CA Spectrum®

设备管理参考指南

版本 9.3

联系技术支持

要获取在线技术帮助以及办公地址、主要服务时间和电话号码的完整列表，请联系技术支持：http://www.ca.com/worldwide。

目录

第 1 章： 入门

此指南针对以下设备介绍 CA Spectrum 设备管理文档（按字母顺序显示）：

- 第 2 章：AM Communications
- 第 3 章：Ceterus Universal
- 第 4 章：Cheetah Gateway
- 第 5 章：HP BladeSystem c-Class 认证
- 第 6 章：Juniper M 系列
- 第 7 章：Netscreen 防火墙
- 第 8 章：Nortel Contivity VPN 交换机

第 2 章： AM Communications

本节针对 AM Communications 集成介绍 CA Spectrum 设备管理文档。

此部分包含以下主题：

支持的设备

AM Communications 为非 SNMP 宽带组件开发网络管理产品。它们监控 RF（射频）和 HFC（混合光纤同轴电缆）组件。NetMentor 软件包 Cheetah 带有可选的 SNMP Agent Module，可将专有事件转换为 SNMPv1/v2 警报和陷阱。此管理模块通过常规 SouthBound 应用程序网关集成为陷阱接收和事件创建提供位置。

此管理模块支持 Omni2000 Proxy Agent。Omni2000 Proxy Agent 是 AM Communications 实现的 HFC 组件监控解决方案。

CA Spectrum 模型

未创建特定的 AM Communications 模型类型。Southbound Gateway 提供了 EventAdmin 和 EventModel 两种模型类型。这些模型类型用于管理 Omni2000 Proxy Agent 发送到 CA Spectrum 的信息。

EventAdmin 是用于表示 Omni2000 Proxy Agent 的容器模型类型。EventModel 表示 Omni2000 Proxy Agent 传递给 CA Spectrum 的陷阱信息的唯一源。EventModel 会自动放置在拓扑视图中，您可以通过从 EventAdmin 模型深入查看来访问。由于这些图标表示事件源，而不一定是物理设备或组件，因此不显示彼此之间的任何连接。

EventAdmin 模型从 Omni2000 Proxy Agent 接收陷阱后，会将陷阱映射到 CA Spectrum 事件。然后，它将事件发送到适当的 EventModel 进行处理。如果表示陷阱信息的唯一源的 EventModel 不存在，则会自动进行创建。

《SouthBound Gateway Toolkit Guide》（SouthBound Gateway 工具包指南）包含创建 EventAdmin 模型的说明。使用 EventAdmin 模型表示 AM Communications 管理应用程序。

创建此模型后，选择 Omni2000 作为管理器名称。

陷阱、事件和警报

本节介绍 AM Communications 集成如何发送陷阱。还介绍 EventAdmin 和 EventModel 如何处理和管理这些陷阱。

当 Omni2000 Proxy Agent 将陷阱发送到 CA Spectrum 时，EventAdmin 模型接收这些陷阱并将其映射到 CA Spectrum 事件。这些事件将会发送到表示陷阱源的 EventModel。陷阱中发送的 NEModelNumber 变量绑定的值用于标识陷阱源。此变量绑定来自 AMC-MIB。如果表示陷阱源的 EventModel 不存在，则会自动进行创建。

EventModel 接收事件后，会对其进行处理并将其用于创建或清除警报。下表显示每个陷阱与 CA Spectrum 事件的映射关系以及如何处理事件。

陷阱	警报	事件代码	说明
NewNEFound		0x3eb0001	HFC 代理检测到新的网络元素。
Communicatio-nsStatus		0x3eb0002	HFC 代理失去或恢复与网络元素的通信。
Configuration Change	橙色	ox3eb0003	（通过任何接口）更改了任何类型的单个变量的配置。
StatusChange		0x3eb0004	活动的警报已被清除。
Alarm	橙色	0x3eb0005	代理检测到警报。
ToBeSendQue-ueOverflow	橙色	0x3eb0006	SNMP 代理的 TrapToBeSendQueue 已满。
NewNELost	橙色	0x3eb0007	HFC 代理检测到新的网络元素丢失。

第 3 章： Ceterus Universal

本节介绍 Ceterus Universal Transport System 设备的通用部署方案，以及如何在 CA Spectrum 中对其建模。

此部分包含以下主题：

陷阱处理

您可以配置远程 Ceterus 设备，以便通过其 EOC 信道将陷阱转发给本地设备。在此配置中，本地设备充当网关并转发这些陷阱。有关此功能的详细信息，请参阅 Ceterus 文档。

也可以使用 SNMP 目标 IP 地址配置远程设备。在此配置中，该设备通过其管理端口发送陷阱。

如果同时配置这两个功能，CA Spectrum 将接收重复的陷阱。Ceterus 管理模块旨在处理这种情况。它评估传入的 Ceterus 陷阱，并在最合适的 CA Spectrum 设备模型上断言这些陷阱。管理模块通过对比陷阱中的 Ceterus 设备团体字符串与设备 sysName 的值来选择适当的模型。

重要说明：CA Spectrum 依赖于设备的团体名称来确定模型。因此，团体名称和 sysName 必须同步。默认情况下，sysName 的轮询间隔为 5 分钟。更改 TID 可能会影响对陷阱的处理，除非 sysName 通过轮询进行了适当更新。当管理员将给定 Ceterus 设备上的 TID (sysName) 从“设备 A”更改为“设备 B”时，该设备会将陷阱发送到该模型。在这种情况下，CA Spectrum 不能再处理该陷阱。sysName 更新后，才会重新开始进行陷阱处理（默认情况下，最长时间为 5 分钟）。

第 4 章： Cheetah Gateway

本节介绍 CA Spectrum 对用于监控的 Cheetah™ 网络管理产品的支持。

此部分包含以下主题：

支持的设备

Cheetah™ 产品（包括 CheetahNet™ ，以前称为 NetMentor™ ）是针对非 SNMP 宽带组件的网络管理产品。它们监控 RF（射频）和 HFC（混合光纤同轴电缆）组件。CheetahNet/NetMentor 软件包带有可选的 SNMP Agent Module，可将专有事件转换为 SNMPv1/v2 警报和陷阱。此管理模块通过 CA Spectrum Southbound Gateway 集成来支持在 CA Spectrum 中接收陷阱和创建事件。

此管理模块提供 CheetahNet/NetMentor 管理应用程序（包括 SNMP Agent Module）与 CA Spectrum 之间的集成。此集成可针对以下类型的 HFC 设备报告事件：

- 电源
- 放大器
- 线路监控器
- 测试点
- 光纤节点
- HEFiber

CA Spectrum 模型

未创建特定的 Cheetah 模型类型。Southbound Gateway 提供 EventAdmin 和 EventModel 两种模型类型。这些模型类型用于管理 NetMentor 发送到 CA Spectrum 的信息。

EventAdmin 是用于表示 NetMentor 管理应用程序的容器模型类型。EventModel 表示 CheetahNet/NetMentor 应用程序传递到 CA Spectrum 的陷阱信息的唯一源。EventModel 会自动放置在拓扑视图中，您可以通过从 EventAdmin 模型深入查看来访问。由于这些图标表示事件源，而不一定是物理设备或组件，因此不显示彼此之间的任何连接。

EventAdmin 模型从 CheetahNet/NetMentor 应用程序接收陷阱后，会将陷阱映射到 CA Spectrum 事件。EventAdmin 还将事件发送到适当的 EventModel 进行处理。如果表示陷阱信息的唯一源的 EventModel 不存在，则会自动进行创建。

创建 EventAdmin 模型

《SouthBound Gateway Toolkit Guide》（SouthBound Gateway 工具包指南）包含创建 EventAdmin 模型的说明。使用 EventAdmin 模型表示 CheetahNet/NetMentor 管理应用程序。创建此模型后，选择 NetMentor 作为管理器名称。

陷阱、事件和警报

本节介绍 EventAdmin 和 EventModel 如何处理和管理 CheetahNet/NetMentor 集成发送的陷阱。

当 CheetahNet/NetMentor 将陷阱发送到 CA Spectrum 时，EventAdmin 模型接收这些陷阱并将其映射到 CA Spectrum 事件。这些事件将会发送到表示陷阱源的 EventModel。陷阱中发送的 **CNAlarmResource** 和 **CNAlarmSubResource** 变量绑定的值用于标识陷阱源。其中每个变量绑定都来自 CNAlarmsMib（CheetahNet 警报 MIB）。如果表示陷阱源的 EventModel 不存在，则会自动进行创建。

EventModel 接收事件后，会对其进行处理并将其用于创建或清除警报。下表介绍每个陷阱与 CA Spectrum 事件的映射关系以及如何处理事件。

陷阱 OID	陷阱名称	生成的事件	生成或清除的警报	警报重要级别
1.3.6.1.4.1.1283.10.6.1	设备已添加	0x3e00001	NA	NA
1.3.6.1.4.1.1283.10.6.2	设备已删除	0x3e00002	NA	NA
1.3.6.1.4.1.1283.10.6.3	配置已更改	0x3e00003	0x3e00003	橙色
1.3.6.1.4.1.1283.10.6.4	清除警报	0x3e00004	清除 0x3e00003、0x3e00005、0x3e00006、0x3e00007、0x3e00008	NA
1.3.6.1.4.1.1283.10.6.5	警告警报	0x3e00005		黄色
1.3.6.1.4.1.1283.10.6.6	次要警报	0x3e00006		黄色
1.3.6.1.4.1.1283.10.6.7	主要警报	0x3e00007		橙色
1.3.6.1.4.1.1283.10.6.8	关键警报	0x3e00008		红色

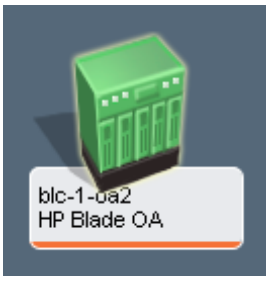
第 5 章： HP BladeSystem c-Class

本节介绍 CA Spectrum 对用于监控的 Hewlett-Packard (HP) BladeSystem c-Class 设备系列的支持。

此部分包含以下主题：

概述

CA Spectrum 采用增强认证支持 HP BladeSystem c-Class 设备系列。顶级管理使用 HP BladeSystem Onboard Administrator (OA) 模型。在拓扑中，为此设备系列建模后使用表示机箱的 OneClick 图标来表示。



CA Spectrum 机箱设备管理包括以下功能：

- 支持 C7000 和 C3000 机箱类型。
- OA 支持，在 CA Spectrum 中使用唯一的模型类型和机箱图标表示。
- 自动刀片建模。OA 建模后，会为每个已占用机箱插槽创建一个非拓扑模块模型。这些模型表示已占用插槽的硬件级别视图。
- 针对在刀片上运行的先前建模的设备模型或托管设备（Pingable 或支持 SNMP）进行自动机箱标识。
- “增强型接口”选项卡，显示给定机箱的刀片和接口的层次结构视图。机箱、托管设备、模块模型和接口在该层次结构中都具有唯一的图标。
- 可以使用右键单击菜单选项手动将托管设备与其机箱关联（或取消关联）。
- 从托管设备模型到其机箱的跳转导航。

- 从模块模型到其托管设备（如果已存在）的跳转导航。
- 支持多种基于机箱的 OneClick 视图。
- 基于机箱的定位器搜索。
- 增强型故障隔离功能可确保针对机箱范围的故障生成单个警报，从而消除多警报方案。

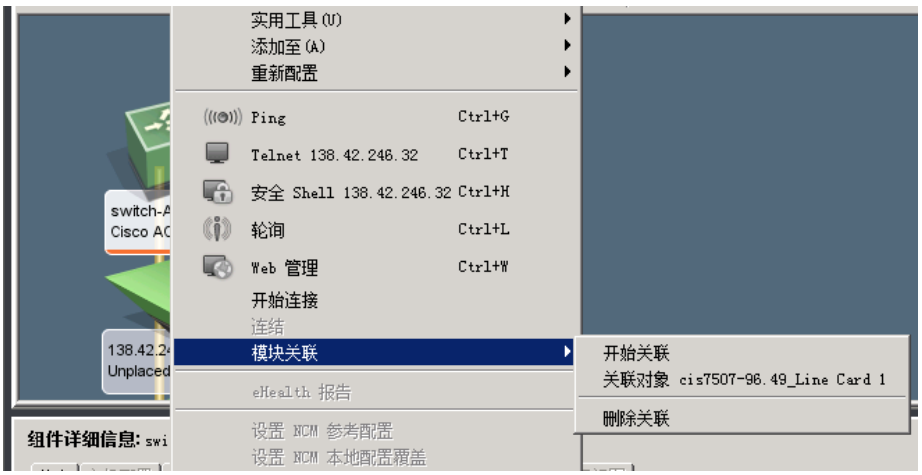
配置

默认情况下，每 5 分钟对机箱建模环境进行一次分析。可以通过修改 *configInterval* 属性，更改服务器和互联刀片的轮询发现间隔。此属性位于与 HPBladeOnboardAdmin 模型关联的单独应用程序模型上。对于服务器刀片，相关的应用程序模型是 HPServerBladeApp。对于互连刀片，相关的应用程序模型是 HPNetworkBladeApp。

使用“应用程序模型”下的“按设备 IP 地址”定位器选项卡，查找并选择相关的应用程序模型。可以使用 OneClick“组件详细信息”面板中的“属性”选项卡修改 *configInterval* 属性。

管理模块关联

建模 OA 会启动自动模块建模，并在模块和机箱之间建立关联。通过序列号标识的现有托管设备模型会自动与机箱关联。HP Insight Manager Agents 会提供所需序列号；这些是建议配置。否则，通过“模块关联”菜单选项使用手动关联。随后的“模块关联”菜单选项允许您通过“开始关联”、“关联对象”或“删除关联”等选项管理您的关联。



可以通过“OA 接口”选项卡查看所包含的模块及其关联的接口。支持列提供机箱位置（前部或后部）、插槽编号、模块类型以及说明。模块图标可帮助您标识硬件的类型。

从模块模型的角度来看，您可以使用资产信息 OneClick 视图中的机箱导航链接来标识父机箱。还可以使用同一视图中的“托管设备”链接来标识关联的托管设备（如果已存在）。

查找机箱

在“导航”面板的“定位器”选项卡中，您现在可以看到下列机箱搜索菜单选项。此功能可帮助您更改轮询发现间隔。

所有机箱

显示所有机箱模型（例如，HP OA 模型）

所有机箱托管设备

显示通过刀片上运行的 CA Spectrum 管理的所有设备模型。此搜索仅包括 Pingable 设备模型或支持 SNMP 的设备模型。不包括为机箱中每个已占用插槽创建的模块模型。

所有模块

显示所有模块模型（机箱中每个已占用插槽都有一个模块模型）。搜索不包括托管设备（支持 SNMP 或 ICMP 的设备）。它们表示已占用插槽的硬件级别视图。

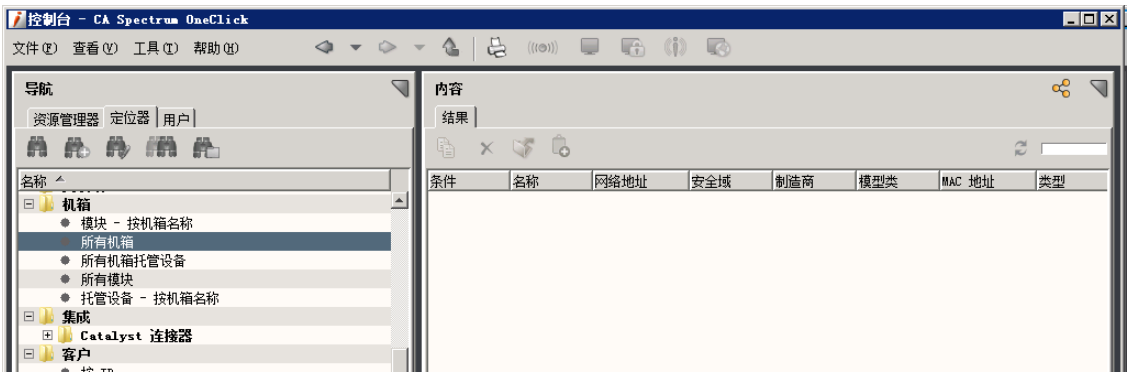
托管设备 - 按机箱名称

显示 CA Spectrum 管理的以及在指定机箱的刀片上运行的所有设备模型。您可以在随后的窗口中输入要查看的关联设备的特定机箱名称。

模块 - 按机箱名称

显示指定机箱的所有模块模型。您可以在随后的窗口中输入要查看的关联模块的特定机箱名称。

例如，选择“所有机箱”机箱搜索选项。将在“内容”面板中显示以下结果：



第 6 章： Juniper M 系列

本节介绍 CA Spectrum 中可用于支持 JnprRedundRtr（M20、M40e 和 M160）路由器的冗余组件监控智能。

此部分包含以下主题：

冗余组件监控智能

Juniper M20、M40e 和 M160 路由器支持冗余组件体系结构。冗余组件包括正常路由功能所必需的各种硬件。这些路由器的下列特定组件可进行被动监控和主动监控。

注意：所有不具备此功能的 Juniper M 系列路由器可按类型建模为 JNPR_Mxxx。此功能提供针对 JNPR_Mxxx 模型类型介绍的基本建模功能。

在调用被动监控或主动监控时，会检查每种冗余组件类型的状态更改。Juniper M 系列路由器的冗余组件根据下列路由器模型而有所不同：

- **Juniper M20 -** 系统和交换机主板、路由引擎。
- **Juniper M40e** - 路由引擎、其他控制系统、系统和转发模块、PFE 时钟发生器。
- **Juniper M160** - 路由引擎、其他控制系统、系统和转发模块、PFE 时钟发生器。

被动监控

仅在 CA Spectrum 与路由器失去联系后，被动监控智能才会报告冗余组件的状态更改。与设备重新建立联系后，CA Spectrum 会查询该设备。查询可确定组件状态是否发生更改。被动监控一直进行，但仅在先前提到的情况中检查组件状态的更改。

注意：与设备重新建立联系后，组件不总是处于“稳定”状态。组件要花费几分钟才能达到稳定状态。每种路由器类型（M20、M40e 或 M160）达到稳定状态所花费的时间不同。因此，在检查 M20、M40e 或 M160 组件的状态之前，被动监控需要等待 60、90 或 120 秒。

主动监控

主动监控用于报告冗余组件的状态更改。活动轮询间隔值确定主动监控的频率。此间隔确定主动监控智能查询设备以查找组件状态更改的频率（以秒为单位）。字段可以读/写。例如，如果活动轮询间隔设置为 60，则会每 60 秒针对组件状态更改查询一次设备。启用主动监控后，它将与被动监控提供的功能同时工作。

有几个其他选项，可用于启用或禁用此功能。首先，可将活动轮询间隔设置为 0，以禁用活动轮询。将此值更改为某个值（以秒为单位），可在主动监控属性设置为 True 时启用此功能。此外，将设备模型的轮询状态更改为 False 可禁用主动监控。

也可将设备模型的轮询间隔更改为 0 来禁用主动监控。禁用主动监控后，将轮询状态更改为 True，或将轮询间隔更改为非零值，不会再次启用主动监控。

从不要将主动轮询间隔设置为小于给定路由器类型的“稳定”状态时间的值。例如，M20 的“稳定”状态时间是 60 秒。主动轮询间隔的设置值必须大于 60。

下列属性用于控制主动监控智能：

- **ActiveMonitor** -启用或禁用主动监控智能。默认值为“已禁用”。
- **ActivePollInt** - 确定主动监控查询设备组件状态更改的频率（以秒为单位）。

第 7 章： Netscreen 防火墙

本节介绍 Netscreen 隧道接口模型类型 (nsTunnelIf) 及其功能。

此部分包含以下主题：

隧道接口

本节介绍 CA Spectrum 对监控 NetScreen 防火墙隧道接口的支持。

模型隧道接口

多种属性控制是否在您的 Netscreen 设备上为站点对站点隧道接口建模。通过使用下列过程，可为其他类型的隧道接口建模。默认情况下，CA Spectrum 不为拔号隧道或监控器状态设置为“关闭”的隧道建模。要启用对这些类型的隧道建模，请使用模型类型编辑器。

遵循这些步骤:

1. 关闭 SpectroSERVER，然后启动 Model Type Editor。
2. 要启用对拔号隧道建模，请使用“属性”选项卡上的“搜索”文本框查找 NSFirewallVPN 模型类型的 TunnelFilterTypes 属性 (0x12a17)。
3. 从此属性的值列表中删除值 1。
4. 要启用对监控器状态为“关闭”的隧道建模，请使用“属性”选项卡上的“搜索”文本框查找 NSFirewallVPN 模型类型的 TunnelFilterStates 属性 (0x12a19)。
5. 从该属性的值列表中删除值 0。
6. 保存您在 Model Type Editor 中的更改，然后重新启动 SpectroSERVER。
7. 使用每个设备模型均可用的“手动轮询设备”选项重新配置 Netscreen 模型。

   将为隧道接口建模。

隧道接口“堆栈”

隧道接口模型将创建为物理接口的子接口，这些物理接口的 IP 地址与隧道的本地地址匹配。此行为在 VPN-MON.mib 中表示。因为 NetScreen 设备不支持 ifStackTable，用于确定较底层接口的该机制是必要且有效的。

自动连接映射

在初始设备建模期间或接口重新配置期间，会首次激活隧道接口模型。然后，CA Spectrum 搜索表示其他隧道端点的隧道接口模型。如果找到这样的模型，将为这两个接口之间的连接建模。CA Spectrum 使用在 VPN-MON.mib 中指示的本地地址和远程地址来查找隧道的其他端点。

接口模型标识

可以通过在 VPN-MON.mib 中指示的本地地址和远程地址来标识隧道接口模型。此标识方法允许 CA Spectrum 在接口的 ifIndex 发生更改时保留此接口模型。

隧道接口的状态监控

在 NetScreen 设备上，隧道接口条目的 ifOperStatus 一直处于“打开”状态，直到其从 ifTable 消失。如果隧道模型变为“陈旧”且没有处理隧道的任何链路断开陷阱，CA Spectrum 将在该模型上生成红色警报。

在以下情况下会抑制该警报：

- 如果物理接口关闭（与抑制链路断开陷阱警报的情况相同）。
- 如果实时管道模型的“阻止链接端口的警报”设置为 TRUE，且满足以下一个条件：
  - 连接的设备不可访问（通过 SpectroSERVER）
  - “链接的”隧道接口模型有警报（红色）

为与隧道接口关联的端口启用活动链路后，此状态监控功能才可用。有关启用活动链路的信息，请参阅*《IT 基础架构建模与管理 - 管理员指南》*。

CA Spectrum 管理设置

建议进行以下 CA Spectrum 管理设置。

自动重新配置接口

如果希望 CA Spectrum 管理设备的分支隧道，请将 NetScreen 模型的此属性设置为 True。对于仅支持“用户”隧道的设备，将此属性设置为 False。如果设置为 True，无论设备的 SNMP 代理的 ifNumber 对象何时发生更改，CA Spectrum 都会重新配置接口模型。

在链路更改时重新配置

我们建议将所有 NetScreen 模型的此属性值设置为 False。如果设置为 True，在接收到每个“链路连通”或“链路断开”陷阱后，CA Spectrum 都会执行接口重新配置。

重新配置属性后发现

建议在重新配置所有 NetScreen 模型的属性后，保持“发现”的默认值 False。CA Spectrum 会为新发现隧道之间的连接建模，无论此设置如何。在大多数链路状态更改后，CA Spectrum 自动发现过程很少或几乎不会增加价值，NetScreen 设备尤为如此。对于这些设备，大多数链路状态更改表示隧道即将联通和断开，而不是配置新路由器或网桥端口。

创建子接口

如果希望 CA Spectrum 监控分支隧道，请将 NetScreen 模型的此属性设置为 True。如果将此属性设置为 False，CA Spectrum 不会为隧道接口创建模型。

阻止链接端口的警报

我们建议将实时管道模型的此属性设置为 True。当连接设备不可访问或链接的端口模型已有警报时，此设置会抑制端口警报。

第 8 章： Nortel Contivity VPN 交换机

本节介绍 CA Spectrum 对用于监控的 Nortel Contivity VPN 交换机的支持。

此部分包含以下主题：

隧道接口

本节介绍 Nortel Contivity 设备的隧道接口筛选功能。

隧道接口筛选

ContivityVPN 设备使用用户和分支 VPN 隧道接口条目填充 **ifTable**。然而，可能存在数千个用户 VPN 隧道接口。ContivityVPN 接口筛选功能可筛选用户隧道接口，并阻止这些接口的不必要建模。

注意：隧道接口筛选仅用于 **ContivityVPN** 类型的模型。

启用和禁用隧道 IF 筛选

下列步骤可启用或禁用隧道 IF 筛选：

遵循这些步骤:

1. 在模型类型编辑器中，设置属性 If_Mtype_Map 句柄 0x011fb4 的默认列表值。
2. 查看值列表，并查找 OID 实例 131。
3. 将值设置为 0。此设置可阻止为接口类型建模。
4. 要禁用隧道接口筛选并启用模型创建，请将此值设置为 220013。

隧道接口的建模

Contivity 设备模型的“创建子接口”属性控制创建表示站点到站点或分支隧道接口的模型。未创建表示“用户”隧道的模型。此行为与先前的版本一致。

隧道接口“堆栈”

隧道接口模型创建为物理接口的子接口。物理接口的 IP 地址与隧道 MIB 中指示的隧道的本地地址匹配。Contivity 设备不支持 ifStackTable。因此，用于确定较底层接口的该机制是必要且有效的。

自动连接映射

在初始设备建模期间或接口重新配置期间，会首次激活隧道接口模型。然后，CA Spectrum 搜索表示其他隧道端点的隧道接口模型。如果找到这样的模型，将为这两个接口之间的连接建模。CA Spectrum 使用在隧道 MIB (rfc2667) 中指示的本地地址和远程地址来查找其他隧道端点。

接口模型标识

可以通过在隧道 MIB (rfc2667) 中指示的本地地址和远程地址来标识隧道接口模型。此标识允许 CA Spectrum 在接口的 ifIndex 发生更改时保留此接口模型。

接口模型老化

在接口重新配置期间，MIB 中不再表示的任何接口模型都标记为“陈旧”，而不是被销毁。此功能允许 CA Spectrum 在隧道关闭时，保持隧道接口和其他设备之间的连接建模。然后，可将连接信息用于事件关联和故障抑制。

在随后的重新配置中，将设备模型的端口过时时间与接口模型的陈旧时段相比较。如果接口不在 MIB 中再次显示，则接口模型会在老化后被销毁。如果接口在 MIB 中再次显示，则接口模型会被标记为“当前”。通过将“isStale”属性设置为 True，将端口标记为陈旧。通过将设备上的“PortAgeOutTime”设置为若干分钟，可为每个设备设置端口老化时间。Contivity 设备的默认老化时间是两个小时（120 分钟）。

链路断开陷阱关联

要避免为单个网络停机发送多个警报，请将“隧道”接口模型的链路断开陷阱与其他状态关联。当较底层（即物理接口）关闭时，会抑制链路断开陷阱的警报。当实时管道模型的“阻止链接端口的警报”设置为 True 时，会抑制链路断开陷阱的警报。在下列情况下会抑制这些警报：

1. 连接的设备不可访问（通过 SpectroSERVER）。
2. “链接的”隧道接口模型有警报（红色）。

隧道接口的状态监控

在 Contivity 设备上，隧道接口条目的 ifOperStatus 一直处于“打开”状态，直到其从 ifTable 消失。当隧道模型变为“陈旧”且没有处理隧道的链路断开陷阱时，CA Spectrum 将在模型上生成红色警报。抑制红色警报与抑制链路断开陷阱警报的情况相同。当较底层（即物理接口）关闭时，会抑制红色警报。当实时管道模型的“阻止链接端口的警报”参数设置为 True 时，会抑制此警报。

在下列情况下会抑制该警报：

1. 连接的设备不可访问（通过 SpectroSERVER）。
2. “链接的”隧道接口模型有警报（红色）。

Contivity 管理设置

建议进行以下 Contivity 设置。

启用隧道 MIB

我们建议启用所有托管 Contivity 设备上的隧道 IP MIB。此设置允许 CA Spectrum 创建表示设备上隧道端点的模型。可从 Contivity Web 管理页面的 ADMIN->SNMP 部分启用和禁用此 MIB。

启用链路连通/断开陷阱

我们建议为物理接口和“关闭的”分支隧道启用链路连通和链路断开陷阱。此设置提供链路状态更改的 CA Spectrum 即时通知。我们的测试显示“OnDemand”隧道的链路陷阱不提供大量值。在陷阱发送前，必须关闭隧道约 15 分钟。

关闭您的监控隧道

我们建议连接监控至关重要的所有隧道是“关闭的”。当“OnDemand”隧道断开时，CA Spectrum 不会针对这些隧道发出警报。具体来说，与 Tunnel_If 模型的链路断开陷阱属性有关的警报可确定其是响应链路断开陷阱还是响应对 isStale 属性的更改。值为 Always (1) 会导致 CA Spectrum 处理这些事件；值为 Never (0) 会导致 CA Spectrum 忽略这些事件。当 CA Spectrum 为 Contivity 创建 Tunnel_If 模型时，它会将“关闭的”分支隧道的此属性设置为“Always”，将“OnDemand”隧道的此属性设置为“Never”。

从全局属性编辑器的“配置”选项卡中，更改链路断开设置相关的警报。我们建议保持 CA Spectrum 已对其进行的设置。

CA Spectrum 管理设置

建议进行以下 CA Spectrum 管理设置。

自动重新配置接口

如果希望 CA Spectrum 管理设备的分支隧道，请将 Contivity 模型的此属性设置为 True。对于仅支持“用户”隧道的设备，将此属性设置为 False。如果设置为 True，无论设备上的 SNMP 代理的 ifNumber 对象何时发生更改，CA Spectrum 都会重新配置接口模型。

在链路更改时重新配置

我们建议将所有 Contivity 模型的此属性设置为 False。如果设置为 True，在接收到每个链路连通或链路关闭陷阱后，CA Spectrum 都会执行接口重新配置。

重新配置后发现

我们建议在重新配置所有 Contivity 模型的属性后，保持“发现”的默认值 False。CA Spectrum 会为新发现隧道之间的连接建模，无论此设置如何。在大多数链路状态更改后，CA Spectrum 自动发现过程很少或几乎不会增加价值，Contivity 设备尤为如此。对于这些设备，大多数链路状态更改表示隧道即将联通和断开，而不是配置新路由器或网桥端口。

创建子接口

如果希望 CA Spectrum 监控分支隧道，请将 Contivity 模型的此属性设置为 True。如果将此属性设置为 False，CA Spectrum 不会为隧道接口创建模型。

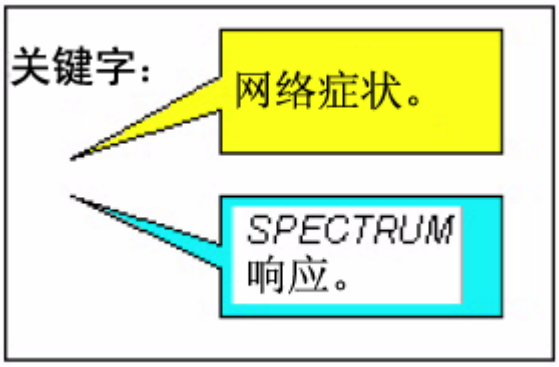
阻止链接端口的警报

我们建议将实时管道模型的此属性设置为 True。当连接设备不可访问或链接的端口模型已有警报时，此设置会抑制端口警报。

Contivity 故障情景

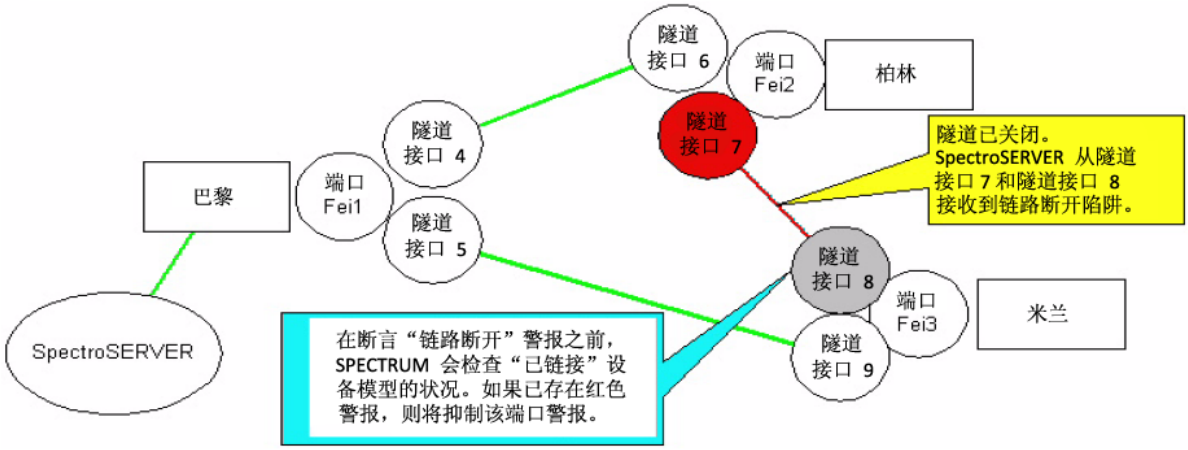
本节介绍 VPN 环境中可能存在的故障情景以及 CA Spectrum 对每个情景的响应。

下列项适用于本节中的每个图表：



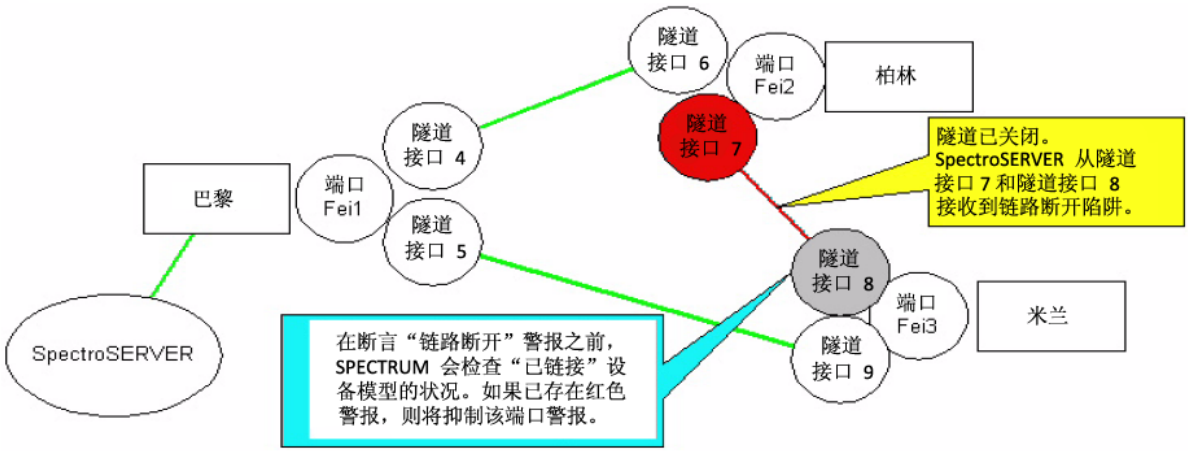
一个关闭隧道的两个链路断开陷阱

在下列情景中，SpectroSERVER 与该网状环境中的所有托管元素保持联系，但两台设备之间的隧道已关闭。CA Spectrum 接收到两个链路断开陷阱。一个隧道接口发出警报；另一个警报被抑制。



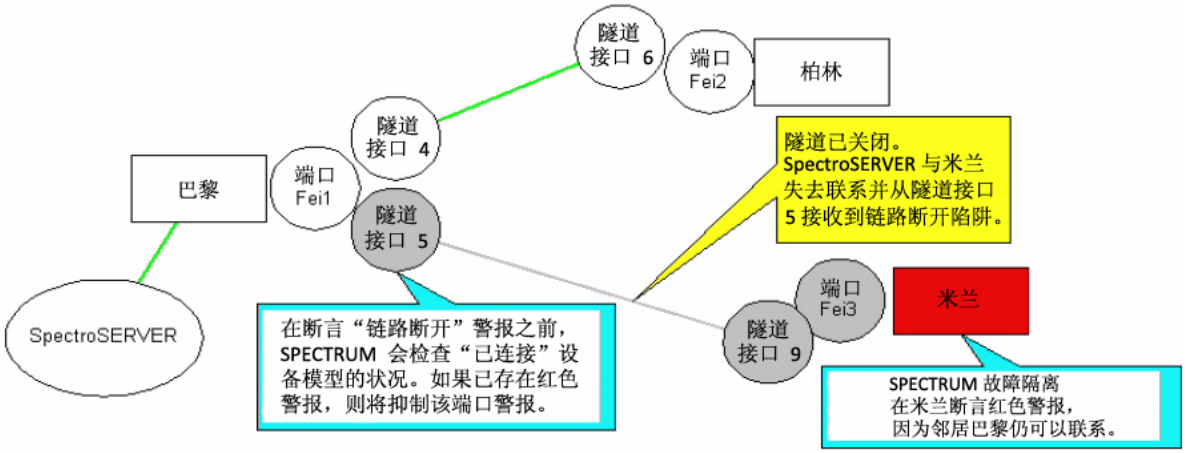
失去联系和链路断开陷阱

在下列情景中，CA Spectrum 与轴辐式网络中的“轮辐”Contivity 失去联系。CA Spectrum 还从中心接收到链路断开陷阱，指示了到丢失设备的隧道。CA Spectrum 为丢失的设备发送警报，并抑制陷阱指示的隧道接口的相关警报。



物理端口关闭、失去联系和链路断开陷阱

在下列情景中，Contivity 的物理端口关闭或失去与公共网络的链接。CA Spectrum 获得 Contivity 的物理端口和隧道的链路断开陷阱，并与远程 Contivity 设备失去联系。隧道接口模型的链路断开警报被抑制，但是 CA Spectrum 故障隔离在丢失的 Contivity 设备模型上创建了红色警报，其原因是其邻近模型处于“打开”状态。



已知异常

CA Spectrum 包含以下已知异常。

Sub-Interface Changes

在创建隧道接口模型后 Contivity 模型的“创建子接口”从 True 变为 False 时，隧道接口模型在接口重新配置后不会被立即销毁。相反，这些模型会变为陈旧并且开始老化。要为 Contivity 设备的子集启用隧道监控，请将“创建子接口”的默认值设置为 False。然后，针对需要隧道监控的 Contivity 设备的各个模型，将“创建子接口”设置为 True。

自动发现和公共地址

通常，VPN 中 Contivity 设备上的公共地址位于不同的子网中，其原因是多个路由器将其分开。具有公共接口的 Contivity 设备可能存在于同一子网上。在这种情况下，CA Spectrum 自动发现可以尝试映射公共接口的连接。结果将是 LAN 容器和带有 Contivity 模型管道的 Contivity 模型位于相同的拓扑视图中。没有 LAN 的扇出模型将连接到 Contivity 设备的公共接口模型。

端口老化

CA Spectrum 端口老化并非主动形成。当隧道变为非活动状态时，隧道接口模型被标记为“陈旧”。在设备“portAgeOutTime”之后出现任何进一步的重新配置都会导致隧道模型被销毁。但如果设备没有出现进一步的重新配置，“陈旧”隧道接口模型仍然会存在。

例如，考虑轮询间隔为 5 分钟以及 portAgeOutTime 为 30 分钟。如果隧道在 10:27 时关闭，CA Spectrum 在 10:30 时轮询，CA Spectrum 会检测到 ifNumber 更改，并执行接口重新配置。在此过程中，隧道接口被标记为陈旧。如果不重新打开隧道，隧道接口模型会在 11:00 被销毁。ifNumber 一周内未再发生变化时，接口重新配置在一周内无法再次运行。此隧道接口模型在一周内仍保持陈旧，然后会被销毁。