HP OpenView Reporting and Network Solutions

Network Node Manager 用
MPLS VPN Smart Plug-in

バージョン : 2.1

ユーザーガイド

HP-UX、Solaris、および Windows® 用

Manufacturing Part Number : None

2004 年 7 月

ご注意

1. 本書に記載した内容は、予告なしに変更することがあります。
2. 当社は、本書に関して特定目的の市場性と適合性に対する保証を含む一切の保証をいたしかねます。
3. 当社は、本書の記載事項の誤り、またはマテリアルの提供、性能、使用により発生した損害については責任を負いかねますのでご了承ください。
4. 本製品パッケージとして提供した本書、CD-ROM などの媒体は本製品用だけにお使いください。プログラムをコピーする場合はバックアップ用だけにしてください。プログラムをそのままの形で、あるいは変更を加えて第三者に販売することは固く禁じられています。

原 典

本書は『*HP OpenView Reporting and Network Solutions MPLS VPN Smart Plug-in to Network Node Manager User's Guide*』(HP Part No. None) を翻訳したものです。

目次

目次

サポート情報

次の HP OpenView の Web サイトにアクセスしてください。

http://support.openview.hp.com/support.jsp?lang=JAPAN

ここには、HP OpenView のお問い合わせ先、製品およびサポートの情報が掲載されています。

HP OpenView サポート Web サイトに直接アクセスすることもできます。

http://support.openview.hp.com/

サポートサイトには次の情報が掲載されています。

- 文書のダウンロード
- トラブルシューティング情報
- パッチと更新
- 障害情報
- トレーニング情報
- サポートプログラム情報

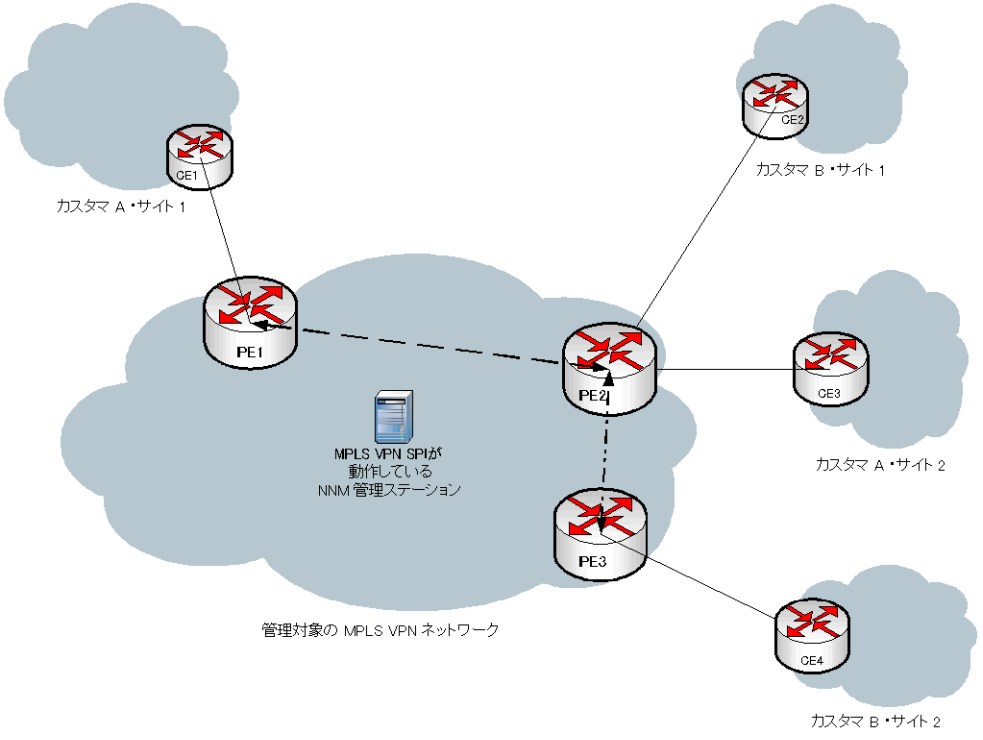
1 MPLS VPN Smart Plug-in の概要

はじめに

IP ネットワークのバックボーンを持つインターネットサービスプロバイダの中には、RFC2547bis で規定されるマルチプロトコルラベルスイッチング (MPLS) を使って仮想プライベートネットワーク (VPN) サービスを提供しているところがあります。カスタマのネットワーク内の 2 つのサイトは、その両サイトを包含する VPN が存在する場合のみ、共通のバックボーンを通して IP 接続することができ、両サイトに共通の VPN が存在しない場合は、バックボーンを通して接続できません。

MPLS を使った VPN (MPLS VPN) は、サービスプロバイダ側ネットワークの周縁にあるルーター (エッジルーター) 上の仮想ルーティング / 転送テーブル (VRF) によって定義されます。1 つの VRF は、1 つ以上のルーターでサポートされる 1 つの VPN のインスタンスを表します。すべてのネットワークデバイスから一致する VRF だけを集めると、実際の VPN になります。図 1-1 に、MPLS VPN ネットワークの例を示します。

図 1-1　　MPLS VPN ネットワークの例



HP OpenView Network Node Manager Smart Plug-in (SPI) for MPLS VPN (MPLS VPN SPI) は、HP OpenView Network Node Manager (NNM) の機能を強化するための製品で、MPLS VPN のエッジルーターをほぼリアルタイムで監視する機能を備えています。サービスプロバイダ側ネットワークの周縁部には、プロバイダエッジ (PE) ルーターがあります。この PE ルーターが仲介となって、一方では MPLS VPN 内のプロバイダ (P) ルーターと通信し、もう一方では、カスタマの管理するカスタマエッジ (CE) ルーターと通信します。MPLS VPN SPI は、MPLS ネットワークの中心で VPN を構成する PE ルーター間の接続を監視して、VPN のネットワークトポロジを把握します。また、この情報を使って、物理的なノード、PE インタフェース、および関連トラップの関係を整理し、VPN サービスに影響するイベントを生成します。

MPLS VPN SPI は、イベント情報追加機能 (イベント間の関係を認識して、イベントに含まれるデータを追加するプロセス) を使って、個々のイベントと同等以上の情報量をもつ、より少数の新しいイベントを生成します。管理者はこの集約されたイベントを見ることになるので、ネットワーク上の問題を効率よく把握して対応することができます。その結果、問題に対する対応が早くなって、MPLS VPN ネットワークで発生する問題の平均復旧時間 (MTTR) が短くなり、サービスの品質が向上します。

MPLS VPN SPI がサポートしているエッジルーターデバイスのリストは、25 ページの「ルーターの要件」を参照してください。

また MPLS VPN SPI には、基盤となる PE ルーターおよび CE ルーターの問題をほぼリアルタイムで診断する機能に加え、VPN 内の 2 つの PE ルーター間でエンドツーエンドの通信が可能かどうかを監視する機能もあります。この監視機能は、Cisco RTTMON MIB に基づくシスコサービス保証エージェント (CSAA。本書ではこれ以降、SAA という略語を使います) のテスト機能を使って実現されています。MPLS VPN SPI は、PE ルーター間に SAA エコーテストを設定して、エッジルーター間の到達可能性をテストします。このテストによって、PE-PE 間の接続をリアルタイムに監視して、障害発生時に SNMP イベントを生成できるようになっています。また、MPLS VPN SPI では、2 つの CE 間のエンドツーエンドの到達可能性テストを、ユーザーが設定することもできます。

HP OpenView Performance Insight (OVPI) を NNM と組み合わせれば、MPLS VPN SPI は NNM および OVPI と連携し、障害データと性能データの両方を解析してレポートを作成できるにようになります。

MPLS VPN SPI の機能と特長

MPLS VPN SPI には、次の機能と特長があります。

- MPLS VPN SPI は、MPLS VPN ネットワーク内に存在する PE ルーターのステータスを監視し、デバイスの障害をレポートします。
- MPLS VPN SPI は、サービスプロバイダからアクセスできる各 CE ルーターについて、CE ルーター自体のステータスと PE-CE 間の接続ステータスを監視します。
- MPLS VPN SPI は、ネットワークステータスイベントに情報を追加することにより、より分かりやすいイベントを新規に生成して NNM アラームブラウザに表示します。
- MPLS VPN SPI は、VPN 内の有効な PE-PE ルーターペアを把握し、そのペア間の到達可能性テストを自動的に設定します (オプション機能)。
- MPLS VPN SPI を使って、PE および CE 固有の様々な種類の到達可能性テストを個別に設定し、テスト対象の接続に変化があったことを示すイベントを生成させることができます。
- OVPI をインストールした場合、キャリアアクセスレート、CSAA、および MPLS VPN のカウンターを監視し、カウンターがしきい値 (設定可) を超えたときに NNM へトラップを送信させることができます。このトラップは NNM アラームブラウザにアラームとして表示されるので、その表示から OVPI レポートを起動して、しきい値を超えたインタフェースの詳細情報を調べることができます。

MPLS VPN SPI の動作

MPLS VPN SPI は、MPLS VPN ネットワークで発生した問題を検出してレポートします。MPLS VPN SPI で検出・分析できるトラップとイベントの種類は次のとおりです。

- PE ルーターのノードステータスとインタフェースステータスの変化を知らせるトラップ
- CE ルーターのノードステータスとインタフェースステータスの変化を知らせるトラップ
- PE-PE、PE-CE、および CE-CE 間の到達可能性をテストするための SAA エコーテストイベント
- MPLS VPN、SAA、または CAR の監視パラメータがしきい値を超えたことを知らせる OVPI しきい値超過トラップ

MPLS VPN SPI はこれらのトラップに情報を追加して、VPN サービスに対する影響が把握できるようなイベントに変換します。このイベントによって、VPN サービス内で影響を受ける VRF を識別することができます。

MPLS VPN SPI とユーザーとの接点

ユーザーは、次の方法で MPLS VPN ネットワークの状態を監視できます。

- アラームカテゴリが MPLS VPN のアラームを監視して、VPN のステータスに影響を与えるような状況を観察する。14 ページの「MPLS VPN のイベント」を参照してください。
- MPLS VPN に関連したビューのウィンドウに表示されるグラフとテーブルで、MPLS VPN ネットワークの状況を調べる。16 ページの「MPLS VPN に関連したビュー」を参照してください。
- OVPI を相互起動して、MPLS VPN ネットワークの動作に関するレポートを作成する。この方法を使う場合は、OVPI と MPLS VPN Report Pack のインストールが必要です。16 ページの「OVPI からのレポート」を参照してください。

MPLS VPN のイベント

MPLS VPN SPI が生成するイベントは、NNM のアラームブラウザに MPLS VPN というカテゴリで表示されます。この MPLS VPN カテゴリをダブルクリックすると、MPLS VPN ブラウザが表示されます。

MPLS VPN に発生した障害を MPLS VPN SPI が 検出すると、次のいずれかのイベントメッセージが生成されます。

- MPLS/VPN: ノード [*node*] の IF [*interface*] が停止中のため、VPN:VRF [*VRF*] が停止中です。
- MPLS/VPN: ノード [*node*] が停止中のため、VPN:VRF [*VRFlist*] が停止中です。
- MPLS/VPN: カード [*card*] が停止中のため、VPN:VRF [*VRFlist*] が停止中です。
- MPLS/VPN: ノード [*node*] が認識不能なステータスのため、VPN:VRF [*VRFlist*] は認識不能なステータスです。
- MPLS/VPN: [*node1 - node2*] の SAA テストが失敗しました。影響を受ける VPN/VRF:[*VRFlist*]。根本原因 : *cause* 。
- MPLS/VPN: [*node1 - node2*] の SAA テストをクリアしました。影響を受ける VPN/VRF:[*VRFlist*]。
- MPLS/VPN: ノード [*node*] の [*interface*] アドレスが停止中のため、VPN:VRF [*VRF*] が停止中です。

- MPLS/VPN: [*source_node*:*interface*] と [*destination_node*:*interface*] の間の接続が停止中のため、VPN:VRF [*VRF*] が停止中です。

イベントメッセージの例を次に示します。

- MPLS/VPN: ノード [mplspe04.cnd.hp.com] の IF [Se0/0] が停止中のため、VPN:VRF [Red_: Red_West] が停止中です。
- MPLS/VPN: ノード [mplspe04.cnd.hp.com] が停止中のため、VPN:VRF [Red_: Red_West Blue:Blue] が停止中です。
- MPLS/VPN: カード [card1] が停止中のため、VPN:VRF [Red_: Red_West Blue:Blue] が停止中です。
- MPLS/VPN: [mplspe04.cnd.hp.com-mplspe01.cnd.hp.com] の SAA テストが失敗しました。影響を受ける VPN/VRF:[Red_:Red_West-Red_East]。根本原因 : Connectivity Failure between mplspe04.cnd.hp.com and mplspe01.cnd.hp.com.
- MPLS/VPN: ノード [mplspe04.cnd.hp.com] の [Se0/0] アドレスが停止中のため、VPN:VRF [Red_: Red_West] が停止中です。
- MPLS/VPN: [mplspe04.cnd.hp.com:Se0/0] と [mplspe01.cnd.hp.com:Se0/0] の間の接続が停止中のため、VPN:VRF [Red_: Red_West] が停止中です。
- MPLS/VPN: ノード [mplspe04.cnd.hp.com] が認識不能なステータスのため、VPN:VRF [Red_: Red_West] は認識不能なステータスです。

MPLS VPN アラームのメッセージフィールドには、発生した MPLS VPN 障害の特性が示されます。また、このフィールドには、それ以外に次の追加情報も含まれます。

- 障害の影響を受ける VPN 内で実際に影響を受ける VRF のリスト。インタフェースが停止した場合は、1 つの VRF にしか影響が出ませんが、ノードが停止した場合は、複数の VRF に影響が出ます。

  たとえば、メッセージフィールドの内容が [Red_: Red_West Blue:Blue] となっていれば、停止によって「Red_」VPN 内の「Red_West」VRF と「Blue」VPN 内の「Blue」VRF に影響が出ることを示しています。

- 停止しているエッジルーターのノード名。たとえば、[mplspe04.cnd.hp.com]。

  または、

  SAA 到達可能性テストの対象となるエッジルーターノードの名前。たとえば、[mplspe04.cnd.hp.com-mplspe01.cnd.hp.com]。

- エッジルーター上の停止しているインタフェースの名前。たとえば、[Se0/0]。

MPLS VPN に関連したビュー

MPLS VPN SPI には、次のビューがあります。

- MPLS VPN **ビュー** − MPLS VPN ネットワーク内に存在する VPN をリストで表示します。
- MPLS VPN **ルーターインベントリ** − MPLS VPN ネットワーク内に存在する MPLS VPN ルーターをリストで表示します。
- MPLS VPN **詳細ビュー** − 特定の VPN について、その中でアクセス可能なすべての PE ルーターと CE ルーターをグラフと表形式で表示します。
- PE **詳細ビュー** − 特定の PE ルーターで定義されている VRF の詳細情報を表示します。各 VRF に関係する VPN も示されます。
- VRF **詳細ビュー** − 特定の VRF 内の PE ルーターと CE ルーターの詳細情報を表示します。

それぞれのビューで使用可能な機能とビュー間のナビゲーション方法については、MPLS VPN SPI と共にインストールされるオンラインヘルプを参照してください。

MPLS VPN ビューに関連したビューの起動

MPLS VPN ビューに関連したビューは、次のいずれかの方法で起動できます。

- NNM GUI (ovw) で、[**ツール： ビュー** -> MPLS VPN] の順に選択する。
- ホームベースで、リストの中から [MPLS VPN **ビュー**] を選択し、[**起動**] をクリックする。
- 任意のビューで [**ツール： ビュー** -> MPLS VPN] の順に選択する。

OVPI からのレポート

OVPI サーバーに MPLS VPN と SAA Report Packs をインストールして、さらに NNM / OVPI Integration Module をインストールしてある場合は、何通りかの方法で、NNM の MPLS VPN 情報から OVPI を起動できます。以下に、その方法を説明します。

NNM アラームブラウザから OVPI を相互起動する

NNM アラームブラウザから次の手順で OVPI を起動できます。

1. MPLS VPN アラームブラウザ内でアラームを 1 つ選択し、[**アクション** -> **アクションの実行**] の順にクリックします。
2. [**アクション**] リストで [OVPI Report] をクリックします。
3. [OK] をクリックします。

   Web ブラウザのウィンドウが開き、アラーム発生元オブジェクトでフィルター処理された OVPI レポートが表示されます。

NNM GUI (ovw) から OVPI を相互起動する

NNM の GUI (ovw) から次の手順で OVPI を起動できます。

1. NNM マップで、MPLS ネットワークに存在するルーターのノードシンボルまたはインタフェースシンボルを選択し、[**アクション** -> **アクションの実行**] の順にクリックします。
2. [**アクション**] リストで [OVPI Report] をクリックします。
3. [OK] をクリックします。

   Web ブラウザのウィンドウが開き、そこに、[Report Launchpad] が表示されます。
4. [Report Launchpad] で、表示したいレポートをクリックします。

Extended Topology のマップから OVPI を相互起動する

Extended Topology のマップから次の手順で OVPI を 起動できます。

1. Extended Topology のマップで、MPLS VPN ネットワークに存在するルーターのノードシンボルを選択し [**アクション** -> **アクションの実行**] の順にクリックします。
2. [**アクション**] リストで [OVPI Report] をクリックします。
3. [OK] をクリックします。

   Web ブラウザのウィンドウが開き、そこに、[Report Launchpad] が表示されます。
4. [Report Launchpad] で、表示したいレポートをクリックします。

MPLS VPN ビューから OVPI を相互起動する

MPLS VPN ビューから次の手順で OVPI を 起動できます。

1. MPLS VPN ビューで、リストの中から [OVPI Report] を選択し、続いて [**起動**] をクリックします。

   Web ブラウザのウィンドウが開き、そこに [Report Launchpad] が表示されるので、表示したいレポートをクリックします。

関連マニュアル

詳細は、次のマニュアルを参照してください。

- 『*HP OpenView NNM ネットワーク管理ガイド*』
- 『*Extended Topology によるネットワーク管理ガイド*』
- 『*MPLS VPN Report Pack User Guide*』
- 『*SAA Report Pack User Guide*』

関連マニュアル

2 MPLS VPN Smart Plug-in のインストール

インストールの準備

MPLS VPN Smart Plug-in (SPI) をインストールする前に、以下に示すハードウェアの要件とソフトウェアの要件が満たされていることを確認します。また、必要なソフトウェアが正しく設定されていることも確認します。

ハードウェア要件

MPLS VPN SPI をインストールする前に、次のディスク空き容量が確保されていることを確認してください。

表 2-1 ディスクの推奨空き容量

場所	容量
UNIX の場合: `$OV_MAIN_PATH` *Windows の場合*: `%OV_MAIN_PATH%`	2 MB

ソフトウェア要件

サポートされているオペレーティングシステム

次のオペレーティングシステムがサポートされています。

- HP-UX 11.0 または HP-UX 11.11
- Solaris 2.8 または Solaris 2.9
- Microsoft® Windows® 2000 service pack 3、Windows® XP、または Windows® 2003

Network Node Manager

管理対象環境内のすべてのシステムに次のソフトウェアがインストールされていること、また、そのソフトウェアに必要な関連ソフトウェアとパッチがインストールされていることを確認してください。

- HP OpenView Network Node Manager Advanced Edition バージョン 7.5

NNM 製品のインストール方法は、『*HP OpenView ネットワークノードマネージャ インストールガイド*』を参照してください。

Network Node Manager Advanced Edition が正しくインストールされていることの確認

NNM Advanced Edition 製品がインストールされていることを、次の方法で確認してください。

UNIX の場合:

```
/usr/sbin/swlist | grep "OpenView Network Node Manager Extended Topology"
```

Windows の場合:

1. [**スタート**] メニューから、[**コントロールパネル**] を選択して開きます。
2. [**アプリケーションの追加と削除**] をダブルクリックします。
3. プログラムリストに HP OpenView Network Node Manager があることを確認します。

インストールされている NNM のバージョンの確認

インストールされている NNM のバージョンを、次のコマンドで確認してください。

UNIX の場合: **/opt/OV/bin/ovnnmversion**

Windows の場合: ***install_dir*¥bin¥ovnnmversion**

NNM の環境変数の設定

次のコマンドまたはバッチファイルを実行して、NNM の環境変数を設定してください。

- *UNIX で sh または ksh を使っている場合*: **. /opt/OV/bin/ov.envvars.sh**
- *UNIX で csh を使っている場合*: **source /opt/OV/bin/ov.envvars.csh**
- *Windows の場合*: コマンドウィンドウで、***install_dir*¥bin¥ov.envvars.bat** を実行

以上の手順により、MPLS VPN SPI に必要な次の環境変数が設定されます。

- *UNIX の場合*: $OV_BIN、$OV_LRF、$OV_CONF、$OV_MAIN_PATH
- *Windows の場合*: %OV_BIN%、%OV_LRF%、%OV_CONF%、%OV_MAIN_PATH%

MIB の要件

MPLS VPN SPI を正しく動作させるには、次の MIB を事前にロードしておく必要があります。

- Cisco SMI MIB － NNM に付属しており、次の場所にインストールされます。

  UNIX の場合: `$OV_SNMP_MIBS/Vendor/Cisco/CISCO-SMI.my`
  Windows の場合: `%OV_SNMP_MIBS%¥Vendor¥Cisco¥CISCO-SMI.my`

- Cisco RTTMON MIB － MPLS VPN SPI に付属しており、次の場所にインストールされます。

  UNIX の場合: `/opt/OV/newconfig/MPLS/CISCO-RTTMON-MIB.my`
  Windows の場合: `%OV_CONF%¥MPLS¥CISCO-RTTMON-MIB.my`

- Juniper SMI MIB － MPLS VPN SPI に付属しており、次の場所にインストールされます。

  UNIX の場合: `$OV_SNMP_MIBS/Vendor/Juniper/jnx-smi.mib`
  Windows の場合: `%OV_SNMP_MIBS%¥Vendor¥Juniper¥jnx-smi.mib`

- Juniper VPN MIB － MPLS VPN SPI に付属しており、次の場所にインストールされます。

  UNIX の場合: `$OV_SNMP_MIBS/Vendor/Juniper/jnx-vpn.mib`
  Windows の場合: `%OV_SNMP_MIBS%¥Vendor¥Juniper¥jnx-vpn.mib`

MPLS VPN SPI をインストールする前に Cisco SMI MIB がすでに NNM 管理ステーションへロードされている場合、その他に必要な MIB は自動的にロードされます。それ以外の場合は、必要な MIB をすべて手動でロードする必要があります。詳細は、77 ページの「MIB がロードされていることを確認する方法」を参照してください。

注記　Windows オペレーティングシステムの場合、NNM のインストールオプションとして [**標準**] を選択すると、Cisco SMI MIB はロードされません。[**カスタム**] インストールオプションを選択すれば、SNMP MIB をロードするように指定できます。また、77 ページの「MIB がロードされていることを確認する方法」の説明に従って MIB をロードすることも可能です。

ルーターの要件

MPLS VPN SPI の今回のリリースでは、以下の種類のルーターデバイスを検出、管理します。

- MplsVpnMIB をサポートしているバージョン 12.2(15)T の Internetwork Operating System (IOS) を備えた Cisco ルーター

  MPLS VPN SPI はこれらのデバイスについて、ステータスの管理、到達可能性テストの設定、および到達可能性ステータスの報告を行うことができます。

- jnx-smi.mib および jnx-vpn.mib をサポートする Juniper Operating System (JunOS) バージョン 6 を備えた Juniper M および T シリーズのルーター

  これらのデバイスについては、MPLS VPN SPI はステータスの管理のみを行うことができます。

Performance Insight

オプションで、別のサーバーに HP OpenView Performance Insight (OVPI) 5.0 をインストールし、NNM / OVPI Integration Module を使って、OVPI による傾向解析と NNM の障害管理機能を統合することができます。OVPI と NNM を統合すると、OVPI で検出されたしきい値の超過が NNM アラームブラウザに表示され、[Report Launchpad] ウィンドウから各種の OVPI レポートへアクセスできるようになります。

MPLS VPN SPI の旧バージョンからの SAA テスト定義のアップデート

旧バージョンの MPLS VPN SPI を使って SAA テストを定義している場合は、以下の手順を実行して、テストの設定を保存しておきます。

1. 次の手順を実行して、既存の SAA テストを管理対象ルーターから削除します。

   a. 既存の SAA テストをすべて、ファイルにエクスポートします。

      - *UNIX の場合*:

        $OV_BIN/saa_config.ovpl -e /tmp/saa_test_A

      - *Windows の場合*:

        %OV_BIN%¥saa_config.ovpl -e C:¥temp¥saa_test_A

      詳細は、65 ページの「SAA テストの定義変更方法」を参照してください。

   b. テキストエディターを使って、saa_test_A ファイルの中に定義されている各テストの OP パラメータを DELETE に変更します。

      詳細は、67 ページの「MPLS VPN SPI を使った SAA の設定」を参照してください。

   c. アップデートした SAA テストの定義を、次のようにして MPLS VPN SPI にインポートします。

      - *UNIX の場合*:

        $OV_BIN/saa_config.ovpl -i /tmp/saa_test_A

      - *Windows の場合*:

        %OV_BIN%¥saa_config.ovpl -i C:¥temp¥saa_test_A

      詳細は、65 ページの「SAA テストの定義変更方法」を参照してください。

   d. saa_test_A ファイルは後で参照するので、保存しておきます。

2. 次のコマンドを実行して、VpnNames.txt ファイルのバックアップを作成します。

   - *UNIX の場合*:

     cp $OV_CONF/VpnNames.txt /tmp/VpnNames-A.txt

   - *Windows の場合*:

     copy %OV_CONF%¥VpnNames.txt C:¥temp¥VpnNames-A.txt

3. 現在の MPLS VPN SPI を削除します。

   削除する方法は、35 ページの「MPLS VPN SPI の削除」を参照してください。

4. 最新バージョンの MPLS VPN SPI をインストールします。

   インストールの方法は、30 ページの「MPLS VPN SPI のインストール」を参照してください。

5. SAA テストのソースとなる各エッジルーターごとに、その SNMP Set 用コミュニティ文字列が NNM に設定されていることを確認します。

   確認の方法は、37 ページの「SNMP アクセスの設定」を参照してください。

6. Extended Topology の検出機能を起動してネットワークを検出させるとともに、MPLS VPN の検出を行わせます。特に指定しない限り、MPLS VPN SPI ではネットワーク内のすべての PE-PE の組み合わせに対して、VRF 非対応 SAA テストが設定されます。

   詳細は、40 ページの「検出処理」を参照してください。

7. 次の手順で新しい SAA テストの定義をアップデートし、以前の SAA テストの定義と整合させます

   a. 自動的に設定された SAA テストを、ファイルにエクスポートします。

      - *UNIX の場合*:

        $OV_BIN/saa_config.ovpl -e /tmp/saa_test_B

      - *Windows の場合*:

        %OV_BIN%¥saa_config.ovpl -e C:¥temp¥saa_test_B

      詳細は、65 ページの「SAA テストの定義変更方法」を参照してください。

注記　自動的に設定された SAA テストがなければ、saa_test_B ファイルは空になっています。その場合は、saa_test_A ファイルをそのまま使用して、手順 b と手順 c を実行します。

---

b. 必要に応じて、SAA テストの定義ファイルをアップデートします。

テキストエディターを使って、saa_test_B ファイルに定義されている SAA テストと saa_test_A ファイル (手順 1 で保存したもの) に定義されている SAA テストを比較します。

- saa_test_B ファイルの中に saa_test_A ファイルに定義されているテストと対応しているものがあれば、saa_test_B ファイル側に定義されているテストの定義を変更して、saa_test_A ファイル内の対応するテストと同じになるようにします。各テストの定義について、OP パラメータを MODIFY に変更します。
- saa_test_A ファイルにのみ定義されているテストがあれば、それを saa_test_B ファイルに追加します。追加したテストの定義について、OP パラメータを ADD に変更します。

注記　MPLS VPN SPI バージョン 2.0 以降では、バージョン 1.0 に比べてより多くの種類の SAA テストを行うことができます。また、SAA テストの識別に 16 進数が使われています。これらの変更点は新旧のテスト定義を比較すれば分かりますが、次に述べるように、ここでの作業には関係ありません。

- saa_test_B ファイルには、旧バージョンになかった要素として TEST_TYPE があります。ただし、この要素をバージョン 1.0 のテスト定義に追加する*必要はありません*。
- saa_test_A ファイルでは OV_TAG 要素が 10 進数で表されていますが、saa_test_B ファイルでは 16 進数で表されています。ただし、バージョン 1.0 のテスト定義でこのタグの値を変更する*必要はありません*。

詳細は、67 ページの「MPLS VPN SPI を使った SAA の設定」を参照してください。

c. アップデートした SAA テストの定義を次のコマンドで MPLS VPN SPI にインポートします。

- *UNIX の場合*:

  $OV_BIN/saa_config.ovpl -i /tmp/saa_test_B

- *Windows の場合*:

  %OV_BIN%¥saa_config.ovpl -i C:¥temp¥saa_test_B

詳細は、65 ページの「SAA テストの定義変更方法」を参照してください。

8. 次の手順を実行し、以前のバージョンで使っていた VPN の名前を新しいバージョンでもそのまま使うようにします。

a. バックアップファイル VpnNames-A.txt (手順 2 で作成) を次の新しい VPN 名ファイルと比較します。

- *UNIX の場合*: $OV_CONF/VpnNames.txt
- *Windows の場合*: %OV_CONF%¥VpnNames.txt

b. 必要に応じて VpnNames.txt ファイルを編集し、新しいバージョンで使う VPN 名が以前のバージョンと同じになるようにします。VPN 名のみを変更します。

詳細は、44 ページの「MPLS VPN SPI 設定ファイル内の VPN 名の変更」を参照してください。

MPLS VPN SPI のインストール

ここではインストール手順を説明します。問題が発生した場合は、71 ページの第 6 章 「MPLS VPN Smart Plug-in のトラブルシューティング」または『*Release Notes for MPLS VPN Smart Plug-in to Network Node Manager*』に解決方法が示されているので、参考にしてください。

重要 初めて MPLS VPN SPI をインストールする場合は、その前に NNM Extended Topology を有効にしてください。またその際の手順や指示などは、NNM Advanced Edition に付属している『*Extended Topology によるネットワーク管理ガイド*』を参照してください。

注記 旧版の MPLS VPN SPI を上書きして新しい MPLS VPN SPI をインストールする場合は、26 ページの「MPLS VPN SPI の旧バージョンからの SAA テスト定義のアップデート」に示されている手順と指示を参照してください。

UNIX オペレーティングシステム上に MPLS VPN SPI をインストールする方法

MPLS VPN SPI を UNIX® オペレーティングシステム上にインストールするには、次の手順を実行します。

1. NNM 管理ステーションにユーザー `root` でログオンします。
2. NNM の環境変数に正しい値が設定されていることを確認します。

   設定手順は、23 ページの「NNM の環境変数の設定」を参照してください。
3. NNM のデータウェアハウスに Oracle データベースを使用している場合は、次の手順を実行して MPLS VPN SPI 用に Oracle を設定します。

   a. **`cd $OV_CONF/nnmet/topology/extensibility`**

   b. **`cp UpdateColumn.xslt UpdateColumn.xslt.orig`**

   c. テキストエディターを使って `UpdateColumn.xslt` ファイルの 36 行目にある単語 `COLUMN` を削除します。
4. Reporting and Network Solutions CD-ROM をマウントします。

5. Reporting and Network Solutions CD-ROM のディレクトリから `setup` を起動します。

   インストールスクリプトが起動されて、ターゲットシステムにインストールされている NNM のバージョンが適切かどうかを調べます。NNM がインストールされていないと、インストールスクリプトはエラーで終了します。詳細は、81 ページの「その他の問題の対処方法」を参照してください。

6. 画面に表示される指示に従って、MPLS VPN SPI をインストールします。インストール処理の途中で表 2-2 に示す質問内容が表示されるので、適切な回答と指示を与えてください。

表 2-2　MPLS VPN SPI を UNIX へインストール中の選択項目

選択項目	説明
インストールする製品のリスト	NNM Smart Plug-in のインストールを選択します。
インストールする SPI のリスト	MPLS VPN SPI のインストールを選択します。
MPLS VPN の検出を開始するかどうか	インストールの最後に Extended Topology の検出 (MPLS VPN の検出も含む) を開始する場合は、**yes** と入力します。 インストールの最後に MPLS VPN ネットワークの検出を開始しない場合は、**no** と入力します。**no** と入力すると、次に Extended Topology の検出を行う時まで、MPLS VPN ネットワークは検出されません。40 ページの「検出処理」を参照してください。

表 2-2　MPLS VPN SPI を UNIX へインストール中の選択項目 (続き)

選択項目	説明
MPLS VPN の定期的な検出が終わるたびに SAA テストを設定するかどうか	MPLS VPN SPI が MPLS VPN の検出を終えた時に、SAA テストの定義を使って、すべての管理対象 PE ルーターに置かれている SAA MIB を自動的にアップデートするようにする場合は、**yes** と入力します。ただし、**yes** と入力する場合は、SNMP 設定データベースに各 PE ルーターの Set 用コミュニティ文字列が設定されていることを確認してください。36 ページの「初期設定」を参照してください。 SAA MIB を自動的にアップデートしない場合は、**no** と入力します。**no** と入力すると、コマンドで具体的に指示しない限り、MPLS VPN SPI は SAA MIB をアップデートしません。66 ページの「SAA の設定」を参照してください。 自動設定のオン / オフは変更できます。66 ページの「SAA 設定パラメータの設定方法」を参照してください。
SAA テストの周期	SAA テストの実行間隔を秒単位で指定します。デフォルト値は 600 秒 (10 分) です。 SAA テストの周期は変更できます。66 ページの「SAA 設定パラメータの設定方法」を参照してください。
SAA テストのタイムアウト	SAA テストが成功しない場合のタイムアウトの時間を、ミリ秒単位で指定します。デフォルト値は 100 ミリ秒です。 SAA テストのタイムアウト値は変更できます。66 ページの「SAA 設定パラメータの設定方法」を参照してください。

Windows オペレーティングシステム上に MPLS VPN SPI をインストールする方法

MPLS VPN SPI を Windows オペレーティングシステム上にインストールするには、次の手順を実行します。

1. NNM 管理ステーションに、ユーザー `administrator` でログオンします。
2. NNM の環境変数に正しい値が設定されていることを確認します。

   詳細は、23 ページの「NNM の環境変数の設定」を参照してください。

3. NNM のデータウェアハウスに Oracle データベースを使用している場合は、次の手順を実行して MPLS VPN SPI 用に Oracle を設定します。

   a. **cd %OV_CONF%¥nnmet¥topology¥extensibility**

   b. **copy UpdateColumn.xslt UpdateColumn.xslt.orig**

   c. テキストエディターを使って UpdateColumn.xslt ファイルの 36 行目にある単語 COLUMN を削除します。

4. Reporting and Network Solutions CD-ROM を CD-ROM ドライブに挿入します。

5. CD-ROM は自動的に起動します。起動しない場合は、Reporting and Network Solutions CD-ROM のディレクトリに移動して setup.bat をダブルクリックします。

   インストールスクリプトが起動されて、ターゲットシステムにインストールされている NNM のバージョンが適切かどうかを調べます。NNM がインストールされていないと、インストールスクリプトはエラーで終了します。詳細は、81 ページの「その他の問題の対処方法」を参照してください。

6. 画面に表示される指示に従って、MPLS VPN SPI をインストールします。インストール処理の途中で表 2-3 に示す質問内容が表示されるので、適切な回答と指示を与えてください。

表 2-3　MPLS VPN SPI を Windows へインストール中の選択項目

選択項目	説明
インストールする製品のリスト	NNM Smart Plug-in のインストールを選択します。
インストールする SPI のリスト	MPLS VPN SPI のインストールを選択します。
MPLS VPN の検出を開始するかどうか	インストールの最後に Extended Topology の検出 (MPLS VPN の検出も含む) を開始する場合は **yes** と入力します。 インストールの最後に MPLS VPN ネットワークの検出を開始しない場合は、**no** を入力します。**no** と入力すると、次に Extended Topology の検出を行う時まで、MPLS VPN ネットワークは検出されません。40 ページの「検出処理」を参照してください。

表 2-3　MPLS VPN SPI を Windows へインストール中の選択項目 (続き)

選択項目	説明
MPLS VPN の定期的な検出が終わるたびに SAA テストを設定するかどうか	MPLS VPN SPI が MPLS VPN の検出を終えた時に、SAA テストの定義を使って、すべての管理対象 PE ルーターに置かれている SAA MIB を自動的にアップデートするようにする場合は、**yes** と入力します。ただし、**yes** と入力する場合は、SNMP 設定データベースに各 PE ルーターの Set 用コミュニティ文字列が設定されていることを確認してください。33 ページの「初期設定」を参照してください。36 ページの「初期設定」を参照してください。 SAA MIB を自動的にアップデートしない場合は、**no** と入力します。**no** と入力すると、コマンドで具体的に指示しない限り、MPLS VPN SPI は SAA MIB をアップデートしません。66 ページの「SAA の設定」を参照してください。 自動設定のオン / オフは変更できます。66 ページの「SAA 設定パラメータの設定方法」を参照してください。
SAA テストの周期	SAA テストの実行間隔を秒単位で指定します。デフォルト値は 600 秒 (10 分) です。 SAA テストの周期は変更できます。66 ページの「SAA 設定パラメータの設定方法」を参照してください。
SAA テストのタイムアウト	SAA テストが成功しない場合のタイムアウトの時間を、ミリ秒単位で指定します。デフォルト値は 100 ミリ秒です。 SAA テストのタイムアウト値は変更できます。66 ページの「SAA 設定パラメータの設定方法」を参照してください。

注記　インストールを行うと C:¥tempschlist ファイルが作成されますが、このファイルは、インストールが終了すれば、使われることはありません。削除しても問題ありません。

MPLS VPN SPI の削除

注記 MPLS VPN SPI を削除しても、NNM アラームブラウザに表示されている MPLS VPN アラームは削除されません。MPLS VPN アラームが不要になった場合は、アラームブラウザの削除機能を使って手動で削除してください。

UNIX オペレーティングシステムから MPLS VPN SPI を削除する方法

UNIX オペレーティングシステムから MPLS VPN SPI を削除するには、次の手順を実行します。

1. NNM 管理ステーションにユーザー `root` でログオンします。
2. 次のコマンドで MPLS VPN SPI の設定を解除して、削除します。

   `mpls_unconfig.ovpl`

3. Solaris オペレーティングシステムの場合*だけは*、次のコマンドを入力します。

   `/usr/sbin/pkgrm HPOvMPLS`
   `/usr/sbin/pkgrm HPOvCisMPLSAgt`

Windows オペレーティングシステムから MPLS VPN SPI を削除する方法

Windows オペレーティングシステムから MPLS VPN SPI を削除するには、以下の手順を実行します。

1. NNM 管理ステーションにユーザー `administrator` でログオンします。
2. 次のコマンドで MPLS VPN SPI の設定を解除して、削除します。

   `mpls_unconfig.ovpl`

注記 削除すると `C:¥tempschlist` ファイルが作成されますが、このファイルは、削除プロセスが終了すれば、使われることはありません。削除しても問題ありません。

初期設定

MPLS VPN SPI では、マルチプロトコルラベルスイッチング環境における仮想プライベートネットワーク (MPLS VPN) 環境の状態を、NNM Advanced Edition の機能を使って監視します。

SNMP ポーリングアクセスの設定

MPLS VPN SPI では、MPLS VPN ネットワーク内のプロバイダエッジ (PE) ルーターとカスタマエッジ (CE) ルーターについて、そのノードおよびインタフェースのステータスを正確に把握する必要がありますが、その処理には NNM の機能を利用しています。NNM では、このステータス情報を、netmon プロセスを使って取得します。netmon はステータスポーリングを実行するので、対象となる各ノードとインタフェースを知っている必要があり、しかもそこへアクセスできる必要があります。

エッジルーターへの SNMP ポーリングアクセスを設定するには、次の手順を実行します。

1. 個々のインタフェースカードごとに、必要な設定作業を決定します。

   - インタフェースカードに IP アドレスが割り当てられていて、管理ステーションから直接到達できる場合は、そのインタフェースカードが NNM のトポロジビューに表示されていることを確認します。

     netmon は、ICMP のエコーリクエストを使ってこれらのインタフェースカードのステータスを調べます。表示確認のほかに必要となる設定作業は特にありません。

   - インタフェースカードに IP アドレスが割り当てられていても管理ステーションからは直接到達*できない*場合は、手順 2 の説明に従って、IP アドレスを `netmon.snmpStatus` ファイルに追加します。

   - インタフェースカードに IP アドレスが*割り当てられていない*場合は、手順 2 の説明に従って、管理対象ノードの IP アドレスを `netmon.snmpStatus` ファイルに追加します。

2. 手順 1 の決定に従って、IP アドレスの情報を `netmon.snmpStatus` ファイルに追加します。このファイルは次のディレクトリにあります。

   UNIX の場合: `$OV_CONF`
   Windows の場合: `%OV_CONF%`

   a. `netmon.snmpStatus` ファイルがない場合は、このファイルを上記ディレクトリに作成します。

b. 可能であれば、IP アドレスをワイルドカードで追加して、NNM 管理ステーションから直接到達できない複数の IP アドレスをまとめて指定します。

IP アドレスワイルドカードは、1 行に 1 つずつ記述します。

c. 追加が必要なインタフェースカードと管理対象ノードの IP アドレスの中で、ワイルドカードで指定しなかったものがあれば、その IP アドレスを個別に追加します

これらの個別 IP アドレスも、1 行に 1 つずつ記述します。

d. このファイルの詳細は、UNIX のマンページまたは Windows のオンラインヘルプにある「netmon.snmpStatus」を参照してください。

netmon は、SNMP リクエストによって ifIndex、ifOperStatus、および ifAdminStatus といった MIB オブジェクトの情報を取得し、これらのインタフェースカードのステータスを調べます。

SNMP アクセスの設定

MPLS VPN 環境では、MPLS VPN SPI から管理対象デバイスへアクセスするために SNMP を使う必要があります。

注記 SAA エコーテストを自動設定するには、このアクセス機能が必要です。Set 用のコミュニティ文字列を指定していないエッジルーターについては、SAA エコーテストを直接設定する必要があります。詳細は、69 ページの「Cisco IOS コマンドを使った SAA の設定方法」を参照してください。

SNMP のデータベースに全エッジルーターの SNMP Set 用コミュニティ文字列を設定するには、次の手順を実行します。

1. 次の SNMP 設定ユーティリティを起動します。
   - *UNIX の場合*: **$OV_BIN/xnmsnmpconf**
   - *Windows の場合*: **%OV_BIN%¥xnmsnmpconf**
2. [SNMP **の設定**] ウィンドウで、エッジルーターごとに Set 用コミュニティ文字列を指定します。

   詳細は、UNIX のマンページまたは Windows のオンラインヘルプにある 「xnmsnmpconf」を参照してください。

SNMP トラップ転送の設定

MPLS VPN SPI で管理対象のデバイスの動作ステータスと到達可能性ステータスを判断するには、それらのデバイスからトラップを受信するように設定する必要があります。

各エッジルーターの SNMP トラップ送信先の 1 つに、NNM 管理ステーションを含むように設定します。設定方法は、ルーターに付属しているマニュアルを参照してください。

3 MPLS VPN の検出

検出処理

MPLS VPN Smart Plug-in (SPI) は、Network Node Manager (NNM) のトポロジの中のどのルーターが、マルチプロトコルラベルスイッチングを使った仮想プライベートネットワーク (MPLS VPN) をサポートしているかを検出します。MPLS VPN SPI は Cisco ルーターデバイスに SNMP クエリを行い、プロバイダエッジ (PE) ルーターの設定および仮想ルーティング / 転送 (VRF) グループの情報を取得します。さらに、MPLS VPN SPI は Extended Topology データベース内のサブネット情報を使って、各カスタマネットワーク内のどのインタフェースが管理対象ネットワーク内の PE ルーターに接続されているかを調べ、そのインタフェースをカスタマエッジ (CE) ルーターとして識別します。

注記　CE ルーターが NNM の管理ドメインに含まれていない場合は、MPLS VPN SPI では PE と CE の接続関係を調べることができません。

MPLS VPN SPI は、MPLS VPN ビューに MPLS VPN ネットワークのモデルを表示するための情報を作成します。モデルには、次の情報が含まれます。

- PE ルーターの詳細情報
  - VRF の詳細情報 (mplsVpnVrfTable から抽出)
  - インタフェースと VRF との関係 (mplsVpnInterfaceConfTable から抽出)
  - 経路ターゲットのインポート / エクスポートリスト (mplsVpnVrfRouteTargetTable から抽出)
- PE ルーター上の送信方向のインタフェースに関する詳細情報
  - インタフェース番号 (mplsVpnInterfaceConfTable から抽出した MplsVpnInterfaceConfIndex)
- PE ルーターに接続されている CE ルーター上の送信方向のインタフェースに関する詳細情報
  - インタフェース番号

- VRF/VPN の設定に関する詳細情報
  - VRF 間の関係 (mplsVpnVrfRouteTargetTable から抽出)

MPLS VPN の検出は、NNM Advanced Edition の Extended Topology による検出と統合されています。つまり、MPLS VPN の検出 では MPLS VPN 検出エージェントとして ovet_daCiscoMplsVpn というプロセスが実行されますが、このプロセスは、Extended Topology による検出が実行されるときは常に実行されます。

Extended Topology による検出の設定を変更したり、Extended Topology を起動したりするには、NNM Advanced Edition の [Extended Topology の設定] ウィンドウを使います。詳細は、NNM Advanced Edition に付属している『*Extended Topology によるネットワーク管理ガイド*』を参照してください。

VPN の命名アルゴリズム

各 VRF オブジェクトには、インポート / エクスポート経路ターゲットのリストがあり、MPLS VPN ネットワーク内の他の VRF を識別するために使われます。MPLS VPN SPI では、このインポート / エクスポートリストにある経路ターゲットの情報を調べ、VRF の隣接グループを識別します。そして、この隣接関係の情報を基に、イントラネットのユーザーへ十分なサービスを提供するためにテストすべき、MPLS VPN ネットワーク内の経路を決定します。

MPLS VPN SPI では、隣接関係によって直接または間接にリンクすることができる VRF を、すべて同じ VPN に存在するものと見なします。MPLS VPN SPI が、完全メッシュ接続の単純なネットワークトポロジだけでなく、ハブやスポークの入り交じった複雑なネットワークトポロジも正しく検出できるのは、このアプローチをとっているからです。

MPLS VPN SPI では、VRF のグループ関係と VPN の名前を VpnNames.txt ファイルに保存して管理します。このファイルの説明は、44 ページの「MPLS VPN SPI 設定ファイル内の VPN 名の変更」を参照してください。

MPLS VPN SPI は、検出した VRF グループに対して、次の命名規則に従って可能な限り意味のある VPN 名を割り当てます。

1. 検出した VRF グループと一致する VRF グループが `VpnNames.txt` ファイル内にある場合は、その VRF グループの VPN 名をそのまま使います。

   一致するかどうかは、検出した VRF グループのリストと `VpnNames.txt` ファイル内の VRF グループのリストに同じ VRF が存在するかどうかで判断します。同じ VRF が 1 つ以上存在すれば、一致と見なします。

2. 検出した VRF グループと一致する VRF グループが `VpnNames.txt` ファイル内にない場合は、検出したグループ内の各 VRF についてその VRF 名を調べ、次の規則に従って新しい VPN 名を作成します。

   - グループ内のすべての VRF の名前が同じで、その名前が他の VPN 名として使われていない場合は、そのテキスト文字列を当該 VRF グループの VPN 名として割り当てます。
   - グループ内のすべての VRF の名前が同じでも、その名前が別の VRF リストの VPN 名としてすでに使われている場合は、VRF 名の後ろにアンダースコア (_) と、この VRF グループの VPN 内部識別番号を付加した文字列として割り当てます。

3. VRF グループ内のすべての名前が先頭から 3 文字以上同じである場合は、その共通文字列全体を VPN 名として割り当てます。

   ただしこの規則では、別の VRF グループでこの VPN 名が使われていないことを前提にしています。

4. 上記のいずれの規則にも該当しない場合は、文字列 Unknown_ の後ろに内部識別番号を付加した文字列を VPN 名として割り当てます。

   VPN 名を変更するには、44 ページの「MPLS VPN SPI 設定ファイル内の VPN 名の変更」の説明に従って、VpnNames.txt ファイルを編集します。ただし、新しい VPN 名はネットワーク内で意味のある名前にしておくことをお勧めします。

表 3-1 に、この VPN 命名アルゴリズムの適用例を示します。

表 3-1 VPN の命名例

VPN 内の VRF	割り当てる VPN 名	説明
Blue Blue	Blue	すべての VRF 名が同じなので、この名前を選択
Red_East Red_West	Red_	先頭の共通文字列を使用
Red_North Red_South	Red__5	先頭の共通文字列にアンダースコアと、一意の VPN 内部識別子を付加
Blue Green Yellow	Unknown_1	VRF 名に一致部分がないか、または VRF 名から意味のある名前を構成できない

MPLS VPN SPI 設定ファイル内の VPN 名の変更

MPLS VPN SPI では、次のファイルに VRF のグループ関係とそれに対応する VPN 名を保存します。

- *UNIX の場合*: `$OV_CONF/VpnNames.txt`
- *Windows の場合*: `%OV_CONF%¥VpnNames.txt`

VPN 名のカスタマイズは、このファイルを編集することで行います。`VpnNames.txt` ファイルの形式は、次のとおりです。

```
VpnName  VPN_Internal_Id  VrfList
```

各エントリーの間には、セパレータとしてタブを 1 つ置きます。空白文字は使えません。

VrfList には、複数のエントリーを記述できます。各エントリーには、PE ルーター名とそのルーター上の VRF 名を指定します。VrfList の各エントリーの形式は、次のとおりです。

```
DeviceName<<>>VrfName  DeviceName<<>>VrfName
```

ルーター名と VRF 名の間には、セパレータとして文字列 `<<>>` を置きます。また、VrfList の各エントリー間には、セパレータとしてタブを 1 つ置きます。

`DeviceName` には、IP アドレスまたはホスト名を指定します。`DeviceName` の値には、NNM のトポロジデータベースに登録されているものを使います。

図 3-1 に、`VpnNames.txt` ファイルの例を示します。

図 3-1　　VpnNames.txt ファイルの例

```
Blue    1    Device1<<>>Blue    Device2<<>>Blue    Device3<<>>Blue
Unknown_2    2    Device3<<>>Red    Device4<<>>Green    Device5<<>>Purple
Cust    3    Device6<<>>CustEast    Device7<<>>CustWest
    Device8<<>>CustNorth    Device9<<>>CustSouth
```

割り当てられている VPN 名を変更する方法は、次のとおりです。

- テキストエディターを使って、VpnNames.txt ファイルを編集します。

  1. 文字列 Unknown_ を含む VPN 名を探し、ネットワーク内で意味のある名前に変更します。
  2. 必要に応じてその他の VPN 名を変更します。

警告	**変更するのは、VpnName フィールドの値のみにしてください。このファイルのそれ以外のフィールドを変更すると、ファイル全体が廃棄されます。**

4 MPLS VPN Smart Plug-in が生成するイベント

MPLS VPN のステータスマネージャ

MPLS VPN Smart Plug-in (SPI) のステータスマネージャは、HP OpenView のイベントサブシステムから特定の SNMP イベントを受信します。イベントを受信した SPI は、それらのイベントの状況を仮想プライベートネットワーク (VPN) に関連付ける、詳細情報を追加した新しい SNMP イベントを生成します。ステータスマネージャは Network Node Manager (NNM) 内に PairWise 相関処理を設定し、必要に応じて NNM アラームブラウザから情報追加イベントを削除できるようにします。

MPLS VPN SPI のステータスマネージャのプロセス (`MPLS_sm`) は、NNM のサービスの 1 つであり、`ovspmd` によって管理されます。このプロセスは、次に示す NNM の標準ログファイルにステータスメッセージを記録します。

- *UNIX の場合*: `$OV_LOG/System.txt`
- *Windows の場合*: `%OV_LOG%¥System.txt`

MPLS VPN SPI が生成する情報追加イベントの詳細は、次の項を参照してください。

- 49 ページの「ルーターステータスイベント」
- 52 ページの「到達可能性ステータスの変化を知らせるイベント」
- 55 ページの「OVPI から受信する Report Pack のしきい値イベント」

ルーターステータスイベント

ここでは、マルチプロトコルラベルスイッチング環境における仮想プライベートネットワーク (MPLS VPN) のエッジルーターが正しく機能しているかについて、MPLS VPN SPI が生成するイベントを説明します。

MPLS VPN SPI は、管理対象 MPLS VPN に存在するプロバイダエッジ (PE) ルーターとカスタマエッジ (CE) ルーターのステータス変化についてのイベントを HP OpenView のイベントサブシステムから受信し、新しいイベントを生成します。MPLS VPN SPI は、PE ルーター側の CE 接続インタフェース、または CE ルーター側の PE 接続インタフェースのステータス変化についてのイベントを受信すると、その変化の根本原因を示す新しいイベントを生成します。また MPLS VPN SPI は、PE および CE ルーターのインタフェースカードまたはノードのステータス変化を示すイベントを待ち受け、変化を検出するたびにイベントを生成します。

MPLS VPN SPI は、MPLS VPN ネットワーク固有の情報を追加した新しいデバイスステータスイベントを生成します。NNM のアラームブラウザでは、生成されたこれらのイベントが MPLS VPN カテゴリに表示されます。

デフォルトでは、MPLS VPN SPI は netmon プロセスからしかイベントを受信しません。アクティブ問題アナライザ (APA) からイベントを受信するように NNM を設定すれば、MPLS VPN SPI は netmon プロセスではなく APA からイベントを受信します。NNM が受信するイベントのソースを変更するには、ovet_apaConfig.ovpl コマンドを使います。詳細は、NNM Advanced Edition に付属している『*Extended Topology によるネットワーク管理ガイド*』を参照してください。

表 4-1 に、MPLS VPN SPI の生成するデバイスステータスイベントとその説明を示します。これらのイベントの形式は、14 ページの「MPLS VPN のイベント」を参照してください。イベントに関連する変数バインディングの詳細は、次のディレクトリにある trapd.conf ファイルを参照してください。

UNIX の場合: `$OV_CONF/C`
Windows の場合: `%OV_CONF%¥C`

表 4-1 MPLS VPN SPI の生成する情報追加ルーターステータスイベント

情報追加イベント名 / HP OpenView イベント OID	説明	入力イベント名 / HP OpenView イベント OID	入力イベントのソース
OV_MPLS_VPN_ADDRDOWN/ 70001009	影響を受ける VPN 内のデバイスのインタフェースカードが、IP アドレスを指定して ping 要求を送っても応答しない	OV_APA_ADDR_DOWN/ 58983011	APA
なし。 アラームブラウザから OV_MPLS_VPN_ADDRDOWN イベントが消える。	インタフェースカードが、その IP アドレスに対する ping 要求に応答するようになった	OV_APA_ADDR_UP/ 58983001	APA
OV_MPLS_VPN_IFDOWN/ 70001000	PE ルーター上で MPLS VPN 用に設定されている CE 接続インタフェースがダウンした	OV_APA_IF_DOWN/ 5893012	APA
		OV_IF_Down/ 58916867	netmon
なし。 アラームブラウザから OV_MPLS_VPN_IFDOWN イベントが消える。	PE ルーター上で MPLS VPN 用に設定されている CE 接続インタフェースが復旧した	OV_APA_IF_UP/ 5893002	APA
		OV_IF_Up/ 58916866	netmon
OV_MPLS_VPN_NODEDOWN/ 70001002	PE ルーターがダウンした	OV_APA_NODE_DOWN/ 58983013	APA
		OV_Node_Down/ 58916865	netmon

表 4-1 MPLS VPN SPI の生成する情報追加ルーターステータスイベント (続き)

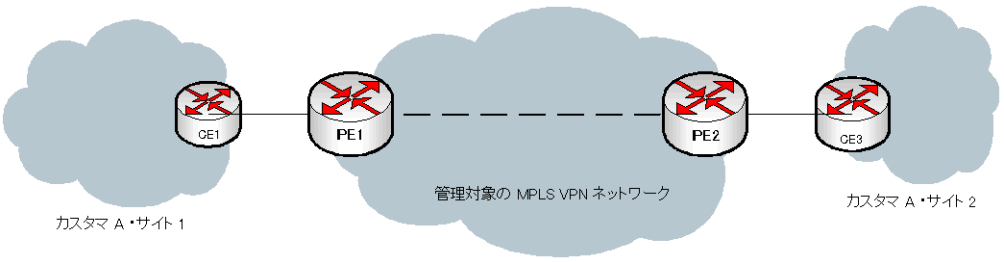
情報追加イベント名 / HP OpenView イベント OID	説明	入力イベント名 / HP OpenView イベント OID	入力イベントのソース
なし。 アラームブラウザから OV_MPLS_VPN_NODEDOWN イベントが消える。	PE ルーターが復旧した	OV_APA_NODE_UP/ 58983003	APA
		OV_Node_Up/ 58916864	netmon
OV_MPLS_VPN_Card_Down/ 70001013	VRF を有効にしたインタフェースを持つカードがダウンした	OV_APA_CARD_DOWN/ 58983035	APA
なし。 アラームブラウザから OV_MPLS_VPN_Card_Down イベントが消える。	VRF を有効にしたインタフェースを持つカードが復旧した	OV_APA_CARD_UP/ 58983034	APA
OV_MPLS_VPN_CONNDOWN/ 70001011	影響を受ける VPN 内の 2 つのデバイスのインタフェースカード間の接続が、正しく動作していない	OV_APA_CONNECTION_DOWN/ 58983014	APA
なし。 アラームブラウザから OV_MPLS_VPN_CONNDOWN イベントが消える。	2 つのインタフェースカードの間の接続が正しく動作するようになった	OV_APA_CONNECTION_UP/ 58983004	APA
OV_MPLS_VPN_NODEUNKNOWN/ 70001004	VRF パスの間にあるデバイスのステータスが把握できない	OV_TOPOLOGY_Status_ Change_Notification/ 60001101	netmon

到達可能性ステータスの変化を知らせるイベント

MPLS VPN SPI では、到達可能性ステータスの変化を知らせるために、ネットワーク固有の情報を追加した新しいイベントを生成します。NNM アラームブラウザでは、生成されたこれらの情報追加イベントが MPLS VPN カテゴリに表示されます。

MPLS VPN SPI は、MPLS VPN ネットワーク内のルーター間の到達可能性テストを設定して、その結果として発生する SNMP トラップを待ち受けます。受信した SNMP トラップの中に到達可能性ステータスの変化を示すものが 1 つでもあると、MPLS VPN SPI は到達可能性ステータスの変化を示すイベントを生成します。図 4-1 に、MPLS VPN ネットワークを経由するパスの例を示します。

図 4-1　　到達可能性テストのパスの例



MPLS VPN SPI でサポートされている到達可能性テストのパスは、次のとおりです。

- PE ルーターと PE ルーターとの間 (たとえば、PE1-PE2 間)
- PE ルーターとその近くの CE ルーターとの間 (たとえば、PE1-CE1 間)
- CE ルーターと CE ルーターとの間 (たとえば、CE1-CE3 間)

CE-CE 間のエンドツーエンドの到達可能性テストでは、ソース CE ルーター → 近くの PE ルーター → 遠くの PE ルーター → 遠くの CE ルーターの順で接続性を調べます。ソース CE ルーターが Cisco デバイスでない場合、MPLS VPN SPI はこのテストを複数の独立した SAA テストに分割して、パス全体をカバーします。

Cisco ルーターの到達可能性テスト

Cisco ルーターの場合、MPLS VPN SPI は、Cisco Internetwork Operating System (IOS) の Service Assurance Agent (SAA) を使って到達可能性テスト行います。この方法では、テストごとに、VPN 内の 1 つの PE ルーターまたは CE ルーターから、別の PE ルーターまたは CE ルーターに対して ICMP エコーリクエストを発行します。SAA はこのエコーリクエストの往復にかかる時間を計算して、応答時間がそのテストのタイムアウト値を超えると、`rttMonCtrlOperTimeoutOccurred` 変数のバインディング値を `TRUE` に設定して `rttMonTimeoutNotification` トラップを 1 つ送信し、テストが失敗したことを知らせます。この SNMP トラップを受信した MPLS VPN SPI は、SAA が失敗したことを示す新しい情報追加トラップを生成して、NNM に送信します。

失敗した SAA テストが 2 つの CE ルーター間にあるパス全体をテストするものであった場合、MPLS VPN SPI は影響を受ける VRF のインタフェースをポーリングしてパス内の障害箇所を特定するよう、NNM に要求します。そして、その特定の障害を示す新し情報追加トラップを生成して NNM に送信します。

SAA は、テストが成功すると、`rttMonCtrlOperTimeoutOccurred` 変数のバインディング値を `FALSE` に設定して `rttMonTimeoutNotification` トラップを 1 つ送信し、テストの成功を知らせます。この SNMP トラップを受信した MPLS VPN SPI は、先に SAA 障害トラップを受信していた場合は、SAA のステータス変化を伝える新しい情報追加トラップを生成して、NNM に送信します。この新しいイベントの到着によって、対応する SAA 障害イベントが アラームブラウザから削除されます。

表 4-2 に、MPLS VPN SPI が SAA テストの状態に応じて生成する情報追加イベントを示します。これらのイベントの形式は、14 ページの「MPLS VPN のイベント」を参照してください。また、イベントに関連する変数バインディングの詳細は、次のディレクトリにある `trapd.conf` ファイルを参照してください。

UNIX の場合: `$OV_CONF/C`
Windows の場合: `%OV_CONF%¥C`

表 4-2 MPLS VPN SPI の生成する情報追加到達可能性ステータスイベント

情報追加イベント名 / HP OpenView イベント OID	説明	SAA MIB オブジェクト / OID = 値
OV_MPLS_VPN_SAA_FAIL/ 70001006	2 つのデバイス間の接続がダウンした	rttMonCtrlOperTimeoutOccurred/ .1.3.6.1.4.1.9.9.42.1.2.9.1.6 = TRUE
OV_MPLS_VPN_SAA_PASS/ 70001007 アラームブラウザから、OV_MPLS_VPN_SAA_FAIL イベントが消える。	2 つのデバイス間の接続が復旧した	rttMonCtrlOperTimeoutOccurred/ .1.3.6.1.4.1.9.9.42.1.2.9.1.6 = FALSE

OVPI から受信する Report Pack のしきい値イベント

OVPI と MPLS VPN Report Pack がインストールされていると、MPLS VPN SPI は OVPI から複数の種類のしきい値イベントを受信します。MPLS VPN SPI は、これらのイベントを NNM アラームブラウザの MPLS VPN Performance カテゴリに載せます。ただし、これらのイベントに情報が追加されることはありません。

表 4-3 に、MPLS VPN SPI が OVPI から受信するしきい値イベントとその説明を示します。

表 4-3 OVPI から受信する MPLS VPN しきい値イベント

OVPI イベント名	説明
VPN_INTERFACEAVAIL_PCT	VPN 内のすべてのインタフェースの平均稼働率が許容可能なしきい値を下回っている
VPN_DISCARD_PCT	VPN 内のすべてのインタフェースの平均パケット廃棄率が許容可能なしきい値を下回っている
VPN_ERROR_PCT	VPN 内のすべてのインタフェースの平均パケットエラー率が許容可能なしきい値を下回っている
VPN_SNMPRESPONSE	VPN 内のすべてのインタフェースについて、OVPI からデバイス / インタフェースまでの平均 SNMP 応答時間が許容可能なしきい値を下回っている
VRF_OPERSTATUS	VRF が動作していない

5　サービス保証エージェントの使い方

サービス保証エージェント

Cisco Internetwork Operating System (IOS) のサービス保証エージェント (SAA) は、Cisco IOS デバイスに組み込まれているソフトウェアエージェントです。このエージェントはネットワークが正常に動作しているかどうかを能動的に監視し、サービスレベルが契約どおりに守られているかどうかを検証します。ルーターの SAA 機能は、そのルーター上の Cisco RTTMON MIB (SAA MIB) 変数で設定します。ネットワークにルーターが複数個ある場合は、ルーターごとに異なる SAA 動作を設定することもできます。

MPLS VPN Smart Plug-in (SPI) は、マルチプロトコルラベルスイッチングを使った仮想プライベートネットワーク (MPLS VPN) 環境内にある各プロバイダエッジ - プロバイダエッジ (PE-PE) ルーターペア間の到達可能性を、ICMP のエコーリクエストを使ってテストするように、SAA を設定します。到達可能性テストがタイムアウトで失敗すると、SAA は Network Node Manager (NNM) に SNMP トラップを送信します。MPLS VPN SPI は、このトラップを HP OpenView のイベントサブシステムから受信すると、そのトラップに MPLS VPN ネットワークに関する情報を追加し、NNM アラームブラウザにそのイベントを表示します。

MPLS VPN SPI がこれらのトラップを処理する仕組みは、52 ページの「到達可能性ステータスの変化を知らせるイベント」を参照してください。

SAA テスト

MPLS VPN SPI は PE-PE ルーターペアのリストを管理して、各ペア間に双方向の到達可能性テストを設定します。たとえば、MPLS VPN SPI は、PE1 上の SAA が PE1 から PE2 へ ICMP エコーリクエストを送るように設定するとともに、PE2 上の SAA が PE2 から PE1 へ ICMP エコーリクエストを送るように設定します。

MPLS VPN SPI でサポートされている到達可能性テストには、次の種類があります。

- *PE-PE 間 VRF 非対応型到達可能性テスト*。このテストでは、対象となる PE ルーターをブラックボックスとみなして、その間の接続性をチェックします。特に指定しない限り、MPLS VPN SPI は MPLS VPN ネットワーク内のすべての PE-PE ペアに対してこのテストを設定します。
- *PE-PE 間 VRF 対応型到達可能性テスト*。このテストでは、VPN 内に定義済みの VRF パスを使って、2 つの PE ルーター間の接続性をチェックします。
- *PE-CE 間 VRF 対応型到達可能性テスト*。このテストでは、VPN 内に存在する PE ルーターと特定のローカル CE ルーターとの間の接続性をチェックします。

- *CE-CE 間エンドツーエンド型到達可能性テスト*。このテストでは、VPN 内に存在する特定の CE-PE-PE-CE パスの接続性をチェックします。

SAA テストの定義

SAA テストの定義情報は、MPLS VPN SPI の内部ファイルに保存されます。MPLS VPN SPI はこのファイルを解釈して、MPLS VPN ネットワーク内の各 SAA を設定します。現在の SAA テストの定義にアクセスするには、saa_config.ovpl コマンドを使います。このコマンドの詳細は、65 ページの「SAA テストの定義変更方法」を参照してください。

SAA テストを最初に設定するときは、新しいテスト定義ファイルを作成した後、そのファイルを MPLS VPN SPI の SAA テスト定義ファイルにインポートします。現在の SAA テストの定義を変更する場合は、SAA テストの定義をファイルにエクスポートして変更するか、新しいテキストファイルを作成して設定したいテストのみを定義した後、そのファイルを MPLS VPN SPI にインポートします。MPLS VPN SPI は、SAA テストの定義ファイルが変更されるたびに、すべての管理対象 PE ルーターおよび Cisco CE ルーター上の SAA テストの定義をアップデートします。

SAA テストの設定で Cisco 以外の CE ルーターをソースルーターに指定すると、MPLS VPN SPI では、そのテストを複数のセグメントに分割して、PE ルーター上に設定します。たとえば、次のネットワークパスを考えてみます。

CE1-PE1-PE2-CE2

CE1 が Cisco デバイスでない場合は、MPLS VPN SPI では、このテストを PE1-CE1 間の到達可能性テストと PE1-CE2 間の到達可能性テストに分割して、PE1 デバイスに設定します。

SAA テスト定義ファイルの形式

SAA テスト定義ファイルは、各 SAA が実行すべき ICMP エコーリクエストを定義する単純なテキストファイルです。このファイルに、個々のテスト (複数可) を BEGIN と END の対で囲んで定義します。63 ページの図 5-1 ～ 64 ページの図 5-4 に、SAA テストの定義の例を示します。

SAA テストの定義に使う要素は、次のとおりです。

- BEGIN ― SAA テストの定義を開始する要素です。

- TEST_TYPE ー 定義する SAA テストの種類です。指定できる値は PE-PE、PE-CE、および CE-CE で、次のように指定します。
  - PE-PE 間 VRF 非対応型テストまたは PE-PE 間 VRF 対応型テストの場合は、PE-PE を指定します。
  - PE - ローカル CE 間 VRF 対応型テストの場合は、PE-CE を指定します。
  - CE-CE 間エンドツーエンド型テストの場合は、CE-CE を指定します。
- SOURCE ー SAA テストの起動側ルーター (ソースルーター) を指定するための選択名です。この値には、NNM トポロジデータベース内の選択名と同じ名前を指定する必要があります。
- DEST ー SAA テストの被検証側ルーター (デスティネーションルーター) を指定するための選択名です。この値には、NNM トポロジデータベース内の選択名と同じ名前を指定する必要があります。
- VRF ー オプションで指定します。この値は PE-PE 間 VRF 対応型テストと PE-CE 間 VRF 対応型テストに対してのみ有効です。指定するときは、ソースルーターとデスティネーションルーターの両方に存在する VRF の名前を指定します。VRF 名は、ソースエッジルーター上のルーター設定ファイルと次のファイルで調べることができます。
  - *UNIX の場合*: $OV_CONF/VpnNames.txt
  - *Windows の場合*: %OV_CONF%¥VpnNames.txt
- OP ー 当該ファイルを SAA テスト設定ツールへインポートするときの操作を指定します。指定できる値は、ADD、DELETE、MODIFY です。
- CONFIG_TYPE ー 設定方法を指定します。指定できる値は、SAA_TEST_CONFIG と SAA_TEST_SYNC です。
  - SAA_TEST_CONFIG を指定すると、このファイルをインポートしたときに、MPLS VPN SPI の SAA 設定プロセスによって、ソースルーター上の SAA MIB にこの SAA テストが設定されます。
  - SAA_TEST_SYNC を指定すると、ソースルーター上の SAA MIB に設定されたこの SAA テストは、SAA 設定プロセスから変更できなくなります。この値を指定した場合は、Cisco IOS コマンドを使って、この SAA テストをソースルーター上の SAA MIB に明示的に設定する必要があります。

- SAA_SRC_ADDR ー オプションで指定します。SAA テストの対象ルーター上にあるソースインタフェースカードの IP アドレスを指定します。このアドレスは、標準の VRF *非*対応型テストに対してのみ有効です。
  - PE-PE 間 VRF *非*対応型テストの場合は、ソースルーターに割り当てられている任意の IP アドレスを指定できます。
  - CE-CE 間エンドツーエンド型テストの場合は、VPN 内のプライベート IP アドレスを指定する必要があります。
- SAA_DEST_ADDR ー オプションで指定します。SAA テストの対象ルーター上にあるデスティネーションインタフェースカードの IP アドレスを指定します。指定する IP アドレスは、この SAA テストのデスティネーションルーターを通って到達可能な VPN のアドレス範囲に入っている必要があります。
  - PE-PE 間 VRF *非*対応型テストの場合は、デスティネーションルーターに割り当てられている任意の IP アドレスを指定できます。
  - PE-PE 間 VRF 対応型テスト、PE-CE 間 VRF 対応型テスト、および CE-CE 間エンドツーエンド型テストの場合は、VPN 内のプライベート IP アドレスを指定する必要があります。
- SET_COMM ー オプションで指定します。ソース PE ルーターの SNMP Set 用コミュニティ文字列を指定します。ソース PE ルーターのコミュニティ文字列が SNMP 設定データベースで設定済みの場合は、SAA テストの定義で指定する必要はありません。この値は、CONFIG_TYPE パラメータの値が SAA_TEST_CONFIG の場合にのみ有効です。
- FREQUENCY ー オプションで指定します。このテストを定期的に行う場合の間隔を指定します。間隔は秒単位で指定します。

  この要素が SAA テストの定義で指定されていない場合は、この SAA が設定される時点での、mpls.conf ファイルの FREQUENCY パラメータの値が使われます。mpls.conf ファイルの詳細は、66 ページの「SAA 設定パラメータの設定方法」を参照してください。
- TIMEOUT ー オプションで指定します。ICMP のエコー応答が帰ってこない場合はテストが失敗したと判断しますが、この要素でその許容時間 (タイムアウト時間) を指定します。タイムアウト時間は、ミリ秒単位で指定します。

  この要素が SAA テストの定義で指定されていない場合は、この SAA が設定される時点での、mpls.conf ファイルの TIMEOUT パラメータの値が使われます。mpls.conf ファイルの詳細は、66 ページの「SAA 設定パラメータの設定方法」を参照してください。

- TAG ― この SAA テストの識別子です。この値は MPLS VPN SPI が決定し、エクスポートモードでのみ有効です。テストの定義を新しく作成する場合は、このパラメータを未定義のままにしておきます。
- END ― SAA テストの定義を終了する要素です。

図 5-1　PE-PE 間 VRF 非対応型 SAA テストの定義例

```
BEGIN
TEST_TYPE=PE-PE
SOURCE=mplspe01
DEST=mplspe04
VRF=
OP=ADD
CONFIG_TYPE=SAA_TEST_CONFIG
SAA_SRC_ADDR=
SAA_DEST_ADDR=
SET_COMM=ntcprivate
FREQUENCY=600
TIMEOUT=100
TAG=
END
```

図 5-2　PE-PE 間 VRF 対応型 SAA テストの定義例

```
BEGIN
TEST_TYPE=PE-PE
SOURCE=mplspe01
DEST=mplspe04
VRF=Red_East
OP=ADD
CONFIG_TYPE=SAA_TEST_CONFIG
SAA_SRC_ADDR=
SAA_DEST_ADDR=10.97.255.27
SET_COMM=ntcprivate
FREQUENCY=600
TIMEOUT=100
TAG=
END
```

図 5-3 PE-CE 間ローカル VRF 対応型 SAA テストの定義例

```
BEGIN
TEST_TYPE=PE-CE
SOURCE=mplspe01
DEST=mplsce01
VRF=Red_East
OP=ADD
CONFIG_TYPE=SAA_TEST_CONFIG
SAA_SRC_ADDR=
SAA_DEST_ADDR=10.10.20.1
SET_COMM=ntcprivate
FREQUENCY=600
TIMEOUT=100
TAG=
END
```

図 5-4 CE-CE 間エンドツーエンド型 SAA テストの定義例

```
BEGIN
TEST_TYPE=CE-CE
SOURCE=mplsce02
DEST=mplsce04
VRF=
OP=ADD
CONFIG_TYPE=SAA_TEST_CONFIG
SAA_SRC_ADDR=
SAA_DEST_ADDR=
SET_COMM=ntcprivate
FREQUENCY=600
TIMEOUT=100
TAG=
END
```

SAA テストの定義変更方法

現在の SAA テストの定義は、次の方法で表示したり変更したりすることができます。

- 現在の SAA テストの定義を表示するには、次のコマンドを実行します。

  saa_config.ovpl -e *filename*

  このコマンドを実行すると、MPLS VPN SPI は、指定したファイル *filename* に SAA テストの定義をエクスポートします。ただし、このコマンドでエクスポートされる SAA テストの定義は、デバイス自体から取得したものではなく、MPLS VPN SPI によって保存されている SAA テスト設定情報から取得したものです。

- 新規または修正済みの SAA テストの定義を作成するには、次のコマンドを実行します。

  saa_config.ovpl -i *filename*

  このコマンドを実行すると、MPLS VPN SPI は、指定したファイル *filename* から SAA テストの定義を読み込み、そこに指定されている PE ルーター上の SAA テストの設定をアップデートします。

SAA テストの定義を変更する手順は、67 ページの「MPLS VPN SPI を使った SAA の設定」を参照してください。

SAA の設定

特に指定しない限り、MPLS VPN SPI では、MPLS VPN の検出が完了したときに SAA テストの定義をアップデートします。また、このアップデートで SAA テストの既存の定義に対する変更が少しでも見つかると、その変更点を、各管理対象ルーター上の SAA MIB の設定に反映します。66 ページの「SAA 設定パラメータの設定方法」を参照してください。

MPLS VPN SPI では SAA との通信に SNMP を使います。そのため、MPLS VPN SPI に単独で SAA テストを設定させる場合は、各ルーターの SNMP Set 用コミュニティ文字列へアクセスできるようにしておく必要があります。67 ページの「MPLS VPN SPI を使った SAA の設定」を参照してください。

ルーターの SNMP Set 用コミュニティ文字列を指定したくない場合は、Cisco IOS コマンドを使ってルーター上の SAA MIB を設定します。69 ページの「Cisco IOS コマンドを使った SAA の設定方法」を参照してください。

SAA 設定パラメータの設定方法

MPLS VPN SPI をインストールすると、MPLS VPN SPI が単独で SAA を設定する場合の制御パラメータがいくつか設定されます。これらのパラメータは、次のファイルに保存されています。

- *UNIX の場合*: `$OV_CONF/mpls.conf`
- *Windows の場合*: `%OV_CONF%¥mpls.conf`

図 5-5 に、`mpls.conf` ファイルの例を示します。

図 5-5　mpls.conf ファイルの例

```
SAA_TRIG=true
FREQUENCY=600
TIMEOUT=100
```

mpls.conf ファイルには、次のパラメータが設定されています。

- SAA_TRIG ― MPLS VPN の検出が完了した後で SAA の設定プロセスを実行するかどうかを制御するパラメータです。指定できる値は、true または false です。
- FREQUENCY ― SAA テストの実行頻度のデフォルト値を制御するパラメータです。SAA テストの定義に頻度が指定されていない場合は、MPLS VPN SPI はここに指定されている頻度値を使って SAA テストを設定します。
- TIMEOUT ― SAA テストのデフォルトのタイムアウト値を制御するパラメータです。SAA テストの定義にタイムアウト値が指定されていない場合は、MPLS VPN SPI はここに指定されているタイムアウト値を使って SAA テストを設定します。

MPLS VPN SPI を通して SAA の設定パラメータを変更するには、次のようにします。

- テキストエディターを使って、mpls.conf ファイルを編集します。

  MPLS VPN SPI は、SAA の設定を実行するたびに mpls.conf ファイルを読み込みます。

注記　FREQUENCY パラメータと TIMEOUT パラメータの値を変更すると、それ以降に新規作成または変更された SAA テストの定義のみ影響を受けます。既存の SAA テストの定義は変更されません。

MPLS VPN SPI を使った SAA の設定

MPLS VPN SPI に SAA を単独で設定させる場合は、対象ルーターの SNMP Set 用コミュニティ文字列へアクセスできるようにする必要があります。SNMP Set 用コミュニティ文字列は、次の 2 つの方法で設定できます。

- xnmsnmpconf コマンドを使って NNM の SNMP 設定データベースにコミュニティ文字列を保存する方法。この方法を使った場合は、NNM のすべての管理機能からルーターにアクセスできます。
- SAA テスト定義ファイルでコミュニティ文字列を指定してインポートする方法。この方法を使った場合は、MPLS VPN SPI の SAA テスト設定機能からしかルーターにアクセスできません。

特に指定しない限り、MPLS VPN SPI は、ネットワーク内の各 VPN に存在するすべての PE-PE ルーターペアを対象に、VRF 非対応型 SAA テストを作成します。

MPLS VPN SPI を使って VRF 対応型 SAA テストを設定する場合、または、VRF 非対応型 SAA テストを追加で設定する場合は、次の手順を実行します。

1. SAA テスト定義ファイルを作成します。

   saa_config.ovpl -e *filename*

   filename で指定したファイルに、SAA テストの現在の定義が出力されます。

2. テキストエディターを使い、次の手順で SAA テスト定義ファイル *filename* を編集して、実行する SAA テストを定義します。

   a. 必要に応じて、既存の定義を変更します。

      - 既存のテストの定義を変更するには、テストの定義を編集して、OP パラメータとして MODIFY を指定します。
      - 既存のテストの定義を削除するには、OP パラメータとして DELETE を指定します。

注記 MPLS VPN SPI が作成したテストの定義は、いったん削除すると、SPI によって再び追加されることはありません。後でこの SAA テストを実行することになった場合は、このテストの定義を新たに作成して、SAA の設定にインポートする必要があります。

---

   b. 必要に応じて、新しいテストの定義を追加します。その際、

      - テスト定義ファイルの形式に従います。
      - OP パラメータには、ADD を設定します。

   c. 必要に応じて、各 SAA テストの定義ごとに SNMP Set 用コミュニティ文字列を指定します。

      - ソース PE ルーターの Set 用コミュニティ文字列が SNMP 設定データベースに保存されている場合は、SAA テストの定義で SET_COMM パラメータを指定しないようにします。
      - ソース PE ルーターの Set 用コミュニティ文字列が SNMP 設定データベースに保存されていない場合は、SAA テストの定義で SET_COMM パラメータに正しい値を指定します。

3. アップデートした SAA テストの定義をインポートします。

   saa_config.ovpl -i *filename*

   MPLS VPN SPI が *filename* で指定したファイル の中に定義されているそれぞれの SAA テストの定義を読み込み、そのテストをソースルーターの SAA MIB に設定します。

Cisco IOS コマンドを使った SAA の設定方法

ルーターの SNMP Set 用コミュニティ文字列が取得できない場合は、Cisco IOS コマンドを使って、ルーター上の SAA テストを設定します。

各 SAA テストには、一意のタグ名があります。MPLS VPN SPI はこのタグ名を使って、SNMP トラップの中の SAA テストを識別します。タグ名は、MPLS VPN SPI が生成したものを使う必要があります。MPLS VPN SPI によって CE-CE 間エンドツーエンド型到達可能性テストが 2 つのテストに分割されている場合は、それぞれのテストの設定に、それぞれ一意のタグ値を指定する必要があります。

Cisco IOS コマンドを使って SAA テストを設定するには、次の手順を実行します。

1. 新しいテキストファイルを作成し、各 SAA テストごとに次の要素とその値を記述します。

   - BEGIN
   - TEST_TYPE
   - SOURCE
   - DEST
   - VRF (有効な場合のみ)
   - OP
   - CONFIG_TYPE = SAA_TEST_SYNC
   - SAA_SRC_ADDR (有効な場合のみ)
   - SAA_DEST_ADDR (有効な場合のみ)
   - END

   ファイルの詳細な形式は、60 ページの「SAA テスト定義ファイルの形式」を参照してください。

2. 各 SAA テストごとに、一意のタグ名を生成します。

   saa_config.ovpl -i *input_filename* -o *output_filename*

   このコマンドを実行すると、MPLS VPN SPI は手順 1 で作成したテキストファイル *input_filename* を読み込み、それぞれの SAA テストの定義にタグ名を追加した SAA テスト定義ファイル *output_filename* を出力します。

3. ソースルーターに接続し、Cisco IOS コマンドを使って各 SAA を設定します。

   その際、テストごとに、対応するタグを指定します。このタグは、手順 2 で MPLS VPN SPI が生成した *output_filename* ファイルで OV_TAG パラメータに設定された値です。

   図 5-6 に SAA テストを設定するための Cisco IOS コマンドシーケンスの例を示します。ルーターの設定方法は、対応する Cisco のドキュメントを参照してください。

図 5-6　　SAA を設定するための Cisco IOS コマンドの例

```
rtr Entry Number
type echo protocol IpIcmp Destination [source-ipaddr Source]
vrf VRF Name
timeout Timeout Value
frequency Frequency
tos 5
tag TagValue
rtr reaction-conf Entry Number threshold-type immediate
action-type trapOnly timeout-enable
rtr schedule Entry Number life 2147483647 start-time now
```

6 MPLS VPN Smart Plug-in のトラブルシューティング

トラブルシューティングのチェックリスト

注記

MPLS VPN Smart Plug-in (SPI) を既存のバージョンに上書きインストールしようとしている場合は、インストールを始める前に、35 ページの「MPLS VPN SPI の削除」の説明に従って既存の MPLS VPN SPI を削除してください。

今回の MPLS VPN SPI のインストールが旧バージョンからのアップデートである場合は、26 ページの「MPLS VPN SPI の旧バージョンからの SAA テスト定義のアップデート」を参照してください。

MPLS VPN SPI で問題が発生したときのチェック項目をまとめると、次のようになります。

- Network Node Manager (NNM) がトポロジに接続できない。

  NNM のプロセスが動作していない可能性があります。

  - ❏ 23 ページの「Network Node Manager Advanced Edition が正しくインストールされていることの確認」を参照して、NNM が正しくインストールされていることを確認します。
  - ❏ 23 ページの「NNM の環境変数の設定」を参照して、NNM の環境変数に正しい値が設定されていることを確認します。
  - ❏ 75 ページの「管理ステーションで NNM のサービスが動作していることを確認する方法」を参照して、NNM のサービスが正常に動作していることを確認します。

- エッジルーターの中に、NNM トポロジまたは MPLS VPN ビューに表示されないものがある。

  NNM がそのデバイスを検出していない可能性があります。

  - ❏ loadhosts コマンドまたはシードファイルを使って、NNM がネットワーク内のすべてのエッジルーターを検出できるようにします。詳細は、『*HP OpenView ネットワークノードマネージャ ネットワーク管理ガイド*』を参照してください。
  - ❏ 78 ページの「MPLS VPN の検出が実行済みであることを確認する方法」を参照して、MPLS VPN の検出が正常に完了していることを確認します。

- MPLS VPN アラームブラウザにイベントが表示されない。

  MPLS VPN SPI が、エッジルーターに関連したイベントを受信していない可能性があります。

- ❏ 77 ページの「MIB がロードされていることを確認する方法」を参照して、必要な MIB がロードされていることを確認します。
- ❏ 管理対象デバイスが、トラップを NNM 管理ステーションへ転送するように正しく設定されていることを確認します。
  - — ルーターに SNMP でアクセスできるコンピュータを SNMP のアクセス制御を使って制限している場合は、すべてのエッジルーターのアクセスリストに、NNM 管理ステーションを追加します。
  - — すべてのエッジルーターが、SNMP トラップ送信先の 1 つとして NNM 管理ステーションを含むように設定します。
  - — これらの設定の詳細は、ルーターに付属しているドキュメントを参照してください。
- ❏ NNM 管理ステーションがデバイスからイベントを受信していることを確認します。
  - — 全アラームブラウザで、エッジルーター関連のイベントが受信できるかどうかを調べます。イベントは、インタフェースカードをネットワークから一時的に切り離すことで、簡単に生成できます。
- ❏ 36 ページの「SNMP ポーリングアクセスの設定」を参照して、NNM がエッジルーターのステータス情報をポーリングできることを確認します。
- ❏ 78 ページの「MPLS VPN の検出が実行済みであることを確認する方法」を参照して、MPLS VPN の検出が実行済みであることを確認します。
- ❏ 76 ページの「MPLS VPN SPI が動作していることを確認する方法」を参照して、MPLS VPN SPI が動作していることを確認します。

- MPLS VPN アラームブラウザに SAA テスト関連のイベントが表示されない。

  MPLS VPN SPI がエッジルーターから SAA イベントを受信していない可能性があります。

  - ❏ 管理対象デバイスが、トラップを NNM 管理ステーションへ転送するように正しく設定されていることを確認します。
    - — ルーターに SNMP でアクセスできるコンピュータを SNMP のアクセス制御を使って制限している場合は、すべてのエッジルーターのアクセスリストに、NNM 管理ステーションを追加します。
    - — すべてのエッジルーターが、SNMP トラップ送信先の 1 つとして NNM 管理ステーションを含むように設定します。
    - — これらの設定の詳細は、ルーターに付属しているドキュメントを参照してください。
  - ❏ NNM 管理ステーションがデバイスからイベントを受信していること確認します。
    - — 全アラームブラウザで、エッジルーター関連のイベントが受信できるかどうかを調べてます。イベントは、インタフェースカードをネットワークから一時的に切り離すことで、簡単に生成できます。
  - ❏ SAA テストが定義されていることを確認します。79 ページの「SAA テストの定義を確認する方法」を参照してください。
  - ❏ MPLS VPN SPI が動作していることを確認します。76 ページの「MPLS VPN SPI が動作していることを確認する方法」を参照してください。

トラブルシューティングに関する追加情報は、Web サイト `http://ovweb.external.hp.com/lpe/doc_serv` の「reporting and network solutions」製品カテゴリから最新の『*Release Notes for MPLS VPN Smart Plug-in to Network Node Manager*』と『*Release Notes for Reporting and Network Solutions*』を入手して、参照してください。

管理ステーションで NNM のサービスが動作していることを確認する方法

管理ステーションで NNM のサービスが動作していることを確認するには、次の手順を実行します。

1. 23 ページの「Network Node Manager Advanced Edition が正しくインストールされていることの確認」の説明に従って、NNM が正しくインストールされていることを確認します。
2. NNM のサービスがどのようなステータスになっているかを調べます。
   - *UNIX の場合*: **`$OV_BIN/ovstatus -v`**
   - *Windows の場合*: **`%OV_BIN%¥ovstatus -v`**

   PMD も含めて、すべてのプロセスが動作している必要があります。
3. NNM とその関連プロセスが 1 つでも動作していない場合は、NNM のサービスを停止して再起動します。
   - *UNIX の場合*:

     ```
     $OV_BIN/ovstop -c
     $OV_BIN/ovstart -c
     ```

   - *Windows の場合*:

     ```
     %OV_BIN%¥ovstop -c
     %OV_BIN%¥ovstart -c
     ```

MPLS VPN SPI が動作していることを確認する方法

管理ステーションで MPLS VPN のステータスマネージャサービスが動作していることを確認するには、次の手順を実行します。

1. MPLS VPN SPI のステータスマネージャのステータスを調べます。

   - *UNIX の場合*: **$OV_BIN/ovstatus -v**
   - *Windows の場合*: **%OV_BIN%¥ovstatus -v**

   MPLS_sm プロセスが動作している必要があります。

2. MPLS_sm プロセスまたは NNM のプロセスが 1 つでも動作していない場合は、NNM のサービスを停止して再起動します。

   - *UNIX の場合*:

     ```
     $OV_BIN/ovstop -c
     $OV_BIN/ovstart -c
     ```

   - *Windows の場合*:

     ```
     %OV_BIN%¥ovstop -c
     %OV_BIN%¥ovstart -c
     ```

MIB がロードされていることを確認する方法

NNM 管理ステーションに必要な MIB がロードされていることを確認するには、次の手順を実行します。

1. NNM の GUI (ovw) で、[オプション -> ロード / アンロード MIB : SNMP] をクリックします。

   [ロード / アンロード MIB : SNMP] ウィンドウが開き、そこに NNM 管理ステーションにロードされている MIB のリストが示されます。

2. 24 ページの「MIB の要件」に示されている MIB がロードされていることを確認します。

3. 必要な MIB がロードされていない場合は、このウィンドウを使って追加します。

   詳細は、『*HP OpenView ネットワークノードマネージャ ネットワーク管理ガイド*』を参照してください。

MPLS VPN の検出が実行済みであることを確認する方法

MPLS VPN SPI が MPLS VPN ネットワーク内の一部のルーターをまだ検出していないと考えられる場合は、MPLS VPN 検出エージェントのステータスを調べます。

- *UNIX の場合*:

```
$OV_BIN/ovstatus -v ovet_daCiscoMplsVpn
$OV_BIN/ovstatus -v ovet_daJunMplsVpn
```

- *Windows の場合*:

```
%OV_BIN%¥ovstatus -v ovet_daCiscoMplsVpn
%OV_BIN%¥ovstatus -v ovet_daJunMplsVpn
```

ステータス出力の `last message` の部分が、MPLS VPN 検出エージェントの現在の状態を表しています。

- このメッセージの内容が検出処理の 1 手順を示していれば、MPLS VPN はまだ検出の途中です。検出処理が完了するのを待って、MPLS VPN ビューにすべての MPLS VPN デバイスが表示されていることを確認します。
- このメッセージが「次回検出サイクルまで待機中」であれば、MPLS VPN 検出エージェントは検出をすでに完了して次の検出サイクルまで待機しています。loadhosts コマンドまたはシードファイルを使って、NNM が MPLS VPN ネットワーク内のすべてのルーターを検出できるようにします。詳細は、『*HP OpenView ネットワークノードマネージャネットワーク管理ガイド*』を参照してください。
- このメッセージがエラー状態を示している場合は、Extended Topology による検出を再起動します。詳細は、『*Extended Topology によるネットワーク管理ガイド*』を参照してください。

SAA テストの定義を確認する方法

MPLS VPN SPI が PE ルーターに設定する SAA テストの定義は、saa_tag.xml ファイルと saa.conf ファイルに保存されています。saa_tag.xml ファイルの方は、テスト定義が XML 形式で保存されています。

SAA テストが定義されていることを確認するには、次のファイルが存在しているかどうかを調べます。

- *UNIX の場合*: $OV_DB/saa_tag.xml saa.conf
- *Windows の場合*: %OV_DB%¥saa_tag.xml saa.conf

saa_tag.xml ファイルを再作成する

saa.conf ファイルが存在していても、saa_tag.xml ファイルが存在していないかまたはそのサイズが 0 である場合は、次の手順を実行して、saa_tag.xml ファイルを再作成します。

1. 現在の SAA テストの定義をファイルにエクスポートします。
   - *UNIX の場合*:

     $OV_BIN/saa_config.ovpl -e /tmp/current_saa.txt
   - *Windows の場合*:

     %OV_BIN%¥saa_config.ovpl -e C:¥temp¥current_saa.txt
2. temp_current_saa.txt ファイルを編集し、どれか 1 つのテスト定義について、OP パラメータの値を MODIFY に変更します。
3. 編集したファイルをインポートします。
   - *UNIX の場合*:

     $OV_BIN/saa_config.ovpl -i /tmp/current_saa.txt
   - *Windows の場合*:

     %OV_BIN%¥saa_config.ovpl -i C:¥temp¥current_saa.txt

   saa_tag.xml ファイルが作成されていて、しかもサイズが 0 になっていないことを確認します。

注記 saa_tag.xml は、MPLS VPN SPI が内部処理に使うファイルです。このファイルは編集しないでください。

saa.conf ファイルを再作成する

saa.conf ファイルが存在していないか、存在していてもサイズが 0 の場合は、次の手順を実行して SAA テストの定義を再作成します。

1. SAA テストのソースとなっているエッジルーターにログオンします。
2. Cisco RTTMON MIB を編集して、SAA テストの設定をすべて削除します。
3. MPLS VPN ネットワーク内で SAA テストのソースとなっているすべてのエッジルーターで、手順 1 と手順 2 を繰り返します。
4. mpls.conf ファイルに定義されている SAA_TRIG パラメータの値が true に設定されていることを確認します。66 ページの「SAA 設定パラメータの設定方法」を参照してください。
5. Extended Topology による検出を起動して、MPLS VPN のトポロジを再検出します。MPLS VPN の検出が完了すると、NNM によって saa.conf が作成されます。

   検出の開始方法は、『*Extended Topology によるネットワーク管理ガイド*』を参照してください。

その他の問題の対処方法

ここでは、MPLS VPN SPI の使用中に発生する可能性があるエラーを挙げて、その対処方法を説明します。72 ページの「トラブルシューティングのチェックリスト」のどの状況にも当てはまらない場合には、このセクションを参照してください。

エッジルーターをリブートすると、SAA MIB にあった SAA テストの定義が消えてしまう

注記　この問題が発生するのは Cisco ルーターだけです。

SAA テストの定義が消えるのを防ぐ方法はありません。

この状況の回避策 :

- エッジルーターをリブートする前に、そのルーターで次の IOS コマンドを実行します。

  `write mem`

  このコマンドを実行すると、ルーターがブートする過程で SAA テストの定義が再ロードされます。

NNM で PE ルーターのシンボルが赤色で表示される

赤色表示は、デバイスが危険域ステータスになっていることを示しています。このステータスは NNM が管理しており、MPLS VPN SPI では管理していません。

このステータスインジケータの表示が誤っていると思われる場合は、このノードに対してデマンドポーリングを実行し、NNM に最新のステータス情報を表示させます。

- *UNIX の場合* : **`$OV_BIN/nmdemandpoll`** ***`nodename`***
- *Windows の場合* : **`%OV_BIN%¥nmdemandpoll`** ***`nodename`***

NNM は SNMP を使って *nodename* に照会し、そのノード上のインタフェースカードのステータスをアップデートします。インタフェースカードのステータスは、そのインタフェースカードが実装されている PE ルーターのシンボルの色に反映されます。

PE ルーターのシンボルが、ひし形ではなく四角形で表示される

四角形のシンボルは、LAN カードが 1 枚しか実装されていないコンピュータを表しています。一方、ひし形のシンボルは、複数の LAN カードが実装されているルーターを表しています。つまり、PE ルーターのシンボルが四角形になっている場合は、NNM が 1 枚の LAN カードの情報しか把握していないことを示しています。したがって、このケースでは、残りの LAN カードについての情報を取得するための SNMP リクエストが成功していないと考えられます。このルーターに SNMP で接続できることを確認してください。

- *UNIX の場合*: **$OV_BIN¥snmpwalk *nodename* system**
- *Windows の場合*: **%OV_BIN%¥snmpwalk *nodename* system**

NNM は、指定したノードに対して snmpwalk を実行し、MIB-2 MIB のシステムセクションを調べます。

- snmpwalk が成功すると、システム変数の値が表示されます。

  LAN カードが複数枚実装されていれば、PE ルーターのシンボルはひし形に変わるはずです。

- snmpwalk が失敗すると 、「タイムアウトになるまで何も応答がありません。」というメッセージが表示されます。

  失敗した場合は、SNMP の設定データベースにその PE ルーターの Set 用コミュニティ文字列を設定して、snmpwalk を再び実行します。

VPN 名が紛らわしい

環境に合わせて意味のある VPN 名を設定することができます。44 ページの「MPLS VPN SPI 設定ファイル内の VPN 名の変更」を参照してください。

MPLS VPN の設定を変更しても、表示に反映されない

MPLS VPN の構造を変更した後、Extended Topology による検出を開始して、MPLS VPN の情報を更新します。詳細は、NNM Advanced Edition に付属している『*Extended Topology によるネットワーク管理ガイド*』を参照してください。

サポート用の情報の収集

本ガイドに書かれていないエラーが発生した場合は、システムや設定に関する情報を次の手順で収集し、問題を当社のサポート担当者へご連絡ください。

1. エラーの情報を書き留めます。
2. NNM が動作していることを確認します。確認の方法は、75 ページの「管理ステーションで NNM のサービスが動作していることを確認する方法」を参照してください。
3. 次の情報を収集して、当社のサポート担当者にお送りください。

   - データファイルと設定ファイル

     UNIX の場合:

     — `$OV_DB/Vpn_Info.xml`

     — `$OV_CONF/VpnNames.txt`

     — `$OV_CONF/mpls.conf`

     Windows の場合:

     — `%OV_DB%¥Vpn_Info.xml`

     — `%OV_CONF%¥VpnNames.txt`

     — `%OV_CONF%¥mpls.conf`

   - SAA のエクスポートファイル (`current_saa.txt`)

     エクスポートファイルを作成します。

     — *UNIX の場合*:

     `$OV_BIN/saa_config.ovpl -e /tmp/current_saa.txt`

     — *Windows の場合*:

     `%OV_BIN%¥saa_config.ovpl -e C:¥temp¥current_saa.txt`

- ファイル ovobjprint.output

  出力ファイルを作成します。

  — *UNIX の場合*:

  ```
  $OV_BIN/ovobjprint > /tmp/ovobjprint.output
  ```

  — *Windows の場合*:

  ```
  %OV_BIN%¥ovobjprint > C:¥temp¥ovobjprint.output
  ```

- 使用している MPLS VPN ネットワークのトポロジ情報。次の情報を含めてください。
  - 接続情報
  - 名前と IP アドレス
- VPN 情報
  - PE ルーター、VRF、およびインタフェースの相互関係
  - VPN の詳細 (どの PE ルーターのどの VRF がどの VPN に対応するか)
- スクリーンショット (参考になると思われるものがある場合)
  - イベント表示中のアラームブラウザ

    (ブラウザのカラム幅を変更して、イベントメッセージテキストができるだけ多く表示されるようにしてください。)
  - NNM のサブマップ
- ネットワークの現在のステータス
  - すべて動作しているか ?
  - 上記のデータを収集している最中にインタフェースやルーターでシャットダウンしたものがあったか ?
- PE ルーターの情報。次の情報を含めてください。
  - ベンダー名 (たとえば、Cisco)
  - モデル名 (たとえば、Catalyst 6509)
  - IOS のバージョン