CA Spectrum®

デバイス管理リファレンス ガイド

リリース 9.4

ca technologies

CA への連絡先

テクニカル サポートの詳細については、弊社テクニカル サポートの Web サイト（http://www.ca.com/jp/support/）をご覧ください。

目次

第 1 章: はじめに 9

第 2 章: AM Communications 11

サポートされているデバイス 11
CA Spectrum モデル 11
トラップ、イベント、アラーム 12

第 3 章: Ceterus Universal 15

トラップ処理 15

第 4 章: Cheetah ゲートウェイ 17

サポートされているデバイス 17
CA Spectrum モデル 18
EventAdmin モデルの作成 18
トラップ、イベント、アラーム 18

第 5 章: HP BladeSystem c- Class 21

概要 21
設定 22
モジュール関連付けの管理 23
シャーシの特定 26

第 6 章: Juniper M シリーズ 29

冗長コンポーネント監視インテリジェンス 29
パッシブ監視 30
アクティブ監視 30

第 7 章: Netscreen ファイアウォール 33

トンネル インターフェース 33
トンネル インターフェースのモデリング 33
トンネル インターフェースの「スタッキング」 34

自動接続マッピング 34
インターフェース モデルの識別 34
トンネル インターフェースのステータス監視 35
CA Spectrum の管理設定 35
インターフェースの自動再設定 35
リンク変更の再設定 36
再設定後にディスカバリ属性 36
サブインターフェースの作成 36
リンクされたポートのアラームを抑制 36

第 8 章 : Nortel Contivity VPN スイッチ 37

トンネル インターフェース 37
トンネル インターフェース フィルタリング 37
トンネル IF フィルタリングの有効化と無効化 38
トンネル インターフェースのモデリング 38
トンネル インターフェースの「スタッキング」 38
自動接続マッピング 39
インターフェース モデルの識別 39
インターフェース モデルの失効 39
リンク ダウン トラップ相関 40
トンネル インターフェースのステータス監視 40
Contivity の管理設定 40
トンネル MIB の有効化 41
リンク アップ/リンク ダウン トラップの有効化 41
監視対象トンネルのネイルアップ 41
CA Spectrum の管理設定 41
インターフェースの自動再設定 42
リンク変更の再設定 42
再設定後にディスカバリ 42
サブインターフェースの作成 42
リンクされたポートのアラームを抑制 43
Contivity の障害シナリオ 43
1 つのダウン トンネルに対する 2 つのリンク ダウン トラップ 44
接続の切断とリンク ダウン トラップ 45
物理的なポート ダウン、接続の切断、およびリンク ダウン トラップ 46
既知の問題 46
サブインターフェースの変更 47
自動ディスカバリとパブリック アドレス 47
ポートの失効 48

第 1 章: はじめに

このガイドでは、（アルファベット順に示された）以下のデバイスに対する CA Spectrum デバイス管理ドキュメントを紹介します。

- 第 2 章： AM Communications
- 第 3 章： Ceterus Universal
- 第 4 章： Cheetah ゲートウェイ
- 第 5 章： HP BladeSystem c-Class 認証
- 第 6 章： Juniper M シリーズ
- 第 7 章：Netscreen ファイアウォール
- 第 8 章：Nortel Contivity VPN スイッチ

第 2 章: AM Communications

このセクションでは、AM Communications 統合用の CA Spectrum デバイス管理ドキュメントについて紹介します。

このセクションには、以下のトピックが含まれています。

サポートされているデバイス (P. 11)
CA Spectrum モデル (P. 11)
トラップ、イベント、アラーム (P. 12)

サポートされているデバイス

AM Communications は、非 SNMP のブロードバンド コンポーネント用のネットワーク管理製品を開発します。 この製品は RF（無線周波数）、HFC（Hybrid Fiber Coax）コンポーネントを監視します。 オプションの SNMP エージェント モジュールが用意された、Cheetah の NetMentor ソフトウェア パッケージは、専用イベントを SNMPv1/v2 のアラームおよびトラップに変換します。 この管理モジュールは、汎用 Southbound Application Gateway の統合を使って、トラップ受信とイベント作成用の場所を提供します。

この管理モジュールは Omni2000 プロキシ エージェントをサポートします。 Omni2000 Proxy Agent は AM Communication の HFC コンポーネント監視ソリューションです。

CA Spectrum モデル

特定の AM Communications モデル タイプは作成されません。 Southbound Gateway は、モデル タイプ EventAdmin および EventModel を提供します。これらのモデル タイプは、Omni2000 プロキシ エージェントが CA Spectrum に送信する情報を管理するために使用されます。

EventAdmin は Omni2000 プロキシ エージェントを表すために使用されるコンテナ モデル タイプです。 EventModels は、Omni2000 プロキシ エージェントが CA Spectrum へ渡すトラップ情報の一意のソースを表します。EventModels は、EventAdmin モデルからドリルダウンすることによってアクセスできるトポロジ ビューに自動的に配置されます。 これらのアイコンはイベント ソース（必ずしも物理デバイスやコンポーネントとは限りません）を表すため、相互の接続を表していません。

EventAdmin モデルが Omni2000 プロキシ エージェントからトラップを受信すると、このトラップは CA Spectrum イベントにマッピングされます。さらに、イベントを適切な EventModel に送信して、処理を行います。 トラップ情報の一意のソースを表す EventModel が存在しない場合、EventModel が自動作成されます。

「SouthBound Gateway Toolkit Guide」には、EventAdmin モデルを作成するための手順が記載されています。AM Communications 管理アプリケーションを表すために EventAdmin モデルを使用します。

このモデルを作成する場合、Omni2000 のマネージャ名を選択します。

トラップ、イベント、アラーム

このセクションでは、AM Communication Integration がトラップを送信する方法について説明します。また、EventAdmin と EventModels がこれらのトラップをどのように処理して管理するかについても説明します。

Omni2000 Proxy Agent が CA Spectrum にトラップを送信する場合、EventAdmin モデルがそのトラップを受信し、CA Spectrum イベントにマッピングします。 これらのイベントは、トラップ ソースを表す EventModel に送信されます。 トラップで送信される NEModelNumber 変数バインディングの値によって、トラップ ソースを識別します。 この変数バインディングは AMC-MIB から取得します。トラップ ソースを表す EventModel が存在しない場合、自動的に作成されます。

EventModel がイベントを受信すると、そのイベントが処理され、アラームの生成またはクリアのために使用できます。次のテーブルは、CA Spectrum イベントへの各トラップのマッピング方法と、イベントの処理方法を示します。

トラップ	アラーム	イベント コード	説明
NewNEFound		0x3eb0001	HFC Proxy は新しい Network Element を検出しました。
Communicatio-nsStatus		0x3eb0002	HFC Proxy は、ネットワーク エレメントとの通信を切断またはリストアしました。
ConfigurationChange	オレンジ	ox3eb0003	任意のタイプの単一変数の設定が（任意のインターフェース経由で）変更されました。
StatusChange		0x3eb0004	アクティブなアラームが解除されました。
Alarm	オレンジ	0x3eb0005	アラームがプロキシ エージェントによって検出されました。
ToBeSendQue-ueOverflow	オレンジ	0x3eb0006	SNMP エージェントの TrapToBeSendQueue はフルです。
NewNELost	オレンジ	0x3eb0007	HFC Proxy は、新しいネットワーク エレメント消失を検出しました。

第 3 章: Ceterus Universal

このセクションでは、Ceterus Universal Transport System デバイスの一般的な展開シナリオと、CA Spectrum でそれらのデバイスをモデリングする方法について説明します。

このセクションには、以下のトピックが含まれています。

トラップ処理 (P. 15)

トラップ処理

EOC チャネルを介してローカル デバイスにトラップを転送するように、リモート Ceterus デバイスを設定することができます。 この設定では、ローカル デバイスはゲートウェイとして機能し、これらのトラップを転送します。 この機能の詳細については、Ceterus のドキュメントを参照してください。

また、SNMP のターゲット IP アドレスを使ってリモート デバイスを設定することもできます。この設定では、デバイスは管理ポートを介してトラップを送信します。

これらの機能を両方とも同時に設定した場合、CA Spectrum は重複したトラップを受信します。 Ceterus 管理モジュールは、このケースを処理するように設計されています。 このモジュールは受信する Ceterus トラップを評価し、最も適切な CA Spectrum デバイス モデルにこれらのトラップを生成します。 管理モジュールは、トラップ内の Ceterus デバイス コミュニティ文字列を、デバイスの sysName の値と比較することにより、適切なモデルを選択します。

重要: CA Spectrum はこの決定を下すために、デバイスのコミュニティ名に依存します。 その結果、コミュニティ名と sysName を同期する必要があります。デフォルトでは、sysName のポーリングが 5 分ごとに発生します。sysName がポーリングを通じて正しく更新されるまで、TID の変更が、トラップの処理に影響を与える可能性があります。 管理者が特定の Ceterus デバイスで TID （sysName）を「デバイス A」から「デバイス B」に変更した場合、デバイスはそのモデルにトラップを送信します。 この場合、CA Spectrum はトラップを処理できなくなります。sysName が更新される（デフォルトでは最大 5 分間）まで、トラップ処理は再開されません。

第 4 章: Cheetah ゲートウェイ

このセクションでは、Cheetah™ ネットワーク管理製品を監視するための CA Spectrum サポートについて説明します。

このセクションには、以下のトピックが含まれています。

サポートされているデバイス (P. 17)
CA Spectrum モデル (P. 18)
EventAdmin モデルの作成 (P. 18)
トラップ、イベント、アラーム (P. 18)

サポートされているデバイス

CheetahNet™（以前の NetMentor™）が含まれる Cheetah™ 製品は、非 SNMP ブロードバンド コンポーネント用のネットワーク管理製品です。 この製品は RF （無線周波数）および HFC （Hybrid Fiber Coax）コンポーネントを監視します。 オプションの SNMP エージェント モジュールが用意された CheetahNet/NetMentor ソフトウェア パッケージは、専用イベントを SNMPv1/v2 のアラームおよびトラップに変換します。 この管理モジュールは、CA Spectrum Southbound Gateway 統合を使って、CA Spectrum でのトラップの受信とイベントの作成を可能にします。

この管理モジュールは、SNMP エージェント モジュールなどの CheetahNet/NetMentor 管理アプリケーションと CA Spectrum 間の統合を実現します。 この統合では、以下のタイプの HFC デバイスに関するイベントをレポートできます。

- 電源
- 増幅器
- ライン モニタ
- テスト ポイント
- ファイバー ノード
- HEFiber

CA Spectrum モデル

特定の Cheetah モデル タイプは作成されません。 Southbound Gateway は EventAdmin および EventModel モデル タイプを提供します。これらのモデル タイプは、NetMentor が CA Spectrum に送信する情報を管理するために使用されます。

EventAdmin は、NetMentor 管理アプリケーションを表すために使われるコンテナ モデル タイプです。 EventModels は、CheetahNet/NetMentor アプリケーションが CA Spectrum へ渡すトラップ情報の一意のソースを表します。 EventModels は、EventAdmin モデルからドリルダウンすることでアクセスできるトポロジ ビューに自動的に配置されます。 これらのアイコンはイベント ソース（必ずしも物理デバイスやコンポーネントとは限りません）を表すため、相互の接続を表していません。

EventAdmin モデルが CheetahNet/NetMentor アプリケーションからトラップを受信すると、このトラップは CA Spectrum イベントにマッピングされます。 EventAdmin はまた、イベントを適切な EventModel に送信して、処理を行います。 トラップ情報の一意のソースを表す EventModel が存在しない場合、EventModel が自動作成されます。

EventAdmin モデルの作成

「SouthBound Gateway Toolkit Guide」には、EventAdmin モデルを作成するための手順が記載されています。 CheetahNet/NetMentor 管理アプリケーションを表すために EventAdmin モデルを使用します。 このモデルを作成する場合、NetMentor のマネージャ名を選択します。

トラップ、イベント、アラーム

このセクションでは、EventAdmin と EventModel が CheetahNet/NetMentor 統合によって送信されるトラップをどのように処理し管理するかについて説明します。

CheetahNet/NetMentor が CA Spectrum にトラップを送信する場合、EventAdmin モデルはこれらのトラップを受信し、トラップを CA Spectrum イベントにマッピングします。 これらのイベントは、トラップ ソースを表す EventModel に送信されます。 トラップで送信される **CNAlarmResource** と **CNAlarmSubResource** 変数バインディングの値によって、トラップ ソースを識別します。 これらの各変数バインディングは、CNAlarmsMib （CheetahNet Alarms MIB）から取得します。 トラップ ソースを表す EventModel が存在しない場合、自動的に作成されます。

EventModel がイベントを受信すると、そのイベントが処理され、アラームの生成またはクリアのために使用できます。次のテーブルは、CA Spectrum イベントへの各トラップのマッピング方法と、イベントの処理方法について説明します。

トラップ OID	トラップ名	生成されるイベント	生成またはクリアされるアラーム	アラーム重大度
1.3.6.1.4.1.1283.10.6.1	追加されたデバイス	0x3e00001	該当なし	該当なし
1.3.6.1.4.1.1283.10.6.2	削除されたデバイス	0x3e00002	該当なし	該当なし
1.3.6.1.4.1.1283.10.6.3	変更された設定	0x3e00003	0x3e00003	オレンジ
1.3.6.1.4.1.1283.10.6.4	アラームのクリア	0x3e00004	0x3e00003、0x3e00005、0x3e00006、0x3e00007、0x3e00008 のクリア	該当なし
1.3.6.1.4.1.1283.10.6.5	警告アラーム	0x3e00005		イエロー
1.3.6.1.4.1.1283.10.6.6	マイナー アラーム	0x3e00006		イエロー
1.3.6.1.4.1.1283.10.6.7	メジャー アラーム	0x3e00007		オレンジ
1.3.6.1.4.1.1283.10.6.8	重大アラーム	0x3e00008		レッド

第 5 章: HP BladeSystem c- Class

このセクションでは、Hewlett-Packard （HP）の BladeSystem c-Class デバイス ファミリを監視するための CA Spectrum のサポートについて説明します。

このセクションには、以下のトピックが含まれています。

概要 (P. 21)
設定 (P. 22)
モジュール関連付けの管理 (P. 23)
シャーシの特定 (P. 26)

概要

HP BladeSystem c-Class デバイス ファミリのサポートは、増強された認証を使用すると CA Spectrum で使用可能になります。 トップレベルの管理は、HP BladeSystem Onboard Administrator （OA）のモデルを使用します。 このデバイス ファミリはモデリングされ、シャーシを表す OneClick アイコンを使って、トポロジ内に表示されます。

CA Spectrum シャーシ デバイス管理には、以下の機能が含まれます。

- C7000 および C3000 シャーシ タイプに対するサポート。
- 一意のモデル タイプおよびシャーシ アイコンを使って CA Spectrum に表示される OA サポート。
- 自動ブレード モデリング。 OA モデリングの実行後、非トポロジ モジュール モデルは、占有されているシャーシ スロットごとに作成されます。 これらのモデルは、専用されているスロットのハードウェア レベル ビューを表します。

- ブレード上で実行されている、以前モデリングされた Ping 可能または SNMP 対応いずれかのデバイス モデル（管理デバイス）の自動シャーシ識別。
- 指定されたシャーシに対するブレードおよびインターフェースの階層ビューを表示する拡張された［インターフェース］タブ。 それぞれが階層内に一意のアイコンを所有している、シャーシ、管理デバイス、モジュール モデル、およびインターフェース。
- 管理デバイスは、右クリック メニュー オプションを使用して、シャーシに手動で関連付ける（または関連付けを解除する）ことができます。
- 管理デバイス モデルからシャーシへのナビゲーション ジャンプ。
- モジュール モデルから管理デバイス（存在する場合）へのナビゲーション ジャンプ。
- 複数のシャーシ ベースの OneClick ビューのサポート。
- シャーシ ベースのロケータ検索。
- 拡張された障害分離機能を使用すると、シャーシ全体に関する障害で単一アラームが確実に生成されるため、複数のアラームが発生するシナリオが除去されます。

設定

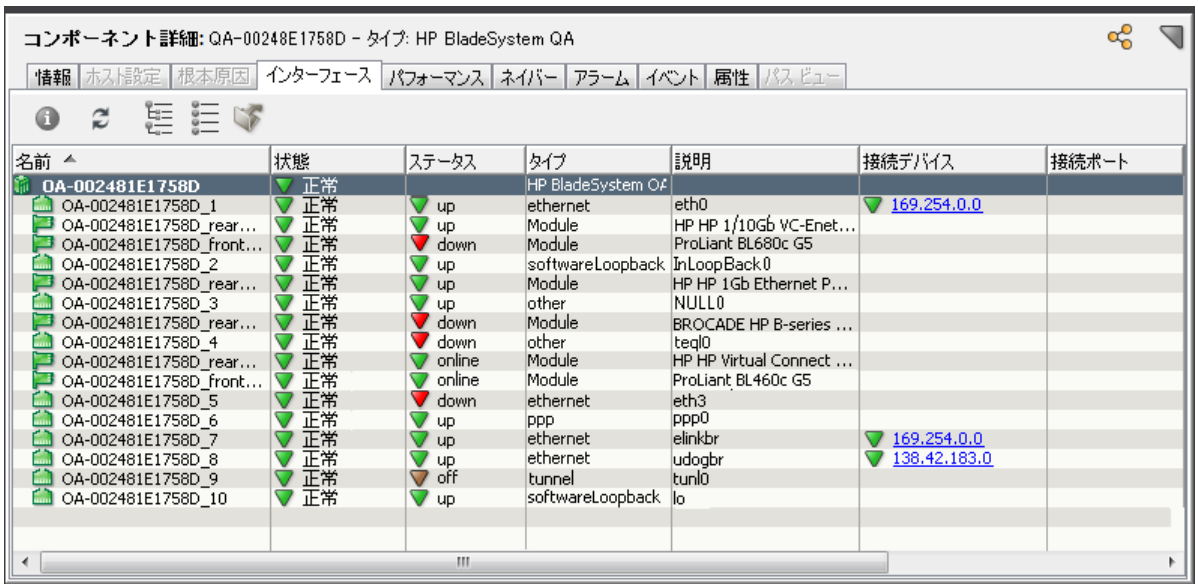
シャーシ モデリング環境の分析は、デフォルトでは 5 分ごとに発生します。 *configInterval* 属性を変更することで、サーバと相互接続ブレードに対するポーリング ディスカバリ間隔を変更できます。 この属性は、HPBladeOnboardAdmin モデルに関連付けられる個別のアプリケーション モデルに設定されます。サーバ ブレードの場合、関連するアプリケーション モデルは HPServerBladeApp です。 相互接続ブレードの場合、関連するアプリケーション モデルは HPNetworkBladeApp です。

［アプリケーション モデル］の下にある［デバイス IP アドレス］ロケータ タブ検索を使って、関連するアプリケーション モデルの特定と選択を行います。 OneClick のコンポーネント詳細画面の［属性］タブを使って、*configInterval* 属性を変更できます。

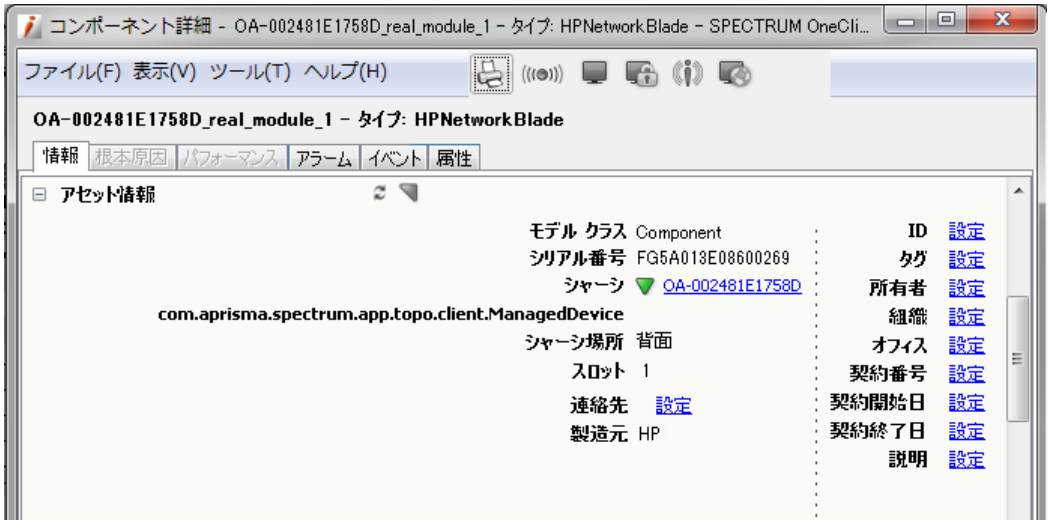
モジュール関連付けの管理

OA をモデリングすると、自動化されたモジュールのモデリングが開始され、モジュールとシャーシ間の関連付けが作成されます。 シリアル番号によって識別可能な、既存の管理対象デバイス モデルは、自動的にシャーシに関連付けられます。HP Insight Manager Agent は、要求されたシリアル番号を提供します。これが推奨設定です。そうでない場合は、［モジュール関連付け］メニュー オプションを介した手動関連付けを使用します。以降の［モジュール関連付け］メニュー オプションでは、［関連付けの開始］、［関連付けの対象］、［関連付けの削除］などのオプションを使って、関連付けを管理することができます。

［OA インターフェース］タブを介して、含まれているモジュールと関連付けられているインターフェースを表示できます。 サポート対象の列は、シャーシ場所（前面または後部）、スロット番号、モジュール タイプおよび説明を提供します。 モジュール アイコンにより、ハードウェアのタイプを識別できます。

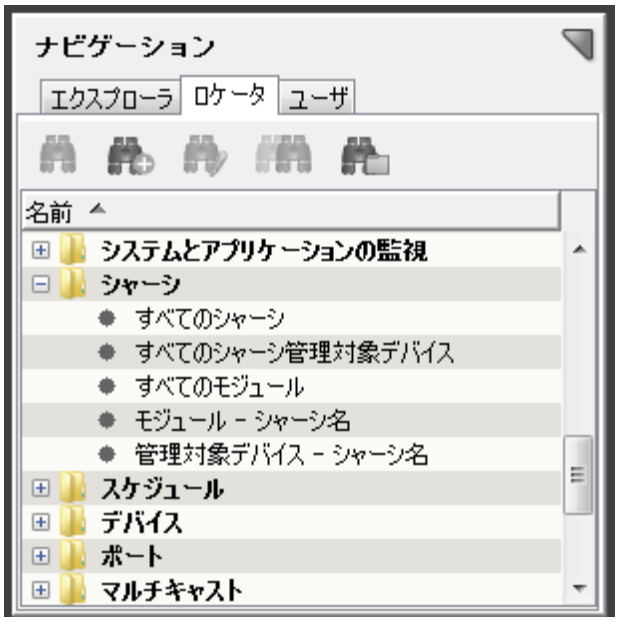


モジュール モデルから見た場合、［アセット情報］ OneClick ビューの［シャーシ］ナビゲーション リンクを使用して、親シャーシを識別できます。 また、同じビューの［管理対象デバイス］のリンクを使用して、関連する管理対象デバイス（存在する場合）を識別することもできます。



シャーシの特定

ナビゲーション画面の［ロケータ］タブには、以下の［シャーシ］検索メニュー オプションがあります。 この機能を使用すると、ポーリング ディスカバリ間隔を変更できます。



すべてのシャーシ

すべてのシャーシ モデルを表示します（HP OA モデルなど）

すべてのシャーシ管理対象デバイス

ブレードで実行されている、CA Spectrum によって管理されているすべてのデバイス モデルを表示します。 この検索では、Ping 可能なデバイス モデル、または SNMP 対応のデバイス モデルだけが対象になります。シャーシの占有されているスロットごとに作成されたモジュール モデルは、対象になりません。

すべてのモジュール

シャーシの占有されているスロットごとに、すべてのモジュール モデルが表示されます。管理対象デバイス（SNMP 対応または ICMP 対応デバイス）は検索の対象になりません。 これらのデバイスは、占有されたスロットのハードウェア レベル ビューを表します。

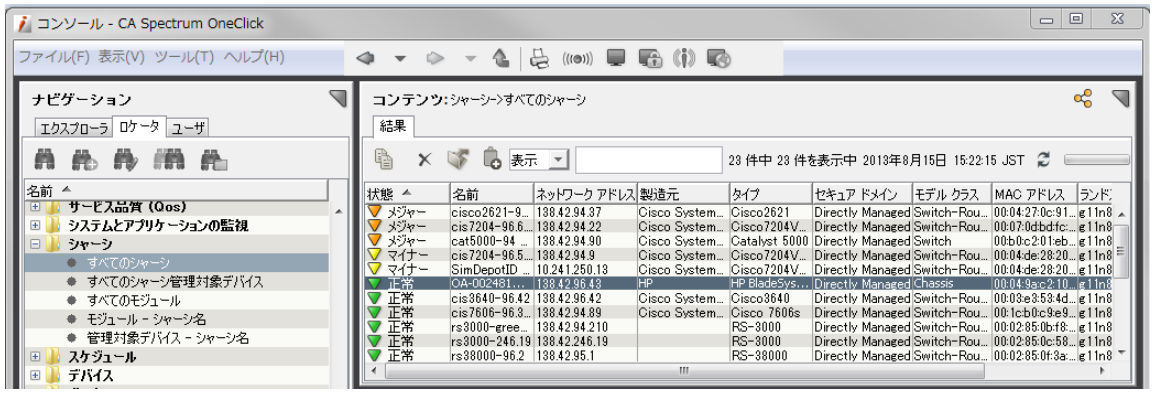
管理対象デバイス - シャーシ名

CA Spectrum が管理し、指定されたシャーシのブレード上で実行されているデバイス モデルがすべて表示されます。 以降のウィンドウでは、関連するデバイスを表示する特定のシャーシ名を入力できます。

モジュール - シャーシ名

指定されたシャーシのモジュール モデルがすべて表示されます。以降のウィンドウでは、関連するモジュールを表示する特定のシャーシ名を入力できます。

例として、シャーシ検索オプションで[すべてのシャーシ]を選択します。コンテンツ画面に次の結果が表示されます。



第 6 章: Juniper M シリーズ

このセクションでは、CA Spectrum 内の JnprRedundRtr （M20、M40e、および M160）ルータのサポートに使用可能な冗長コンポーネント監視インテリジェンスについて説明します。

このセクションには、以下のトピックが含まれています。

冗長コンポーネント監視インテリジェンス (P. 29)

冗長コンポーネント監視インテリジェンス

Juniper M20、M40e、および M160 ルータは、冗長コンポーネント アーキテクチャをサポートしています。 冗長コンポーネントには、適切なルーティング機能に必要なハードウェアも含まれています。 これらのルータ用の固有コンポーネントは、パッシブ監視とアクティブ監視です。

注: この機能がない場合、Juniper M シリーズ ルータはすべて、JNPR_Mxxx タイプとしてモデリングできます。 JNPR_Mxxx モデル タイプに対して説明されているように、この機能は基本的なモデリング機能を提供します。

パッシブ監視アクティブ監視のいずれかが呼び出されると、冗長コンポーネントの各タイプでステータス変更がないかチェックされます。 Juniper M シリーズ ルータの冗長コンポーネントは、以下のルータ モデルに基づいて異なります。

- **Juniper M20** - システム、スイッチ ボード、ルーティング エンジン
- **Juniper M40e** - エンジン、その他のコントロール システム、システムと転送モジュール、PFE クロック ジェネレータ
- **Juniper M160** - エンジン、その他のコントロール システム、システムと転送モジュール、PFE クロック ジェネレータ

パッシブ監視

CA Spectrum がルータとの接続を喪失した後はじめて、パッシブ監視インテリジェンスは、冗長コンポーネントの状態をレポートします。 デバイスとの接続が再確立されると、CA Spectrum はデバイスへのクエリを実行します。 クエリによって、コンポーネントのステータス変更が発生したかどうかが判断されます。 パッシブ監視 Monitoring は常にオンですが、パッシブ監視はあらかじめ指定されたケースのコンポーネント ステータス変更だけをチェックします。

注: デバイスとの接続が再確立された場合、コンポーネントは必ずしも「安定した」状態とは限りません。 コンポーネントの状態が安定するまで数分かかります。 各ルータ タイプ（M20、M40e、または M160）は、安定状態になるまでの時間が異なります。そのため、パッシブ監視では、M20、M40e、または M160 コンポーネントの状態を確認する前に 60、90、または 120 秒待機します。

アクティブ監視

アクティブ監視は、冗長コンポーネントのステータスの変化をレポートするために使用されます。 アクティブ ポーリング間隔の値は、アクティブ監視の頻度を決定します。 この間隔によって、アクティブ監視インテリジェンスがコンポーネントのステータス変更を確認するために、どれくらいの頻度でデバイスへのクエリを実行するかが決まります。 このフィールドは読み書き可能です。 たとえば、アクティブ ポーリング間隔を 60 に設定すると、コンポーネント ステータスの変更がないか、60 秒ごとにデバイスへのクエリが実行されます。 アクティブ監視が有効な場合、パッシブ監視が提供する機能への追加として、アクティブ監視が機能します。

この機能を有効にするか無効にすることについては、他にいくつかのオプションがあります。 まず、アクティブ ポーリング間隔を 0 に設定して、アクティブなポーリングを無効にすることができます。 アクティブ監視属性を True に設定した場合、この機能を有効にするには、値を秒単位の値に変更します。デバイス モデルのポーリング ステータスを False に変更しても、アクティブ監視は無効になります。

デバイス モデルのポーリング間隔を 0 に設定しても、アクティブ監視は無効になります。 アクティブ監視が無効な場合、ポーリング ステータスを True に変更したり、ポーリング間隔を 0 以外の値に変更しても、アクティブ監視は有効になりません。

指定されたルータ タイプに対して「安定」状態に達する時間より小さな値を、アクティブ ポーリング間隔に設定しないでください。 たとえば、M20 が「安定」状態に達するまでの時間は 60 秒です。 アクティブ ポーリング間隔は 60 より大きな値に設定します。

次の属性は、アクティブ監視インテリジェンスをコントロールします。

- **ActiveMonitor** - アクティブ監視インテリジェンスの有効/無効を切り替えます。 デフォルト値は「無効」です。
- **ActivePollInt** - コンポーネント ステータス変更目的で、デバイスへのアクティブ監視クエリの頻度（秒）を決定します。

第 7 章: Netscreen ファイアウォール

このセクションでは、Netscreen トンネル インターフェース モデル タイプ（nsTunnelIf）とその機能について説明します。

このセクションには、以下のトピックが含まれています。

トンネル インターフェース (P. 33)
CA Spectrum の管理設定 (P. 35)

トンネル インターフェース

このセクションでは、NetScreen Firewall トンネル インターフェースを監視に関する CA Spectrum のサポートについて説明します。

トンネル インターフェースのモデリング

さまざまな属性によって、サイト間のトンネル インターフェースを Netscreen デバイスでモデリングするかどうかが制御されます。 以下の手順に従うことにより、他のタイプのトンネル インターフェースをモデリングできます。 デフォルトでは、CA Spectrum は、ダイヤルアップ トンネル、または監視状態がオフに設定されているトンネルはモデリングしません。 これらのタイプのトンネルのモデリングを有効にするには、Model Type Editor を使用します。

次の手順に従ってください:

1. SpectroSERVER をシャットダウンし、Model Type Editor を起動します。
2. ダイヤルアップ トンネルのモデリングを有効にするには、［属性］タブの［検索］テキストボックスを使って、NSFirewallVPN モデル タイプの TunnelFilterTypes 属性（0x12a17）を検索します。
3. この属性に対する値のリストから値 1 を削除します。
4. 監視状態がオフのトンネルのモデリングを有効にするには、［属性］タブの［検索］テキスト ボックスを使用し、NSFirewallVPN モデル タイプの TunnelFilterStates 属性（0x12a19）を見つけます。
5. この属性に対する値のリストから値 0 を削除します。

6. Model Type Editor に変更を保存し、SpectroSERVER を再起動します。
7. 各デバイス モデルに対して使用可能な［Manually Poll Device］オプションを使用して、Netscreen モデルを再設定します。

   トンネル インターフェースがモデリングされます。

トンネル インターフェースの「スタッキング」

トンネル インターフェース モデルは、その IP アドレスがトンネルのローカル アドレスと一致する物理インターフェースのサブインターフェースとして作成されます。この動作は VPN-MON.mib に示されます。NetScreen デバイスは ifStackTable をサポートしないため、下位レイヤのインターフェースを確定するためのこのメカニズムは必要かつ効果的なものになります。

自動接続マッピング

トンネル インターフェース モデルは、デバイスの初期モデリング実行中またはインターフェースの再設定中に初めてアクティブになります。 その後、CA Spectrum は、トンネルのもう一方のエンドポイントを表すトンネル インターフェース モデルを検索します。このモデルが検出されると、この 2 つのインターフェース間の接続がモデリングされます。 CA Spectrum は、トンネルのもう一方のエンドポイントを検索するため、VPN-MON.mib に示されるローカル アドレスおよびリモート アドレスを使用します。

インターフェース モデルの識別

トンネル インターフェース モデルは、VPN-MON.mib に示されているように、そのローカル アドレスおよびリモート アドレスによって識別できます。この識別方法を使うと、インターフェースの ifIndex が変更されても、CA Spectrum はインターフェース モデルを保持することができます。

トンネル インターフェースのステータス監視

NetScreen デバイスでは、トンネル インターフェース エントリの ifOperStatus は、ifTable から消えるまで、必ず「Up」になります。 トンネル モデルが「最新状態でなくなり」、そのトンネルに対してリンク ダウン トラップが処理されていない場合、CA Spectrum はモデルに関する赤いアラームを生成します。

このアラームが抑制される原因として以下が考えられます。

- 物理インターフェースがダウンしている（リンク ダウン トラップ アラームの抑制と同じ）場合。
- ライブ パイプ モデルの［リンクされたポートのアラームを抑制］設定が True に設定され、以下の条件のどちらかに適合する場合：
  - （SpectroSERVER が）接続デバイスにアクセスできない
  - 「リンク先の」トンネル インターフェース モデルにアラーム（赤）がある

トンネル インターフェースに関連付けられているポートに対してライブ リンクが有効な場合のみ、このステータス監視機能は使用可能です。 ライブ リンクの有効化の詳細については、「IT インフラストラクチャのモデリング/管理 - 管理者ガイド」を参照してください。

CA Spectrum の管理設定

以下の CA Spectrum 管理設定をお勧めします。

インターフェースの自動再設定

CA Spectrum がデバイスのブランチ トンネルを管理することを望む場合は、NetScreen モデルに対してこの属性を True に設定します。「ユーザ」トンネルだけをサポートするデバイスについては、この属性を False に設定します。 True に設定すると、デバイスの SNMP エージェントの ifNumber オブジェクトが変更されると、CA Spectrum は必ずインターフェース モデルを再設定します。

リンク変更の再設定

すべての NetScreen モデルに対して、この属性値を False に設定することをお勧めします。 True に設定すると、CA Spectrum が「リンク アップ」または「リンク ダウン」トラップを受信すると、必ずインターフェース再設定を実行します。

再設定後にディスカバリ属性

すべての NetScreen モデルに対して、再設定後にディスカバリ属性はデフォルト値の False のまま保持することをお勧めします。 この設定にかかわらず、CA Spectrum は新しく検出されたトンネル間の接続をモデリングします。 CA Spectrum 自動ディスカバリ プロセスは、特に NetScreen デバイスに対して、ほとんどのリンク状態変更後に、値を追加することはほとんどないか、まったくありません。 これらのデバイスの場合、ほとんどのリンク状態変更は、新しいルータやブリッジ ポートの設定ではなく、トンネルを昇るか下がるかを意味します。

サブインターフェースの作成

CA Spectrum がブランチ トンネルを監視することを望む場合は、NetScreen モデルに対してこの属性を True に設定します。この属性を False に設定すると、CA Spectrum はトンネル インターフェース用のモデルを作成しません。

リンクされたポートのアラームを抑制

ライブ パイプ モデルのこの属性は True に設定することをお勧めします。接続デバイスがアクセス不可状態か、リンクしたポート モデルにはすでにアラームが存在する場合、この設定によりポート アラームが抑制されます。

第 8 章: Nortel Contivity VPN スイッチ

このセクションでは、Nortel Contivity VPN スイッチを監視するための CA Spectrum のサポートについて説明します。

このセクションには、以下のトピックが含まれています。

トンネル インターフェース (P. 37)
Contivity の管理設定 (P. 40)
CA Spectrum の管理設定 (P. 41)
Contivity の障害シナリオ (P. 43)
既知の問題 (P. 46)

トンネル インターフェース

このセクションでは、Nortel Contivity デバイスのトンネル インターフェース フィルタ機能について説明します。

トンネル インターフェース フィルタリング

ContivityVPN デバイスは、ユーザとブランチの両方の VPN トンネル インターフェース エントリを使って、**ifTable** にデータを入力します。ただし、何千ものユーザ VPN トンネル インターフェースが存在している可能性があります。 ContivityVPN インターフェース フィルタリング機能は、ユーザ トンネル インターフェースをフィルタ除外し、これらのインターフェースの不要なモデリングを防ぎます。

注: トンネル インターフェース フィルタリングは、タイプ **ContivityVPN** のモデルに対してのみ使用可能です。

トンネル IF フィルタリングの有効化と無効化

トンネル IF フィルタリングの有効/無効を切り替えるには、以下の手順に従います。

次の手順に従ってください:

1. モデル タイプ エディタで、属性 If_Mtype_Map handle のデフォルトリスト値を 0x011fb4 に設定します。
2. 値のリストを見て、OID インスタンス 131 を見つけます。
3. 値を 0 に設定します。この設定を実行すると、インターフェース タイプのモデリングが防止されます。
4. トンネル インターフェース フィルタリングを無効化して、モデル作成を有効にするには、この値を 220013 に設定します。

トンネル インターフェースのモデリング

Contivity デバイス モデルの Create Sub-Interface 属性は、サイト間インターフェースまたはブランチ トンネル インターフェースを表すためのモデル作成を制御します。「ユーザ」トンネルを表すモデルは作成されません。この動作は、以前のバージョンと同じです。

トンネル インターフェースの「スタッキング」

トンネル インターフェース モデルは、物理インターフェースのサブインターフェースとして作成されます。 物理インターフェースの IP アドレスは、Tunnel MIB で示されているトンネルのローカル アドレスと一致します。Contivity デバイスは ifStackTable をサポートしません。 その結果、下位レイヤ インターフェースを確定するため、このメカニズムは必要かつ効果的なものになります。

自動接続マッピング

トンネル インターフェース モデルは、デバイスの初期モデリング実行中またはインターフェースの再設定中に初めてアクティブになります。 その後、CA Spectrum は、トンネルのもう一方のエンドポイントを表すトンネル インターフェース モデルを検索します。このモデルが検出されると、この 2 つのインターフェース間の接続がモデリングされます。 CA Spectrum は、トンネルのもう一方のエンドポイントを検索するため、トンネル MIB （rfc2667）に示されるローカル アドレスおよびリモート アドレスを使用します。

インターフェース モデルの識別

トンネル インターフェース モデルは、トンネル MIB （rfc2667）に示されているように、そのローカル アドレスおよびリモート アドレスによって識別できます。 この識別により、インターフェースの ifIndex が変更されても、CA Spectrum はインターフェース モデルを保持することができます。

インターフェース モデルの失効

インターフェース再設定中に、MIB に示されなくなったインターフェース モデルは破棄される代わりに、「最新状態でない」としてマークされます。この機能を使用すると、トンネル ダウン時、CA Spectrum はトンネル インターフェースと他のデバイス間の接続モデリングを保持することができます。 その後、イベント相関および障害抑制に、接続情報を使用できます。

以降の再設定では、デバイス モデルのポートの失効時間は、インターフェース モデルが最新状態でない期間と比較されます。 インターフェースが MIB に再表示されない場合、インターフェース モデルは失効後、破棄されます。インターフェースが MIB 再表示された場合、インターフェース モデルには「最新状態」としてマークされます。「isStale」属性を True に設定することにより、ポートは、最新状態でないとしてマークされます。デバイスごとに、ポートの失効時間を設定できます。デバイスの「PortAgeOutTime」に分数を設定します。 Contivity デバイスのデフォルトの失効時間は 2 時間（120 分）です。

リンク ダウン トラップ相関

1 回のネットワーク停止に対して複数のアラームが送信されないようにするには、「トンネル」インターフェース モデルのリンク ダウン トラップを他の条件と相関します。 下位レイヤ（すなわち物理インターフェース）がダウンしている場合、リンク ダウン トラップのアラームは抑制されます。ライブ パイプ モデルの［リンクされたポートのアラームを抑制］が True に設定されると、リンク ダウン トラップのアラームはすべて抑制されます。 アラームは以下の条件で抑制されます。

1. （SpectroSERVER が）接続デバイスにアクセスできない。
2. 「リンク先の」トンネル インターフェース モデルにアラーム（赤）がある

トンネル インターフェースのステータス監視

Contivity デバイスでは、トンネル インターフェース エントリの ifOperStatus は、ifTable から消えるまで、必ず「Up」になります。 トンネル モデルが「最新状態でなくなり」、トンネルに対してリンク ダウン トラップが処理されていない場合、CA Spectrum は、モデルに関して赤いアラームを生成します。 赤いアラームは、リンク ダウン トラップ アラームが抑制されるのと同じ場合に抑制されます。 下位レイヤ（すなわち物理インターフェース）がダウンしている場合、赤いアラームが抑制されます。ライブ パイプ モデルの［リンクされたポートのアラームを抑制］パラメータが True に設定されると、このアラームが抑制されます。

アラームは以下の条件で抑制されます。

1. （SpectroSERVER が）接続デバイスにアクセスできない。
2. 「リンク先の」トンネル インターフェース モデルにアラーム（赤）がある

Contivity の管理設定

以下の Contivity 設定をお勧めします。

トンネル MIB の有効化

管理対象のすべての Contivity デバイスでは、トンネル IP MIB を有効にすることをお勧めします。 この設定を使用すると、デバイスのトンネル エンドポイントを表すために、CA Spectrum はモデルを作成します。 この MIB は、Contivity Web の管理ページの［管理］ -> ［SNMP］セクションから有効と無効を切り替えることができます。

リンク アップ/リンク ダウン トラップの有効化

物理インターフェース、および「ネイルアップ」ブランチ トンネルでは、リンク アップ トラップとリンク ダウン トラップを有効にすることをお勧めします。 この設定を使用すると、CA Spectrum は直ちに、リンク状態変更通知を受け取ります。 当社のテストでは、「オンデマンド」トンネルのリンク トラップは、あまり意味がないことがわかりました。 トラップが送信されるまで、トンネルは約 15 分間ダウンしている必要があります。

監視対象トンネルのネイルアップ

接続監視が重要なトンネルはすべて、「ネイルアップ」することを推奨します。 「オンデマンド」トンネルがダウンしても、CA Spectrum はアラームを発行しません。特に、Tunnel_If モデルの LINK down Trap 属性に関するアラームによって、そのモデルがリンク ダウン トラップに応答するか、isStale 属性に変更するかが決定します。 値 1 （常時）を設定すると、CA Spectrum はこれらのイベントを処理します。値 0 （対応しない）を設定すると、これらのイベントは無視されます。 CA Spectrum が Contivity 用の Tunnel_If モデルを作成した場合、この属性は「ネイルアップ」ブランチ トンネルに対しては「常時」、「オンデマンド」トンネルに対しては「対応しない」に設定されます。

グローバル属性エディタの［設定］タブから、リンク ダウンに関するアラーム設定を変更します。 CA Spectrum が自動設定するように、この設定はそのまま変更しないことをお勧めします。

CA Spectrum の管理設定

以下の CA Spectrum 管理設定をお勧めします。

インターフェースの自動再設定

CA Spectrum がデバイスのブランチ トンネルを管理する場合は、Contivity モデルに対してこの属性を True に設定します。 「ユーザ」 トンネルだけをサポートするデバイスについては、この属性を False に設定します。 この属性を True に設定した場合、SNMP エージェントの ifNumber オブジェクトがデバイス上で変更されると、CA Spectrum はインターフェース モデルを再設定します。

リンク変更の再設定

すべての Contivity モデルに対して、この属性を False に設定することをお勧めします。 この属性を True に設定した場合、リンク アップ トラップまたはリンク ダウン トラップの受信後、CA Spectrum は必ずインターフェースの再設定を実行します。

再設定後にディスカバリ

すべての Contivity モデルに対して、再設定後にディスカバリ属性はデフォルト値の False のまま保持することをお勧めします。 この設定にかかわらず、CA Spectrum は新しく検出されたトンネル間の接続をモデリングします。 CA Spectrum 自動ディスカバリ プロセスは、特に Contivity デバイスに対して、ほとんどのリンク状態変更後に、値を追加することはほとんどないか、まったくありません。 これらのデバイスの場合、ほとんどのリンク状態変更は、新しいルータやブリッジ ポートの設定ではなく、トンネルを昇るか下がるかを意味します。

サブインターフェースの作成

CA Spectrum がブランチ トンネルを監視することを望む場合は、Contivity モデルに対して、この属性を True に設定します。 この属性を False に設定すると、CA Spectrum はトンネル インターフェース用のモデルを作成しません。

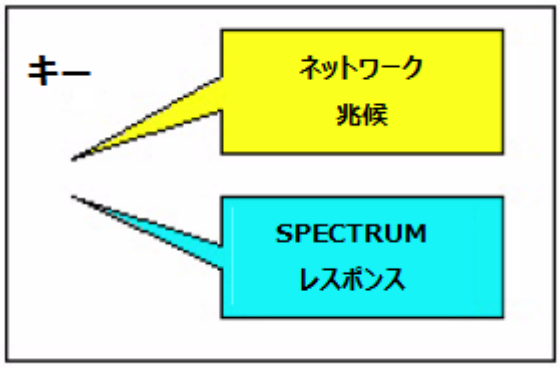
リンクされたポートのアラームを抑制

ライブ パイプ モデルのこの属性は True に設定することをお勧めします。接続デバイスがアクセス不可状態か、リンクしたポート モデルにはすでにアラームが存在する場合、この設定によりポート アラームが抑制されます。

Contivity の障害シナリオ

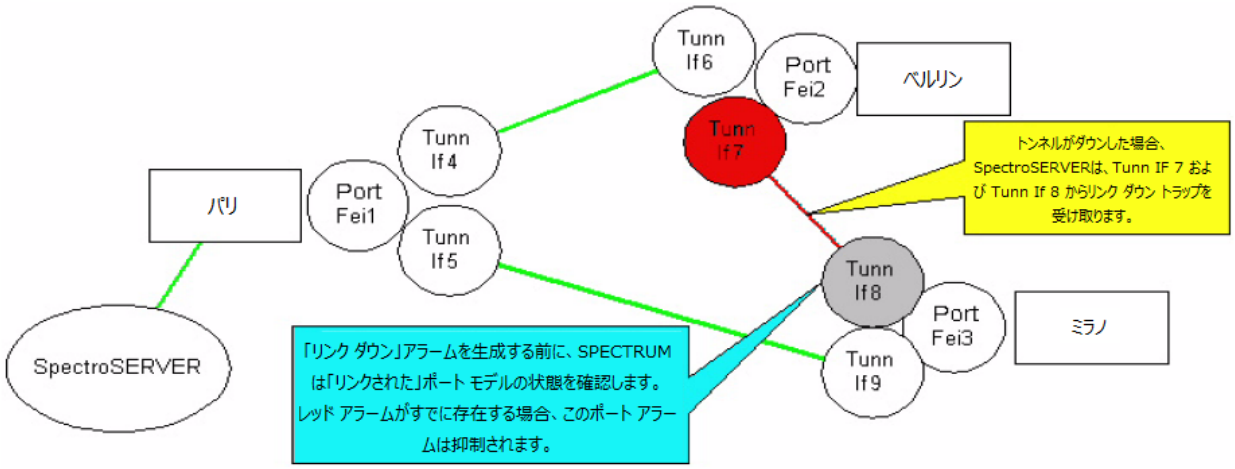
このセクションでは、VPN 環境で発生する可能性が高い障害シナリオと、各シナリオに対する CA Spectrum の対応について説明します。

このセクションの各図に対して、以下のキーが適用されます。



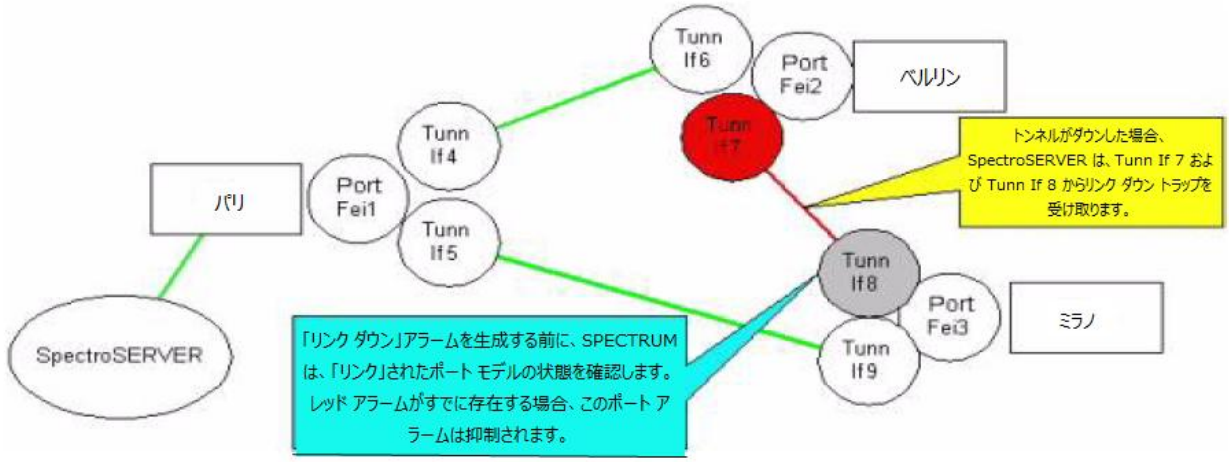
1 つのダウントンネルに対する 2 つのリンク ダウン トラップ

次のシナリオでは、SpectroSERVER は、このメッシュ環境内のすべての管理対象エレメントと接続を保持しますが、2 つのデバイス間のトンネルはダウンします。 CA Spectrum は、2 つのリンク ダウン トラップを受信します。 1 つはトンネル インターフェース アラーム、もう 1 つのアラームは抑制されます。



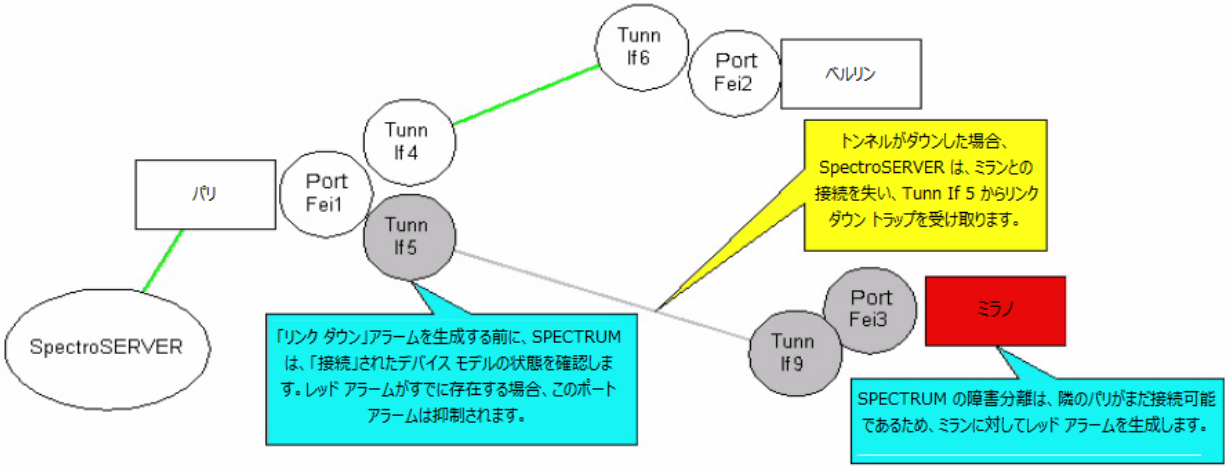
接続の切断とリンク ダウン トラップ

次のシナリオでは、CA Spectrum は、ハブおよびスポーク ネットワーク内の「スポーク」Contivity と接続が切断されます。 CA Spectrum はまた、接続が切断されたデバイスへのトンネルを示すリンク ダウン トラップをハブから受信します。 CA Spectrum は接続が切断されたデバイスに対してアラームを送信し、このトラップによって示されたトンネル インターフェースに関するアラームを抑制します。



物理的なポート ダウン、接続の切断、およびリンク ダウン トラップ

次のシナリオでは、Contivity の物理ポートがダウンするか、パブリック ネットワークへのリンクとの接続が切断されたとします。 CA Spectrum は Contivity の物理ポートとトンネルに対して、リンク ダウン トラップを取得します。また、リモート Contivity デバイスとの接続が切断されます。トンネル インターフェース モデル上のリンク ダウン アラームは抑制されますが、CA Spectrum の障害分離機能によって、接続が切断された Contivity デバイス モデルに関して赤いアラームが生成されます。これは、デバイス モデルに「アップ」状態の隣接関係が発生したためです。



既知の問題

CA Spectrum には、以下の既知の問題があります

サブインターフェースの変更

トンネル インターフェース モデルを作成した後、Contivity モデルに対して［サブインターフェースの作成］を True から False に変更すると、インターフェースを再設定しても、トンネル インターフェース モデルは直ちに破棄されません。 代わりに、これらのモデルは状態が古くなり、失効処理が開始されます。Contivity デバイスのサブセットに対してトンネル監視を有効にするには、［サブインターフェースの作成］のデフォルト値を False に設定します。 その後、トンネル監視を必要とする Contivity デバイスの個々のモデルに対して、［サブインターフェースの作成］を True に設定します。

自動ディスカバリとパブリック アドレス

通常、VPN 内の Contivity デバイスのパブリック アドレスはサブネットが異なっています。これは複数のルータがデバイスを個々に処理するためです。 パブリック インターフェースを備えた Contivity デバイスは、同じサブネット上に存在する可能性があります。この場合、CA Spectrum 自動ディスカバリにより、パブリック インターフェースの接続のマッピングを試行することができます。 実行結果は、Contivity モデルへのパイプを持った Contivity モデルと同じトポロジ ビュー内の LAN コンテナとして表示されます。 LAN に接続されていない FanOut モデルは、Contivity デバイスのパブリック インターフェース モデルに接続されます。

ポートの失効

CA Spectrum ポートの失効は積極的に実行されません。 トンネルが非アクティブになる場合、トンネル インターフェース モデルは「最新状態でない」としてマークされます。 デバイスの「portAgeOutTime」後に再設定が実行されると、そのトンネル モデルは必ず破棄されます。 ただし、その後にデバイスの再設定が発生しない場合、「最新状態でない」トンネル インターフェース モデルはそのまま残ります。

たとえば、ポーリング間隔を 5 分、portAgeOutTime を 30 分として検証してみましょう。 10 時 27 分にトンネルがダウンし、10 時 30 分に CA Spectrum がポーリングを実行すると、CA Spectrum は ifNumber の変更を検出し、インターフェースの再設定を実行します。 このプロセス中、トンネル インターフェースは最新状態でないとマーキングされます。 トンネルがアップ状態に戻らない場合、トンネル インターフェース モデルは 11 時に破棄されます。 ifNumber が 1 週間再変更されない場合、インターフェース再設定は 1 週間再実行できません。 このトンネル インターフェース モデルは、最新状態でないまま 1 週間保持され、その後破棄されます。