CHAPTER 53

Network Admission Control（NAC）の設定

この章では、Cisco IOS Release 12.2SX で Network Admission Control（NAC）を設定する手順を説明します。

（注） この章で使用しているコマンドの構文および使用方法の詳細については、次のマニュアルを参照してください。

- 次の URL の『Cisco IOS Master Command List, Release 12.2SX』
  http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html
- 次の URL の『*Network Admission Control*』フィーチャ モジュール
  http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/gt_nac.html
- 次の URL の『*Cisco IOS Security Command Reference*, Release 12.3』
  http://www.cisco.com/en/US/docs/ios/12_3/security/command/reference/secur_r.html

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。
http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

この章で説明する内容は、次のとおりです。

NAC の概要

ここでは NAC について説明します。

NAC の概要

NAC はシスコの自己防衛型ネットワーク イニシアティブの一部であり、ネットワーク上でのセキュリティ脅威の識別、阻止、および適合に役立ちます。ネットワーク化したビジネス環境において、ワームやウイルスの脅威や影響が強まっています。NAC を使用すると、このような脅威にネットワーク アクセスを許可する前に、エンドポイントやクライアントのアンチウイルス ステータスを検査および検証できます。

Release 12.2(18)SXF2 以降のリリースでは、NAC レイヤ 2 IP 検証をサポートしています。
Release 12.2(33)SXH およびリビルドでは、NAC レイヤ 3 IP 検証をサポートしています。
Release 12.2(33)SXI 以降のリリースでは、NAC レイヤ 3 IP 検証をサポートしていません。

NAC レイヤ 2 IP（LAN ポート IP とも呼ばれます）はエッジ スイッチのレイヤ 2 ポートで動作します。NAC レイヤ 2 IP 検証は、NAC レイヤ 2 IEEE802.1x とは異なる方法によって検証の開始、メッセージ交換、およびポリシーの適用を行います。ホスト PC 上では、LAN ポート IP に対する IEEE802.1x のサポートは必要ありません。IEEE 802.1x の詳細については、第 54 章「IEEE 802.1X ポートベース認証の設定」を参照してください。

NAC をサポートする装置の全一覧については、次の URL の『*Release Notes for Network Admission Control*, Release 2.1』を参照してください。

http://www.cisco.com/en/US/docs/security/nac/2.1/release_notes/NAC21RN.html

NAC レイヤ 3 IP（NAC Gateway IP とも呼ばれます）は、ディストリビューション レイヤ スイッチのレイヤ 3 インターフェイスで動作します。NAC レイヤ 3 IP の利点は、NAC 機能を使用するためにアクセス レイヤ スイッチで変更が不要な点です。

（注） NAC 機能により、IPv4 トラフィックに対してだけアクセス制御が適用されます。NAC はレイヤ 2 ブリッジド トラフィックを制限しません。

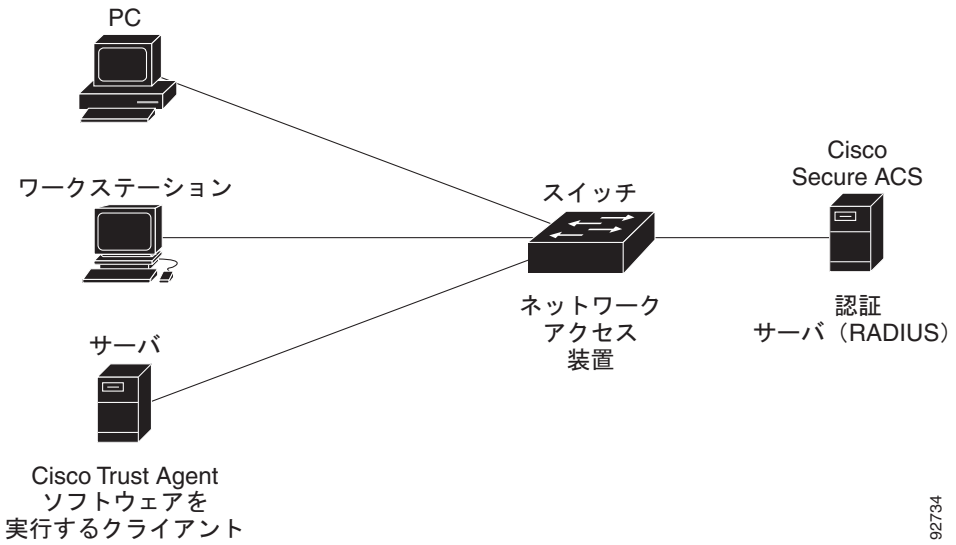
NAC はルーティングされたトラフィックに対し、*ポスチャ検証*を行います。ポスチャ検証を行うことで、ウイルスによるネットワークの被害を低減できます。この機能は、ネットワーク アクセスを要求するネットワーク装置のアンチウイルス クレデンシャルに基づき、ネットワーク アクセスを許可します。このクレデンシャルには、アンチウイルス ソフトウェア、ウイルス定義ファイル、または特定のウイルス スキャン エンジンのバージョンを使用できます。ホストのアンチウイルス クレデンシャルに基づき、要求を行う装置はネットワークへのアクセスを許可または制限されます。

クライアント ホストのクレデンシャル検証が失敗した場合は、*復旧*機能を使用することで、ネットワークへの部分的なアクセスが許可されます。この復旧プロセスにより、クライアント ホストからの HTTP トラフィックは、最新のアンチウイルス ファイルへのアクセスを提供する Web ページの URL にリダイレクトされます。復旧プロセスによって使用される URL は、ネットワーク アクセス ポリシーの一部として定義された復旧サーバのアドレスを解決します。復旧サーバとは、最新のアンチウイルス ファイルが保存されるサーバです。ここから、アンチウイルス ファイルをダウンロードまたはアップグレードできます。

NAC 装置のロール

図 53-1 に示すように NAC を使用する場合、ネットワーク上の各装置は、それぞれ特定のロールを担います。

図 53-1　ポスチャ検証装置



ネットワーク上で NAC をサポートする装置は、それぞれ次のロールを実行します。

- エンドポイント システムまたはクライアント：これは、PC、ワークステーション、サーバなどのネットワーク上にある装置（ホスト）です。ホストは Cisco Trust Agent（CTA）ソフトウェアを実行し、LAN へのアクセスおよびスイッチ サービスを要求し、スイッチからの要求に応答します。このエンドポイント システムはウイルス感染元となりうるので、ホストにネットワーク アクセスを認可する前に、そのアンチウイルス ステータスを検証する必要があります。
  - NAC レイヤ 2 IP の場合、装置が直接接続、IP 電話、またはワイヤレス アクセス ポイントを介してアクセス ポートに接続されています。
  - NAC レイヤ 3 IP の場合、装置はスイッチから 1 レイヤ 3 ホップ以上離れています。

  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*とも呼びます。
- スイッチ：これはネットワーク アクセス装置で、検証サービスとポリシーの適用を行います。
  - エッジ スイッチ：ネットワーク エッジで、NAC レイヤ 2 IP 検証サービスの提供とポリシーの適用を行うネットワーク アクセス装置です。また、クライアントのアクセス ポリシーに基づき、ネットワークへの物理アクセスを制御します。
  - ディストリビューション スイッチ：これは NAC ゲートウェイで、レイヤ 3 ネットワーク エッジで検証サービスの提供とポリシーの適用を行います。また、クライアントのアクセス ポリシーに基づき、レイヤ 3 ネットワークへのアクセスを制御します。

  Extensible Authentication Protocol（EAP; 拡張認証プロトコル）メッセージ内のカプセル化情報は、User Datagram Protocol（UDP; ユーザ データグラム プロトコル）を基にすることができます。UDP を使用する場合は、スイッチは EAP over UDP（EAPoUDP）フレームを使用します。これは EoU フレームと呼ばれることもあります。

  スイッチは、エンドポイントと認証サーバとの間で EAP メッセージをリレーします。

- 認証サーバ：実際のクライアント検証を行う装置です。認証サーバはクライアントのアンチウイルス ステータスを検証し、アクセス ポリシーを決定し、LAN およびスイッチ サービスへのアクセスがクライアントに許可されているかどうかをスイッチに通知します。スイッチはプロキシの役割を果たすため、スイッチと認証サーバ間の EAP メッセージ交換は、スイッチには透過的です。

  スイッチは RADIUS、Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）、および EAP 拡張を備えた Cisco Secure Access Control Server（ACS）Version 4.0 以降をサポートします。

  認証サーバは、*ポスチャ サーバ*とも呼ばれます。

AAA ダウン ポリシー

AAA ダウン ポリシーは、AAA サーバが使用できないときであっても、ホストのネットワーク接続を維持するための機能です。NAC の一般的な展開では、Cisco Secure ACS を使用してクライアントの状態（ポスチャ）を検証し、ポリシーを Network Access Device（NAD; ネットワーク アクセス装置）に返します。ポスチャ検証の実行時に AAA サーバが到達不可能になっている場合は、ユーザを拒否する（ネットワークへのアクセスを提供しない）のではなく、管理者はホストに適用可能なデフォルトの AAA ダウン ポリシーを設定できます。

このポリシーには、次のような利点があります。

- AAA が使用不可能である場合、ホストは制限されることはあっても、ネットワークへの接続は維持できます。
- AAA サーバが再稼動すると、ユーザは再検証を受けることが可能であり、ユーザのポリシーを ACS からダウンロードできます。

（注） AAA サーバの停止時には、ホストに他の既存のポリシーが関連付けられていない場合に限り、AAA ダウン ポリシーが適用されます。通常、AAA サーバが停止した場合の再検証時には、ホストに使用されていたポリシーは維持されます。

AAA ポリシーが適用される際、セッション ステートは AAA DOWN に維持されます。

NAC IP 検証

ここでは NAC IP 検証について説明します。

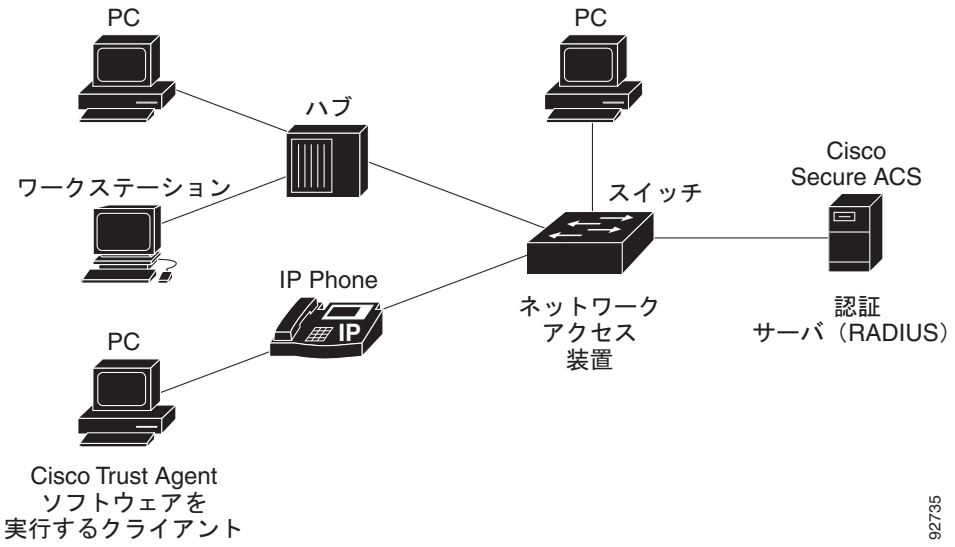
- 「NAC レイヤ 2 IP 検証」（P.53-5）
- 「NAC レイヤ 3 IP 検証」（P.53-5）
- 「ポスチャ検証」（P.53-6）
- 「Cisco Secure ACS と AV ペア」（P.53-8）
- 「監査サーバ」（P.53-9）
- 「ACL」（P.53-9）
- 「NAC タイマー」（P.53-10）

NAC レイヤ 2 IP 検証

エンドポイント システムまたはクライアントが接続されているエッジ スイッチのアクセス ポートでは、NAC レイヤ 2 IP を使用できます。装置（ホストまたはクライアント）は、PC、ワークステーション、またはサーバです。これらは図 53-2 に示すように、直接接続、または IP 電話やワイヤレス アクセス ポイントを経由して、アクセス ポートに接続されています。

NAC レイヤ 2 IP をイネーブルにすると、EAPoUDP は IPv4 トラフィックだけに対して機能します。スイッチはエンドポイント装置またはクライアントのアンチウイルス ステータスを検査して、アクセス制御ポリシーを適用します。

図 53-2　NAC レイヤ 2 IP を使用するネットワーク



NAC レイヤ 2 IP は、図 53-2 に示すように、同一レイヤ 2 ポートに接続された複数のホストのポスチャ検証をサポートします。

ホストが接続されているレイヤ 2 ポートで NAC レイヤ 2 IP 検証をイネーブルにすると、スイッチは DHCP スヌーピングおよび Address Resolution Protocol（ARP; アドレス解決プロトコル）スヌーピングを使用して、接続されたホストを識別できるようになります。スイッチは、ARP パケットを受信したあと、または DHCP スヌーピングのバインディング エントリを作成したあとに、ポスチャ検証を開始します。NAC レイヤ 2 IP 検証をイネーブルにすると、接続ホストを検出するデフォルトの手段は ARP スヌーピングとなります。DHCP スヌーピング バインディング エントリの作成時にスイッチがホストを検出するようにするには、DHCP スヌーピングをイネーブルにする必要があります。

NAC レイヤ 3 IP 検証

ゲートウェイ IP 機能は、2 種類の Posture Validation（PV; ポスチャ検証）トリガーをサポートしています。

- インターセプト ACL
- ARP ベースのトリガー（SVI インターフェイスのみ）

インターセプト ACL は、クライアントからのインバウンド トラフィックを代行受信して、トラフィックが ACL と一致する場合に PV を開始するよう設定されています。

インターフェイスに設定されている IP 許可ルールに関連インターセプト ACL がない場合、ゲートウェイでは ARP または DHCP イベントを使用してインターフェイスのポスチャ検証がトリガーされます。

ゲートウェイは ARP キャッシュ内で新規クライアントを学習すると、そのクライアントで PV を開始します。ARP ベースのトリガーを使用すると ACL TCAM の使用率が低下しますが、これはゲートウェイから 1 レイヤ 3 ホップ離れたクライアントに限り有効です。したがって、インターセプト ACL なしで IP 許可ルールを持つように SVI（でルータ ポートでないもの）だけを設定できます。

ポスチャ検証

レイヤ 2 ポートに割り当てられたアクセス VLAN で、Dynamic ARP Inspection（DAI; ダイナミック ARP インスペクション）だけをイネーブルにしている場合は、ARP パケットが DAI を通過したときにポスチャ検証が開始されます。ただし、DHCP スヌーピングと DAI の両方をイネーブルにしている場合は、DHCP スヌーピング バインディング エントリの作成時に、DHCP によってポスチャ検証が開始されます。

ポスチャ検証が開始されると、スイッチはセッション テーブル内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、次のプロセスに従って NAC ポリシーを決定します。

1. ホストが例外リスト内に含まれている場合は、スイッチはユーザ設定の NAC ポリシーをこのホストに適用します。
2. EoU バイパスをイネーブルにしている場合は、スイッチは非応答ホスト要求を Cisco Secure ACS に送信し、サーバからのアクセス ポリシーをホストに適用します。スイッチは要求の中に RADIUS AV ペアを挿入し、この要求が非応答ホストのものであることを指定します。
3. EoU バイパスがディセーブルの場合は、スイッチは EAPoUDP hello パケットをホストに送信し、ホストのアンチウイルス状態を要求します。指定の回数だけ試行してもホストから応答が得られない場合は、スイッチはこのホストをクライアントレスとして分類し、非応答ホストと見なします。スイッチは非応答ホスト要求を Cisco Secure ACS に送信し、サーバからのアクセス ポリシーをホストに適用します。

（注） クライアントに対する DHCP スヌーピング バインディング エントリを削除すると、スイッチはセッション テーブルからこのクライアントのエントリを削除します。以降は、このクライアントは認証されません。

例外リスト

例外リストには、ローカル プロファイルとポリシー設定が指定されています。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、または装置タイプに基づき、装置をスタティック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、アクセス制御属性を指定するローカル ポリシーに関連付けられています。

特定のホストを例外リストに指定し、このホストにユーザ設定ポリシーを適用することで、このホストのポスチャ検証をバイパスできます。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を例外リストに照合します。ホストが例外リスト内に含まれている場合は、スイッチは設定された NAC ポリシーをホストに適用します。また、スイッチはクライアントの検証ステータスを POSTURE ESTAB と指定して、EAPoUDP セッション テーブルを更新します。

EoU バイパス

スイッチは EoU バイパス機能を使用することで、CTA を使用していないホストのポスチャ検証を迅速に行うことができます。EoU バイパスがイネーブルの場合は、スイッチはアンチウイルス ステータスを要求するメッセージをホストに送信しません。代わりに、スイッチは Cisco Secure ACS に対し、このホストの IP アドレス、MAC アドレス、サービス タイプ、および EAPoUDP セッション ID を含めた要求を送信します。Cisco Secure ACS はこのホストに対するアクセス制御を判断し、ポリシーをスイッチに送信します。

EoU バイパスがイネーブルであり、ホストが非応答の場合は、スイッチは非応答ホスト要求を Cisco Secure ACS に送信し、サーバからのアクセス ポリシーをこのホストに適用します。

EoU バイパスがイネーブルであり、ホストで CTA を使用している場合、スイッチは非応答ホスト要求を Cisco Secure ACS に送信し、サーバからのアクセス ポリシーをこのホストに適用します。

EAPoUDP セッション

EoU バイパスがディセーブルの場合は、スイッチは EAPoUDP パケットを送信し、ポスチャ検証を開始します。ポスチャ検証の実行中、スイッチはデフォルトのアクセス ポリシーを適用します。スイッチが EAPoUDP メッセージをホストに送信し、これに対してホストがアンチウイルス状態の要求に応答すると、スイッチはこの EAPoUDP 応答を Cisco Secure ACS に転送します。所定の回数だけ試行してもホストから応答が得られない場合には、スイッチはこのホストを非応答として分類します。ACS がクレデンシャルを確認したあと、認証サーバはポスチャ トークンとポリシー属性を含めた Access-Accept メッセージ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、アクセス制限を適用します。これにより、不適切なポスチャのクライアントを区分および検疫するか、またはネットワーク アクセスを拒否します。

ポスチャ検証の実行中に適用されるポリシーには、次の 2 タイプがあります。

- ホスト ポリシー：ホスト ポリシーは、ポスチャ検証の結果に基づいて判断されたアクセス制限を適用する ACL を使用します。
- 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 または HTTPS トラフィックを復旧サーバにリダイレクトする機能を持ちます。これにより、非適合ホストは、適合ホストとなるために必要なアップグレード アクションを実行できます。

URL リダイレクトの拒否 ACE（通常は HTTP トラフィックの復旧サーバ宛てのリダイレクトをバイパスする目的）は、これらの ACE 宛てのトラフィックをハードウェアで転送します。デフォルトのインターフェイス ポリシー、およびダウンロードしたホスト ポリシーは適用されません。

このトラフィック（URL リダイレクトの拒否 ACE と一致するトラフィック）をフィルタリングするには、レイヤ 2 のアクセス VLAN で、VLAN ACL を定義する必要があります。

URL リダイレクト ポリシーは、次の要素で構成されます。

- 復旧サーバをポイントする URL
- ホストからのすべての HTTP または HTTPS パケット（復旧サーバ アドレス宛てのものを除く）をキャプチャし、スイッチ ソフトウェアにリダイレクトして、適切な HTTP リダイレクションを実行するためのスイッチ 上の ACL

ホスト ポリシーの ACL 名、リダイレクト URL、および URL リダイレクト ACL は、RADIUS の Attribute-Value オブジェクトを使用して伝送されます。

Cisco Secure ACS と AV ペア

NAC IP 検証をイネーブルにすると、Cisco Secure ACS は RADIUS を使用した 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 ステータス情報を取得し、エンドポイントのアンチウイルス状態を検証します。

RADIUS の Vendor-specific Attribute（VSA; ベンダー固有属性）である *cisco-av-pair* を使用すると、Cisco Secure ACS で次の Attribute-Value（AV）ペアを設定できます。

- CiscoSecure-Defined-ACL：Cisco Secure ACS 上のダウンロード可能な ACL の名前を指定します。スイッチは ACL 名を、次の形式の CiscoSecure-Defined-ACL AV ペアから取得します。

  #ACL#-IP-*name-number*

  name は ACL の名前、*number* は 3f783768 などのバージョン番号を表します。

  Auth-Proxy ポスチャ コードは、指定のダウンロード可能 ACL の Access Control Entry（ACE; アクセス制御エントリ）が、以前にダウンロード済みかどうかを調べます。まだダウンロードされていない場合は、Auth-Proxy ポスチャ コードはダウンロード可能 ACL 名をユーザ名として指定した AAA 要求を送信し、この ACE がダウンロードされるようにします。これで、このダウンロード可能 ACL が、名前付き ACL としてスイッチ上に作成されます。この ACL には、送信元アドレスが「any」の ACE が含まれます。リストの最後に暗黙的な deny ステートメントは含まれません。ポスチャ検証の完了後に、ダウンロード可能 ACL がインターフェイスに適用されると、送信元アドレスが「any」からホストの送信元 IP アドレスに変更されます。これらの ACE は、エンドポイント装置が接続されたスイッチ インターフェイスに適用された、ダウンロード可能 ACL に追加されます。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。

- url-redirect および url-redirect-acl：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、これらの cisco-av-pair VSA を次の形式で使用します。

  - url-redirect = <HTTP または HTTPS URL>
  - url-redirect-acl = ACL の名前または番号

  これらの AV ペアを使用すると、スイッチはエンドポイント装置からの HTTP または HTTPS 要求を代行受信して、指定のリダイレクト アドレスにクライアントのブラウザを転送します。リダイレクト先のサイトでは、クライアントは最新のアンチウイルス ファイルをダウンロードできます。Cisco Secure ACS の url-redirect AV ペアには、ブラウザのリダイレクト先となる URL が含まれます。url-redirect-acl AV ペアは、リダイレクトする HTTP または HTTPS トラフィックを指定する ACL の名前または番号を示します。ACL はスイッチ上に定義しておく必要があります。この結果、リダイレクト ACL 内の許可エントリに一致するトラフィックがリダイレクトされます。

  ホストのポスチャが適切でない場合は、状況に応じてこれらの AV ペアが送信されます。

  （注）　HTTP または HTTPS トラフィック用に URL をリダイレクトできますが、両方は同時にリダイレクトできません。Cisco IOS ソフトウェア HTTP サーバは、HTTP ポートまたは HTTPS ポートを待ち受けることができますが、両方を同時に待ち受けることはできないためです。

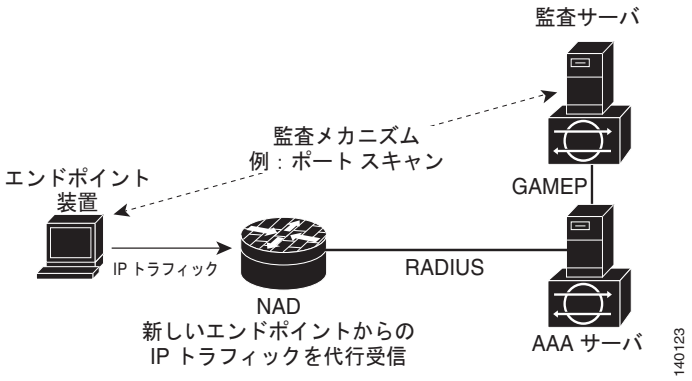
Cisco IOS ソフトウェアのサポートする AV ペアの詳細については、AAA クライアント上で実行されるソフトウェア リリースについての ACS コンフィギュレーションおよびコマンド リファレンス マニュアルを参照してください。

監査サーバ

Cisco Trust Agent（CTA）を実行していないエンド デバイスは、ネットワーク アクセス装置から確認を受けたときに、クレデンシャルを提供できません。このような装置を、*エージェントレス*または*非応答*と表現します。NAC のアーキテクチャは、監査サーバを組み込めるように拡張されています。監査サーバとは、CTA が実装されていないホストのセキュリティ適合性を調査、スキャン、および判別できるサードパーティ製サーバです。監査サーバの検査結果はアクセス サーバに反映させることができるので、すべての非応答ホストに対して共通の制限ポリシーを適用するのではなく、ホスト固有のネットワーク アクセス ポリシーを判断できます。任意のサードパーティ製監査処理を NAC アーキテクチャに統合することで、より堅牢なホスト監査および検査機能を構築できます。

図 53-3 は、一般的なトポロジに監査サーバを組み込む方法を示します。

図 53-3　NAC 装置のロール



このアーキテクチャでは、ホストが監査サーバと通信できるように、監査サーバが到達可能であることを前提としています。ホスト（エンドポイント装置）がポスチャ検査用に設定された NAD を介してネットワーク アクセスを行うと、最終的に NAD は AAA サーバ（Cisco Secure ACS）に対し、このホストに適用するアクセス ポリシーを要求します。AAA サーバは、外部の監査サーバによるホストのスキャンをトリガーするように設定できます。監査サーバによるスキャンは非同期に行われ、完了までに数秒かかることがあります。監査サーバによるスキャンの実行中は、AAA サーバは NAD に対し、適用する最小限の制限セキュリティ ポリシー、および短いポーリング タイマー（セッション タイムアウト）を伝送します。監査サーバから結果が返されるまで、NAD は所定の時間間隔で AAA サーバに対してポーリングを行います。AAA サーバは監査結果を受け取ると、監査結果に基づいてアクセス ポリシーを計算し、次に要求を受けたときに NAD にこのポリシーを送信し、適用を依頼します。

ACL

インターフェイスで NAC IP 検証を設定する場合は、同じインターフェイス上にデフォルトのセキュリティ ACL も設定しておく必要があります。ポスチャ検証を完了していないホストからの IP トラフィックに対しては、デフォルトの ACL が適用されます。

スイッチにデフォルトの ACL を設定している場合に、Cisco Secure ACS がホストのアクセス ポリシーをスイッチに送信すると、スイッチはレイヤ 2 ポートに接続されたホストからのトラフィックに対し、このポリシーを適用します。ポリシーがトラフィックに適用されると、スイッチはこのトラフィックを転送します。ポリシーがトラフィックに適用されない場合は、スイッチはデフォルトの ACL を適用します。デフォルト ACL が設定されていない場合、トラフィックは許可されます。

Cisco Secure ACS がスイッチに対し、ポリシーマップ アクションとしてリダイレクト URL を指定したダウンロード可能 ACL を送信した場合は、レイヤ 2 ポートに設定されたデフォルトの ACL より、このダウンロード可能 ACL の方が優先されます。また、リダイレクト URL ACL ポリシーは、ホストにすでに設定されたポリシーよりも優先されます。スイッチにデフォルトのポート ACL が設定されていない場合であっても、スイッチは Cisco Secure ACS からのダウンロード可能 ACL を適用できます。

NAC タイマー

スイッチは、次のタイマーをサポートします。

- 「ホールド タイマー」（P.53-10）
- 「アイドル タイマー」（P.53-10）
- 「再送信タイマー」（P.53-11）
- 「再検証タイマー」（P.53-11）
- 「ステータス クエリー タイマー」（P.53-12）

ホールド タイマー

ホールド タイマーは、EAPoUDP セッションを検証しようとする試みが失敗したあとに、次の新規セッションがすぐに開始されないように抑制します。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場合だけに使用されます。

ホールド タイマーのデフォルト値は 180 秒（3 分）です。

EAPoUDP セッションの検証が失敗するのは、ホストのポスチャ検証が失敗した場合、セッション タイマーが満了した場合、スイッチまたは Cisco Secure ACS が無効なメッセージを受信した場合などです。スイッチまたは認証サーバが無効なメッセージを連続して受信する場合は、悪意あるユーザが Denial-of-service（DoS; サービス拒絶）攻撃を仕掛けようとしている可能性もあります。

アイドル タイマー

アイドル タイマーは、ポスチャ検証を行っているホストから ARP パケットが送信されるまで、または IP 装置追跡テーブル内のエントリが更新されるまでのスイッチの待機時間を制御し、ホストが接続されているかどうかを確認します。アイドル タイマーは既知のホスト リストを使用して、ポスチャ検証を開始したホスト、および IP 装置追跡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時点、または IP 装置追跡テーブル内のエントリが更新された時点でリセットされます。アイドル タイマーが満了すると、スイッチはこのホストに対する EAPoUDP セッションを終了し、このホストは検証されなくなります。

アイドル タイマーのデフォルト値は、プローブの実行間隔に、プローブの再試行数を掛けた値として計算されます。デフォルトでは、アイドル タイマーのデフォルト値は 90 秒であり、これはプローブの実行間隔である 30 秒に、プローブの再試行数 3 を掛けた値です。

スイッチは既知のホスト リストを維持し、ポスチャ検証を開始したホストを追跡します。スイッチは ARP パケットを受信すると、このリストのエージング タイマー、およびアイドル タイマーをリセットします。リストのエージング時間が満了すると、スイッチは ARP プローブを送信し、このホストが存在するかどうかを確認します。ホストが存在する場合は、ホストはスイッチに対して応答メッセージを送信します。スイッチはこれを受け、既知のホスト リストの該当エントリを更新します。さらに、スイッチはリストのエージング タイマーおよびアイドル タイマーをリセットします。スイッチで応答がない場合、スイッチは Cisco Secure ACS とのセッションを終了し、このホストの検証も中止されます。

スイッチは IP 装置追跡テーブルを使用して、スイッチに接続されているホストを検出および管理します。また、スイッチはホストの検出に ARP または DHCP スヌーピングも使用します。デフォルトでは、スイッチの IP 装置追跡機能はディセーブルに設定されています。

NAC IP 検証を使用するには、IP 装置追跡機能をイネーブルにする必要があります。

IP 装置追跡をイネーブルにした場合、ホストが検出されると、スイッチは IP 装置追跡テーブルにエントリを追加します。このエントリには、次の情報が含まれます。

- 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
- ホストの検出時に ACTIVE に設定されるホスト状態

インターフェイスで NAC レイヤ 2 またはレイヤ 3 IP 検証をイネーブルにしている場合は、IP 装置追跡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 装置追跡テーブルでは、テーブルからエントリを削除する前に、スイッチがこのエントリに対して ARP プローブを送信する回数を設定できます。また、スイッチが ARP プローブを再送信するまでの待機時間（秒単位）も設定できます。スイッチで IP 装置追跡テーブルのデフォルト設定を使用する場合は、スイッチはすべてのエントリに対し、30 秒おきに ARP プローブを送信します。ホストがプローブに応答すると、このホストの状態が更新され、アクティブの状態で維持されます。スイッチで応答がない場合、スイッチはさらに 3 つの ARP プローブを 30 秒おきに送信できます。スイッチは最大数の ARP プローブを送信したあと、テーブルからこのホスト エントリを削除します。EAPoUDP セッションがセットアップされている場合、スイッチはこのホストのセッションを終了します。

IP 装置追跡を行うことで、DHCP の限界を克服し、ホストをタイムリーに検出できます。リンクが停止した場合は、このインターフェイスに関連付けられた IP 装置追跡エントリは削除されず、これらのエントリの状態は非アクティブに変わります。スイッチでは IP 装置追跡テーブル内のアクティブ エントリ数に制限はありませんが、非アクティブ エントリを削除するための上限が適用されます。テーブルがテーブル サイズ制限に到達すると、スイッチが非アクティブ エントリを削除します。テーブル内に非アクティブ エントリが含まれない場合は、IP 装置追跡テーブル内のエントリ数は単純に増加します。ホストが非アクティブになると、スイッチはこのホスト セッションを終了します。

テーブル サイズ制限は 2048 です。

インターフェイス 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付けられたエントリに対して ARP プローブを送信します。ARP プローブに応答しないホストのエントリはスイッチで期限切れとなります。スイッチは、応答のあったホストの状態をアクティブに変更し、ポスチャ検証を開始します。

再送信タイマー

再送信タイマーは、ポスチャ検証の実行中に、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。このタイマーの設定値が低すぎると、不必要な再送信が行われる可能性があり、設定値が高すぎると、応答時間が長くな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

再検証タイマーは、ポスチャ検証の実行中に EAPoUDP メッセージを使用していたクライアントに対し、NAC ポリシーが適用される期間を制御します。このタイマーは、最初のポスチャ検証が完了した時点で開始されます。ホストが再検証されると、このタイマーはリセットされます。再検証タイマーのデフォルト値は 36000 秒（10 時間）です。

スイッチに再検証タイマーの値を指定するには、**eou timeout revalidation** *seconds* グローバル コンフィギュレーション コマンドを使用します。また、インターフェイスに再検証タイマーの値を指定するには、**eou timeout revalidation** *seconds* インターフェイス コンフィギュレーション コマンドを使用します。

（注）　再検証タイマーはスイッチ上でローカルに設定することも、コントロール サーバからダウンロードすることもできます。

再検証タイマーは、AAA を実行する Cisco Secure ACS からの Access-Accept メッセージに含まれる Session-Timeout RADIUS 属性（属性 [27]）、および Termination-Action RADIUS 属性（属性 [29]）に基づいて動作します。スイッチが Session-Timeout 値を受信した場合は、この値はスイッチ上の再検証タイマー値よりも優先されます。

再検証タイマーが満了した場合のスイッチのアクションは、次の Termination-Action 属性値のいずれかに応じて異なります。

- Termination-Action RADIUS 属性値がデフォルト値の場合は、セッションは終了します。
- スイッチが受信した Termination-Action 属性値がデフォルト以外の場合は、ポスチャ検証の実行中、EAPoUDP セッションおよび現在のアクセス ポリシーは有効な状態を維持します。
- Termination-Action 属性値が RADIUS の場合は、スイッチはクライアントを再検証します。
- サーバからのパケットに Termination-Action 属性が含まれない場合は、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

ステータス クエリー タイマーは、以前検証したクライアントが存在し、そのポスチャが変更されていないことを確認するまでの、スイッチの待機時間を制御します。EAPoUDP メッセージによって認証されたクライアントだけが、このタイマーを使用します。このタイマーは、クライアントの最初の検証が完了した時点で開始されます。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。

ホストが再認証されると、このタイマーはリセットされます。このタイマーが満了すると、スイッチはホストに Status-Query メッセージを送信して、ホストのポスチャ検証の状態を確認します。ホストがポスチャが変更されたことを示す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 およびスイッチオーバー

RPR モードの冗長性を設定している場合は、スイッチオーバーが発生すると、現在ポスチャを検証されているホストの情報がすべて失われます。すべてのセッションが再検証されます。ユーザは検証されず、サービスが中断する可能性があります。

Release 12.2(33)SXH 以降のリリースでは、SSO モード冗長性を使用している場合、**ip admission ha** コマンドを入力してスタンバイ スーパーバイザ エンジンとのホスト セッション テーブル同期をイネーブルにすることができます。ハイ アベイラビリティ機能がイネーブルの場合、スイッチオーバーによる中断がないため、スイッチオーバーが発生しても確立しているポスチャ済みホストは再検証不要です。SSO の前に未確立のポスチャ セッションは、スイッチオーバー後に再検証が必要です。

NAC の設定

ここでは、NAC を設定する手順について説明します。

- 「NAC のデフォルト設定」（P.53-13）
- 「NAC IP に関する注意事項、制限事項、および制約事項」（P.53-13）
- 「NAC IP 検証の設定」（P.53-15）

NAC のデフォルト設定

デフォルトでは、NAC IP 検証はディセーブルです。

NAC IP に関する注意事項、制限事項、および制約事項

- NAC 機能により、IPv4 トラフィックに対してだけアクセス制御が適用されます。NAC はレイヤ 2 ブリッジド トラフィックを制限しません。
- IPv6 トラフィックはポスチャ検証をトリガーせず、NAC IP は IPv6 トラフィックにアクセス ポリシーを適用しません。
- NAC IP が正しく動作するためには、EAPoUDP トラフィックがデフォルト ACL によって許可される必要があります。
- DHCP スヌーピングが正しく動作するには、インターフェイスのデフォルト ACL およびホスト ポリシーで DHCP トラフィックが許可される必要があります。
- エンドポイント装置からの HTTP および HTTPS 要求を指定の URL に転送するには、HTTP サーバ機能をイネーブルにする必要があります。url-redirect-acl AV ペアを、URL ACL 名として定義してください。この ACL には、**deny tcp any** *remediation server address* **eq www** コマンドに続けて、リダイレクトする HTTP トラフィックに対する許可 ACE を指定する必要があります。

NAC レイヤ 2 IP 検証に関する注意事項、制限事項、および制約事項

NAC レイヤ 2 IP 検証を設定する場合、次の注意事項、制限事項、および制約事項に従ってください。

- レイヤ 2 IP 検証が正しく実行されるには、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。
- ポートの親 VLAN に VACL キャプチャが設定されている場合は、レイヤ 2 IP 検証は許可されません。
- CPU にリダイレクトされた LAN Port IP（LPIP; LAN ポート IP）ARP トラフィックは、SPAN 機能によってスパニングされません。
- NAC レイヤ 2 IP 検証は、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 ポートではサポートされません。Catalyst 6500 シリーズ スイッチは、EtherChannel 上でレイヤ 2 IP をサポートします。
- NAC レイヤ 2 IP 検証をイネーブルにしている場合は、ホストが接続されたレイヤ 2 ポート上で ACL を設定する必要があります。
- レイヤ 2 ポートがプライベート VLAN の一部である場合は、NAC レイヤ 2 IP はサポートされません。
- CPU にリダイレクトされた NAC レイヤ 2 IP ARP トラフィックは、SPAN 機能によってスパニングされません。

- 送信元 IP アドレスの異なる大量の ARP パケットがスイッチに送信される場合は、DoS 攻撃が行われている可能性があります。この問題を回避するには、**mls rate-limit layer2 ip-admission** コマンドを使用して、IP アドミッション MLS レート制限機能を設定する必要があります。
- レイヤ 2 ポートの親 VLAN 上で DAI もイネーブルにされている場合は、CPU に転送される ARP パケットの IP アドミッション レート制限は無効になります。この状況では、ARP インスペクションによるレート制限が機能します。ARP インスペクションによるレート制限はソフトウェアで行われ、IP アドミッション レート制限はハードウェアで行われます。
- NAC レイヤ 2 IP および NAC レイヤ 2 IEEE 802.1x が同一アクセスポートでイネーブルの場合、IEEE 802.1x 認証が優先されます。ポートが接続されているホストのポスチャはすでに検証されている可能性があり、スイッチは IEEE 802.1x に基づいてアクセス制限を適用しています。
- スイッチで DHCP リース許可を使用して接続ホストを識別するには、DHCP スヌーピングをイネーブルにする必要があります。DHCP 環境では、DHCP パケットはデフォルト インターフェイス、およびダウンロードされたホスト ポリシーの両方で許可されます。
- ポスチャ検証が行われる前に、エンド ステーションが DNS 要求を送信できるようにするには、レイヤ 2 ポート上で名前付きのダウンロード可能 ACL を設定し、ACE で DNS パケットを許可する必要があります。
- 音声 VLAN に属するレイヤ 2 ポートに NAC レイヤ 2 IP 検証が設定されている場合は、このスイッチは IP 電話のポスチャを検証しません。IP 電話が例外リストに指定されていることを確認してください。
- NAC レイヤ 2 IP 検証がイネーブルにされている場合は、入力インターフェイス上に設定されている VLAN ACL およびルータ ACL より、NAC レイヤ 2 IP 設定の方が優先されます。たとえば、VLAN ACL とルータ ACL が設定されている場合は、各ポリシーは LPIP ポリシー、VLAN ACL、ルータ ACL の順に 1 つずつ適用されます。次のポリシーは、トラフィックが 1 つ前のポリシー検査を通過した場合に限り適用されます。順次適用されるポリシーのいずれかでトラフィックが拒否された場合は、このトラフィックはアクセスを拒否されます。ダウンロードされた LPIP ホスト ポリシーは、デフォルトのインターフェイス ポリシーを常に上書きします。
- 入力 VLAN で DAI をイネーブルにしている場合は、ARP パケットの検証後に限り、スイッチでポスチャ検証が開始されます。
- URL リダイレクトの拒否 ACE に送信されたトラフィックは、ハードウェアで転送され、デフォルト インターフェイス ポリシーおよびダウンロードされたホスト ポリシーは適用されません。このトラフィック（URL リダイレクト の拒否 ACE と一致するトラフィック）をフィルタリングするには、レイヤ 2 のアクセス VLAN で、VLAN ACL を定義する必要があります。このように設定することで、復旧サーバ宛ての HTTP トラフィックのリダイレクションをバイパスできます。

NAC レイヤ 3 IP 検証に関する注意事項、制限事項、および制約事項

NAC レイヤ 3 IP 検証を設定する場合、次の注意事項、制限事項、および制約事項に従ってください。

- Release 12.2(33)SXH およびリビルドだけが、NAC レイヤ 3 IP 検証をサポートしています。Release 12.2(33)SXI 以降のリリースでは、NAC レイヤ 3 IP 検証をサポートしていません。
- NAC ゲートウェイ機能は Supervisor Engine 720 および Supervisor Engine 32-8GE でサポートされています。
- ARP ベース トリガーの場合、GWIP が ARP プロービング メカニズムを使用してホストの存在を検出します。
- インターフェイスで NAC ゲートウェイ IP 検証をイネーブルする場合は、同じインターフェイス上にデフォルトの Cisco IOS ACL も設定しておく必要があります。

- URL リダイレクトの拒否 ACE に送信されたトラフィックは、ハードウェアで転送され、デフォルト インターフェイス ポリシーおよびダウンロードされたホスト ポリシーは適用されません。このトラフィック（URL リダイレクト の拒否 ACE と一致するトラフィック）でフィルタリングが必要な場合、インターフェイス上で Cisco IOS ACL を定義する必要があります。このように設定することで、復旧サーバ宛ての HTTP トラフィックのリダイレクションをバイパスできます。
- シングルホスト モードの IEEE 802.1x 認証と NAC レイヤ 2 IP 検証がレイヤ 2 ポートで設定されていて、接続されている ホストの IEEE 802.1x 認証が失敗した場合、DHCP または ARP パケットをホストから受信する際にスイッチは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場合、クライアントが正常に認証されるまでポートは EAPOL フレーム以外のトラフィックを送受信しません。

NAC IP 検証の設定

NAC レイヤ 2 IP 検証を設定するには、特権 EXEC モードで、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# ip admission name` *rule_name* `eapoudp`	ルール名を指定して、IP NAC ルールを作成および設定します。 IP NAC ルールをスイッチから削除するには、**no ip admission name** *rule-name* **eapoudp** グローバル コンフィギュレーション コマンドを使用します。
ステップ 3	`Router(config)# mls rate-limit layer 2 ip ip-admission` *pps* (*burst*) または `Router(config)# mls rate-limit unicast ip features` *pps* (*burst*)	レイヤ 2 ポートの場合、CPU 宛ての IP アドミッション トラフィックのレート制限をイネーブルにします。 レイヤ 3 ポートの場合、CPU 宛ての IP アドミッション トラフィックのレート制限をイネーブルにします。

	コマンド	目的
ステップ 4	Router(config)# **access-list** *access_list_number* {**deny** | **permit**} *source* [*source_wildcard*] [**log**]	送信元アドレスとワイルドカードを使用して、ACL を定義します。 *access_list_number* 値は、1 ～ 99 または 1300 ～ 1999 の範囲の 10 進数値です。 **deny** または **permit** を入力して、条件が一致した場合にアクセスを拒否するのか許可するのかを指定します。 *source* 値は、パケットの送信元となるネットワークまたはホストのアドレスであり、次の形式で指定されます。 • ドット付き 10 進表記による 32 ビット長の値。 • *source*、および *source_wildcard* 0.0.0.0 255.255.255.255 の略を意味するキーワード **any**。*source_wildcard* を入力する必要はありません。 • source、および source-wildcard *source* 0.0.0.0 の略を意味するキーワード **host**。 （任意）*source_wildcard* を指定すると、ワイルドカード ビットが送信元アドレスに適用されます。 （任意）**log** を入力すると、エントリと一致するパケットの詳細を示すロギング メッセージがコンソールに送信されます。
ステップ 5	Router(config)# **interface** *interface_id*	インターフェイス コンフィギュレーション モードを開始します。
ステップ 6	Router(config)# **ip access-group** {*access_list_number* | *name*} **in**	指定のインターフェイス宛てのアクセスを制御します。
ステップ 7	Router(config)# **ip admission name** *rule_name*	指定の IP NAC ルールをインターフェイスに適用します。 指定のインターフェイスに適用された IP NAC ルールを削除するには、**no ip admission name** *rule-name* インターフェイス コンフィギュレーション コマンドを使用します。
ステップ 8	Router(config)# **exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 9	Router(config)# **aaa new-model**	AAA をイネーブルにします。
ステップ 10	Router(config)# **aaa authentication eou default group radius**	EAPoUDP の認証方法を設定します。 EAPoUDP 認証方法を削除するには、**no aaa authentication eou default** グローバル コンフィギュレーション コマンドを使用します。
ステップ 11	Router(config)# **ip device tracking**	IP 装置追跡テーブルをイネーブルにします。 IP 装置追跡テーブルをディセーブルにするには、**no device tracking** グローバル コンフィギュレーション コマンドを使用します。

	コマンド	目的
ステップ 12	`Router(config)# ip device tracking probe {count count | interval interval}`	（任意）IP 装置追跡テーブルに対し、次のパラメータを設定します。 • **count** *count*：スイッチが ARP プローブを送信する回数を設定します。有効値の範囲は 1 ～ 5 です。デフォルトは 3 です。 • **interval** *interval*：スイッチが ARP プローブを再送する前に、応答を待機する秒数を設定します。有効値の範囲は 30 ～ 300 秒です。デフォルト値は 30 秒です。
ステップ 13	`Router(config)# radius-server host {hostname | ip_address} key string`	（任意）RADIUS サーバの各パラメータを設定します。 *hostname* または *ip_address* 値には、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。 **key** *string* 値には、RADIUS サーバ上で動作する RADIUS デーモンとスイッチとの間で使用する認証および暗号キーを指定します。キーはテキスト ストリングで、RADIUS サーバで使用する暗号キーと一致する必要があります。 **（注）** キーは、**radius-server host** コマンド構文の末尾で設定してください。これは、先頭のスペースは無視されるが、キーのストリング内または末尾のスペースは使用されるためです。キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。このキーは RADIUS デーモンで使用される暗号と一致する必要があります。 複数の RADIUS サーバを使用する場合は、このコマンドを再度入力します。
ステップ 14	`Router(config)# radius-server attribute 8 include-in-access-req`	スイッチが非応答ホストに接続されている場合は、アクセス要求パケットまたはアカウンティング要求パケット内で、Framed-IP-Address RADIUS 属性（属性 [8]）を送信するようにスイッチを設定します。
ステップ 15	`Router(config)# radius-server vsa send authentication`	VSA を認識および使用するようにネットワーク アクセス サーバを設定します。

	コマンド	目的
ステップ 16	`Router(config)# ip device tracking [probe {count count | interval interval}]`	（任意）IP 装置追跡テーブルに対し、次のパラメータを設定します。 • **probe count** *count*：IP 装置追跡テーブルからエントリを削除する前に、スイッチがエントリに対する ARP プローブを送信する回数を設定します。有効値の範囲は 1 ～ 5 です。デフォルトは 3 です。 • **probe interval** *interval*：スイッチが ARP プローブを再送する前に、応答を待機する秒数を設定します。有効値の範囲は 30 ～ 300 秒です。デフォルト値は 30 秒です。
ステップ 17	`Router(config)# eou logging`	（任意）EAPoUDP システム ロギング イベントをイネーブルにします。
ステップ 18	`Router(config)# end`	特権 EXEC モードに戻ります。
ステップ 19	`Router# 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。
ステップ 20	`Router# show ip device tracking {all | interface interface_id | ip ip_address | mac mac_address}`	IP 装置追跡テーブル内の各エントリの情報を表示します。
ステップ 21	`Router# show ip access lists interface interface`	Cisco IOS ソフトウェアの設定において、ダウンロードされたホスト ポリシーを表示します。
ステップ 22	`Router# copy running-config startup-config`	（任意）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。

NAC IP 検証を設定する場合は、次の注意事項に留意してください。

- IP NAC ルールをスイッチから削除するには、**no ip admission name** *rule_name* **eapoudp** グローバル コンフィギュレーション コマンドを使用します。指定のインターフェイスに適用された IP NAC ルールを削除するには、**no ip admission** *admission_name* インターフェイス コンフィギュレーション コマンドを使用します。
- EAPoUDP 認証方法を削除するには、**no aaa authentication eou default** グローバル コンフィギュレーション コマンドを使用します。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 auth-proxy ポスチャ コードを設定するには、**no aaa authorization auth-proxy default** グローバル コンフィギュレーション コマンドを使用します。
- IP 装置追跡テーブルをディセーブルにし、テーブルの各パラメータをデフォルト値に戻すには、**no device tracking** および **no device tracking probe** {**count** | **interval**} グローバル コンフィギュレーション コマンドを使用します。
- Framed-IP-Address 属性を送信しないようにスイッチを設定するには、**no radius-server attribute 8 include-in-access-req** グローバル コンフィギュレーション コマンドを使用します。
- 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 コンフィギュレーション コマンドを使用します。
- スイッチまたは指定のインターフェイスから、すべての NAC クライアント装置エントリを消去するには、**clear eou** 特権 EXEC コマンドを使用します。IP 装置追跡テーブル内のエントリを消去するには、**clear ip device tracking** 特権 EXEC コマンドを使用します。
- シングルホスト モードの IEEE 802.1x 認証と NAC レイヤ 2 IP 検証がレイヤ 2 ポートで設定されていて、接続されているホストの IEEE 802.1x 認証が失敗した場合、DHCP または ARP パケットをホストから受信する際にスイッチは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場合、クライアントが正常に認証されるまでポートは EAPOL フレーム以外のトラフィックを送受信しません。

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

```
Router# configure terminal
Router(config)# ip admission name nac eapoudp
Router(config)# access-list 5 permit any any
Router(config)# interface gigabitethernet 2/0/1
Router(config-if)# ip access-group 5 in
Router(config-if)# ip admission nac
Router(config-if)# exit
Router(config)# aaa new-model
Router(config)# aaa authentication eou default group radius
Router(config)# radius-server host admin key rad123
Router(config)# radius-server vsa send authentication
Router(config)# ip device tracking probe count 2
Router(config)# eou logging
Router(config)# end
```

EAPoUDP の設定

EAPoUDP を設定するには、特権 EXEC モードで、次の作業を行います。

	コマンド	目的
ステップ 1	Router# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Router(config)# **eou allow** {**clientless** | **ip-station-id**} **eou default** **eou logging** **eou max-retry** *number* **eou port** *port_number* **eou ratelimit** *number* **eou timeout** {**aaa** *seconds* | **hold-period** *seconds* | **retransmit** *seconds* | **revalidation** *seconds* | **status-query** *seconds*} **eou revalidate**	EAPoUDP 値を指定します。 **allow**、**default**、**logging**、**max-retry**、**port**、**rate-limit**、**revalidate**、および **timeout** の各キーワードの詳細については、このリリースおよび『*Network Admission Control*』フィーチャ モジュールのコマンド リファレンスを参照してください。
ステップ 3	Router(config)# **interface** *interface_id*	インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	Router(config)# **eou default** **eou max-retry** *number* **eou timeout** {**aaa** *seconds* | **hold-period** *seconds* | **retransmit** *seconds* | **revalidation** *seconds* | **status-query** *seconds*} **eou revalidate**	指定のインターフェイスに対し、EAPoUDP の関連付けをイネーブル化および設定します。 **default**、**max-retry**、**revalidate**、および **timeout** の各キーワードの詳細については、このリリースおよび『*Network Admission Control*』フィーチャ モジュールのコマンド リファレンスを参照してください。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	Router# **show eou** {**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 エントリについての情報を表示します。
ステップ 7	Router# **copy running-config startup-config**	（任意）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。

グローバルなデフォルトの EAPoUDP 値に戻すには、**eou** グローバル コンフィギュレーション コマンドの **no** 形式を使用します。EAPoUDP 関連付けをディセーブルにするには、**eou** インターフェイス コンフィギュレーション コマンドの **no** 形式を使用します。

アイデンティティ プロファイルおよびアイデンティティ ポリシーの設定

アイデンティティ プロファイルおよびアイデンティティ ポリシーを設定するには、特権 EXEC モードで、次の作業を行います。

	コマンド	目的
ステップ 1	Router# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Router(config)# **identity policy** *policy_name*	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 コンフィギュレーション モードを開始します。
ステップ 3	Router(config-identity-policy)# **access-group** *access_group*	アイデンティティ ポリシーに対するネットワーク アクセス属性を定義します。
ステップ 4	Router(config)# **identity profile eapoudp**	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 コンフィギュレーション モードを開始します。
ステップ 5	Router(config-identity-prof)# **device** {**authorize** | **not-authorize**} {**ip-address** *ip_address* | **mac-address** *mac_address* | **type cisco ip phone**} [**policy** *policy_name*]	指定の IP 装置を許可し、この装置に指定のポリシーを適用します。
ステップ 6	Router(config)# **exit**	アイデンティティ プロファイル コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 7	Router# **end**	特権 EXEC モードに戻ります。
ステップ 8	Router# **show running-config**	設定を確認します。
ステップ 9	Router# **copy running-config startup-config**	（任意）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。

スイッチからアイデンティティ ポリシーを削除するには、**no identity-policy** *policy_name* グローバル コンフィギュレーション コマンドを使用します。アイデンティティ プロファイルを削除するには、**no identity rofile eapoudp** グローバル コンフィギュレーション コマンドを使用します。指定の IP 装置を許可しないようにし、この装置から指定のポリシーを削除するには、**no device** {**authorize** | **not-authorize**} {**ip-address** *ip_address* | **mac-address** *mac_address* | **type cisco ip phone**} [**policy** *policy_name*] インターフェイス コンフィギュレーション コマンドを使用します。

次に、アイデンティティ プロファイルおよびアイデンティティ ポリシーを設定する例を示します。

```
Router# configure terminal
Router(config)# identity policy policy1
Router(config-identity-policy)# access-group group1
Router(config)# identity profile eapoudp
Router(config-identity-prof)# device authorize ip address 10.10.142.25 policy policy1
Router(config-identity-prof)# exit
Router(config)# end
```

NAC ハイ アベイラビリティの設定

IP アドミッション ハイ アベイラビリティを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# ip admission ha`	IP アドミッション ハイ アベイラビリティをイネーブルにします。
ステップ 3	`Router(config)# ip admission ha update` *update_interval*	アクティブ スーパーバイザ エンジンが同期アップデートをスタンバイに送信する頻度を定義します。 インターバルは 30 ～ 60 秒の範囲です。
ステップ 4	`Router# show ip admission ha stats`	セッション同期に関連した統計を表示します。
ステップ 5	`Router# clear ip admission ha stats`	（任意）セッション同期に関連した統計を消去します。

（注）　アクティブな Web ベース認証またはポスチャ セッションがある場合、IP アドミッション ハイ アベイラビリティ機能をイネーブルにはできません。

スイッチからの IP アドミッション ハイ アベイラビリティをディセーブルにするには、**no ip admission ha** コンフィギュレーション コマンドを使用します。

次に、IP アドミッション ハイ アベイラビリティを設定する例を示します。

```
Router# configure terminal
Router(config)# ip admission ha
Router(config)# ip admission ha update 50
Router(config)# end
Router(config)# clear ip admission ha stats
Router(config-identity-prof)# show ip admission ha stats
```

NAC AAA ダウン ポリシーの設定

NAC AAA ダウン ポリシーを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# ip admission name` *rule-name* **eapoudp event timeout aaa policy identity** *identity_policy_name*	NAC ルールを作成し、AAA サーバが到達不可能な場合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。 ルールをスイッチから削除するには、**no ip admission name** *rule-name* **eapoudp event timeout aaa policy identity** グローバル コンフィギュレーション コマンドを使用します。

	コマンド	目的
ステップ 3	Router(config)# **access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] [**log**]	送信元アドレスとワイルドカードを使用して、デフォルトのポート ACL を定義します。 *access-list-number* 値は、1 ～ 99 または 1300 ～ 1999 の範囲の 10 進数値です。 **deny** または **permit** を入力して、条件が一致した場合にアクセスを拒否するのか許可するのかを指定します。 *source* 値は、パケットの送信元となるネットワークまたはホストのアドレスであり、次の形式で指定されます。 • ドット付き 10 進表記による 32 ビット長の値。 • *source*、および *source-wildcard* 値 0.0.0.0 255.255.255.255 の略を意味するキーワード **any**。*source-wildcard* 値を入力する必要はありません。 • source、および source-wildcard *source* 0.0.0.0 の略を意味するキーワード **host**。 （任意）*source-wildcard* を使用して、ワイルドカード ビットを送信元アドレスに適用します。 （任意）**log** を入力すると、エントリと一致するパケットの詳細を示すロギング メッセージがコンソールに送信されます。
ステップ 4	Router(config-if)# **interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	Router(config-if)# **ip access-group** {*access-list-number* | *name*} **in**	指定のインターフェイス宛てのアクセスを制御します。
ステップ 6	Router(config-if)# **ip admission** *rule-name*	指定の IP NAC ルールをインターフェイスに適用します。 指定のインターフェイスに適用された 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 コンフィギュレーション コマンドを使用します。
ステップ 7	Router(config)# **exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 8	Router(config)# **aaa new-model**	AAA をイネーブルにします。
ステップ 9	Router(config)# **aaa authentication eou default group radius**	EAPoUDP の認証方法を設定します。 EAPoUDP 認証方法を削除するには、**no aaa authentication eou default** グローバル コンフィギュレーション コマンドを使用します。
ステップ 10	Router(config)# **aaa authorization network default local**	許可方法をローカルに設定します。許可方法を削除するには、**no aaa authorization network default local** コマンドを使用します。
ステップ 11	Router(config)# **ip device tracking**	IP 装置追跡テーブルをイネーブルにします。 IP 装置追跡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 コンフィギュレーション コマンドを使用します。
ステップ 12	Router(config)# **ip device tracking** [**probe** {**count** *count* | **interval** *interval*}]	（任意）IP 装置追跡テーブルに対し、次のパラメータを設定します。 • **count** *count* : スイッチが ARP プローブを送信する回数を設定します。有効値の範囲は 1 ～ 5 です。デフォルトは 3 です。 • **interval** *interval* : スイッチが ARP プローブを再送する前に、応答を待機する秒数を設定します。有効値の範囲は 30 ～ 300 秒です。デフォルト値は 30 秒です。

	コマンド	目的
ステップ 13	`Router(config)# radius-server host {hostname | ip-address} test username username idle-time 1 key string`	（任意）RADIUS サーバの各パラメータを設定します。 *hostname* または *ip-address* 値には、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。 **key** *string* 値には、RADIUS サーバ上で動作する RADIUS デーモンとスイッチとの間で使用する認証および暗号キーを指定します。キーはテキスト ストリングで、RADIUS サーバで使用する暗号キーと一致する必要があります。 **（注）** キーは、**radius-server host** コマンド構文の末尾で設定してください。これは、先頭のスペースは無視されるが、キーのストリング内または末尾のスペースは使用されるためです。キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。このキーは RADIUS デーモンで使用される暗号と一致する必要があります。 **test username** パラメータは、AAA サーバがアクティブかどうかをテストするための、ダミーのユーザ名の設定に使用します。 **idle-time** パラメータは、サーバの動作ステータスを確認するために行うサーバ テストの実行頻度を設定します。RADIUS サーバへのトラフィックがない場合は、NAD はこの idle-time 値に基づき、RADIUS サーバにダミーの RADIUS パケットを送信します。 複数の RADIUS サーバを使用する場合は、このコマンドを再度入力します。
ステップ 14	`Router(config)# radius-server attribute 8 include-in-access-req`	（任意）スイッチが非応答ホストに接続されている場合に、アクセス要求パケットまたはアカウンティング要求パケット内で、Framed-IP-Address RADIUS 属性（属性 [8]）を送信するようにスイッチを設定します。 Framed-IP-Address 属性を送信しないようにスイッチを設定するには、**no radius-server attribute 8 include-in-access-req** グローバル コンフィギュレーション コマンドを使用します。
ステップ 15	`Router(config)# radius-server vsa send authentication`	VSA を認識および使用するようにネットワーク アクセス サーバを設定します。
ステップ 16	`Router(config)# radius-server dead-criteria {tries | time} value`	1 つまたは両方の基準値（RADIUS サーバを停止状態としてマーキングするために使用）を、指定の定数値に強制的に設定します。
ステップ 17	`Router(config)# eou logging`	（任意）EAPoUDP システム ロギング イベント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 コンフィギュレーション コマンドを使用します。
ステップ 18	`Router(config)# end`	特権 EXEC モードに戻ります。
ステップ 19	`Router# 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。
ステップ 20	`Router# show ip device tracking {all | interface interface-id | ip ip-address | mac mac-address}`	IP 装置追跡テーブル内の各エントリの情報を表示します。
ステップ 21	`Router(# copy running-config startup-config`	（任意）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 ポリシーを適用する例を示します。

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

Show running output
-------------------
aaa new-model
aaa authentication eou default group radius
aaa authorization network default local

ip admission name AAA_DOWN eapoudp event timeout aaa policy identity global_policy

identity policy global_policy
 access-group global_acl

interface FastEthernet2/13
 switchport
 switchport access vlan 222
 switchport mode access
 no ip address
 ip access-group 115 in
 ip admission AAA_DOWN
!
ip access-list extended global_acl
 permit ip any any

radius-server dead-criteria tries 3
radius-server attribute 8 include-in-access-req
radius-server host 40.0.0.4 auth-port 1645 acct-port 1646 test username administrator
idle-time 1 key cisco
radius-server vsa send authentication

Router# 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
Auth-proxy name AAA_DOWN
   eapoudp list not specified auth-cache-time 60 minutes
   Identity policy name global_policy for AAA fail policy
```

NAC のモニタリングおよびメンテナンス

ここでは、NAC を監視およびメンテナンスするために行う作業について説明します。

テーブル エントリの消去

EAPoUDP セッション テーブル内のクライアント エントリを消去するには、**clear eou** 特権 EXEC コマンドを使用します。エントリの削除後、新たにエントリが作成されるのは、スイッチがホストから ARP パケットを受信したあと、またはスイッチがホストに対する DHCP バインディング エントリを作成したあとだけです。

スイッチの IP 装置追跡テーブル内のエントリを消去するには、**clear ip device tracking** 特権 EXEC コマンドを使用します。

NAC 情報の表示

NAC 情報を表示するには、次の作業のいずれかを行います。

コマンド	目的
Router# **show dot1x** [**all** | **interface** *interface_id* | **statistics interface** *interface_id*]	IEEE 802.1x 統計情報、管理ステータス、および動作ステータスを表示します。
Router# **show eou** {**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 エントリについての情報を表示します。
Router# **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。
Router# **show ip device tracking** {**all** | **interface** *interface_id* | **ip** *ip_address* | **mac** *mac_address*}	IP 装置追跡テーブル内の各エントリの情報を表示します。

ヒント　Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。
http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

ヒント