



ネットワーク アドミッションコントロール ソフトウェア コンフィギュレーション ガイド

このドキュメントでは、Catalyst シリーズ スイッチに Network Admission Control (NAC; ネットワーク アドミッションコントロール) を設定する方法について説明します。NAC は、企業がネットワーク内のセキュリティの脅威を特定して防止し、この脅威に適応できるようにサポートするシスコの自己防衛型ネットワーク構想の一部として機能します。ネットワークを活用する企業にとって、ワームとウイルスの脅威と影響が増大しているため、NAC は、ネットワークへのアクセスを許可する前に、エンドポイントまたはクライアントのアンチウイルスの状態のアセスメントを実施します。

NAC は、Cisco IOS Release 12.3 (8) T で稼動する Cisco IOS ルータにも実装されます。すべてのスイッチに実装される NAC は、ルータに実装される NAC との下位互換性がありません。スイッチは、デフォルト ACL (Access Control List) および Cisco Secure Access Control Server (ACS) の Downloadable ACL をサポートしていますが、Intercept ACL はサポートしません。

NAC には、NAC レイヤ 2 IEEE 802.1X 認証と検証 (NAC-L2-802.1x) と、NAC レイヤ 2 IP 検証 (NAC-L2-IP) の 2 つの方式があります。次の表に示すように、サポートされる方式はシャーシによって異なります。

表 1 NAC サポート マトリクス

NAC 方式	7600	6500	4500	3750 Metro	3750	3560	3550 (12.2S)	3550 (12.1S)	2970	2960	2955	2950 -LRE	2950	2940	Cisco Aironet
NAC レイヤ 2 IEEE 802.1X 認証と検証 (NAC-L2-802.1x)	X	X	X	—	X	X	X	X	X	X	X	—	X	X	X
NAC レイヤ 2 IP 検証 (NAC-L2-IP)	X	X	X	—	X	X	X	—	—	—	—	—	—	—	—



注

Cisco IOS Release 12.2 (18) SXF で稼動する Catalyst 6500 シリーズ スイッチは、エッジスイッチでの NAC レイヤ 2 IEEE 802.1X 認証と検証をサポートしていません。

NAC レイヤ 2 検証の 2 つの方式 (IEEE 802.1X および IP) は、ともにエッジスイッチで機能しますが、検証開始、メッセージ交換、およびポリシー実施方法が異なります。NAC をサポートするデバイスの完全なリストは、『Network Admission Control リリース ノート』を参照してください。



注

この文書に記載されている新しいコマンドおよび修正されたコマンドの完全なシンタックスと使用方法に関する情報については、この文書のコマンドのセクション (37 ページの「コマンド リファレンス)、または次の URL に掲載されている『Cisco IOS Security Command Reference, Release 12.3』を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/secur_r/



注

『Network Admission Control バージョン 2.0 リリース ノート』(英語) は、次の URL に掲載されています。

http://www.cisco.com/en/US/netsol/ns617/networking_solutions_release_notes_list.html

本書の内容

本書は、次の章で構成されています。

- NAC の設定 2 ページ
- コマンド リファレンス 37 ページ
- メッセージとリカバリ手順 81 ページ

NAC の設定

この章は、次のセクションで構成されています。

- NAC について 2 ページ
- NAC の設定 17 ページ
- EAPoUDP テーブルのクリア 36 ページ

NAC について

ウイルス感染は、深刻なネットワーク セキュリティの侵害を引き起こします。ウイルスの感染源は、安全性が低下した PC やサーバなどのエンドポイントです。アンチウイルス ソフトウェアがインストールされていない、またはディセーブルにされたデバイスは、最もセキュリティ リスクが高いと考えられます。アンチウイルス ソフトウェアがイネーブルにされているデバイスでも、ウイルス定義ファイルおよびスキャン エンジンが最新でないことがあります。アンチウイルス ベンダーでは、アンチウイルス ソフトウェアを容易にディセーブルにできないようにしていますが、ウイルス定義ファイルおよびスキャン エンジンが最新のものとリスクは存在します。

NAC は、ウイルスに感染したデバイスがネットワークに悪影響を与えることがないように、エンドポイント デバイスまたはクライアントを認証し、アクセス コントロール ポリシーに適合させます。NAC は、ネットワークへのアクセスを許可する前に、エンドポイント システムまたはクライアントのアンチウイルスの状態 (ポストチャ) をチェックします。NAC は、ポリシーに非適合のデバイスに対してはアクセスの拒否、検疫ネットワーク セグメントへの配置、またはコンピューティング リソースへの限定的なアクセスの提供を行い、これらの安全性の低いノードからネットワークへのウイルス感染を防止します。

このセクションでは、NAC の次の内容について説明します。

- NAC デバイスの役割 3 ページ
- ポストチャ 検証 4 ページ
- AAA ダウン ポリシー 5 ページ

- NAC レイヤ 2 IEEE 802.1X 認証と検証 6 ページ
- NAC レイヤ 2 IP 検証 9 ページ

NAC デバイスの役割

図 1 に示すように、NAC ではネットワーク内のデバイスが特定の役割を果たします。

- **エンドポイント デバイス/クライアント/ホスト** — 保護された LAN へのアクセスを要求し、企業の社内 IT セキュリティ ポリシーとの照合によってポスチャが検証されるホストです。デスクトップ PC、サーバ、ラップトップ、その他の非 IOS デバイス（プリンタまたはスキャナ）はホストとなります。これらのエンドポイント デバイスには、認証サーバとエンドポイント デバイス上のサードパーティ製ソフトウェアとのインターフェイスとして機能する Cisco Trust Agent (CTA) が設定されています。CTA が設定されたホストは、CTA ホストと呼ばれます。CTA が設定されていない Cisco IP Phone、非 IOS デバイス、PC/ラップトップは、Non-Responsive Host (NRH; 非応答ホスト) と呼ばれます。認証サーバは、CTA ホストと NRH 両方にポリシーを提供します。CTA には、インターフェイスとして機能するポスチャ エージェント ソフトウェアと、クライアント上のポスチャ状態の実際の情報を提供するポスチャ プラグイン DLL が含まれています。



注

Cisco IOS Release 12.3 (4)JA またはそれ以降で稼動する Cisco Aironet アクセス ポイントは、デフォルトで NAC レイヤ 2 IEEE 802.1X 認証と検証をサポートしています。アクセス ポイントへの設定は不要です。アクセス ポイントは、クライアントとスイッチ間の NAC 通信の中継のみを行います。

CTA ソフトウェアは、ポスチャ エージェント、またはアンチウイルス クライアントとも呼ばれます。

- **Network Access Device (NAD; ネットワーク アクセス デバイス)** — NAC を実施するデバイスです。NAD として機能するのは、エンドポイント デバイスが接続するネットワーク エッジのレイヤ 2 またはレイヤ 3 デバイスです。NAD は、ポスチャ検証プロセスを開始するとエンドポイント デバイスと認証サーバをブリッジし、User Datagram Protocol を使用して Extensible Authentication Protocol (EAP) メッセージを中継します。NAC は、EAP over UDP (EAPoUDP) と呼ばれるこのプロトコルを使用します。
 - アクセス ポイントと Catalyst 2970、2960、2955、2950 および 2940 シリーズ スイッチの場合、EAP メッセージの情報のカプセル化は IEEE 802.1X ポートベース認証をベースに行います。認証に IEEE 802.1X を使用する場合、スイッチは EAP over LAN (EAPOL) フレームを使用します。
 - Catalyst 2970、2960、2955、2950 および 2940 以外のスイッチの場合、EAP メッセージの情報のカプセル化は IEEE 802.1X ポートベース認証または UDP をベースに行うことができます。認証に IEEE 802.1X を使用する場合、スイッチは EAP over LAN (EAPOL) フレームを使用し、UDP を使用する場合は EAPoUDP フレーム (EoU フレーム) を使用します。



注

中継として機能できるデバイスには、Catalyst 6500、4500、3750、3560、3550、2960、2970、2955、2950 および 2940 スイッチ、Catalyst 7600 シリーズ ルータ、Cisco Gigabit Ethernet Switching Module (CGESM) スイッチが含まれます。これらのデバイス上では、RADIUS クライアントおよび IEEE 802.1X をサポートするソフトウェアが稼動している必要があります。

- **Authentication Server (AS; 認証サーバ)** — エンドポイント デバイスのポスチャ クレデンシャルを最初に検証し、各エンドポイント デバイスに適用する Network Access Profile (NAP; ネットワーク アクセス プロファイル) を NAD にダウンロードする Posture Validation Server (PVS; ポスチャ検証サーバ) のインスタンスです。NAP には、Endpoint Device (EPD; エンドポイント デバイス) セッションに適用する必要があるアクセス ポリシーが含まれています。NAP は、企業の社内 IT セキュリティ ポリシーと照合して EPD のポスチャ クレデンシャル ステートが検証された後に作成されます。NAD は EPD と AS との間に EoU セッションを開始した後、2 つのデバイス間の透過的なブリッジとしてのみ機能します。

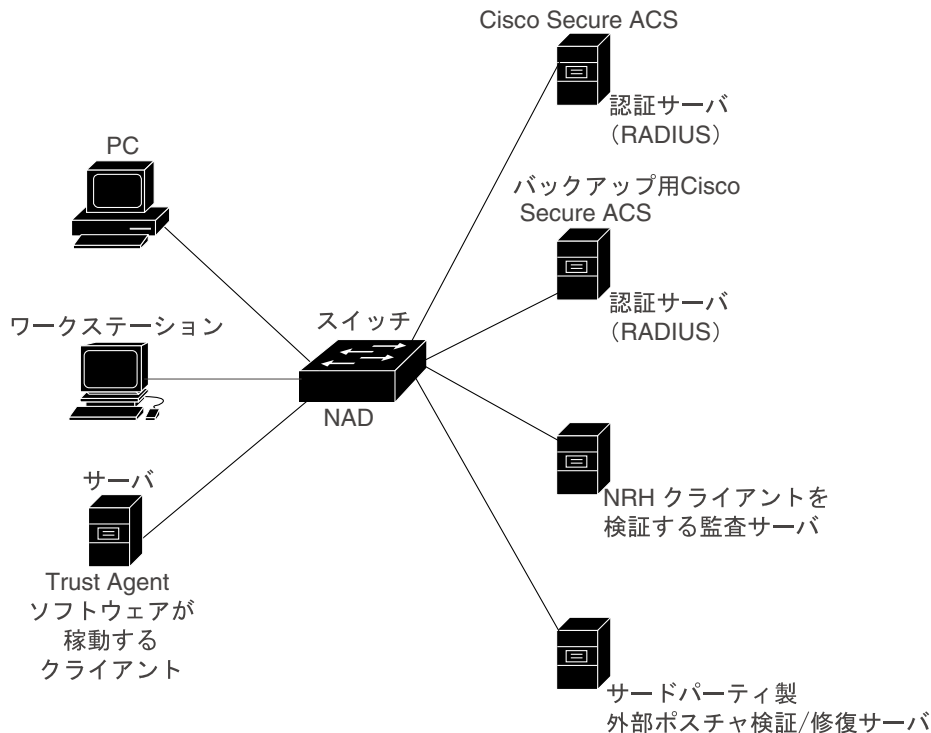
AS は、サードパーティ製の修復サーバ、または NRH クライアントを検証する監査サーバとしても機能できます。



注

Cisco Secure ACS 4.0 またはそれ以降は、NAC の RADIUS/TACACS (AS) インスタンスです。NAC リリース 2.0 では、Catalyst スイッチは Cisco Secure ACS Version 4.0 またはそれ以降、RADIUS、Authentication, Authorization, and Accounting (AAA; 認証、許可、アカウントिंग)、および EAP 拡張をサポートします。

図 1 NAD デバイスの役割



144614

ポスチャ検証 (Posture Validation)

NAC では、ホスト上のソフトウェアのステートに基づいて、NAD がホストのネットワークへのアクセスを許可または拒否します。このプロセスをポスチャ検証と呼びます。

ポスチャ検証では、クライアントのアンチウイルスの状態またはクレデンシャルを確認し、ネットワーク クライアントから送信されたセキュリティ ポスチャ クレデンシャルの検証を行い、システム ポスチャに基づいて適切なネットワーク アクセス ポリシーが NAD に送信されます。

Catalyst スイッチは、スイッチ ポート上で次の手順でポスチャ検証を実行します (図 1 を参照)。

1. エンドポイントまたはクライアントが、エッジスイッチなどの Cisco NAD を介してネットワークへの接続を試みると、スイッチはアンチウイルスの状態 (ウイルス定義ファイル、アンチウイルス ソフトウェア とスキャンエンジンのバージョンなど) についてエンドポイントにチャレンジ要求を行います。
2. CTA ソフトウェアで稼動するエンドポイント システムは、アンチウイルス情報 (使用するアンチウイルス ソフトウェアのタイプなど) を収集し、スイッチにこの情報を送信します。

エンドポイントで CTA ソフトウェアが稼動していない場合、スイッチはこのエンドポイントをクライアントレス デバイスとして分類し、非応答ホストまたは NAC エージェントレス ホストとみなします。

非応答ホストの詳しい情報については、6 ページの「非応答ホスト」を参照してください。クライアントレス エンドポイント システムと非応答ホストの詳しい情報については、10 ページの「ポストチャ検証とレイヤ 2 IP 検証」を参照してください。

『CTA アドミニストレータ ガイド 2.0』は、次の URL に掲載されています。

http://www.cisco.com/jp/service/manual_j/sec/ta/taag1/

『Cisco Trust Agent 2.0 リリース ノート』は、次の URL に掲載されています。

<http://www.cisco.com/jp/product/hs/security/cta/prodlit/pdf/TrustAgentReleaseNote.pdf>

Web で公開されている CTA ドキュメンテーションのリストは、次の URL に掲載されています。

<http://www.cisco.com/jp/product/hs/security/cta/>

3. スイッチは、NAC ポリシーを決定する Cisco Secure ACS にこの情報を送信します。

Cisco Secure ACS は、エンドポイントのアンチウイルスの状態を検証して NAC ポリシーを決定し、このポリシーをスイッチに返します。スイッチは、エンドポイントに対してこのアクセス ポリシーを適用します。

検証が成功すると、Cisco Secure ACS はアクセス制限に基づいてクライアントのネットワーク アクセスを許可します。

検証が失敗すると、ポリシーに非適合のデバイスは、アクセスが拒否されるか、検疫ネットワーク セグメントに配置されるか、コンピュータ リソースへの限定的なアクセスが与えられます。検証が失敗するのは、クライアントがワームまたはウイルスに感染している場合、ホスト上でポリシーに適合するソフトウェアが稼動していない場合、またはホストが古いバージョンのアンチウイルス ソフトウェアを使用している場合です。

Cisco Secure ACS for the Windows の情報については、次の URL を参照してください。

<http://www.cisco.com/jp/product/hs/security/acs/acsw/>

Cisco Secure ACS Solution Engine の情報については、次の URL を参照してください。

<http://www.cisco.com/jp/product/hs/security/acs/acsse/>

AAA ダウン ポリシー

NAC の一般的な実装では、Cisco Secure ACS を使用してクライアントのポストチャを検証し、ポリシーを NAD に渡します。管理者は、デフォルトの AAA ダウン ポリシーを設定することにより、ポストチャ検証時に AAA サーバが使用できない場合にユーザを拒否（ネットワークへのアクセスを与えない）せずに、ホストにこのポリシーを適用することができます。

この機能には次のようなメリットがあります。

- AAA サーバが使用できない場合、ホストは制限付きでもネットワークに接続できる
- AAA サーバが使用可能になると、ホストの検証を実施し、ホストのポリシーを ACS からダウンロードできる



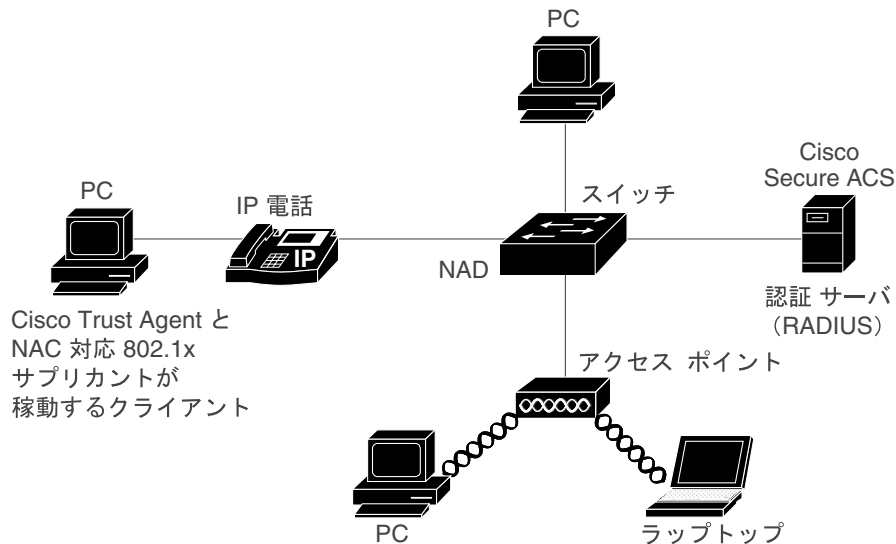
注

AAA サーバがダウンしている場合に AAA ダウン ポリシーが適用されるのは、ホストに既存のポリシーが適用されていないときのみです。通常は、再検証中に AAA サーバがダウンすると、ホストに適用されていたポリシーがそのまま使用されます。

NAC レイヤ 2 IEEE 802.1X 認証と検証

NAC レイヤ 2 IEEE 802.1X 認証と検証は、デバイス（エンドポイント システムまたはクライアント）が接続するエッジ スイッチのアクセス ポートで実施できます。この場合のデバイスは、スイッチ アクセス ポートに直接接続する PC、ワークステーション、Cisco Aironet アクセス ポイント、またはサーバです。

図 2 NAC レイヤ 2 IEEE 802.1X を使用するネットワーク



ポスチャ検証は、クライアントまたはスイッチが開始できます。スイッチは、エンドポイントと Cisco Secure ACS 間の EAPOL メッセージを中継します。Cisco Secure ACS がアクセス制御の決定を送信すると、スイッチはアクセス制限を実施し、認証ポートにポスチャ非適合のクライアントのセグメント化と検疫を行う特定の VLAN を割り当てるか、ネットワーク アクセスを拒否します。

このセクションは、次のトピックで構成されます。

- 非応答ホスト 6 ページ
- 定期的なポスチャ再検証 7 ページ
- スイッチのアクション 7 ページ
- NAC レイヤ 2 IEEE 802.1X の AAA ダウン ポリシー（「Inaccessible Authentication Bypass」） 8 ページ

非応答ホスト (Nonresponsive Hosts)

非応答ホストとは、NAC をサポートしない従来の IEEE 802.1x 対応 サブリカントが稼動するデバイスか、IEEE 802.1x 対応 サブリカントがインストールされていないデバイスです。ポスチャ検証要求に応答しないホストまたはクライアントは、次のいずれかの方法で検証することができます。

- 802.1x ゲスト VLAN (IEEE 802.1x 対応 サブリカントがインストールされていないデバイス)
- 802.1x アイデンティティ + 未知のポスチャ

従来の IEEE 802.1x 対応クライアントソフトウェアが稼動するホストがスイッチに接続すると、スイッチは Cisco Secure ACS とのセッションを開始し、この認証サーバにホスト情報を送信します。認証サーバは、ホストの既知のアイデンティティと未知のポスチャに基づいたアクセス ポリシーを返します。この場合のポリシーは、VLAN 割り当て、またはネットワーク アクセス拒否です。スイッチは、このポリシーをホストに適用します。

また認証サーバは、ホストがポスチャ情報を提供しなかったためにポスチャの Attribute-Value (AV; アトリビュート値) ペアが *Unknown* に設定されたことを示す情報をスイッチに送信します。この情報は、スイッチがホストにアクセス ポリシーを適用する方法に影響を与えません。

定期的なポスチャ再検証

ポスチャの変更は、クライアントまたは Cisco Secure ACS の変更によって発生します。

- ホストに変更があると (例: オペレーティング システムのパッチの適用、アンチウイルス ソフトウェアの更新)、ホストの CTA はこの変更を検知し、EAPOL-Start メッセージをスイッチに送信して再検証を開始します。
- 認証サーバに変更があると (例: 新しいアンチウイルス .DAT ファイルが使用可能になる)、定期的な再認証タイマーが失効したときにスイッチがポスチャ再検証を開始します。

スイッチに応答ホストの定期的なポスチャ再検証を実行させるには、IEEE 802.1x クライアントの定期的な再認証をイネーブルにし、その間隔を指定します。CTA ではなく、従来のサブリカントが稼動しているデバイスには、非応答ホストの定期的なポスチャ再検証を設定できます。



注

IEEE 802.1x 対応 サブリカントが稼動していないデバイスの場合は、非応答ホストの定期的なポスチャ再検証は設定できません。

NAC レイヤ 2 IEEE 802.1x の場合、再認証の試行間隔 (秒) を指定するには、手動で秒数を指定するか、Cisco Secure ACS から送信される Access-Accept メッセージの Session-Timeout RADIUS アトリビュートの値をスイッチが使用するように設定します。

スイッチは、ポスチャ検証の際に Termination-Action RADIUS アトリビュートも使用します。このアトリビュート値に応じて、スイッチは自動的にクライアントを再検証するか、EAPOL ベースのセッションを終了してからクライアントの再検証を行います。

スイッチのアクション

スイッチは、定期的な再認証のステート、再検証時間の値、Session-Timeout RADIUS アトリビュート値に応じて、表 2 に示すいずれかのアクションを実行します。

- 秒数を手動で設定している場合、スイッチはタイマーが失効したときにホストを再検証します。
- Access-Accept メッセージに Session-Timeout AV ペアが含まれていない場合、スイッチはホストを再認証しません。
- Access-Accept メッセージに Session-Timeout AV ペアが含まれている場合、スイッチは Cisco Secure ACS の再認証時間を使用します。



注

Access-Accept メッセージは Accept フレームとも呼ばれます。

- スイッチは、RADIUS アトリビュートの Termination-Action の値に応じてホストの再認証を行います。
 - Termination-Action AV ペアが存在し、値が RADIUS-Request の場合、スイッチはホストを再認証しません。
 - Termination-Action AV ペアが存在しない、または値が Default の場合、スイッチは Cisco Secure ACS とのセッションを終了し、ホストは許可されません。

表 2 定期的な再検証

定期的な再検証	再検証時間	Session-Timeout アトリビュート	Termination-Action 値	スイッチのアクション
ディセーブル	NA	NA	NA	再認証は発生しない
イネーブル	手動で秒数を設定	NA	NA	スイッチは手動で設定された秒数を使用して再認証を実施
イネーブル	自動的に Cisco Secure ACS の再認証時間を使用	Access-Accept メッセージに含まれない	NA	再認証は発生しない
イネーブル	自動的に Cisco Secure ACS の再認証時間を使用	Access-Accept メッセージに含まれる	Default または値なし	サーバの再認証時間が経過するとセッションを終了
イネーブル	自動的に Cisco Secure ACS の再認証時間を使用	Access-Accept メッセージに含まれる	RADIUS-Request	サーバの再認証時間を使用して再認証を実施

NAC レイヤ 2 IEEE 802.1X の AAA ダウン ポリシー (「Inaccessible Authentication Bypass」)



注

この機能は、Catalyst 3560 および Catalyst 3750 シリーズ スイッチでのみ使用可能です。(最新の状況は各スイッチのマニュアルを参照ください)

Inaccessible Authentication Bypass を使用するには、ポートをクリティカル ポートに指定する必要があります。クリティカル ポートの処理プロセスは次のとおりです。

1. 新しい IEEE 802.1X 認証セッションが検出されます。
2. 認証が開始され、AAA サーバが使用不能であることが分かると、クリティカル認証ポリシーが適用され、ポートは Critical-Auth ステータスに移行されます。ポリシーの適用は、VLAN 割り当ての形で行われます。
3. AAA サーバが再び使用可能になると、このホストに対する再認証が再度開始されます。

**注**

AAA サーバがダウンした場合、AAA ダウン ポリシーが適用されるのは、既存のポリシーがホストに適用されていない場合のみです。したがって、認証が以前に成功してポートに VLAN が割り当てられている場合、ホストにはそのままこの VLAN が適用されます。ポートが Critical-Auth ステートに移行される前にアクセスが許可されていない場合は、ポートに設定済みのアクセス VLAN が割り当てられます。

Catalyst 3750 および 3560 シリーズ スイッチの Inaccessible Authentication Bypass 機能の詳細な情報については、次の URL を参照してください。

http://www.cisco.com/jp/service/manual_j/sw/cat37/3750ssc_s/chapter10/16180_06_10.shtml

http://www.cisco.com/jp/service/manual_j/sw/cat37/3750scg/index.shtml

NAC レイヤ 2 IP 検証

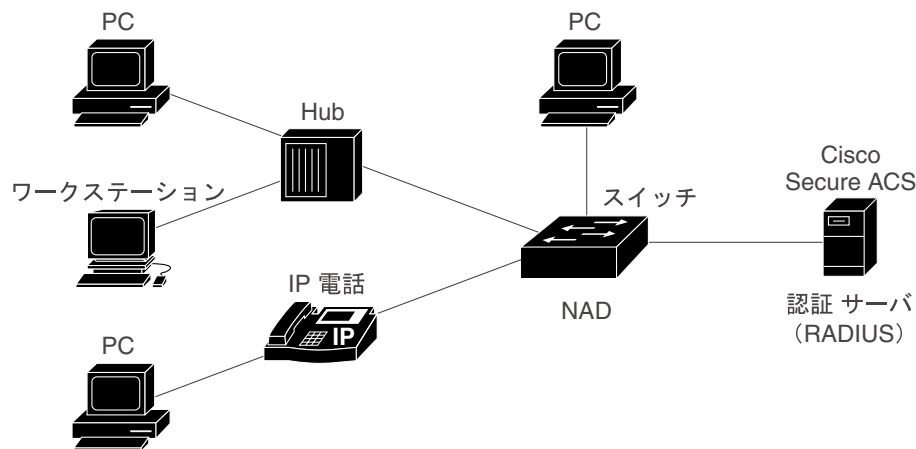
NAC レイヤ 2 IP 認証は、デバイス (エンドポイント システムまたはクライアント) が接続するエッジ スイッチのアクセス ポートで実施できます。この場合のデバイスは、図 3 に示すように、直接接続でスイッチ アクセス ポートに接続する PC、ワークステーション、サーバや、IP 電話、ハブ、アクセス ポイントです。

**注**

Cisco Aironet アクセス ポイントは NAC レイヤ 2 検証をサポートしていません。

NAC レイヤ 2 IP をイネーブルにした場合、EAPoUDP は IPv4 トラフィックのみに対応します。スイッチは、エンドポイント デバイスまたはクライアントのアンチウイルスの状態を確認し、アクセス コントロール ポリシーを適用します。

図 3 NAC レイヤ 2 IP を使用するネットワーク



Cisco Trust Agent
ソフトウェアが稼動する
クライアント

92735

このセクションは、次のトピックで構成されます。

- ポスチャ検証と NAC レイヤ 2 IP 検証 10 ページ
- Cisco Secure ACS とアトリビュート値ペア 12 ページ

- 監査サーバ 13 ページ
- デフォルト ACL 14 ページ
- NAC タイマー 14 ページ
- NAC レイヤ 2 IP 検証とスイッチ スタック 16 ページ
- NAC レイヤ 2 IP 検証と冗長モジュラ スイッチ 17 ページ
- NAC レイヤ 2 IP 検証の AAA ダウン ポリシー 17 ページ

ポスチャ検証と NAC レイヤ 2 IP 検証

NAC レイヤ 2 IP 検証は、図 3 に示すように、同一のスイッチ ポート上で複数のホストのポスチャ検証をサポートします。

ホストが接続しているスイッチ ポート上で NAC レイヤ 2 IP 検証をイネーブルにすると、スイッチは DHCP スヌーピングまたは Address Resolution Protocol (ARP) スヌーピングを使用して接続しているホストを特定します。DHCP スヌーピングによって開始されたポスチャ検証は、ARP スヌーピングによって開始されたポスチャ検証より優先されます。スイッチは、ARP パケットの受信後、または DHCP スヌーピング バインディング エントリの作成の後にポスチャ検証を開始します。



注

ARP スヌーピングは、デフォルトの接続ホスト検出方式です。スイッチが DHCP スヌーピング バインディング エントリの存在に基づいてホストを検出できるようにするには、DHCP スヌーピングをイネーブルにする必要があります。

スイッチ ポートに割り当てられているアクセス VLAN 上でダイナミック ARP インспекションのみがイネーブルの場合、ポスチャ検証は ARP パケットがダイナミック ARP インспекションのチェックに適合したときに開始されます。ただし、DHCP スヌーピングとダイナミック ARP インспекションがともにイネーブルにされている場合、ポスチャ検証は DHCP スヌーピング バインディング エントリが作成されたときに開始されます。

悪質なホストは、偽造した ARP パケットを送信してポスチャ検証のバイパスを試みます。未検証ホストによるネットワーク アクセスを防止するために、スイッチ ポートでは IP ソース ガードをイネーブルにすることができます。



注

Catalyst 7600 シリーズ ルータおよび Catalyst 6500 シリーズ スイッチは、IP ソース ガードをサポートしていません。

ポスチャ検証が開始されると、スイッチは EAPoUDP セッション テーブルにエントリを作成してホストのポスチャ検証ステータスを追跡し、NAC ポリシーを決定するために次の決定階層を監視します。

1. ホストが例外リスト (11 ページ「例外リスト」を参照) に含まれている場合、スイッチはユーザ定義の NAC ポリシーをホストに適用します。
2. EoU バイパス (11 ページ「EoU バイパス」を参照) がイネーブルにされている場合、スイッチは Cisco Secure ACS に非応答ホスト要求を送信し、サーバから送信されたアクセス ポリシーをホストに適用します。スイッチは、この要求が非応答ホストに関連することを示すために、要求に RADIUS AV ペアを挿入します。
3. EoU バイパスがディセーブルにされている場合、スイッチはホストに hello パケットを送信し、ホストのアンチウイルス状態を要求します (11 ページ「EAPoUDP セッション」を参照)。要求を指定回数送信してもホストから応答を受信しない場合、スイッチはホストをクライアントレスに分類し、非応答ホストとみなします。スイッチは、Cisco Secure ACS に非応答ホスト要求を送信し、サーバから送信されたアクセス ポリシーをホストに適用します。

例外リスト (Exception Lists)

例外リストには、ローカルのプロファイルとポリシー設定が含まれています。このアイデンティティ プロファイルは、IP アドレス、MAC アドレス、または デバイス タイプに基づいてデバイスを静的に許可または検証するために使用します。アイデンティティ プロファイルは、アクセス制御アトリビュートを指定するローカル ポリシーと関連付けられます。

特定のホストがポストチャ検証をバイパスできるようにするには、例外リストにこれらのホストを指定し、ユーザ定義のポリシーを適用します。EAPoUDP セッション テーブルにエントリが追加されると、スイッチはこのホスト情報と例外リストを比較します。ホストが例外リストに含まれている場合、スイッチはホストに設定済みの NAC ポリシーを適用するとともに、EAPoUDP セッション テーブルのクライアントの検証ステータスを *POSTURE ESTAB* に更新します。

EoU バイパス (EoU Bypass)

スイッチは、EoU バイパス機能を使用して CTA が稼動していないホストのポストチャ検証を高速化できます。EoU バイパスをイネーブルにすると、スイッチはホストにコンタクトしてアンチウイルスの状態を要求する代わりに、ホストの IP アドレス、MAC アドレス、サービスタイプ、EAPoUDP セッション ID を含む要求を Cisco Secure ACS に送信します。Cisco Secure ACS は、アクセス制御の決定を下し、スイッチにポリシーを送信します。

EoU バイパスがイネーブルでホストが非応答ホストの場合は、スイッチは Cisco Secure ACS に非応答ホスト要求を送信し、サーバから送信されたアクセス ポリシーをホストに適用します。

EoU バイパスがイネーブルでホストが CTA を使用している場合も、スイッチは Cisco Secure ACS に非応答ホスト要求を送信し、サーバから送信されたアクセス ポリシーをホストに適用します。

EAPoUDP セッション

EoU はデフォルトでイネーブルにされています。EoU バイパスがディセーブルの場合、スイッチは EAPoUDP パケットを送信してポストチャ検証を開始します。ポストチャ検証中、スイッチはデフォルト アクセス ポリシーをホストに適用します。スイッチがホストに EAPoUDP メッセージを送信し、ホストがアンチウイルスの状態を返すと、スイッチはこの EAPoUDP 応答を Cisco Secure ACS に転送します。指定された回数要求を試みてもホストから応答を受信しない場合、スイッチはホストをクライアントレスに分類し、非応答ホストとみなします。ACS はクレデンシャル検証が完了すると、Access-Accept メッセージとともにポストチャ トークンとポリシーアトリビュートをスイッチに返します。スイッチは、EAPoUDP セッション テーブルを更新してアクセス制限を実施し、ポストチャが非適合のクライアントのセグメント化と検疫を行うか、ネットワーク アクセスを拒否します。

ポストチャ検証の結果に基づき、ポートには 2 つのタイプのポリシーを適用できます。

- ホスト ポリシー：ホスト ポリシーは、ポストチャ検証の結果決定されたアクセス制限を実施する ACL で構成されます。
- URL リダイレクト ポリシー：URL リダイレクト ポリシーは、すべての HTTP/HTTPS トラフィックを修復サーバにリダイレクトし、非適合ホストがポリシーに適合するために必要なアップグレードを実施するメカニズムを提供します。このポリシーは、次の要素で構成されます。
 - 修復サーバを参照する URL
 - 必要な HTTP リダイレクトを行うために、アドレスが修復サーバ以外のホストからのすべての HTTP/HTTPS パケットをキャプチャしてスイッチ ソフトウェアにリダイレクトするスイッチ上の ACL

ホスト ポリシーの ACL 名、リダイレクト URL、URL リダイレクト ACL は、RADIUS アトリビュート値オブジェクトを使用して転送されます。



注

クライアントの DHCP スヌーピング エントリが削除されると、スイッチは EAPoUDP セッション テーブルからクライアントのエントリを削除するため、クライアントの認証は行われません。

Cisco Secure ACS とアトリビュート値ペア

NAC レイヤ 2 IP 検証をイネーブルにすると、Cisco Secure ACS は RADIUS を使用して NAC AAA サービスを提供します。Cisco Secure ACS は、エンドポイント システムのアンチウイルス クレデンシャルに関する情報を入手し、エンドポイントのアンチウイルスの状態を検証します。

Cisco Secure ACS には、RADIUS の cisco-av-pair Vendor Specific Attribute (VSA; ベンダー固有アトリビュート) 使用して次の AV ペアを設定できます。

- CiscoSecure-Defined-ACL _ Cisco Secure ACS 上の Downloadable ACL 名を指定します。スイッチは、次のフォーマットの CiscoSecure-Defined-ACL AV ペアによって Downloadable ACL 名を取得します。

#ACL#-IP-name-number

name は ACL 名、*number* は、3f783768 などのバージョン番号です。

Auth-Proxy ポスチャ コードは、指定された Downloadable ACL の Access Control Entry (ACE) が以前にダウンロードされているかどうかをチェックします。ダウンロードされていない場合、Auth-Proxy ポスチャ コードは ACE をダウンロードするために AAA 要求とともにユーザ名として Downloadable ACL 名を送信します。これによりスイッチ上に名前付き ACL として Downloadable ACL が作成されます。この ACL には、ソース アドレス any の ACE が含まれ、最後に暗示的な deny ステートメントは含まれません。ポスチャ検証後にこの Downloadable ACL がインターフェイスに適用されると、ソース アドレスが any からホストのソース IP アドレスに変更されます。この ACE は、エンドポイント デバイスが接続しているスイッチ インターフェイスに適用されるデフォルト ACL の前に付加されます。トラフィックが CiscoSecure-Defined-ACL ACE に一致すると、適切な NAC アクションが実行されます。

次にインターフェイス ACL の例を示します。

```
access-list 115 permit udp any any eq bootps (for bootps requests)
access-list 115 permit ip any 20.0.0.0 0.0.0.255 (NAC Ingress source N/W)
access-list 115 permit ip any host 40.0.0.5 (Audit Server)
```

- url-redirect および url-redirect-acl ースイッチ上のローカル URL ポリシーを指定します。スイッチは、次の cisco-av-pair VSA を使用します。
 - url-redirect = <HTTP または HTTPS URL>
 - url-redirect-acl = スイッチ ACL 名または番号

これらの AV ペアにより、スイッチはエンドポイント デバイスからの HTTP および / または HTTPS 要求を代行受信し、最新のアンチウイルス ファイルをダウンロードできる指定のリダイレクト アドレスにクライアントの Web ブラウザを転送します。Cisco Secure ACS の url-redirect AV ペアには、Web ブラウザがリダイレクトされる URL が含まれます。



注

URL リダイレクトは、HTTP または HTTPS に対して実行できますが、同時に両方に対して実行することはできません。

url-redirect-acl AV ペアには、リダイレクトする HTTP および / または HTTPS トラフィックを指定する ACL の名前または番号が含まれます。スイッチには、この ACL を定義する必要があります。リダイレクト ACL の permit エントリに一致するトラフィックはリダイレクトされます。これらの AV ペアは、ホストのポスチャが健全でない場合に送信されることがあります。

次に url-re-direct-acl の例を示します。

```
ip access-list extended url-redirect-acl
permit tcp any <protected-server-vlan-network>
```

Cisco IOS ソフトウェアにサポートされている AV ペアの詳しい情報については、AAA クライアントが稼動するソフトウェア リリースのドキュメンテーションを参照してください。

ACS for the Windows Server の情報については、次の URL を参照してください。

<http://www.cisco.com/jp/product/hs/security/acs/acsw/>

ACS Solution Engine の情報については、次の URL を参照してください。

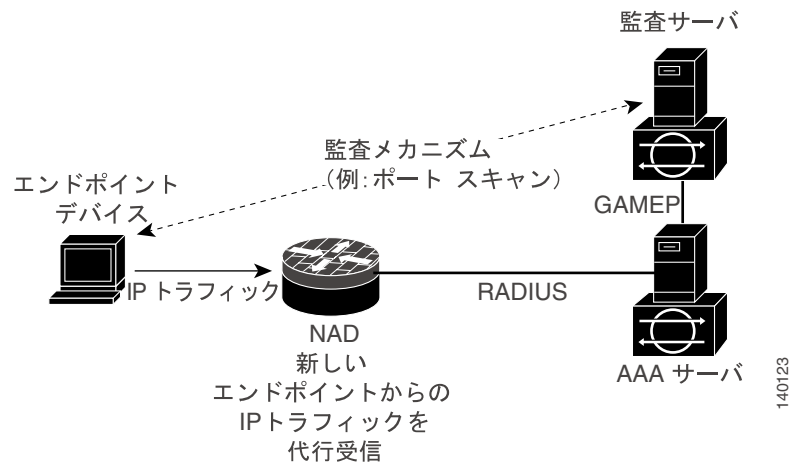
<http://www.cisco.com/jp/product/hs/security/acs/acsse/>

監査サーバ (Audit Servers)

CTA が稼動していないエンドポイント デバイスは、NAD によるチャレンジ要求に対してクレデンシャルを提供できません。このようなホストは、エージェントレスまたは非応答ホストと呼ばれます。

図 4 に、監査サーバを使用する一般的なトポロジを示します。

図 4 NAC デバイスの役割



NAC アーキテクチャは、エージェントレス ホストの包括的な検証の実施のために拡張され、ホストの CTA を使用せずにエージェントレス ホストのセキュリティ適合性、脆弱性、脅威のプロブとスキャンを実行できる監査サーバが組み込まれました。したがってアクセスサーバは、すべての非応答ホストに共通制限ポリシーを適用するのではなく、監査の結果に基づいてホスト別にネットワーク アクセス ポリシーを決定できます。NAC アーキテクチャにサードパーティ製の監査メカニズムを統合することにより、ホストの強力な監査/検証機能が実現します。

NAC アーキテクチャでは、監査サーバが稼動中で、ホストと通信できることが前提となります。ホストが、ポスチャ検証が設定された NAD を通じてネットワークにアクセスすると、NAD はホストに適用するアクセス ポリシーを AAA サーバ (Cisco Secure ACS) に要求します。AAA サーバは、外部検証サーバを使用してホストのスキャンを開始できます。監査スキャンは非同期で行われ、数秒で完了します。AAA サーバは、監査中にホストに適用する最小限のアクセス許可セキュリティ ポリシーと短い間隔のポーリング タイマー (Session-Timeout) を NAD に送信します。NAD は、監査サーバから結果を入手できるまで指定された間隔で AAA サーバにポーリングを行います。AAA サーバは、監査結果を受信するとその結果をもとにアクセス ポリシーを決定し、次の要求を受信したときにホストに適用するポリシーを NAD に送信します。

デフォルト ACL

**注**

デフォルト ACL では、NAC レイヤ 2 IP 検証が機能できるように EAPoUDP トラフィックを許可する必要があります。

スイッチ ポートに NAC レイヤ 2 IP 検証を設定する場合、デフォルト ポート ACL もスイッチ ポートに設定し、IP トラフィックに適用する必要があります。

スイッチは、デフォルト ACL が設定されている場合に Cisco Secure ACS からホスト用のアクセス ポリシーを受信すると、スイッチ ポートに接続しているホストからのトラフィックにこのポリシーを適用します。スイッチがホストごとに適用するポリシーを Cisco Secure ACS からダウンロードすると、受信トラフィックはこのポリシーと照合され、一致しないトラフィックはデフォルト ポリシーと照合されます。

Cisco Secure ACS がポリシー マップ アクションとしてリダイレクト URL を指定する Downloadable ACL をスイッチに送信した場合、この ACL はスイッチ ポートに設定済みのデフォルト ACL に優先して適用されます。Downloadable ACL は、常にデフォルト ACL よりも優先されます。デフォルト ポート ACL が設定されていない場合、Downloadable ACL をプログラムすることはできません。

NAC タイマー

スイッチは次の 3 つのタイマーをサポートしています。

- 保留タイマー (Hold Timer) 14 ページ
- アイドルタイマー (Idle Timer) 14 ページ
- 再送信タイマー (Retransmission Timer) 16 ページ
- 再検証タイマー (Revalidation Timer) 16 ページ
- ステータス クエリー タイマー (Status-Query Timer) 16 ページ

保留タイマー (Hold Timer)

保留タイマーは、EAPoUDP セッションの検証の試みが失敗した直後に新しい EAPoUDP セッションが開始されることを防止します。このタイマーは、Cisco Secure ACS がスイッチに Accept-Reject メッセージを送信したときのみ使用されます。

保留タイマーのデフォルト値は 180 秒 (3 分) です。

EAPoUDP セッションは、ホストのポストチャ検証の失敗、セッション タイマーの失効、スイッチ /Cisco Secure ACS が無効メッセージを受信したなどの理由で検証できないことがあります。スイッチまたは認証サーバが無効のメッセージを受信し続けているときは、悪意あるユーザが DoS (サービス不能) 攻撃を仕掛けている可能性があります。

アイドルタイマー (Idle Timer)

アイドルタイマーは、スイッチが、ポストチャ検証済みのホストからの ARP パケットの受信、または IP デバイス トラッキング テーブルのエントリの更新によってホストがまだ接続中であることを確認するまで待機する期間を制御します。アイドルタイマーは、既知のホストのリストを利用して、ポストチャ検証を開始したホストと IP デバイス トラッキング テーブルを追跡します。

アイドルタイマーは、スイッチが ARP パケットを受信したとき、または IP デバイス トラッキング テーブルが更新されたときにリセットされます。アイドルタイマーが失効すると、スイッチはホスト上の EAPoUDP セッションを終了するため、ホストの検証は行われなくなります。



注

IP デバイス トラッキング テーブルは、ネットワークに接続した新しいホストを追跡するために使用します。IP デバイス トラッキング テーブルは、IP ARP インスペクションと IP DHCP スヌーピング（オプション）を通じてホストを検出します。IP ARP インスペクションは、IP デバイス トラッキングをイネーブルにすると自動的にイネーブルにされます。

デフォルトのプロブ間隔は 30 秒です。タイムアウト時間は、実際のプロブ間隔にプロブ回数を乗じた値です。デフォルトのプロブ間隔は 30 秒でプロブ再試行数は 3 回なので、アイドル タイマーのデフォルト値は 90 秒です。

スイッチは、ポスチャ検証を開始したホストを追跡するために、既知のホストのリストを保持しています。スイッチは ARP パケットを受信すると、このリストの生存時間タイマーとアイドル タイマーをリセットします。リストの生存時間タイマーが失効すると、スイッチは ARP プロブを送信してホストがまだ存在しているかどうか確認します。存在している場合、ホストがスイッチに応答を送信し、スイッチは既知のホストのリストを更新します。次にスイッチは、リストの生存時間タイマーとアイドル タイマーをリセットします。スイッチは、ホストから応答を受信しないと Cisco Secure ACS とのセッションを終了するため、ホストの検証は行われなくなります。

またスイッチは、IP デバイス トラッキング リストを使用してスイッチに接続されているホストの検知と管理を行います。スイッチは、ホストの検出に ARP または DHCP スヌーピングを使用します。スイッチの IP デバイス トラッキング機能は、デフォルトでディセーブルにされています。P デバイス トラッキング テーブルをイネーブルにした後にホストが検出されると、スイッチは次の情報を含む IP デバイス トラッキング テーブルにエントリを追加します。

- ホストの IP および MAC アドレス
- スイッチがホストを検出したインターフェイス
- ホストが検出されたときに ACTIVE に設定されたホスト ステート

NAC レイヤ 2 IP 検証がインターフェイスでイネーブルにされている場合は、IP デバイス トラッキング テーブルにエントリが追加されるとポスチャ検証が開始されます。

IP デバイス トラッキング テーブルには、スイッチがテーブルからエントリを削除する前にエントリに ARP プロブを送信する回数と、ARP プロブを再送信するまでに待機する秒数を設定できます。スイッチは、IP デバイス トラッキング テーブルのデフォルト設定を使用する場合、すべてのエントリに対して 30 秒間隔で ARP プロブを送信します。ホストがプロブに回答すると、ホストのステートが更新され、ACTIVE が維持されます。応答を受信しない場合、スイッチは最大で 3 回 30 秒間隔で ARP プロブを送信できます。ARP プロブの最大回数の送信後、スイッチはテーブルからこのホストのエントリを削除します。セッションが確立されている場合、スイッチはこのホストの EAPoUDP セッションを終了します。

IP デバイス トラッキングを使用することにより、DHCP 使用の制限に関わらず、ホストをタイムリーに検出することができます。リンクがダウンしても、インターフェイスに関連づけられている IP デバイス トラッキング エントリは削除されず、エントリのステートが INACTIVE に変更されます。スイッチは、IP デバイス トラッキング テーブルのエントリ数を制限しませんが、INACTIVE エントリを削除するための制限を設けています。すべてのエントリは、この制限に到達するまで IP デバイス トラッキング テーブルに保持されます。この制限に到達したときにテーブルに INACTIVE エントリがある場合、スイッチは INACTIVE エントリを削除して新しいエントリを追加します。テーブルに INACTIVE エントリがない場合は、IP デバイス トラッキング テーブルのエントリ数はそのまま増加していきます。ホストが INACTIVE になると、スイッチはホストセッションを終了します。

- Catalyst 3750、3560、3550、2970、2960、2955、2950 および 2940 スイッチ、および Cisco EtherSwitch サービスマジュールでは、INACTIVE エントリを削除するための制限は 512 です。
- Catalyst 4500 および 6500 シリーズ スイッチ、および Catalyst 7600 シリーズ ルータの場合、制限は 2048 です。

インターフェイスのリンクが復元されると、スイッチはこのインターフェイスに関連づけられている各エントリに ARP プロブを送信し、ARP プロブに回答しないホストのエントリを削除します。またスイッチは、応答したホストのステートを ACTIVE に変更し、ポスチャ検証を開始します。

再送信タイマー (Retransmission Timer)

再送信タイマーは、ポスチャ検証中に、スイッチが要求を再送信する前にクライアントからの応答を待機する時間を制御します。このタイマーを低く設定しすぎると不必要な再送信が行われ、高く設定しすぎると応答時間が低下する可能性があります。

再送信タイマーのデフォルト値は3秒です。

再検証タイマー (Revalidation Timer)

再検証タイマーは、ポスチャ検証中に EAPoUDP メッセージを使用したクライアントに、NAC ポリシーを適用する時間を制御します。このタイマーは最初のポスチャ検証の完了後に開始され、ホストが再検証されるとリセットされます。再検証タイマーのデフォルト値は36000秒(10時間)です。

再検証タイマーの値は、**eu timeout revalidation** グローバル設定コマンドを使用して、スイッチまたはスイッチのインターフェイスに指定できます。



注

再検証タイマーは、スイッチのローカルに設定することも、Cisco ACS Server からダウンロードすることもできます。

再検証タイマーの動作は、AAA で稼動する Cisco Secure ACS から送信される Access-Accept メッセージの Session-Timeout RADIUS アトリビュートと Terminate-Action RADIUS アトリビュートに基づいています。スイッチが Session-Timeout 値を受信すると、この値によりスイッチの再検証タイマーの値は無効になります。

再検証タイマーが失効すると、スイッチは Termination-Action 値に応じて動作します。

- Termination-Action RADIUS アトリビュート値が Default の場合、セッションは終了します。
- スイッチが Default 以外の Termination-Action 値を受け取ると、ポスチャの再検証中も EAPoUDP セッションと現在のアクセス ポリシーが有効になります。
- Termination-Action アトリビュートの値が RADIUS の場合、スイッチはクライアントを再検証します。
- サーバから送信されるパケットに Termination-Action アトリビュートが含まれていない場合、EAPoUDP セッションは終了します。

ステータス クエリー タイマー (Status-Query Timer)

ステータス クエリー タイマーは、前回検証されたクライアントが現在も存在し、そのポスチャに変更がないことの確認を行うまでにスイッチが待機する時間を制御します。このタイマーを使用するのは、EAPoUDP メッセージで認証されたホストのみです。このタイマーはクライアントの最初の検証の後に開始されます。ステータス クエリー タイマーのデフォルト値は300秒(5分)です。

このタイマーは、ホストが再認証されるとリセットされます。このタイマーが失効すると、スイッチはホストにステータス クエリー メッセージを送信してホストのポスチャを確認します。ホストがポスチャ変更を通知するメッセージをスイッチに送信すると、スイッチはホストのポスチャを再検証します。

NAC レイヤ 2 IP とスイッチ スタック



注

この情報は、Catalyst 3750 シリーズ スイッチおよび EtherSwitch サービス モジュールに適用されます。

新しいスタック マスターが選択されたときに、ホストが接続しているインターフェイスで NAC レイヤ 2 IP がまだイネーブルな場合は、スイッチ スタックに接続中の以前に検証済みのすべてのホストの再検証が必要となります。インターフェイスで NAC レイヤ 2 IP がディセーブルの場合は、以前に検証済みのホストの再検証は実施できません。

NAC レイヤ 2 IP 検証と冗長モジュラ スイッチ

**注**

この情報は、Catalyst 4500 および 6500 スイッチ、および Catalyst 7600 ルータに適用されます。

Route Processor Redundancy (RPR) モードの冗長性が設定されている場合、スイッチオーバーが発生すると現在ポスチャ検証済みのホストに関するすべての情報は失われます。Stateful Switch Over (SO) モードの冗長性が設定されている場合は、スイッチオーバーが発生するとポスチャ検証済みのすべてのホストのポスチャ再検証が開始されます。

NAC レイヤ 2 IP 検証の AAA ダウン ポリシー

**注**

この情報は、Catalyst 6500 スイッチ、および Catalyst 7600 ルータにのみ適用されます。

AAA ダウン ポリシーに対し、システムは次のように動作します。

1. 新しいセッションが検出されます。
2. ポスチャ検証が開始される前に AAA サーバが使用不能であることが分かると、AAA ダウン ポリシーが適用され、セッション ステートは AAA DOWN として維持されます。
3. AAA サーバが再び使用可能になると、このホストに対する再認証が再度開始されます。

**注**

AAA サーバがダウンした場合に AAA ダウン ポリシーが適用されるのは、ホストに既存のポリシーが適用されていない場合のみです。通常は再検証中に AAA サーバがダウンすると、ホストに適用されていたポリシーがそのまま使用されます。

NAC の設定

このセクションは、次のトピックで構成されています。

- デフォルトの NAC 設定 18 ページ
- NAC 設定の考慮点と制限 18 ページ
- NAC レイヤ 2 IEEE 802.1X の設定 21 ページ
- NAC レイヤ 2 IP 検証 の設定 21 ページ
- EAPoUDP の設定 24 ページ
- アイデンティティ プロファイルとポリシーの設定 26 ページ
- IP デバイス トラッキングの設定 27 ページ
- NAC の IP DHCP スヌーピングの設定 (オプション) 28 ページ
- IP ARP インスペクションと ARP フィルタ リストの設定 (オプション) 29 ページ
- IP ARP インスペクションと IP DHCP スヌーピングの設定 (オプション) 30 ページ
- NAC AAA ダウン ポリシーの設定 (オプション) 32 ページ

デフォルトの NAC 設定

デフォルトの NAC レイヤ 2 IEEE 802.1X 設定については、ソフトウェア コンフィギュレーション ガイドの「802.1X Port-Based Authentication」の章の「Default IEEE 802.1X Configuration」を参照してください。

デフォルトでは、NAC レイヤ 2 IP 検証はディセーブルにされています。

NAC 設定の考慮点と制限

ここでは、次の設定上の考慮点と制限について説明します。

- NAC レイヤ 2 IEEE 802.1X の考慮点と制限 18 ページ
- NAC レイヤ 2 IP の考慮点と制限 19 ページ

NAC レイヤ 2 IEEE 802.1X の考慮点と制限



注

次の考慮点は、Catalyst 4900、4500、3750、3560、3550、2970、2960、2955、2950 および 2940 スイッチ、Cisco Gigabit Ethernet Switching Module (CGESM) および Cisco EtherSwitch サービス モジュールに適用されます。

次の事項は、ACS サーバによってポートに割り当てられた VLAN に適用されます。

- VLAN は、スイッチ上の有効な VLAN である必要があります。
- スイッチ ポートは、非プライベート VLAN に割り当てられた静的なアクセス ポートとして設定できます。
- スイッチ ポートは、セカンダリ プライベート VLAN に属するプライベート VLAN ポートとして設定できます。このスイッチ ポートに接続されているすべてのホストには、ポスチャ検証が成功したかどうかに関わらず、プライベート VLAN に割り当てられます。

Access-Accept メッセージの VLAN タイプがクライアントに割り当てられているスイッチ ポートの VLAN タイプと一致しない場合、VLAN 割り当ては失敗します。

ポートにプライベート VLAN を割り当てる場合は、セカンダリ プライベート VLAN を指定します。スイッチは、スイッチ上のプライマリおよびセカンダリ プライベート VLAN アソシエーションを使用してプライマリ プライベート VLAN を決定します。

- NAC レイヤ 2 IEEE 802.1X を設定できないポートのリストは、ソフトウェア コンフィギュレーション ガイドの「Understanding and Configuring 802.1X Port-Based Authentication」の章の「IEEE 802.1X Configuration Guidelines」を参照してください。
- 非応答ホストを割り当てるゲスト VLAN を設定するときは、このゲスト VLAN タイプを適切なポートタイプに対応させる必要があります。VLAN タイプがスイッチ ポートタイプに対応していないと、非応答ホストはネットワークへのアクセスを拒否されます。
- ゲスト VLAN をアクセス ポートに設定する場合、VLAN タイプは非プライベート VLAN になります。ゲスト VLAN をプライベート VLAN ポートに設定する場合、VLAN タイプはプライベート VLAN になります。

NAC をサポートするには、アクセス ポイントに EAP 認証および VLAN を設定する必要があります。アクセス ポイントに EAP 認証を設定する方法については、次の URL に掲載されている『Cisco Aironet アクセス ポイント Cisco IOS ソフトウェア コンフィギュレーション ガイド』の「認証タイプの設定」の章を参照してください。

http://www.cisco.com/jp/service/manual_j/wr/airo1k/caapciscg/chapter10/7092_01_10.shtml

アクセス ポイントに VLAN を設定する方法については、次の URL に掲載されている『Cisco Aironet アクセス ポイント Cisco IOS ソフトウェア コンフィギュレーション ガイド』の「VLAN の設定」の章を参照してください。

http://www.cisco.com/jp/service/manual_j/wr/airo1k/caapcisg/chapter13/7092_01_13.shtml

- NAC レイヤ 2 IEEE 802.1X は、次の方法で他の機能をやりとりします。
 - プライベート VLAN ポートには音声 VLAN を設定できないため、ホストが音声 VLAN に割り当てられている場合は、スイッチはホストのポスチャ検証を行いません。
 - 非応答ホストは、デフォルトでゲスト VLAN に割り当てられます。ポスチャ検証が成功したホスト、および NAC 非対応の従来の IEEE 802.1X 対応クライアント ソフトウェアが稼動するホストはすべて、アクセス制御の決定に基づいてネットワーク アクセスが与えられます。
 - 他の機能とのやりとりに関する詳しい情報については、ソフトウェア コンフィギュレーション ガイドの『Configuring 802.1X Port-Based Authentication』の章の「IEEE 802.1X Configuration Guidelines」を参照してください。
- NAC レイヤ 2 IEEE 802.1X の AAA ダウン ポリシーは、Catalyst 3560 および Catalyst 3750 シリーズ スイッチでのみサポートされています。(最新の状況は各スイッチのマニュアルを参照ください)

NAC レイヤ 2 IP の考慮点と制限



注

これらの考慮点は、CGESM スイッチ、Cisco EtherSwitch サービス モジュール、Catalyst 7600 ルータ、および Catalyst 6500、4900、4500、3750、3560、3550 スイッチに適用されます。

NAC レイヤ 2 IP は、次の考慮点と制限に従って設定してください。

- NAC レイヤ 2 IP をイネーブルにするには、スイッチからホストへのレイヤ 3 ルートを設定する必要があります。
- デフォルト ACL は、LPIP が機能できるように EAPoUDP トラフィックを許可する必要があります。
- Catalyst 6500 以外のすべてのスイッチおよび Catalyst 7600 シリーズ ルータ以外では、トランク ポート、トンネル ポート、EtherChannel、EtherChannel メンバー、またはルーテッド ポート上での NAC レイヤ 2 IP 検証はサポートされていません。
- NAC レイヤ 2 IP 検証をイネーブルにしている場合は、ホストが接続しているスイッチ ポートにデフォルト ポート ACL を設定する必要があります。
- NAC レイヤ 2 IP は、IPv6 トラフィックのポスチャを検証しません。また、IPv6 トラフィックにアクセス ポリシーを適用しません。
- スイッチが、異なる送信元 IP アドレスからの大量 ARP パケットを受信すると、DoS 攻撃が発生する可能性があります。

ARP パケットのレート制限の情報については、次の URL に掲載されている『Cisco IOS コマンド リファレンス』(英語)の「**ip arp inspection limit**」に関するセクションを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgr/sec_r/sec_plg.htm

- NAC レイヤ 2 IP と NAC レイヤ 2 IEEE 802.1X が同一のポートでイネーブルにされている場合は、IEEE 802.1X の認証が常に優先されます(つまり、IEEE 802.1X の認証が失敗すると NAC レイヤ 2 IP 検証は行われません)。ポートに接続されているホストのポスチャが検証されている場合も、スイッチは IEEE 802.1X に基づいてアクセス制限を適用します。
- スイッチが DHCP リース許可を使用して接続ホストを特定できるようにするには、DHCP スヌーピングをイネーブルにする必要があります。
- DHCP スヌーピングを機能させるには、インターフェイス デフォルト ACL およびホスト ポリシーで DHCP トラフィックを許可する必要があります。

- DHCP 環境では、デフォルト インターフェイスおよびダウンロードされたホスト ポリシーで DHCP パケットを許可する必要があります。
- ポスチャ検証の発生前にエンド ステーションに DNS 要求を送信させるには、DNS パケットを許可する ACE を含む名前付き Downloadable ACL をスイッチ ポートに設定する必要があります。
- エンドポイント デバイスからの HTTP および HTTPS 要求を特定の URL に転送するには、HTTP サーバ機能をイネーブルにし、url-redirect-acl に URL ACL 名を定義する必要があります。URL ACL は、スイッチのローカルに定義する必要があります。この ACL には、通常 「deny tcp any <修復サーバアドレス> eq www」 が含まれ、次にリダイレクトが必要な HTTP トラフィックのための許可 ACE が続きます。
- 音声 VLAN に属するスイッチ ポートに NAC レイヤ 2 IP が設定されている場合、スイッチは IP 電話のポスチャを検証しません。IP 電話は例外リストに含むようにしてください。
- NAC レイヤ 2 IP 検証がイネーブルで VLAN ACL とルータ ACL が設定されている場合、ポリシーは「NAC レイヤ 2 LP IP ポリシー > VLAN ACL > ルータ ACL」の順に連続して適用されます。2 つめからのポリシーが適用されるのは、トラフィックが直前のポリシー チェックを通過したときのみです。いずれかのポリシーがトラフィックを拒否すると、トラフィックは拒否されます。



注

(ACS からダウンロードされた) NAC レイヤ 2 IP ホスト ポリシーは、常にデフォルト インターフェイス ポリシーを無効にします。

- 着信 VLAN でダイナミック ARP インスペクションがイネーブルの場合、スイッチがポスチャ検証を開始するのは、ARP パケットの検査の後だけです。
- スwitch ポートで IP ソース ガードと NAC レイヤ 2 IP がイネーブルの場合は、IP ソース ガードによってブロックされたトラフィックのポスチャ検証は開始されません。
- シングルホスト モードの IEEE 802.1X 認証と NAC レイヤ 2 IP 検証がスイッチ ポートに設定されているときに、接続ホストの IEEE 802.1X 認証が失敗すると、スイッチはホストから DHCP または ARP パケットを受信してもポスチャ検証を開始しません。
IEEE 802.1X 認証がポートに設定されていると、ポートはクライアントが認証に成功するまで EAPOL フレーム以外のトラフィックの送受信を行えません。
- Catalyst 4500 シリーズ スイッチでは、access-group mode コマンドを使用して、NAC レイヤ 2 IP ホスト ポリシー ACL によって VLAN ACL および ルータ ACL を無効にするか、または IP ホスト ポリシー ACL を VLAN ACL および ルータ ACL と統合するかを制御できます。
- Catalyst 6500 シリーズ スイッチおよび Catalyst 7600 シリーズ ルータでは、URL-Redirect deny ACE に適合するトラフィックは、デフォルトのインターフェイスおよびダウンロードされたホスト ポリシーが適用されずに、ハードウェアで転送されます。このトラフィック (deny URL-Redirect ACE に一致するトラフィック) のフィルタが必要な場合は、スイッチ ポートのアクセス VLAN に VLAN ACL を定義する必要があります。
- Catalyst 6500 シリーズ スイッチおよび Catalyst 7600 シリーズ ルータでは、トランク ポート、トンネル ポート、EtherChannel メンバー、またはルーテッド ポート上での NAC レイヤ 2 IP 検証はサポートされていません。ただし Catalyst 6500 シリーズ スイッチおよび Catalyst 7600 シリーズ ルータは Etherchannel 上でレイヤ 2 IP をサポートします。
- Catalyst 6500 シリーズ スイッチおよび Catalyst 7600 シリーズ ルータでは、ポートの親 VLAN に VLAN ACL (VACL) キャプチャおよび / または IOS ファイアウォール Context-Based Access Control (CBAC) が設定されている場合、スイッチポート上での NAC レイヤ 2 IP は許可されません。
- Catalyst 6500 シリーズ スイッチおよび Catalyst 7600 シリーズ ルータでは、スイッチ ポートがプライベート VLAN の一部である場合、NAC レイヤ 2 IP はサポートされません。
- Catalyst 6500 シリーズ スイッチおよび Catalyst 7600 シリーズ ルータでは、CPU にリダイレクトされる NAC レイヤ 2 LPIP ARP トラフィックは SPAN 機能を使用してスパンできません。

NAC レイヤ 2 IEEE 802.1X の設定

Catalyst 4500 シリーズ スイッチに NAC レイヤ 2 IEEE 802.1X を設定するときは、ソフトウェア コンフィギュレーション ガイドの「802.1X ポートベースの認証の概要および設定」および「スイッチ /RADIUS サーバ通信の設定」のセクションを参照してください。掲載されている他のタスクはすべてオプションです。

http://www.cisco.com/jp/service/manual_j/index_sw_cat4500.shtml

それ以外のスイッチに設定する場合は、ソフトウェア コンフィギュレーション ガイドの「802.1x ポートベースの認証の設定」および「RADIUS によるスイッチアクセスの制御」のセクションを参照してください。

Catalyst 3750 シリーズ スイッチを使用する場合は、次の URL を参照してください。

http://www.cisco.com/jp/service/manual_j/index_sw_cat3750.shtml

Catalyst 3560 シリーズ スイッチを使用する場合は、次の URL を参照してください。

http://www.cisco.com/jp/service/manual_j/index_sw_cat3560.shtml

Catalyst 3550 シリーズ スイッチを使用する場合は、次の URL を参照してください。

http://www.cisco.com/jp/service/manual_j/index_sw_cat3550.shtml

Catalyst 2970 シリーズ スイッチを使用する場合は、次の URL を参照してください。

http://www.cisco.com/jp/service/manual_j/index_sw_cat2970.shtml

Catalyst 2960 シリーズ スイッチを使用する場合は、次の URL を参照してください。

http://www.cisco.com/jp/service/manual_j/index_sw_cat2960.shtml

Catalyst 2955 および 2950 シリーズ スイッチを使用する場合は、次の URL を参照してください。

http://www.cisco.com/jp/service/manual_j/index_sw_cat2950.shtml

Catalyst 2940 シリーズ スイッチを使用する場合は、次の URL を参照してください。

http://www.cisco.com/jp/service/manual_j/index_sw_cat2940.shtml

NAC レイヤ 2 IP 検証の設定

NAC レイヤ 2 IP 検証を設定するには、次の手順を実行します。

	コマンド	目的
手順 1	<code>configure terminal</code>	グローバル設定モードに入ります。
手順 2	<code>ip admission name rule-name eapoudp</code>	ルール名を指定して IP NAC ルールを作成し、設定します。 スイッチから IP NAC ルールを削除するには、 <code>no ip admission name rule-name eapoudp</code> グローバル設定コマンドを使用します。

	コマンド	目的
手順 3	<code>access-list access-list-number {deny permit} source [source-wildcard] [log]</code>	<p>送信元アドレスおよびワイルドカードを使用して、デフォルトポート ACL を定義します。</p> <p><i>access-list-number</i> は、1 ~ 99 または 1300 ~ 1999 の 10 進数です。</p> <p>deny または permit を入力し、条件と一致した場合にアクセスを拒否するか、許可するかを指定します。</p> <p><i>source</i> は、パケットを送信するネットワークまたはホストの送信元アドレスです。次のように指定されます。</p> <ul style="list-style-type: none"> ドット付き 10 進表記で 32 ビットの値 0.0.0.0 255.255.255.255 という <i>source</i> および <i>source-wildcard</i> の省略形を表すキーワード any。<i>source-wildcard</i> の入力は不要です。 <i>source</i> 0.0.0.0 という <i>source</i> および <i>source-wildcard</i> の省略形を表すキーワード host <p>(オプション) <i>source-wildcard</i> によって、ワイルドカードビットが <i>source</i> に適用されます。</p> <p>(オプション) log を入力すると、エントリに一致するパケットに関するインフォメーションなロギングメッセージがコンソールに送信されます。</p>
手順 4	<code>interface interface-id</code>	インターフェイス設定モードに入ります。
手順 5	<code>ip access-group {access-list-number name} in</code>	指定したインターフェイスへのアクセスを制御します。
手順 6	<code>ip admission name rule-name</code>	<p>指定した IP NAC ルールをインターフェイスに適用します。</p> <p>特定のインターフェイスに適用されている IP NAC ルールを削除するには、no ip admission rule-name インターフェイス設定コマンドを使用します。</p>
手順 7	<code>exit</code>	グローバル設定モードに戻ります。
手順 8	<code>aaa new-model</code>	AAA をイネーブルにします。
手順 9	<code>aaa authentication eou default group radius</code>	<p>EAPoUDP の認証方式を設定します。</p> <p>EAPoUDP の認証方式を削除するには、no aaa authentication eou default グローバル設定コマンドを使用します。</p>
手順 10	<code>ip device tracking</code>	<p>IP デバイス トラッキング テーブルをイネーブルにします。</p> <p>IP デバイス トラッキング テーブルをディセーブルにするには、no ip device tracking グローバル設定コマンドを使用します。</p>
手順 11	<code>ip device tracking [probe {count count} interval interval]</code>	<p>(オプション) IP デバイス トラッキング テーブルに次のパラメータを設定します。</p> <ul style="list-style-type: none"> count count_ スイッチが ARP プローブを送信する回数を 1 ~ 5 の範囲で指定します。デフォルト値は 3 です。 interval interval_ スイッチが ARP プローブを再送信するまでに応答を待機する秒数を 30 ~ 300 の範囲で指定します。デフォルト値は 30 秒です。

	コマンド	目的
手順 12	<code>radius-server host {hostname ip-address} key string</code>	(オプション) RADIUS サーバパラメータを設定します。 <i>hostname ip-address</i> には、リモート RADIUS サーバのホスト名または IP アドレスを指定します。 <i>key string</i> には、スイッチと RADIUS サーバ上で稼働する RADIUS デーモンとの間で使用する認証および暗号鍵を指定します。鍵は、RADIUS サーバ上で使用する暗号鍵と照合する必要があるテキスト文字列です。 注 鍵は、必ず <code>radius-server host</code> コマンドシンタックスの最後の項目として設定します。先行スペースは無視されますが、鍵の内部および末尾のスペースは使用されます。鍵にスペースを使用する場合は、鍵の一部として引用符を使用する場合を除いて、鍵を引用符で囲まないとくずさないでください。この鍵は、RADIUS デーモンで使用される暗号鍵と一致する必要があります。 複数の RADIUS サーバを使用するときは、このコマンドを再度入力します。
手順 13	<code>radius-server attribute 8 include-in-access-req</code>	(オプション) スイッチに非応答ホストが接続されているときに、スイッチが Access-Request または Accounting-Request パケットで Framed-IP-Address RADIUS アトリビュート (Attribute[8]) を送信するように設定します。 スイッチが Framed-IP-Address アトリビュートを送信しないように設定するには、 <code>no radius-server attribute 8 include-in-access-req</code> グローバル設定コマンドを使用します。
手順 14	<code>radius-server vsa send authentication</code>	ネットワーク アクセス サーバがベンダー固有アトリビュートを認識し、使用するよう設定します。
手順 15	<code>eou logging</code>	(オプション) EAPoUDP システム イベントのログギングをイネーブルにします。 EAPoUDP システム イベントのログギングをディセーブルにするには、 <code>no eou logging</code> グローバル設定コマンドを使用します。
手順 16	<code>end</code>	特権 EXEC モードに戻ります。
手順 17	<code>show ip admission {[cache][configuration] [eapoudp]}</code>	NAC 設定または ネットワーク アドミッション キャッシュ エントリを表示します。
手順 18	<code>show ip device tracking {all interface interface-id ip ip-address mac mac-address}</code>	IP デバイス トラッキング テーブルのエントリに関する情報を表示します。
手順 19	<code>copy running-config startup-config</code>	(オプション) エントリをコンフィギュレーション ファイルに保存します。

認証プロキシ ポスチャードが AAA サーバからセキュリティアソシエーションを取得しないように設定するには、`no aaa authorization auth-proxy default` グローバル設定コマンドを使用します。

スイッチ、または特定のインターフェイス上のすべての NAC クライアント デバイス エントリをクリアするには、`clear eou` 特権 EXEC コマンドを使用します。IP デバイス トラッキング テーブルのエントリをクリアするには、`clear ip device tracking` 特権 EXEC コマンドを使用します。

スイッチ インターフェイス上に NAC レイヤ 2 IP 検証を設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip admission name nac eapoudp
Switch(config)# access-list 5 permit any any
Switch(config)# interface gigabitethernet 2/0/1
```

```
Switch(config-if)# ip access-group 5 in
Switch(config-if)# ip admission name nac
Switch(config-if)# exit
Switch(config)# aaa new-model
Switch(config)# aaa authentication eou default group radius
Switch(config)# ip device tracking
Switch(config)# ip device tracking probe count 2
Switch(config)# radius-server host admin key rad123
Switch(config)# radius-server vsa send authentication
Switch(config)# eou logging
Switch(config)# end
Switch# show ip admission configuration

Authentication global cache time is 60 minutes Authentication global absolute time is 0
minutes Authentication global init state time is 2 minutes Authentication Proxy Watch-list
is disabled

Authentication Proxy Rule Configuration
Auth-proxy name nac
    eapoudp list not specified auth-cache-time 60 minutes

Switch# show ip device tracking all
IP Device Tracking = Enabled
-----
IP Address      MAC Address      Interface          STATE
-----
10.5.0.25       0060.b0f8.fbf8  GigabitEthernet1/0/4  ACTIVE
```

EAPoUDP の設定

EAPoUDP は、NAC レイヤ 2 IP がエンドポイント システムとポスチャ情報を交換するために使用するプロトコルです。EAPoUDP ステート マシン パラメータを調整するには、次の手順を実行します。

	コマンド	目的
手順 1	<code>configure terminal</code>	グローバル設定モードに入ります。
手順 2	<code>eou allow {clientless ip-station-id}</code> <code>eou default</code> <code>eou logging</code> <code>eou max-retry number</code> <code>eou port port-number</code> <code>eou ratelimit number</code> <code>eou timeout {aaa seconds hold-period seconds retransmit seconds revalidation seconds status-query seconds}</code> <code>eou revalidate</code>	EAPoUDP 値を指定します。 allow 、 default 、 logging 、 max-retry 、 port 、 rate-limit 、 revalidate および timeout オプションのキーワードの詳細な情報については、本書のコマンド リファレンスのセクションを参照してください。
手順 3	<code>interface interface-id</code>	インターフェイス設定モードに入ります。

	コマンド	目的
手順 4	euo default euo max-retry number euo timeout {aaa seconds hold-period seconds retransmit seconds revalidation seconds status-query seconds} euo revalidate	指定したインターフェイスの EAPoUDP アソシエーションをイネーブルにして設定します。 default 、 max-retry 、 revalidate 、および timeout オプションのキーワードの詳細な情報については、本書のコマンド リファレンスのセクションを参照してください。
手順 5	end	特権 EXEC モードに戻ります。
手順 6	show euo {all authentication {clientless eap static} interface interface-id ip ip-address mac mac-address posturetoken name}	EAPoUDP 設定またはセッション キャッシュ エントリに関する情報を表示します。
手順 7	copy running-config startup-config	(オプション) エントリをコンフィギュレーション ファイルに保存します。

デフォルトの EAPoUDP 値に戻すには、**euo** グローバル設定コマンドの **no** 形式を使用します。EAPoUDP アソシエーションをディセーブルにするには、**euo** インターフェイス設定コマンドの **no** 形式を使用します。スイッチ インターフェイスの EAPoUDP 設定方法の例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# euo logging
Switch(config)# euo allow clientless
Switch(config)# euo timeout revalidation 2400
Switch(config)# euo revalidate
Switch(config)# interface gigabitEthernet 1/0/4
Switch(config-if)# euo timeout status-query 600
Switch(config-if)# end
Switch# show euo
```

```
Global EAPoUDP Configuration
-----
EAPoUDP Version = 1
EAPoUDP Port = 0x5566
Clientless Hosts = Enabled
IP Station ID = Disabled
Revalidation = Enabled
Revalidation Period = 2400 Seconds
ReTransmit Period = 3 Seconds
StatusQuery Period = 300 Seconds
Hold Period = 180 Seconds
AAA Timeout = 60 Seconds
Max Retries = 3
EAP Rate Limit = 20
EAPoUDP Logging = Enabled
```

```
Interface Specific EAPoUDP Configurations
-----
Interface GigabitEthernet1/0/4
    StatusQuery Period = 600 Seconds
```

アイデンティティ プロファイルとポリシーの設定

アイデンティティ プロファイルとポリシーを設定するには、次の手順を実行します。

	コマンド	目的
手順 1	<code>configure terminal</code>	グローバル設定モードに入ります。
手順 2	<code>identity policy policy-name</code>	アイデンティティ ポリシーを作成し、アイデンティティ ポリシー設定モードに入ります。 アイデンティティ ポリシーを削除するには、 <code>no identity-policy policy-name</code> グローバル設定コマンドを使用します。
手順 3	<code>access-group access-group</code>	(オプション) アイデンティティ ポリシーのネットワーク アクセス アトリビュートを定義します。
手順 4	<code>identity profile eapoudp</code>	アイデンティティ プロファイルを作成し、アイデンティティ プロファイル設定モードに入ります。 アイデンティティ プロファイルを削除するには、 <code>no identity profile eapoudp</code> グローバル設定コマンドを使用します。
手順 5	<code>device {authorize not-authorize} {ip-address ip-address mac-address mac-address type cisco ip phone} [policy policy-name]</code>	指定した IP デバイスを許可し、指定したポリシーをこのデバイスに適用します。 指定した IP デバイスを許可せずに、デバイスから指定したポリシーを削除するには、 <code>no device {authorize not-authorize} {ip-address ip-address mac-address mac-address type cisco ip phone} [policy policy-name]</code> インターフェイス設定コマンドを使用します。
手順 6	<code>exit</code>	アイデンティティ プロファイル設定モードを終了し、グローバル設定モードに戻ります。
手順 7	<code>end</code>	特権 EXEC モードに戻ります。
手順 8	<code>show identity [policy profile]</code>	設定したアイデンティティ および / またはプロファイルを表示します。
手順 9	<code>show running-config</code>	エントリを確認します。
手順 10	<code>copy running-config startup-config</code>	(オプション) エントリをコンフィギュレーション ファイルに保存します。

次に、IP アドレスに基づいてホストを許可するプロファイルを設定し、ホストとローカル ポリシーを関連付ける方法の例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# identity policy policy1
Switch(config-identity-policy)# access-group group1
Switch(config)# identity profile eapoudp
Switch(config-identity-prof)# device authorize ip address 10.10.142.25 policy policy1
Switch(config-identity-prof)# exit
Switch(config)# end
Switch# show identity policy
Policy Name      ACL          Redirect ACL   Redirect URL
=====
policy1          group1       NONE           NONE

Switch# show identity profile
No identity profile of type default is configured.

No identity profile of type dot1x is configured.
```

Service Type: eapoudp

Device / Address / Mask	Allowed	Policy
10.5.0.99 / 0.0.0.0	Authorized	policy1

IP デバイス トラッキングの設定



注

このタスクを実行するには、レイヤ 2 IP 検証をイネーブルにする必要があります。

NAC レイヤ 2 IP 検証は、ポスチャ検証を開始するトラフィックのサブセットの定義に Intercept ACL を使用しません (この点が レイヤ 3 実装とは異なります)。代わりに、IP デバイス トラッキング テーブルを使用してネットワークに接続する新しいホストを追跡します。IP デバイス トラッキング テーブルは、次のメカニズムを通じてホストを検出します。

- IP ARP インспекション
- IP DHCP スヌーピング (オプション)

IP ARP インспекションは、IP デバイス トラッキングをイネーブルにすると自動的にイネーブルになります。ARP インспекションは、ARP パケットを監視して新しいホストの存在を検出します。IP DHCP スヌーピングは、イネーブルになると、DHCP がホストに IP アドレスを割り当てたときまたは無効にしたときに新しいホストの存在または削除を検出します。



注

ダイナミック ARP インспекションがイネーブルの場合、デバイス トラッキング テーブルを使用した新しいホストの検出の対象になるのは、検査された ARP パケットのみです。

IP デバイス トラッキング テーブルに追加されたデバイスは、定期的な ARP プロブによって監視されます。これらのプロブに回答しなかったパケットは、デバイス トラッキング テーブルから削除されます。



注

オプションでプロブのタイムアウトおよび最大プロブ数を設定できます。プロブは、NAD がホストを認識した後のホストの追跡に使用されます。

IP デバイス トラッキングを設定するには、次の手順を実行します。

	コマンド	目的
手順 1	<code>configure terminal</code>	グローバル設定モードに入ります。
手順 2	<code>ip device tracking</code>	(必須) IP デバイス トラッキングをイネーブルにします。 これにより、IP アドミッションがイネーブルにされているポートで、ARP パケットのスヌーピングを通じてレイヤ 2 IP デバイスをラーニングできるようになります。
手順 3	<code>ip device tracking probe count n</code>	(オプション) IP デバイス トラッカーがデバイスにプロブを送信する最大回数を変更します。デフォルト値は 3 です。
手順 4	<code>ip device tracking probe interval interval_number</code>	(オプション) プロブ間隔を変更します。デフォルト値は 30 秒です。
手順 5	<code>exit</code>	アイデンティティ プロファイル設定モードを終了し、グローバル設定モードに戻ります。
手順 6	<code>end</code>	特権 EXEC モードに戻ります。

	コマンド	目的
手順 7	<code>show ip device tracking [all]</code>	スイッチ上で検出された IP ホストのリストを表示します。これらのホストは、NAC レイヤ 2 IP ポスチャ検証の対象となります
手順 8	<code>show running-config</code>	エントリを確認します。
手順 9	<code>copy running-config startup-config</code>	(オプション) エントリをコンフィギュレーション ファイルに保存します。

次に IP デバイス トラッキングの設定方法の例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip device tracking
Switch(config)# ip device tracking probe count 3
Switch(config)# ip device tracking probe interval 60
Switch(config)# end
Switch# show ip device tracking all
IP Device Tracking = Enabled
-----
IP Address   MAC Address      Interface          STATE
-----
8.0.0.1      0060.b0f8.fbf8  GigabitEthernet1/0/4  ACTIVE
```



注

NAC では、IP デバイス トラッキングとともに、IP DHCP スヌーピングまたは IP ARP インспекションを設定する必要があります。

NAC の IP DHCP スヌーピングの設定 (オプション)

レイヤ 2 IP 検証の開始 / デバイス ラーニング メカニズムとして DHCP を使用する場合は、IP DHCP スヌーピングの設定が必要です。DHCP スヌーピングは、IP アドミッションがイネーブルにされているスイッチポートの音声 VLAN およびデータ VLAN 両方でイネーブルにする必要があります。

IP DHCP スヌーピングを設定するには、次の手順を実行します。

	コマンド	目的
手順 1	<code>configure terminal</code>	グローバル設定モードに入ります。
手順 2	<code>ip dhcp snooping</code>	スイッチで IP DHCP スヌーピングをイネーブルにします。
手順 3	<code>ip dhcp snooping vlan <i>vlan_id</i></code>	スイッチの着信 VLAN で IP DHCP スヌーピングをイネーブルにします。
手順 4	<code>ip dhcp snooping trust</code>	インターフェイスの DHCP スヌーピング信頼ステートをイネーブルにします。 DCHP スヌーピング信頼ステートは、DHCP サーバが接続されているアップリンク ポートでイネーブルにする必要があります。
手順 5	<code>exit</code>	アイデンティティ プロファイル設定モードを終了し、グローバル設定モードに戻ります。
手順 6	<code>end</code>	特権 EXEC モードに戻ります。
手順 7	<code>show ip dhcp snooping [binding]</code>	現在の DHCP スヌーピング設定を表示します。 オプションの binding キーワードを使用すると、DHCP スヌーピングで検出された DHCP リースのリストを表示できます。
手順 8	<code>show running-config</code>	エントリを確認します。
手順 9	<code>copy running-config startup-config</code>	(オプション) エントリをコンフィギュレーション ファイルに保存します。

次に NAC での IP DHCP スヌーピングの設定方法の例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 8
Switch(config)# end
Switch# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
1,10,1001
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed Verification of hwaddr field is enabled
Interface                Trusted Rate limit (pps)
-----
Switch# show ip dhcp snooping binding
MacAddress                IpAddress                Lease(sec)  Type                   VLAN  Interface
-----
00:60:B0:F8:FB:FB        8.0.0.1                  79464      dhcp-snooping         8     GigabitEthernet1/0/4
Total number of bindings: 1
```

IP ARP インспекションのみを使用する場合は、次のいずれかの前提条件を満たす必要があります。

- 信頼する必要がある（また NAD での ARP エントリの作成を許可する）IP デバイスのみを許可する静的な ARP フィルタ リストが存在する
- IP ARP インспекション機能による IP ARP エントリの検証を許可する IP DHCP スヌーピング バインディング エントリがスイッチに含まれている
- NAC 着信インターフェイスが IP ARP インспекションに信頼されている。ただし、NAC 着信インターフェイスは監視の対象なので、これは一般的に現実的ではありません。

IP ARP インспекションと ARP フィルタ リストの設定（オプション）

このタスクでは、ダイナミック ARP インспекションの検証チェックの対象となる IP アドレスを静的に指定することにより、レイヤ 2 IP デバイスをラーニングできるようにします。

IP ARP インспекションと ARP フィルタ リストを設定するには、次の手順を実行します。

	コマンド	目的
手順 1	<code>configure terminal</code>	グローバル設定モードに入ります。
手順 2	<code>arp access-list static-arp-list</code>	IP N/W および MAC アドレスの信頼を許可する静的 IP ARP フィルタ ACL を NAD に設定します。
手順 3	<code>deny [ip [any host sender-ip [sender-ip-mask]]] [mac any]</code>	一致する基準に基づいて ARP パケットをドロップします。
手順 4	<code>permits [ip [any host sender-ip [sender-ip-mask]]] [mac any]</code>	一致する基準に基づいて ARP パケットを転送します。
手順 5	<code>exit</code>	アイデンティティ プロファイル設定モードを終了し、グローバル設定モードに戻ります。
手順 6	<code>ip arp inspection vlanvlan_id</code>	VLAN で IP ARP インспекションをイネーブルにします。
手順 7	<code>ip arp inspection filter static-arp-list vlan vlan_id</code>	スイッチの着信 VLAN で IP ARP インспекションをイネーブルにします。 注 この手順は、テストされるデバイスで IP DHCP スヌーピング エントリが作成されない場合に実行します。

	コマンド	目的
手順 8	<code>end</code>	特権 EXEC モードに戻ります。
手順 9	<code>show ip arp inspection [statistics] [vlan <i>vlan_id</i>]</code>	現在の ARP インспекション設定または統計情報を表示します。オプションの <code>vlan</code> キーワードを使用すると、特定の VLAN の情報を表示できます。
手順 10	<code>show running-config</code>	エントリを確認します。
手順 11	<code>copy running-config startup-config</code>	(オプション) エントリをコンフィギュレーションファイルに保存します。

次に IP ARP インспекションと ARP フィルタ リストの設定方法の例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# arp access-list arp-list
Switch(config-arp-nacl)# deny ip host 101.50.1.54 mac any
Switch(config-arp-nacl)# deny ip host 101.50.1.51 mac any
Switch(config-arp-nacl)# permit ip 101.50.1.0 0.0.0.255 mac any
Switch(config-arp-nacl)# exit
Switch(config)# ip arp inspection vlan 101
Switch(config)# ip arp inspection filter arp-acl vlan 101
Switch(config)# end
Switch# show ip arp inspection vlan 101

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

Vlan    Configuration      Operation      ACL Match      Static ACL
----    -
101     Enabled               Active         arp-acl        No

Vlan    ACL Logging            DHCP Logging
----    -
101     Deny                  Deny

Switch# show ip arp inspection statistics

Vlan    Forwarded      Dropped      DHCP Drops      ACL Drops
----    -
101     9              2            0               4

Vlan    DHCP Permits    ACL Permits    Source MAC Failures
----    -
101     9              0             0

Vlan    Dest MAC Failures  IP Validation Failures  Invalid Protocol Data
----    -
101     0               0                   0
```

IP ARP インспекションと IP DHCP スヌーピングの設定 (オプション)

このタスクでは、ARP インспекション機能の検証チェックの対象のレイヤ 2 IP デバイスをラーニングできるようにします。デフォルトでは、ARP パケットは DHCP スヌーピング バインディングを使用して検証されます。



注

このタスクを実行するには、まず ARP インспекションがイネーブルにされる VLAN と同じ VLAN 上で DHCP スヌーピングをイネーブルにする必要があります。

IP ARP インспекションと IP DHCP スヌーピングを設定するには、次の手順を実行します。

	コマンド	目的
手順 1	<code>configure terminal</code>	グローバル設定モードに入ります。
手順 2	<code>ip dhcp snooping</code>	スイッチで IP DHCP スヌーピングをイネーブルにします。
手順 3	<code>ip dhcp snooping vlan <i>vlan_id</i></code>	スイッチの着信 VLAN で IP DHCP スヌーピングをイネーブルにします。
手順 4	<code>ip dhcp snooping trust</code>	インターフェイスの DHCP スヌーピング信頼ステートをイネーブルにします。
手順 5	<code>ip arp inspection vlan <i>vlan_id</i></code>	VLAN で IP ARP インспекションをイネーブルにします。 注 DHCP スヌーピングは、IP ARP インспекションがイネーブルにされるこの VLAN でイネーブルにする必要があります。
手順 6	<code>ip arp inspection vlan trust</code>	インターフェイスの ARP インспекション信頼ステートをイネーブルにします。 DHCP サーバが接続されている アップリンク ポートで ARP インспекション信頼をイネーブルにする必要があります。これは、サーバからの ARP トラフィックを検証を行わずに許可するためです。
手順 7	<code>ip arp inspection filter <i>static-arp-list</i> vlan <i>vlan_id</i></code>	スイッチの着信 VLAN で IP ARP インспекションをイネーブルにします。 注 この手順は、テストされるデバイスで DHCP スヌーピング エントリが作成されない場合に実行します。
手順 8	<code>end</code>	特権 EXEC モードに戻ります。
手順 9	<code>show ip arp inspection [statistics] [vlan <i>vlan_id</i>]</code>	現在の ARP インспекション設定または統計情報を表示します。オプションの <code>vlan</code> キーワードを使用すると、特定の VLAN の情報を表示できます。
手順 10	<code>show running-config</code>	エントリを確認します。
手順 11	<code>copy running-config startup-config</code>	(オプション) エントリをコンフィギュレーションファイルに保存します。



注 この設定では、静的な ARP フィルタ リストの設定は必要ありません。

次に IP ARP インспекションと IP DHCP スヌーピングの設定方法の例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip dhcp snooping vlan 8
Switch(config)# ip arp inspection vlan 8
Switch(config)# end
Switch# show ip arp inspection vlan 8

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

Vlan  Configuration  Operation  ACL Match  Static ACL
----  -
      8  Enabled        Active

Vlan  ACL Logging  DHCP Logging
----  -
      8  Deny        Deny
```

```
Switch# show ip arp inspection statistics vlan 8

Vlan  Forwarded  Dropped  DHCP Drops  ACL Drops
-----
      8           4           0           0           0

Vlan  DHCP Permits  ACL Permits  Source MAC Failures
-----
      8           4           0           0

Vlan  Dest MAC Failures  IP Validation Failures  Invalid Protocol Data
-----
      8                 0                 0
```

NAC AAA ダウン ポリシーの設定 (オプション)



注

この機能は、Catalyst 6500 シリーズ スイッチおよび Catalyst 7600 ルータのみで使用できます。ただし、今後、対応する製品が追加される可能性があります。最新の対応状況については、各スイッチおよびルータのマニュアルを参照してください。

NAC AAA ダウン ポリシーを設定するには、次の手順を実行します。

	コマンド	目的
手順 1	<code>configure terminal</code>	グローバル設定モードに入ります。
手順 2	<code>ip admission name rule-name eapoudp event timeout aaa policy identity identity_policy_name</code>	NAC ルールを作成し、AAA サーバが使用不能なときにセッションに適用するアイデンティティ ポリシーを関連付けます。 スイッチからこのルールを削除するには、 <code>no ip admission name rule-name eapoudp event timeout aaa policy</code> グローバル設定コマンドを使用します。
手順 3	<code>access-list access-list-number {deny permit} source [source-wildcard] [log]</code>	送信元アドレスおよびワイルドカードを使用して、デフォルト ポート ACL を定義します。 <i>access-list-number</i> は、1 ~ 99 または 1300 ~ 1999 の 10 進数です。 deny または permit を入力し、条件と一致した場合にアクセスを拒否するか、許可するかを指定します。 <i>source</i> は、パケットを送信するネットワークまたはホストの送信元アドレスです。次のように指定されます。 <ul style="list-style-type: none"> ドット付き 10 進表記で 32 ビットの値 0.0.0.0 255.255.255.255 という <i>source</i> および <i>source-wildcard</i> の省略形を表すキーワード any。<i>source-wildcard</i> の入力は不要です。 <i>source</i> 0.0.0.0 という <i>source</i> および <i>source-wildcard</i> の省略形を表すキーワード host (オプション) <i>source-wildcard</i> によって、ワイルドカード ビットが <i>source</i> に適用されます。 (オプション) log を入力すると、エントリに一致するパケットに関するインフォメーションなログイング メッセージがコンソールに送信されます。
手順 4	<code>interface interface-id</code>	インターフェイス設定モードに入ります。
手順 5	<code>ip access-group {access-list-number name} in</code>	指定したインターフェイスへのアクセスを制御します。

	コマンド	目的
手順 6	<code>ip admission name rule-name</code>	指定した IP NAC ルールをインターフェイスに適用します。 特定のインターフェイスに適用されている IP NAC ルールを削除するには、 no ip admission rule-name インターフェイス設定コマンドを使用します。
手順 7	<code>exit</code>	グローバル設定モードに戻ります
手順 8	<code>aaa new-model</code>	AAA をイネーブルにします。
手順 9	<code>aaa authentication eou default group radius</code>	EAPoUDP の認証方式を設定します。 EAPoUDP の認証方式を削除するには、 no aaa authentication eou default グローバル設定コマンドを使用します。
手順 10	<code>aaa authorization network default local</code>	許可方式をローカルに設定します。この許可方式を削除するには、 no aaa authorization network default local コマンドを使用します。
手順 11	<code>ip device tracking</code>	IP デバイス トラッキング テーブルをイネーブルにします。 IP デバイス トラッキング テーブルをディセーブルにするには、 no ip device tracking グローバル設定コマンドを使用します。
手順 12	<code>ip device tracking [probe {count count} interval interval]</code>	IP デバイス トラッキング テーブルに次のパラメータを設定します。 <ul style="list-style-type: none"> count count — スイッチが ARP プロブを送信する回数を 1 ~ 5 の範囲で指定します。デフォルト値は 3 です。 interval interval — スイッチが ARP プロブを再送信するまでに応答を待機する秒数を 30 ~ 300 の範囲で指定します。デフォルト値は 30 秒です。
手順 13	<code>radius-server host {hostname ip-address} test username username idle-time 1 key string</code>	RADIUS サーバパラメータを設定します。 <i>hostname ip-address</i> には、リモート RADIUS サーバのホスト名または IP アドレスを指定します。 <i>key string</i> には、スイッチと RADIUS サーバ上で稼働する RADIUS デーモンとの間で使用する認証および暗号鍵を指定します。鍵は、RADIUS サーバ上で使用する暗号鍵と照合する必要があるテキスト文字列です。 注 鍵は、必ず radius-server host コマンドの最後の項目として設定します。先行スペースは無視されますが、鍵の内部および末尾のスペースは使用されません。鍵にスペースを使用する場合は、鍵の一部として引用符を使用する場合を除いて、鍵を引用符で囲まないとはいけません。この鍵は、RADIUS デーモンで使用される暗号鍵と一致する必要があります。 test username は、AAA サーバがアクティブかどうかをテストするダミーユーザ名の設定に使用します。 idle-time パラメータは、サーバの生存をテストする間隔の設定に使用します。RADIUS サーバにトラフィックが送信されない場合、NAD はこのアイドルタイムに基づいて RADIUS サーバにダミー RADIUS パケットを送信します。 複数の RADIUS サーバを使用するときは、このコマンドを再度入力します。

	コマンド	目的
手順 14	radius-server attribute 8 include-in-access-req	スイッチに非応答ホストが接続されているときに、スイッチが Access-Request または Accounting-Request パケットで Framed-IP-Address RADIUS アトリビュート (Attribute[8]) を送信するように設定します。 スイッチが Framed-IP-Address アトリビュートを送信しないように設定するには、 no radius-server attribute 8 include-in-access-req グローバル設定コマンドを使用します。
手順 15	radius-server vsa send authentication	ネットワーク アクセス サーバがベンダー固有アトリビュートを認識し、使用するように設定します。
手順 16	radius-server dead-criteria {tries time} value	(オプション) RADIUS サーバを使用不能としてマークするために使用する、1 つまたは両方の基準を指定の定数に設定します。
手順 17	eou logging	(オプション) EAPoUDP システム イベントのロギングをイネーブルにします。 EAPoUDP システム イベントのロギングをディセーブルにするには、 no eou logging グローバル設定コマンドを使用します。
手順 18	end	特権 EXEC モードに戻ります。
手順 19	show ip admission {cache}[configuration] [eapoudp]}	NAC 設定または ネットワーク アドミッション キャッシュ エントリを表示します。
手順 20	show ip device tracking {all interface interface-id ip ip-address mac mac-address}	IP デバイス トラッキング テーブルのエントリに関する情報を表示します。
手順 21	show aaa servers	スイッチ上に設定されている AAA サーバのステータスを表示します。
手順 22	copy running-config startup-config	(オプション) エントリをコンフィギュレーション ファイルに保存します。

次に AAA ダウン ポリシーの適用方法の例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip admission name AAA_DOWN eapoudp event timeout aaa policy identity
global_policy
Switch(config)# aaa new-model
Switch(config)# aaa authorization network default local
Switch(config)# aaa authentication eou default group radius
Switch(config)# identity policy global_policy
Switch(config-identity-policy)# ac
Switch(config-identity-policy)# access-group global_acl
Switch(config)# ip access-list extended global_acl
Switch(config-ext-nacl)# permit ip any any
Switch(config-ext-nacl)# exit
Switch(config)# radius-server host 40.0.0.4 test username administrator idle-time 1 key
cisco
Switch(config)# radius-server dead-criteria tries 3
Switch(config)# radius-server vsa send authentication
Switch(config)# radius-server attribute 8 include-in-access-req
Switch(config)# int fastEthernet 2/13
Switch(config-if)# ip admission AAA_DOWN
Switch(config-if)# exit
Switch# show ip admission configuration
Authentication global cache time is 60 minutes Authentication global absolute time is 0
minutes Authentication global init state time is 2 minutes Authentication Proxy Watch-list
is disabled
```

```

Authentication Proxy Rule Configuration
Auth-proxy name AAA_DOWN
  eapoudp list not specified auth-cache-time 60 minutes
  Identity policy name global_policy for AAA fail policy

Switch# show aaa servers
RADIUS: id 1, priority 1, host 40.0.0.4, auth-port 1645, acct-port 1646
  State: current UP, duration 5122s, previous duration 9s
  Dead: total time 79s, count 3
  Authen: request 158, timeouts 14
    Response: unexpected 1, server error 0, incorrect 0, time 180ms
    Transaction: success 144, failure 1
  Author: request 0, timeouts 0
    Response: unexpected 0, server error 0, incorrect 0, time 0ms
    Transaction: success 0, failure 0
  Account: request 0, timeouts 0
    Response: unexpected 0, server error 0, incorrect 0, time 0ms
    Transaction: success 0, failure 0
  Elapsed time since counters last cleared: 2h13m

Switch#show aaa method-lists authentication authen queue=AAA_ML_AUTHEN_LOGIN authen
queue=AAA_ML_AUTHEN_ENABLE authen queue=AAA_ML_AUTHEN_PPP authen queue=AAA_ML_AUTHEN_SGBP
authen queue=AAA_ML_AUTHEN_ARAP authen queue=AAA_ML_AUTHEN_EAPOUDP
  name=default valid=1 id=0 state=ALIVE : SERVER_GROUP radius authen
queue=AAA_ML_AUTHEN_DOT1X
  name=default valid=1 id=0 state=ALIVE : SERVER_GROUP radius permanent lists
  name=Permanent Enable None valid=1 id=0 ALIVE : ENABLE NONE
  name=Permanent Enable valid=1 id=0 ALIVE : ENABLE
  name=Permanent None valid=1 id=0 ALIVE : NONE
  name=Permanent Local valid=1 id=0 ALIVE : LOCAL
    
```

NAC 情報の表示



注 アクセス ポイントは次のコマンドをサポートしていません。

NAC 情報を表示するには、次のいずれかの特権 EXEC コマンドを使用します。

表 3 NAC 情報を表示するコマンド

コマンド	目的
<code>show dot1x {all interface interface-id statistics interface interface-id}</code>	IEEE 802.1x 統計情報、管理ステータス、稼動ステータスを表示します。
<code>show eou {all authentication {clientless eap static} interface interface-id ip ip-address mac mac-address posturetoken name}</code>	EAPoUDP 設定またはセッション キャッシュ エントリに関する情報を表示します。
<code>show ip admission [{cache} [configuration] [eapoudp]]</code>	NAC 設定またはアドミッション キャッシュ エントリを表示します。
<code>show ip device tracking {all interface interface-id ip ip-address mac mac-address}</code>	IP デバイス トラッキング テーブルのエントリに関する情報を表示します。

次に、新しいホストが検出されたときのサンプル出力を示します。

```
00:45:15: %EOU-6-SESSION: IP=10.5.0.25 | HOST=DETECTED | Interface=GigabitEthernet1/0/4
00:45:15: %EOU-6-CTA: IP=10.5.0.25 | CiscoTrustAgent=DETECTED
00:45:16: %EOU-6-POLICY: IP=10.5.0.25 | TOKEN=Healthy
00:45:16: %EOU-6-POLICY: IP=10.5.0.25 | URL=http://10.5.0.43
00:45:16: %EOU-6-POLICY: IP=10.5.0.25 | URL ACL=s-acl
00:45:16: %EOU-6-POLICY: IP=10.5.0.25 | ACLNAME=#ACSACL#-IP-Healthy-42dbdd9d
00:45:16: %EOU-6-POLICY: IP=10.5.0.25 | HOSTNAME=CMELTER-XP:dsbu
00:45:16: %EOU-6-POSTURE: IP=10.5.0.25 | HOST=AUTHORIZED | Interface=GigabitEthernet1/0/4
00:45:16: %EOU-6-AUTHTYPE: IP=10.5.0.25 | AuthType=EAP
```

```
Switch# show eou all
```

```
-----
Address      Interface          AuthType    Posture-Token  Age (min)
-----
10.5.0.25   GigabitEthernet1/0/4  EAP         Healthy        0
```

```
Switch# show eou ip 10.5.0.25
```

```
Address          : 10.5.0.25
MAC Address      : 0060.b0f8.fbf8
Interface        : GigabitEthernet1/0/4
AuthType         : EAP
Audit Session ID : 0000000000296E2E000000040A050019
PostureToken     : Healthy
Age (min)        : 0
URL Redirect     : http://10.5.0.43
URL Redirect ACL : s-acl
ACL Name         : #ACSACL#-IP-Healthy-42dbdd9d
User Name        : HOST-XP:dsbu
Revalidation Period : 600 Seconds
Status Query Period : 600 Seconds
Current State    : AUTHENTICATED
```

EAPoUDP セッション テーブルのクリア

EAPoUDP セッション テーブルのクライアント エントリをクリアするには、**clear eou** 特権 EXEC コマンドを使用します。削除されたエントリは、スイッチがホストから ARP パケットを受信するか、ホストの DHCP スヌーピング バインディング エントリを作成するまで作成されません。スイッチの IP デバイス トラッキング テーブルのエントリをクリアするには、**clear ip device tracking** 特権 EXEC コマンドを使用します。

コマンドリファレンス

**注**

アクセス ポイントは、本書のこのセクションのコマンドをサポートしていません。

このセクションでは、Cisco IOS の汎用コマンド以外の NAC レイヤ 2 IP コマンドについて説明します。Cisco IOS の汎用コマンドについては、次の URL を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_8/gt_nac.htm

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/secur_r/sec_p1g.htm

aaa authentication eou

aaa authentication eou グローバル設定コマンドは、スイッチに EAPoUDP (EoU 認証方式を設定するために使用します。認証方式を削除するには、このコマンドの **no** 形式を使用します。

aaa authentication eou default group radius

no aaa authentication eou default

シンタックスの説明

このコマンドに引数またはキーワードはありません。

デフォルト設定

EAPoUDP 認証方式は設定されていません。

コマンドモード

グローバル設定

コマンド履歴

リリース	修正
12.2(18)SXF, 12.2(25)SED, 12.2(25)SG	このコマンドの導入

使用時の考慮点

EAPoUDP 認証方式は、ACL を設定し、IP ネットワーク NAC ルールを定義した後にスイッチに設定できません。また、**aaa authorization auth-proxy default group radius** グローバル設定コマンドを使用すると、認証プロキシ方式も設定できます。

使用例

EAPoUDP 認証方式の設定の例を示します。

```
Switch(config)# aaa authentication eou default group radius
```

show running-config 特権 EXEC コマンドを入力すると、この設定を確認できます。

関連コマンド

コマンド	説明
aaa authorization auth-proxy default	EAPoUDP 認証方式をイネーブルにして設定します。
identity profile eapoudp	アイデンティティ プロファイルを作成し、EAPoUDP プロファイル設定モードに入ります。シンタックス情報を確認するには、 Cisco IOS Software Configuration > Cisco IOS Release 12.3 > New Feature Documentation > 12.3 T New Features and System Messages > New Features in Release 12.3(8)T > Network Admission Control を選択します。
ip admission name eapoudp	IP NAC ルールを作成し、設定します。

コマンド	説明
<code>show ip admission</code>	NAC キャッシュ エントリまたは NAC 設定に関する情報を表示します。シンタックス情報を確認するには、 Cisco IOS Software Configuration > Cisco IOS Release 12.3 > New Feature Documentation > 12.3 T New Features and System Messages > New Features in Release 12.3(8)T > Network Admission Control を選択します。
<code>show running-config</code>	稼働設定を表示します。シンタックス情報を確認するには、 Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands を選択します。

aaa authorization auth-proxy default

aaa authorization auth-proxy default グローバル設定コマンドは、認証プロキシ ポスチャ コードが AAA サーバからセキュリティ アソシエーションを取得するために使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa authorization auth-proxy default group radius

no aaa authorization auth-proxy default



注

コマンドライン ヘルプの文字列には表示されていますが、**cache**、**server-group-name** および **tacacs+** キーワードはサポートされていません。

シンタックスの説明

このコマンドに引数またはキーワードはありません。

デフォルト設定

認証プロキシ ポスチャ コードは、AAA サーバからセキュリティ アソシエーションを取得しません。

コマンドモード

グローバル設定

コマンド履歴

リリース	修正
12.2(18)SXF, 12.2(25)SED, 12.2(25)SG	このコマンドの導入

使用時の考慮点

認証プロキシの認証方式は、ACL を設定し、IP ネットワーク NAC ルールを定義した後に設定します。また、**aaa authentication cou default group radius** グローバル設定コマンドを使用すると、EAPoUDP 認証方式も設定できます。

使用例

AAA サーバからセキュリティ アソシエーションを取得する例を示します。

```
Switch(config)# aaa authorization auth-proxy default group radius
```

show running-config 特権 EXEC コマンドを入力すると、この設定を確認できます。

関連コマンド

コマンド	説明
<code>aaa authentication eou</code>	EAPoUDP 認証方式を設定します。
<code>identity profile eapoudp</code>	アイデンティティ プロファイルを作成し、EAPoUDP プロファイル設定モードに入ります。シンタックス情報を確認するには、 Cisco IOS Software Configuration > Cisco IOS Release 12.3 > New Feature Documentation > 12.3 T New Features and System Messages > New Features in Release 12.3(8)T > Network Admission Control を選択します。
<code>ip admission name eapoudp</code>	IP NAC ルールを作成し、設定します。
<code>show ip admission</code>	NAC キャッシュ エントリまたは NAC 設定に関する情報を表示します。シンタックス情報を確認するには、 Cisco IOS Software Configuration > Cisco IOS Release 12.3 > New Feature Documentation > 12.3 T New Features and System Messages > New Features in Release 12.3(8)T > Network Admission Control を選択します。
<code>show running-config</code>	稼動設定を表示します。シンタックス情報を確認するには、 Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands を選択します。

clear ip admission

clear ip admission 特権 EXEC コマンドは、スイッチの IP アドミッション エントリをクリアするために使用します。

```
clear ip admission {{cache | watch-list} [* | ip-address]}
```

シンタックスの説明

cache	IP アドミッション エントリを削除します。
watch-list	IP アドミッション エントリ ウォッチリスト エントリを削除します。
*	すべてのキャッシュ エントリを削除します。
ip-address	指定した IP アドレスのキャッシュ エントリを削除します。

デフォルト設定

デフォルト設定はありません。

コマンドモード

特権 EXEC

コマンド履歴

リリース	修正
12.2(18)SXF, 12.2(25)SED, 12.2(25)SG	このコマンドの導入

使用例

すべての IP アドミッション キャッシュ エントリをクリアする例を示します。

```
Switch# clear ip admission *
```

show eou または **show ip admission** 特権 EXEC コマンドを入力すると、この設定を確認できます。

関連コマンド

コマンド	説明
ip admission name eapoudp	IP NAC ルールを作成し、設定します。
show eou	EAPoUDP 設定またはセッション キャッシュ エントリに関する情報を表示します。
show ip admission	NAC キャッシュ エントリまたは NAC 設定に関する情報を表示します。シンタックス情報を確認するには、 Cisco IOS Software Configuration > Cisco IOS Release 12.3 > New Feature Documentation > 12.3 T New Features and System Messages > New Features in Release 12.3(8)T > Network Admission Control を選択します。

clear ip device tracking

clear ip device tracking 特権 EXEC コマンドは、スイッチの IP デバイス トラッキング テーブルをクリアするために使用します。

```
clear ip device tracking {all | interface interface-id | ip ip-address | mac mac-address}
```

シンタックスの説明

all	すべての IP デバイス トラッキング エントリを削除します。
interface interface-id	指定したインターフェイスのすべての IP デバイス トラッキング エントリを削除します。
ip ip-address	指定した IP アドレスのすべての IP デバイス トラッキング エントリを削除します。
mac mac-address	指定した MAC アドレスのすべての IP デバイス トラッキング エントリを削除します。

デフォルト設定

デフォルト設定はありません。

コマンドモード

特権 EXEC

コマンド履歴

リリース	修正
12.2(18)SXF, 12.2(25)SED, 12.2(25)SG	このコマンドの導入

使用時の考慮点

clear ip device tracking 特権 EXEC コマンドを使用して IP デバイス トラッキング エントリを削除すると、スイッチは削除されたホストに ARP プローブを送信します。存在しているホストは ARP プローブに応答し、スイッチはこのホストを IP デバイス トラッキング エントリに追加します。

使用例

IP デバイス トラッキング テーブルのすべてのエントリをクリアする例を示します。

```
Switch# clear ip device tracking all
```

show ip device tracking 特権 EXEC コマンドを入力すると、この設定を確認できます。

関連コマンド

コマンド	説明
ip device tracking	IP デバイス トラッキング テーブルをイネーブルにし、IP デバイス トラッキング テーブルのパラメータを設定します。
show ip device tracking	IP デバイス トラッキング テーブルのエントリに関する情報を表示します。

debug eou

debug eou 特権 EXEC コマンドは、EAPoUDP のデバッグをイネーブルにするために使用します。デバッグをディセーブルにするには、このコマンドの no 形式を使用します。

```
debug eou {all | eap | errors | events | obj-create | obj-destroy | obj-link | obj-unlink | packets | ratelimit | sm}
```

```
no debug eou {all | eap | errors | events | obj-create | obj-destroy | obj-unlink | packets | ratelimit | sm}
```

シンタックスの説明

all	すべての EAPoUDP 情報を表示します。
eap	EAPoUDP パケットを表示します。
errors	EAPoUDP パケット エラーに関する情報を表示します。
events	EAPoUDP パケット イベントに関する情報を表示します。
obj-create	作成された EAPoUDP セッションに関する情報を表示します。
obj-destroy	削除された EAPoUDP セッションに関する情報を表示します。
obj-link	ハッシュ テーブルに追加された EAPoUDP セッションに関する情報を表示します。
obj-unlink	ハッシュ テーブルから削除された EAPoUDP セッションに関する情報を表示します。
packets	EAPoUDP パケット情報を表示します。
ratelimit	EAPoUDP ポスチャ検証情報を表示します。
sm	EAPoUDP ステート マシンの移行に関する情報を表示します。

デフォルト設定

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	修正
12.2(18)SXF, 12.2(25)SED, 12.2(25)SG	このコマンドの導入

使用時の考慮点

undebg eou コマンドは、no debug eou コマンドと同じです。

Catalyst 3750 スイッチおよび EtherSwitch サービス モジュールでデバッグをイネーブルにすると、スタック マスターでのみデバッグがイネーブルになります。スタック メンバーでデバッグをイネーブルにするには、**session switch-number** 特権 EXEC コマンドを使用してスタック マスター からセッションを開始し、次にスタック メンバーのコマンドラインプロンプトで **debug** コマンドを入力します。また、スタック マスター スイッチで **remote command stack-member-number LINE** 特権 EXEC コマンドを使用すると、セッションを開始せずにメンバー スイッチでデバッグをイネーブルにできます。

関連コマンド

コマンド	説明
<code>show debugging</code>	イネーブルにされているデバッグのタイプに関する情報を表示します。シンタックス情報を確認するには、 Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2 > System Management > Troubleshooting and Fault Management を選択します。
<code>show eou</code>	EAPoUDP グローバル設定またはセッション キャッシュ エントリに関する情報を表示します。

debug ip admission

debug ip admission 特権 EXEC コマンドは、IP アドミッション イベントのデバッグをイネーブルにするために使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug ip admission {api | dos | eapoudp | function-trace | object-creation | object-deletion | timers}

no debug ip admission {api | dos | eapoudp | function-trace | object-creation | object-deletion | timers}

シンタックスの説明

api	IP アドミッション Application Program Interface (API) イベントを表示します。
dos	認証プロキシ DoS (サービス拒絶) 防止情報を表示します。
eapoudp	EAPoUDP ポスチャ検証イベントに関する情報を表示します。
function-trace	認証プロキシ機能トレースに関する情報を表示します。
object-creation	作成された認証プロキシオブジェクトに関する情報を表示します。
object-deletion	削除された認証プロキシオブジェクトに関する情報を表示します。
timers	認証プロキシタイマーイベントに関する情報を表示します。

デフォルト設定

デバッグはディセーブルです。

コマンドモード

特権 EXEC

コマンド履歴

リリース	修正
12.2(18)SXF, 12.2(25)SED, 12.2(25)SG	このコマンドの導入

使用時の考慮点

undebug ip admission コマンドと **no debug ip admission** コマンドは同じです。

Catalyst 3750 スイッチおよび EtherSwitch サービス モジュールでデバッグをイネーブルにすると、スタック マスターでのみデバッグがイネーブルになります。スタック メンバーでデバッグをイネーブルにするには、**session switch-number** 特権 EXEC コマンドを使用してスタック マスター からセッションを開始し、次にスタック メンバーのコマンドラインプロンプトで **debug** コマンドを入力します。また、スタック マスター スイッチで **remote command stack-member-number LINE** 特権 EXEC コマンドを使用すると、セッションを開始せずにメンバー スイッチでデバッグをイネーブルにできます。

関連コマンド

コマンド	説明
<code>show debugging</code>	イネーブルにされているデバッグのタイプに関する情報を表示します。シンタックス情報を確認するには、 Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2 > System Management > Troubleshooting and Fault Management を選択します。
<code>show eou</code>	EAPoUDP グローバル設定またはセッション キャッシュ エントリに関する情報を表示します。
<code>show ip admission</code>	NAC キャッシュ エントリまたは NAC 設定に関する情報を表示します。シンタックス情報を確認するには、 Cisco IOS Software Configuration > Cisco IOS Release 12.3 > New Feature Documentation > 12.3 T New Features and System Messages > New Features in Release 12.3(8)T > Network Admission Control を選択します。

debug ip device tracking

debug ip device tracking 特権 EXEC コマンドは、スイッチ ポートで NAC のデバッグをイネーブルするために使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug ip device tracking {all | events | obj-create | obj-destroy | redundancy}

no debug ip device tracking {all | events | obj-create | obj-destroy | redundancy}

シンタックスの説明

all	すべての EAPoUDP 情報を表示します。
events	EAPoUDP パケット イベントに関する情報を表示します。
obj-create	作成された EAPoUDP セッションに関する情報を表示します。
obj-destroy	削除された EAPoUDP セッションに関する情報を表示します。
redundancy	EAPoUDP セッションのスタンドバイ スーパーバイザ エンジンの SSO ステータスに関する情報を表示します。
	注 このキーワードは、Catalyst 4500 シリーズ スイッチでのみ使用できます。

デフォルト設定

デバッグはディセーブルです。

コマンドモード

特権 EXEC

コマンド履歴

リリース	修正
12.2(18)SXF, 12.2(25)SED, 12.2(25)SG	このコマンドの導入

使用時の考慮点

undebug ip device tracking コマンドと **no debug ip device tracking** コマンドは同じです。

Catalyst 3750 スイッチおよび EtherSwitch サービス モジュールでデバッグをイネーブルにすると、スタック マスターでのみデバッグがイネーブルになります。スタック メンバーでデバッグをイネーブルにするには、**session switch-number** 特権 EXEC コマンドを使用してスタック マスターからセッションを開始し、次にスタック メンバーのコマンドラインプロンプトで **debug** コマンドを入力します。また、スタック マスター スイッチで **remote command stack-member-number LINE** 特権 EXEC コマンドを使用すると、セッションを開始せずにメンバー スイッチでデバッグをイネーブルにできます。

debug sw-ip-admission

debug sw-ip-admission 特権 EXEC コマンドは、ARP および DHCP バインディング イベントなど、スイッチ固有の NAC レイヤ 2 IP 処理のデバッグをイネーブルにするために使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

```
debug sw-ip-admission [packet]
```

```
no debug sw-ip-admission [packet]
```

シンタックスの説明

packet (オプション)	NAC レイヤ 2 IP ホストの追跡に使用するパケットのデバッグをイネーブルにします。
-----------------------	--

シンタックスの説明

このコマンドに引数またはキーワードはありません。

デフォルト設定

デバッグはディセーブルにされています。

コマンドモード

特権 EXEC

コマンド履歴

リリース	修正
12.2(18)SXF, 12.2(25)SED, 12.2(25)SG	このコマンドの導入

使用時の考慮点

undebug sw-ip-admission コマンドは **no debug sw-ip-admission** コマンドと同じです。

Catalyst 3750 スイッチおよび EtherSwitch サービス モジュールでデバッグをイネーブルにすると、スタック マスターでのみデバッグがイネーブルになります。スタック メンバーでデバッグをイネーブルにするには、**session switch-number** 特権 EXEC コマンドを使用してスタック マスターからセッションを開始し、次にスタック メンバーのコマンドラインプロンプトで **debug** コマンドを入力します。また、スタック マスター スイッチで **remote command stack-member-number LINE** 特権 EXEC コマンドを使用すると、セッションを開始せずにメンバー スイッチでデバッグをイネーブルにできます。

関連コマンド

コマンド	説明
show debugging	イネーブルにされているデバッグのタイプに関する情報を表示します。シンタックス情報を確認するには、 Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2 > System Management > Troubleshooting and Fault Management を選択します。
show eou	EAPoUDP グローバル設定またはセッション キャッシュ エントリに関する情報を表示します。

コマンド	説明
<code>show ip admission</code>	NAC キャッシュ エントリまたは NAC 設定に関する情報を表示します。シンタックス情報を確認するには、 Cisco IOS Software Configuration > Cisco IOS Release 12.3 > New Feature Documentation > 12.3 T New Features and System Messages > New Features in Release 12.3(8)T > Network Admission Control を選択します。

description

description アイデンティティ ポリシー設定モード コマンドは、アイデンティティ ポリシーの説明を入力するために使用します。説明をクリアするには、このコマンドの **no** 形式を使用します。

description *line-of-description* [*line-of-description*] [*line-of-description*] ...

no description *line-of-description* [*line-of-description*] [*line-of-description*] ...

シンタックスの説明

line-of-description アイデンティティ ポリシーの説明を入力します。

デフォルト設定

説明は設定されていません。

コマンドモード

アイデンティティ ポリシー設定

コマンド履歴

リリース	修正
12.2(18)SXF, 12.2(25)SED, 12.2(25)SG	このコマンドの導入

使用時の考慮点

アイデンティティ ポリシーの説明として、複数行の文字列を入力できます。

使用例

policy 100 と呼ばれるアイデンティティ ポリシーの説明を入力する例を示します。

```
Switch(config)# identity policy policy100
Switch(config-identity-policy)# description Admin policy for the engineering group
```

show running-config 特権 EXEC コマンドを入力すると、この設定を確認できます。

関連コマンド

コマンド	説明
description (アイデンティティ プロファイル設定)	アイデンティティ ポリシーの説明を入力します。シンタックス情報を確認するには、 Cisco IOS Software Configuration > Cisco IOS Release 12.3 > New Feature Documentation > 12.3 T New Features and System Messages > New Features in Release 12.3(8)T > Network Admission Control を選択します。
show running-config	稼動設定を表示します。シンタックス情報を確認するには、 Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands を選択します。

device

device アイデンティティ プロファイル設定モード コマンドは、デバイスを手動で許可または拒否するために使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
device {authorize | not-authorize} {ip-address ip-address | mac-address mac-address | type cisco ip phone}
[policy policy-name]
```

```
no device {authorize | not-authorize} {ip-address ip-address | mac-address mac-address | type cisco ip
phone} [policy policy-name]
```

シンタックスの 説明

authorize	許可するデバイスを設定します。
not-authorize	許可しないデバイスを設定します。
ip-address ip-address	デバイスの IP アドレスを指定します。
mac-address mac-address	デバイスの MAC アドレスを指定します。
type cisco ip phone	デバイスを Cisco IP Phone に指定します。
policy policy-name	デバイスに適用するポリシーを指定します。

デフォルト設定

デバイスは、手動で許可または拒否されません。

コマンドモード

アイデンティティ プロファイル設定

コマンド履歴

リリース	修正
12.2(18)SXF, 12.2(25)SED, 12.2(25)SG	このコマンドの導入

使用時の考慮点

device アイデンティティ プロファイル設定コマンドを使用する前に、**identity profile {default | dot1x | eapoudp}** グローバル設定コマンドを使用してアイデンティティ プロファイルを作成する必要があります。

使用例

MAC アドレス 1234.abcd.5678 のデバイスをローカル ポリシー policy1 を使用して静的に許可する例を示します。

```
Switch(config)# identity profile eapoudp
Switch(config-identity-prof)# device authorize mac-address 1234.abcd.4578 policy policy1
```

show running-config 特権 EXEC コマンドを入力すると、この設定を確認できます。

関連コマンド

コマンド	説明
access-group (アイデンティティ ポリシー)	アイデンティティ ポリシーを適用するアクセス グループを指定します。シンタックス情報を確認するには、 Cisco IOS Software Configuration > Cisco IOS Release 12.3 > New Feature Documentation > 12.3 T New Features and System Messages > New Features in Release 12.3(8)T > Network Admission Control を選択します。
identity profile eapoudp	アイデンティティ プロファイルを作成し、EAPoUDP プロファイル設定モードに入ります。シンタックス情報を確認するには、 Cisco IOS Software Configuration > Cisco IOS Release 12.3 > New Feature Documentation > 12.3 T New Features and System Messages > New Features in Release 12.3(8)T > Network Admission Control を選択します。
show running-config	稼動設定を表示します。シンタックス情報を確認するには、 Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands を選択します。

eou initialize

eou initialize 特権 EXEC コマンドは、EAPoUDP ステート マシンを手動でリセットするために使用します。

```
eou initialize {all | authentication {clientless | eap | static} | interface interface-id | ip ip-address |
  mac mac-address | posturetoken name}
```

シンタックスの 説明

all	すべての EAPoUDP クライアントを再検証します。
authentication	次のいずれかの EAPoUDP 認証タイプを再検証します。 <ul style="list-style-type: none"> • clientless — エンドポイントシステムで CTA ソフトウェアが稼動していない • eap — 認証タイプが EAP • static — 認証タイプが静的に設定されている
interface <i>interface-id</i>	指定したインターフェイス上の EAPoUDP クライアントを再検証します。
ip <i>ip-address</i>	指定した IP アドレスの EAPoUDP クライアントを再検証します。
mac <i>mac-address</i>	指定した MAC アドレスの EAPoUDP クライアントを再検証します。
posturetoken <i>name</i>	指定したポストチャ トークンを持つ EAPoUDP クライアントを再検証します。

デフォルト設定

デフォルト設定はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	修正
12.2(18)SXF, 12.2(25)SED, 12.2(25)SG	このコマンドの導入

使用時の考慮点

eou initialize 特権 EXEC コマンドを入力すると、設定されている EAPoUDP セッションはリセットされます。

使用例

すべての EAPoUDP アソシエーションのリセットを開始する例を示します。

```
Switch# eou initialize
```

show eou 特権 EXEC コマンドを入力すると、この設定を確認できます。

関連コマンド

コマンド	説明
<code>eou revalidate</code> (グローバルおよび インターフェイス設定)	スイッチまたは指定したインターフェイス上の EAPoUDP アソシエーションの再検証をイネーブルにします。
<code>eou revalidate</code> (特権 EXEC)	EAPoUDP アソシエーションの再検証を手動で開始します。
<code>show eou</code>	EAPoUDP 設定またはセッション キャッシュ エントリに関する情報を表示します。

eou max-retry (グローバルおよびインターフェイス設定)

eou max-retry グローバル設定およびインターフェイス設定コマンドは、EAPoUDP 再検証の試行回数を指定するために使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

eou max-retry *number*

no eou max-retry

シンタックスの説明

<i>number</i>	スイッチが EAPoUDP アソシエーションの再検証を試行する回数を 1 ~ 3 の範囲で指定します。
---------------	---

デフォルト設定

デフォルトの再検証試行回数は 3 回です。

コマンドモード

グローバル設定およびインターフェイス設定

コマンド履歴

リリース	修正
12.2(18)SXF, 12.2(25)SED, 12.2(25)SG	このコマンドの導入

使用時の考慮点

再検証の試行回数は、**eou max-retry number** グローバル設定コマンドを使用して設定できます。特定のインターフェイスの再検証試行回数は、**eou max-retry number** インターフェイス設定コマンドを使用して設定できます。

使用例

スイッチ全体の再検証試行回数を 2 回に設定する例を示します。

```
Switch(config)# eou max-retry 2
```

インターフェイスの再検証試行回数を 1 回に設定する例を示します。

```
Switch(config-if)# eou max-retry 1
```

show eou 特権 EXEC コマンドを入力すると、この設定を確認できます。

関連コマンド

コマンド	説明
show eou	EAPoUDP 設定またはセッション キャッシュ エントリに関する情報を表示します。

eou ratelimit

eou ratelimit グローバル設定コマンドは、EAPoUDP ポスチャ検証の同時実行数を指定するために使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

eou ratelimit number

no eou ratelimit

シンタックスの説明

<i>number</i>	同時に検証するクライアント数を 0 ～ 200 の範囲で指定します。
---------------	------------------------------------

デフォルト設定

デフォルト値は 20 クライアントです。

コマンドモード

グローバル設定

コマンド履歴

リリース	修正
12.2(18)SXF, 12.2(25)SED, 12.2(25)SG	このコマンドの導入

使用時の考慮点

eou rate-limit 0 コマンドを入力すると、レート制限機能はディセーブルになります。

同時に検証するクライアント数を 100 に設定しているときにスイッチに 101 のクライアントが接続すると、最後のクライアント (クライアント 101) のポスチャ検証は、別のクライアントが EAPoUDP セッションを終了するまで開始されません。

デフォルト設定に戻すには、**eou default** または **no eou ratelimit** グローバル設定コマンドを使用します。

使用例

検証を同時に実行するクライアント数を 40 に設定する例を示します。

```
Switch(config)# eou ratelimit 40
```

デフォルト設定の 20 クライアントに戻す例を示します。

```
Switch(config-if)# eou default
```

show eou 特権 EXEC コマンドを入力すると、この設定を確認できます。

関連コマンド

コマンド	説明
<code>eou default</code>	グローバル EAPoUDP パラメータをデフォルト設定にリセットします。シンタックス情報を確認するには、 Cisco IOS Software Configuration > Cisco IOS Release 12.3 > New Feature Documentation > 12.3 T New Features and System Messages > New Features in Release 12.3(8)T > Network Admission Control を選択します。
<code>show eou</code>	EAPoUDP 設定またはセッション キャッシュ エントリに関する情報を表示します。

eou revalidate (グローバルおよびインターフェイス設定)

eou revalidate グローバル設定およびインターフェイス設定コマンドは、EAPoUDP アソシエーションの再検証をイネーブルにするために使用します。

eou revalidate

シンタックスの説明

このコマンドに引数またはキーワードはありません。

デフォルト設定

デフォルト設定はありません。

コマンドモード

グローバル設定およびインターフェイス設定

コマンド履歴

リリース	修正
12.2(18)SXF, 12.2(25)SED, 12.2(25)SG	このコマンドの導入

使用時の考慮点

スイッチの EAPoUDP アソシエーションの再検証は、**eou revalidate** グローバル設定コマンドを使用してイネーブルにできます。また、**eou revalidate** インターフェイス設定コマンドを使用すると、インターフェイスの EAPoUDP アソシエーションの再検証をイネーブルにできます。

再検証タイマーの値は、AAA が稼動する Cisco Secure ACS から送信される Access-Accept メッセージの Session-Timeout RADIUS アトリビュート (Attribute[27]) および Termination-Action RADIUS アトリビュート (Attribute[29]) に基づいています。スイッチが Session-Timeout 値を受け取ると、この値により、スイッチに設定されている再検証タイマーの値は無効になります。

再検証タイマーが失効すると、スイッチは Termination-Action アトリビュートの値に基づいて次のようなアクションを実行します。

- Termination-Action RADIUS アトリビュート値が Default の場合、スイッチがセッションの再検証を開始するまでセッションは終了します。
- スイッチが Default 以外の Termination-Action アトリビュート値を受け取ると、ポスチャの再検証中も EAPoUDP セッションが継続され、現在のアクセス ポリシーが適用されます。
- Termination-Action アトリビュートの値が RADIUS の場合、スイッチはクライアントを再検証します。
- サーバから送信されるパケットに Termination-Action アトリビュートが含まれていない場合、EAPoUDP セッションは終了し、スイッチはポスチャ検証を再度開始します。

使用例

EAPoUDP アソシエーションのグローバルな再検証を開始する例を示します。

```
Switch(config)# eou revalidate
```

インターフェイス上で EAPoUDP アソシエーションの再検証を開始する例を示します。

```
Switch(config)# interface gigabitethernet 1/0/1
Switch(config-if)# eou revalidate
```

show eou 特権 EXEC コマンドを入力すると、この設定を確認できます。

関連コマンド

コマンド	説明
eou initialize	EAPoUDP ステート マシンを手動でリセットします。
eou allow (グローバル設定および インターフェイス設定)	追加の EAPoUDP オプションを許可します。シンタックス情報を確認するには、 Cisco IOS Software Configuration > Cisco IOS Release 12.3 > New Feature Documentation > 12.3 T New Features and System Messages > New Features in Release 12.3(8)T > Network Admission Control を選択します。
eou logging	EAPoUDP システム イベントのロギングをイネーブルにします。シンタックス情報を確認するには、 Cisco IOS Software Configuration > Cisco IOS Release 12.3 > New Feature Documentation > 12.3 T New Features and System Messages > New Features in Release 12.3(8)T > Network Admission Control を選択します。
eou port	EAPoUDP の UDP ポートを設定します。シンタックス情報を確認するには、 Cisco IOS Software Configuration > Cisco IOS Release 12.3 > New Feature Documentation > 12.3 T New Features and System Messages > New Features in Release 12.3(8)T > Network Admission Control を選択します。
eou revalidate (特権 EXEC)	EAPoUDP アソシエーションの再検証を手動で開始します。
show eou	EAPoUDP 設定またはセッション キャッシュ エントリに関する情報を表示します。

eou revalidate (特権 EXEC)

eou revalidate 特権 EXEC コマンドは、EAPoUDP アソシエーションの再検証を手動で開始するために使用します。

```
eou revalidate {all | authentication {clientless | eap | static} | interface interface-id | ip ip-address
               | mac mac-address | posturtoken name}
```

シンタックスの説明

all	すべての EAPoUDP クライアントを再検証します。
authentication	次のいずれかの EAPoUDP 認証タイプを再検証します。 <ul style="list-style-type: none"> clientless — エンドポイント システムで CTA ソフトウェアが稼動していない eap — 認証タイプが EAP static — 認証タイプが静的に設定されている
interface interface-id	指定したインターフェイス上の EAPoUDP クライアントを再検証します。
ip ip-address	指定した IP アドレスの EAPoUDP クライアントを再検証します。
mac mac-address	指定した MAC アドレスの EAPoUDP クライアントを再検証します。
posturtoken name	指定したポストチャ トークンを持つ EAPoUDP クライアントを再検証します。

デフォルト設定

デフォルト設定はありません。

コマンドモード

特権 EXEC

コマンド履歴

リリース	修正
12.2(18)SXF, 12.2(25)SED, 12.2(25)SG	このコマンドの導入

使用時の考慮点

eou revalidate 特権 EXEC コマンドは、スイッチ上の EAPoUDP アソシエーションの再検証を手動で開始するときに使用します。

使用例

すべての EAPoUDP クライアントの再検証を開始する例を示します。

```
Switch# eou revalidate all
```

特定のインターフェイス上の EAPoUDP クライアントの再検証を開始する例を示します。

```
Switch# eou revalidate interface gigabitethernet 1/0/2
```

show eou 特権 EXEC コマンドを入力すると、この設定を確認できます。

関連コマンド

コマンド	説明
<code>eou initialize</code>	EAPoUDP ステート マシンを手動でリセットします。
<code>eou revalidate</code> (グローバルおよび インターフェイス設定)	スイッチまたは指定したインターフェイス上の EAPoUDP アソシエーションの再検証をイネーブルにします。
<code>show eou</code>	EAPoUDP 設定またはセッション キャッシュ エントリに関する情報を表示します。

eou timeout (グローバルおよびインターフェイス設定)

eou timeout グローバル設定およびインターフェイス設定コマンドは、EAPoUDP タイマーの設定に使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

```
eou timeout {aaa seconds | hold-period seconds | retransmit seconds | revalidation seconds | status-query seconds}
```

```
no eou timeout {aaa | hold-period | retransmit | revalidation | status-query}
```

シンタックスの説明

aaa seconds	スイッチが AAA サーバへのパケットの再送信まで待機する期間 (秒) を 1 ~ 60 の範囲で設定します。
hold-period seconds	認証の試行に失敗した後に、スイッチがホストの再認証を開始するまで待機する期間 (秒) を 60 ~ 86400 の範囲で設定します。
retransmit seconds	スイッチがアンチウイルス状態の要求を再送信する前にクライアントからの応答を待機する期間 (秒) を 1 ~ 60 の範囲で設定します。
revalidation seconds	ポスチャ検証中に EAPoUDP メッセージを使用したクライアントに NAC ポリシーを適用する期間 (秒) を 5 ~ 86400 の範囲で設定します。
status-query seconds	前回検証されたクライアントが現在も存在し、ポスチャが変更されていないことの確認を開始するまでスイッチが待機する期間 (秒) を 10 ~ 1800 の範囲で設定します。

デフォルト設定

デフォルトの AAA 時間は 60 秒 (1 分) です。
 デフォルトの保留時間は 180 秒 (3 分) です。
 デフォルトの再送信時間は 3 秒です。
 デフォルトの再検証時間は 600 分 (10 時間) です。
 デフォルトのステータス クエリー時間は 300 秒 (5 分) です。

コマンドモード

グローバル設定およびインターフェイス設定

コマンド履歴

リリース	修正
12.2(18)SXF, 12.2(25)SED, 12.2(25)SG	このコマンドの導入

使用時の考慮点

スイッチのグローバルな EAPoUDP タイマーは、**eou timeout** グローバル設定コマンドを使用して設定できます。また、特定のインターフェイスの EAPoUDP タイマーは、**eou timeout** インターフェイス設定コマンドを入力して設定できます。

EAPoUDP タイマーの詳細な情報については、14 ページの「NAC タイマー」のセクションを参照してください。

使用例

スイッチ全体の再送信タイマーを 45 秒に設定する例を示します。

```
Switch(config)# eou timeout retransmit 45
```

インターフェイスの再検証タイマーを 800 秒に設定する例を示します。

```
Switch(config-if)# eou timeout revalidation 800
```

show eou 特権 EXEC コマンドを入力すると、この設定を確認できます。

関連コマンド

コマンド	説明
eou default	グローバル EAPoUDP パラメータをデフォルト設定にリセットします。シンタックス情報を確認するには、 Cisco IOS Software Configuration > Cisco IOS Release 12.3 > New Feature Documentation > 12.3 T New Features and System Messages > New Features in Release 12.3(8)T > Network Admission Control を選択します。
eou allow (グローバル設定および インターフェイス設定)	追加の EAPoUDP オプションを許可します。シンタックス情報を確認するには、 Cisco IOS Software Configuration > Cisco IOS Release 12.3 > New Feature Documentation > 12.3 T New Features and System Messages > New Features in Release 12.3(8)T > Network Admission Control を選択します。
eou logging	EAPoUDP システム イベントのロギングをイネーブルにします。シンタックス情報を確認するには、 Cisco IOS Software Configuration > Cisco IOS Release 12.3 > New Feature Documentation > 12.3 T New Features and System Messages > New Features in Release 12.3(8)T > Network Admission Control を選択します。
eou port	EAPoUDP の UDP ポートを設定します。シンタックス情報を確認するには、 Cisco IOS Software Configuration > Cisco IOS Release 12.3 > New Feature Documentation > 12.3 T New Features and System Messages > New Features in Release 12.3(8)T > Network Admission Control を選択します。
show eou	EAPoUDP 設定またはセッション キャッシュ エントリに関する情報を表示します。

identity policy

identity policy グローバル設定モードは、アイデンティティ ポリシーを作成し、EAPoUDP ポリシー設定モードに入るために使用します。ポリシーを削除するには、このコマンドの **no** 形式を使用します。

identity policy *policy-name*

no identity policy *policy-name*

シンタックスの説明

<i>policy-name</i>	EAPoUDP ポリシー名を指定します。
--------------------	----------------------

デフォルト設定

EAPoUDP ポリシーは作成されていません。

コマンドモード

グローバル設定

コマンド履歴

リリース	修正
12.2(18)SXF, 12.2(25)SED, 12.2(25)SG	このコマンドの導入

使用時の考慮点

IP アドレス、MAC アドレス、またはデバイス タイプに基づいてデバイスを手動で認証したあとに、**identity policy** *policy-name* グローバル設定モードを使用して、デバイスに適用するポリシーを定義できます。詳しい情報については、「NAC の設定」の章の「アイデンティティ プロファイルとポリシーの設定」を参照してください。

使用例

アイデンティティ ポリシーを作成し、EAPoUDP ポリシー設定モードに入る例を示します。

```
Switch(config)# identity policy policy11
```

show running-config 特権 EXEC コマンドを入力すると、この設定を確認できます。

関連コマンド

コマンド	説明
access-group (アイデンティティ ポリシー)	アイデンティティ ポリシーを適用するアクセス グループを指定します。シンタックス情報を確認するには、 Cisco IOS Software Configuration > Cisco IOS Release 12.3 > New Feature Documentation > 12.3 T New Features and System Messages > New Features in Release 12.3(8)T > Network Admission Control を選択します。
identity profile eapoudp	アイデンティティ プロファイルを作成し、EAPoUDP プロファイル設定モードに入ります。シンタックス情報を確認するには、 Cisco IOS Software Configuration > Cisco IOS Release 12.3 > New Feature Documentation > 12.3 T New Features and System Messages > New Features in Release 12.3(8)T > Network Admission Control を選択します。
show running-config	稼動設定を表示します。シンタックス情報を確認するには、 Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands を選択します。

ip admission name eapoudp

ip admission name eapoudp グローバル設定コマンドは、IP NAC ルールを作成するために使用します。ルールを削除するには、このコマンドの **no** 形式を使用します。

ip admission name *rule-name* eapoudp

no ip admission name *rule-name* eapoudp

シンタックスの説明

rule-name	IP NAC ルール名を指定します。
------------------	--------------------

デフォルト設定

IP NAC ルールは設定されていません。

コマンド モード

グローバル設定

コマンド履歴

リリース	修正
12.2(18)SXF, 12.2(25)SED, 12.2(25)SG	このコマンドの導入

使用時の考慮点

IP NAC ルールは、NAC の適用方法を定義します。

IP NAC ルールをエッジ スイッチのアクセス ポートに適用するときは、**ip admission admission-name** インターフェイス設定コマンドを使用します。

使用例

rule 11 という名前の IP NAC ルールを作成する例を示します。

```
Switch(config)# ip admission name rule11 eapoudp
```

show ip admission 特権 EXEC コマンドを入力すると、この設定を確認できます。

関連コマンド

コマンド	説明
clear eou	スイッチ、または特定のインターフェイスのすべての NAC クライアント デバイス エントリをクリアします。シンタックス情報を確認するには、 Cisco IOS Software Configuration > Cisco IOS Release 12.3 > New Feature Documentation > 12.3 T New Features and System Messages > New Features in Release 12.3(8)T > Network Admission Control を選択します。
ip admission admission-name (インターフェイス設定)	特定のインターフェイスに適用する NAC ルールを作成します。シンタックス情報を確認するには、 Cisco IOS Software Configuration > Cisco IOS Release 12.3 > New Feature Documentation > 12.3 T New Features and System Messages > New Features in Release 12.3(8)T > Network Admission Control を選択します。

コマンド	説明
<code>show eou</code>	EAPoUDP グローバル設定またはセッション キャッシュ エントリに関する情報を表示します。
<code>show ip admission</code>	NAC キャッシュ エントリまたは NAC 設定に関する情報を表示します。シンタックス情報を確認するには、 Cisco IOS Software Configuration > Cisco IOS Release 12.3 > New Feature Documentation > 12.3 T New Features and System Messages > New Features in Release 12.3(8)T > Network Admission Control を選択します。

ip admission name eapoudp bypass

ip admission name eapoudp bypass グローバル設定コマンドは、EAPoUDP (EoU) バイパス機能をイネーブルにし、設定するために使用します。ルールを削除するには、このコマンドの **no** 形式を使用します。

```
ip admission name rule-name eapoudp bypass {auth-cache-list cache-time [list {acl-name | acl-number}] |
list {access-list-name | access-list-number}}
```

```
no ip admission name rule-name eapoudp
```

シンタックスの説明

rule-name	IP NAC ルール名を指定します。
auth-cache-list cache-time	認証キャッシュ エントリが失効するまでの時間を 1 ~ 135791 分の範囲で指定します。デフォルトは 60 分です。
list {acl-name acl-number}	認証プロキシに適用する標準または拡張 ACL 名または番号を指定します。 auth-cache-time cache-time キーワードの後に入力する場合、これらのキーワードはオプションです。 注 このオプションは、Catalyst 6500 シリーズ スイッチおよび Catalyst 7600 シリーズ ルータではサポートされていません。

デフォルト設定

EoU バイパスはディセーブルにされています。

コマンドモード

グローバル設定

コマンド履歴

リリース	修正
12.2(18)SXF, 12.2(25)SED, 12.2(25)SG	このコマンドの導入

使用時の考慮点

EoU バイパスをイネーブルにすると、スイッチはホストにコンタクトしてアンチウイルスの状態を要求する代わりに、ホストの IP アドレス、MAC アドレス、サービスタイプ、EAPoUDP セッション ID を含む要求を Cisco Secure Access Control Server(ACS) に送信します。Cisco Secure ACS は、アクセス制御の決定を下し、スイッチにポリシーを送信します。

指定したルールは、ACL と関連付け、NAC で認証するホストを制御することができます。標準の ACL が設定されていない場合、スイッチは NAC ルールを使用して NAC 対応ポートに接続されているすべてのホストからの IP トラフィックを代行受信します。

auth-cache-time cache-time キーワードを使用すると、キャッシュ エントリが失効してホストの再検証が必要となる時間を指定できます。

list {acl-name | acl-number} キーワードを使用すると、NAC ルールに関連付ける ACL 名および ACL 番号を指定できます。IP 接続が ACL 内のホストから開始されると、最初の接続要求は NAC 機能によって代行受信されます。

使用例

EoU バイパスをイネーブルにし、番号付きの ACL と関連付ける例を示します。スイッチは、ACL に一致するパケットを許可する代わりに、NAC を使用して ACL に一致する IP トラフィックのアンチウイルスの状態を検証します。

```
Switch(config)# ip admission name rule11 eapoudp bypass list 101
```

EoU バイパスをイネーブルにし、キャッシュ エントリ タイマーを指定する例を示します。

```
Switch(config)# ip admission name rule11 eapoudp bypass auth-cache-time 30
```

EoU バイパスをディセーブルにする例を示します。

```
Switch(config)# ip admission name rule11 eapoudp bypass
```

show ip admission 特権 EXEC コマンドを入力すると、この設定を確認できます。

関連コマンド

コマンド	説明
clear eou	スイッチ、または特定のインターフェイスのすべての NAC クライアント デバイス エントリをクリアします。シンタックス情報を確認するには、 Cisco IOS Software Configuration > Cisco IOS Release 12.3 > New Feature Documentation > 12.3 T New Features and System Messages > New Features in Release 12.3(8)T > Network Admission Control を選択します。
show eou	EAPoUDP グローバル設定またはセッション キャッシュ エントリに関する情報を表示します。
show ip admission	NAC キャッシュ エントリまたは NAC 設定に関する情報を表示します。シンタックス情報を確認するには、 Cisco IOS Software Configuration > Cisco IOS Release 12.3 > New Feature Documentation > 12.3 T New Features and System Messages > New Features in Release 12.3(8)T > Network Admission Control を選択します。

ip device tracking

ip device tracking グローバル設定コマンドは、IP デバイス トラッキング機能をイネーブルにし、IP デバイス トラッキング テーブルパラメータを設定するために使用します。この機能をディセーブルにし、デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
ip device tracking [probe {count count | interval interval}]
```

```
no ip device tracking [probe {count | interval}]
```

シンタックスの説明

probe	(オプション) IP デバイス トラッキング テーブルのパラメータを設定します。
count count	スイッチが IP デバイス トラッキング テーブルからエントリを削除する前に、エントリに ARP プローブを送信する回数を 1 ~ 5 の範囲で設定します。
interval interval	スイッチが ARP プローブを再送信するまでに待機する秒数を 30 ~ 300 の範囲で設定します。

デフォルト設定

IP デバイス トラッキングは、ディセーブルにされています。

スイッチからエントリへの ARP プローブ送信回数のデフォルト値は 3 です。

スイッチが ARP プローブ再送信までに待機する秒数のデフォルト値は 30 秒です。

コマンドモード

グローバル設定

コマンド履歴

リリース	修正
12.2(18)SXF, 12.2(25)SED, 12.2(25)SG	このコマンドの導入

使用時の考慮点

IP デバイス トラッキング機能と IP デバイス トラッキング テーブルの情報については、14 ページの「NAC タイマー」を参照してください。

IP デバイス トラッキングをイネーブルにする例を示します。

```
Switch(config)# ip device tracking
```

スイッチの ARP プローブ送信回数を 4 に設定する例を示します。

```
Switch(config)# ip device tracking probe count 4
```

show ip device tracking 特権 EXEC コマンドを入力すると、この設定を確認できます。

関連コマンド

コマンド	説明
<code>clear ip device tracking</code>	スイッチの IP デバイス トラッキング テーブルのエントリをクリアします。
<code>show ip device tracking</code>	IP デバイス トラッキング テーブルのエントリに関する情報を表示します。

mls rate-limit layer2 ip-admission



注

このコマンドは、Catalyst 6500 スイッチ、および Catalyst 7600 ルータに固有のコマンドです。

mls rate-limit layer2 ip ip-admission グローバル設定コマンドは、ハードウェア レートリミッタで (CPU にリダイレクトする) IP アドミッション レイヤ 2 トラフィックのレート制限を行うために使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

```
mls rate-limit layer2 ip ip-admission pps [burst]
```

```
no mls rate-limit layer2 ip ip-admission
```

シンタックスの説明

<i>pps</i>	1 秒当たりのレート制限パケット数を 10 ~ 1000000 の範囲で設定します。
<i>burst</i>	(オプション) バーストで許可する最大パケット数を 1 ~ 255 の範囲で設定します。 このキーワードが設定されない場合、バーストの値は 10 に設定されます。

デフォルト設定

レート制限はイネーブルにされていません。

コマンドモード

特権 EXEC

コマンド履歴

リリース	修正
12.2(18)SXF, 12.2(25)SED, 12.2(25)SG	このコマンドの導入

使用時の考慮点

NAC レートリミッタは、デフォルトでオフにされているため、シナリオと一致するすべてのパケットは RP に送信されます。

使用例

パケット レートを 1 秒あたり 1000 パケット、バースト レートを最大 100 パケットに設定する例を示します。

```
Switch(config)# mls rate-limit layer2 ip-admission 1000 100
```

radius-server attribute 8

radius-server attribute 8 グローバル設定モードは、スイッチが Access-Request または Accounting-Request パケットで Framed-IP-Address RADIUS アトリビュート (Attribute[8]) を送信するように設定するために使用します。スイッチがこの RADIUS アトリビュート (Attribute[8]) を送信しないように設定するには、このコマンドの **no** 形式を使用します。

radius-server attribute 8 include-in-access-req

no radius-server attribute 8 include-in-access-req

シンタックスの説明

このコマンドにキーワードまたは引数はありません。

デフォルト設定

スイッチは、RADIUS Access-Request または Accounting-Request パケットで Framed-IP-Address RADIUS アトリビュート (Attribute[8]) を送信しません。

コマンドモード

グローバル設定

コマンド履歴

リリース	修正
12.2(18)SXF, 12.2(25)SED, 12.2(25)SG	このコマンドの導入

使用時の考慮点

スイッチが非応答ホスト (NAC エージェントレス ホスト) のポスチャを検証するときは、**radius-server attribute 8 include-in-access-req** グローバル設定コマンドを使用する必要があります。

radius-server attribute 8 include-in-access-req グローバル設定コマンドを入力すると、スイッチは RADIUS Access-Request または Accounting-Request パケットで Framed-IP-Address RADIUS アトリビュートを送信します。

使用例

スイッチが Access-Request または Accounting-Request パケットで Framed-IP-Address RADIUS アトリビュート (Attribute[8]) を送信するように設定する例を示します。

```
Switch(config)# radius-server attribute 8 include-in-access-req
```

show eou 特権 EXEC コマンドを入力すると、この設定を確認できます。

関連コマンド

コマンド	説明
show eou	EAPoUDP 設定またはセッション キャッシュ エントリに関する情報を表示します。

redirect

redirect 設定モードは、スイッチがクライアントをリダイレクトする URL を指定するために使用します。URL を削除するには、このコマンドの **no** 形式を使用します。

```
redirect url url [match acl-name]
```

```
no redirect url url [match]
```



注

このコマンドは、Catalyst 3750、3560、2970、2960 スイッチおよび Cisco EtherSwitch サービス モジュールではサポートされていません。

シンタックスの説明

<i>url</i>	クライアントのリダイレクト先の URL を指定します。
match <i>acl-name</i>	指定した ACL に一致するトラフィックをこの URL にリダイレクトするように指定します。

デフォルト設定

URL および ACL は設定されていません。

コマンドモード

アイデンティティ ポリシー設定

コマンド履歴

リリース	修正
12.2(18)SXF, 12.2(25)SED, 12.2(25)SG	このコマンドの導入

使用時の考慮点

リダイレクト URL を指定するときは、アイデンティティ ポリシーが EAPoUDP アイデンティティ プロファイルと関連付けられている必要があります。

使用例

policy 100 というアイデンティティ ポリシーを作成し、EAPoUDP ポリシー設定モードに入る例を示します。

```
Switch(config)# identity policy policy100
Switch(config-identity-policy)# redirect tftp:172.20.10.30/nac_authen.tar match
authen_policy
```

show running-config 特権 EXEC コマンドを入力すると、この設定を確認できます。

関連コマンド

コマンド	説明
<code>identity profile eapoudp</code>	アイデンティティ プロファイルを作成し、EAPoUDP プロファイル設定モードに入ります。シンタックス情報を確認するには、 Cisco IOS Software Configuration > Cisco IOS Release 12.3 > New Feature Documentation > 12.3 T New Features and System Messages > New Features in Release 12.3(8)T > Network Admission Control を選択します。
<code>show running-config</code>	稼動設定を表示します。シンタックス情報を確認するには、 Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands を選択します。

show eou

show eou 特権 EXEC コマンドは、EAPoUDP 設定またはセッション キャッシュ エントリに関する情報を表示するために使用します。

```
show eou {all | authentication {clientless | eap | static} | interface interface-id | ip ip-address |
mac mac-address | posturetoken name} [| {begin | exclude | include} expression]
```

シンタックスの 説明

all	すべての EAPoUDP クライアントに関する情報を表示します。
authentication	次のいずれかの EAPoUDP 認証タイプに関する情報を表示します。 <ul style="list-style-type: none"> clientless — エンドポイントシステムで CTA ソフトウェアが稼動していない eap — 認証タイプが EAP static — 認証タイプが静的に設定されている
interface interface-id	指定したインターフェイス上の EAPoUDP 情報を表示します。
ip ip-address	指定した IP アドレスの EAPoUDP 情報を表示します。
mac mac-address	指定した MAC アドレスの EAPoUDP 情報を表示します。
posturetoken name	指定したポストチャ トークンの EAPoUDP 情報を表示します。
 begin	(オプション) <i>expression</i> との一致から始まる行を表示します。
 exclude	(オプション) <i>expression</i> との一致を含まない行を表示します。
 include	(オプション) 指定した <i>expression</i> との一致を含む行を表示します。
expression	参照ポイントとして使用する出力の表現です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	修正
12.2(18)SXF, 12.2(25)SED, 12.2(25)SG	このコマンドの導入

使用時の考慮点

ポートを指定しない場合は、グローバル パラメータとサマリーが表示されます。ポートを指定すると、そのポートの詳細情報が表示されます。

表現は大文字と小文字が区別されます。たとえば、**| exclude output** と入力すると、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

使用例

show eou 特権コマンドからの出力の例を示します。

```
Switch# show eou
Global EAPoUDP Configuration
-----
EAPoUDP Version = 1
EAPoUDP Port = 0x5566
Clientless Hosts = Disabled
```

```

IP Station ID           = Disabled
Revalidation            = Enabled
Revalidation Period    = 36000 Seconds
ReTransmit Period      = 3 Seconds
StatusQuery Period     = 300 Seconds
Hold Period            = 180 Seconds
AAA Timeout            = 60 Seconds
Max Retries            = 3
EAP Rate Limit         = 20
EAPoUDP Logging        = Disabled

Interface Specific EAPoUDP Configurations
-----
Interface GigabitEthernet1/0/1
  No interface specific configuration

```

表 4 に、表示されるフィールドの説明を示します。

表 4 show eou フィールドの説明

フィールド	説明
EAPoUDP Version	EAPoUDP プロトコルのバージョンを表示します。
EAPoUDP Port	EAPoUDP ポート番号を表示します。
Clientless Hosts	クライアントレス ホストのステータス（イネーブルまたはディセーブル）を表示します。
IP Station ID	IP アドレスが AAA ¹ ステーション ID フィールドに許可されているかどうかを表示します。 デフォルトでは、このフィールドはディセーブルです。
Revalidation	再検証ステータスを表示します。
Revalidation Period	ホストの再検証間隔を表示します。
ReTransmit Period	EAPoUDP パケットの再送信間隔を表示します。
StatusQuery Period	検証されたホストの EAPoUDP ステータス クエリー間隔を表示します。
Hold Period	スイッチが NAC 認証失敗の後に待機する時間を表示します。
AAA Timeout	AAA タイムアウト期間を表示します。
Max Retries	許可されている再送信回数を表示します。
EAPoUDP Logging	ロギング ステータスを表示します。

1. AAA = Authentication, Authorization, and Accounting (認証、認可、アカウントिंग)

関連コマンド

コマンド	説明
eou default	グローバル EAPoUDP パラメータをデフォルト設定にリセットします。シンタックス情報を確認するには、 Cisco IOS Software Configuration > Cisco IOS Release 12.3 > New Feature Documentation > 12.3 T New Features and System Messages > New Features in Release 12.3(8)T > Network Admission Control を選択します。
eou max-retry (グローバルおよび インターフェイス設定)	EAPoUDP 再検証の試行回数を指定します。
eou ratelimit	同時に実行する EAPoUDP ポスチャ検証回数を指定します。
eou timeout	EAPoUDP タイマーを指定します。

show ip access-lists interface

show ip access-lists 特権 EXEC コマンドは、LP IP ホスト ポリシーを表示するために使用します。

show ip access-lists interface *interface*

シンタックスの 説明

<i>interface</i>	表示するインターフェイスを指定します。
------------------	---------------------

コマンドモード

特権 EXEC

コマンド履歴

リリース	修正
12.2(18)SXF, 12.2(25)SED, 12.2(25)SG	このコマンドの導入

使用例

show ip device tracking all 特権 EXEC コマンドからの出力の例を示します。

```
Switch# show ip access-lists GigabitEthernet3/4
IP Admission access control entires (Inbound)
  permit ip host 102.50.1.54 any
```

show ip device tracking

show ip device tracking 特権 EXEC コマンドは、IP デバイス トラッキング テーブルのエントリに関する情報を表示するために使用します。

```
show ip device tracking {all | interface interface-id | ip ip-address | mac mac-address} [| {begin |
exclude | include} expression]
```

シンタックスの 説明

all	すべての IP デバイス トラッキング テーブル エントリを表示します。
interface <i>interface-id</i>	指定したインターフェイス上の IP デバイス トラッキング テーブル エントリを表示します。
ip <i>ip-address</i>	指定した IP アドレスの IP デバイス トラッキング テーブル エントリを表示します。
mac <i>mac-address</i>	指定した MAC アドレスの IP デバイス トラッキング テーブル エントリを表示します。
 begin	(オプション) <i>expression</i> との一致から始まる行を表示します。
 exclude	(オプション) <i>expression</i> との一致を含まない行を表示します。
 include	(オプション) 指定の <i>expression</i> との一致を含む行を表示します。
<i>expression</i>	参照ポイントとして使用する出力の表現です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	修正
12.2(18)SXF, 12.2(25)SED, 12.2(25)SG	このコマンドの導入

使用時の考慮点

表現は大文字と小文字が区別されます。たとえば、**| exclude output** と入力すると、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

使用例

show ip device tracking all 特権 EXEC コマンドからの出力の例を示します。

```
Switch# show ip device tracking all
-----
  IP Address  MAC Address      Interface          STATE
-----
  1.1.1.1     cf2a.220a.12f4   GigabitEthernet1/0/1  ACTIVE
  1.2.1.1     df4a.1235.ef1a   GigabitEthernet1/0/2  INACTIVE
```

関連コマンド

コマンド	説明
ip device tracking	IP デバイス トラッキング テーブルをイネーブルにし、IP デバイス トラッキング テーブルのパラメータを設定します。

メッセージとリカバリ手順

このセクションは、次のトピックで構成されています。

- AP メッセージ 81 ページ
- EOU メッセージ 82 ページ

AP メッセージ

ここでは、NAC レイヤ 2 IP 検証の認証プロキシメッセージについて説明します。

- Catalyst 6500 および 4500 シリーズ スイッチと Catalyst 7600 シリーズ ルータは、ここで説明するすべてのメッセージをサポートしています。
- Catalyst 3750、3560、3550、2970、2960、2955、2950 および 2940 スイッチは、AP-4-POLICY_URL_REDIRECT と AP-6-POSTURE_POLICY メッセージのみをサポートしています。

エラー メッセージ AP-4-AUTH_PROXY_NOMEM: Sufficient memory was not available to [chars].

説明 システム メモリが不十分なため特定のオペレーションを実行できません。[chars] はオペレーションです。

推奨するアクション メモリ要求を削減するために他のシステム アクティビティ数を減らします。より多くのメモリ リソースを割り当てることもできます。

エラー メッセージ AP-4-POLICY_URL_REDIRECT: Failed to locate match access control list [chars] for host [inet].

説明 スイッチは、ホストからの HTTP または HTTPS トラフィックをリダイレクト URL にリダイレクトできませんでした。url-redirect アトリビュート値 (AV) ペアは、リダイレクト URL と、リダイレクトする HTTP および HTTPS トラフィックを指定する *match-all* という ACL で構成されます。この ACL が設定されていない、またはリダイレクトするトラフィックが指定されていない場合、スイッチはホストからの要求をリダイレクトしません。[inet] はホストの IP アドレスです。

推奨するアクション ホストが接続しているスイッチ インターフェイス上に ACL を設定し、適用します。また、url-redirect AV ペアがリダイレクト URL と ACL で構成されていることを確認します。

エラー メッセージ AP-4-POSTURE_EXCEED_MAX_INIT: Exceeded maximum limit [dec] on entries in authentication proxy.

説明 認証プロキシ ポスチャ キャッシュ内の *INIT* ステートのエントリ数が制限を越えています。この状況は、ポスチャ検証のための認証プロキシがスイッチに設定されていて、スイッチが送信元 IP アドレスが異なる多数のホストから要求を受信したときに発生します。これは DoS 攻撃の可能性があります。ポスチャ キャッシュ カウントのエントリ数が最大数より少なければ、新しいキャッシュ エントリは作成されます。[dec] は、認証プロキシ キャッシュで許可されているエントリ数です。

推奨するアクション アクションは必要ありません。ポスチャ キャッシュ カウントのエントリ数が最大数より少なければ、新しいキャッシュ エントリは作成されます。

エラー メッセージ AP-6-POSTURE_DOWNLOAD_ACL: Send AAA request to download [chars] named access control list.

説明 スイッチが、特定の ACL を取得するために AAA サーバに要求を送信しました。[chars] は、ACL 名または番号です。

推奨するアクション アクションは必要ありません。

エラー メッセージ AP-6-POSTURE_POLICY: [chars] [chars] [chars] policy for host [inet].

説明 特定のホスト用に対して特定のポリシーが実施されたか、または削除されました。ポリシーは、ACL または リダイレクト URL です。最初の 2 つの [chars] は、スイッチがポリシーを実施または削除するために行うアクション、3 つめの [chars] は ACL または リダイレクト URL です。

推奨するアクション アクションは必要ありません。

エラー メッセージ AP-6-POSTURE_START_VALIDATION: IP=[inet] | Interface=[chars].

説明 スイッチが認証プロキシ ポスチャ キャッシュにホストのエントリを作成し、ポスチャ検証プロセスを開始しました。[inet] はホストの IP アドレス、[chars] はホストが接続しているスイッチ インターフェイスです。

推奨するアクション アクションは必要ありません。

エラー メッセージ AP-6-POSTURE_STATE_CHANGE: IP=[inet] | STATE=[chars].

説明 認証プロキシ ポスチャ検証キャッシュ内の特定のホストのポスチャ検証ステートが変更されました。[inet] はホストの IP アドレス、[chars] はポスチャ検証ステートです。

推奨するアクション アクションは必要ありません。

EOU メッセージ

ここでは、NAC レイヤ 2 IP 検証の EAPoUDP (EoU) メッセージについて説明します。



注

Catalyst 6500、4500、3750、3560、3550、2970、2960、2955、2950、2940 スイッチ、および Catalyst 7600 ルータは、ここで説明するすべてのメッセージをサポートしています。

エラー メッセージ EOU-2-PROCESS_ERR: Router could not create a EAPoUDP process.

説明 スイッチは EAPoUDP セッションを作成できませんでした。

推奨するアクション デバイスをリロードします。

エラー メッセージ EOU-4-BAD_PKT: IP=[inet] | Bad Packet=[chars].

説明 ルータは、特定のホストから無効の EAPoUDP パケットを受信しました。[inet] はホスト IP アドレス、[chars] は問題のあるパケットに関する情報です。

推奨するアクション ホストの NAC レイヤ 2 IP 設定を確認します。

エラー メッセージ EOU-4-MSG_ERR: Unknown message event received.

説明 EAPoUDP 検証プロセスが未知のメッセージイベントを受信しました。

推奨するアクション このメッセージが再度発生した場合は、デバイスをリロードします。

エラー メッセージ EOU-4-PROCESS_STOP: PROCESS=[chars] | ACTION=[chars].

説明 特定のプロセスが停止しました。最初の [chars] はプロセス、2 つめの [chars] はプロセス上で実行されたアクションです。

推奨するアクション デバイスをリロードします。

エラー メッセージ EOU-4-SOCKET: EAPoUDP socket binding fails for PORT=[hex]. Check if the interface has valid IP address.

説明 スイッチは、ポートを有効な IP アドレスにバインドできませんでした。[hex] はポート MAC アドレスです。

推奨するアクション スイッチ ポートに有効な IP アドレスを設定します。

エラー メッセージ EOU-4-UNKN_EVENT_ERR: UNKNOWN Event for HOST=%i | Event=%d.

説明 スイッチが未知の EAPoUDP イベントを受信しました。

推奨するアクション コンソールまたはシステム ログの表示どおりにメッセージをコピーし、Output Interpreter を使用してエラーを調査して解決を試みます。Bug Toolkit を使用すると、レポートされている類似する問題を調査できます。それでも解決できない場合は、Cisco Technical Assistance Center (TAC) でケースをオープンするか、シスコテクニカルサポートにコンタクトし、担当者に収集した情報を伝えてください。

エラー メッセージ EOU-4-UNKN_PROCESS_ERR: An unknown operational error occurred.

説明 内部システム エラーのため EAPoUDP プロセスが稼働できません。

推奨するアクション デバイスをリロードします。

エラーメッセージ EOU-4-UNKN_TIMER_ERR: An unknown Timer operational error occurred.

説明 内部システム エラーのため EAPoUDP 検証プロセスが稼動できません。

推奨するアクション デバイスをリロードします。

エラーメッセージ EOU-4-VALIDATION: Unable to initiate validation for HOST=[inet] | INTERFACE=[chars].

説明 スイッチは特定のホストに対するポストチャ検証を開始できませんでした。

推奨するアクション アクションではありませんが、おそらく EAPoUDP ポート バインディングの失敗が原因です。

エラーメッセージ EOU-4-VERSION_MISMATCH: HOST=[inet] | Version=[dec].

説明 特定のホストおよびスイッチの EAPoUDP バージョンに互換性がありません。[inet] はホスト IP アドレス、[dec] はホストの EAPoUDP バージョンです。

推奨するアクション 各デバイスの EAPoUDP バージョンを確認します。

エラーメッセージ EOU-5-RESPONSE_FAILS: Received an EAP failure response from AAA for host=[inet].

説明 スイッチは、ホストのアンチウイルス状態が検証できなかったことを通知する EAP 失敗応答を AAA サーバから受信しました。

推奨するアクション アクションは必要ありません。

エラーメッセージ EOU-6-AUTHSTATUS: [chars] | [inet].

説明 特定のホストの認証ステータスが Success または Failure です。[chars] はステータス、[inet] はホストの IP アドレスです。

推奨するアクション アクションは必要ありません。

エラーメッセージ EOU-6-AUTHTYPE: IP=[inet] | AuthType=[chars].

説明 特定のホストの認証タイプが [chars] です。[inet] はホストの IP アドレスです。

推奨するアクション アクションは必要ありません。

エラー メッセージ EOU-6-CTA: IP=[inet] | CiscoTrustAgent=[chars].

説明 特定のホストで CTA が検出されました。[inet] はホストの IP アドレス、[chars] は CTA 名です。

推奨するアクション CTA が検出されなかった場合は、ホストに CTA をインストールします。

エラー メッセージ EOU-6-IDENTITY_MATCH: IP=[inet] | PROFILE=EAPoUDP |
POLICYNAME=[chars].

説明 スイッチは特定のホストと EAPoUDP アイデンティティ プロファイルを検出しました。特定のポリシーが適用されている場合、スイッチのポスチャは検証されません。[inet] はホストの IP アドレス、[chars] はポリシー名です。

推奨するアクション ホストのポスチャ検証を行う必要がある場合は、EAPoUDP アイデンティティ プロファイルからホストのエントリを削除します。

エラー メッセージ EOU-6-POLICY: IP=[inet] | [chars]=[chars].

説明 スイッチは、特定のホストに対して実施するアクセス ポリシーを AAA サーバから受信しました。

推奨するアクション アクションは必要ありません。

エラー メッセージ EOU-6-POSTURE: IP=[inet] | HOST=[chars] | Interface=[chars].

説明 特定のホストのポスチャ検証ステータスが変更されました。[inet] はホスト IP アドレス、最初の [chars] はホスト名、2 つめの [chars] はインターフェイスです。

推奨するアクション アクションは必要ありません。

エラー メッセージ EOU-6-SESSION: IP=[inet] | HOST=[chars] | Interface=[chars].

説明 特定のインターフェイスに、ホストのエントリが作成または削除されました。[inet] はホスト IP アドレス、最初の [chars] は *DETECTED* または *REMOVED* などのアクション、2 つめの [chars] はインターフェイスです。

推奨するアクション アクションは必要ありません。

エラー メッセージ EOU-6-SQ: IP=[inet] | STATUSQUERY|[chars].

説明 特定のホストのステータス クエリーの結果が失敗または無効です。[inet] はホスト IP アドレス、[chars] はステータス クエリーの結果 (failure: 失敗、invalid: 無効、または no response: 応答なし) です。

推奨するアクション アクションは必要ありません。

