障害はレポートされません。

データ パス

データ パス（図 11-20 を参照）は、テスト対象の 2 つのサイト間のパスを図で示します。MPLS Traffic Engineered トンネルで障害が見つかった場合は、データ パスにはトンネルが表示されます。パス内の障害ポイントよりも前で見つかった、重複していない P-P、PE-P、または P-PE MPLS TE トンネルも、データパスに表示されます。

図 11-20　データ パス



1. デバイスのロール（CE、PE、または P）。
2. MPLS ラベル（入力/出力）。
3. 障害の発生したデバイス。

4. トンネルの方向を示す矢印。
5. トンネル名。
6. トンネル ラベル。
7. デバイスのホスト名。
8. インターフェイス名。

MPLS TE トンネルが存在する場合は、デバイス パスの下に表示されます。

カスタマー デバイス IP アドレスを指定した場合は、この IP アドレスは「Customer Device」という文字の横に表示されます。

（注）　MPLS TE トンネルは、そのトンネルが接続の問題の原因であると判明した場合のみ表示されます。

障害が見つかった場合は、データ パスで障害のあるデバイスまたはリンクが強調表示されます。データ パス内で使用されるデバイスの色については、表 11-11 を参照してください。

表 11-11　データ パスのデバイス カラー コード

色	アイコン	説明
緑色		デバイスはテスト済みで、正常に機能しています。
青色		デバイスはテストされていないか、ステータスが不明です。
赤		デバイスに障害が発生しています。
黄色		デバイスに障害が発生している可能性があります。
グレー		デバイスにアクセスできません。

データ パス内で使用されるリンクの色については、表 11-12 を参照してください。

表 11-12　データ パスのリンク カラー コード

色	アイコン	説明
赤		接続の問題が見つかっています。この障害の原因は、接続されているデバイスの片方または両方の問題である可能性があります。

各コア PE および P デバイスの場合は、次の情報が表示されます。

- ロール（PE または P）
- デバイス名
- インターフェイス名
- 入力および出力 MPLS ラベル（MPLS コアの障害のみ）

CE デバイスおよびカスタマー デバイスについては、最小限の情報しか表示されません。通常、これらのデバイスについては、テストの設定時に指定された情報だけが表示されます。

MPLS Traffic Engineered トンネルについては、次の情報が表示されます。

- トンネル名
- トンネルの方向（方向を示す矢印）
- トンネル ラベル

（注）　[Test Result] ウィンドウのデータ パスからは、デバイスには Telnet 接続できません。

Test Details

[Test Results] ウィンドウの [Test Details] セクション（図 11-19（P.11-40）を参照）には、自動トラブルシューティングおよび診断結果の概要、トラブルシューティング中の観察結果、その他の障害固有の情報、および推奨アクションが表示されます。Diagnostics によってレポートされる障害および観察結果の詳細について、およびトラブルシューティングの一環として Diagnostics により実行される IOS および IOS XR コマンドすべてのリストの詳細については、「障害シナリオ」（P.11-59）を参照してください。

テストの詳細の概要は、すべての場合で表示されます。テストの詳細の概要は、次の 3 つの詳細説明フィールドで構成されています。

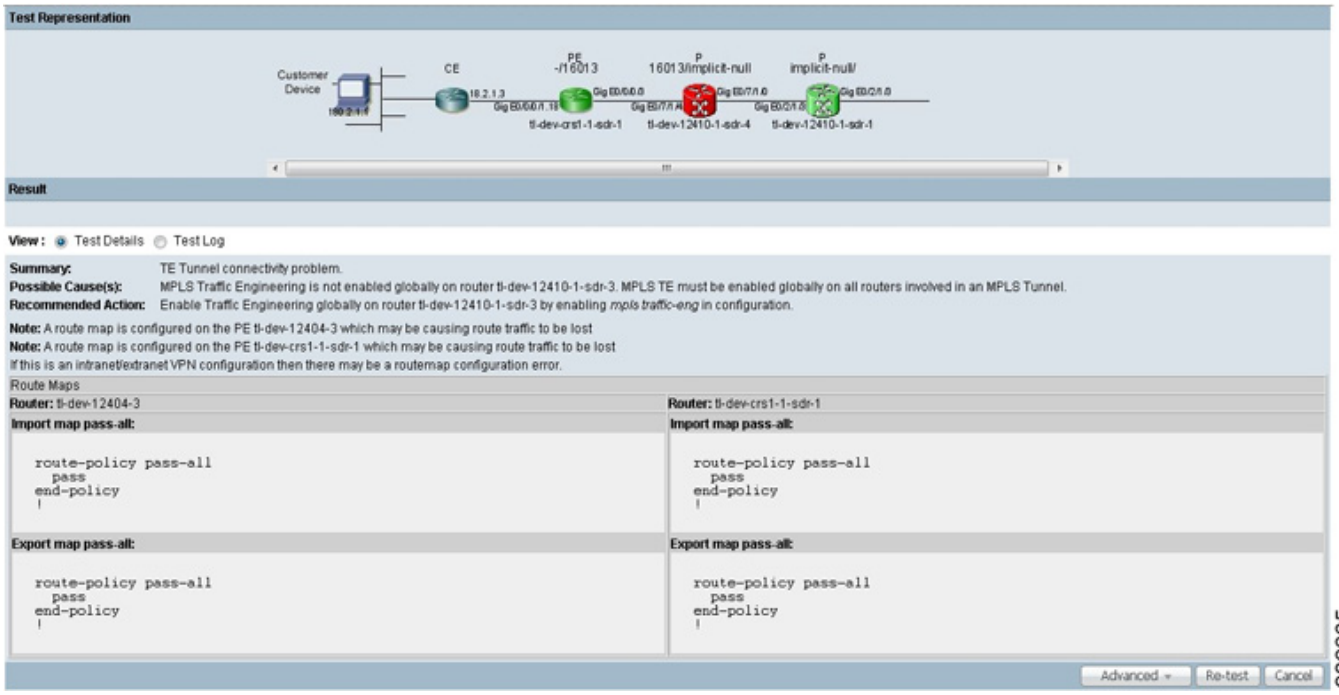
- [Summary]：見つかった障害の簡単な概要が表示されます。
- [Possible Cause(s)]：考えられる障害の原因です。
- [Recommended Action]：問題を解決するために推奨されるアクションです。

その他の障害固有の情報は、必要に応じて概要の下に表示されます。これが表示された場合は、見つかった問題についてのその他の情報が提供されます。たとえば、Forwarding Information Base（FIB; 転送情報ベース）、ラベル転送情報ベース（LFIB）、ボーダー ゲートウェイ プロトコル（BGP）のテーブル エントリおよびルート ターゲット インポート/エクスポートです。このその他の障害固有の情報は、FIB、LFIB、BGP の矛盾およびルート ターゲット インポート/エクスポートの不一致などの問題を明確にするために役立ちます。一部の障害については、その他の情報は表示されません。

図 11-19（P.11-40）に、テストの詳細の概要の下に障害固有の情報が表示された [Test Results] ウィンドウの例を示します。[Test Details] オプション ボタンはデフォルトで選択されています。

トラブルシューティング中に観察された内容は、テストの詳細の概要の下に注記として表示されます。観察の注記は、障害に関連する可能性のある、トラブルシューティング中に観察された内容の詳細を示します。この内容は、追加のトラブルシューティング情報と見なします。図 11-21 に、観察の注記が 2 つ表示された [Test Results] ウィンドウの例を示します。観察の注記は、まったく表示されない場合、または複数表示される場合があります。

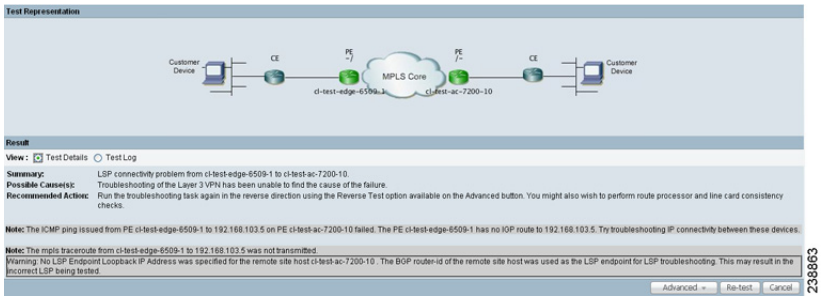
図 11-21　観察の注記が表示された [Test Results] ウィンドウ



Test Log

[Test Log]（図 11-22 を参照）オプション ボタンをクリックして、すべてのトラブルシューティングおよび診断ステップの詳細を、実行された順序で表示します。

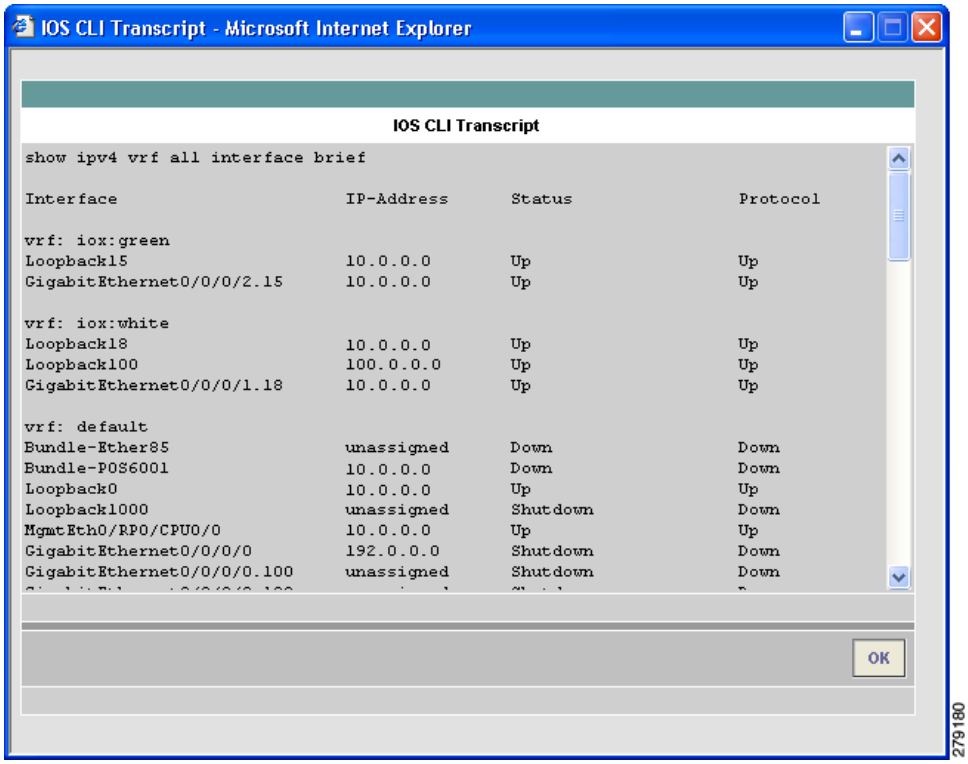
図 11-22　[Test Results] ウィンドウ：テスト ログ



一部のステップでは、IOS または IOS XR CLI コマンドの実行など、デバイスからの入力が必要な場合があります。これらのステップは、テスト ログではハイパーリンクとして表示されます。ハイパーリンクをクリックすると、そのステップの IOS または IOS XR CLI トランスクリプトを示したポップ

アップ ウィンドウが表示されます（図 11-23 を参照）。このトランスクリプトには、実行された IOS または IOS XR コマンドおよびすべての結果の出力が含まれます。

図 11-23　[IOS CLI Transcript] ウィンドウ



Export

テスト ログをエクスポートして、トラブル チケットに含めたり、問題をエスカレーションしたり、または Cisco TAC に問い合わせしたりする際に使用できます。テスト ログは、テスト ログの下部にある [Export] ボタン（図 11-22（P.11-44）を参照）を使用してファイルにエクスポートできます。IOS および IOS XR CLI トランスクリプトを含め、テスト ログに表示されるすべてのステップはテキスト形式でエクスポートされます。

ステップ 1　[Export] ボタンをクリックします。

ブラウザ標準のファイル ダウンロード ウィンドウが表示され、ファイル名はデフォルトで「*export.rtf*」と表示されます。

ステップ 2　ファイルを保存します。

高度なトラブルシューティング オプション

この項では、次の高度なトラブルシューティング オプションについて説明します。

- 「リバース パス テスト」（P.11-46）

- 「LSP 可視化」（P.11-46）

高度なトラブルシューティングにより提供される追加オプションを、ネットワークのトラブルシューティングに使用できます。

サポートされている高度なトラブルシューティング オプションの詳細については、表 11-13 を参照してください。

表 11-13　高度なトラブルシューティング オプション

高度なトラブルシューティング オプション	説明
リバース パス テスト	障害が見つかった場合に使用できます。
LSP 可視化	障害が見つからなかった場合に使用できます。
LSP トラブルシューティング	IP の障害が見つかった場合に使用できます。

高度なトラブルシューティング オプションは、[Test Results] ウィンドウの下部にある [Advanced] ドロップダウン ボタンを使用して適切なものを使用できます。

リバース パス テスト

（注）　リバース パス テスト オプションは、PE to attached CE テスト タイプ以外のすべてのテスト タイプで使用できます。

場合によっては、MPLS VPN 接続性検証テストは接続の問題を検出しても、障害の原因を特定できない場合があります。逆方向（つまり、ローカル サイトとリモート サイトの設定を逆にした状態）でテストを繰り返すことにより、問題の原因を特定できる場合があります。その他の場合では、逆方向でテストを繰り返すことにより、結果として見つかった問題がさらに正確に診断される場合もあります。たとえば、接続性テストを進行方向で実行している間に、LSP 接続の問題がデバイスで特定される場合があります。しかし、この問題はダウンストリームの LSP ネイバーでの LDP 誤設定によって引き起こされた可能性もあります。逆方向でテストを繰り返すことにより、誤設定されたダウンストリーム ルータに最初に遭遇し、LDP 後設定が診断されます。この状況が発生した場合、[Test Results] ウィンドウに表示されるテストの詳細には、テストを逆方向で実行するように勧めるメッセージが表示されます。リバース テスト オプションは、[Test Results] ウィンドウの [Advanced] ドロップダウン ボタンから使用できます。

高度なトラブルシューティングのリバース テスト オプションを選択すると、逆方向状態で MPLS VPN 接続性検証テストが起動されます。それ以上の設定は必要ありません。

リバース パス テストの結果は、[Test Results] ウィンドウに表示されます。

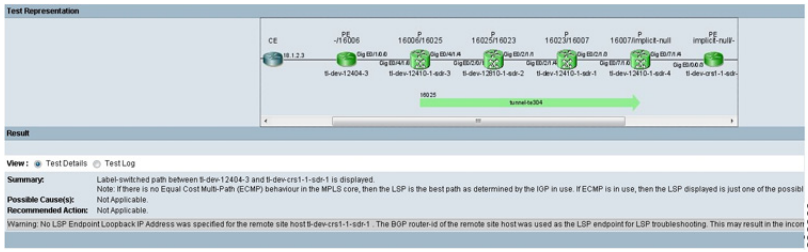
LSP 可視化

（注）　LSP 可視化は、PE to attached CE テスト タイプ以外のすべてのテスト タイプで使用できます。

障害が見つからなかった場合、[Test Results] ウィンドウのデータ パスには、実行されたテストの概要が表示されます。テストされたコアを通過するパスの詳細は表示されません。LSP 可視化は、ローカル サイトとリモート サイト間の MPLS ラベル スイッチド パス（LSP）のホップバイホップ データ パスの図を表示します（図 11-24 を参照）。LSP 可視化では、転送パスの中間に見つかった、すべての重複していない PE-P 間、P-P 間、および P-PE 間のトンネルが表示されます。表示されるパスは、

MPLS VPN 接続性検証テスト中にテストされたパスです。

図 11-24　[Test Results] ウィンドウ：LSP 可視化



データ パスには、テストされたパス内の各 PE および P デバイスについて、次の内容が表示されます。

- ロール（PE または P）
- デバイス名
- インターフェイス名
- 入力および出力ラベル

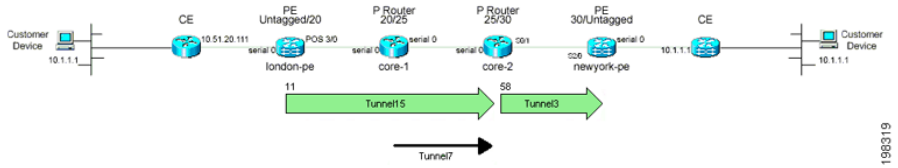
データ パスには、各 PE-PE 間の MPLS Traffic Engineered トンネルについて、次の内容が表示されます。

- トンネル名
- トンネルの方向（方向を示す矢印）
- トンネル ラベル
- トンネル タイプ

（注） 複数の MPLS TE トンネルが設定されている場合は、実際にトラフィックを伝送しているトンネルのみがデータパスに表示されます。

次の例では、Tunnel 7 は重複している（つまり、Tunnel 7 のヘッドエンドはアップストリーム ルータに設定されている Tunnel 15 のミッドポイントに設定されている）ため、表示されません。

図 11-25　複数の MPLS TE トンネル設定



データ パスに表示される内容についての詳細は、「データ パス」（P.11-41）を参照してください。

LSP 可視化は、MPLS VPN 接続性検証テストで接続の問題が検出されなかった場合のみ提供されます。

（注） MPLS VPN 接続性検証テストをポストプロビジョニング検証に使用している場合は、LSP 可視化では MPLS コアを通過する LSP パスを表示することで、より高度な検証を提供します。

トンネル チェックのオフ：他社製 P ルータを使用したネットワークの場合

トンネルの診断中、Diagnostics はすべてのデバイスを確認して、そのポイントにトンネルが存在するかを確認する必要が生じる場合があります。Diagnostics は、他社製のデバイスにはログインしないため、他社製デバイスで発生している障害の誤診断を招き、（たとえそのデバイスが障害の実際の原因ではないとしても）トラブルシューティング ワークフローを進めることができなくなる場合があります。そのため、他社製デバイスが含まれるネットワークでは、トンネル診断をディセーブルにすることが役立ちます。

デフォルトでは、トンネル診断はイネーブルになっています。デフォルト値は、Admin ユーザが Prime Provisioning Control Center（[Administration] タブ > [Control Center] > [Hosts]）で変更できます。トンネル診断は、Command Flow Runner（CFR）コンポーネント（disableTunnelDiagnostics パラメータ）でイネーブルまたはディセーブルにできます。適切な disableTunnelDiagnostics パラメータが true に設定されている場合は、Diagnostics はトンネル診断を実行しません。

[Test Results] ウィンドウには、Diagnostics のトンネル診断がディセーブルであることを示す観察メッセージが表示されます。デバイスがインベントリに含まれていないことを示すエラー メッセージは、パス上の他社製デバイスが原因である可能性があること、およびエラーがこのデバイスまたはその近くのネイバーで発生していることを意味します。

Diagnostics の動作

この章では、Diagnostics アプリケーションの動作について説明します。

MPLS VPN 接続性検証テストは、接続性テスト、トラブルシューティング、および診断のステップで構成されています。各テストで実行される実際のステップは、検出された障害、およびネットワーク内の障害の場所によって異なります。テスト設定は簡単で結果はわかりやすいため、トラブルシューティングおよび診断のロジックについて理解する必要はほとんどありません。ただし、特にテスト ログを調べる場合など、トラブルシューティングおよび診断のプロセスを理解した方がよい場合があります。この章では、接続性のテスト、トラブルシューティング、および診断ロジックの概要について説明します。

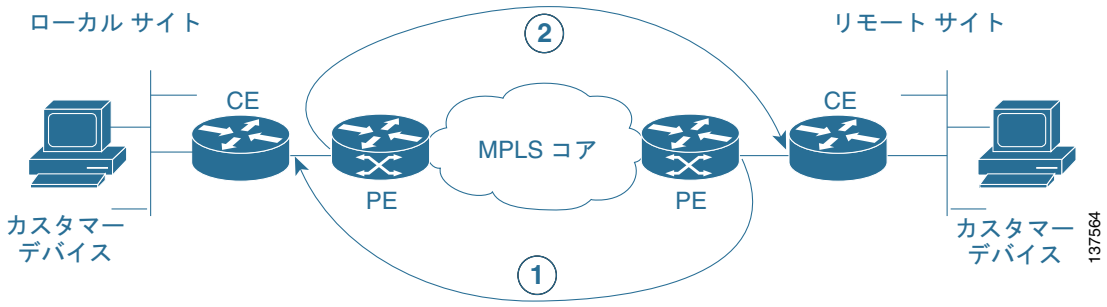
（注） この章で詳しく説明する手順は、Diagnostics が実行するテストのタイプの実例を示しています。ただし、このテストの一覧はすべてを網羅しているわけではなく、Diagnostics はこの他にも多くのテストを実行します。

テスト範囲は、入力したテスト設定によって決まります。たとえば各サイトでは、テストは、サイト内のカスタマー デバイスに対して実行することも、CE アクセス回線インターフェイスに対して実行することもできます。簡単にするために、この章ではすべてのサイトのテストが、CE アクセス回線インターフェイスに対するものであることを前提としています。

最初のステップでは、2 つのサイト間の VPN 接続性をテストして、問題がないかどうか判断します。これは、Cisco IOS VRF の ping 機能を使用して行います。このテストは、ローカル サイト サブネットのデバイスから、リモート サイト サブネットの宛先 IP アドレスに対して開始されることが理想的です。ただし、Prime Provisioning は管理対象および管理対象外のシスコ製 CE デバイスおよび他社製 CE デバイスをサポートしています。トラブルシューティングおよび診断の機能は、すべての場合に有効です。このため、このテストはコア ネットワーク内の PE および P デバイスからのみ開始できます。

この制限を回避するには、接続性テストを 2 段階に分けて実行する必要があります（図 11-26 を参照）。

図 11-26　IOS VRF ping 接続性テスト



1. 第 1 段階（図 11-26 を参照）では、リモート サイト PE からローカル サイト CE への接続性をテストします。これは、Cisco IOS の **ping vrf** コマンドを使用して、宛先としてローカル サイト CE アクセス回線インターフェイスの IP アドレスを指定し、送信元 IP アドレスとしてリモート サイト PE アクセス回線インターフェイスを指定して実行します。
2. 第 2 段階（図 11-26 を参照）では、ローカル サイト PE からリモート サイト CE への接続性をテストします。このテストは、最初のテストの **ping vrf** コマンドで接続が正常であることが示された場合のみ実行します。これは、Cisco IOS **ping vrf** コマンドを使用し、宛先としてリモート サイト CE アクセス回線インターフェイスを指定し、送信元 IP アドレスとしてローカル サイト PE アクセス回線インターフェイスを指定して実行します。

リモート サイト PE からローカル サイト CE への接続性テストを先に実行しておくと、ローカル アクセス回線での問題が先に見つかるようになります。そのため、順方向パスの問題よりも前に、リバース パス MPLS VPN、MPLS コア、および MPLS TE トンネルの問題が見つかります。

2 段階に分けて接続性をテストすることにより、トラブルシューティングおよび診断機能で、ローカル サイトの CE からリモート サイトの CE へのエンドツーエンド テストのシミュレーションが可能になるため、サイト間のあらゆる VPN 接続の問題を識別できます。この接続性テストでは、2 つのサイト間の VPN、MPLS、および IP 接続を調べます。

VPN 接続性の問題は検出されないため、トラブルシューティングおよび診断は実行されません。VRF 接続の問題が検出された場合は、さらに一連の接続性テストを実行して、接続の問題の分離を試みます。これらのテストは PE デバイス上で開始され、VPN の障害が検出された方向で実行されます。次の内容で構成されています。

- コアから PE アクセス回線インターフェイス全体にわたる VRF ping。これにより、障害がアクセス回線にあるのか、CE と PE 間にあるのか、またはコア内にあるのか識別されます。
- コアから PE ループバック全体にわたる ICMP ping：これにより、IP 接続がコア全体で動作しているかどうか確認されます。
- コアから PE ループバック全体にわたる LSP ping：これにより、MPLS LSP パスがコア全体で動作しているかどうか確認されます。

障害が分離されると、テストがいずれかのポイントで停止することがあります。その後、自動トラブルシューティングおよび診断のステップが実行され、障害の原因が診断されます。実行されるステップは、障害の性質および場所によって異なります。トラブルシューティングは次の順序で実行されます。

1. アクセス回線（ローカルおよびリモート）。
   a. L3 接続性（CE およびカスタマー デバイスへの VRF ping とトレース）およびルート チェック。
   b. L2（ATM、イーサネット、フレーム リレー、シリアル）接続性およびステータス チェック。

c. PE-CE ルーティング プロトコル判定およびステータス チェック。
d. PE-CE ルーティング プロトコルおよび MP-BGP 再配布チェック。

2. MPLS VPN エッジ。
   a. MP-BGP ネイバーおよび VPN ルート チェック。
   b. VRF ルート制限およびチェック。
   c. ルート マップの存在チェック。
   d. PE–PE VRF（MPLS コア全体の VRF ping とトレース）接続性チェック。
   e. PE MPLS OAM 機能チェック。
3. MPLS Traffic Engineered（TE）トンネル。
   a. トンネル接続性（TE 対応の ping とトレース）およびステータス チェック。
4. MPLS コア。
   a. IP 接続性（ICMP ping）チェック。
   b. LSP 接続性（LSP ping とトレース）およびステータス チェック。
   c. LSP データパス生成。
   d. LSP 障害ローカリゼーション。
   e. LDP セッションおよびネイバー チェック。
   f. ラベル チェック。
   g. MPLS VPN エッジ。
   h. VPN ラベル チェック。
   i. VRF ルート ターゲット チェック。

（注） コアのトラブルシューティングは、Cisco IOS の MPLS LSP ping および traceroute 機能をサポートしている PE デバイスのみに対して実行されます。サポートされているデバイス タイプおよび MPLS OAM がサポートされる Cisco IOS バージョンの詳細については、「サポートされているハードウェア、IOS、および IOS XR バージョン」（P.11-3）を参照してください。

（注） プライマリ トンネルに FRR 保護が設定されている場合は、Diagnostics はプライマリ トンネルをトラブルシューティングし、（プライマリ トンネルに FRR 保護を提供しながら）プライマリ トンネルおよびバックアップ トンネルで検出された、障害の可能性をレポートします。トラブルシューティングの対象となるバックアップ トンネルは、ABR 間に設定された、FRR に対応しているプライマリ トンネルを保護するように設定されたトンネルに限られます。

障害の診断後、[Test Results] ウィンドウに診断結果および障害を解決するための適切な推奨アクションが表示されます。実行された接続性テストと、自動トラブルシューティングおよび診断の正確なステップは、[Test Results] ウィンドウの [Test Log] セクションに表示できます。

よくあるご質問

Q. MPLS VPN 接続性検証テストを実行すると、[Progress] ウィンドウがハングアップするように見え、同じステップが最大 5 分間実行されます。5 分後、[Test Results] ウィンドウに次のメッセージが表示されます。

```
Summary: Cannot connect or login to device router1.
Possible Cause(s): Device could be down, there could be problems with network
connectivity, or the login details in the repository might be incorrect
Recommended Action: Restore connectivity to the device before attempting the test.
If in-band network management is in use then you might want to consider performing
a Traceroute from the management station to device router1 to find where IP
connectivity fails.
```

A. デバイスにログインしようとしても、デバイスが応答しません。デバイスがダウンしていないことを確認します。Prime Provisioning サーバからデバイスへの IP 接続が確立されていることを確認します。Prime Provisioning リポジトリに設定されているデバイスのログイン詳細情報が、物理デバイスに設定されているログイン詳細情報に一致していることを確認します。デバイス上の使用可能なすべての VTY セッションが、使用されていないことを確認します。

Q. MPLS VPN 接続性検証テストを実行すると、ローカル サイトとして設定したデバイスが、時々 [Test Results] ウィンドウのデータ パスの左側に表示されることがあります。その他の場合では、ローカル サイト デバイスは [Test Results] ウィンドウのデータ パスの右側に表示されます。なぜでしょうか。

A. MPLS VPN での接続の問題は、特定の方向だけしか検出できない場合が多くあります。MPLS VPN 接続性検証テストでは、両方向（ローカル サイトからリモート サイト、およびその逆）についてテストされます。問題が発見されたときのテストの方向によって、ローカル サイトのデバイスは [Test Results] ウィンドウのデータ パスの左側または右側のいずれかに表示されます。

Q. 同じクライアント マシンで複数の MPLS VPN 接続性検証テストを並行して実行すると、このうちの 1 つのテスト結果が、すべてのテストの結果画面に表示されます。その他のテストの結果は失われます。回避する方法を教えてください。

A. 同じクライアント マシンで並行して複数の MPLS VPN 接続性検証テストを実行する場合は、各テストが異なる HTTP セッションを使用して実行されていることを確認する必要があります。これを実行するには、コマンドライン、またはデスクトップのブラウザのアイコン、または [Start] メニューから起動した個別のブラウザで各テストを実行します。同じブラウザ ウィンドウの別のタブ、または既存のブラウザ ウィンドウから起動したブラウザ ウィンドウで、複数のテストを並行して実行しないでください。

VPN トポロジ

この付録では、サポートされる VPN トポロジに MPLS VPN 接続性検証テストを実行する方法の詳細を示します。この付録の内容は、次のとおりです。

フル メッシュ VPN トポロジでのテスト

デフォルトで、MPLS VPN 接続性検証テストでは、ローカル サイトとリモート サイトはフル メッシュ VPN トポロジで接続され、これらのサイトは直接通信できると見なされます。フル メッシュ VPN トポロジに MPLS VPN 接続性検証テストを設定する方法の詳細については、「MPLS VPN 接続性検証テストの実行」（P.11-18）を参照してください。

ハブ アンド スポーク VPN トポロジでのテスト

ハブ アンド スポーク VPN で接続されたカスタマー サイト同士は直接通信できません。カスタマー サイト（スポーク）はハブ ルータで通信します。ハブ アンド スポーク VPN で接続された 2 サイト間の接続性をテストする場合は、次の手順でテストを実行します。

ステップ 1　ローカル サイトとリモート サイト間の MPLS VPN 接続性検証テスト。

ステップ 2　ローカル サイトと、ルートをインポートするハブ PE インターフェイスに接続されたハブ CE インターフェイス間の MPLS VPN 接続性検証テスト。

ステップ 3　リモート サイトと、ルートをインポートするハブ PE インターフェイスに接続されたハブ CE インターフェイス間の MPLS VPN 接続性検証テスト。

ステップ 4　ローカル サイトと、ルートをエクスポートするハブ PE インターフェイスに接続されたハブ CE インターフェイス間の MPLS VPN 接続性検証テスト。

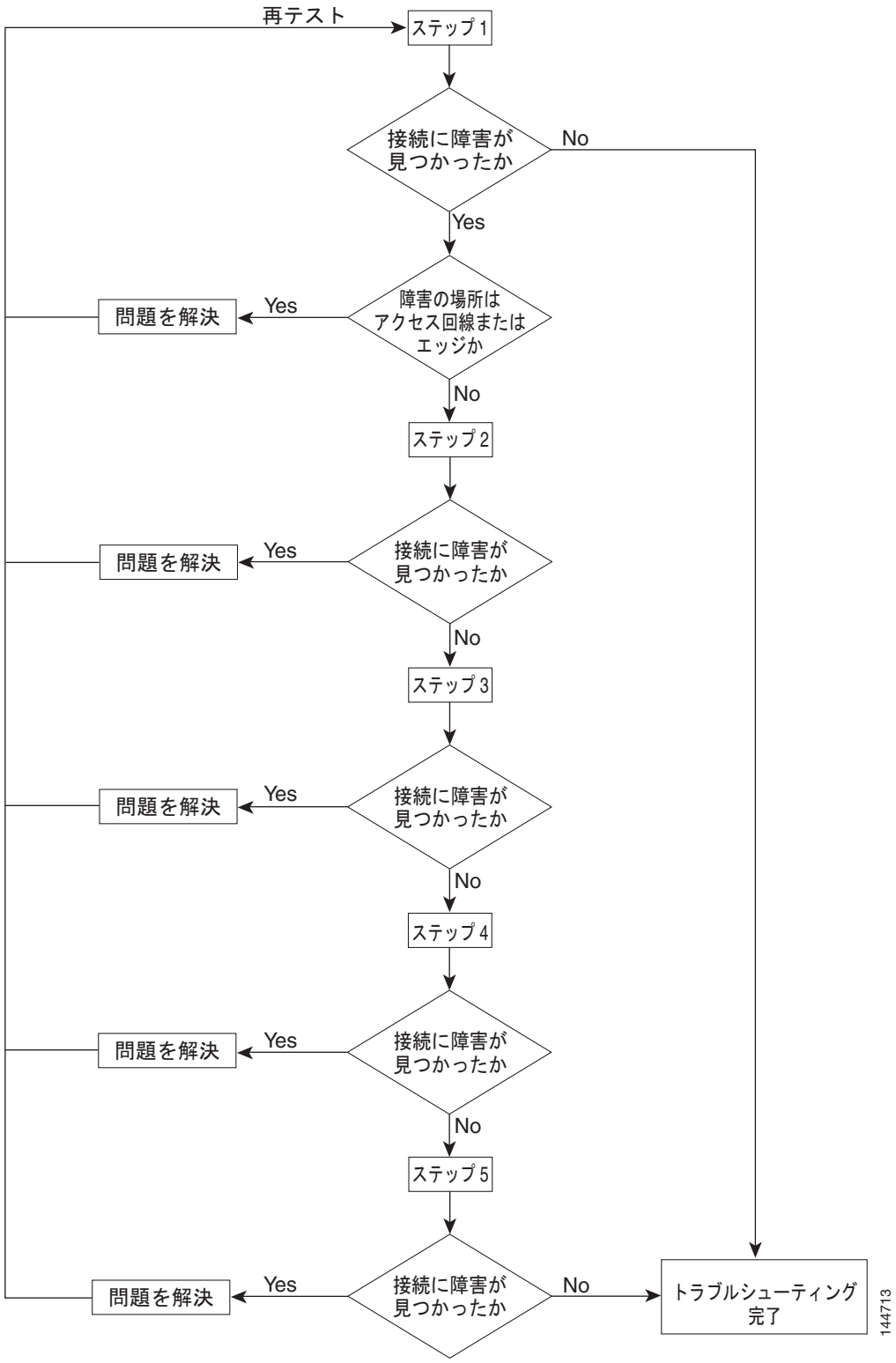
ステップ 5　リモート サイトと、ルートをエクスポートするハブ PE インターフェイスに接続されたハブ CE インターフェイス間の MPLS VPN 接続性検証テスト。

各ステップでは、さまざまなポイント間で MPLS VPN 接続性検証テストを実行します。接続性障害があるかどうかと、この障害の場所によっては、5 つすべてのステップを実行する必要がない場合があります。図 11-27 に、ハブ アンド スポーク VPN をテストするワークフローを示します。

ステップ 1 からステップ 5 で報告された問題を解決してから、ステップ 1 を繰り返してサイト間の接続性が復元されたことを確認してください。

（注）　アクセス回線または VPN エッジの問題に起因する接続性障害がステップ 1 で検出された場合、その問題は、ステップ 1 で実行した MPLS VPN 接続性検証テストによって正しく診断されます。テスト結果の説明に従って問題を解消してください。接続性障害がハブ アンド スポーク MPLS VPN のコア内部の問題に起因する場合、ステップ 1 で報告される結果は正しくないことがあるため無視してください。ステップ 2 からステップ 5 を、問題が正しく診断されるまで実行してください。

図 11-27　ワークフロー

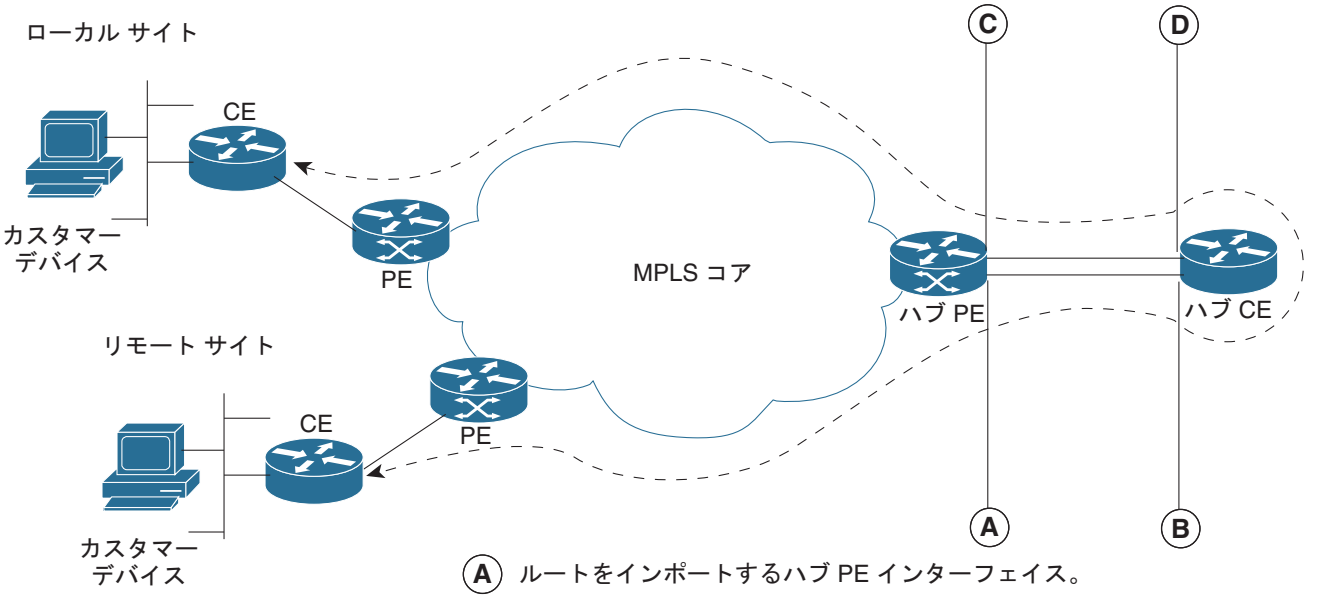


1. ローカル サイトとリモート サイト間の MPLS VPN 接続性検証テストを実行します。このテストで接続性の問題が見つからなければ、トラブルシューティングはこれ以上必要ありません。このテストで MPLS の問題が原因による接続性障害が報告された場合は、テスト結果を無視して 2. に進みます。MPLS VPN 接続性検証テストはフル メッシュ VPN トポロジを前提としているため、報告される問題は正しくありません。ハブ アンド スポーク VPN での問題を識別するためにさらに MPLS VPN 接続性検証テストを実行する必要があります。このテストで MPLS 以外の問題（たとえば、アクセス回線または VPN エッジの障害）が原因による接続性障害が報告された場合は、報告されたとおりに問題を解決して再度テストを行います。

（注）　接続性障害がコアで見つかった場合、1. で実行した MPLS VPN 接続性検証テストでは、ハブ アンド スポーク VPN トポロジがテスト中であることが検出され、以下のステップで説明されている、ハブ アンド スポークに固有のトラブルシューティングの実行を提案されることがあります。MPLS VPN 接続性検証テストは、ルート ターゲットのインポートおよびエクスポートを調べることでハブ アンド スポーク VPN トポロジを検出します。同じルート ターゲットが一方または両方の PE ルータによってインポートおよびエクスポートされると、ハブ アンド スポーク VPN と見なされます。

図 11-28 に、ハブ アンド スポーク VPN の 2 サイト間の接続性をテストするために必要な MPLS VPN 接続性検証テストを示します。

図 11-28　ハブ アンド スポーク VPN トポロジのテスト：ステップ 1



A　ルートをインポートするハブ PE インターフェイス。

B　ルートをインポートするハブ PE インターフェイスに直接接続されたハブ CE インターフェイス。

C　ルートをエクスポートするハブ PE インターフェイス。

D　ルートをエクスポートするハブ PE インターフェイスに直接接続されたハブ CE インターフェイス。

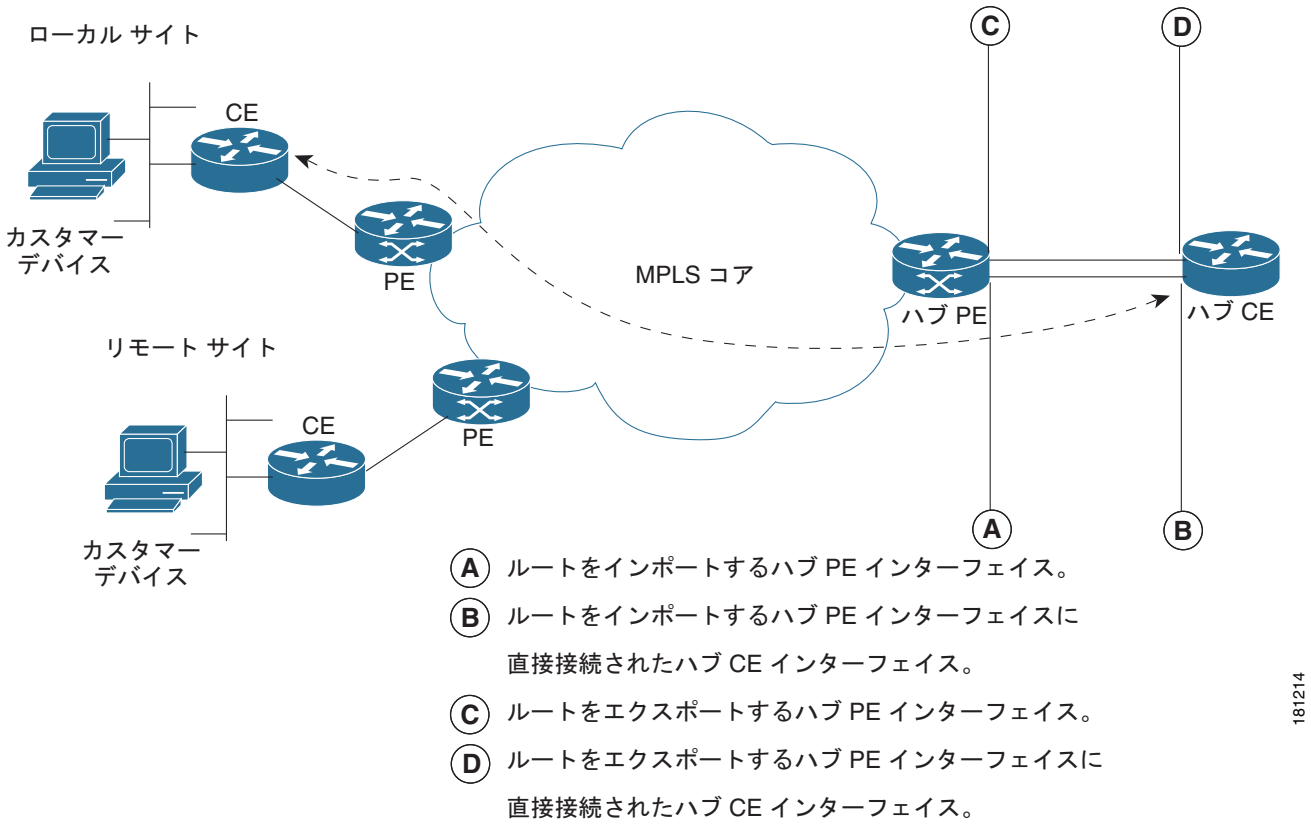
2. ローカル サイト（スポーク）と、ルートをインポートするハブ PE インターフェイスに接続されたハブ CE インターフェイス（図 11-29 の *B*）間の MPLS VPN 接続性検証テストを実行します。MPLS VPN 接続性検証テストを設定する際は、[MPLS VPN Connectivity Verification

Configuration] ウィンドウの [Local Site] フィールドに、ローカル カスタマー サイトの詳細を設定する必要があります。[Remote Site] フィールドには、ルートをインポートするハブ PE および CE インターフェイス（図 11-29 の *A* および *B*）の詳細を設定する必要があります（表 11-14 を参照）。

表 11-14　テストの設定：ルート インポート ハブ インターフェイスのテスト

フィールド名	ハブの詳細
PE Device Name	ハブ PE デバイス名
PE Access Circuit Interface	ルートをインポートするハブ PE インターフェイス。
CE Access Circuit Interface IP Address	ルートをインポートするハブ PE インターフェイスに直接接続されたハブ CE インターフェイスの IP アドレス。
Customer Device IP Address	ブランクのままにします。

図 11-29　ハブ アンド スポーク VPN トポロジのテスト：ステップ 2



A　ルートをインポートするハブ PE インターフェイス。

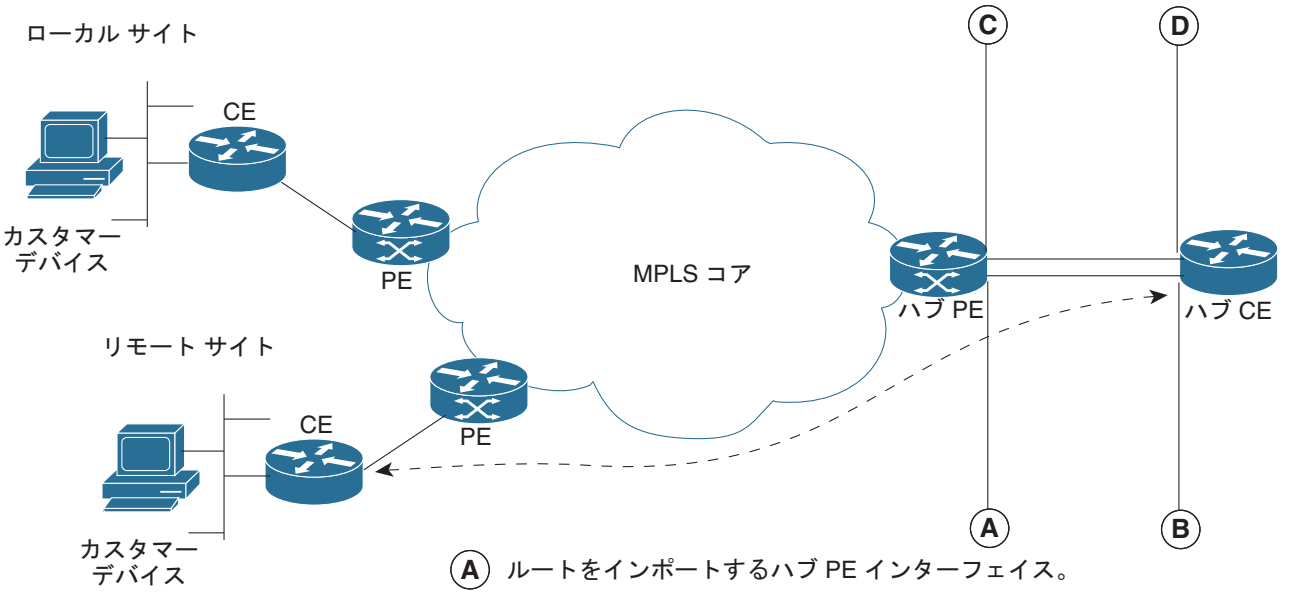
B　ルートをインポートするハブ PE インターフェイスに直接接続されたハブ CE インターフェイス。

C　ルートをエクスポートするハブ PE インターフェイス。

D　ルートをエクスポートするハブ PE インターフェイスに直接接続されたハブ CE インターフェイス。

3. リモート サイト（スポーク）と、ルートをインポートするハブ PE インターフェイスに接続されたハブ CE インターフェイス（図 11-30 の *B*）間の MPLS VPN 接続性検証テストを実行します。MPLS VPN 接続性検証テストを設定する際は、[Local Site] フィールドに、ルートをインポートするハブ PE および CE インターフェイス（図 11-30 の *A* および *B*）の詳細を設定する必要があります（表 11-14 を参照）。[MPLS VPN Connectivity Verification Configuration] ウィンドウの [Remote Site] フィールドには、リモート カスタマー サイトの詳細を設定する必要があります。

図 11-30　ハブ アンド スポーク VPN トポロジのテスト：ステップ 3



A　ルートをインポートするハブ PE インターフェイス。

B　ルートをインポートするハブ PE インターフェイスに直接接続されたハブ CE インターフェイス。

C　ルートをエクスポートするハブ PE インターフェイス。

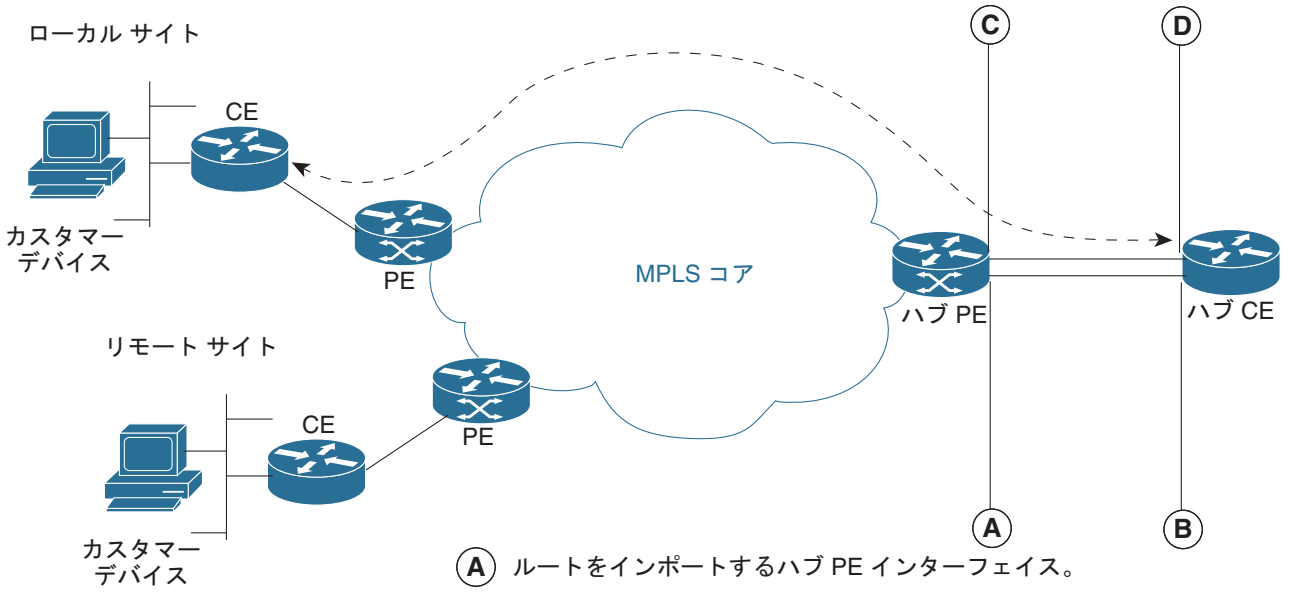
D　ルートをエクスポートするハブ PE インターフェイスに直接接続されたハブ CE インターフェイス。

4. ローカル サイト（スポーク）と、ルートをエクスポートするハブ PE インターフェイスに接続されたハブ CE インターフェイス（図 11-31 の *D*）間の MPLS VPN 接続性検証テストを実行します。MPLS VPN 接続性検証テストを設定する際は、[MPLS VPN Connectivity Verification Configuration] ウィンドウの [Local Site] フィールドに、ローカル カスタマー サイトの詳細を設定する必要があります。[Remote Site] フィールドには、ルートをエクスポートするハブ PE および CE インターフェイス（図 11-31 の *C* および *D*）の詳細を設定する必要があります（表 11-15 を参照）。

表 11-15　テストの設定：ルート エクスポート ハブ インターフェイスのテスト

フィールド名	ハブの詳細
PE Device Name	ハブ PE デバイス名
PE Access Circuit Interface	ルートをエクスポートするハブ PE インターフェイス。
CE Access Circuit Interface IP Address	ルートをエクスポートするハブ PE インターフェイスに直接接続されたハブ CE インターフェイスの IP アドレス。
Customer Device IP Address	ブランクのままにします。

図 11-31　ハブ アンド スポーク VPN トポロジのテスト：ステップ 4



A　ルートをインポートするハブ PE インターフェイス。

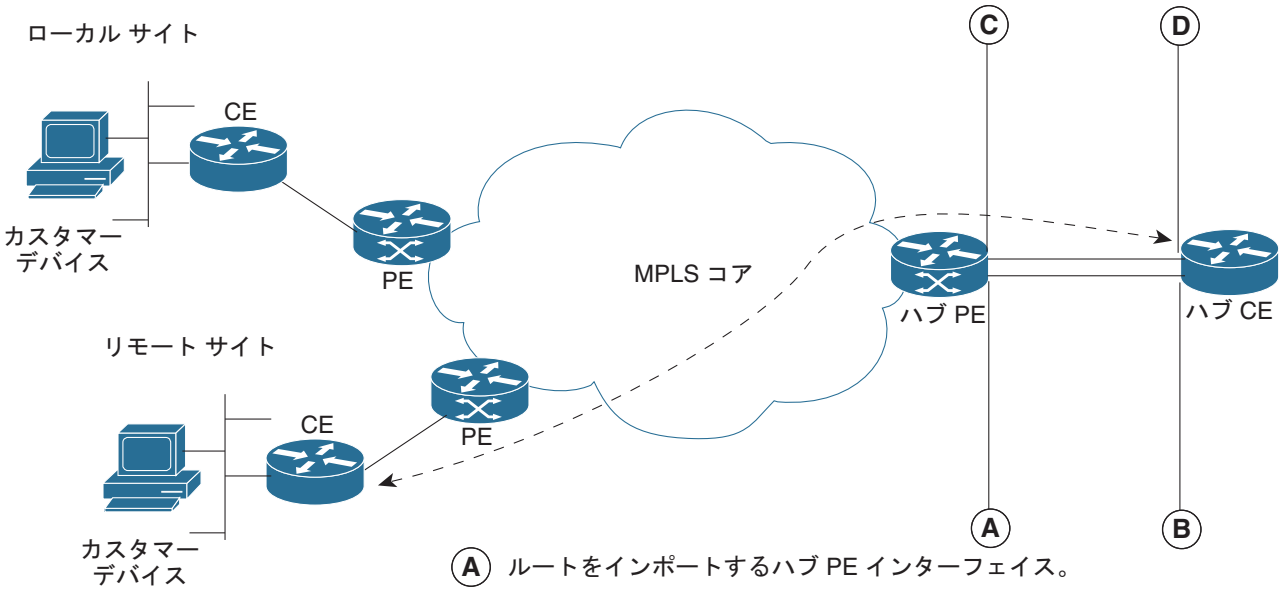
B　ルートをインポートするハブ PE インターフェイスに直接接続されたハブ CE インターフェイス。

C　ルートをエクスポートするハブ PE インターフェイス。

D　ルートをエクスポートするハブ PE インターフェイスに直接接続されたハブ CE インターフェイス。

5. リモート サイト（スポーク）と、ルートをエクスポートするハブ PE インターフェイスに接続されたハブ CE インターフェイス（図 11-32 の *D*）間の MPLS VPN 接続性検証テストを実行します。MPLS VPN 接続性検証テストを設定する際は、[Local Site] フィールドに、ルートをエクスポートするハブ PE および CE インターフェイス（図 11-32 の *C* および *D*）の詳細を設定する必要があります（表 11-15 を参照）。[MPLS VPN Connectivity Verification Configuration] ウィンドウの [Remote Site] フィールドには、リモート カスタマー サイトの詳細を設定する必要があります。

図 11-32　ハブ アンド スポーク VPN トポロジのテスト：ステップ 5



A　ルートをインポートするハブ PE インターフェイス。

B　ルートをインポートするハブ PE インターフェイスに直接接続されたハブ CE インターフェイス。

C　ルートをエクスポートするハブ PE インターフェイス。

D　ルートをエクスポートするハブ PE インターフェイスに直接接続されたハブ CE インターフェイス。

Intranet/Extranet VPN トポロジでのテスト

Intranet/Extranet VPN トポロジを介して接続しているサイト間では、フル メッシュ VPN トポロジの場合と同様に、直接通信が可能です。Intranet/Extranet VPN で接続された 2 サイト間の MPLS VPN 接続性検証テストを設定する際は、通常どおりにテストを設定する必要があります。

Intranet/Extranet VPN で接続されたサイト間の接続性をテストすると、Diagnostics はアクセス回線、VPN エッジ、および MPLS コアの問題を含む MPLS VPN 接続性の問題をトラブルシューティングします。Diagnostics は、不足しているルート マップまたは誤設定されたルート マップなど、Intranet/Extranet VPN に固有の問題のトラブルシューティングは行いません。

MPLS VPN 接続性検証テストによって接続性障害が検出されたが、その障害の原因はアクセス回線、VPN エッジ、および MPLS コアの問題を含む MPLS VPN 接続性の問題にあると考えられない場合は、イントラネット/エクストラネット構成のトラブルシューティングが [Test Results] ウィンドウで推奨されます。

（注）　いずれかの PE でルート マップが設定されていることを見つけると、Diagnostics は、Intranet/Extranet VPN トポロジであると見なします。

セントラル サービス VPN トポロジでのテスト

セントラル サービス VPN トポロジでは、クライアント サイトは 1 つ以上のセントラル サイトと直接通信できますが、クライアント サイト同士では通信できません。セントラル サービス VPN トポロジを介して接続しているクライアント サイトと中央サイト間では、MPLS VPN 接続性検証テストは実行できません。クライアント サイトはローカル サイト、中央サイトはリモート サイトとして入力することで、通常どおりにテストを設定する必要があります。

セントラル サービス VPN の 2 クライアント サイト間の MPLS VPN 接続性検証テストを実行することはできません。

障害シナリオ

この章では、Diagnostics アプリケーションで報告されるすべての障害シナリオの詳細について説明します。また、IOS XR サポート警告についても説明します。

詳細については、mpls-diagnostics-expert@cisco.com まで電子メールでお問い合わせください。

（注）　Diagnostics は、サブインターフェイス/インターフェイスに実装された L3 サービスのみをサポートします。

障害シナリオ

この項では、Diagnostics によって報告される次の障害シナリオについて説明します。

- 「アクセス回線」（P.11-59）
- 「MPLS エッジ」（P.11-71）
- 「MPLS コア」（P.11-77）
- 「カスタマー サイト」（P.11-86）

各障害シナリオの表に、その障害シナリオが 5 つの Diagnostics テスト タイプそれぞれでサポートされているかどうかを示します。この表では、障害シナリオが IOS および IOS XR でサポートされているかどうかを示します。また、障害シナリオが IPv4 および IPv6 向けにサポートされるかどうかも示します。

（注）　この表で、NA は該当なし、NS はサポート適用外を意味します。

アクセス回線

IP 接続をブロックするアクセス回線

プロバイダー（PE）ルータのアクセス回線インターフェイスから送信先への IP 接続を阻止するブロッキング アクセス リストがあります。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	Yes

無効な PE インターフェイスが指定されている

PE ルータ上にインターフェイスが存在しません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	Yes	該当なし	Yes	Yes	Yes	Yes

ATM インターフェイスに VPI/VCI がない

PE ルータ上の非同期転送モード（ATM）アクセス回線インターフェイスに Virtual Path Identifier（VPI; 仮想パス識別子）または Virtual Channel Identifier（VCI; 仮想チャネル識別子）が割り当てられていないか、VPI/VCI が宛先 IP アドレスにマッピングされていません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	NS

ATM インターフェイスのプロトコルがダウン

PE ルータで ATM アクセス回線インターフェイスのプロトコルがダウンしています。「IOS XR サポート」（P.11-86）を参照してください。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	NS

ATM サブインターフェイスのプロトコルがダウン

PE ルータで ATM アクセス回線サブインターフェイスのプロトコルがダウンしています。この障害は、間違ったサブインターフェイス パラメータか、あるいは障害を検出して自動的にインターフェイスをダウンさせる ATM Operation, Administration, and Maintenance（OAM; 運用管理および保守）機能が原因で発生することがあります。「IOS XR サポート」（P.11-86）を参照してください。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	NS

CE アクセス回線インターフェイス IP アドレスの計算は、PE インターフェイスがアンナンバード インターフェイスではなく、PE に /30 サブネット マスク インターフェイスがある場合のみ可能

PE 用のカスタマー エッジ（CE）アクセス回線インターフェイス IP アドレスを計算できません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	該当なし

詳細については、「IPv6 サポート」（P.11-87）を参照してください。

ピアの eBGP 最大プレフィックスを超過

PE と CE 間で exterior Border Gateway Protocol（eBGP; 外部ボーダー ゲートウェイ プロトコル）が動作していますが、ボーダー ゲートウェイ プロトコル（BGP）ネイバーが確立されていません。ピアが設定されたプレフィックス最大数を超えました。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	Yes

eBGP ネイバーが確立されていない、ルートが存在しない

PE と CE 間で eBGP が動作していますが、PE で BGP ネイバーが確立されていません。BGP ネイバーは PE とは異なるサブネット上にあり、VPN Routing/Forwarding（VRF; VPN ルーティング/転送）内にネイバーへのルートがありません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	Yes

eBGP ネイバーが確立されていない、設定ミスの可能性

PE と CE 間で eBGP が動作していますが、PE で BGP ネイバーが確立されていません。VRF 内に BGP ネイバーへのルートがあり、ping を介して BGP ネイバーに到達可能です。CE または PE BGP コンフィギュレーションに問題があります。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	Yes

eBGP ネイバーが確立されていない、ルートは存在する

PE と CE 間で eBGP が動作していますが、PE で BGP ネイバーが確立されていません。BGP ネイバーは PE とは異なるサブネット上にあり、VRF 内にネイバーへのルートが存在します。ただし、ping を介してこの BGP ネイバーに到達できません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	Yes

複数の eBGP サイトが同じ AS 番号を使用している

ローカル サイトとリモート サイトが eBGP を使用し、同一の AS 番号を使用しており、ローカル PE ルータの VRF 内で BGP ネイバーに「allowas-in」も「as-override」も設定されていません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	該当なし	該当なし	該当なし	該当なし	Yes	Yes	Yes

EIGRP がルートを交換していない

PE と CE 間で Enhanced Interior Gateway Routing Protocol（EIGRP）が動作しており、ピア関係が確立されています。ただし、CE の EIGRP からルートを受信していません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	NS

イーサネット インターフェイス プロトコルのダウン

PE ルータ プロトコルのイーサネット アクセス回線インターフェイスがダウンしています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	Yes

イーサネット サブインターフェイス プロトコルのダウン

PE ルータ プロトコルのイーサネット アクセス回線サブインターフェイスがダウンしています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	Yes

フレーム リレー インターフェイスに DLCI がない

PE ルータのフレーム リレー アクセス回線インターフェイスに Data-Dink Connection Identifier（DLCI; データリンク接続識別子）が割り当てられていないか、DLCI が宛先 IP アドレスにマッピングされていません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	NS

フレーム リレー インターフェイス プロトコルのダウン

PE ルータ プロトコルのフレーム リレー アクセス回線インターフェイスがダウンしています。原因として、回線パラメータまたはケーブル配線のミスが考えられます。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	NS

フレーム リレー インターフェイスに DLCI がない

PE ルータ上のアクセス回線インターフェイスのマルチポイント フレーム リレー相手先固定接続（PVC）に、宛先 IP アドレスにマッピングされた DLCI がありません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	NS

フレーム リレー インターフェイスに DLCI がない

PE ルータのアクセス回線インターフェイスで、ポイントツーポイント フレーム リレー PVC に DLCI が割り当てられていません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	NS

フレーム リレー PVC が削除済みとしてマークされている

PE ルータのアクセス回線インターフェイスで、フレーム リレー PVC が削除済みとしてマークされています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	該当なし	Yes	NS

フレーム リレー PVC が停止中としてマークされている

PE ルータのアクセス回線インターフェイスで、マルチポイント フレーム リレー PVC が停止中としてマークされています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	該当なし	Yes	NS

フレーム リレー PVC が停止中としてマークされている

PE ルータのアクセス回線インターフェイスで、ポイントツーポイント フレーム リレー PVC が停止中としてマークされています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	NS

シリアル インターフェイスの搬送波が不完全

PE ルータのシリアル アクセス回線インターフェイスに不完全な搬送波があります。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	NS

インターフェイスが管理上のダウン状態

PE ルータのアクセス回線インターフェイス（またはサブインターフェイス）が管理上の理由でダウンしています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	Yes

インターフェイスが管理上のダウン状態

PE ルータのアクセス回線サブインターフェイスが管理上の理由でダウンしています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	Yes

プロトコルのインターフェイスがダウン状態

PE ルータ プロトコルのアクセス回線インターフェイスがダウンしています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	Yes

PE のインターフェイスはバンドル リンクの仮想アクセス インターフェイスである

この PE のインターフェイスは、有効なアクセス回線インターフェイスではありません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	Yes	該当なし	Yes	該当なし	Yes	NS

インターフェイスが運用停止状態

PE ルータのアクセス回線インターフェイスが動作を停止しています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	Yes

（ATM ネクスト ホップとの）断続的 ATM 障害

ATM アクセス回線は、ATM ネクスト ホップに断続的に ATM 接続しています。「IOS XR サポート」（P.11-86）を参照してください。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	NS

（送信先との）断続的 ATM 障害

ATM アクセス回線は、送信先に断続的に ATM 接続しています。「IOS XR サポート」（P.11-86）を参照してください。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	NS

無効なアクセス回線 IP アドレス コンフィギュレーション

CE ルータのアクセス回線インターフェイス IP アドレスが、接続先 PE のアクセス回線インターフェイス IP アドレスと同じサブネット内にありません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	Yes

無効なアクセス回線 IP アドレス コンフィギュレーション

この CE のアクセス回線インターフェイス IP アドレスがネットワーク アドレスです。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	該当なし

詳細については、「IPv6 サポート」（P.11-87）を参照してください。

無効なアクセス回線 IP アドレス コンフィギュレーション

この CE のアクセス回線インターフェイス IP アドレスがネットワーク ブロードキャスト アドレスです。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	該当なし

詳細については、「IPv6 サポート」（P.11-87）を参照してください。

無効なアクセス回線 IP アドレス コンフィギュレーション

CE のアクセス回線インターフェイス IP アドレスと、接続先 PE のアクセス回線インターフェイス IP アドレスが同じです。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	Yes

IP 接続の問題

IP 接続に関する未知の問題。PE インターフェイスから CE への VRF インスタンスで、アクセス回線の接続に問題が生じています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
該当なし	Yes	該当なし	該当なし	該当なし	Yes	Yes	Yes	Yes

ルートの欠落

PE ルータのアクセス回線インターフェイスから送信先へのルートが存在しません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	Yes

ルートの欠落

PE ルータのアクセス回線インターフェイスからカスタマーの送信先へのルートが存在しません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	Yes

EIGRP ピア関係が確立されていない

PE と CE 間でルーティング プロトコル EIGRP は動作していますが、ピア関係が確立されていません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	NS

EIGRP ピア関係が確立されていない

PE と CE 間では、ルーティング プロトコル EIGRP が動作しています。PE および CE インターフェイスは異なるサブネット上にあり、IP アンナンバードを使用していません。PE と CE が異なるサブネット上にあるため、ピア関係が確立されていません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	NS

ルート再配布でルート ポリシーが指定されていない

PE と CE 間でルーティング プロトコル EIGRP が動作し、MP-BGP にルートが再配布されています。ただし、発信ルート ポリシーが指定されていないため、すべてのルートはアドバタイズされずにドロップされます。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	該当なし	Yes	Yes	NS

OSPF ピアがない

PE と CE 間で Open Shortest Path First（OSPF）が動作していますが、PE にピアが存在しません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	NS

ピア インターフェイスの OSPF がイネーブルでない

ルータ上のインターフェイスで OPSF がイネーブルになっていません。両方のネイバー インターフェイスで OSPF をイネーブルにしておく必要があります。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	NS	Yes	Yes	NS

ピア インターフェイスの OSPF がパッシブ モード

ルータ上のインターフェイスで OSPF がパッシブ モードになっています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	NS	Yes	Yes	NS

OSPF エリアの不一致

ネイバー インターフェイス上で OSPF がイネーブルになっていますが、これらのインターフェイスは異なるエリア内に設定されています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	NS	Yes	Yes	NS

OSPF エリア タイプの不一致

ネイバー インターフェイス上で OSPF がイネーブルになっていますが、これらのインターフェイスは異なるエリア タイプに設定されています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	NS	Yes	Yes	NS

PE と CE 間で動作するルーティング プロトコルが確定しておらず、スタティック ルートが存在しない

VRF 内のアクセス回線に問題があります。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	Yes

OSPF がルートを交換していない

PE と CE 間で OSPF が動作していますが、ピア関係が確立されています。ただし、CE の OSPF からルートを受信していません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	NS

OSPF ピアが確立されていない

PE と CE 間で OSPF が動作していますが、ピア関係が確立されていません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	該当なし

OSPF 時間の不一致

ネイバー インターフェイス上で OSPF はイネーブルになっていますが、これらのインターフェイスの [hello|dead] タイマーにはそれぞれ異なる値が設定されています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	NS	Yes	Yes	NS

OSPF ピアが確立されていない

PE と CE 間では OSPF が動作しています。ただし、PE および CE インターフェイスは異なるサブネット上にあり、IP アンナンバードを使用していないため、ピア関係が確立されていません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	NS

ルート再配布でルート ポリシーが指定されていない

PE と CE 間でルーティング プロトコル OSPF が動作し、MP-BGP にルートが再配布されています。ただし、発信ルート ポリシーが指定されていないため、すべてのルートはアドバタイズされずにドロップされます。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	NS	Yes	Yes	NS

PE に CE へのルートがない

接続されている PE および CE インターフェイスは、異なるサブネット上にあります。PE と CE 間で動作するルーティング プロトコルが確定しておらず、CE へのスタティック ルートが存在しません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	該当なし	Yes	NS

RIB 障害

PE から VRF 内の宛先へのルートが VRF ルーティング テーブルに設定されていません。これは Routing Information Base（RIB; ルーティング情報ベース）障害と見なされます。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	Yes	該当なし	Yes	該当なし	Yes	NS

RIP の設定ミス

PE と CE 間で Routing Information Protocol（RIP）が動作していますが、CE の RIP からルートを受信していません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	NS

RIP がルートを交換していない

PE と CE 間で RIP が動作していますが、PE および CE インターフェイスは異なるサブネット上にあり、IP アンナンバードを使用していないため、CE の RIP からルートを受信していません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	NS

ルート再配布でルート ポリシーが指定されていない

PE と CE 間でルーティング プロトコル RIP が動作し、MP-BGP にルートが再配布されています。ただし、発信ルート ポリシーが指定されていないため、すべてのルートはアドバタイズされずにドロップされます。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	該当なし	Yes	Yes	NS

ループバック モードのシリアル インターフェイス

PE ルータのシリアル アクセス回線インターフェイスがループバック モードに設定されています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	NS

シリアル インターフェイスが運用停止状態

PE ルータのシリアル アクセス回線インターフェイスが動作を停止しています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	NS

ATM ポイントツーポイント インターフェイスのスタティック IP アドレス

ATM アクセス回線の ATM ポイントツーポイント サブインターフェイスに、スタティック IP アドレス マッピングが指定されています。ポイントツーポイント サブインターフェイスでは、トラフィックに対する VC とパスはそれぞれ 1 つだけなので、スタティック マッピングもアドレス解決プロトコル（ARP）も必要ありません。「IOS XR サポート」（P.11-86）を参照してください。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	NS

プロトコルのサブインターフェイスがダウン状態

PE ルータ プロトコルのアクセス回線サブインターフェイスがダウンしています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	Yes

未診断の ATM 障害（ATM ping は失敗したが、ATM セグメントの ping は成功）

ATM アクセス回線の接続が中断されています。エンドツーエンド ATM ping は失敗しましたが、ATM セグメントの ping は成功しました。原因として、ATM 回線パラメータの間違い、ATM ルーティングの設定ミス、CE または ATM クラウド インターフェイスのダウン、デバイスの停止など、さまざまな問題が考えられます。「IOS XR サポート」（P.11-86）を参照してください。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	NS

未診断の ATM 障害（エンドツーエンドおよびセグメント ATM ping が失敗）

ATM アクセス回線の接続が中断されています。エンドツーエンド ping とセグメント ATM ping がどちらも失敗しました。原因として、ATM 回線パラメータの間違い、ATM ネクスト ホップでの ATM ルーティングの設定ミス、ネクスト ホップ インターフェイスのダウン、デバイスの停止など、さまざまな問題が考えられます。「IOS XR サポート」（P.11-86）を参照してください。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	NS

PE アクセス回線インターフェイスに仮想テンプレート インターフェイスが指定されている

この PE の PE インターフェイスは、有効なアクセス回線インターフェイスではありません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	Yes	該当なし	Yes	該当なし	Yes	NS

MPLS エッジ

BGP ネクスト ホップ インターフェイスが管理上のダウン状態

PE の BGP ネクスト ホップがループバック インターフェイスに割り当てられています。ただし、このインターフェイスは管理上の理由でダウンしています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	Yes	Yes	Yes

BGP ネクスト ホップがインターフェイスに割り当てられていない

リモート サイト PE へのルートの BGP ネクスト ホップが、リモート PE のインターフェイスに割り当てられていません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	Yes	Yes	Yes

BGP が非アクティブ

PE ルータで BGP がアクティブになっていません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	Yes	該当なし	Yes	Yes	Yes	Yes

複数の BGP ピアが同じ BGP ネクスト ホップを使用している

複数の BGP VPNv4/VPNv6 ピアが同一の BGP ネクスト ホップを使用しています。このため、PE ルートの正しいルート配布ができません。これ以外のルーティング問題も発生する可能性があります。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	該当なし	Yes	Yes	Yes	Yes

複数の BGP ピアが同じ Router Identifier（RID; ルータ ID）を使用している

複数の BGP VPNv4/VPNv6 ピアが同一のルータ ID を使用しています。このため、PE ルートの正しいルート配布ができません。これ以外のルーティング問題も発生する可能性があります。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	Yes	Yes	Yes

同じサブネット内に複数のアクセス回線がある

LSP 接続およびコントロール プレーンに関する問題。リモート PE ルータに対して現在選択されている BGP ルートのネクスト ホップが、ローカル PE ルータのインターフェイスに割り当てられていません。ローカル PE ルータの VRF に、リモート プレフィックスへの VPNv4/VPNv6 ルートが複数存在します。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	該当なし	該当なし	該当なし	Yes	Yes	Yes	Yes

BGP と LFIB の不一致

BGP テーブルとラベル転送情報ベース（LFIB）テーブルのタグなしエントリが一致しません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	Yes	該当なし	Yes	Yes	Yes	Yes

BGP と LFIB の不一致

Forwarding Information Base（FIB; 転送情報ベース）と BGP のエントリが一致しません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	Yes	該当なし	Yes	Yes	Yes	Yes

BGP ネクスト ホップの重複

ネットワーク内で、PE の BGP ネクスト ホップの IP アドレスが重複しています。

CE から CE	PE から接続先 CE	CEからコア上のPE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	Yes	Yes	Yes

IP アドレスの重複

PE ルータに、アクセス回線インターフェイスと重複する IP アドレスが設定されています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	Yes

IP アドレスの重複

ネットワーク内で、PE の BGP ルータ ID の IP アドレスが重複しています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	Yes	Yes	Yes

eBGP が MP-BGP に接続ルートを再配布していない

PE と CE 間でルーティング プロトコル eBGP が動作していますが、PE の eBGP は接続ルートを Multi Protocol（MP; マルチ プロトコル）-BGP に再配布しておらず、明示的なネットワーク文もありません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	Yes

FIB と LFIB の不一致

FIB テーブルと LFIB テーブルの集約エントリが一致しません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	Yes

入力 FIB と出力 LFIB の不一致

入力 FIB と出力 LFIB が一致しません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	Yes	該当なし	Yes	Yes	Yes	Yes

BGP エントリの不一致

VRF の BGP エントリが一致しません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	Yes	該当なし	Yes	Yes	Yes	Yes

ラベルの不一致、または異なる VPN にあるインターフェイスがダウン

VRF で、PE から送信先への VPN 接続に問題が生じています。プレフィックスの BGP VPNv4/VPNv6 ラベルが一致しません。これは、ラベルの不一致、またはインターフェイスが異なる VPN にあることを示している可能性があります。選択されたインターフェイスが同じ VRF にあることを確認してください。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
該当なし	該当なし	該当なし	Yes	該当なし	Yes	Yes	Yes	Yes

PE インターフェイスが管理上のダウン状態

PE ルータのアクセス回線インターフェイスが管理上の理由でダウンしています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	NS

Router Identifier（RID; ルータ ID）の欠落

PE のローカル ルータ ID を特定できません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
該当なし	該当なし	該当なし	該当なし	Yes	Yes	Yes	Yes	Yes

VPNv4 アドレス ファミリ コンフィギュレーションの欠落

VPNv4 コンフィギュレーションが欠落しています。バーチャル プライベート ネットワーク（VPN）ラベルの交換に問題があります。PE ルータの BGP ルータ コンフィギュレーションで、VPNv4 アドレス ファミリ コンフィギュレーションが欠落しています。このためルートはドロップされます。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	該当なし	Yes	Yes	Yes	Yes

VPNv6 アドレス ファミリ コンフィギュレーションの欠落

VPNv6 コンフィギュレーションが欠落しています。バーチャル プライベート ネットワーク（VPN）ラベルの交換に問題があります。PE ルータの BGP ルータ コンフィギュレーションで、VPNv6 アドレス ファミリ コンフィギュレーションが欠落しています。このためルートはドロップされます。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	該当なし	該当なし	Yes	該当なし	Yes

IOS XR ルータで MPLS LDP パッケージがイネーブルでない

IOS XR ルータで MPLS LDP パッケージがイネーブルになっていません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	該当なし	Yes	Yes	Yes

IOS XR ルータに MPLS パッケージがインストールされているがアクティブでない

IOS XR ルータに MPLS パッケージがインストールされていますが、アクティブになっていません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	該当なし	Yes	Yes	Yes

IOS XR ルータに MPLS パッケージがインストールされていない

IOS XR ルータに MPLS パッケージがインストールされていません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	該当なし	Yes	Yes	Yes

MP-BGP ネイバーがない

PE ルータで MP-BGP ネイバーが定義されていません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	該当なし	Yes	Yes	Yes	Yes

MP-BGP ネイバー セッションが確立されていない

PE ルータで MP-BGP ネイバー セッションが確立されていません。

CE から CE	PE から接続先 CE	CEからコア上のPE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	該当なし	Yes	Yes	Yes	Yes

プレフィックスの VPN ラベルがない

プレフィックスに VPN ラベルが割り当てられていません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	該当なし	Yes	Yes	Yes	Yes

PE インターフェイスに VRF が関連付けられていない

PE ルータのインターフェイスに VRF が関連付けられていません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	該当なし	Yes	Yes	Yes	Yes

OSPF ループバック インターフェイスが /32 以外のネットマスクを使用している

PE によって VPNv4 ルートが IBGP ネイバーにアドバタイズされています。ネクスト ホップのアドレスは、/32 マスクが定義されていないループバック インターフェイスです。OSPF はこのループバック インターフェイス上で使用されており、このインターフェイスの OSPF ネットワーク タイプはループバックです。マスクの設定に関係なく、OSPF はこの IP アドレスをホスト ルートとして（マスク /32 を使用して）アドバタイズします。このアドバタイジングは、設定済みマスクを使用する TDP/LDP と

競合します。したがって、TDP/LDP ネイバーは、このルータによってアドバタイズされるルートのラベルを受信できない場合があります。このため、同じ VPN に属するサイト間の接続が中断される可能性があります。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	該当なし	Yes	該当なし

PE インターフェイスに IP アドレスがない

PE ルータのインターフェイスに IP アドレスがありません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	該当なし	Yes	Yes	Yes	Yes

ルータ ID ループバック インターフェイスのダウン

PE のローカル ルータ ID の関連付けに使用するループバック インターフェイスが管理上の理由でダウンしています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	Yes

MP-BGP との間でルートが再配布されていない

PE の MP-BGP との間でルートが再配布されていません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	該当なし	Yes	該当なし

リモート プレフィックスへのスタティック ルート

PE の VRF 内で、リモート プレフィックスへのスタティック ルートが設定されています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	該当なし	Yes	Yes	Yes	Yes

トラフィックの管理上のブロック

トラフィックが管理上の理由でブロックされているため、PE から送信先への VPN 接続に問題が生じています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	該当なし	該当なし	Yes	Yes	Yes	Yes

レイヤ 3 VPN のトラブルシューティングで障害の原因を特定できない

LSP 接続の問題。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	Yes	Yes	Yes

レイヤ 3 VPN のトラブルシューティングで障害の原因を特定できない

VRF で、PE から送信先への VPN 接続に問題が生じています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	該当なし	Yes	Yes	Yes	Yes

VRF ルート ターゲット インポート/エクスポートの不一致

PE デバイス間で VRF ルート ターゲット インポート/エクスポートが一致しません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	該当なし	Yes	Yes	Yes	Yes

MPLS コア

無効な PE インターフェイスが指定されている

LSP エンドポイントとして指定されたインターフェイスは、PE ルータ上に存在しません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
該当なし	該当なし	該当なし	該当なし	Yes	Yes	Yes	Yes	該当なし

LDP ネイバー セッションの中断

ダウンストリーム ネイバーとの LDP セッションが中断されました。ルータのルート プロセッサ/ラインカード転送に不一致があります。「IOS XR サポート」（P.11-86）を参照してください。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	該当なし	Yes	Yes

ルータの CEF がイネーブルでない

ルータ上で CEF がイネーブルになっていません。「IOS XR サポート」（P.11-86）を参照してください。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	該当なし	Yes	Yes

配布された LFIB テーブルの不一致

ルート プロセッサとラインカードの LFIB テーブルが一致しません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	該当なし	Yes	Yes	Yes	Yes

配布された FIB テーブルの不一致

ルート プロセッサとラインカードの FIB テーブルが一致しません。

CE から CE	PEから接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	該当なし	Yes	Yes	Yes	Yes

ラベルの不一致

ルータ上で、LFIB ローカル タグ、受信パケット、および LDP ローカル バインディング ラベルに不一致があります。「IOS XR サポート」（P.11-86）を参照してください。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	該当なし	Yes	Yes

LDP ホストが到達不能

ラベル スイッチ ルータ（LSR）からホストに到達できません。原因として、ダウンストリーム ルータとの LDP セッションがルータ上で確立されていない、IGP の問題によって LDP ID に到達できない、LDP パケットをブロックする ACL が設定されている、認証上の問題などが考えられます。

CE から CE	PE から接続先 CE	CEからコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	Yes	Yes	Yes

LDP ラベルの不一致

プレフィックス用に受信したラベルと送信したラベルが一致しません。「IOS XR サポート」（P.11-86）を参照してください。

CE から CE	PE から接続先 CE	CEからコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	該当なし	Yes	Yes

LDP ネイバーが見つからない

LDP ネイバーが検出されませんでした。これは、ダウンストリーム ネイバーとデバイスとのインターフェイスでよく見られる LDP 検出問題です。「IOS XR サポート」（P.11-86）を参照してください。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	該当なし	Yes	Yes

LDP ネイバーが見つからない

LDP ネイバーが検出されませんでした。ルータのインターフェイスに ACL が設定されているため、LDP ネイバーを検出できない場合があります。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	Yes	Yes	Yes

LDP ネイバーが確立されていない

LSP 接続およびコントロール プレーンに関する問題。LDP セッションが確立されていません。インターフェイスに ACL が設定されているため、ポート 646 で LDP セッションを確立できない場合があります。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	Yes	Yes	Yes

LDP/TDP の不一致

リンクの一方の終端では LDP、もう一方の終端では TDP がイネーブルになっています。「IOS XR サポート」（P.11-86）を参照してください。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	Yes	Yes	Yes

LSP 応答パスの問題

LSP 接続の応答パスに問題があります。「IOS XR サポート」（P.11-86）を参照してください。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	該当なし	Yes	Yes

LFIB エントリの欠落

LFIB エントリがありません。原因として、以前のルータでのルーティング ミス、またはループバックの重複が考えられます。「IOS XR サポート」（P.11-86）を参照してください。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	該当なし	Yes	Yes

リターン パスの欠落、またはタグのないリターン パス

コア ルータからのリターン パスがないか、リターン パスにプレフィックスのタグが付いていません。「IOS XR サポート」（P.11-86）を参照してください。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	該当なし	Yes	Yes

MPLS ラベル スペースの枯渇

ルータの MPLS ラベル スペースがなくなりました。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	Yes	Yes	Yes

MPLS がグローバルにイネーブル化されていない

MPLS がルータ上でグローバルにイネーブル化されていません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	該当なし	Yes	Yes

インターフェイスの MPLS がイネーブルでない

MPLS がインターフェイス上でイネーブルになっていません。「IOS XR サポート」（P.11-86）を参照してください。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	Yes	Yes	Yes

ラベルのエントリがない

送信先プレフィックスへの着信ラベルの LFIB にエントリがありません。「IOS XR サポート」（P.11-86）を参照してください。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	該当なし	Yes	Yes

ネイバーとの LDP セッションがない

ルータに上ネイバーとの LDP セッションが存在しません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	Yes	Yes	Yes

有効なネクスト ホップ エントリがない

現在のデバイスで、ネクスト ホップの有効なエントリが見つかりません。「IOS XR サポート」（P.11-86）を参照してください。

CE から CE	PEから接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	該当なし	Yes	Yes

転送パスのルーティング ループ

転送パスにルーティング ループがあります。

CE から CE	PEから接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	Yes	Yes	Yes

コアに接続するすべての MPLS 対応インターフェイスがダウン

LSP 接続およびコントロール プレーンに関する問題。MPLS 対応インターフェイスが動作していません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	Yes	Yes	Yes

ラベル アドバタイジングがイネーブルでない

ルータ上でラベル アドバタイジングがディセーブルになっています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	Yes	Yes	Yes

ラベル アドバタイジングが ACL によって拒否される

ラベル アドバタイジングはグローバルにディセーブル化されていますが、一部は 1 つまたは複数のアクセス リストに対してイネーブルになっています。送信先プレフィックスへのラベルのアドバタイジングを ACL が拒否している可能性があります。

CE から CE	PE から接続先 CE	CEからコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	Yes	Yes	Yes

TTL の伝播がディセーブル

デバイスが存続可能時間（TTL）を伝播していないため、障害箇所のトラブルシューティングまたは検出ができません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	Yes	Yes	Yes

トンネル トラフィック アドミッション ポリシーを確認

TE トンネルに（autoroute announce を介して、あるいは Policy Based Tunnel Selection（PBTS; ポリシー ベースのトンネル選択）またはスタティック ルートなどの）トラフィック アドミッション ポリシーが設定されていません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	該当なし	Yes	Yes	Yes

トンネル インターフェイスで MPLS がイネーブルかどうかを確認

MPLS TE トンネル インターフェイスで不完全なコンフィギュレーションが検出されました。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	該当なし	Yes	NS	Yes	Yes	Yes

プライマリおよびバックアップ トンネルのインターフェイスが動作していることを確認

ルータのトンネル インターフェイスが管理上の理由でダウンしています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	NS	Yes	Yes	Yes

ヘッドエンドにトンネル コンフィギュレーションがない

ヘッドエンド ルータに TE トンネル コンフィギュレーションが存在しません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	NS	Yes	Yes	Yes

トンネルの発信インターフェイスが動作していることを確認

ルータに設定された FRR プライマリ トンネルの発信インターフェイスが動作を停止しています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	NS	Yes	Yes	Yes

ルータの TE がグローバルにイネーブル化されていない

MPLS トラフィック エンジニアリングが、ルータ上でグローバルにイネーブル化されていません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	NS	Yes	Yes	Yes

インターフェイスの TE がグローバルにイネーブル化されていない

MPLS トラフィック エンジニアリングが、ルータのインターフェイスでイネーブルになっていません。

CE から CE	PE から接続先 CE	CEからコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	NS	Yes	Yes	Yes

IP アドレスがトンネルに割り当てられていない

MPLS トラフィック エンジニアリング トンネルに IP アドレスが割り当てられていません。

CE から CE	PE から接続先 CE	CEからコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	NS	Yes	Yes	Yes

トンネルの宛先が無効

トンネルに設定されている宛先アドレスは到達不能です。

CE から CE	PE から接続先 CE	CEからコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	NS	Yes	Yes	Yes

トンネルが管理上のシャットダウン状態

管理上の理由により、ルータのトンネルがシャットダウンされました。

CE から CE	PE から接続先 CE	CEからコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	NS	Yes	Yes	Yes

TE の OSPF コンフィギュレーションの欠落

MPLS TE の OSPF がルータに設定されていません。

CE から CE	PE から接続先 CE	CEからコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	NS	Yes	Yes	Yes

ノードが MPLS TE リンクをアドバタイズしていない

ルータは、自身を MPLS TE リンクとして OSPF 経由でアドバタイズしていません。

CE から CE	PE から接続先 CE	CEからコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	NS	Yes	Yes	Yes

ターゲット LDP セッションがピア PE 間に存在しない

リモート サイト PE ルータが、ターゲット LDP セッション要求を受け付けません。

CE から CE	PE から接続先 CE	CEからコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	該当なし	Yes	NS	Yes	Yes	Yes

ブロッキング ACL を原因とするターゲット LDP セッションのセットアップ問題

ルータは、（TCP ポート 646 で）LDP メッセージをブロックするアクセス コントロール リストを保持しています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	NS	Yes	Yes	Yes

PE 間でターゲット LDP が確立されていない、または動作していない

ピア PE ルータが到達不能なため、LDP はデバイス間でターゲット セッションを確立できませんでした。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	NS	Yes	Yes	Yes

トンネル接続の障害、ターゲット LDP コンフィギュレーションがない

ネイバー デバイスに対する LDP 検出が失敗しました。トンネル テール エンド デバイスが、LDP ターゲット hello を受け付けません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	Yes	Yes	Yes

リンク保護のため、保護されたインターフェイスをバックアップ トンネルが通過しないよう確認

ルータに FRR バックアップ トンネルが設定されています。FRR バックアップ トンネルは、プライマリ トンネルが通過するパス上にあるルータ（NHOP）でリンクを保護するように設定されています。しかし、設定済みバックアップ トンネルは、このリンクを経由するように設定されています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	NS	Yes	Yes	Yes

プライマリ トンネルで「fast-reroute」を使用して FRR がイネーブルになっていることを確認

ルータ上でトンネルが検出されました。このトンネルはプライマリ トンネルとして使用されますが、必要とされる fast-reroute の設定が行われていないようです。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	該当なし	Yes	NS	Yes	Yes	Yes

ノードの保護：バックアップ トンネル パスが明示的かどうかと、保護されたノード インターフェイスがパスに含まれていないかどうかを確認

FRR バックアップ トンネルがルータに設定されています。FRR バックアップ トンネルは、プライマリ トンネルが通過するパス上にあるルータ（NNHOP）を保護するように設定されています。しかし、設定済みバックアップ トンネルは、このルータ上のリンクを経由するように設定されています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	NS	Yes	Yes	Yes

プライマリおよびバックアップ トンネルのマージ ポイントが到達可能かどうかを確認

FRR プライマリ トンネルと FRR バックアップ トンネルのマージ ポイント ルータが到達不能です。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	NS	Yes	Yes	Yes

TE ping の失敗

ping mpls traffic-eng tunnel コマンドで failure が返されました。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	該当なし	Yes	NS	Yes	Yes	Yes

トンネルが運用停止状態

show mpls traffic-eng tunnels コマンドで、TE トンネルがダウンしていることが示されました。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	該当なし	Yes	NS	Yes	Yes	Yes

トンネル接続の障害

MPLS TE 接続に関する未知の問題。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	該当なし	Yes	Yes	Yes

MPLS TE 接続の問題をトラブルシューティングできない

このルータは OAM Cisco IOS 以外のバージョンを実行しています。トンネルの接続をテストできません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	Yes	Yes	Yes

未知の LSP 接続問題

LSP 接続、データ プレーン、または未知の原因による問題。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	Yes	Yes	Yes

サポートされていない IOS バージョン

コア ルータはサポートされていない IOS バージョンを実行しています。この IOS バージョンは、必要な OAM 機能をサポートしていません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	該当なし	Yes	NS

VPN 接続テストが実行され、障害は検出されなかった（ただし CE への ping はブロックされ、VPN 接続の検証は不可）

VRF 内の PE から送信先への VPN 接続を検証できません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

カスタマー サイト

カスタマー側のルーティングに問題がある可能性

PE には CE からの複数のルートがありますが、CE が ping に応答できません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	Yes

IOS XR サポート

この項では、IOS XR サポート警告について説明します。

1. 「インターフェイスの MPLS がイネーブルでない」（P.11-80）

   IOS XR にはパッケージの概念が取り入れられています。Diagnostics に関係するパッケージの 1 つが MPLS パッケージです。Diagnostics トラブルシューティングでコアの IOS XR ルータを中心に扱う場合、さまざまな準備チェックが行われ、ルータが適切に設定されている、つまり、MPLS パッケージがインストールされてアクティブであることを確認してから、必要な機能（MPLS OAM および MPLS LDP）がイネーブルになっていることを確認します。これらのチェックのいずれかで不合格になると、障害シナリオが報告されます。「インターフェイスの MPLS がイネーブルでない」（P.11-80）は、IOS デバイスに対して、あるいは IOS XR デバイスのインターフェイスで MPLS がディセーブルの場合、引き続き有効です。

2. 「ルータの CEF がイネーブルでない」（P.11-77）

Diagnostics はこれまでどおり、コアの IOS ルータで CEF がディセーブルになっている状況を特定できます。たとえば、CLI コンフィギュレーションによって、あるいはルータが過負荷になって自動的にシャットダウンした場合に CEF がディセーブルになることがあります。その場合、IOS CLI コマンド **show cef state** によって CEF が *enabled/running* または *disabled/not running* のいずれの状態であるかが報告され、Diagnostics は CEF がディセーブルであると判断できます。

IOS XR ルータで CEF をディセーブルにすることはできません。IOS XR ルータの CEF スイッチング機能が過負荷になっても、ルータはシャットダウンしません。代わりに、CEF スイッチング プロセスの負荷を減らす目的で、未処理要求のキューにバック プレッシャーを適用します。このため、IOS XR ルータでは関連する CLI **show** コマンドで CEF の運用停止状態は報告されません。したがって、この障害シナリオは IOS XR ルータでは有効ではありません。

3. 「LDP/TDP の不一致」（P.11-79）

   直接接続された IOS XR ルータが存在する場合、これは有効なシナリオではありません。なぜなら、IOS XR は Label Distribution Protocol（LDP; ラベル配布プロトコル）を 1 つしかサポートしないからです。IOS-IOS XR、IOS XR-IOS、または IOS-IOS コンフィギュレーションで設定されたアプリケーションでは、LDP-TDP の不一致が検出される場合があります。

4. 「LDP ネイバー セッションの中断」（P.11-77）

   「ラベルの不一致」（P.11-78）

   「LDP ラベルの不一致」（P.11-78）

   「LDP ネイバーが見つからない」（P.11-78）

   「LSP 応答パスの問題」（P.11-79）

   「LFIB エントリの欠落」（P.11-79）

   「リターン パスの欠落、またはタグのないリターン パス」（P.11-80）

   「ラベルのエントリがない」（P.11-80）

   「有効なネクスト ホップ エントリがない」（P.11-81）

   これらの障害シナリオは、IOS バージョン固有のバグが原因であり、IOS XR には適用されません。

5. 「ATM インターフェイスのプロトコルがダウン」（P.11-60）

   「ATM サブインターフェイスのプロトコルがダウン」（P.11-60）

   「（ATM ネクスト ホップとの）断続的 ATM 障害」（P.11-64）

   「（送信先との）断続的 ATM 障害」（P.11-65）

   「ATM ポイントツーポイント インターフェイスのスタティック IP アドレス」（P.11-70）

   「未診断の ATM 障害（ATM ping は失敗したが、ATM セグメントの ping は成功）」（P.11-70）

   「未診断の ATM 障害（エンドツーエンドおよびセグメント ATM ping が失敗）」（P.11-70）

   CRS-1 プラットフォーム上の ATM インターフェイスの場合、これらの障害はサポートされません。ただし、IOS デバイスと、Cisco 12000 XR シリーズに搭載された IOS XR には適用されます。

IPv6 サポート

この項では、IPv6 サポート警告について説明します。

- IOS および IOS XR デバイス向けの IPv4 トラブルシューティングに加え、PE-CE リンクで IPv6 アドレッシングが使用される IOS XR デバイスにもトラブルシューティングが拡張されています。IPv6 は、IOS デバイスではサポートされません。

- イーサネットは、IOS XR デバイスで IPv6 アドレッシングが使用される場合に Diagnostics がトラブルシューティングに利用できる、唯一のアクセス回線インターフェイス テクノロジーです。
- IPv6 サポートは限定的に拡張され、PE-CE ルーティング プロトコルとして eBGP のみをサポートします。
- IPv6 アドレスの範囲は接続回線リンク間に限られているので、LSP の終端は両側とも IPv6 または IPv4 のいずれかであり、一方が IPv6 で他方が IPv4、あるいはその逆になることはありません。
- IPv6 サポートでは、グローバル ユニキャスト IPv6 アドレスだけを使用する PE-CE リンク コンフィギュレーションをトラブルシューティングできます。
- IPv6 サポートでは、IPv4 ルータ ID は、BGP や LDP などのプロトコル向けにピア ルータを識別するために使用されます。
- IPv4 の場合と異なり、（適用可能なテスト タイプの）CE アクセス回線インターフェイス IP アドレスは自動的に入力されません。これは、IPv6 アンナンバードが IOS XR デバイスでサポートされておらず、IPv6 には /30 および /31 アドレスの概念がないためです。
- 次の障害シナリオは IOS XR には適用されますが、これらの検証は最初のデータ検証で行われるので、IPv6 のコンテキストには適用されません。この障害シナリオは、CE アクセス回線インターフェイス IP アドレスがネットワーク アドレスであることを報告するためのもので、最初のデータ検証で実行されます。IPv6 にブロードキャスト アドレスの概念はありません。
  - ブロードキャスト アドレス
  - ネットワーク アドレス

観察結果

観察結果とは、接続上の問題に発展する可能性のある状況です。Diagnostics は接続問題の原因を 1 つのカテゴリとして判断できないため、これらの状況は観察結果として報告されます。

詳細については、mpls-diagnostics-expert@cisco.com まで電子メールでお問い合わせください。

PE に ACL が設定されている

プロバイダー エッジ（PE）ルータにアクセス コントロール リスト（ACL）が設定されています。ACL は、この PE からリモート PE への VPN Routing/Forwarding instance（VRF; VPN ルーティング/転送インスタンス）ping が失敗する原因となります。ただしシスコでは、ACL の使用状況を確認するための分析は行っていません。ACL が原因で、PE からローカル カスタマー エッジ（CE）ルータまたはカスタマー デバイスへの接続に障害が発生することはありません。

BGP ネイバー セッションの問題

ボーダー ゲートウェイ プロトコル（BGP）ネイバー セッションで問題が検出されました。[BGP Neighbor]（ネイバー IP アドレス）および [BGP State]（BGP ネイバーの状態）カラムがある表が表示されます。

BGP ルータ ID がループバック インターフェイスでない

PE のローカル BGP ルータ ID がループバック インターフェイスに割り当てられていません。重複の可能性を減らすため、および安定性を高めるために、ルータ ID はループバック インターフェイスから取得することを推奨します。

接続ルートが MP-BGP に再配布されていない

直接接続されたルートは、MP-BGP に再配布されない場合があります。

コアのトラブルシューティングを実行できない。VPN ルートが外部ルートである。

コアのトラブルシューティングを実行できませんでした。PE <*PE Name*> が VRF <*VRF name*> 内のリモート プレフィックス <*IP address*> への有効な VPN ルートを保持していないため、Diagnostics はテスト対象のラベルスイッチド パス（LSP）を特定できません。このルートは、内部のボーダー ゲートウェイ プロトコル（BGP）VPNv4 ネイバーからは特定できません。<*Routing Protocol Name*> から判断できます。この外部ルートのネクスト ホップは <*IP address*> です。トラフィックは、予測どおりに MPLS コアを通過しません。これは意図的なバック ドア リンクの可能性もありますが、多くの場合、PE と CE 間のルーティングミスの症状を示しています。LSP 接続をテストするには、PE から PE コアへのテストを実行します。このテストでは、LSP エンドポイントを手動で指定できます。

コアのトラブルシューティングを実行できない。VPN ルートが外部ルートで、ネクスト ホップにアクセスできない。

コアのトラブルシューティングを実行できませんでした。PE <*PE Name*> が VRF <*IP address*> 内のリモート プレフィックス <*IP address*> への有効なバーチャル プライベート ネットワーク（VPN）ルートを保持していないため、Diagnostics はテスト対象の LSP を特定できません。このルートは、内部の BGP VPNv4 ネイバーからは特定できません。<*Routing Protocol Name*> から判断できます。この外部ルートのネクスト ホップにはアクセスできません。これは意図的なバック ドア リンクの可能性もありますが、多くの場合、PE と CE 間のルーティングミスの症状を示しています。LSP 接続をテストするには、PE から PE コアへのテストを実行します。このテストでは、LSP エンドポイントを手動で指定できます。

コアのトラブルシューティングを実行できない。VPN ルートのネクスト ホップにアクセスできない。

コアのトラブルシューティングを実行できませんでした。PE <*PE Name*> が VRF <*VRF name*> 内のリモート プレフィックス <*IP address*> への有効な VPN ルートを保持していないため、Diagnostics はテスト対象の LSP を特定できません。ネクスト ホップにアクセスできません。原因として、コアの Interior Gateway Protocol（IGP）または IP 接続の障害が考えられます。LSP 接続をテストするには、PE から PE コアへのテストを実行します。このテストでは、LSP エンドポイントを手動で指定できます。

BGP ルータ ID の重複

リストされているデバイスの 1 つまたは複数のインターフェイス上で、PE の BGP ルータ ID が重複しています。

eBGP 最大プレフィックス

PE と eBGP ネイバー間の exterior Border Gateway Protocol（eBGP; 外部ボーダー ゲートウェイ プロトコル）セッションの最大プレフィックス数が PE に設定されています。このネイバーからの VRF には、現在 *X* 個のプレフィックスがあります。

eBGP ネイバーが確立されていない

PE と CE 間のルーティング プロトコルとして eBGP が実行されているようです。PE および CE インターフェイスは異なるサブネット上にあり、この PE には CE へのルートがありません。CE へのルートが確定するまで、この eBGP セッションは確立されません。

eBGP ネイバーが確立されていない

eBGP ネイバーは VRF 内で指定されていますが、確立されていないため到達不能です。

EIGRP ピア関係が確立されていない

PE インターフェイスは IP アンナンバードを使用して設定されています。Enhanced Interior Gateway Routing Protocol（EIGRP）でピア関係が確立されるには、CE インターフェイスも IP アンナンバードを使用するか、PE インターフェイスと同じサブネット上に存在する必要があります。

フルメッシュ VPN トポロジ

これらのルータは、フルメッシュ VPN コンフィギュレーションを使用して接続されているようです。これが正しくない場合、ルート ターゲット コンフィギュレーションに問題が生じます。

ハブ アンド スポーク VPN トポロジ

これらのルータは、ハブ アンド スポーク VPN コンフィギュレーションを使用して接続されているようです。これが正しくない場合、ルート ターゲット コンフィギュレーションに問題が生じます。

ハブ間およびハブ アンド スポーク VPN トポロジ

これらのルータは、ハブ間およびハブ アンド スポーク VPN コンフィギュレーションを使用して接続されているようです。これが正しくない場合、ルート ターゲット コンフィギュレーションに問題が生じます。

不完全な CEF 隣接

アクセス回線インターフェイス上の Cisco Express Forwarding（CEF; シスコ エクスプレス フォワーディング）隣接が不完全です。

不正なマルチリンク仮想アクセス インターフェイスが指定されている

PE にマルチリンク仮想アクセス回線インターフェイスを指定する場合は、指定する仮想アクセス インターフェイスがアクティブなマルチリンク バンドル インターフェイスであり、アクティブなバンドル リンクを保持していることを確認してください。

VLAN にインターフェイスがない

警告：イーサネット アクセス回線インターフェイスに仮想 LAN（VLAN）が関連付けられていません。

断続的な ping の成功

ping で断続的な接続のみが表示されました。

FR インターフェイスでインバース ARP がディセーブル

フレーム リレー インターフェイスは動的に設定されていますが、インバース アドレス解決プロトコル（ARP）が明示的にディセーブルになっています。

FR インターフェイスでインバース ARP が暗黙的にディセーブル

インターフェイス上にフレーム リレー スタティック マップがあります。このインターフェイスは動的に設定されますが、スタティック マップが存在するため、その副作用としてインバース ARP がディセーブルになります。

フレーム リレー インターフェイス上で LMI がディセーブル

警告：ローカル管理インターフェイス（LMI）がディセーブルになっているため、フレームリレー相手先固定接続（PVC）のステータスを確認できません。

LSP エンドポイントがループバック インターフェイスでない

VPNv4 ルートが IBGP ネイバーに送信されています。ただしネクスト ホップ アドレスは、直接接続された物理インターフェイスのうちの 1 つです。VPNv4 IBGP ネイバーのネクスト ホップにはループバック インターフェイスを使用することを推奨します。IGP 経由の正しいホップでこのアドレスを使用できない場合は、転送ラベル情報を入手できないので、VPN サイト間の接続は中断されます。

IOS XR ルータで MPLS OAM パッケージがイネーブルでない

IOS XR ルータで MPLS OAM パッケージがイネーブルになっていません。

IOS XR ルータで MPLS TE パッケージがイネーブルでない

IOS XR ルータで MPLS TE パッケージがイネーブルになっていません。

複数の等コスト パス

Equal Cost Multiple Path（ECMP; 等コスト マルチ パス）が検出されました。

PE ルータの IOS バージョンが不適合

プロバイダー エッジ（PE）ルータが MPLS OAM に適合しない Cisco IOS バージョンを実行しているため、コアのトラブルシューティングを実行できませんでした。

eBGP からルートを受信していない

PE と CE 間のルーティング プロトコルとして eBGP が実行されているようです。ただし、ネイバーからはルートを受信していません。

eBGP からリモート プレフィックスへのルートを受信していない

PE と CE 間のルーティング プロトコルとして eBGP が実行されているようです。ただし、ネイバーからはリモート プレフィックスへのルートを受信していません。PE とカスタマー エッジ（CE）の BGP コンフィギュレーションを確認してください。

VRF にプレフィックスの VPN ラベルがない

デバイスの VPN Routing/Forwarding（VRF; VPN ルーティング / 転送）のアドレスに、バーチャル プライベート ネットワーク（VPN）ラベルが見つかりませんでした。

OSPF ピア関係が確立されていない

PE インターフェイスは IP アンナンバードを使用して設定されています。Open Shortest Path First（OSPF）でピア関係が確立されるには、CE インターフェイスも IP アンナンバードを使用するか、PE インターフェイスと同じサブネット上に存在する必要があります。

PE と PE コア間でテストのみが実行され、オプションのループバック IP アドレス パラメータが入力されていない

テストされた LSP は、リモート サイト PE の BGP ルータ ID に基づいて選択されました。2 つの PE 間に複数の LSP がある場合、報告された結果はカスタマー トラフィックに使用された LSP の状態を正確に反映していない可能性があります。正しい LSP をテストするには、テストの入力ウィンドウで LSP エンドポイントを入力します。

バックアップ リンクの可能性

PE から送信プレフィックスへの ping は成功しましたが、想定していた PE インターフェイスを介して PE から送信プレフィックスへのルートを特定できませんでした。バックアップ リンクが動作中であるか、間違ったパラメータを入力した可能性があります。

ブロッキング ルート マップの可能性

PE にルート マップが設定されており、ルート トラフィックが失われる原因になっています。内部/外部 VPN コンフィギュレーションの場合は、ルート マップ コンフィギュレーション エラーの可能性があります。

コア IP 障害の可能性

ローカル PE からリモート PE に発行されたインターネット制御メッセージ プロトコル（ICMP）ping が失敗しました。ローカル PE の Interior Gateway Protocol（IGP）ルート テーブルに、リモート PE へのルートがありません。これらのデバイス間の IP 接続をトラブルシューティングしてください。

イーサネット デュプレックスの不一致の可能性

警告：アクセス回線インターフェイスにレイト コリジョンが発生しました。原因として、イーサネット デュプレックスの不一致が考えられます。

ルート制限に到達

デバイスのルート数がルート制限に達しました。

traceroute が送信されない

MPLS traceroute が送信されませんでした。

この章では、Cisco Prime Provisioning 6.3 リリースの Diagnostics アプリケーションでのトラブルシューティング ワークフローで実行される IOS および IOS XR コマンドの詳細を説明します。

IOS コマンド

この項では、Diagnostics で使用される IOS コマンドを示します。TACACS+（またはその他の認証/認可システム）を使用する場合は、これらすべてのコマンドが Diagnostics に対して許可されていることを確認してください。

（注）　このリストは、Diagnostics リリースまたはパッチが入手可能になると更新されます。最新のリストについては、mpls-diagnostics-expert@cisco.com まで E メールでお問い合わせください。

1. attach <*slot*> show version
2. execute-on slot <*slot*> 'show mpls forwarding-table <*destinationPrefix*> <*subnetMask*>'
3. execute-on slot <*slot*> 'show mpls forwarding-table <*destinationPrefix*>'
4. execute-on slot <*slot*> 'show mpls forwarding-table vrf <*vrfName*> <*destinationPrefix*> <*subnetMask*>'
5. execute-on slot <*slot*> 'show mpls forwarding-table vrf <*vrfName*> <*destinationPrefix*>'
6. execute-on slot <*slot*> 'show mpls forwarding-table vrf <*vrfName*>'
7. execute-on slot <*slot*> 'show mpls forwarding-table'
8. execute-on slot <*slot*> show ip cef vrf <*vrfName*> <*networkPrefix*>
9. execute-on slot <*slot*> show ip cef vrf <*vrfName*> <*networkPrefix*> <*subnetMask*>
10. execute-on slot <*slot*> show version
11. ping（対話型）
12. ping <*targetIp*>

13. ping mpls ipv4 <*targetIp*>/<*targetIpSubnetMask*> source <*source*> sweep <*minSweepSize*> <*maxSweepSize*> <*sweepInterval*> <*repeatCount*> timeout <*timeout*> replyMode <*replyMode*>
14. ping mpls traffic-eng Tunnel <*tunnelNumber*>
15. ping vrf <*vrfName*>（対話型）
16. show access-lists <*listName*>
17. show atm map
18. show atm pvc <*interface*>
19. show cef drop
20. show cef drop | include ^<*slot*>
21. show frame-relay lmi
22. show frame-relay lmi interface <*interface*>
23. show frame-relay map
24. show frame-relay pvc <*interface*> dlci <*dlci*>
25. show interfaces <*interface*>
26. show ip bgp summary
27. show ip bgp vpnv4 <*vrfName*> rib-failure
28. show ip bgp vpnv4 all neighbors
29. show ip bgp vpnv4 all neighbors <*destIp*>
30. show ip bgp vpnv4 all | include local router
31. show ip bgp vpnv4 vrf <*vrfName*> <*networkPrefix*>
32. show ip bgp vpnv4 vrf <*vrfName*> neighbors <*destIp*>
33. show ip bgp vpnv4 vrf <*vrfName*> <*prefix*> <*subnetMask*>
34. show ip bgp vpnv4 vrf <*vrfName*> labels | include <*networkPrefix*>/<*subnetMask*> | [0-9]+\.[0-9]+\.[0-9]+\.[0-9]+
35. show ip bgp vpnv4 vrf <*vrfName*> labels | include <*classfulPrefix*>
36. show ip bgp vpnv4 vrf <*vrfName*> labels | include <*networkPrefix*>/<*subnetMask*>
37. show ip cef <*destinationPrefix*>
38. show ip cef summary
39. show ip cef vrf <*vrfName*> <*networkPrefix*> <*subnetMask*> detail
40. show ip cef vrf <*vrfName*> <*networkPrefix*> detail
41. show ip cef vrf <*vrfName*> adjacency <*interface*> <*destip*> detail
42. show ip eigrp <*vrfName*> interfaces <*vrfInterface*>
43. show ip interface <*interface*>
44. show ip interface <*interface*> | include access list is
45. show ip interface brief <*interface*>
46. show ip interface brief | include <*ip-address*>
47. show ip ospf <*processId*> <*area*> interface <*intName*>
48. show ip ospf mpls traffic-eng link

49. show ip protocols <*vrfName*>
50. show ip route <*targetIp*>
51. show ip route vrf <*vrfName*> <*targetIp*>
52. show ip traffic
53. show ip vrf detail <*vrfName*>
54. show ip vrf interfaces <*vrfName*>
55. show mpls forwarding-table <*destinationPrefix*>
56. show mpls forwarding-table <*destinationPrefix*> <*subnetMask*>
57. show mpls forwarding-table <*destinationPrefix*> detail
58. show mpls forwarding-table labels <*label*>
59. show mpls forwarding-table labels <*label*> detail
60. show mpls forwarding-table vrf <*vrfName*>
61. show mpls forwarding-table vrf <*vrfName*> <*destinationPrefix*>
62. show mpls forwarding-table
63. show mpls interfaces <*interface*>
64. show mpls interfaces all
65. show mpls ip binding <*destinationPrefix*> <*destinationMask*>
66. show mpls ip binding local
67. show mpls ip binding summary
68. show mpls label range
69. show mpls ldp bindings <*ip*> <*subnetMask*>
70. show mpls ldp bindings neighbor <*neighbor ip*> <*subnetMask*>
71. show mpls ldp discovery
72. show mpls ldp neighbor
73. show mpls ldp neighbor <*interface*>
74. show mpls traffic-eng tunnels
75. show mpls traffic-eng tunnels <*status*>
76. show mpls traffic-eng tunnels <*tunnelId*>
77. show mpls traffic-eng tunnels destination <*destination*> <*status*>
78. show mpls traffic-eng tunnels destination <*destination*>
79. show mpls traffic-eng tunnels role <*role*>
80. show mpls traffic-eng tunnels role <*role*> <*status*>
81. show mpls traffic-eng tunnels role <*role*> destination <*destination*> <*status*>
82. show mpls traffic-eng tunnels role <*role*> destination <*destination*> up
83. show mpls traffic-eng tunnels role head brief
84. show ppp multilink interface <*interface*>
85. show route-map <*mapName*>
86. show running-config

87. show running-config interface <*interface*>
88. show running-config interface <*interface*> | include frame-relay interface-dlci
89. show running-config interface <*interface*> | include map-group
90. show running-config interface <*interface*> | include no frame-relay inverse-arp
91. show running-config | begin router bgp
92. show running-config | include advertise-
93. show running-config | include ldp password
94. show running-config | include mpls label protocol
95. show running-config | include no
96. show version
97. show vlans
98. traceroute mpls ipv4 <*ipAddress*>/<*subnetMask*> source <*source*> destination <*destination*> ttl 15
99. traceroute mpls traffic-eng Tunnel <*tunnelNumber*>
100. traceroute vrf <*vrfName*>（対話型）

IOS XR コマンド

この項では、Diagnostics で使用される IOS XR コマンドを示します。TACACS+（またはその他の認証/認可システム）を使用する場合は、これらすべてのコマンドが Diagnostics に対して許可されていることを確認してください。

（注）　このリストは、Diagnostics リリースまたはパッチが入手可能になると更新されます。最新のリストについては、mpls-diagnostics-expert@cisco.com まで E メールでお問い合わせください。

1. ping <*targetIp*>
2. ping atm interface <*interface*> <*vpi*>/<*vci*>
3. ping atm interface <*interface*> <*vpi*>/<*vci*> end-loopback
4. ping atm interface <*interface*> <*vpi*>/<*vci*> seg-loopback
5. ping mpls ipv4 <*destination*>/<*subnetMask*>
6. ping mpls ipv4 <*destination*>/<*subnetMask*> reply mode router-alert
7. ping mpls ipv4 <*destination*>/<*subnetMask*> source <*source*>
8. ping mpls traffic-eng Tunnel <*tunnelId*>
9. ping vrf <*vrfName*>
10. ping vrf <*vrfName*> <*targetIp*> <*sourceInterface*> <*minSweepSize*> <*maxSweepSize*> <*sweepInterval*>
11. show access-lists ipv4 <*listName*>
12. show bgp ipv4 all summary
13. show bgp vpnv4 unicast neighbors
14. show bgp vpnv4 unicast summary

15. 14.show bgp vpnv4 unicast vrf <*vrfName*> <*networkPrefix*>
16. show bgp vpnv4 unicast vrf <*vrfName*> <*prefix*> <*mask*>
17. show bgp vpnv4 unicast vrf <*vrfName*> labels
18. show bgp vrf <*vrfName*> advertised neighbor <*neighboreId*> summary | include <*ceDeviceIpAddr*>
19. show bgp vrf <*vrfName*> ipv4 unicast
20. show bgp vrf <*vrfName*> neighbors
21. show bgp vrf <*vrfName*> vpnv4 unicast neighbors
22. show cef ipv4 <*destinationPrefix*>
23. show cef ipv4 drops
24. show cef ipv4 drops location <*slot*>
25. show cef ipv4 summary
26. show cef vrf <*vrfName*> ipv4 <*networkPrefix*> detail
27. show cef vrf <*vrfName*> ipv4 <*networkPrefix*> <*subnetMask*> detail
28. show cef vrf <*vrfName*> <*networkPrefix*> <*subnetMask*> location <*location*>
29. show eigrp <*vrfName*> interfaces <*vrfInterface*>
30. show frame-relay lmi
31. show frame-relay lmi interface <*interface*>
32. show install active summary
33. show install inactive summary
34. show install location <*slot*>
35. show interfaces <*interface*>
36. show ip cef vrf <*vrfName*> adjacency <*interface*> <*destip*> detail
37. show ip ospf <*processId*> <*area*> interface <*intName*>
38. show ipv4 interface <*interface*>
39. show ipv4 interface brief <*interface*>
40. show ipv4 interface brief | include <*ip-address*>
41. show ipv4 traffic
42. show ipv4 vrf <*vrfName*> interface brief
43. show ipv4 vrf <*vrfName*> interface <*interface*>
44. show ipv4 vrf all interface brief
45. show mpls forwarding
46. show mpls forwarding labels <*label*>
47. show mpls forwarding prefix <*destinationPrefix*>/<*subnetMask*>
48. show mpls forwarding prefix <*destinationPrefix*>/<*subnetMask*> detail
49. show mpls forwarding vrf <*vrf*>
50. show mpls forwarding vrf <*vrf*> prefix <*destinationPrefix*>/<*subnetMask*>

51. show mpls forwarding vrf <*vrfName*> prefix <*destinationPrefix*>/<*subnetMask*> labels <*label*> location <*location*>
52. show mpls forwarding vrf <*vrfName*> prefix <*destinationPrefix*>/<*subnetMask*> location <*location*>
53. show mpls interfaces
54. show mpls interfaces <*interface*>
55. show mpls label range
56. show mpls label table summary
57. show mpls ldp bindings <*ip*> <*mask*>
58. show mpls ldp bindings neighbor <*neighbor*> <*ip*> <*mask*>
59. show mpls ldp discovery
60. show mpls ldp neighbor
61. show mpls ldp neighbor <*interface*>
62. show mpls traffic-eng tunnels
63. show mpls traffic-eng tunnels backup <*tunnelId*>
64. show mpls traffic-eng tunnels brief role head
65. show mpls traffic-eng tunnels <*status*> detail
66. show mpls traffic-eng tunnels <*tunnel-id*>
67. show mpls traffic-eng tunnels <*tunnelNumber*> detail
68. show mpls traffic-eng tunnels destination <*destination*>
69. show mpls traffic-eng tunnels name <*name*>
70. show mpls traffic-eng tunnels destination <*destination*> <*status*> detail
71. show mpls traffic-eng tunnels destination <*destination*> detail
72. show mpls traffic-eng tunnels detail
73. show mpls traffic-eng tunnels role <*role*> <*status*> detail
74. show mpls traffic-eng tunnels role <*role*> destination <*destination*> <*status*> detail
75. show mpls traffic-eng tunnels role <*role*> destination <*destination*> up detail
76. show mpls traffic-eng tunnels role <*role*> detail
77. show ospf
78. show ospf vrf <*vrf*>
79. show ospf border-routers | include ABR
80. show ospf | include ID
81. show ospf mpls traffic-eng link
82. show ospf vrf <*vrfName*> interface brief
83. show ospf vrf <*vrfName*> interface <*interfaceName*>
84. show protocols | include OSPF
85. show rib ipv4 tables
86. show rib vrf <*vrf*> ipv4 unicast statistics <*protocolName*>

87. show rib vrf <*vrf*> protocols
88. show rip vrf <*vrf*>
89. show route ipv4 <*targetIp*>
90. show route vrf <*vrfName*> ipv4 <*targetIp*>
91. show rpl route-policy <*mapName*>
92. show rsvp neighbors
93. show running-config
94. show running-config explicit-path name <*explicitPathName*>
95. show running-config interface <*interface*>
96. show running-config mpls ldp
97. show running-config mpls ldp label advertise
98. show running-config mpls traffic-eng
99. show running-config router bgp
100. show running-config router bgp <*asNumber*> vrf <*vrfName*> neighbor <*neighborIpAddr*>
101. show running-config router bgp <*asNumber*> neighbor-group <*neighborGroupName*>
102. show running-config router bgp | include redistribute <*protocol*>
103. show running-config router ospf
104. show running-config router <*protocol ID*> vrf <*vrf*>
105. show running-config rsvp interface <*interface-name*>
106. show vlan interface
107. show version
108. show vrf <*vrfName*> ipv4 detail
109. traceroute mpls ipv4 <*destination*>/<*subnetMask*>
110. traceroute mpls traffic-eng Tunnel <*tunnelId*>
111. traceroute vrf <*vrf*>
112. ping vrf <*vrfName*> <*targetIpv6Address*> <*sourceInterface*> <*minSweepSize*> <*maxSweepSize*> <*sweepInterval*>
113. show bgp vpnv6 unicast neighbors
114. show bgp vpnv6 unicast neighbors <*destIp*>
115. show bgp vpnv6 unicast vrf <*vrfName*> <*networkPrefix*>
116. show bgp vpnv6 unicast vrf <*vrfName*> <*networkPrefix*>/<*subnetMask*>
117. show bgp vpnv6 unicast vrf <*vrfName*> labels | include <*networkPrefix*>/<*subnetMask*>| [0-9A-Fa-f:]+[0-9A-Fa-f]*
118. show bgp vpnv6 unicast summary | include BGP router identifier
119. show bgp vrf <*vrfName*> ipv6 unicast
120. show bgp vrf <*vrfName*> ipv6 unicast advertised neighbor <*neighborId*> summary | include <*ceDeviceIpAddr*>
121. show cef ipv6 summary

122.show cef vrf <*vrfName*> ipv6 <*networkPrefix*> detail

123.show cef vrf <*vrfName*> ipv6 <*networkPrefix*>/<*subnetMask*> detail

124.show cef vrf <*vrfName*> ipv6 <*networkPrefix*> location <*location*>

125.show cef vrf <*vrfName*> ipv6 <*networkPrefix*>/<*subnetMask*> location <*location*>

126.show ipv6 interface <*interface*>

127.show ipv6 interface brief <*interface*>

128.show ipv6 vrf all interface brief

129.show ipv6 vrf <*vrfName*> interface brief

130.show ipv6 vrf <*vrfName*> interface <*interface*>

131.show rib ipv6 tables

132.show route ipv6 <*targetIp*>

133.show route vrf <*vrfName*> ipv6 <*targetIp*>

134.show vrf <*vrfName*> ipv6 detail