ステータスと統計情報

この章は、次の項で構成されています。

システム概要

[System Summary] には、デバイスの状態、ハードウェア、ファームウェアバージョン、一般的な PoE ステータスなどのシステム情報のプレビューが表示されます。

システム情報を表示するには、[Status and Statistics] > [System Summary] をクリックします。

システム情報

[System Information] セクションでは、デバイスに関する情報を簡単に取得できます。このセクションでは、次の情報を確認できます。以下の設定を編集するには、[Edit] をクリックし、システム設定に移動してこの値を入力します。

- [System Description]：システムの説明。
- [System Location]：デバイスの物理的な場所。
- [System Contact]：担当者の名前。
- [Host Name]：デバイスの名前。デフォルトでは、デバイスホスト名は、単語「switch」にデバイスの MAC アドレスの 3 最下位バイト（最も右側の16進数の 6 桁）が連結されて構成されます。
- [System Object ID]：エンティティに含まれるネットワーク管理サブシステムの一意なベンダー ID（SNMP で使用される）。
- [System Uptime]：最後のリブートから経過した時間。

（注） システム稼働時間については、スイッチが 21 日 + 20 時間 + 14 分および 58 秒経過すると、時間がリセットされます。スイッチが再起動しない場合、21 日 + 20 時間 + 14 分および 58 秒で稼働時間がリセットされ、最初から開始されます。

- [Current Time]：現在のシステム時刻。
- [Base MAC Address]：デバイスの MAC アドレス。
- [Jumbo Frames]：ジャンボフレームサポートステータス。このサポートは、ポート設定で有効または無効にできます。

（注） ジャンボ フレームのサポートは、有効にした後、デバイスがリブートした後でのみ反映されます。

ソフトウェア情報

[Software Information] セクションでは、デバイスで実行されているソフトウェアに関する情報をすばやく取得できます。このセクションでは、次の情報を確認できます。

- ファームウェア バージョン（Firmware Version）（アクティブ イメージ）：アクティブなイメージのファームウェア バージョン番号。
- ファームウェア MD5 チェックサム（Firmware MD5 Checksum）（アクティブイメージ）：アクティブなイメージの MD5 チェックサム。
- ファームウェア バージョン（非アクティブ）（Firmware Version (Non-active)）：非アクティブなイメージのファームウェアバージョン番号。システムがスタック内に存在する場合、アクテイブユニットのバージョンが表示されます。

- ファームウェア MD5 チェックサム（非アクティブ）（Firmware MD5 Checksum (Non-active)）：非アクティブなイメージの MD5 チェックサム。

TCP/UDPサービスステータス

次のフィールドをリセットするには、[Edit] をクリックします。以下の設定が表示されます。

- HTTP サービス（HTTP Service）：HTTP が有効か無効かを示します。
- HTTPS サービス（HTTPS Service）：HTTPS が有効か無効かを示します。
- SNMP サービス（SNMP Service）：SNMP が有効か無効かを示します。
- Telnet サービス（Telnet Service）：Telnet が有効か無効かを示します。
- SSH サービス（SSH Service）：SSH が有効か無効かを示します。

PoE 対応デバイスの PoE 電源情報

[PoE Power Information on Device Supporting PoE] セクションでは、デバイスの PoE 情報を簡単に取得できます。このセクションでは、次のように表示されます。

- [PoE Power Information]：[Detail] をクリックすると、プロパティに直接リンクします。このページには PoE 電源情報が表示されます。
- [Maximum Available PoE Power (W)]：スイッチによって供給可能な最大の使用可能電力。
- [Total PoE Power Allocated (W)]：接続されている PoE デバイスに割り当てられている合計 PoE 電力。
- [PoE Power Mode]：ポート制限またはクラス制限。

ユニットはグラフィカルに表示され、ポートにカーソルを置くとその名前が表示されます。

ユニットごとに、次の情報が表示されます。

- [Unit 1 (Active)]：デバイスモデル ID。
- [Serial Number]：シリアル番号。
- [PID VID]：ポート番号とバージョン ID。

CPU 使用率

デバイス CPU は、管理インターフェイスでのエンドユーザ トラフィック処理に加え、次のタイプのトラフィックを処理します。

- 管理トラフィック

- プロトコル トラフィック
- スヌーピング トラフィック

過剰なトラフィック負荷が CPU にかかると、通常のデバイス操作が妨げられることがあります。デバイスは、セキュアコアテクノロジー（SCT）を使用することにより、管理トラフィックとプロトコルトラフィックの受信および処理を確実に実行できます。SCT はデバイスでデフォルトで有効になっています。無効にすることはできません。

CPU 使用率を表示するには、次の手順を実行します。

手順

ステップ 1 [Status and Statistics] > [CPU Utilization] の順にクリックします。

[CPU Input Rate] フィールドに、1 秒あたりの CPU への入力フレームのレートが表示されます。ウィンドウには、デバイスの CPU 使用率を表示するグラフが含まれています。Y 軸が使用率で、X 軸がサンプル番号です。

ステップ 2 [Enable] をオンにして、CPU 使用率を有効にします。

ステップ 3 統計を更新する前に経過させる [Refresh Rate]（秒単位の期間）を選択します。期間ごとに新しいサンプルが作成されます。

デバイスの CPU 使用率を表示するグラフを含むウィンドウが表示されます。

ポート使用率

[Port Utilization] ページには、ポートごとのブロードバンド（着信と発信の両方）の使用率が表示されます。

ポート使用率を表示するには、次の手順を実行します。

手順

ステップ 1 [Status and Statistics] > [Port Utilization] をクリックします。

ステップ 2 インターフェイスのイーサネットの統計を更新する前の経過期間として、[Refresh Rate] を選択します。

ポートごとに、次のフィールドが表示されます。

- [Interface]：ポートの名前。
- [Tx Utilization]：発信パケットによって使用された帯域幅の量。
- [Rx Utilization]：着信パケットによって使用された帯域幅の量。

ポートの時間の経過に伴う履歴使用率のグラフを表示するには、ポートを選択し、[View Interface History Graph] をクリックします。上記に加えて、次のフィールドが表示されます。

- [TX Utilization]：オンにすると、TX 使用率データが表示されます。
- [RX Utilization]：オンにすると、RX 使用率データが表示されます。
- [Time Span]：時間の単位を選択します。グラフには、この時間単位のポート使用率が表示されます。

インターフェイス

[Interface] ページには、トラフィック統計情報がポート別に表示されます。このページは、送受信されるトラフィック量とその分散（ユニキャスト、マルチキャスト、ブロードキャスト）を分析するのに便利です。

イーサネット統計情報を表示したり、リフレッシュレートを設定したりするには、次の手順を実行します。

手順

ステップ 1 [Status and Statistics] > [Interface] をクリックします。

ステップ 2 テーブル表示またはグラフィック表示で統計カウンタを表示するには、次の手順を実行します。

- すべてのカウンタをクリアするには、[Clear Interface Counters] をクリックします。
- カウンタを更新するには、[Refresh] をクリックします。
- すべてのポートをテーブル表示で確認するには、[View All Interfaces Statistics] をクリックします。
- これらの結果をグラフィック形式で表示するには、[View Interface History Graph] をクリックします。そのインターフェイスに関する統計を表示するには、[Interface] を選択します。

ステップ 3 パラメータを入力します。

- [Interface]：イーサネット統計を表示するインターフェイスを選択します。
- [Refresh Rate]：インターフェイス イーサネット統計情報がリフレッシュされ るまでの時間を選択します。

ステップ 4 [Receive Statistics] セクションには次の統計が表示されます。

- [Total Bytes (Octets)]：受信オクテット数。不良パケットと FCS オクテットを含むが、フレーミング ビットは除く。
- [Unicast Packets]：受信された正常なユニキャスト パケット数。
- [Multicast Packets]：受信された正常なマルチキャスト パケット数。

- [Broadcast Packets]：受信された正常なブロードキャスト パケット数。
- [Packets with Errors]：受信されたエラーのあるパケット数。

ステップ 5 [Transmit Statistics] セクションには次の統計が表示されます。

- [Total Bytes (Octets)]：送信オクテット数。不良パケットと FCS オクテットを含むが、フレーミング ビットは除く。
- [Unicast Packets]：送信された正常なユニキャスト パケット数。
- [Multicast Packets]：送信された正常なマルチキャスト パケット数。
- [Broadcast Packets]：送信された正常なブロードキャスト パケット数。

Etherlike

[Etherlike] ページには、Etherlike MIB 規格定義に従って統計情報がポート別に表示されます。情報のリフレッシュ レートを選択できます。このページは、トラフィックを中断させる可能性がある物理層（レイヤ 1）でのエラーに関するより詳細な情報を提供します。

Etherlike統計情報を表示したり、リフレッシュレートを設定したりするには、次の手順を実行します。

手順

ステップ 1 [Status and Statistics] > [Etherlike] をクリックします。

ステップ 2 パラメータを入力します。

- [Interface]：イーサネット統計情報が表示される特定のインターフェイスを選択します。
- [Refresh Rate]：Etherlike 統計情報が更新されるまでの時間を選択します。

選択したインターフェイスに関する次のフィールドが表示されます。

- [Frame Check Sequence (FCS) Errors]：CRC（Cyclic Redundancy Check）に失敗した受信フレーム数。
- [Single Collision Frames]：シングルコリジョンに含まれるが、正常に送信されたフレーム数。
- [Late Collisions]：データの最初の 512 ビットの後に検出されたコリジョン。
- [Excessive Collisions]：過剰コリジョンが原因で拒否された送信回数。
- [Oversize Packets]：2000 オクテットを超える受信パケット。
- [Internal MAC Receive Errors]：受信側のエラーにより拒否されたフレーム。
- [Pause Frames Received]：受信したフレームの数。

• [Pause Frames Transmitted]：送信されたフレームが一時停止した数。

（注）
上記のいずれかのフィールドにエラーの数（0 以外）が表示されている場合は、最後のアップタイムが表示されます。

ステップ 3 テーブル表示で統計カウンタを表示するには、テーブル表示ですべてのポートを確認するために、[View All Interfaces Statistics] をクリックします。[Refresh] をクリックして統計情報を更新するか、または [Clear Interface Counters] をクリックしてカウンタをクリアします。

GVRP

[Generic Attribute Registration Protocol (GARP) VLAN Registration Protocol (GVRP)] ページには、ポートとの間で送受信された GVRP フレームに関する情報が表示されます。GVRP は、各種の標準規格に準拠したレイヤ 2 ネットワーク プロトコルで、スイッチ上の VLAN 情報を自動設定するためのものです。802.1Q-2005 の 802.1ak 修正で定義されています。ポートの GVRP 統計情報は、GVRP がグローバルに、ポートで有効になっている場合にのみ表示されます。

GVRPの統計情報を表示したり、リフレッシュレートを設定したりするには、次の手順を実行します。

手順

ステップ 1 [Status and Statistics] > [GVRP] をクリックします。

ステップ 2 パラメータを設定します。

Interface	GVRP の統計情報が表示される特定のインターフェイスを選択します。
Refresh Rate	GVRP ページが更新されるまでの経過時間を選択します。[Attribute Counter] ブロックには、インターフェイスごとのさまざまなパケット タイプのカウンタが表示されます。これらは、[Received] および [Transmitted] パケットについて表示されます。

受信済み：送信済み

Join Empty	送受信された GVRP の Join Empty パケット数。
Empty	送受信された GVRP の Empty パケット数。
Leave Empty	送受信された GVRP の Leave Empty パケット数。
Join In	送受信された GVRP の Join In パケット数。
Leave In	送受信された GVRP の Leave In パケット数。

Leave All	送受信された GVRP の Leave All パケット数。[GVRP Error Statistics] セクションには、GVRP エラー カウンタが表示されます。

GVRPエラー統計情報

Invalid Protocol ID	無効なプロトコル ID エラー。
Invalid Attribute Type	無効な属性 ID エラー。
Invalid Attribute Value	無効な属性値エラー。
Invalid Attribute Length	無効な属性長エラー。
Invalid Event	無効なイベント。

ステップ 3 インターフェイスカウンタをクリアするには、[Clear All Interface Counters] をクリックします。

ステップ 4 データを更新するには、ツールバーの [Refresh] をクリックします。

ステップ 5 すべてのインターフェイス統計を表示するには、[View Interfaces Statistics] をクリックして、単一のページですべてのポートを確認してください。

802.1X EAP

[802.1X EAP] ページには、送受信された Extensible Authentication Protocol（EAP; 拡張可能認証プロトコル）フレームが表示されます。EAPの統計情報を表示したり、リフレッシュレートを設定したりするには、次の手順を実行します。

手順

ステップ 1 [Status and Statistics] > [802.1x EAP] をクリックします。

ステップ 2 統計をポーリングする [Interface] を選択します。

ステップ 3 EAP 統計を更新する前に経過させる [Refresh Rate]（期間）を選択します。

選択したインターフェイスに関する値が表示されます。

受信済みEAPOL EAPフレーム	ポートで受信した有効な EAPOL フレーム。
受信済みEAPOL開始フレーム	ポートで受信した有効な EAPOL 開始フレーム。
受信済みEAPOLログオフフレーム	ポートで受信した EAPOL ログオフフレーム。
受信済みEAPOL Announcementフレーム	ポートで受診した EAPOL 通知フレーム。
受信済みEAPOL Announcement要求フレーム	ポートで受診した EAPOL 通知要求フレーム。

受信済みEAPOL無効フレーム	ポートで受信した EAPOL 無効フレーム。
受信済みEAPOL EAP長エラーフレーム	このポートで受信したパケット本体の長さが無効な EAPOL フレーム。
受信済みCKN未認識MKPDUフレーム	このポートで受信した未認識 CKN を含む EAP フレーム。
受信済みMKPDU無効フレーム	ポートで受信した MKPDU 無効フレーム。
最終EAPOLフレームバージョン	最後に受信した EAPOL フレームに関連付けられているプロトコルバージョン番号。
最終EAPOLフレーム送信元	最後に受信した EAPOL フレームに関連付けられている送信元 MAC アドレス。
送信済みEAPOL EAPサプリカントフレーム	ポートで送信した EAPOL EAP サプリカントフレーム。
送信済みEAPOL開始フレーム	ポートで送信した EAPOL 開始フレーム。
送信済みEAPOLログオフフレーム	ポートで送信した EAPOL ログオフフレーム。
送信済みEAPOL Announcementフレーム	ポートで送信した EAPOL 通知フレーム。
送信済みEAPOL Announcement要求フレーム	ポートで送信した EAPOL 通知要求フレーム。
送信済みEAPOL認証コードフレーム	ポートで送信した EAP オーセンティケータフレーム。
送信済みCKNなしEAPOL MKAフレーム	ポートで送信したCKNを含まないMKAフレーム。

ステップ 4 [Clear Interface Counters] をクリックして、すべてのインターフェイス カウンタをクリアします。

ステップ 5 カウンタを更新するには、[Refresh] をクリックします。

ステップ 6 [View All Interfaces Statistics] をクリックして、すべてのインターフェイスのカウンタを表示します。

ACL

ACL ロギング機能が有効になっている場合は、ACL 規則に一致するパケットに関する情報 SYSLOG メッセージが生成されます。ACL に基づいてパケットが転送または拒否されたインターフェイスを表示するには、次の手順を実行します。

手順

ステップ 1 [Status and Statistics] > [ACL] をクリックします。

ステップ 2 ページを更新する前に経過させる [Refresh Rate]（秒単位の期間）を選択します。期間ごとに新しいインターフェイス グループが作成されます。

次の情報が表示されます。

- [Global Trapped Packet Counter]：リソース不足のためにグローバルにトラップされたパケット数。
- [Trapped Packets - Port/LAG Based]：ACL ルールに基づいてパケットが転送または拒否されたインターフェイス。
- [Trapped Packets - VLAN Based]：ACL ルールに基づいてパケットが転送または拒否された VLAN。

ステップ 3 統計カウンタをクリアするには、[Clear Counters] をクリックするか、[Refresh] をクリックしてカウンタを更新します。

ハードウェアリソース使用率

このページには、アクセスコントロールリスト（ACL）やサービス品質（QoS）など、デバイスが使用するリソースが表示されます。一部のアプリケーションは、それらの開始時に規則を割り当てます。また、システムブート時に初期化されるプロセスは、起動プロセス中にそれらのルールの一部を使用します。

ハードウェアリソース利用率を表示するには、[Status and Statistics] > [Hardware Resource Utilization] をクリックします。

[Hardware Resources Table] には、次のフィールドが表示されます。

- IPエントリ
  - [In Use]：IP ルールで使用されている TCAM エントリ数。
  - [Maximum]：IP ルールで使用可能な TCAM エントリ数。
- ACLとQoSのルール
  - [In Use]：ACL および QoS ルールで使用される TCAM エントリの数。
  - [Maximum]：ACL および QoS ルールで使用可能な TCAM エントリの数。

健全性と電力

[Health and Power] ページは、すべての関連デバイスの温度ステータス、電源ステータス、およびファンステータスをモニターします。デバイス上のファンは、モデルによって異なります。[Health and Power] ページにアクセスするには、[Status and Statistics] > [Health and Power] の順に移動します。

次のセクションが表示されます。

環境ステータス

- [Fan Status]：ファンが利用できない（[N/A]）か、利用可能で正常に動作している（[OK]）か、動作していない（[Failure]）かが表示されます。
- [Sensor Status]：センサーが機能している（[OK]）か、機能していない（[Failure]）かが表示されます。
- [Temperature]：次のいずれかのオプションが表示されます。
  - OK：温度が警告しきい値未満です。
  - 警告（Warning）：温度が警告しきい値と重大しきい値の間です。
  - 重大（Critical）：温度が重大しきい値を超えています。
  - [N/A]：利用できません。

電源装置ステータス

[Main Power Supply Status]：主電源について、次のいずれかが表示されます。

- [Active]：電源は使用されています。
- [Failure]：主電源に障害が発生しました。

電力の削減

- [Current Green Ethernet and Port Power Savings]：現在のすべてのポートでの節電量。
- [Cumulative Green Ethernet and Port Power Savings]：デバイスの電源が投入された以降の、すべてのポートでの累積節電量。
- [Projected Annual Green Ethernet and Port Power Savings]：1 週間におけるデバイスでの予測節電量。この値は、前週に発生した節減量に基づいて計算されます。

SPAN および RSPAN

SPAN 機能（ポート ミラーリングまたはポート モニタリングとも呼ばれる）は、ネットワーク アナライザによって分析するネットワーク トラフィックを選択します。ネットワークアナライザは、シスコ スイッチプローブデバイスまたはその他のリモートモニタリング（RMON）プローブとして使用できます。

ポート ミラーリングは、ネットワーク デバイスが、単一のデバイス ポート、複数のデバイス ポート、またはVLAN全体で検出したネットワーク パケットのコピーを、デバイスの別のポートのネットワーク モニタリング接続に送信するために使用されます。これは、侵入検知システムのように、ネットワーク トラフィックのモニタリングが必要な場合に、一般的に使用されます。モニタリング ポートに接続されているネットワーク アナライザが、データ パケットを処理します。ネットワーク ポートで受信され、ミラーリングの対象となる VLAN に指定されたパケットは、パケットが最終的にトラップまたは廃棄される場合でも、アナライザ ポートにミラーされます。デバイスによって送信されたパケットは、送信（Tx）ミラーリングがアクティブな場合に、ミラーされます。

ミラーリングは、送信元ポートからのすべてのトラフィックがアナライザ（宛先）ポートで受信されることは保証しません。サポート可能な量を超えるデータがアナライザ ポートに送信された場合、一部のデータは失われる可能性があります。

VLAN ミラーリングは、手動で作成されなかった VLAN 上では、アクティブにすることはできません。たとえば、VLAN 23 が GVRP によって作成された場合、ポート ミラーリングは動作しません。

RSPAN

RSPAN は、ネットワーク全体にわたり複数スイッチのモニタリングを可能にし、アナライザ ポートをリモート スイッチ上に定義できるようにすることで、SPANを拡張します。開始（送信元）および最終（宛先）スイッチに加えて、トラフィックが流れる中間スイッチを定義できます。各 RSPAN セッションのトラフィックは、ユーザーが指定した RSPAN VLAN 上で伝送されます。この RSPAN VLAN は、参加しているすべてのスイッチで RSPAN セッション専用です。開始デバイスの送信元インターフェイスからのトラフィックは、リフレクタポートを介して RSPAN VLAN にコピーされ、その後、中間デバイスの全般モードで構成されたトランク ポートを経由して、RSPAN VLAN をモニタリングしている最終スイッチの宛先セッションへ転送されます。リフレクタ ポートは、RSPANVLANへパケットをコピーするメカニズムです。それは、さまざまなタイプのトラフィックを処理するネットワーク ポートです。RSPANVLANは、すべての中間スイッチに設定されている必要があります。

RSPAN VLAN

RSPAN VLAN は、RSPAN 送信元と宛先のセッション間で SPAN トラフィックを伝送します。また、開始デバイス、中間デバイス、最終デバイスで定義する必要があります。

（注） VLAN を RSPAN VLAN として設定するには、VLAN 設定画面を使用して VLAN データベースに追加する必要があります。

VLAN を RSPAN VLAN として設定するには、次の手順を実行します。

手順

ステップ 1 [Status and Statistics] > [SPAN & RSPAN] > [RSPAN VLAN] の順にクリックして、以前に定義した RSPAN VLAN を表示します。

ステップ 2 VLAN を RSPAN VLAN として設定するには、VLAN の [RSPAN VLAN] ドロップダウンリストから選択します。

ステップ 3 [Apply] をクリックします。

SPANセッションの宛先

モニタリングセッションは、1 つ以上の送信元ポートと単一の宛先ポートで構成されます。宛先ポートは、開始デバイスと最終デバイスで設定する必要があります。開始デバイスでは、これは、リフレクタ ポートです。最終デバイスでは、アナライザポートになります。

宛先ポートを追加するには、次の手順を実行します。

手順

ステップ 1 [Status and Statistics] > [SPAN & RSPAN] > [Session Destinations] をクリックします。

ステップ 2 [Session Destinations Table] で、[Add] をクリックします。

ステップ 3 次のフィールドに入力します。

- [Session ID]：セッション ID を選択します。これは、送信元ポートのセッション ID に一致している必要があります。
- [Destination Type]：次のいずれかのオプションを選択します。
  - [Local Interface]：送信元ポートと同じデバイス上の宛先ポートです（SPAN に関係）。
  - [Remote VLAN]：送信元ポートとは異なるデバイス上の宛先ポートです（RSPAN に関連）。
- [Port]：ドロップダウンリストからポートを選択します。
- [Network Traffic]：選択すると、ポート上で、モニタ対象のトラフィック以外のトラフィックを有効にすることができます。

ステップ 4 [Apply] をクリックします。

SPANセッションの送信元

単一のローカル SPAN または RSPAN セッションの送信元では、受信（Rx）、送信（Tx）、または双方向（両方）のポートトラフィックをモニターできます。スイッチは、任意の数の送信元ポート（スイッチで使用可能なポートの最大数まで）および任意の数の送信元 VLAN をサポートしています。

ミラーする送信元ポートを設定するには、次の手順を実行します。

手順

ステップ 1 [Status and Statistics] > [SPAN & RSPAN] > [Session Sources] をクリックします。

ステップ 2 [Session Source Table] で、[Add] をクリックします。

ステップ 3 セッション ID を選択します。これは、すべての送信元ポートと宛先ポートで同じである必要があります。

ステップ 4 開始スイッチでは SPAN または RSPAN に対して、トラフィックのモニタ元のユニットとポートまたは VLAN（[Source Interface]）を選択します。最終スイッチ上の RSPAN に対して、リモート VLAN を選択します。

ステップ 5 [Monitor Type] フィールドで、ミラーするトラフィックのタイプとして、着信、発信、またはその両方を選択します。

- [Tx and Rx]：着信パケットと発信パケットの両方に対するポートミラーリング。
- [Rx]：着信パケットに対するポートミラーリング。
- [Tx]：発信パケットに対するポートミラーリング。

ステップ 6 [Apply] をクリックします。ミラーリングの送信元インターフェイスが設定されます。

診断

診断を使用して、デバイスがライブネットワークに接続されている間に、システムのハードウェアコンポーネント（シャーシ、スーパーバイザエンジン、モジュール、および ASIC）の機能をテストして検証できます。診断では、ハードウェア コンポーネントをテストして、データ パスおよび制御信号を検証するパケット スイッチング テストが行われます。

カッパーテスト

[Copper Test] ページには、カッパー ケーブルに対して Virtual Cable Tester（VCT）によって実行された統合ケーブル テストの結果が表示されます。

VCT は、2 つのタイプのテストを実行します。

- タイム ドメイン反射率計（TDR）技術は、ポートにアタッチされている銅ケーブルの品質と特性をテストします。最長 140m のケーブルをテストすることができます。これらの結果は、[Copper Test] ページの [Test Results] ブロックに表示されます。
- DSP ベースのテストは、ケーブル長を測定するために、アクティブな XG リンク上で実行されます。これらの結果は、[Copper Test] ページの [Advanced Information] ブロックに表示されます。このテストは、リンク速度が 10G のときにのみ実行できます。

カッパーテストを実行するための前提条件

テストを実施する前に、次の手順を実行します。

- （必須）ショートリーチモードの無効化（プロパティを参照）。
- （任意）EEE の無効化（プロパティを参照）。

VCT を使用してケーブルをテストする場合は、CAT6a データ ケーブルを使用します。

テスト結果の精度は、詳細テストの場合は +/- 10 のエラー範囲、基本テストの場合は +/- 2 のエラー範囲になります。

注意 ポートをテストする場合、ポートはダウン状態に設定され、通信は中断されます。テスト後に、ポートはアップ状態に戻ります。カッパーポートテストの実行により、デバイスと通信できなくなるため、Web ベースのスイッチ設定ユーティリティの実行に使用しているポートに対してカッパーポートテストを実行することは推奨できません。

ポートに接続されている銅ケーブルをテストするには、次の手順を実行します。

手順

ステップ 1 [Status and Statistics] > [Diagnostics] > [Copper Test] の順にクリックします。

ステップ 2 テストを実行するポートを選択します。

ステップ 3 [Copper Test] をクリックします。

ステップ 4 メッセージが表示されたら、[OK] をクリックして、リンクをダウンできることを確認するか、または [Cancel] をクリックしてテストを中止します。[Test Results] ブロックに次のフィールドが表示されます。

- [Last Update]：ポートに対して最後のテストが実行された時刻。
- [Test Results]：ケーブル テストの結果。値は次のとおりです。

- [OK]：ケーブルはテストに合格しました。
- [No Cable]：ケーブルがポートに接続されていません。
- [Open Cable]：ケーブルが一方側にしか接続されていません。
- [Short Cable]：ケーブルにショートが発生しています。
- [Unknown Test Result]：エラーが発生しています。

- [Distance to Fault]：障害が検出されたケーブル位置からポートまでの距離。
- [Operational Port Status]：ポートの状態（アップまたはダウン）が表示されます。

[Advanced Information] ブロック（一部のポートタイプでサポート）に次の情報が表示されます（情報はページを開くたびに更新されます）。

- [Cable Length]：長さの見積もりを提供します。
- [Pair]：テスト対象のケーブルワイヤペア
- [Status]：ワイヤペアの状態。赤色は障害を示し、緑色は状態が良好であることを示します。
- [Channel]：ワイヤがストレートかクロスオーバーであるかどうかを示すケーブル チャネル。
- [Polarity]：自動極性検出と修正機能がワイヤペアに対して有効になっているかどうかを示します。
- [Pair Skew]：ワイヤペア間の遅延差

光モジュールステータス

[Optical Module Status] ページには、SFP（Small Form-factor Pluggable）トランシーバによってレポートされた稼動状況が表示されます。

次の GE SFP（1000Mbps）トランシーバがサポートされています。

- CWDM-SFP-1490
- CWDM-SFP-1510
- CWDM-SFP-1550
- CWDM-SFP-1570
- CWDM-SFP-1590
- MGBLH1：1000BASE-LH SFP トランシーバ、シングルモードファイバ用、波長 1310 nm、最大 40 km まで対応
- MGBLX1：1000BASE-LX SFP トランシーバ、シングルモードファイバ用、波長 1310 nm、最大 10 km まで対応

- MGBSX1：1000BASE-SX SFP トランシーバ、マルチモード ファイバ用、波長 850 nm、最大 550 m まで対応
- MGBT1：1000BASE-T SFP トランシーバ、カテゴリ 5 銅線用、最大 100 m まで対応
- GLC-SX-MMD：1000BASE-SX 短波長、DOM あり
- GLC-LH-SMD：1000BASE-LX/LH 長波長、DOM あり
- GLC-BX-D：1000BASE-BX10-D ダウンストリーム双方向シングルファイバ、DOM あり
- GLC-BX-U：1000BASE-BX10-U アップストリーム双方向シングルファイバ、DOM あり
- GLC-TE：1000BASE-T（標準）

次の XG SFP+（10,000Mbps）トランシーバがサポートされます。

- SFP-10G-ER
- SFP-10G-ER-S
- SFP-10G-BXD-I
- SFP-10G-BXU-I
- Cisco SFP-10GBase-T
- Cisco SFP-10G-SR
- Cisco SFP-10G-LR
- Cisco SFP-10G-SR-S
- Cisco SFP-10G-LR-S

次の XG パッシブ ケーブル（Twinax/DAC）がサポートされます。

- SFP-H10GB-CU1-5M
- SFP-H10GB-CU2M
- SFP-H10GB-CU2-5M
- SFP-H10GB-ACU10M
- SFP-10G-AOC1M
- SFP-10G-AOC3M
- SFP-10G-AOC5M
- SFP-10G-AOC7M
- SFP-10G-AOC10M
- Cisco SFP-H10G-CU1M
- Cisco SFP-H10G-CU3M
- Cisco SFP-H10G-CU5M

光テストの結果を表示するには、[Status and Statistics] > [Diagnostics] > [Optical Module Status] の順にクリックします。

このページには、次のフィールドが表示されます。

- [Port]：SFP が接続されているポート番号
- [Description]：光トランシーバの説明
- [Serial Number]：光トランシーバのシリアル番号
- [PID]：トランシーバの製品 ID
- [VID]：トランシーバのバージョン ID
- [Temperature]：SFP の動作温度（摂氏）
- [Voltage]：SFP の動作電圧
- [Current]：SFP の電流消費量
- [Output Power]：送出された光電力
- [Input Power]：受け取った光電力
- [Transmitter Fault]：リモート SFP から報告される信号損失。値は [TRUE]、[FALSE]、および [N/S]（信号なし）になります。
- [Loss of Signal]：ローカル SFP から報告される信号損失。値は [TRUE] か [FALSE] になります。
- [Data Ready]：SFP が稼動しているかどうか。値は [TRUE] か [FALSE] になります。

テクニカルサポート情報

このページは、デバイスの状態の詳細なログを提供します。単一のコマンドで複数の show コマンド（debug コマンドを含む）の出力が得られるため、この情報は、テクニカルサポートがユーザーの問題解決を支援する場合に役立ちます。

デバッグ目的で役立つテクニカル サポート情報を表示するには、次の手順を実行します。

手順

ステップ 1 [Status and Statistics] > [Diagnostics] > [Tech-Support Information] の順にクリックします。

ステップ 2 [Generate] をクリックします。

（注）

このコマンドの出力を生成するために多少時間がかかる場合があります。情報が生成されたら、[Select tech-support data] をクリックすることで、画面上のテキストボックスからテキストをコピーして別のドキュメントに貼り付けることができます。

オンボード パケット キャプチャ

（注） オンボード パケット キャプチャのサポートがリリース 4.1.3x で追加され、すべての Catalyst 1200 および Catalyst 1300 スイッチでサポートされています。

オンボード パケット キャプチャ（OBC）は、デバイスの障害対応機能を強化します。スイッチの CPU（コントロールプレーンとして知られている）によって送受信されるパケットをキャプチャする機能を提供します。パケットキャプチャはその後、ローカルストレージに保存され、オフライン分析用にエクスポートされます。キャプチャパラメータを定義し、キャプチャをアクティブ化するために使用されるエンティティは、キャプチャポイントと呼ばれます。デバイスは、最大4つのキャプチャポイントとキャプチャされたパケット用のバッファとして20メガバイトをサポートします。

キャプチャバッファをローカルフラッシュまたはUSB上のファイルにエクスポートするには、[Buffer File Operation] を選択します。

1. [Crash Capture Destination] は、デバイスがクラッシュした場合にキャプチャファイルをエクスポートするために使用される設定です。このシナリオでは、ユーザーはファイルを手動でエクスポートできません。したがって、エクスポート先を手動で定義する必要があります。ファイルを保存する宛先デバイスを選択します。
   - [Flash]：ファイルをデバイスのフラッシュに保存します。
   - [USB]：デバイスに接続されている USB ストレージデバイスにファイルを保存します。

（注） この場合、キャプチャファイルの名前は自動的に設定され、キャプチャの日時が示されます。

キャプチャポイント設定

（注） この設定は、[Advanced Mode] でのみ使用できます。

キャプチャポイントを定義してアクティブにするには、次の手順を実行します。

手順

ステップ 1 [Status and Statistics] > [Onboard Packet Capture] > [Capture Point Settings] の順に移動します。

ステップ 2 [Add] をクリックしてキャプチャポイントを追加し、以下を設定します。

- [Capture Point Name]：キャプチャポイントの名前。
- [Buffer Mode]：キャプチャモードを次のいずれかに定義します。
  - [Linear]：キャプチャバッファがいっぱいになると、キャプチャが終了します。
  - [Circular]：バッファがいっぱいになると、キャプチャが終了し、バッファの先頭にあるパケットが書き換えられます。
- [Buffer Size (MB)]：キャプチャバッファのサイズを MB 単位で定義します。すべてのキャプチャポイントのバッファは 20 MB を超えることはできません。
- [Interface]：コントロールプレーン（CPU）インターフェイスのみがサポートされます。
- [Capture Direction]：キャプチャするトラフィックの方向を定義します（インバウンドトラフィックとアウトバンドトラフィックの両方（[both]）、インバウンドトラフィックのみ（[in]）、またはアウトバンドトラフィックのみ（[out]））。

ステップ 3 [Apply] をクリックします。

ステップ 4 キャプチャポイントを編集または削除するには、キャプチャポイントを選択し、[Edit] または [Delete] をクリックします。

ステップ 5 キャプチャポイントをアクティブにするには、テーブルからキャプチャポイントの 1 つを選択し、[Operations] をクリックします。[Capture Point Operation] フィールドで、[Activate] を選択し、[Apply] をクリックします。[Capture Point Settings] テーブルのキャプチャポイントの状態が [Active] に設定されます。

ステップ 6 アクティブなキャプチャポイントを非アクティブにするには、アクティブなキャプチャポイントを選択し、[Operations] をクリックします。[Capture Point Operation] フィールドで、[Deactivate] を選択し、[Apply] をクリックします。[Capture Point Settings] テーブルのキャプチャポイントの状態が [Inactive] に設定されます。

バッファファイル操作

（注） この設定は、[Advanced Mode] でのみ使用できます。

キャプチャされたパケットは、メモリバッファに保存されます。さらにデバッグするためにパケットを不揮発性メモリにコピーするには、次の手順を実行します。

手順

ステップ 1 [Status and Statistics] > [Onboard Packet Capture] > [Buffer File Operation] の順に移動します。

ステップ 2 キャプチャ中にデバイスがクラッシュした場合、パケットは自動的に不揮発性メモリに保存されます。クラッシュレポートを保存する接続先デバイスを選択します。

- [Flash]：ファイルをデバイスのフラッシュに保存します。（デフォルト）
- [USB]：デバイスに接続されている USB ストレージデバイスにファイルを保存します。

ステップ 3 [Apply] をクリックして、[Crash Capture Destination] の設定を保存します。

ステップ 4 キャプチャポイントバッファの 1 つを手動でエクスポートするには、画面の [Export Capture] セクションに移動し、次のように設定します。

- [Capture Point Name]：エクスポートするキャプチャポイントを選択します。
- [Capture File Name]：エクスポートするファイルの名前を定義します。
- [Export Destination]：ファイルを保存する宛先デバイスを選択します。
  - [Flash]：ファイルをデバイスのフラッシュに保存します。
  - [USB]：デバイスに接続されている USB ストレージデバイスにファイルを保存します。

ファイルは、選択に基づいてフラッシュまたは USB にエクスポートできます。

ステップ 5 キャプチャポイントファイルをエクスポートするには、[Export] をクリックします。

バッファ統計

（注） この設定は、[Advanced Mode] でのみ使用できます。

キャプチャバッファ統計情報を表示するには、次の手順を実行します。

手順

ステップ 1 [Status and Statistics] > [Onboard Packet Capture] > [Buffer Statistics] の順に移動します。

ステップ 2 [Capture Point Name] フィールドで、ドロップダウンリストからキャプチャバッファを選択して統計情報を表示します。

ステップ 3 次に、次のオプションから [Refresh Rate] を選択します。

- リフレッシュなし
- 15秒
- 30 秒
- 60 秒

ステップ 4 次の統計情報が表示されます。

- [Buffer State]：アクティブまたは非アクティブ
- [Buffer Mode]：線形または円形
- [Buffer Size (KB)]：バッファのサイズ（キロバイト単位）
- [Captured Packets]：キャプチャされたパケットの数
- [Buffer Used (KB)]：使用されている実際のバッファサイズ。
- [Packet Capture Rate per Second]：キャプチャされたトラフィックの 1 秒あたりのパケットレート。
- [Packets Dropped]：キャプチャセッション中にドロップされたパケットの数。

ステップ 5 情報を手動で更新するには、[Refresh] をクリックします。

ステップ 6 バッファをクリアするには、[Clear Buffer] をクリックします。

RMON

リモート ネットワーク モニタリング（RMON）を使用すると、デバイスの SNMP エージェントが、トラフィック統計情報の監視をプロアクティブに一定期間行い、トラップを SNMP マネージャに送信できます。ローカルの SNMP エージェントは、実際のリアルタイム カウンタを事前に定義されたしきい値と比較し、アラームを生成します。中央の SNMP 管理プラットフォームによるポーリングは必要ありません。これは、ネットワークのベースラインに応じて正しいしきい値を設定している場合に、プロアクティブな管理の効果的なメカニズムとなります。

RMONでは、SNMPマネージャが情報を取得するために頻繁にデバイスをポーリングする必要がないため、マネージャとデバイス間のトラフィックが減少します。さらに、デバイスがイベントの発生時にそれらをレポートするため、マネージャはタイムリーに状態レポートを取得できます。

この機能を使用すると、次のアクションを実行できます。

- 現在の統計を表示する（カウンタ値がクリアされた時点以降）。また、一定期間、これらのカウンタの値を収集して、収集したデータのテーブルを表示できます。収集されたセットがそれぞれ、[History] タブの 1 行になります。

- 「一定数のレイトコリジョンに達した」などのカウンタ値の興味のある変化を定義し（アラームを定義）、このイベントが発生したときにどのアクションを実行するかを指定します（ログ、トラップ、またはログとトラップ）。

統計情報

[Statistics] ページには、パケット サイズについての詳細情報および物理レイヤ エラーについての情報が表示されます。情報は、RMON 標準規格に従って表示されます。オーバーサイズ パケットは、次の条件を満たすイーサネット フレームとして定義されます。

- パケット長が、MRU バイト サイズを超えている。
- コリジョンイベントは検出されていない。
- レイトコリジョンイベントは検出されていない。
- 受信（Rx）エラーイベントは検出されていない。
- パケットは、有効な CRC を保持している。

RMON統計情報を表示したり、リフレッシュレートを設定したりする場合は、次の手順を実行します。

手順

ステップ 1 [Status and Statistics] > [RMON] > [Statistics] の順にクリックします。

ステップ 2 イーサネット統計を表示する [Interface] を選択します。

ステップ 3 インターフェイスの統計を更新する前の経過期間として、[Refreshed Rate] を選択します。

選択インターフェイスに関する次の統計が表示されます。

Bytes Received	受信したオクテット数（不良パケットや FCS オクテットも含まれますが、フレーミングビットは含まれません）。
Drop Events	ドロップされたパケット数。
Packets Received	マルチキャストパケットとブロードキャストパケットを含む、受信済みの正常なパケット数。
Broadcast Packets Received	受信した良好なブロードキャストパケット数。マルチキャストパケットは、この数には含まれません。
Multicast Packets Received	受信した良好なマルチキャストパケット数。
CRC & Align Errors	発生した CRC および配置エラー数。
Undersize Packets	受信したアンダーサイズパケット数（64オクテット未満）。

Oversize Packets	受信したオーバーサイズパケット数（2000 オクテット以上）。
Fragments	受信したフラグメント（フレーミングビットは含まず、FCS オクテットを含む、64 オクテット未満のパケット）の数。
Jabbers	1632 オクテットを超える受信済みパケット数。この数では、フレームビットは除外されますが、整数のオクテットを持つ不良 FCS（フレームチェックシーケンス）（FCS エラー）、または非整数のオクテット（配置エラー）数の不良 FCS のいずれかを伴う FCS オクテットは含まれます。Jabber パケットは、次の条件を満たすイーサネット フレームとして定義されます。
Collisions	受信したコリジョン数。ジャンボ フレームが有効な場合、Jabber フレームのしきい値は、ジャンボ フレームの最大サイズにまで引き上げられます。
Frames of 64-Bytes	送受信された 64 バイトを格納するフレーム数。
Frames of 65–127 Bytes	送受信された 65 ～ 127 バイトを格納するフレーム数。
Frames of 128–255 Bytes	送受信された 128 ～ 255 バイトを格納するフレーム数。
Frames of 256–511 Bytes	送受信された 256 ～ 511 バイトを格納するフレーム数。
Frames of 512–1023 Bytes	送受信された 512 ～ 1023 バイトを格納するフレーム数。
Frames of 1024 Bytes or More	送受信された 1024 ～ 2000 バイトを格納するフレーム、およびジャンボフレームの数。

（注）
前述のいずれかのフィールドにいくつかの（0 ではない）エラーが表示された場合、[Last Update] 時間が表示されます。

ステップ 4 テーブルビューまたはグラフィックビューでカウンタを管理するには、次の手順を実行します。

- データをクリアするには、[Clear Interface Counters] をクリックします。
- データをリフレッシュするには、[Refresh] をクリックします。
- すべてのポートをテーブル表示で確認するには、[View All Interfaces Statistics] をクリックします。
- これらの結果をグラフィック形式で表示するには、[Graphic View] をクリックします。この表示では、結果を表示する [Time Span] とフレームサイズを選択できます。

履歴

RMON 機能によって、インターフェイスごとに統計をモニタリングできます。

[History] ページでは、サンプリング頻度、保存するサンプル数、およびデータ収集元ポートを定義できます。データは、サンプリングおよび保存された後に、[History Table] ページに表示されます。このページは、[History Table] をクリックすると表示できます。

RMON の制御情報を入力するには、次の手順を実行します。

手順

ステップ 1 [Status and Statistics] > [RMON] > [History] の順にクリックします。このページに表示されるフィールドは、以下の [Add RMON History] ページで定義されます。このページで、[Add RMON History] ページで定義されない唯一のフィールドが、次のフィールドです。

- [Current Number of Samples]：RMON は、規格により、要求されたすべてのサンプルを許可するのではなく、要求ごとにサンプル数を制限するようになっています。したがって、このフィールドは、要求に対して許可されたサンプル数（要求値以下）を表します。

ステップ 2 [Add] をクリックします。

ステップ 3 パラメータを入力します。

- [New History Entry]：新しい [History] テーブルエントリの番号が表示されます。
- [Source Interface]：履歴サンプルを取得するインターフェイスのタイプを選択します。
- [Max No. of Samples to Keep]：保存されるサンプル数を入力します。
- [Sampling Interval]：ポートからサンプルが収集される秒数を入力します。フィールドの値の範囲は 1 ～ 3600 です。
- [Owner]：RMON 情報を要求した RMON ステーションまたはユーザーを入力します。

ステップ 4 [Apply] をクリックします。エントリが [History Control Table] ページに追加され、実行コンフィギュレーション ファイルが更新されます。

ステップ 5 [History Table] をクリックして、実際の統計情報を表示します。

ステップ 6 [History Control Table] をクリックして、履歴制御テーブルを表示します。

ステップ 7 [History Entry No.] ドロップダウン メニューから表示するサンプルのエントリ番号を選択します。

選択したサンプルに関するフィールドが表示されます。

- [Owner]：履歴テーブルエントリの所有者。
- [Sample No.]：このサンプルから取得された統計情報。
- [Drop Events]：サンプリング中にネットワークリソース不足によりドロップされたパケット数。これは、正確なドロップされたパケット数ではなく、ドロップされたパケットが検出された回数を表しています。

- [Bytes Received]：受信したオクテット数。不良パケットと FCS オクテットが含まれますが、フレーミングビットは含まれません。
- [Packets Received]：不良パケット、マルチキャストパケット、ブロードキャストパケットを含む受信済みパケット数。
- [Broadcast Packets]：正常なブロードキャストパケット数。マルチキャストパケットは含まれません。
- [Multicast Packets]：受信した正常なマルチキャストパケット数。
- [CRC Align Errors]：発生した CRC とアラインメントエラー数。
- [Undersize Packets]：受信したアンダーサイズパケット数（64 オクテット未満）。
- [Oversize Packets]：受信したオーバーサイズパケット数（2000 オクテット超過）。
- [Fragments]：受信したフラグメント数（64 オクテット未満のパケット）。フレーミングビットは含まれませんが、FCS オクテットは含まれます。
- [Jabbers]：2000 オクテットを超える受信したパケット合計数。この数では、フレーム ビットは除外されますが、整数のオクテットを持つ不良 FCS（フレーム チェック シーケンス）（FCS エラー）、または非整数のオクテット（配置エラー）数の不良 FCS のいずれかを伴う FCS オクテットは含まれます。
- [Collisions]：受信したコリジョン数。
- [Utilization]：インターフェイスが処理できる、最大トラフィックと比較した現在のインターフェイス トラフィックの割合。

イベント

アラームをトリガーする頻度と発生する通知のタイプを制御できます。これは、次のように実行します。

- [Events] ページ：アラームがトリガーされたときにどうするかを設定します。これは、ログとトラップの任意の組み合わせになります。
- [Alarms] ページ：アラームをトリガーする頻度を設定します。

RMON イベントを定義するには、次の手順を実行します。

手順

ステップ 1 [Status and Statistics] > [RMON] > [Events] の順にクリックします。

ステップ 2 [Add] をクリックします。

ステップ 3 パラメータを入力します。

- [Event Entry]：新しいエントリのイベント エントリ インデックス番号が表示されます。

- [Community]：トラップが送信されるときに含める SNMP コミュニティ文字列を入力します。
- [Description]：イベントの名前を入力します。この名前は、[Add RMON Alarm] ページで、アラームをイベントにアタッチするために使用されます。
- [Notification Type]：このイベントの結果生じるアクションのタイプを選択します。値は次のとおりです。
  - [None]：アラームが作動したときにアクションを実行しません。
  - [Log (Event Log Table)]：アラームがトリガーされたときに、[Event Log] テーブルにログ エントリを追加します。
  - [Trap (SNMP Manager and Syslog Server)]：アラームが作動したときに、リモート ログ サーバにトラップを送信します。
  - [Log and Trap]：[Event Log] テーブルにログ エントリを追加し、アラームが作動したときに、リモート ログ サーバにトラップを送信します。
- [Owner]：イベントを定義したデバイスまたはユーザを入力します。

ステップ 4 [Apply] をクリックします。RMON イベントが実行コンフィギュレーション ファイルに保存されます。

ステップ 5 [Event Log Table] をクリックして、発生してログに書き込まれたアラームのログを表示します。

次のデータが表示されます。

- [Event Entry No.]：イベントのエントリ番号
- [Log No.]：イベントのログ番号
- [Log Time]：イベントログの時間
- [Description]：イベントログの説明。

アラーム

RMON アラームは、エージェントによって維持されるカウンタまたはその他の任意の SNMP オブジェクト カウンタで例外イベントを生成するための、しきい値とサンプリング間隔を設定するメカニズムを提供します。アラームに、上昇しきい値と下限しきい値の両方を設定する必要があります。上昇しきい値を超えた後は、対応する下限しきい値を下回るまで、上昇イベントは生成されません。下限アラームが発行された後は、上昇しきい値を超えたときに、次のアラームが発行されます。

1 つ以上のアラームがイベントにバインドされます。イベントは、アラームが発生したときに実行するアクションを示しています。

アラーム カウンタは、絶対値またはカウンタの値の変化（差分）のいずれかによってモニタできます。

RMON アラームを入力するには、次の手順を実行します。

手順

ステップ 1 [Status and Statistics] > [RMON] > [Alarms] の順にクリックします。

定義済みのすべてのアラームが表示されます。フィールドについては、以下の [Add RMON Alarm] ページで説明されています。それらのフィールドに加え、次のフィールドが表示されます。

- [Counter Value]：最後のサンプリング期間の統計値が表示されます。

ステップ 2 [Add] をクリックします。

ステップ 3 パラメータを入力します。

Alarm Entry	アラームエントリ番号が表示されます。
Interface	RMON 統計情報の表示対象となるインターフェイスのタイプを選択します。
Counter Name	測定される発生タイプを示す MIB 変数を選択します。
Sample Type	アラームを生成するサンプリング方法を選択します。次のオプションがあります。 • [Absolute]：しきい値を超える、または下回った場合にアラームが生成されます。 • [Delta]：現在の値から最後にサンプリングされた値を減算します。その値の差がしきい値と比較されます。しきい値を超える、または下回った場合にアラームが生成されます。
Rising Threshold	上昇しきい値アラームをトリガーする値を入力します。
Rising Event	上昇イベントがトリガーされたときに実行するイベントを選択します。イベントはイベント （26 ページ）で設定されます。
Falling Threshold	下降しきい値アラームをトリガーする値を入力します。
Falling Event	下降イベントがトリガーされたときに実行するイベントを選択します。
Startup Alarm	アラームの生成を開始する最初のイベントを選択します。上昇は、低い値のしきい値からより高い値のしきい値へと、その値を超えることとして定義されます。 • [Rising Alarm]：上昇値が上昇しきい値アラームをトリガーします。 • [Falling Alarm]：下降値が下限しきい値アラームをトリガーします。 • [Rising and Falling]：上昇値と下降値の両方がアラームをトリガーします。

Interval	アラーム間隔を秒単位で入力します。
Owner	アラームを受信するユーザーまたはネットワーク管理システムの名前を入力します。

ステップ 4 [Apply] をクリックします。RMON アラームが実行コンフィギュレーション ファイルに保存されます。

sFlow

sFlow モニタリング システムは、sFlow エージェント（スイッチまたはルータ、もしくはスタンド アロン プローブに組み込まれている）と、sFlow コレクタと呼ばれる、中央のデータ コレクタで構成されています。sFlow エージェントは、サンプリング技術を使用して、モニタリングしているデバイスからトラフィックと統計をキャプチャします。sFlow データグラムは、分析のために、サンプリングされたトラフィックと統計を sFlow コレクタに転送するために使用されます。

sFlow V5 では、以下が定義されています。

- トラフィックのモニタ方法。
- sFlow エージェントを制御する sFlow MIB。
- 中央のデータ コレクタにデータを転送する際に、sFlow エージェントによって使用されるサンプル データの形式。デバイスは、フロー サンプリングとカウンタ サンプリングの 2 つのタイプの sFlow サンプリングをサポートしています。sFlow V5 に従って、次のカウンタ サンプリングが実行されます（インターフェイスによってサポートされている場合）。
  - 汎用インターフェイス カウンタ（RFC 2233）
  - イーサネット インターフェイス カウンタ（RFC 2358）

sFlow受信機

sFlow 受信機は、sFlow エージェントと sFlow コレクタの間の sFlow セッションを維持するために使用される一連のオブジェクトを定義します。sFlow受信機のパラメータを設定するには、次の手順を実行します。

手順

ステップ 1 [Status and Statistics] > [sFlow] > [sFlow Receivers] の順にクリックします。

ステップ 2 次のフィールドに入力します。

- [IPv4 Source Interface]：IPv4 送信元インターフェイスを選択します。

（注）
自動（Auto）オプションを選択すると、システムは発信インターフェイスで定義されているIPアドレスから送信元 IP アドレスを取得します。

- [IPv6 Source Interface]：IPv6 送信元インターフェイスを選択します。

ステップ 3 受信機（sFlow アナライザ）を追加するには、[Add] をクリックして、[Receiver Index] で事前に定義されたサンプリング定義インデックスのいずれかを選択します。

ステップ 4 受信者のアドレス フィールドに入力します。

- [Server Definition]：[By IP address] または [By name] のいずれかで sFlow サーバを指定するかを選択します。

  [Server Definition] が [By IP Address] の場合：

- [IP Version]：サーバーが IPv4 または IPv6 のどちらのアドレスを使用するかを選択します。
- [IPv6 Address Type]：IPv6 を使用する場合、IPv6 アドレス タイプを選択します。次のオプションがあります。
  - [Link Local]：IPv6 アドレスによって、単一ネットワークリンク上のホストが一意に識別されます。リンク ローカル アドレスのプレフィックスは FE 80 で、ルーティングはできません。また、ローカル ネットワーク上の通信にのみ使用できます。1 つのリンク ローカル アドレスのみがサポートされます。リンク ローカルアドレスがインターフェイス上に存在する場合、このエントリは構成内のアドレスを置き換えます。
  - [Global]：IPv6アドレスは、他のネットワークからも認識かつアクセス可能なグローバルユニキャスト IPv6 タイプになります。
- [Link Local Interface]：リストからリンク ローカル インターフェイスを選択します（IPv6 を使用する場合）。

ステップ 5 次のフィールドに入力します。

- [Server IP Address/Name]：サーバーの IP アドレスまたは名前を入力します。どちらでも構いません。
- [Port]：SYSLOG メッセージが送信されるポート。
- [Maximum Datagram Size]：単一のサンプル データグラム（フレーム）で、受信者に送信できる最大バイト数。

ステップ 6 [Apply] をクリックします。

sFlowインターフェイス設定

ポートからデータグラムまたはカウンタをサンプリングするには、ポートを受信機に関連付ける必要があります。sFlow ポートは、sFlow受信機 （29 ページ）ページで受信機を定義してからしか設定できません。

サンプリングを有効にして、sFlow 情報を収集するポートを設定するには、次の手順を実行します。

手順

ステップ 1 [Status and Statistics] > [sFlow] > [sFlow Interface Settings] の順にクリックします。

sFlow インターフェイス設定が表示されます。

ステップ 2 sFlow 受信者をポートに関連付けるには、[Edit] をクリックして、次のフィールドに入力します。

- [Interface]：情報の収集元となるユニット/ポートを選択します。
- [(Flow Sampling) State]：フロー サンプリングを有効/無効にします。
- [Sampling Rate]：x が入力された場合は、フローサンプルが x フレームごとに取得されます。

  （注）
  [Sampling Rate]：x が入力された場合は、フローサンプルが x フレームごとに取得されます。インターフェイスには、最大 3 つのサンプリングレート値を設定できます。サンプリングレートは、インターフェイスで設定されているときにカウントされます。複数のインターフェイスで、3 つの許容レートのうちの特定のサンプリングレートを設定できます。インターフェイスで 4 番目のレートを設定しようとすると、拒否されます。

- [Maximum Header Size (Bytes)]：サンプリングされたパケットからコピーする必要がある最大バイト数。
- [Receiver Index]：sFlow受信機 （29 ページ）ページで定義したインデックスのいずれかを選択します。
- [(Counter Sampling) State]：カウンタ サンプリングを有効/無効にします。
- [Sampling Interval (Sec.)]：x が入力されている場合、x 秒ごとにカウンタサンプルが取得されるように指定します。
- [Receiver Index]：これらのsFlow受信機 （29 ページ）ページで定義したインデックスのいずれかを選択します。

ステップ 3 [Apply] をクリックします。

sFlow統計情報

sFlow 統計情報を表示するには、次の手順を実行します。

手順

ステップ 1 [Status and Statistics] > [sFlow] > [sFlow Statistics] の順にクリックします。

ステップ 2 [Refresh Rate] ドロップダウンメニューからリフレッシュレートを選択します。

インターフェイスごとに次の sFlow 統計情報が表示されます。

- [Port]：サンプルが収集されたポート。
- [Packets Sampled]：サンプリングされたパケットの数。
- [Datagrams Sent to Receiver]：送信された sFlow サンプリングパケットの数。

ステップ 3 すべてのポートの sFlow 統計をクリアするには、[Clear All Interface Counters] または [Clear Interface Counters] をクリックします。

ログの表示

デバイスは、次のログに書き込むことができます。

- RAM 内のログ（リブート時にクリアされる）
- フラッシュメモリ内のログ（ユーザーコマンドの実行時にのみクリアされる）

シビラティ（重大度）別に各ログに書き込まれるメッセージを設定できます。メッセージは、外部 SYSLOG サーバ上に存在するログを含め、複数のログに記録することができます。

RAMメモリ

[RAM Memory] ページには、RAM（キャッシュ）に保存されたすべてのメッセージが時間順に表示されます。すべてのエントリが RAM ログに保存されます。

ポップアップ SYSLOG 通知

新しい SYSLOG メッセージが RAM ログファイルに書き込まれると、Web GUI にその内容に関する通知が表示されます。Web GUI は 10 秒ごとに RAM ログをポーリングします。過去 10 秒間に作成されたすべての SYSLOG に関する SYSLOG 通知ポップアップが画面右下に表示されます。

ログエントリを表示するには、[Status and Statistics] > [View Log] > [RAM Memory] の順にクリックします。

ページの上部に、以下が表示されます。

- [Alert Icon Blinking]：無効と有効を切り替えます。

- [Pop-Up Syslog Notifications]：前述したようにポップアップ SYSLOG の受信を有効にします。
- [Current Logging Threshold]：生成されるロギングのレベルを指定します。これは、フィールドの名前の横にある [Edit] をクリックして、変更できます。

このページには、各ログファイルに関する次のフィールドが含まれます。

- [Log Index]：ログ ID
- [Log Time]：メッセージが生成された時刻。
- [Severity]：イベントのシビラティ（重大度）。
- [Description]：イベントについて説明するメッセージテキスト。

ログ メッセージをクリアするには、[Clear Logs] をクリックします。

フラッシュ メモリ

[Flash Memory] ページには、フラッシュメモリに保存されたメッセージが、時系列で表示されます。ログの最小シビラティ（重大度）はログ設定で設定します。フラッシュのログは、デバイスのリブート時に存続します。ログは手動でクリアすることができます。

フラッシュのログを表示するには、[Status and Statistics] > [View Log] > [Flash Memory] の順にクリックします。

[Current Logging Threshold] は、生成されるロギングのレベルを指定します。これは、フィールドの名前の横にある [Edit] をクリックして、変更できます。

フラッシュ メモリ ログ テーブルには、ログファイルごとに次のフィールドがあります。

- [Log Index]：ログエントリ番号。
- [Log Time]：メッセージが生成された時刻。
- [Severity]：イベントのシビラティ（重大度）。
- [Description]：イベントについて説明するメッセージテキスト。

メッセージをクリアするには、[Clear Logs] をクリックします。メッセージがクリアされます。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。