HP OpenView 报告与网络解决方案

网络节点管理器

MPLS VPN 智能插件
用户指南

软件版本：2.1

适用于 HP-UX、 Solaris 和 Windows® 操作系统

生产部件号： 无
2004 年 7 月

法律公告

保修。

对与本文档有关的内容，包括但不限于对用于任何特定目的商销性和适应性所包含的保证，惠普公司不做任何担保。对于此处包含的错误或与本书的提供、执行或使用有关的直接、间接、附带性或后果性损失，惠普公司概不负责。

可以从当地销售和服务办事处，获取适用于您的惠普产品的具体保修条款副本。

限定权利图例。

美国政府使用、复制或公开本产品，必须符合 DFARS 252.227-7013 的技术数据和计算机软件权利条款 (c)(1)(ii) 小节中提出的限制规定。

美国
惠普公司

美国国防部之外的其他政府部门和机构的权利，应符合 FAR 52.227-19(c)(1,2) 的规定。

版权公告。

商标公告。

Windows® 是 Microsoft 公司的美国注册商标。

UNIX® 是 Open Group 的注册商标。

目录

目录

目录

支持

请访问 HP OpenView 网站：

http://openview.hp.com/

在此您可以找到联系人信息，以及有关 HP OpenView 提供的产品、服务和支持的细节。

可以直接访问 HP OpenView 支持网站：

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

支持站点包括：

- 可下载的文档
- 疑难解答信息
- 补丁和更新
- 问题报告
- 培训信息
- 支持计划信息

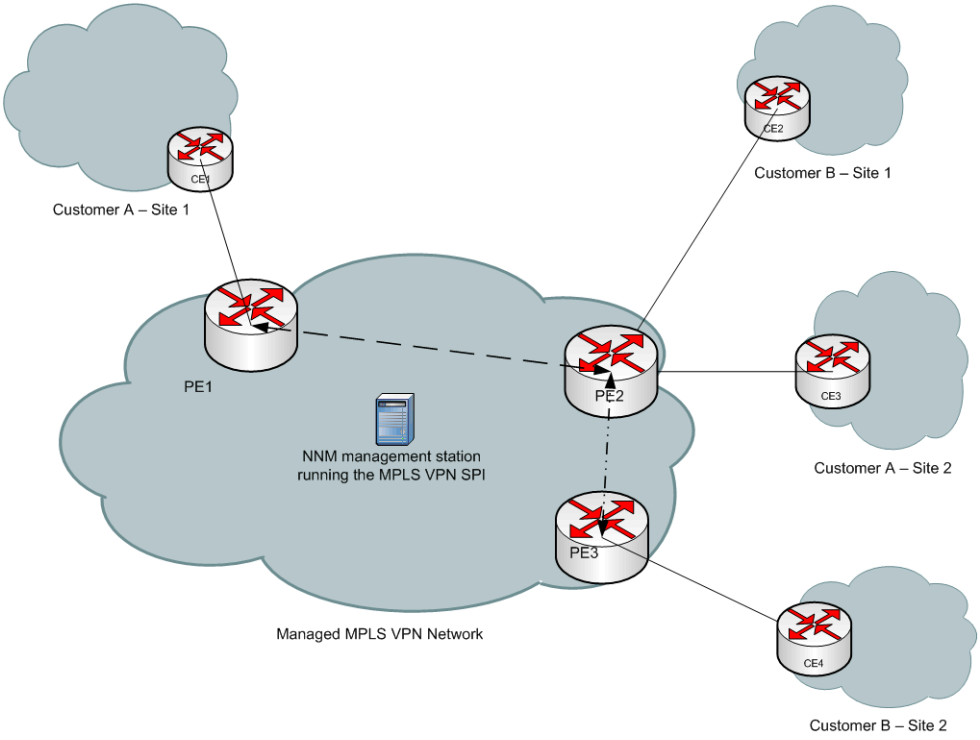
1 介绍 MPLS VPN 智能插件

引言

拥有 IP 主干网的 internet 服务提供商，可以使用多协议标号切换 （MPLS）技术，向客户提供虚拟专有网络 （VPN）服务。而 RFC2547bis 对 MPLS 进行了定义。只有当某个包含客户网络内部的两个站点的 VPN 存在时，这两个站点才能在公共主干网上实现 IP 连通性。没有共同的 VPN，这两个站点就无法在主干网上实现 IP 连通性。

通过服务提供商的边缘路由器上的虚拟路由转发表 （VRF），可以定义 MPLS VPN。VRF 代表由一个或多个路由器支持的 VPN 的实例。来自所有网络设备的匹配的 VRF 的集合，构成了实际的 VPN。图 1-1 显示 MPLS VPN 网络的示例。

图 1-1 MPLS VPN 网络的示例



HP OpenView 网络节点管理器 MPLS VPN 智能插件 （SPI），通过近实时监视 MPLS VPN 边缘路由器，向 HP OpenView 网络节点管理器 (NNM) 提供增值服务功能。提供商边缘 （PE）路由器，位于服务提供商网络的周边。它们与位于 MPLS VPN 云中的提供商 （P）路由器和服务提供商的客户管理的客户边缘路由器进行通信。 MPLS VPN SPI 监视核心 MPLS 网络内部扮演 VPN 角色的 PE 路由器之间的连通性，并搜索 VPN 网络拓扑。它利用这一信息，映射原始节点、 PE 接口和影响 VPN 服务事件相关的陷阱信号。

MPLS VPN SPI 采用事件浓缩进程，识别事件之间的关系，浓缩事件包含的数据，从而生成数量较少的新事件，每个事件将拥有同样或更加详细的信息内容。这些事件有助于更有效地理解和处理网络出现的问题。加快反应速度，既可以缩短修复 MPLS VPN 网络内部的 （MTTR）问题的平均时间，还能够提升服务质量。

有关 MPLS VPN SPI 支持的边缘路由器设备的列表，请参阅第 24 页上的“路由器需求”。

除了近实时诊断 PE 和 CE 路由器基础结构问题之外， MPLS VPN SPI 还允许监视扮演 VPN 角色的两个 PE 路由器之间的端到端路径的可访问性。这种监视手段的实现，采用的是基于思科 RTTMON MIB 的思科服务保障代理程序 （SAA）测试。 MPLS VPN SPI 配置 PE 路由器之间的 SAA 回声测试，以测试跨边缘路由器的可访问性。这种测试不但可以实时监视 PE-PE 连接，而且如果出现故障，还能生成 SNMP 事件。 MPLS VPN SPI 还支持两个 CE 路由器之间的用户配置的端到端可访问性测试。

当 HP OpenView 性能洞察 (OVPI) 与 NNM 集成时， MPLS VPN SPI 就能与 NNM 和 OVPI 一起协作，预防性地提供故障和性能数据分析报告。

MPLS VPN SPI 的功能和优点

下面的列表列举了 MPLS VPN SPI 的功能与优点：

- MPLS VPN SPI 不但监视 MPLS VPN 网络中 PE 路由器的状态，而且报告设备停机状态。
- 对于服务提供商可以访问的每个 CE 路由器， MPLS VPN SPI 监视 CE 路由器和 PE-CE 连接的状态。
- 借助浓缩网络状态事件， MPLS VPN SPI 生成更适合于在 NNM 警报浏览器中显示的更有意义的新事件。
- 作为任选项， MPLS VPN SPI 可以自动配置对 VPN 内部有效的 PE-PE 路由器对进行可访问性测试。
- MPLS VPN SPI 允许用户配置不同类型的 PE 特定和 CE 特定可访问性测试，并生成各种事件来指明被测连接的变化。
- OVPI 安装之后， OVPI 就可以监视载波访问速率、 SAA 和 MPLS VPN 计数器。当任何计数器超越配置的阈值时，就向 NNM 发送陷阱信号。NNM 警报浏览器将此陷阱信号显示为一个警报，借助它可以启动 OVPI 报告，其中包含有关超越阈值的接口的其他信息。

MPLS VPN SPI 的行为

MPLS VPN SPI 探测和报告 MPLS VPN 网络的各种问题。MPLS VPN SPI 探测和分析的事件与陷阱信号的类型包括：

- PE 路由器的节点和接口状态变化陷阱信号
- CE 路由器的节点和接口状态变化陷阱信号
- PE-PE、 PE-CE 和 CE-CE 可访问性测试的 SAA 回声测试事件
- MPLS VPN、 SAA 和 CAR 阈值突破的 OVPI 阈值超越陷阱信号

MPLS VPN SPI 浓缩这些陷阱信号，并根据所影响的服务将它们转换成各种事件。这些事件标识 VPN 服务中影响的 VRF。

与 MPLS VPN SPI 的用户接口

用户可以用多种方式监视 MPLS VPN 网络的状态：

- 通过监视 MPLS VPN 警报分类中的警报，观察有关影响一个或多个 VPN 状态的情况的警报。参见第 14 页上的 “MPLS VPN 事件”。
- 借助 MPLS VPN 视图中可用的各种窗口，检查 MPLS VPN 网络的图形和表格表达形式。参见第 16 页上的 “MPLS VPN 视图”。
- 当安装 OVPI 和 MPLS VPN 报告包时，通过交叉启动 OVPI，创建关于 MPLS VPN 网络的活动的报告。参见第 16 页上的 “来自 OVPI 的报告”。

MPLS VPN 事件

MPLS VPN SPI 生成的事件，出现在 NNM 警报浏览器的 MPLS VPN 分类中。双击 MPLS VPN 分类，以打开 MPLS VPN 浏览器。

当 MPLS VPN SPI 探测到 MPLS VPN 故障时，它就生成下列事件之一：

- `MPLS/VPN: VPN:VRF [VRF] Down due to [interface] IF down on node [node].`
- `MPLS/VPN: VPN:VRF(s) [VRFlist] Down due to node [node] down.`
- `MPLS/VPN: VPN:VRF(s) [VRFlist] Down due to card [card] down.`
- `MPLS/VPN: VPN:VRF(s) [VRFlist] Unknown status due to node [node] unknown status`
- `MPLS/VPN: SAA test failed between [node1-node2] affected VPN/VRF(s):[VRFlist]. Root cause is cause.`
- `MPLS/VPN: SAA test cleared between [node1-node2] affected VPN/VRF(s):[VRFlist]`
- `MPLS/VPN: VPN:VRF [VRF] Down due to [interface] IF ADDRESS down on node [node]`

- `MPLS/VPN: VPN:VRF [VRF] Down due to connection down between [source_node:interface] and [destination_node:interface]`

后续某些示例消息：

??? 必须对失败的 SAA 测试添加根本原因示例 ???

```
MPLS/VPN: VPN:VRF [Red_: Red_West] Down due to [Se0/0] IF down on node [mplspe04.cnd.hp.com]

MPLS/VPN: VPN:VRF [Red_: Red_West Blue:Blue] Down due to node [mplspe04.cnd.hp.com] down

MPLS/VPN: VPN:VRF [Red_: Red_West Blue:Blue] Down due to card [card1] down

MPLS/VPN: SAA test failed between [mplspe04.cnd.hp.com-mplspe01.cnd.hp.com] affected VPN/VRF:[Red_:Red_West-Red_East]. Root cause is Connectivity Failure between mplspe04.cnd.hp.com and mplspe01.cnd.hp.com.

MPLS/VPN: VPN:VRF [Red_: Red_West] Down due to [Se0/0] IF ADDRESS down on node [mplspe04.cnd.hp.com]

MPLS/VPN: VPN:VRF [Red_: Red_West] Down due to connection down between [mplspe04.cnd.hp.com:Se0/0] and [mplspe01.cnd.hp.com:Se0/0]

MPLS/VPN: VPN:VRF [Red_: Red_West] Unknown status due to node [mplspe04.cnd.hp.com] unknown status
```

MPLS VPN 警报的消息字段指出已经出现 MPLS VPN 故障的性质。它还包含下列信息：

- 受停机影响的每个 VPN 中受影响的 VRF 的列表。只影响一个 VRF 的接口关闭条件。可以影响多个 VRF 的节点关闭条件。

  例如，`[Red_:Red_West Blue:Blue]` 表示，停机影响了 Red_ VPN 上的 Red_West VRF，以及 Blue VPN 上的 Blue VRF。

- 处于停机状态的边缘路由器的节点名称。例如，`[mplspe04.cnd.hp.com]`。

  或者

  SAA 可访问性测试中边缘路由器节点的名称。例如，`[mplspe04.cnd.hp.com-mplspe01.cnd.hp.com]`。

- 如果可行，提供边缘路由器上停机接口的名称。例如，`[Se0/0]`。

MPLS VPN 视图

MPLS VPN SPI 可以提供若干视图：

- MPLS VPN 视图 — MPLS VPN 网络中 VPN 的列表。
- MPLS VPN 路由器清单 — MPLS VPN 网络中 MPLS VPN 路由器的列表。
- MPLS VPN 详细 — 指定 VPN 中所有可访问的 PE 和 CE 路由器的图表视图。
- PE 详细 — 为指定 PE 路由器定义的 VRF 的描述信息，包括每个 VRF 参与的 VPN。
- VRF 详细 — 指定 VRF 中 PE 和 CE 路由器的描述信息。

有关每个视图中可用的功能和视图之间导航的信息，参见与 MPLS VPN SPI. 一起安装的在线帮助。

启动 MPLS VPN 视图

访问 MPLS VPN 视图可以采用下列方式：

- 若要从 NNM GUI (ovw) 打开 MPLS VPN 视图，单击 工具：视图 ->MPLS VPN.
- 若要从首页打开 MPLS VPN 视图，请在列表中选择 MPLS VPN 视图，然后单击启动。
- 若要从任何视图打开 MPLS VPN 视图，请单击 工具：视图 ->MPLS VPN。

来自 OVPI 的报告

如果已经将 MPLS VPN 和 SAA 报告包安装到 OVPI 服务器上，并安装了 NNM / OVPI 集成模块，那么可以有几种方式来启动来自 OVPI 的报告，获取 NNM. 的 MPLS VPN 信息。下面介绍这些启动方式。

从 NNM 警报浏览器交叉启动 OVPI

若要从 NNM 警报浏览器启动 OVPI，请执行下列步骤：

1. 从 MPLS VPN 警报浏览器选择警报，然后单击动作 -> 其他动作。
2. 在动作列表中，单击 `OVPI` 报告。
3. 单击确定。

   web 浏览器窗口将出现 OVPI 报告，其中包括针对生成此警报的对象预先过滤的信息。

从 NNM GUI (ovw) 交叉启动 OVPI

??? 纳入该案例确实有意义吗？用户真的不喜欢启动来自 MPLS VPN 视图的报告吗？
我特意制作了这一过程。请确认其所有细节 ???

若要从 NNM GUI (ovw) 启动 OVPI，请执行下列步骤：

1. 在 NNM 映射中，选择表示 MPLS VPN 网络中路由器的节点或接口图标，并单击动作 -> 其他动作。
2. 在 动作列表中，单击 `OVPI` 报告。
3. 单击确定。

   web 浏览器窗口出现 `Report Launchpad` 内容。
4. 在 `Report Launchpad` 中，单击待查看的报告。

从扩展拓扑映射中交叉启动 OVPI

??? 纳入该案例确实有意义吗？用户真的不喜欢启动来自 MPLS VPN 视图的报告吗？
我特意制作了这一过程。请确认其所有细节。必须从 Meer 输入吗 ???

若要从扩展拓扑映射启动 OVPI，请执行下列步骤：

1. 在扩展拓扑映射中，选择表示 MPLS VPN 网络中路由器的节点图标，并单击动作 -> 其他动作。
2. 在动作列表中，单击 `OVPI` 报告。
3. 单击确定。

   web 浏览器窗口出现 `Report Launchpad` 内容。

4. 在 Report Launchpad 中，单击待查看的报告。

从 MPLS VPN 视图交叉启动 OVPI

若要从 MPLS VPN 视图启动 OVPI，请执行下列步骤：

1. 在 MPLS VPN 视图中，在列表中选择 `OVPI` 报告，然后单击启动。

   web 浏览器窗口将出现包含 `Report Launchpad` 的内容，您可以选择待查看的报告。

相关文档

有关详情，请参阅下列文档：

- 用 HP OpenView 管理您的网络网络节点管理器
- 使用扩展拓扑
- MPLS VPN 报告包用户指南
- SAA 报告包用户指南

2 安装 MPLS VPN 智能插件

安装准备

安装 MPLS VPN 智能插件 （SPI）之前，既要验证计算机满足软硬件需求，又要验证已经正确设置了软件的先决条件。

硬件需求

在安装 MPLS VPN SPI 之前，验证配置了下列硬盘空间：

表 2-1 推荐的硬盘空间设置

位置	大小
UNIX: $OV_MAIN_PATH Windows: %OV_MAIN_PATH%	2 MB

软件需求

支持的操作系统

支持下列操作系统：

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

网络节点管理器

验证下列软件和所有先决条件与补丁，都已安装在被管环境的所有系统上：

- HP OpenView 网络节点管理器高级版，版本 7.5

关于如何安装 NNM 产品的指示信息，参见网络节点管理器安装指南。

验证正确安装了网络节点管理器高级版

若要验证 NNM 高级版 产品是否安装，请执行下列步骤：

UNIX:

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

Windows:

1. 从开始 菜单，启动控制面板。
2. 双击添加 / 删除程序。
3. 验证 HP OpenView 网络节点管理器被预先发送到程序列表中。

确定安装了哪个版本的 NNM

若要确定安装了哪个版本的 NNM：

UNIX: `/opt/OV/bin/ovnnmversion`

Windows: `install_dir\bin\ovnnmversion`

设置 NNM 环境变量

若要确定 NNM 环境变量的来源：

- UNIX 使用 sh 或 ksh: `. /opt/OV/bin/ov.envvars.sh`
- UNIX 使用 csh: `source /opt/OV/bin/ov.envvars.csh`
- Windows：在命令窗口内运行 `install_dir\bin\ov.envvars.bat`

这一步设置 MPLS VPN SPI 要求的环境变量，包括：

- UNIX: `$OV_BIN`, `$OV_LRF`, `$OV_CONF`, `$OV_MAIN_PATH`
- Windows: `%OV_BIN%`, `%OV_LRF%`, `%OV_CONF%`, `%OV_MAIN_PATH%`

MIB 附件

必须加载下列 MIB， MPLS VPN SPI 才能正常工作：

- 思科 SMI MIB — 连同 NNM 一起交付和安装到下列位置：

  UNIX: `$OV_SNMP_MIBS/Vendor/Cisco/CISCO-SMI.my`
  Windows: `%OV_SNMP_MIBS%\Vendor\Cisco\CISCO-SMI.my`

- 思科 RTTMON MIB — 连同 MPLS VPN SPI 一起交付和安装到下列位置：

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

- Juniper SMI MIB — 与 MPLS VPN SPI 一同交付，并安装到下列位置：

  UNIX: `$OV_SNMP_MIBS/Vendor/Juniper/jnx-smi.mib`
  Windows: `%OV_SNMP_MIBS%\Vendor\Juniper\jnx-smi.mib`

- Juniper VPN MIB — 与 MPLS VPN SPI 一同交付，并安装到下列位置：

  UNIX: `$OV_SNMP_MIBS/Vendor/Juniper/jnx-vpn.mib`
  Windows: `%OV_SNMP_MIBS%\Vendor\Juniper\jnx-vpn.mib`

如果安装 MPLS VPN SPI 之前将思科 SMI MIB 加载到 NNM 管理工作站上， MPLS VPN SPI 安装进程就加载其他所需的 MIB。否则，必须手工加载所有必需的 MIB。有关详情，参见第 75 页上的 “验证 MIB 是否加载”。

注释

在 Windows 操作系统下， `Typical` NNM 安装选项并没有加载思科 SMI MIB。可以选择 `Custom` NNM 安装选项，并指定加载 SNMP MIB。作为备选方案，也可以加载 MIB。详见第 75 页上的 “验证 MIB 是否加载”。

路由器需求

此版本的 MPLS VPN SPI 发现并管理以下类型的路由器设备：

- 采用 Internetwork 操作系统 (IOS) 版本 12.2(15)T，支持 MplsVpnMIB 的思科路由器。

  MPLS VPN SPI 可以对这些设备执行状态管理、可访问性测试配置及可访问性状态报告。

- Juniper M 和 T 系列路由器，采用 Juniper 操作系统 (JunOS) 版本 6，支持 jnx-smi.mib 和 jnx-vpn.mib。

  MPLS VPN SPI 只能对这些设备执行状态管理。

性能洞察

作为任选项，可以在独立的服务器上安装 HP OpenView 性能洞察 (OVPI) 5.0，并使用 NNM / OVPI 集成模块，将 OVPI 的趋势分析与 NNM 的故障管理能力融为一体。如果将 OVPI 和 NNM 集成起来， OVPI 检测到的阈值超限就出现在 NNM 警报浏览器上， Report Launchpad 窗口可以访问大量的 OVPI 报告。

更新上一版本 MPLS VPN SPI 中的 SAA 测试定义

如果您已经使用上一版本的 MPLS VPN SPI 定义 SAA 测试，那么请执行下列步骤来保存您的测试配置。

1. 从被管的路由器删除现有的 SAA 测试定义

   a. 将所有现有的 SAA 测试导入文件

      - UNIX:

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

      - Windows:

        ```
        %OV_BIN%\saa_config.ovpl -e C:\temp\saa_test_A
        ```

      有关详情，参见第 62 页上的 “修改 SAA 测试定义”。

   b. 使用任何文本编辑器，在 `saa_test_A` 文件中，将每个测试定义的 `OP` 参数修改为 `DELETE`。

      有关详情，参见第 64 页上的 “使用 MPLS VPN SPI 配置 SAA”。

   c. 将更新后的 SAA 测试定义导入 MPLS VPN SPI：

      - UNIX:

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

      - Windows:

        ```
        %OV_BIN%\saa_config.ovpl -i C:\temp\saa_test_A
        ```

      有关详情，参见第 62 页上的 “修改 SAA 测试定义”。

   d. 保存 `saa_test_A` 文件，以备将来参考。

2. 备份 VpnNames.txt 文件：

   - UNIX:

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

   - Windows:

     ```
     copy %OV_CONF%\VpnNames.txt C:\temp\VpnNames-A.txt
     ```

3. 删除 MPLS VPN SPI。

   有关指示信息，参见第 34 页上的 “删除 MPLS VPN SPI”。

4. 安装最新版本的 MPLS VPN SPI。

   有关指示信息，参见第 30 页上的 “安装 MPLS VPN SPI”。

5. 验证 NNM 是否已对属于一个或多个 SAA 测试源的每个边缘路由器，配置了 SNMP 设置社区字符串。

   有关指示信息，参见第 36 页上的 “配置 SNMP 访问”。

6. 触发扩展拓扑搜索，以便搜索您的网络并执行 MPLS VPN 搜索。默认情况下， MPLS VPN SPI 为您的网络配置所有可能的 PE-PE VRF 非敏感 SAA 测试。

   有关指示信息，参见第 40 页上的 “搜索进程”。

7. 更新新定义的 SAA 测试定义，以便与原先的 SAA 测试定义匹配：

   a. 将自动配置 SAA 测试导出到文件

      - UNIX:

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

      - Windows:

        ```
        %OV_BIN%\saa_config.ovpl -e C:\temp\saa_test_B
        ```

      有关详情，参见第 62 页上的 “修改 SAA 测试定义”。

注释

如果没有自动配置的 SAA 测试， saa_test_B 文件将为空白。此时，可以直接操作 saa_test_A 文件实施步骤 b 和 c。

b. 必要时，更新 SAA 测试定义文件。

使用任何文本编辑器，比较 saa_test_B 文件和 saa_test_A 文件（来自步骤 1）中定义的 SAA 测试：

- 修改 saa_test_B 文件中的测试，以便匹配 saa_test_A 文件中的相应测试。将每个测试定义的 OP 参数修改为 MODIFY
- 将 saa_test_A 文件中定义的任何其他测试添加到 saa_test_B 文件。将每个测试定义的 OP 参数修改为 ADD。

注释

与 MPLS VPN SPI 版本 1.0 相比， MPLS VPN SPI 版本 2.0 （以及更高版本）允许使用更多的 SAA 测试类型。它也使用十六进制数字标识 SAA 测试。这也不同于与先前的版本。当比较测试定义时将看到这些变化，但不影响其效果：

- saa_test_B 文件包括一个 TEST_TYPE 元素。您不必将此元素添加到版本 1.0 测试定义中。
- OV_TAG 元素，在 saa_test_B 文件中采用十六进制表示，在 saa_test_A 文件中则是十进制表示。您不必修改版本 1.0 测试定义的选项卡值。

有关详情，参见第 64 页上的 “使用 MPLS VPN SPI 配置 SAA”。

c. 将更新后的 SAA 测试定义导入 MPLS VPN SPI：

- UNIX:

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

- Windows:

  ```
  %OV_BIN%\saa_config.ovpl -i C:\temp\saa_test_B
  ```

有关详情，参见第 62 页上的 “修改 SAA 测试定义”。

8. 验证先前版本中使用的 VPN 名称是否在新版本中继续保留：

a. 比较备份文件 `VpnNames-A.txt` （来自步骤 2）和新的 VPN 名称文件：

- UNIX: `$OV_CONF/VpnNames.txt`
- Windows: `%OV_CONF%\VpnNames.txt`

b. 必要时，编辑 `VpnNames.txt` 文件，以便匹配原先版本的 VPN 名称。只修改 VPN 名称。

有关详情，参见第 44 页上的 “在 MPLS VPN SPI 配置中更改 VPN 名称”。

安装 MPLS VPN SPI

如果执行上述安装遇到问题，请参见第 69 页上的第 6 章 “MPLS VPN 智能插件疑难解答”或网络节点管理器 MPLS VPN 智能插件发布通知，以寻求可能的帮助。

重要信息

如果现在正在安装 MPLS VPN SPI，那么试图安装 MPLS VPN SPI 之前，请启用 NNM 扩展拓扑。有关特定指示信息，参见纳入 NNM 高级版的使用扩展拓扑指南。

注释

如果正在现有的 MPLS VPN SPI 上覆盖安装 MPLS VPN SPI，请参见第 26 页上的 “更新上一版本 MPLS VPN SPI 中的 SAA 测试定义”，以获取特定的指示信息。

在 UNIX 操作系统上安装 MPLS VPN SPI

若要将 MPLS VPN SPI 安装到 UNIX® 操作系统上，请执行下列步骤：

1. 将 NNM 管理工作站登录为用户 `root`。
2. 验证 NNM 环境变量来源是否合适。

   有关指示信息，参见第 23 页上的 “设置 NNM 环境变量”。
3. 如果正在使用 Oracle 数据库作为 NNM 数据仓库，请执行下列步骤配置 MPLS VPN SPI 用的 Oracle：

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

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

   c. 使用任何文本编辑器，从 `UpdateColumn.xslt` 文件的第 36 行删除单词 `COLUMN`。
4. 安装报告与网络解决方案光盘

5. 从报告与网络解决方案光盘目录，启动安装

   安装脚本验证目标系统已经安装了正确版本的 NNM。如果没有安装 NNM，就退出安装脚本，返回一个出错信息。有关详情，参见第 79 页上的 “处理其他问题”。

6. 遵循屏幕上的指示，安装 MPLS VPN SPI。表 2-2 列举了安装进程期间需要进行的决策。

表 2-2　　MPLS VPN SPI UNIX 安装选项

选项	描述
安装产品类型列表	选择安装 NNM 智能插件。
安装的 SPI 列表	选择安装 MPLS VPN SPI。
启动 MPLS VPN 搜索吗？	输入 yes，启动扩展拓扑搜索，在安装结束时纳入 MPLS VPN 搜索。 输入 no，离开 MPLS VPN 网络不进行搜索。如果输入 no，直到下次运行扩展拓扑搜索时才搜索 MPLS VPN 网络。参见第 40 页上的 “搜索进程”。
每个 MPLS VPN 搜索周期结束时配置 SAA 测试吗？	输入 yes，在 MPLS VPN 搜索完成之后，让 MPLS VPN SPI 利用 SAA 测试定义，自动更新每个被管 PE 路由器上的 SAA MIB。如果输入 yes，一定要确保 SNMP 配置数据库包含每个 PE 路由器的设置社区字符串。参见第 35 页上的 “初始配置”。 输入 no，防止自动更新 SAA MIB。如果输入 no，MPLS VPN SPI 只能依靠显式命令来更新 SAA MIB。参见第 63 页上的 “SAA 配置”。 可以修改自动配置设置。参见第 63 页上的 “设置 SAA 配置参数”。
SAA 测试频率	输入 SAA 测试执行之间的秒数。默认值是 600 秒 （10 分钟）。 可以修改 SAA 测试频率。参见第 63 页上的 “设置 SAA 配置参数”。
SAA 测试超时	输入 SAA 测试超时之前的毫秒数。默认值是 100 毫秒。 可以修改 SAA 测试超时值。参见第 63 页上的 “设置 SAA 配置参数”。

在 Windows 操作系统上安装 MPLS VPN SPI

若要将 MPLS VPN SPI 安装到 Windows 操作系统上，请执行下列步骤：

1. 将 NNM 管理工作站登录为用户 `administrator`。
2. 验证 NNM 环境变量来源是否合适。

   有关指示信息，参见第 23 页上的 “设置 NNM 环境变量”。
3. 如果正在使用 Oracle 数据库作为 NNM 数据仓库，请执行下列步骤配置 MPLS VPN SPI 用的 Oracle：

   a. `cd %OV_CONF%\nnmet\topology\extensibility`

   b. `copy UpdateColumn.xslt UpdateColumn.xslt.orig`

   c. 使用任何文本编辑器，从 `UpdateColumn.xslt` 文件的第 36 行删除单词 `COLUMN`。
4. 将报告与网络解决方案光盘插入光驱：
5. 光驱应当自动启动。如果没有自动启动，就进入报告与网络解决方案目录，然后双击 `setup.bat`。

   安装脚本验证目标系统已经安装了正确版本的 NNM。如果没有安装 NNM，就退出安装脚本，返回一个出错信息。有关详情，参见第 79 页上的 “处理其他问题”。
6. 请遵循屏幕上的指示，安装 MPLS VPN SPI。表 2-3 列举了安装进程期间需要进行的决策。

表 2-3 MPLS VPN SPI Windows 安装选项

选项	描述
安装的产品类型列表	选择安装 NNM 智能插件。
安装的 SPI 列表	选择安装 MPLS VPN SPI。
启动 MPLS VPN 搜索吗？	输入 yes，启动扩展拓扑搜索，在安装结束时纳入 MPLS VPN 搜索。 输入 no，离开 MPLS VPN 网络不进行搜索。如果输入 no，直到下次运行扩展拓扑搜索时才搜索 MPLS VPN 网络。参见第 40 页上的 “搜索进程”。

表 2-3 MPLS VPN SPI Windows 安装选项 （续）

选项	描述
每个 MPLS VPN 搜索周期结束时配置 SAA 测试吗？	输入 yes，在 MPLS VPN 搜索完成之后，让 MPLS VPN SPI 利用 SAA 测试定义，自动更新每个被管 PE 路由器上的 SAA MIB。如果输入 yes，一定要确保 SNMP 配置数据库包含每个 PE 路由器的设置社区字符串。参见第 35 页上的“初始配置”。 输入 no，防止自动更新 SAA MIB。如果输入 no， MPLS VPN SPI 只能依靠显式命令来更新 SAA MIB。参见第 63 页上的“SAA 配置”。 可以修改自动配置设置。参见第 63 页上的 “设置 SAA 配置参数”。
SAA 测试频率	输入 SAA 测试执行之间的秒数。默认值是 600 秒 （10 分钟）。 可以修改 SAA 测试频率。参见第 63 页上的“设置 SAA 配置参数”。
SAA 测试超时	输入 SAA 测试超时之前的毫秒数。默认值是 100 毫秒。 可以修改 SAA 测试超时值。参见第 63 页上的“设置 SAA 配置参数”。

注释 这一安装进程创建了 `C:\tempschlist` 文件。安装进程完成之后这个文件就不再使用。可以很安全地将它删除。

删除 MPLS VPN SPI

注释

删除 MPLS VPN SPI 并不能从 NNM 警报浏览器中删除 MPLS VPN 警报。如果您不再需要这些警报，那么使用警报浏览器手动进行删除即可删除此功能。

在 UNIX 操作系统上删除 MPLS VPN SPI

若要删除 UNIX 操作系统上的 MPLS VPN SPI，请执行下列步骤：

1. 将 NNM 管理工作站登录为用户 `root`。
2. 撤消配置并删除 MPLS VPN SPI：

   ```
   mpls_unconfig.ovpl
   ```

3. 只有在 Solaris 操作系统上，输入命令：

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

删除 Windows 操作系统上的 MPLS VPN SPI

若要删除 Windows 操作系统上的 MPLS VPN SPI，请执行下列步骤：

1. 将 NNM 管理工作站登录为用户 `administrator`。
2. 撤消配置并删除 MPLS VPN SPI：

   ```
   mpls_unconfig.ovpl
   ```

注释

这一删除进程创建了 `C:\tempschlist` 文件。删除进程完成之后这个文件就不再使用。可以很安全地将它删除。

初始配置

MPLS VPN SPI 使用 NNM 高级版功能，监视多协议标号切换 （MPLS VPN）环境下虚拟专有网络的状态。

配置 SNMP 轮询访问

MPLS VPN SPI 依靠 NNM，了解 MPLS VPN 网络中提供商边缘 （PE）和客户边缘 （CE）路由器的节点和接口的正确状态。 NNM 使用执行状态轮询的 netmon 进程来确定状态信息。 netmon 必须知道并能够访问每个节点和接口。

若要配置对边缘路由器的 SNMP 轮询访问，请执行下列步骤：

1. 对每个接口卡，确定需要的配置动作：
   - 如果接口卡的 IP 地址可以由管理工作站直接访问，就验证接口卡是否显示在 NNM 拓扑视图中。

     netmon 使用 ICMP 回声请求来确定接口卡的状态。您不必进行任何其他的配置工作。
   - 如果接口卡的 IP 地址**不**能从管理工作站直接访问，请将 IP 地址添加到 `netmon.snmpStatus` 文件，详见步骤 2。
   - 如果接口卡**没有** IP 地址，就将被管节点的 IP 地址添加到 `netmon.snmpStatus` 文件，详见步骤 2。
2. 正如步骤 1 所确定的那样，将 IP 地址信息添加到 `netmon.snmpStatus` 文件。该文件位于下列目录：

   UNIX: `$OV_CONF`
   Windows: `%OV_CONF%`

   a. 如果 `netmon.snmpStatus` 文件不存在，就在指定目录中创建该文件。

b. 如果可能，请添加 IP 地址通配符，以便覆盖 NNM 管理工作站不能直接访问的多个 IP 地址。

使用单独一行表示每个 IP 地址通配符条目。

c. 必要时，添加特定的 IP 地址，来表示不属于指定 IP 地址通配符范围的接口卡和被管节点。

使用单独一行表示每个指定的 IP 地址条目

d. 有关文件详情，参见 UNIX 手册页 `netmon.snmpStatus`，或者 Windows 在线帮助信息。

netmon 使用 ifIndex、 ifOperStatus 和 ifAdminStatus MIB 对象的 SNMP 请求，来确定这些接口卡的状态。

配置 SNMP 访问

MPLS VPN SPI 需要 SNMP 访问 MPLS VPN 环境下的被管设备

注释

这一访问是自动配置 SAA 回声测试的必要条件。如果没有指定边缘路由器的设置社区字符串，就必须直接配置该路由器的 SAA 回声测试。有关指示信息，参见第 66 页上的 “使用思科 IOS 命令配置 SAA”。

若要用所有边缘路由器的 SNMP 设置字符串配置 SNMP 配置数据库，请执行下列步骤：

1. 启动 SNMP 配置实用程序：
   - UNIX: `$OV_BIN/xnmsnmpconf`
   - Windows: `%OV_BIN%\xnmsnmpconf`
2. 在 `SNMP` 配置窗口，指定每个边缘路由器的设置社区字符串。

   有关详情，参见 UNIX 手册页 `xnmsnmpconf`，或者 Windows 在线帮助信息。

配置 SNMP 陷阱信号转发

MPLS VPN SPI 必须从被管的边缘设备接收陷阱信号，才能确定这些路由器的操作状态和可访问性状态。

配置每个边缘路由器，以便将 NNM 管理工作站纳入为 SNMP 陷阱信号接收者之一。有关如何执行此配置的信息，参见路由器随机提交的文档。

3 理解 MPLS VPN 探索

搜索进程

MPLS VPN 智能插件 （SPI）使用多协议标号切换 （MPLS VPN）技术，确定网络节点管理器 (NNM) 拓扑中的哪些路由器支持虚拟专有网络。 MPLS VPN SPI 执行思科路由器设备的 SNMP 查询，以确定提供商边缘 （PE）路由器配置和虚拟路由转发 （VRF）分组。此外，它还使用扩展拓扑数据库的子网信息，识别被管网络中连接到 PE 路由器上的每个客户网络的接口，并将它们标识为客户边缘 （CE）路由器。

注释

如果 CE 路由器没有纳入 NNM 管理域，MPLS VPN SPI 就无法确定 PE-CE 关系。

MPLS VPN SPI 生成 MPLS VPN 视图用来显示 MPLS VPN 网络模型的信息。该模型包含下列信息：

- 关于 PE 路由器的细节：
  - VRF 细节 （来自 mplsVpnVrfTable）
  - 接口与 VRF 的关系 （来自 mplsVpnInterfaceConfTable）
  - 路由目标导入 / 导出列表 （来自 mplsVpnVrfRouteTargetTable）
- 关于 PE 路由器外向接口卡的细节：
  - 接口号 （来自 mplsVpnInterfaceConfTable 的 MplsVpnInterfaceConfIndex）
- 关于连接到一个或多个 PE 路由器的 CE 路由器的外向接口的细节：
  - 接口号
- 关于 VRF/VPN 配置的细节：
  - VRF 之间的关系 （来自 mplsVpnVrfRouteTargetTable）

MPLS VPN 搜索与 NNM 高级版的扩展拓扑搜索融为一体。ovet_daCiscoMplsVpn 进程就是 MPLS VPN 搜索代理程序。只要扩展拓扑搜索运行，它就运行。

若要修改扩展拓扑搜索配置，或要将扩展拓扑初始化，请使用 NNM 高级版中的配置扩展拓扑窗口。有关详情，请参见纳入 NNM 高级版的使用扩展拓扑指南。

VPN 命名算法

每个 VRF 对象都包含导入和导出路由目标的列表，这些目标标识 MPLS VPN 网络中的其他 VRF。MPLS VPN SPI 从这些导入和导出列表中读取路由目标，以便识别 VRF 邻居组。这些关系可以确定，必须测试哪些 MPLS VPN 网络中的路由，才能确保向您的内部网客户提供满意的服务。

可以借助邻居关系直接或间接连接的 VRF，被当作属于同一个 VPN。这种方法使 MPLS VPN SPI 既能正确搜索完全啮合的简单网络拓扑，还能正确搜索采用集中星型设计的复杂网络拓扑。

MPLS VPN SPI 将 VRF 分组关系和 VPN 名称存放在 VpnNames.txt 文件中。该文件在第 44 页上的 “在 MPLS VPN SPI 配置中更改 VPN 名称”中进行了描述。

MPLS VPN SPI 试图根据下列规则，向每个搜索到的 VRF 组分配一个有意义的 VPN 名称：

1. 如果搜索到的 VRF 组与存放在 `VpnNames.txt` 文件中的 VRF 组匹配，就继续使用存储的 VRF 组的 VPN 名称。

   如果两个 VRF 列表中存在一个或多个 VRF，搜索到的 VRF 组就与存储的 VRF 组相匹配。

2. 如果搜索到的 VRF 组与存储在 `VpnNames.txt` 文件中的 VRF 组不匹配，就要检查此组中每个 VRF 特有的 VRF 名称，以创建新的 VPN 名称：

   - 如果组中的每个 VRF 名称相同，该名称是唯一的 VPN 名称，那么将此文本字符串指定为该 VRF 组的 VPN 名称。
   - 如果组中的每个 VRF 名称相同，该名称早已是另一个 VRF 列表的 VPN 名称，那么将该 VPN 名称指定为 VRF 名称，再加一个下划线，后面加上该 VRF 组的 VPN 内部标识号。

3. 如果 VRF 组中每个名称至少前三个字符匹配，就将 VPN 名称设置为最大数量的初始匹配字符构成的字符串。

   此规则假设，该名称并没有指定给不同的 VRF 组。

4. 如果上述规则均不适用，就将 VPN 名称设置为字符串 `Unknown_`，再后续 VPN 内部标识号。

   若要更改 VPN 名称，请手工编辑 `VpnNames.txt` 文件，将 VPN 名称更改为对您的网络有意义的名称。详见第 44 页上的 “在 MPLS VPN SPI 配置中更改 VPN 名称”。

表 3-1 显示 VPN 命名算法的若干应用。

表 3-1 VPN 命名的示例

VPN 中的 VPF	选定 VPN 名称	说明
蓝 蓝	蓝	所有 VRF 名称都相同；选择该名称
Red_East Red_West	Red_	共同的初始字符
Red_North Red_South	Red__5	共同的初始字符与下划线，为了唯一性再加上 VPN 内部标识符
蓝 绿 黄	Unknown_1	VRF 名称不能匹配或构成有意义的名称

在 MPLS VPN SPI 配置中更改 VPN 名称

MPLS VPN SPI 将 VRF 分组关系和相关的 VPN 名称存储在文件：

- UNIX: `$OV_CONF/VpnNames.txt`
- Windows: `%OV_CONF%\VpnNames.txt`

您可以修改此文件以便定制 VPN 名称。 `VpnNames.txt` 文件的格式如下：

```
VpnName  VPN_Internal_Id  VrfList
```

条目之间的分隔符是一个制表符。不允许有其他空白。

VrfList 可能包含多个条目。每个条目指定 PE 路由器的名称和该路由器上 VRF 的名称。 VrfList 每个条目的格式如下：

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

路由器和 VRF 名称之间的分隔符是字符串 `<<>>`。 VrfList 条目之间的分隔符是一个制表符。

`DeviceName` 可以是 IP 地址或主机名。 `DeviceName` 的值来自 NNM 拓扑数据库。

图 3-1 显示 `VpnNames.txt` 文件的示例。

图 3-1 VpnNames.txt 文件示例

```
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
```

若要更改指定的 VPN 名称：

- 使用任何文本编辑器，编辑 `VpnNames.txt` 文件：

  1. 将每个包含字符串 `Unknown_` 的 VPN 名称，更改成对该网络有意义的名称。
  2. 根据需要更改其他 VPN 名称。

警告

只修改 `VpnName` 字段的值。更改此文件其他字段，将导致整个文件被遗弃。

4 理解来自 MPLS VPN 智能插件的事件

MPLS VPN 状态管理器

MPLS VPN 智能插件 （SPI）状态管理器，从 HP OpenView 事件子系统接收指定的 SNMP 事件。然后生成浓缩后的新 SNMP 事件，将事件的态势与网络中的虚拟专有网络 （VPN）联系起来。状态管理器配置网络节点管理器 (NNM) 中的成对相关，以便适当时从 NNM 警报浏览器清除浓缩的事件。

MPLS VPN SPI 状态管理器进程 （`MPLS_sm`）是一个由 `ovspmd` 管理的 NNM 服务。它将状态消息记录到标准的 NNM 日志文件：

- UNIX:`$OV_LOG/System.txt`
- Windows:`%OV_LOG%\System.txt`

有关 MPLS VPN SPI 生成的浓缩事件的信息，参见下列章节：

- 第 49 页上的 “路由器状态事件”
- 第 52 页上的 “可访问性状态变化事件”
- 第 54 页上的 “OVPI 报告包阈值事件”

路由器状态事件

本节描述 MPLS VPN SPI 生成的各种事件，介绍多协议标号切换 （MPLS VPN）环境下虚拟专有网络的边缘路由器的相应功能。

MPLS VPN SPI 与 HP OpenView 事件子系统连接，以便接收被管的 MPLS VPN 中提供商边缘 （PE）和客户边缘 （CE）路由器的状态变化事件。当 MPLS VPN SPI 收到一个事件，反映 PE 路由器上面向 CE 的接口或 CE 路由器上面向 PE 的接口出现状态变化，它就生成一个新的事件，描述变化的根本原因。 MPLS VPN SPI 还监听每个描述 PE 或 CE 路由器接口卡或节点的状态变化的事件，并对每一个变化生成一个事件。

MPLS VPN SPI 生成新的设备状态事件，浓缩了 MPLS VPN 网络的特定信息。 NNM 警报浏览器显示 MPLS VPN 分类中的浓缩事件。

默认情况下， MPLS VPN SPI 只从 netmon 进程接收事件。如果将 NNM 配置为从活动问题分析器 (APA) 接收事件，那么 MPLS VPN SPI 将从 APA 接收事件，而不是从 netmon 进程。若要更改 NNM 的输入事件源，请使用 ovet_apaConfig.ovpl 命令。有关详情，参见纳入 NNM 高级版的使用扩展拓扑指南。

表 4-1 列举并描述了 MPLS VPN SPI 生成的设备状态事件。第 14 页上的“MPLS VPN 事件”描述了这些事件的格式。有关与事件关联的变量绑定信息，参见下列目录中的 trapd.conf 文件：

UNIX:$OV_CONF/C
Windows:%OV_CONF%\C

表 4-1 MPLS VPN SPI 生成的路由器状态事件

浓缩事件名称 / HP OpenView 事件 OID	含义	输入事件名称 / HP OpenView 事件 OID	输入事件源
OV_MPLS_VPN_ADDRDOWN/ 70001009	受影响的 VPN 中的设备接口卡，没有响应其 IP 地址的 ping 请求。	OV_APA_ADDR_DOWN/ 58983011	APA

表 4-1 MPLS VPN SPI 生成的路由器状态事件 （续）

浓缩事件名称 / HP OpenView 事件 OID	含义	输入事件名称 / HP OpenView 事件 OID	输入事件源
无；从警报浏览器清除 OV_MPLS_VPN_ADDRDOWN 事件	接口卡正在响应其 IP 地址的 ping 请求	OV_APA_ADDR_UP/ 58983001	APA
OV_MPLS_VPN_IFDOWN/ 70001000	PE 路由器上为 MPLS VPN 配置的面向 CE 的接口关闭	OV_APA_IF_DOWN/ 5893012	APA
		OV_IF_Down/ 58916867	netmon
无；从警报浏览器清除 OV_MPLS_VPN_IFDOWN 事件	PE 路由器上为 MPLS VPN 配置的面向 CE 的接口恢复正常	OV_APA_IF_UP/ 5893002	APA
		OV_IF_Up/ 58916866	netmon
OV_MPLS_VPN_NODEDOWN/ 70001002	PE 路由器关闭	OV_APA_NODE_DOWN/ 58983013	APA
		OV_Node_Down/ 58916865	netmon
无；从警报浏览器清除 OV_MPLS_VPN_NODEDOWN 事件	PE 路由器恢复正常	OV_APA_NODE_UP/ 58983003	APA
		OV_Node_Up/ 58916864	netmon
OV_MPLS_VPN_Card_Down/ 70001013	带有支持 VRF 的接口的卡关闭	OV_APA_CARD_DOWN/ 58983035	APA
无；从警报浏览器清除 OV_MPLS_VPN_Card_Down 事件	带有支持 VRF 的接口的卡恢复正常	OV_APA_CARD_UP/ 58983034	APA
OV_MPLS_VPN_CONNDOWN/ 70001011	受影响的 VPN 的设备上的两个接口卡之间的连接功能不正常	OV_APA_CONNECTION_DOWN/ 58983014	APA

表 4-1 MPLS VPN SPI 生成的路由器状态事件 （续）

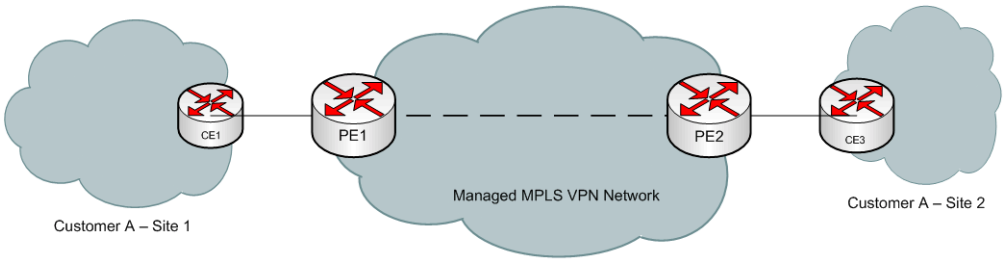
浓缩事件名称 / HP OpenView 事件 OID	含义	输入事件名称 / HP OpenView 事件 OID	输入事件源
无；从警报浏览器清除 OV_MPLS_VPN_CONNDOWN 事件	两个接口卡之间的连接现在功能正常	OV_APA_CONNECTION_UP/ 58983004	APA
OV_MPLS_VPN_NODEUNKNOWN/ 70001004	无法确定 VRF 路径中介设备的状态	OV_TOPOLOGY_Status_ Change_Notification/ 60001101	netmon

可访问性状态变化事件

MPLS VPN SPI 生成新的可访问性状态变化事件，浓缩了 MPLS VPN 网络的特定信息。 NNM 警报浏览器显示 MPLS VPN 分类中的浓缩事件。

MPLS VPN SPI 配置 MPLS VPN 网络的路由器之间的可访问性测试，并监听产生的 SNMP 陷阱信号。当其中的一个陷阱信号显示可访问性状态发生变化时，MPLS VPN SPI 就生成一个可访问性状态变化事件。图 4-1 显示通过 MPLS VPN 网络的路径示例。

图 4-1 可访问性测试路径示例



MPLS VPN SPI 支持下列路径的可访问性测试：

- PE 路由器到 PE 路由器 （例如， PE1 到 PE2）
- PE 路由器到近 CE 路由器 （例如， PE1 到 CE1）
- CE 路由器到 CE 路由器 （例如， CE1 到 CE3）

CE-CE 端到端可访问性测试，检查源 CE 路由器到近 PE 路由器到远 PE 路由器到远 CE 路由器的连通性。如果源 CE 路由器不是思科设备， MPLS VPN SPI 就将该测试分解成覆盖整个路径、独立的 SAA 测试。

思科路由器可访问性测试

对于思科路由器， MPLS VPN SPI 使用思科 Internetwork 操作系统 （IOS）服务保障代理程序 （SAA）来进行可访问性测试。每个测试都是一个 ICMP 回声请求，从一个 PE 或 CE 路由器连接到 VPN 中的另一个 PE 或 CE 路由器。 SAA 计算出回声请求的整个旅行时间。如果响应时间大于该测试的超时值， SAA 就指出测试失败，发送 `rttMonTimeoutNotification` 陷阱信号

的副本，将 rttMonCtrlOperTimeoutOccurred 变量绑定的值设置为 TRUE。 MPLS VPN SPI 接收 SNMP 陷阱信号，并向 NNM 发送一个描述 SAA 失败的浓缩的新陷阱信号。

如果失败的 SAA 测试是两个 CE 路由器之间整个路径的测试， MPLS VPN SPI 就触发 NNM，轮询受影响的 VRF 的各个接口，以确定路径内部的故障点。然后向 NNM 发送一个表示特定故障的浓缩的新陷阱信号。

如果 SAA 测试成功， SAA 就会显示测试成功，发送 rttMonTimeoutNotification 陷阱信号的副本，将 rttMonCtrlOperTimeoutOccurred 变量绑定的值设置为 FALSE。 MPLS VPN SPI 接收 SNMP 陷阱信号，如果该陷阱信号后续一个 SAA 失败陷阱信号，就向 NNM 发送一个描述 SAA 状态变化的浓缩的新陷阱信号。这个新事件清除来自 NNM 警报浏览器的 SAA 失败事件。

表 4-2 列举了 MPLS VPN SPI 生成的表示 SAA 测试条件的浓缩事件。第 14 页上的 “MPLS VPN 事件”描述了这些事件的格式。有关与事件关联的变量绑定信息，参见下列目录中的 trapd.conf 文件：

UNIX:$OV_CONF/C
Windows:%OV_CONF%\C

表 4-2 MPLS VPN SPI 生成的浓缩的可访问性事件

浓缩事件名称 / HP OpenView 事件 OID	含义	SAA MIB Object/ OID = Value
OV_MPLS_VPN_SAA_FAIL/ 70001006	两个设备之间的连接关闭	rttMonCtrlOperTimeoutOccurred/ .1.3.6.1.4.1.9.9.42.1.2.9.1.6 = TRUE
OV_MPLS_VPN_SAA_PASS/ 70001007 从警报浏览器清除 OV_MPLS_VPN_SAA_FAIL 事件	两个设备之间的连接恢复正常	rttMonCtrlOperTimeoutOccurred/ .1.3.6.1.4.1.9.9.42.1.2.9.1.6 = FALSE

OVPI 报告包阈值事件

如果安装了 OVPI 和 MPLS VPN 报告包， MPLS VPN SPI 就从 OVPI 接收若干阈值事件。 MPLS VPN SPI 将这些事件发送给 NNM 警报浏览器的 MPLS VPN 性能分类。它并没有向这些事件添加任何信息。

表 4-3 列举并描述了 MPLS VPN SPI 从 OVPI 接收的阈值事件。

表 4-3 来自 OVPI 的 MPLS VPN 阈值事件

OVPI 事件名称	含义
VPN_INTERFACEAVAIL_PCT	VPN 所有接口的平均可用性低于可接受的阈值。
VPN_DISCARD_PCT	VPN 所有接口的平均包丢弃百分比低于可接受的阈值。
VPN_ERROR_PCT	VPN 所有接口的平均包出错百分比低于可接受的阈值。
VPN_SNMPRESPONSE	从 OVPI 到 VPN 所有接口的设备 / 接口的平均 SNMP 响应，低于可接受的阈值。
VRF_OPERSTATUS	VRF 处于非操作状态。

5 使用服务保障代理程序

服务保障代理程序

思科 Internetwork 操作系统 (IOS) 服务保障代理程序 (SAA)，是思科 IOS 设备中内嵌的软件代理程序。它主动执行网络状态的监视任务，可以确认是否满足服务水平协议。路由器上思科 RTTMON MIB (SAA MIB) 变量的值，确定该设备的 SAA 配置。可以对网络中的每个路由器分别配置待执行的 SAA。

MPLS VPN 智能插件 (SPI) 配置 SAA，使用 ICMP 回声请求，测试多协议标号切换 （MPLS VPN）环境下虚拟专有网络中每个提供商边缘 - 提供商边缘（PE-PE）路由器对的可访问性。如果可访问性测试超时， SAA 就向网络节点管理器 (NNM) 发送 SNMP 陷阱信号。 MPLS VPN SPI 从 HP OpenView 事件子系统接收这一陷阱信号，用有关 MPLS VPN 网络的信息对它浓缩，并在 NNM 警报浏览器中显示事件。

第 52 页上的 “可访问性状态变化事件”，描述 MPLS VPN SPI 如何处理这些陷阱信号。

SAA 测试

MPLS VPN SPI 不但保存 PE-PE 路由器对的列表，而且配置每对路由器之间的可访问性的双向测试。例如， MPLS VPN SPI 配置 PE1 上的 SAA 发送从 PE1 到 PE2 的 ICMP 回声请求。MPLS VPN SPI 还配置 PE2 上的 SAA 发送从 PE2 到 PE1 的 ICMP 回声请求。

MPLS VPN SPI 支持下列类型的可访问性测试：

- PE-PE VRF 非敏感可访问性测试，按照黑箱来检查 PE 路由器之间的连通性。默认情况下， MPLS VPN SPI 对 MPLS VPN 网络中的所有 PE-PE 对配置这些测试。
- PE-PE VRF 敏感可访问性测试，在 VPN 预先定义的 VRF 路径上检查两个 PE 路由器之间的连通性。
- PE-CE VRF 敏感可访问性测试，检查 PE 路由器和 VPN 中指定的本地 CE 路由器之间的连通性。
- CE-CE 端到端可访问性测试，检查 VPN 的指定 CE-PE-PE-CE 路径的连通性。

SAA 测试定义

SAA 测试定义被存储在一个 MPLS VPN SPI 内部文件中。MPLS VPN SPI 处理此文件，并配置 MPLS VPN 网络中的每个 SAA。使用 saa_config.ovpl 命令可以访问当前的 SAA 测试定义。有关该命令的信息，参见第 62 页上的“修改 SAA 测试定义”。

若要配置 SAA 测试，请创建新的测试定义文件，并将该文件导入 MPLS VPN SPI SAA 测试定义文件。您可以将当前 SAA 测试定义导出到一个文件中，再用自己的修改对文件进行编辑，也可以创建新的文本文件，其中只包含您希望配置的测试。然后将更新后的 SAA 测试定义导入 MPLS VPN SPI。只要 SAA 测试定义文件发生变化， MPLS VPN SPI 就会更新每个被管路由器和每个思科 CE 路由器上的 SAA 测试配置。

如果在 SAA 测试配置中将非思科 CE 路由器指定为源路由器， MPLS VPN SPI 就将测试分解成多个可以在 PE 路由器上配置的段。例如，考虑下列网络路径：

CE1-PE1-PE2-CE2

如果 CE1 不是思科设备， MPLS VPN SPI 就把测试分解成 PE1-CE1 可访问性测试和 PE1-CE2 可访问性测试。它将这些测试配置到 PE1 设备上。

SAA 测试定义文件格式

SAA 测试定义文件是普通文本文件，定义每个待执行的 SAA 的 ICMP 回声请求。该文件包含一个或多个 `BEGIN`/`END` 对，每对定义一个指定的测试。第 60 页上的图 5-1 到第 61 页上的图 5-4，显示了 SAA 测试定义的示例。

SAA 测试定义内部的元素具体如下：

- `BEGIN` — 表示 SAA 测试定义开始的元素。

- TEST_TYPE — 定义的 SAA 测试的类型。可能的值为 PE-PE、 PE-CE 和 CE-CE：
  - 使用 PE-PE 可以进行 PE-PE VRF 非敏感测试或 PE-PE VRF 敏感测试。
  - 使用 PE-CE 可以进行 PE 本地 CE VRF 敏感测试。
  - 使用 CE-CE 可以进行端到端 CE-CE 测试。
- SOURCE — SAA 测试的源路由器的选定名称。该值必须与 NNM 拓扑数据库的选定名称相匹配。源路由器是 SAA 测试的发起者。
- DEST — SAA 测试的目标路由器的选定名称。该值必须与 NNM 拓扑数据库的选定名称相匹配。目标路由器是由 SAA 测试确认的设备。
- VRF — 任选项。该值只适用于 PE-PE VRF 敏感测试和 PE-CE VRF 敏感测试。 VRF 名称既出现在源路由器上，也出现在目标路由器上。 VRF 名称可以从源边缘路由器的路由器文件中得到，也可以来自文件：
  - UNIX:$OV_CONF/VpnNames.txt
  - Windows:%OV_CONF%\VpnNames.txt
- OP — 该文件被导入 SAA 测试配置工具时执行的操作。可能的值为 ADD、DELETE 和 MODIFY。
- CONFIG_TYPE — 采用的配置方法。可能的值为 SAA_TEST_CONFIG 和 SAA_TEST_SYNC：
  - 使用 SAA_TEST_CONFIG，可以引起 MPLS VPN SPI SAA 配置进程，导入此文件时将该 SAA 测试配置到源路由器的 SAA MIB。
  - 使用 SAA_TEST_SYNC，可以防止 SAA 配置进程修改源路由器上的 SAA 中的 SAA 测试配置。如果使用此值，就必须使用思科 IOS 命令，显式地配置源路由器上 SAA MIB 的 SAA 测试。

- SAA_SRC_ADDR — 任选项。 SAA 测试的路由器上的源接口卡的 IP 地址。此值只适用于标准的 VRF 非敏感测试。
  - — 对于 PE-PE VRF 非敏感测试，此值可以是源路由器上的任何 IP 地址。
  - — 对于 CE-CE 端到端测试，此值必须是 VPN 内部的专有 IP 地址。
- SAA_DEST_ADDR — 任选项。 SAA 测试的路由器上的目标接口卡的 IP 地址。该地址必须在通过这次 SAA 测试指定的目标路由器可以访问的 VPN 地址范围之内。
  - — 对于 PE-PE VRF 非敏感测试，此值可以是目标路由器上的任何 IP 地址。
  - — 对于 PE-PE VRF 敏感测试、PE-CE VRF 敏感测试或 CE-CE 端到端测试，此值必须是 VPN 内部的专有 IP 地址。
- SET_COMM — 任选项。源 PE 路由器的 SNMP 设置社区字符串。如果 SNMP 配置数据库中配置了源 PE 路由器的社区字符串，就不必在 SAA 测试定义中再提供。只有当 CONFIG_TYPE 参数的值为 SAA_TEST_CONFIG 时，才可以适用该值
- FREQUENCY — 任选项。此测试实例之间的时间间隔。指定该时间间隔的秒数。

  如果该元素没有纳入 SAA 测试定义，这次测试就将采用配置 SAA 测试时 mpls.conf 文件的 FREQUENCY 参数的值。有关 mpls.conf 文件的信息，参见第 63 页上的 “设置 SAA 配置参数”。
- TIMEOUT — 任选项。认为测试失败之前允许 ICMP 回声响应的时间长度。指定超时值的毫秒数。

  如果该元素没有纳入 SAA 测试定义，这次测试就将采用配置 SAA 测试时 mpls.conf 文件的 TIMEOUT 参数的值。有关 mpls.conf 文件的信息，参见第 63 页上的 “设置 SAA 配置参数”。
- TAG — SAA 测试的标识符。该值取决于 MPLS VPN SPI，只适用于导出模式。对于新的测试定义，请保留此参数不要定义。
- END — 表示 SAA 测试定义结束的元素。

图 5-1 PE-PE VRF 非敏感 SAA 测试的测试定义示例

```
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
```

图 5-2 PE-PE VRF 敏感 SAA 测试的测试定义示例

```
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
```

图 5-3 PE-CE 本地 VRF 敏感 SAA 测试的测试定义示例

```
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
```

图 5-4 CE-CE 端到端 SAA 测试的测试定义示例

```
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
```

修改 SAA 测试定义

您可以观察和修改当前 SAA 测试定义：

- 若要观察当前 SAA 测试定义：

```
saa_config.ovpl -e filename
```

MPLS VPN SPI 将 SAA 测试定义导出到指定的 `filename`。这些测试定义来自由 MPLS VPN SPI 存储的 SAA 测试配置信息，并非来自设备本身。

- 若要创建新的或修改 SAA 测试定义：

```
saa_config.ovpl -i filename
```

MPLS VPN SPI 从指定的 文件名 读取 SAA 测试定义，并在相应的 PE 路由器上更新 SAA 测试配置。

关于如何修改 SAA 测试定义的分步指导信息，参见第 64 页上的 “使用 MPLS VPN SPI 配置 SAA”。

SAA 配置

默认情况下， MPLS VPN SPI 在 MPLS VPN 搜索结束时更新 SAA 测试定义。然后它在每个被管路由器上配置 SAA MIB，对现有的 SAA 测试定义进行修改。参见第 63 页上的 “设置 SAA 配置参数”。

因为 MPLS VPN SPI 使用 SNMP 与 SAA 通信，所以无辅助配置的 SAA 测试，需要访问每个路由器的 SNMP 设置社区字符串。参见第 64 页上的 “使用 MPLS VPN SPI 配置 SAA” .

如果不希望向路由器提供 SNMP 设置社区字符串，就可以使用思科 IOS 命令配置路由器上的 SAA MIB。参见第 66 页上的 “使用思科 IOS 命令配置 SAA”。

设置 SAA 配置参数

MPLS VPN SPI 安装进程设置若干控制无辅助 SAA 配置的参数值。这些参数被存储在文件：

- UNIX:`$OV_CONF/mpls.conf`
- Windows:`%OV_CONF%\mpls.conf`

图 5-5 显示 `mpls.conf` 文件的示例。

图 5-5 mpls.conf 文件示例

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

mpls.conf 文件中的参数具体如下：

- SAA_TRIG — 确定 MPLS VPN 搜索完成之后是否运行 SAA 配置进程。可能的值为 true 和 false。
- FREQUENCY — 设置 SAA 测试的默认运行频率。如果 SAA 测试定义没有指定频率， MPLS VPN SPI 就用该频率值配置 SAA 测试。
- TIMEOUT — 设置 SAA 测试的默认超时值。如果 SAA 测试定义没有指定超时值， MPLS VPN SPI 就用该超时值配置 SAA 测试。

若要经由 MPLS VPN SPI 修改 SAA 配置参数：

- 使用任何文本编辑器，编辑 mpls.conf 文件。

  MPLS VPN SPI 每读取一次 mpls.conf 文件，就执行一次 SAA 配置。

注释

修改 FREQUENCY 或 TIMEOUT 参数值，只影响新的或修改的 SAA 测试定义。现有的 SAA 测试定义没有变化。

使用 MPLS VPN SPI 配置 SAA

无辅助 SAA 配置需要访问路由器的 SNMP 设置社区字符串。有两种方法支持提供 SNMP 设置社区字符串：

- 使用命令 xnmsnmpconf，可以将社区字符串存储在 NNM 的 SNMP 配置数据库。这种方法可以让路由器访问 NNM 所有的管理功能。
- 向导入的 SAA 测试定义文件提供社区字符串。这种方法使得路由器只能访问 MPLS VPN SPI 的 SAA 测试配置。

默认情况下， MPLS VPN SPI 对网络中的每个 VPN 的每个 PE-PE 路由器对，创建 VRF 非敏感 SAA 测试。

若要使用 MPLS VPN SPI 配置 VRF 敏感 SAA 测试或其他的 VRF 非敏感 SAA 测试，请执行下列步骤：

1. 创建 SAA 测试定义文件：

```
saa_config.ovpl -e filename
```

`filename` 包含当前的 SAA 测试定义。

2. 使用任何文本编辑器，在 `filename` 中，定义将要在 SAA 测试定义文件中执行的 SAA 测试：

   a. 必要时，修改现有的定义：

   - 若要修改现有的测试定义，先对测试定义进行适当编辑，再将 `OP` 参数设置为 `MODIFY`。
   - 若要删除现有的测试定义，请将 `OP` 参数设置为 `DELETE`。

注释

如果删除原先由 MPLS VPN SPI 创建的测试定义，那么 SPI 将不会重新添加该测试定义。如果后来决定执行该 SAA 测试，就必须编写这个测试定义，并导入 SAA 配置。

   b. 必要时，添加新的测试定义：

   - 遵循测试定义文件的格式。
   - 将 `OP` 参数设置为 `ADD`。

   c. 必要时，向每个 SAA 测试定义提供 SNMP 设置社区字符串：

   - 如果源 PE 路由器的设置社区字符串被存储在 SNMP 配置数据库中，就忽略 SAA 测试定义中的 `SET_COMM` 参数。
   - 如果源 PE 路由器的设置社区字符串**没有**存储在 SNMP 配置数据库中，就把正确的值提供给 SAA 测试定义的 `SET_COMM` 参数。

3. 导入更新的 SAA 测试定义

```
saa_config.ovpl -i filename
```

MPLS VPN SPI 读取 `filename` 中的每个 SAA 测试定义，并在源路由器的 SAA MIB 中配置测试。

使用思科 IOS 命令配置 SAA

如果路由器的 SNMP 设置社区字符串不可用，就使用思科 IOS 命令来配置该路由器上的 SAA 测试。

每个 SAA 测试都包括一个唯一的选项卡名称。 MPLS VPN SPI 使用此选项卡名称来标识 SNMP 陷阱信号中的 SAA 测试。必须使用 MPLS VPN SPI 生成的选项卡名称。如果 MPLS VPN SPI 将一个 CE-CE 端到端可访问性测试分解成两个独立的测试，就必须将每个测试唯一的选项卡包含在配置中。

若要经由思科 IOS 命令配置 SAA 测试，请执行下列步骤：

1. 在新的文本文件中，对于每个 SAA 测试，输入下列元素和对应的值：

   - BEGIN
   - TEST_TYPE
   - SOURCE
   - DEST
   - VRF （如果可用）
   - OP
   - CONFIG_TYPE = SAA_TEST_SYNC
   - SAA_SRC_ADDR （如果可用）
   - SAA_DEST_ADDR （如果可用）
   - END

   有关文件格式的信息，参见第 57 页上的 “SAA 测试定义文件格式”。

2. 为每个 SAA 测试生成唯一的选项卡值

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

MPLS VPN SPI 读取 `input_filename`，即第一步创建的文本文件，再写到 `output_filename`，即修改后的 SAA 测试文件，对每个 SAA 测试定义都有一个选项卡名称。

3. 连接到源路由器，再使用思科 IOS 命令来配置每个 SAA。

对于每个测试，指定对应的选项卡，那是 MPLS VPN SPI 通过第 2 步生成的 `output_filename` 的 `OV_TAG` 参数设置的。

图 5-6 显示了配置 SAA 测试的思科 IOS 命令序列的示例。关于配置路由器的指导信息，参见相关的思科文档。

图 5-6　思科 IOS 命令 SAA 配置示例

```
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 智能插件疑难解答

疑难解答清单

注释

如果正在试图覆盖现有版本安装 MPLS VPN 智能插件 （SPI），请在执行 MPLS VPN SPI 安装步骤之前，按照第 34 页上的 “删除 MPLS VPN SPI” 所述，删除 MPLS VPN SPI。

如果这次安装是从原先版本的 MPLS VPN SPI 进行更新，参见第 26 页上的 “更新上一版本 MPLS VPN SPI 中的 SAA 测试定义”。

下列内容是 MPLS VPN SPI 遇到困难需要考虑的事项的总结：

- 网络节点管理器 (NNM) 无法连接拓扑。

  NNM 进程不在运行。

  - ❑ 验证 NNM 是否已经安装，详见第 23 页上的 “验证正确安装了网络节点管理器高级版”。
  - ❑ 验证 NNM 环境变量来源是否适当，详见第 23 页上的 “设置 NNM 环境变量”。
  - ❑ 验证 NNM 服务是否运行正常，详见第 73 页上的 “验证 NNM 服务正在管理工作站上运行”。

- 一个或多个边缘路由器没有出现在 NNM 拓扑或 MPLS VPN 视图中。

  NNM 没有搜索到这个设备。

  - ❑ 使用 loadhosts command 或种子文件，可以帮助 NNM 定位网络中的所有边缘路由器。关于指示信息，参见用 HP OpenView 网络节点管理器管理您的网络指南。
  - ❑ 验证 MPLS VPN 搜索是否成功完成，详见 第 76 页上的 “验证 MPLS VPN 搜索是否已经出现”。

- MPLS VPN 警报浏览器中没有出现任何事件。

  MPLS VPN SPI 不在接收边缘路由器的事件。

  - ❑ 验证所需的 MIB 是否被加载，详见第 75 页上的 “验证 MIB 是否加载”。

- ❑ 验证被管设备是否配置恰当，可以将陷阱信号转发到 NNM 管理工作站：
  - — 如果使用 SNMP 访问控件限制计算机对路由器的 SNMP 访问，就将 NNM 管理工作站纳入每个边缘路由器的访问列表。
  - — 配置每个边缘路由器，以便将 NNM 管理工作站纳入 SNMP 陷阱信号接收者之一。
  - — 有关配置信息，参见路由器随机带来的文档。
- ❑ 验证 NNM 管理工作站正在从这些设备接收事件：
  - — 在所有警报浏览器中查看有关边缘路由器的事件。创建事件的简单方式，是从网络临时断开一个接口卡。
- ❑ 验证 NNM 能否轮询边缘路由器以获取状态信息，详见第 35 页上的“配置 SNMP 轮询访问”。
- ❑ 验证 MPLS VPN 搜索是否已经出现，详见第 76 页上的“验证 MPLS VPN 搜索是否已经出现”。
- ❑ 验证 MPLS VPN SPI 是否在运行，详见第 74 页上的 “验证 MPLS VPN SPI 正在运行”。

- MPLS VPN 警报浏览器中没有出现任何 SAA 测试事件。

  MPLS VPN SPI 不在接收来自边缘路由器的 SAA 事件。

  - ❑ 验证被管设备是否配置恰当，可以将陷阱信号转发到 NNM 管理工作站：
    - — 如果使用 SNMP 访问控件限制计算机对路由器的 SNMP 访问，就将 NNM 管理工作站纳入每个边缘路由器的访问列表。
    - — 配置每个边缘路由器，以便将 NNM 管理工作站纳入 SNMP 陷阱信号接收者之一。
    - — 有关配置信息，参见路由器随机带来的文档。
  - ❑ 验证 NNM 管理工作站正在从这些设备接收事件：
    - — 在所有警报浏览器中查看有关边缘路由器的事件。创建事件的简单方式，是从网络临时断开一个接口卡。
  - ❑ 验证 SAA 测试定义是否存在。参见第 77 页上的 “验证 SAA 测试定义”。
  - ❑ 验证 MPLS VPN SPI 是否正在运行。参见第 74 页上的 “验证 MPLS VPN SPI 正在运行”。

有关其他疑难解答信息，参见最新的网络节点管理器 MPLS VPN 智能插件发布通知，以及报告与网络解决方案的发布通知，后者可以在网站 `http://ovweb.external.hp.com/lpe/doc_serv` 的报告与网络解决方案产品分类中找到。

验证 NNM 服务正在管理工作站上运行

若要验证 NNM 服务正在管理工作站上运行，请执行下列步骤：

1. 验证 NNM 是否已经安装，详见第 23 页上的 “验证正确安装了网络节点管理器高级版”。
2. 确定 NNM 服务的状态：
   - UNIX: `$OV_BIN/ovstatus -v`
   - Windows: `%OV_BIN%\ovstatus -v`

   所有进程，包括 PMD 在内，都应当在运行。
3. 如果 NNM 和所有关联进程不在运行，请停止并重新启动 NNM 服务：
   - UNIX:

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

     ```
     %OV_BIN%\ovstop -c
     %OV_BIN%\ovstart -c
     ```

验证 MPLS VPN SPI 正在运行

若要验证 MPLS VPN 状态管理器服务正在管理工作站上运行，请执行下列步骤：

1. 确定 MPLS VPN SPI 状态管理器的状态：

   - UNIX: `$OV_BIN/ovstatus -v`
   - Windows: `%OV_BIN%\ovstatus -v`

   `MPLS_sm` 进程应当在运行。

2. 如果 `MPLS_sm` 进程或任何 NNM 进程不在运行，请停止并重新启动 NNM 服务：

   - UNIX:

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

   - Windows:

     ```
     %OV_BIN%\ovstop -c
     %OV_BIN%\ovstart -c
     ```

验证 MIB 是否加载

若要验证所需的 MIB 是否加载到 NNM 管理工作站，请执行下列步骤：

1. 在 NNM GUI （ovw），单击 选项 -> 加载 / 卸载 MIB：SNMP。

   将出现加载 / 卸载 MIB：SNMP 窗口。该窗口列举已经安装到 NNM 管理工作站上的 MIB。

2. 验证第 24 页上的 “MIB 附件”中指定的 MIB 是否安装。

3. 如果一个或多个所需的 MIB 没有安装，请使用此窗口添加所需的 MIB。

   有关详情，参见使用 HP OpenView 网络节点管理器管理您的网络指南。

验证 MPLS VPN 搜索是否已经出现

如果认为 MPLS VPN SPI 没有搜索到 MPLS VPN 网络中所有的路由器，就检查 MPLS VPN 搜索代理程序的状态：

- UNIX:

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

- Windows:

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

状态输出中的上次消息，描述 MPLS VPN 搜索代理程序的当前状态：

- 如果此消息描述的是搜索进程中的某一步骤，那么 MPLS VPN 搜索正在运行。等待搜索进程完成，然后在 MPLS VPN 视图中查找期望的 MPLS VPN 设备。
- 如果此消息是等待下次搜索周期，那么 MPLS VPN 搜索代理程序已经完成搜索，正处于空闲状态等待下次搜索周期。使用 loadhosts 命令或种子文件，可以帮助 NNM 定位 MPLS VPN 网络中的所有路由器。有关详情，参见用 HP OpenView 网络节点管理器管理您的网络指南。
- 如果此消息显示的是错误状态，请重新启动扩展拓扑搜索。有关详情，参见使用扩展拓扑指南。

验证 SAA 测试定义

saa_tag.xml 和 saa.conf 文件，存储 MPLS VPN SPI 配置 PE 路由器的 SAA 测试定义。 saa_tag.xml 文件存储这些 XML 格式的测试定义。

若要验证 SAA 测试定义是否存在，请检查下列文件的存在性：

- UNIX: $OV_DB/saa_tag.xml saa.conf
- Windows: %OV_DB%\saa_tag.xml saa.conf

重新创建 saa_tag.xml 文件

如果 saa_tag.xml 文件不存在或大小为零，并且 saa.conf 文件不存在，请执行下列步骤重新创建 saa_tag.xml 文件：

1. 将当前 SAA 测试定义导出到文件：
   - UNIX:

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

   - Windows:

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

2. 编辑 temp_current_saa.txt 文件，将参数定义之一的 OP 参数值修改为 MODIFY。
3. 导入修改后的文件：
   - UNIX:

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

   - Windows:

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

   saa_tag.xml 文件现在应当存在。

注释 saa_tag.xml 文件是 MPLS VPN SPI 的内部文件。切勿编辑该文件。

重新创建 saa.conf 文件

如果 saa.conf 文件不存在或大小为零，请执行下列步骤重新创建 SAA 测试定义：

1. 登录作为一个或多个 SAA 测试源的边缘路由器
2. 编辑思科 RTTMON MIB，删除所有 SAA 测试配置。
3. 对于 MPLS VPN 网络中一个或多个 SAA 测试源的每个边缘路由器，重复步骤 1 和 2。
4. 确保 mpls.conf 文件的 SAA_TRIG 参数设置为 true。参见第 63 页上的“设置 SAA 配置参数”。
5. 启动扩展拓扑搜索，以重新搜索 MPLS VPN 拓扑。 MPLS VPN 搜索完成之后， NNM 就生成 saa.conf 文件。

   有关启动搜索的信息，参见使用扩展拓扑指南。

处理其他问题

本节列举了使用 MPLS VPN SPI 过程中可能遇到的错误，并描述了问题的解决方法。如果第 70 页上的 “疑难解答清单”描述的情景无一可以满足您的需求，请阅读本节。

重新引导边界路由器，从 SAA MIB 删除 SAA 测试定义

注释 这种情景只适用于思科设备。

没有任何方法可以阻止删除 SAA 测试定义。

围绕这一情景展开工作

- 重新引导边缘路由器之前，请在该路由器上执行下列 IOS 命令：

  `write mem`

  该命令使得路由器可以在引导序列期间重新加载 SAA 测试。

在 NNM 中， PE 路由器图标显示为红色

红色表示这些设备处于临界状态。该状态受 NNM 管理，不受 MPLS VPN SPI 管理。

如果认为该状态指示器不正确，请执行此节点的需求轮询，以确保 NNM 正在显示最新的状态信息：

- UNIX: `$OV_BIN/nmdemandpoll nodename`
- Windows: `%OV_BIN%\nmdemandpoll nodename`

NNM 使用 SNMP 查询 nodename，并更新此节点的接口卡的状态。 PE 路由器图标的颜色反映了包含的接口卡的状态。

PE 路由器图标是正方形，不是菱形

正方形图标表示只有一块 LAN 卡的计算机。菱形图标表示带有多块 LAN 卡的路由器。如果 PE 路由器图标为正方形， NNM 就只有一块 LAN 卡的信息。 SNMP 请求其他 LAN 卡信息没有成功。请验证此路由器的 SNMP 连通性：

- UNIX: `$OV_BIN/snmpwalk nodename system`
- Windows: `%OV_BIN%\snmpwalk nodename system`

NNM 途径 MIB-2 MIB 系统节寻找指定节点。

- 成功时， `snmpwalk` 显示系统变量的值。

  如果有多个 LAN 卡， PE 路由器图标现在应当是菱形。

- 失败时， `snmpwalk` 显示消息 “超时之前没有出现任何响应。”

  在 SNMP 配置数据库中为 PE 路由器设置设置社区字符串，然后再次执行 snmp walk。

VPN 名称混乱

可以配置 VPN 名称，使之对您的环境有意义。参见第 44 页上的 “在 MPLS VPN SPI 配置中更改 VPN 名称”。

MPLS VPN 配置变化没有出现

修改 MPLS VPN 结构之后，请启动扩展拓扑搜索，以更新 MPLS VPN 信息。有关详情，参见纳入 NNM 高级版的使用扩展拓扑指南。

收集 HP 支持信息

如果该指南中找不到出现的错误，请执行下列步骤收集系统和配置信息，然后将问题报告 HP 支持代表。

1. 记住该错误。
2. 验证 NNM 是否在运行。有关指示信息，参见第 73 页上的 “验证 NNM 服务正在管理工作站上运行”。
3. 收集 HP 支持代表所需的下列信息：
   - 数据和配置文件：

     UNIX:

     — `$OV_DB/Vpn_Info.xml`

     — `$OV_CONF/VpnNames.txt`

     — `$OV_CONF/mpls.conf`

     Windows:

     — `%OV_DB%\Vpn_Info.xml`

     — `%OV_CONF%\VpnNames.txt`

     — `%OV_CONF%\mpls.conf`
   - SAA 导出文件 （`current_saa.txt`）：

     创建导出文件：

     — UNIX:

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

     — Windows:

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

- 文件 `ovobjprint.output`：

  创建输出文件：

  — UNIX:

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

  — Windows:

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

- MPLS VPN 网络拓扑包括：
  — 连通性信息
  — 名称， IP 地址
- VPN 信息：
  — PE 路由器 — VRF — 接口关系
  — VPN 细节 （哪个 PE 路由器上的哪个 VRF 对应于哪个 VPN）
- 适当时的屏幕快照：
  — 警报浏览器显示各种事件

  （修改浏览器的列宽，以便尽可能多地显示事件消息文本。）

  — NNM 子图
- 网络的当前状态
  — 一切正常吗？
  — 采集上述数据时，有接口或路由器关闭了吗？
- PE 路由器信息包括：
  — 厂商 （例如，思科）
  — 型号名称 （例如， Catalyst 6509）
  — IOS 版本