コントローラと AP の設定を構成する

CLI セッションのプロトコル設定

多くの Prime Infrastructure のワイヤレス機能（自律アクセス ポイントおよびコントローラのコマンドライン インターフェイス（CLI）テンプレートや移行テンプレートなど）では、自律アクセス ポイントまたはコントローラに対して CLI コマンドを実行する必要があります。これらの CLI コマンドを入力するには、Telnet または SSH セッションを確立します。CLI セッション ページでは、セッション プロトコルを選択できます。

CLI テンプレートでは、質問に対する回答操作（コマンドに対して「はい（Yes）」または「いいえ（No）」で回答する、*Enter* キーを押して続行する、など）は不要です。これは Prime Infrastructure によって自動的に実行されます。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [ネットワークとデバイス（Network and Device）] > [CLI セッション（CLI Session）]** の順に選択します。

ステップ 2 [コントローラ セッション プロトコル（Controller Session Protocol）] を選択します。[SSH] または [Telnet] を選択できます（[SSH] がデフォルト）。

ステップ 3 [Autonomous AP Session Protocol] を選択します。[SSH] または [Telnet] を選択できます（[SSH] がデフォルト）。

ステップ 4 デフォルトでは、[Run Autonomous AP Migration Analysis on discovery] オプション ボタンは [No] に設定されています。Autonomous AP を検出し、移行分析を実行する場合は、[Yes] を選択します。

ステップ 5 [Save] をクリックします。

Prime Infrastructure での Unified AP ping 到達可能性設定の有効化

Cisco Prime Infrastructure で Unified AP が検出されるたびに、Prime Infrastructure はその AP が ping に対応するかどうかを判別し、それに応じて Prime Infrastructure データベース内の ping 対応ステータスを更新します。

次の条件に応じて、さまざまなアラームが起動されます。

- Unified AP が関連付け解除された場合、その AP が FlexConnect モードであれば、Prime Infrastructure は AP に到達可能であるかどうかをチェックします。AP が ping に対応し、ping で到達可能である場合、Prime Infrastructure は低シビラティ（重大度）のアラームを起動します。AP が ping に対応しない場合、または ping で到達可能でない場合は、高シビラティ（重大度）のアラームを起動します。
- Unified AP が関連付け解除された場合、その AP が FlexConnect モードでなければ、Prime Infrastructure は高シビラティ（重大度）のアラームを起動します。

デフォルトでは、Unified AP の ping 到達可能性機能は、Prime Infrastructure バージョン 3.3 以降で有効です。ただし、3.2 以前のバージョンでは無効です。有効にするには、次の手順に従います。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [ネットワークとデバイス（Network and Device）] > [Unified AP ping 到達可能性（Unified AP Ping Reachability）]** の順に選択します。

ステップ 2 [PrimeがAPの到達可能性を取得できるようにする（Allow Prime to learn about AP Reachability）] オプション ボタンを選択して、Cisco Prime Infrastructure が AP の到達可能性を取得できるようにします。これにより、バックグラウンド タスクがトリガーされ、各アクセス ポイントに対して ping が実行されて、その結果が Prime Infrastructure データベースに保存されます。

ステップ 3 ユーザーには、ping 到達可能性を取得するためにバックグラウンド ジョブがトリガーされることを伝えるアラートでプロンプトが出されます。[OK] をクリックして、先へ進みます。

AP の到達可能性を取得するために、Prime Infrastructure 内でバックグラウンド ジョブがトリガーされて、関連付けられているすべての API に対して実行されます。新しいジョブは、[ジョブ ダッシュボード（Job Dashboard）] で次の情報を使用して作成します。

ステップ 4 [Prime からすべてのアクセス ポイントに ping で到達可能（All access points are ping reachable from Prime）] オプション ボタンを選択すると、管理者はすべての Unified AP を ping 対応としてマークします。

ステップ 5 **[管理（Administration）] > [ダッシュボード（Dashboards）] > [ジョブ ダッシュボード（Job Dashboard）] > [システム ジョブ（System Jobs）] > [ステータス（Status）]** を選択し、ジョブのステータスを表示します。

ステップ 6 ジョブの詳細を検索するには、[クイック フィルタ（Quick Filter）] オプションを使用して、[名前（Name）] 検索フィールドに **[Unified AP ping 機能の詳細（Learn Unified AP Ping Capability）]** を入力します。

結果は [ステータス（Status）] テーブルに表示されます。このテーブルには、次の情報が表示されます。

- ジョブ タイプ（**Job Type**）
- **Status**（ステータス）
- 最終実行ステータス（**Last Run Status**）
- 前回の開始時間（**Last Start Time**）
- デュレーション（**Duration**）
- 次回の開始時間（**Next Start Time**）
- 詳細を表示するには、[AP ping 到達可能性の詳細（Learn AP Ping Reachability）] リンクをクリックします。[AP ping 到達可能性の詳細（Learn AP Ping Reachability）] ページに、次の情報が表示されます。すべてのジョブ インスタンスの詳細を表示するには、[すべて表示（Show All）] をクリックします。
  - 定例（**Recurrence**）
  - インターバル（**Interval**
  - 実行 ID（**Run ID**）
  - **Status**（ステータス）
  - デュレーション（**Duration**）
  - 開始時刻（**Start Time**）
  - 完了時刻（**Completion Time**）

アップグレード後のコントローラの更新

[コントローラ アップグレード（Controller Upgrade）] ページでは、コントローラのアップグレード後に自動更新を行って、コントローライメージに変更があるたびに自動的に設定を復元することができます。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [ネットワークとデバイス（Network and Device）] > [コントローラ アップグレード（Controller Upgrade）]** の順に選択します。

ステップ 2 [アップグレード後の自動更新（Auto refresh After Upgrade）] チェックボックスをオンにすると、コントローラのイメージに変更があるたびに設定は自動的に復元されます。

ステップ 3 [Save Config トラップで同期（Sync on Save Config Trap）] チェックボックスをオンにすると、Prime Infrastructure が Save Config トラップを受信するとコントローラで同期がトリガーされます。このチェックボックスをオンにすると、次のいずれかのオプションを選択できます。

- Prime Infrastructure データベースに設定を保持（Retain the configuration in the Prime Infrastructure database）
- [コントローラ上の現在の設定を使用（Use the configuration on the controller currently）]

ステップ 4 [Save] をクリックします。

不正 AP に接続したスイッチ ポートの追跡

は、不正なアクセス ポイントが接続されているネットワーク スイッチ ポートを自動的に識別できます。この機能は自動スイッチ ポート トレーシングに基づくものであり、その動作には Prime Infrastructure のフル ライセンスが要求されることに注意してください。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [ネットワークとデバイス（Network and Device）] > [スイッチ ポート トレース（SPT）（Switch Port Trace (SPT)）] > [自動 SPT（Auto SPT）]** の順に選択します。[自動 SPT（Auto SPT）] ページが表示されます。

ステップ 2 [自動スイッチ ポート トレースの有効化（Enable Auto Switch Port Tracing）] チェックボックスをオンにして、Prime Infrastructure が不正アクセス ポイントの接続先スイッチ ポートを自動的にトレースできるようにします。次に、以下を含む自動ポート トレース用のパラメータを指定します。

- 不正 API とポート間のトレースを実行する間隔（分）
- 有線で検出された不正 AP をトレースするかどうか
- 含めるシビラティ（重大度）（重大、メジャー、マイナー）

ステップ 3 [自動封じ込みの有効化（Enable Auto Containment）] チェックボックスをオンにして、Prime Infrastructure がシビラティ（重大度）に応じて自動的に不正 AP を封じ込めるようにします。次に、自動封じ込み用の以下のパラメータを指定します。

- ポート トレースによって有線で検出された不正 AP を除外するかどうか
- 封じ込み対象に含めるシビラティ（重大度）（重大、メジャー）
- 封じ込みレベル（最大 4 つの AP）

ステップ 4 [OK] をクリックします。

スイッチ ポート トレースを設定する

現在、Prime Infrastructure では、コントローラから情報を取得することによって、不正アクセス ポイントを検出できます。不正アクセス ポイント表には、ネイバー リストにないフレームから検出された BSSID アドレスが記載されています。指定された期間の終わりに、不正アクセス ポイント表の内容が、CAPWAP Rogue AP Report メッセージでコントローラに送信されます。この方式では、Prime Infrastructure がコントローラから受信した情報を収集します。この機能拡張により、検出された不正アクセス ポイントに対応し、今後発生する攻撃を回避できま

す。トレース情報は不正アクセス ポイントの Prime Infrastructure ログだけで使用でき、不正クライアントのログには使用できません。

不正アクセス ポイントに接続した不正クライアントの情報を使用して、ネットワークで不正アクセス ポイントに接続しているスイッチ ポートを追跡します。危険性のない不正アクセス ポイントまたは削除された不正アクセス ポイントにトレーシングを設定しようとすると、警告メッセージが表示されます。

スイッチ ポート トレーシングで、v3 を使用してスイッチ ポートを正常にトレースするには、すべての OID を SNMP v3 のビューに含める必要があり、SNMP v3 グループ内の VLAN ごとに VLAN の内容を作成する必要があります。[Switch Port Trace] ページでは、回線上で検出された不正アクセス ポイントに対するトレースを実行できます。

適切にトレースして不正アクセス ポイントを封じ込めるには、以下の情報を正しく指定する必要があります。

- レポート AP：不正アクセス ポイントは 1 台以上の管理対象アクセス ポイントによってレポートされる必要があります。
- AP CDP ネイバー：シード スイッチを判別するために、アクセス ポイント CDP ネイバー情報が必要です。
- スイッチの IP アドレスと SNMP のクレデンシャル：トレース対象のすべてのスイッチは管理 IP アドレスを持つ必要があり、SNMP 管理が有効にされている必要があります。個々のスイッチだけを追加するのではなく、ネットワーク アドレスをベースに項目を追加できます。正しい write コミュニティ ストリングを指定して、スイッチ ポートを有効または無効にする必要があります。トレーシングの場合は、read コミュニティ ストリングで十分です。/32 サブネット マスクを使用したネットワーク アドレスは、グローバル SNMP クレデンシャルの設定ではサポートされていません。詳細なガイダンス情報については、「関連項目」の「不正およびスイッチ ポート トレーシングに関して頻繁に寄せられる質問」を参照してください。
- スイッチ ポートの設定：トランキング スイッチ ポートを正しく設定する必要があります。スイッチのポート セキュリティを無効にする必要があります。
- スイッチ ポート トレーシングは、Cisco イーサネット スイッチおよび Catalyst スイッチ 2960、3560、3560-E、3750-E、3850、4500 シリーズのみでサポートされます。
- スイッチ VLAN 設定が適切に構成されている必要があります。Prime Infrastructure は、Cisco Discovery Protocol ネイバー情報を使用して、スイッチの IP アドレスを取得します。そのスイッチ内の VLAN 情報を使用して、スイッチの CAM テーブル エントリを読み取ります。スイッチ内の VLAN 情報が正しく設定されていないと、Prime Infrastructure は CAM テーブル エントリを読み取れません。したがって、スイッチの不正 AP をトレースすることができません。
- CDP プロトコルがすべてのスイッチ上で有効にされている必要があります。
- 不正アクセス ポイントとシスコ製スイッチの間にイーサネット接続が存在している必要があります。
- 不正なイーサネット スイッチ ポート情報を高い信頼性で検出する場合、不正アクセス ポイントとイーサネット スイッチ間のイーサネット MAC アドレスの差がおおむね 3 以上であれば、これらの間にトラフィックが存在するとみなします。

- 不正アクセス ポイントは、最大ホップ カウントの制限内でスイッチに接続される必要があります。
- SNMPv3 を選択している場合は、メイン グループのための 1 個（VLAN ベースでない MIB 用に必要）の他に、コンテキスト オプションを使用して、VLAN ごとに 1 個作成します。

（注） ベンダー OUI の一致を効果的に使用して一致の誤検出を排除するには、スイッチ ポートにロケーション情報を設定しておく必要があります。設定されていないスイッチ ポートは、ロケーション別の削除の実行後も OUI の一致対象のままとなります。

関連トピック

不正およびスイッチ ポート トレーシングに関して頻繁に寄せられる質問 （11 ページ）

SNMP クレデンシャルの設定

スイッチ ポート トレースの詳細を表示するには、次の手順を実行します。

ステップ 1 [管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [ネットワークとデバイス（Network and Device）] > [ポート トレースのスイッチ（SPT）（Switch Port Trace (SPT)）] > [SPT 設定（SPT Configuration）] の順に選択します。

ステップ 2 次の基本設定値を設定します。

- [MAC address +1/-1 search]：有効にするには、チェックボックスをオンにします。

この検索では、無線 MAC アドレスに 1 加算するか 1 減算することによって不正アクセス ポイントの有線側の MAC アドレスを得る、慣習的な MAC アドレス +1/-1 方式を使用します。

- [Rogue client MAC address search]：有効にするには、チェックボックスをオンにします。

不正クライアントが存在していると、検索可能な MAC アドレスのリストにクライアントの MAC アドレスが追加されます。

- [ベンダー（OUI）検索（Vendor (OUI) search）]：有効にするには、チェックボックスをオンにします。OUI は組織固有識別子の検索を意味し、MAC アドレスの先頭 3 バイトで検索します。
- [スイッチ トランク ポートの除外（Exclude switch trunk ports）]：スイッチ ポートのトレースからスイッチ トランク ポートを除外する場合に、このチェックボックスをオンにします。

（注） 特定の MAC アドレスについて複数ポートをトレースする場合は、精度を向上させるために、追加のチェックが実行されます。追加のチェックには、トランク ポートのチェック、ポート上にある AP でない CDP ネイバーのチェック、およびこの MAC アドレスがこのポート上の唯一のアドレスであるかどうかのチェックが含まれます。

- [デバイス リストの除外（Exclude device list）]：トレースから追加のデバイスを除外する場合に、このチェックボックスをオンにします。スイッチ ポート トレースから除外する各デバイスをデバイス リスト テキスト ボックスに入力します。各デバイス名をコンマで区切って入力してください。
- [最大ホップ数（Max hop count）]：このトレースに対するホップの最大数を入力します。ホップ カウントを大きくするほど、スイッチ ポート トレースの実行時間が長くなることに留意してください。

（注）　このホップ カウント値は自動 SPT に適用できません。

- [ベンダー リストの除外（Exclude vendor list）]：スイッチ ポート トレースから除外するすべてのベンダーをベンダー リスト テキスト ボックスに入力します。ベンダー名はカンマで区切ります。ベンダー リストでは、大文字と小文字が区別されません。

ステップ 3 次の詳細設定値を設定します。

- [不正 AP タスク最大スレッドのトレース（TraceRogueAP task max thread）]：スイッチ ポート トレーシングで、複数のスレッドを使用して不正アクセス ポイントをトレースします。このフィールドは、並列スレッドでトレースできる不正アクセス ポイントの最大数を示します。
- [不正 AP 最大キュー サイズのトレース（TraceRogueAP max queue size）]：スイッチ ポート トレーシングでは、キューを保持して、不正アクセス ポイントをトレースします。トレーシングする不正アクセス ポイントを選択すると、処理待ちのキューに入ります。このフィールドは、キューに保管できる項目の最大数を示します。
- [スイッチ タスク最大スレッド（SwitchTask max thread）]：スイッチ ポート トレーシングでは、複数のスレッドを使用して、スイッチ デバイスをクエリーします。このフィールドは、並列スレッドでクエリーできるスイッチ デバイスの最大数を示します。

これらのパラメータのデフォルト値は、通常の運用に適しています。これらのパラメータは、スイッチ ポート トレーシングと Prime Infrastructure のパフォーマンスに直接影響します。必要な場合を除き、これらのパラメータは変更しないことを推奨します。

- [CDP デバイス機能の選択（Select CDP device capabilities）]：有効にするには、チェックボックスをオンにします。

Prime Infrastructure では、トレーシング中にネイバーを検出するために CDP を使用します。ネイバーが検証されると、Prime Infrastructure では、[CDP 機能（CDP capabilities）] フィールドを使用して、ネイバー デバイスが有効なスイッチであるかどうかを判別します。ネイバー デバイスが有効なスイッチでない場合は、トレースされません。

ステップ 4 行った変更を保存するには [Save] をクリックします。ページを元の設定に戻すには、[Reset] をクリックします。出荷時の初期状態に設定を戻すには、[初期設定へのリセット（Factory Reset）] をクリックします。

スイッチポート トレースの詳細表示

スイッチ ポート トレースの詳細を表示するには、次の手順を実行します。

ステップ 1 [設定（Configure）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）] ページを使用して、フル ライセンスを持つスイッチを追加します。

ステップ 2 [管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [ネットワークとデバイス（Network and Device）] > [スイッチポートトレース（SPT）（Switch Port Trace (SPT)）] > [自動 SPT（Auto SPT）] ページで自動スイッチポートトレースを有効にします。

ステップ 3 [管理（Administration）] > [ダッシュボード（Dashboards）] > [ジョブ ダッシュボード（Job Dashboard）] ページで、有線クライアント ステータス メジャー ポーリング バックグラウンド タスクを実行するようにスケジュール設定します。

ステップ 4 [不正 API の詳細（Rogue AP detail）] ページで、トレース スイッチ ポート アイコンをクリックします。新しいポップアップに、トレースされたスイッチ ポートの詳細が表示されます。詳細ステータスをクリックして、「起動済み/検出済み（started/Found）」などのトレース ステータスをチェックします。

（注） Prime Infrastructure にスイッチを追加しなくても、手動 SPT は機能します。しかし、[管理（Administration ）] > [設定（Settings ）] > [システム設定（System Settings）] > [ネットワークとデバイス（Network and Device）] > [スイッチポートトレース（SPT）（Switch Port Trace (SPT)）] > [手動 SPT（Manual SPT）] ページの SNMP クレデンシャルを正しく設定する必要があります。「プライベート」はデフォルトのクレデンシャルです。特に設定されていない場合、これが手動のスイッチポートトレース中に使用されます。

- [設定（Configuration）] > [ネットワーク（Network）] > [ネットワークおよびデバイス（Network and Device）] の順に選択することによってスイッチが Prime Infrastructure に追加された場合、そのスイッチに対して入力された SNMP クレデンシャルは、ここで入力されたあらゆるスイッチ SNMP クレデンシャルより優先され、スイッチ ポート トレーシングに使用されます。[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークおよびデバイス（Network and Device）] ページで、スイッチの SNMP クレデンシャルを変更できます。Prime Infrastructure は、SPT を使用してスイッチを追加するためのライセンスを必要とせず、スイッチに接続された有線クライアントを表示しません。[モニター（Monitor）] > [管理対象要素（Managed Elements）] > [ネットワーク デバイス（Network Devices）] > [デバイス グループ（Device Groups）] > [デバイス タイプ（Device Type）] > [スイッチとハブ（Switches and Hubs）] ページには、SPT を使用して追加されたスイッチの詳細は表示されません。
- Prime Infrastructure には、スイッチを追加するためのフルライセンスが必要です。[モニター（Monitor）] > [管理対象要素（Managed Elements）] > [ネットワーク デバイス（Network Devices）] > [デバイス グループ（Device Groups）] > [デバイス タイプ（Device Type）] > [スイッチとハブ（Switches and Hubs）] ページには、フル ライセンスを使用して追加されたスイッチの詳細が表示されます。Prime Infrastructure には、スイッチに接続された有線クライアントも表示されます。スイッチの場所は MSE を使用して追跡されます。

スイッチ ポート トレーシングの確立

ステップ 1 [ダッシュボード（Dashboard）] > [ワイヤレス（Wireless）] > [セキュリティ（Security）] の順に選択します。

ステップ 2 [Malicious Rogue APs]、[Unclassified Rogue APs]、[Friendly Rogue APs]、[Custom Rogue APs]、および [Adhoc Rogues] ダッシュレットで、過去 1 時間または過去 24 時間に識別された不正 AP の数、またはアクティブ

な不正 AP の合計数を表す数値リンクをクリックします。[アラーム（Alarms）] ウィンドウが開き、不正の疑いがある AP に対してアラームが示されます。

ステップ 3 スイッチ ポート トラッキングをセットアップする対象の不正 AP の隣にあるチェックボックスをオンにして、その不正 AP を選択します。

ステップ 4 該当するアラームを展開し、アラーム詳細の [スイッチ ポート トレーシング（Switch Port Tracing）] サブセクションにある [スイッチ ポートのトレース（Trace Switch Port）] ボタンを手動で選択します。

検索可能な MAC アドレスを 1 つ以上使用できる場合、Prime Infrastructure では CDP を使用して、検出中のアクセス ポイントから最大 2 ホップ離れて接続されているすべてのスイッチを検出します。各 CDP が検出したスイッチの MIB は、対象の MAC アドレスのいずれかが含まれているかどうかを確認するために検証されます。いずれかの MAC アドレスが見つかった場合、該当するポート番号が返され、不正スイッチ ポートとして報告されます。

[スイッチ ポート トレースの詳細（Switch Port Tracing Details）] ダイアログボックスに関する追加情報については、スイッチ ポート トレースの詳細 （10 ページ）を参照してください。

不正 AP トレース用の SNMP クレデンシャルの設定

[SNMP クレデンシャル（SNMP Credentials）] ページでは、不正アクセス ポイントのトレースに使用するクレデンシャルを指定できます。番号ベースのエントリを使用しても特定のエントリを確認できない場合は、このオプションを使用します。スイッチ クレデンシャルが Cisco Prime Infrastructure に追加されていない場合は、このページの SNMP クレデンシャルを使用してスイッチに接続できます。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** の順に選択し、**[ネットワークとデバイス（Network and Device）] > [スイッチ ポート トレース（SPT）（Switch Port Trace (SPT)）] > [手動 SPT（Manual SPT）]** を選択します。[手動 SPT（Manual SPT）] ページが表示されます。

ステップ 2 現在の SNMP クレデンシャル エントリの詳細を表示または編集します。目的のエントリの [ネットワーク アドレス（Network Address）] リンクをクリックすることで操作できます。

この作業の詳細については、「関連項目」の「グローバル SNMP の設定」および「SNMP クレデンシャル詳細の表示」を参照してください。

デフォルト エントリは、ネットワーク 0.0.0.0 に対応します。これは、ネットワーク全体を意味します。SNMP クレデンシャルはネットワークごとに定義されるため、ネットワーク アドレスのみを指定できます。ネットワーク 0.0.0.0 に対して定義された SNMP クレデンシャルは、SNMP クレデンシャルのデフォルトです。これは、SNMP クレデンシャルが定義されていないときに使用されます。事前に設定された SNMP クレデンシャルを独自の SNMP 情報で更新する必要があります。

ステップ 3 新しい SNMP エントリを追加するには、[コマンドの選択（Select a command）] > [SNMP エントリの追加（Add SNMP Entries）] > [実行（Go）] の順に選択します（「SNMP クレデンシャルの追加」を参照）。

関連トピック

グローバル SNMP の設定

SNMP クレデンシャルの詳細表示
SNMP クレデンシャルの追加

スイッチ ポート トレースの詳細

[スイッチ ポート トレースの詳細（Switch Port Tracing Details）] ダイアログボックスでは、スイッチ ポートの有効化および無効化、スイッチ ポートのトレース、およびアクセス ポイント スイッチ トレースの詳細ステータスの表示を行うことができます。

スイッチ ポート トレーシングの詳細については、以下の関連項目を参照してください。

[スイッチ ポート トレースの詳細（Switch Port tracing Details）] ダイアログボックスで、次のいずれかを実行します。

- [スイッチ ポートの有効化/無効化（Enable/Disable Switch Port(s)）] をクリック：選択した任意のポートを有効または無効にします。
- [スイッチ ポートのトレース（Trace Switch Port(s)）] をクリック：別のスイッチ ポート トレースを実行します。
- [詳細ステータスの表示（Show Detail Status）] をクリック：このアクセス ポイントのスイッチ ポート トレースに関する詳細を表示します。
- [閉じる（Close）] をクリックします。

関連トピック

スイッチ ポート トレースを設定する （4 ページ）
不正 AP トレース用の SNMP クレデンシャルの設定 （9 ページ）

スイッチ ポート トレースのトラブルシューティング

スイッチポートトレース（SPT）は、ベストエフォート方式で動作します。SPT では、適切にトレースして不正 AP を組み込むために、以下の情報を必要とします。

- レポート アクセス ポイント：不正アクセス ポイントは 1 台以上の管理対象アクセス ポイントによってレポートされる必要があります。
- アクセス ポイント CDP ネイバー：シード スイッチを判別するには、アクセス ポイント Cisco Discovery Protocol（CDP）ネイバー情報が必要です。
- スイッチの IP アドレスと SNMP のクレデンシャル
  - トレースする必要のあるすべてのスイッチは管理IPアドレスを持つ必要があり、SNMP管理が有効にされている必要があります。
  - SNMPクレデンシャルが新しく変更される場合は、個々のスイッチをPrime Infrastructureに追加するのではなく、ネットワーク アドレスに基づき追加できます。
  - この新しい SNMP クレデンシャル機能は、read と write の両方についてデフォルトのコミュニティ ストリングを「private」とするデフォルトエントリ 0.0.0.0 を持ちます。
  - スイッチ ポートを有効または無効にするには、正しい write コミュニティ ストリングを指定する必要があります。トレーシングの場合には、read コミュニティ ストリングのみで十分です。

- スイッチ ポートの設定
  - トランキングされているスイッチ ポートは、トランク ポートとして正しく設定されている必要があります。
  - スイッチのポート セキュリティを無効にする必要があります。
- スイッチ ポート トレーシングは、Cisco イーサネット スイッチおよび Catalyst スイッチ 2960、3560、3560-E、3650、3750-E、3750-X、3850、4500 および 6500 シリーズのみでサポートされます。
- スイッチ VLAN 設定が適切に構成されている必要があります。
- すべてのスイッチについて CDP プロトコルが有効にされている必要があります。
- 不正アクセス ポイントとシスコ製スイッチの間にイーサネット接続が存在している必要があります。
- 不正アクセス ポイントとイーサネット スイッチの間に何らかのトラフィックが存在する必要があります。
- 不正アクセス ポイントは、最大ホップ カウントの制限内で、スイッチに接続される必要があります。デフォルト ホップは 2 です。最大ホップは 10 です。
- SNMPv3 を使用する場合は、メイン グループのための 1 個（VLAN ベースでない MIB 用に必要）の他に、コンテキスト オプションを使用して、VLAN ごとに 1 個作成してください。

不正およびスイッチ ポート トレーシングに関して頻繁に寄せられる質問

下記の「関連項目」では、Prime Infrastructure の不正 AP 検出およびスイッチ ポート トレーシング（SPT）に関するさまざまな質問の答えを提供しています。

関連トピック

自動 SPT の設定方法を教えてください

自動 SPT を設定するには、次の手順を実行します。

ステップ 1 [Configuration] > [Network] > [Network and Device] > [Network] を使用して、[License Level] が [Full] のスイッチを追加します。

ステップ 2 [Administration] > [Settings]> [System Settings] > [Network and Device] > [Switch Port Trace (SPT)] > [Auto SPT] の順に選択し、[Enable Auto Switch Port Tracing] を選択します。[OK] をクリックします。

ステップ 3 [Administration] > [Settings] > [Background Tasks] > [Wired Client Status] の順に選択します。このタスクが有効化され、1 日に 2 回以上実行するようにスケジュール設定されていることを確認してください。

関連トピック

SPT の結果（手動および自動）はどこで確認できますか （13 ページ）
自動 SPT を円滑に実行するにはどうすればよいですか。
不正およびスイッチ ポート トレーシングに関して頻繁に寄せられる質問 （11 ページ）

自動 SPT と手動 SPT はどのように違いますか

手動 SPT は、個別の不正 AP アラームに対して実行されます。不正 AP アラームの詳細ページで [Trace Switch Port] アイコンをクリックすることにより、この機能をトリガーする必要があります。

自動 SPT は、アラームのバッチに基づき、有線クライアント ステータス バックグラウンド タスクに対して定義されたスケジュールで自動的に実行されます。

手動 SPT のトリガーは、アクセス ポイントで有効化された CDP および適切な SNMP コミュニティ文字列を持つスイッチに依存する点に注意してください。手動 SPT およびその動作の詳細については、「関連項目」の「WCS Switch Port Trace Demonstration」リンクを参照してください。

自動および手動の SPT では、ライセンスおよびスイッチの「ライセンス レベル」の取り扱い方法にも違いがあります。スイッチの「ライセンス レベル」は、スイッチを追加する際に [Full] または [Switch Port Trace Only] のいずれかに設定できます。相違点を次の 3 つのケースで例示します。

- **「フル」ライセンス レベルのスイッチを追加する場合**：Prime Infrastructure は、追加されたフル ライセンス レベルのスイッチごとにライセンスを消費します。スイッチに接続されたすべての有線クライアントは、[モニター（Monitor）] > [管理対象デバイス（Managed Elements）] > [ネットワーク デバイス（Network Devices）] > [デバイス タイプ（Device Type）] > [スイッチおよびハブ（Switches and Hubs）] の順に選択することで表示できます。また、MSE を使用してスイッチの場所を追跡することもできます。「フル」ライセンス レベルは、自動 STP の動作に必須です。
- **スイッチを追加しない場合**：スイッチを追加しなくても、手動 SPT は動作します。ただし、すべてのスイッチに対して SNMP クレデンシャルを適切に設定する必要があることに注意してください。設定には、[Administration] > [Settings]> [System Settings] > [Network and Device] > [Switch Port Trace (SPT)] > [Manual SPT] を使用します。
- **「Switch Port Trace Only」ライセンス レベルのスイッチを追加する場合**：[Configuration] > [Network]> [Network Devices] > [Add Device] を使用してスイッチを Prime Infrastructure に追加し、[Switch Port Trace Only] ライセンス レベルを選択する場合、スイッチを追加する

ときに入力した SNMP クレデンシャルは、[Administration] > [Settings]> [System Settings] > [Network and Device] > [Switch Port Trace (SPT)] > [Manual SPT] を使用して入力された SNMP クレデンシャルより優先されます。入力した SNMP クレデンシャルは、スイッチ ポート トレーシングに使用されます。これが、スイッチを追加しない場合と、「スイッチ ポート トレース専用」のライセンス レベルのスイッチを追加する場合との主な違いです。Prime Infrastructure は、SPT 専用ライセンス レベルのスイッチに対してライセンスを消費せず、[モニター（Monitor）] > [管理対象要素（Managed Elements）] > [ネットワーク デバイス（Network Devices）] > [デバイス タイプ（Device Type）] > [スイッチとハブ（Switches and Hubs）] にこれらのスイッチは表示しません。また、これらのスイッチに接続された有線クライアントも表示しません。

詳細については、「WCS Switch Port Trace Demonstration」を参照してください。

関連トピック

「メジャー ポーリング」と「マイナー ポーリング」の違いについて教えてください （16 ページ）
不正およびスイッチ ポート トレーシングに関して頻繁に寄せられる質問 （11 ページ）

SPT の結果（手動および自動）はどこで確認できますか

ステップ 1 必要な不正 AP アラームの詳細を表示します。次に例を示します。

a) 任意の Prime Infrastructure ページの上部にある [Alarm Summary] アイコンをクリックします。アラーム カテゴリの一覧が表示されます。

b) リスト内の [不正 AP（Rogue AP）] リンクをクリックします。Prime Infrastructure が不正 AP アラームの一覧を表示します。

c) 詳細を表示する不正 AP アラームを展開します。そのアラームに関する詳細ページが表示されます。

ステップ 2 [Switch Port Tracing] ペインで、[Trace Switch Port] アイコンをクリックします。[Switch Port Trace] ウィンドウにトレースされたスイッチ ポートの詳細が表示されます。

SPT が実行されていない場合は、[Trace Switch Port(s)] をクリックしてトレースを開始します。[詳細ステータスの表示（Show Detail Status）] ボタンをクリックすると、進行中のトレースのステータスの詳細を取得できます。

関連トピック

不正およびスイッチ ポート トレーシングに関して頻繁に寄せられる質問 （11 ページ）

自動 SPT の方が有線の不正の検出に時間がかかるのはなぜですか

自動 SPT の方が手動 SPT より有線の不正の検出に比較的時間がかかる理由は、以下のとおりです。

1. 自動 SPTは、有線クライアント検出プロセスに依存しており、このプロセスは有線クライアント ステータス メジャー ポーリング バックグラウンド タスクが実行されているときだけに起動されます。デフォルトでは、このバックグラウンド タスクのメジャー ポーリン

グは、2 つのマイナー ポーリングごと、または 4 時間ごとのみに実行されるようにスケジュール設定されています。

2. 有線の不正 AP はスイッチに接続されますが、有線の不正 AP の状態が「関連付け状態」の場合、Prime Infrastructure は有線ポートのみを検出します。Prime Infrastructure は、有線クライアントのステータスが関連付け状態か関連付け解除状態かを常に確認しています。有線クライアントのステータスが関連付け解除状態の場合、Prime Infrastructure はこれをポート未接続として表示します。
3. 不正トレーシングはバッチで実行されます。特定の有線の不正検出に要する時間は、Prime Infrastructure が処理するバッチによって異なります。特定の不正が前回のバッチで処理されていた場合、そのトレースにはさらに時間がかかります。
4. 任意の有線の不正検出に要する時間は、Prime Infrastructure に存在する不正アラームの数と、有線クライアント ステータス メジャー ポーリングの間隔よって異なります。

関連トピック

「メジャー ポーリング」と「マイナー ポーリング」の違いについて教えてください （16 ページ）
不正およびスイッチ ポート トレーシングに関して頻繁に寄せられる質問 （11 ページ）

トランク ポート上の有線の不正を検出するにはどうすればいいですか

トランク ポート上の有線の不正は、次の手順で検出できます。

ただし、Cisco 2950 スイッチのトランク ポート上の不正を検出する場合は、先に Prime Infrastructure Device Pack 5.0 に含まれるアップデート版の 2950 サポートをインストールする必要があります。

ステップ 1 [管理（Administration）] > [設定（Settings）]> [システム設定（System Settings）] > [ネットワークおよびデバイス（Network and Device）] > [スイッチ ポート トレース（SPT）（Switch Port Trace (SPT)）] > [SPT 設定（SPT Configuration）] の順に選択します。

ステップ 2 [Exclude switch trunk ports] チェック ボックスをオフにして、[Save] をクリックします。

ステップ 3 [Administration] > [Settings] > [System Settings] > [Client and User] > [Client] の順に選択します。

ステップ 4 [Discover wired clients on trunk ports] チェック ボックスをオンにして、[Save] をクリックします。

スイッチは、有線クライアント ステータス バックグラウンド タスクによるメジャー ポーリングの次回実行時から、トランク ポート上の有線クライアントの検出を開始します。

関連トピック

自動 SPT の設定方法を教えてください （11 ページ）
「メジャー ポーリング」と「マイナー ポーリング」の違いについて教えてください （16 ページ）
不正およびスイッチ ポート トレーシングに関して頻繁に寄せられる質問 （11 ページ）

どのようにスイッチ ポートの場所を設定しますか。

スイッチ ポートの場所を設定するには、次の手順を実行します。

ステップ 1 [設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）] > [スイッチとハブ（Switches and Hubs）] の順に選択します。

ステップ 2 デバイス名をクリックします。デフォルトでは、[設定（Configuration）] タブが開きます。

ステップ 3 右上隅の [スイッチ ポートの場所（Switch Port Location）] をクリックします。

ステップ 4 場所を設定するポートを 1 つ以上選択し、ドロップダウン リストから [場所の設定（Configure Location）] を選択して [実行（Go）] をクリックします。

ステップ 5 [マップ ロケーション（Map Location）] グループで、次のように設定します。

- [キャンパス/サイト（Campus/Site）] ドロップダウン リストから、スイッチまたはスイッチ ポートのキャンパス マップを選択します。
- [建物（Building）] ドロップダウン リストから、スイッチまたはスイッチ ポートの建物マップ ロケーションを選択します。
- [フロア（Floor）] ドロップダウン リストから、フロア マップを選択します。
- [キャンパス/サイト（Campus/Site）]、[建物（Building）]、[フロア（Floor）] の詳細が設定されたファイルをすでに保存している場合は、[シビックのインポート（Import Civic）] をクリックします。これにより、Prime Infrastructure を使用して MSE のシビック情報がインポートされます。テキスト ファイル名を入力するか、ファイル名を参照して、[インポート（Import）] をクリックします。

ステップ 6 [ELIN とシビック ロケーション（ELIN and Civic Location）] グループ ボックスで、次のように設定できます。

- [ELIN] テキスト ボックスに緊急ロケーション ID 番号（ELIN）を入力します。ELIN は、自動ロケーション情報（ALI）データベースとも呼ばれるマスター データベースで発信者の地理的な位置を調べるために、公安応答局（PSAP）で使用される番号です。また、ELIN により、PSAP は、電話の接続が切断された場合、緊急の発信者に直接連絡することもできます。
- [住所（Civic Address）] および [詳細（Advanced）] タブの必須フィールドを入力します。
- ファイル内に ELIN およびシビック ロケーション情報が保存されている場合、[スイッチ ロケーションのインポート（Import Switch Location）] をクリックするとインポートできます。

ステップ 7 [保存（Save）] をクリックします。

関連トピック

自動 SPT を円滑に実行するにはどうすればいいですか。
自動 SPT の設定方法を教えてください （11 ページ）
不正およびスイッチ ポート トレーシングに関して頻繁に寄せられる質問 （11 ページ）

自動 SPT の [ロケーション別の削除（Eliminate By Location）] 機能を使用するにはどうすればいいですか

[ロケーション別の削除（Eliminate By Location）] は、Prime Infrastructure が有線の不正を検出するために使用するアルゴリズムの 1 つです。このアルゴリズムでは、不正 AP の場所情報を使用して、関連付け状態のスイッチ ポートを検索します。このアルゴリズムは、検出 AP のフロア ID を使用した自動 SPT 処理中の誤検出削減に役立ち、有線の不正の追跡精度を向上させます。

「ロケーション別の削除（Eliminate by location）」を有効にすると、有線クライアント ステータス バックグラウンド タスクによって、管理スイッチのすべての有線クライアントが検出されます。次回の自動 SPT の実行時、「ロケーション別の削除（eliminate by location）」アルゴリズムに基づいてスイッチ ポートがフィルタリングされます。

「Eliminate by location」を有効にするには、次の手順を実行してください。

ステップ 1 Cisco Mobility Service Engine（MSE）を Prime Infrastructure と統合します。

ステップ 2 検出 AP が配置されたフロア定義領域と MSE が同期していることを確認します。MSE が不正を追跡できるはずです。

ステップ 3 すべてのスイッチを Prime Infrastructure に追加します。

ステップ 4 すべてのスイッチが PI に追加されており、管理対象状態にある場合は、使用するアルゴリズムのスイッチ ポートをすべて設定する必要があります。スイッチ ポートのすべてのスイッチが設定されていない場合、誤検出結果が生成されます。[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）] > [スイッチとハブ（Switches and Hubs）] から [デバイス名（Device Name）] をクリックし、右上隅で [スイッチ ポートの場所（Switch Port Location）] をクリックして設定できます。

ステップ 5 マップに検出アクセス ポイントをマッピングしてから、Cisco MSE が同期され、不正 AP がフロアで検出されることを確認します。

[ロケーション別の削除（Eliminate By Location）] アルゴリズムは、検出 AP のフロア ID を取得し、他のすべての ID を削除します。一部のスイッチ ポートが設定されていない場合、これらのポートの値はゼロに設定されて考慮されます。そのため、結果には誤検出が含まれる場合があり、正確なフロア ID と値がゼロのフロア ID が含まれます。

ステップ 6 必ずすべてのポートが正しいフロア領域に割り当てられるように、スイッチ ポートの場所を設定します。

関連トピック

どのようにスイッチ ポートの場所を設定しますか。（15 ページ）
自動 SPT の設定方法を教えてください（11 ページ）
不正およびスイッチ ポート トレーシングに関して頻繁に寄せられる質問（11 ページ）

「メジャー ポーリング」と「マイナー ポーリング」の違いについて教えてください

自動 SPT 定義をトリガーする有線クライアント ステータス バックグラウンド タスクは次のとおりです。

メジャー ポーリング：メジャー ポーリング中、Prime Infrastructure は、重要クライアント情報のすべてをデータベースと同期させることにより、すべての有線デバイス ポートでのクライアント検出をトリガーします。Prime Infrastructure 2.2 の場合、このポーリングの頻度は 1 日 2 回よりも少なくなっていました。現在は、完全に設定可能になっています。

マイナー ポーリング：マイナー ポーリング中、Prime Infrastructure は、最近アクティブになったデバイス インターフェイスおよびポート上のみのクライアント検出をトリガーします。Prime Infrastructure はインターフェイス稼働時間データを使用して、いずれかのクライアントによってポートやインターフェイスが追加または削除されたのがいつなのかを検出します。

関連トピック

自動 SPT と手動 SPT はどのように違いますか （12 ページ）
自動 SPT の方が有線の不正の検出に時間がかかるのはなぜですか （13 ページ）
不正およびスイッチ ポート トレーシングに関して頻繁に寄せられる質問 （11 ページ）

「メジャー ポーリング」と「マイナー ポーリング」の違いについて教えてください

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。