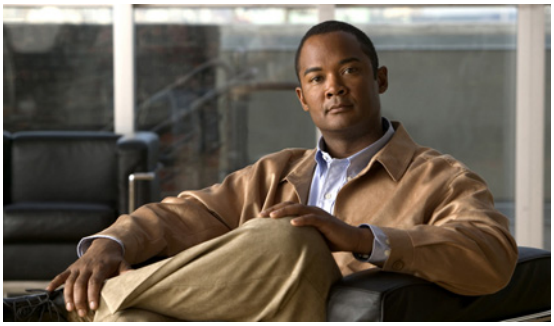


ネットワーク アドミッション コントロール

ネットワーク アドミッション コントロール機能は、増大するワームやウイルスがビジネスのネットワークに与える脅威や影響に対応します。この機能は、顧客がセキュリティの脅威を認識して防御し、適合するのに役立つ Cisco Self-Defending Network Initiative（自己防衛型ネットワーク構想）の一部です。

Cisco Network Admission Control（NAC; ネットワーク アドミッション コントロール）機能は、その初期段階で、エンドポイントがネットワークに接続しようとしたときに Cisco ルータがアクセス権限を制限できるようにします。このアクセスの決定は、現在のアンチウイルスの状態などのエンドポイント装置の情報に基づいて行うことができます。アンチウイルスの状態には、アンチウイルス ソフトウェアのバージョン、ウイルス定義、およびスキャン エンジンのバージョンなどの情報が含まれます。

ネットワーク アドミッション コントロール システムにより、非準拠デバイスのアクセスの拒否、検疫エリアへの配置、またはコンピューティング リソースへの制限付きアクセスの許可が可能になり、非セキュアなノードからネットワークに感染するのを防ぐことができます。

Cisco NAC プログラムの主要なコンポーネントは Cisco Trust Agent です。このコンポーネントはエンドポイント システムに常駐して、ネットワーク上の Cisco ルータと通信します。Cisco Trust Agent は、使用されているアンチウイルス ソフトウェアなどのセキュリティ状態の情報を収集し、この情報を Cisco ルータに送信します。次に、この情報は、Cisco Secure Access Control Server（ACS）にリレーされ、そこでアクセス コントロールが決定されます。ACS は、Cisco ルータに、エンドポイントに対し強制を実施するよう指示します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「ネットワーク アドミッション コントロールの機能情報」（P.29）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

この章の構成

ネットワーク アドミッション コントロールの前提条件

- Cisco IOS ルータでは、Cisco IOS ソフトウェア リリース 12.3(8)T 以降を実行する必要があります。
- エンドポイント装置（PC や ラップトップなど）には Cisco Trust Agent をインストールする必要があります。
- Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）には Cisco Secure ACS が必要です。
- Access Control List（ACL; アクセス コントロール リスト）および AAA の設定に関する豊富な知識と技術が必要です。

ネットワーク アドミッション コントロールの制約事項

- この機能は、Cisco IOS ファイアウォール フィーチャ セットのみで使用できます。

ネットワーク アドミッション コントロールの概要

ネットワーク アドミッション コントロール機能を設定する前に、次の概念を理解しておく必要があります。

ウイルスの感染とネットワークへの影響

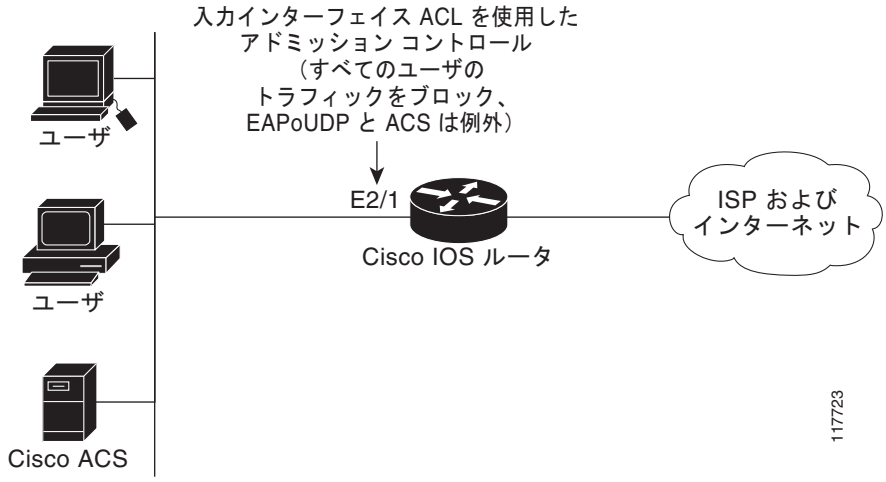
ウイルスの感染は、ネットワークに対する重大なセキュリティ違反のうち、単独では最大の原因であり、経済的に多大な損失をもたらすことが少なくありません。ウイルス感染源は非セキュアなエンドポイント（PC、ラップトップ、およびサーバなど）にあります。エンドポイントにアンチウイルス ソフトウェアがインストールされている場合でも、そのソフトウェアがディセーブルになっている場合がよくあります。ソフトウェアがイネーブルになっていても、エンドポイントに最新のウイルス定義やスキャン エンジンがない場合もあります。セキュリティのリスクを拡大するのは、アンチウイルス ソフトウェアをインストールしていない装置です。現在のアンチウイルス ベンダーは、アンチウイルス ソフトウェアを簡単にディセーブルにできないようにしていますが、古いウイルス定義やスキャン エンジンのリスクには対応していません。

ネットワーク アドミッション コントロールのしくみ

通常、エンドポイント システムまたはクライアントは、PC、ラップトップ、ワークステーション、およびサーバなどのネットワーク上のホストになっています。エンドポイント システムは潜在的なウイルス感染源であるため、ネットワーク アクセスを許可する前に、これらのアンチウイルスの状態を検証する必要があります。エンドポイントがアップストリームのシスコ ネットワーク アクセス装置（通常は Cisco IOS ルータ）を介してネットワークに IP 接続しようとすると、ルータはエンドポイントにアンチウイルスの状態を要求します。エンドポイント システムは Cisco Trust Agent と呼ばれるクライアントを実行して、エンド デバイスからアンチウイルスの状態に関する情報を収集し、その情報をシスコのネットワーク アクセス装置に転送します。次に、この情報は Cisco Secure ACS に送信されます。ACS では、エンドポイントのアンチウイルスの状態を検証し、アクセス コントロールを決定して、シスコ ネットワーク アクセス装置に返します。ネットワーク デバイスでは、エンド デバイスの許可、拒否、または検疫が行われます。Cisco Secure ACS では、エンドポイントのアンチウイルスの状態を評価する際に、バックエンドのアンチウイルス ベンダー固有のサーバを順に使用することもできます。

図 1 に、Cisco Network Admission Control の動作を示します。

図 1　　Cisco IOS Network Admission Control システム



ネットワーク アクセス装置

通常、Network Access Device（NAD; ネットワーク アクセス装置）は、Cisco IOS ルータ（レイヤ 3 Extensible Authentication Protocol over User Datagram Protocol（EAPoUDP）アクセス ポイント）であり、インターネットやリモートの企業ネットワークなどの外部ネットワークに接続しています。Cisco Network Admission Control 機能にはインターセプト ACL がある場合があります。インターセプト ACL は、ネットワーク アドミッション用に代行受信される接続を決定します。アクセス リストと一致するエンドポイントからの接続はネットワーク アドミッション コントロールによって代行受信され、ネットワーク アクセスを許可する前に、レイヤ 3 アソシエーションに対してアンチウイルスの状態が要求されます。

Cisco Trust Agent

Cisco Trust Agent は、エンドポイント システムで実行される専門のソフトウェアです。Cisco Trust Agent は、エンドポイント システムのアンチウイルスの状態に関するルータからの要求に応答します。エンドポイント システムが Cisco Trust Agent を実行していない場合、ネットワーク アクセス装置（ルータ）はそのエンドポイント システムを「クライアントレス」として分類します。ネットワーク アクセス装置は EOU clientless ユーザ名と EOU clientless パスワードを使用します。これは、Cisco Secure ACS での検証のためにエンドポイント システムのクレデンシャルとしてネットワーク アクセス装置に設定されます。このユーザ名に関連付けられるポリシー アトリビュートは、エンドポイント システムに対して実行されます。

Cisco Secure ACS

Cisco Secure ACS は、業界標準の RADIUS 認証プロトコルを使用して、ネットワーク アドミッション コントロールに認証、認可、およびアカウンティング 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のクレデンシャルに基づいて、ネットワーク アクセス装置にアクセス コントロールの決定を返します。

RADIUS の cisco_av_pair Vendor-Specific Attributes（VSA; ベンダー固有アトリビュート）を使用して、Cisco Secure ACS に次の Attribute-Value ペア（AV ペア）を設定できます。AV ペアは、他のアクセス コントロール アトリビュートと一緒にネットワーク アクセス装置に送信されます。

- url-redirect：AAA クライアントが HTTP 要求を代行受信し、それを新しい URL にリダイレクトできるようにします。このリダイレクションは、ポスチャ検証の結果、ネットワーク アクセス コントロールのエンドポイントが修復 Web サーバで利用可能なアップデートまたはパッチが必要となる場合に特に便利です。たとえば、新しいウイルスの Directory Administration Tool（DAT）ファイルまたはオペレーティング システムのパッチをダウンロードして適用する場合に、修復 Web サーバにユーザをリダイレクトすることができます（次の例を参照してください）。

  ```
  url-redirect=http://10.1.1.1
  ```

- posture-token：Cisco Secure ACS が、ポスチャ確認で取得した System Posture Token（SPT）のテキスト バージョンを送信できるようにします。SPT は常に数値形式で送信されます。posture-token AV ペアを使用すると、AAA クライアントでポスチャ検証要求の結果を簡単に表示できます（次の例を参照してください）。

  ```
  posture-token=Healthy
  ```

  有効な SPT は次のとおりです（最善のものから順に示します）。

  - Healthy
  - Checkup

  - Quarantine
  - Infected
  - Unknown

- status-query-timeout : AAA クライアントの status-query のデフォルト値をユーザが指定した値（秒）で上書きします（次の例を参照してください）。

  ```
  status-query-timeout=150
  ```

Cisco IOS ソフトウェアがサポートする AV ペアの詳細については、ご使用の AAA クライアントに実装されている Cisco IOS ソフトウェア リリースのマニュアルを参照してください。

修復

ネットワーク アドミッション コントロールは、任意の HTTP 要求をエンドポイント装置から指定されたリダイレクト アドレスにリダイレクトする HTTP リダイレクションをサポートします。このサポート メカニズムにより、すべての HTTP 要求は発信元から指定された Web ページ（URL）にリダイレクトされ、そこで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。HTTP リダイレクションが機能するには、ACS で「url-redirect」VSA の値を設定し、それに応じてエンドポイント システムのアクセスを許可するダウンロード可能な ACL のアクセス コントロール エントリをリダイレクト URL アドレスに関連付ける必要があります。url-redirect VSA の値が設定され、アクセス コントロール エントリが関連付けられたら、IP アドミッション インターセプト ACL に一致する HTTP 要求は、指定されたリダイレクト URL アドレスにリダイレクトされます。

ネットワーク アドミッション コントロールと認証プロキシ

ネットワーク アドミッション コントロールと認証プロキシを、特定のインターフェイスの同じホストセットに設定することができます。それぞれのケースで、IP アドミッションの EAPoUDP と認証プロキシのインターセプト ACL が同じである必要があります。プロキシ認証を使用する IP アドミッション プロキシを最初に設定し、その後で IP アドミッション コントロールを設定する必要があります。

NAC MIB

NAC MIB 機能は、NAC サブシステムに Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）のサポートを追加します。管理者は、SNMP コマンド（get および set 操作）を使用して、NAD の NAC セッションをモニタおよび制御することができます。

SNMP の get および set 操作の詳細については、「その他の参考資料」の「関連資料」を参照してください。

SNMP Get 操作および Set 操作と Cisco CLI の相互関係

NAC MIB（CISCO-NAC-NAD-MIB.my）のオブジェクト テーブルにあるほとんどのオブジェクトは、NAD のセットアップに適用できるさまざまな EAPoUDP およびセッション パラメータを表しています。SNMP のさまざまな get 操作および set 操作を実行することによって、これらのプロパティを表示したり変更できます。また、対応する Command-Line Interface（CLI; コマンドライン インターフェイス）をルータに設定することで、多くのテーブル オブジェクトの値を表示したり変更することもできます。たとえば、SNMP get 操作を cnnEOUGlobalObjectsGroup テーブルで実行したり、**show eou** コ

マンドをルータに設定したりすることができます。SNMP get 操作で取得されるパラメータ情報は、**show eou** コマンドの出力と同じです。同様に、SNMP get 操作を cnnEouIfConfigTable で実行すると、**show eou** コマンドの出力にも表示可能なインターフェイス固有のパラメータが提供されます。

SNMP set 操作は、対応する CLI コマンドがあるテーブル オブジェクトに使用できます。これを使用してテーブル オブジェクトの値を変更できます。たとえば、cnnEouHostValidateAction MIB テーブルの cnnEouHostValidateAction オブジェクトの値の範囲を 2 に変更するには、SNMP set 操作を実行するか、ルータに **eou initialize all** コマンドを設定します。

NAC MIB の出力例については、「ネットワーク アドミッション コントロールの設定例」の「NAC MIB の出力：例」を参照してください。

セッションの初期化と再検証

NAC を使用すると、管理者は次の CLI コマンドを使用してセッションの初期化と再検証を実行できます。

- **eou initialize all**
- **eou initialize authentication clientless**
- **eou initialize authentication eap**
- **eou initialize authentication static**
- **eou initialize ip** {*ip-address*}
- **eou initialize mac** {*mac-address*}
- **eou initialize posturetoken** {*string*}
- **eou revalidate all**
- **eou revalidate authentication clientless**
- **eou revalidate authentication eap**
- **eou revalidate authentication static**
- **eou revalidate ip** {*ip-address*}
- **eou revalidate mac** {*mac-address*}
- **eou revalidate posturetoken** {*string*}

また、cnnEouHostValidateAction テーブルのオブジェクトに SNMP set 操作を実行することで、初期化と再検証のアクションを実行することもできます。セッションの初期化と再検証の詳細については、「cnnEouHostValidateAction テーブル オブジェクトに関連する CLI コマンド」を参照してください。

cnnEouHostValidateAction テーブル オブジェクトに対して実行可能な変更に関連する CLI コマンドの例については、「ネットワーク アドミッション コントロールの設定例」の「NAC MIB の出力：例」を参照してください。

Session-Specific 情報

NAC MIB では、cnnEouHostQueryTable と cnnEouHostResultTable を使用して session-specific の詳細を表示する方法を用意しています。クエリーを作成するには、cnnEouHostQueryTable を使用します。クエリーは、**show eou ip** {*ip-address*} コマンドと同じ形式です（つまり、IP アドレスは **show eou ip** コマンドの場合と同様（例：10.1.1.1）に表示されます）。管理者は、cnnEouHostQueryTable のオブジェクトに対して SNMP set 操作を使用して、クエリーを作成する必要があります。クエリーの結果は cnnEouHostResultTable の行として保存されます。session-specific の詳細の表示については、「MIB クエリーの結果の表示」を参照してください。

show コマンドを使用した MIB オブジェクト情報の表示

CLI コマンド **show eou**、**show eou all**、**show eou authentication**、**show eou initialize**、**show eou ip**、**show eou mac**、**show eou posturetoken**、**show eou revalidate**、および **show ip device tracking all** を使用すると、SNMP get 操作を使用した場合の CISCO-NAC-NAD-MIB テーブルと同じ出力情報が得られます。

MIB オブジェクト テーブルでも表示可能な **show** コマンドの出力情報の例については、「ネットワーク アドミッション コントロールの設定例」の「NAC MIB の出力：例」を参照してください。

ネットワーク アドミッション コントロールの設定方法

ここでは、次の各手順について説明します。

ACL およびアドミッション コントロールの設定

ネットワーク アドミッション コントロールは、すべてのインターフェイスの着信方向に適用されます。ネットワーク アドミッション コントロールをインターフェイスの着信に適用すると、ネットワーク アドミッション コントロールはルータを介してインターセプト エンド システムの最初の IP 接続を代行受信します。

図 1 に、LAN インターフェイスで適用される IP アドミッション コントロールを示します。ルータを介して最初の IP 接続が行われるときに、すべてのネットワーク装置でアンチウイルスの状態を検証する必要があります。それまでは、エンドポイント システムからのすべてのトラフィック（EAPoUDP および Cisco Secure ACS のトラフィックを除く）はインターフェイスでブロックされます。

次に、エンドポイント システムには、EAPoUDP アソシエーションのアンチウイルスの状態が要求されます。Cisco Secure ACS によって評価されたときに、エンドポイント システムがネットワーク アドミッション コントロール ポリシーに準拠していれば、エンドポイント システムはネットワークにアクセスすることができます。エンドポイント システムが準拠していなかった場合、その装置はアクセスを拒否されるか、検疫されます。

インターセプト ACL を設定するには、次の手順の詳細を実行します。

この設定では、インターセプト ACL は「101」として定義され、インターセプト ACL は IP アドミッション コントロール ルール「greentree」に関連付けられます。192.50.0.0 のネットワークを宛先とするすべての IP トラフィックが検証の対象となります。また、ステップ 5 以降では、インターセプト ACL はネットワーク アドミッション コントロールに関連付けられたインターフェイスに対する着信に適用されます。通常、この ACL は、エンドポイント システムが検証されるまでエンドポイント システムへのアクセスをブロックします。この ACL はデフォルト アクセス リストと呼ばれます。

手順の概要

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* {**permit** | **deny**} *protocol source destination*
4. **ip admission name** *admission-name* [**eapoudp** | **proxy** {**ftp** | **http** | **telnet**}] [**list** {*acl* | *acl-name*}]
5. **interface** *type slot*/*port*
6. **ip address** *ip-address mask*
7. **ip admission** *admission-name*
8. **exit**
9. **access-list** *access-list-number* {**permit** | **deny**} *protocol source destination*
10. **ip access-group** {*access-list-number* | *access-list-name*} **in**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `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 3	**access-list** *access-list-number* {**permit** | **deny**} *protocol source destination* **例：** `Router (config)# access-list 101 permit ip any 192.50.0.0 0.0.0.255`	番号付きのアクセス リストを定義します。

	コマンドまたはアクション	目的
ステップ 4	**ip admission name** *admission-name* [**eapoudp** | **proxy** {**ftp** | **http** | **telnet**}] [**list** {*acl* | *acl-name*}] **例：** `Router (config)# ip admission name greentree eapoudp list 101`	IP ネットワーク アドミッション コントロール ルールを作成します。このルールは、アドミッション コントロールを適用する方法を定義します。次のルールがあります。 • **eapoudp**：EAPoUDP を使用して IP ネットワーク アドミッション コントロールを指定します。 • **proxy ftp**：認証プロキシを起動する FTP を指定します。 • **proxy http**：認証プロキシを起動する HTTP を指定します。 • **proxy telnet**：認証プロキシを起動する Telnet を指定します。 名前付きのルールを ACL と関連付けて、アドミッション コントロール機能を使用するホストを制御できます。標準のアクセス リストが定義されていない場合、設定されたインターフェイスで接続開始パケットを受信するすべてのホストからの IP トラフィックを、名前付きのアドミッション ルールが代行受信します。 list オプションを使用すると、標準、拡張（1 ～ 199）、または名前付きのアクセス リストを名前付きのアドミッション コントロール ルールに適用できます。アクセス リストにあるホストによって開始された IP 接続は、アドミッション コントロール機能によって代行受信されます。
ステップ 5	**interface** *type slot/port* **例：** `Router (config)# interface ethernet 2/1`	インターフェイスを定義し、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	**ip address** *ip-address mask* **例：** `Router (config-if)# ip address 192.0.0.1 255.255.255.0`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。
ステップ 7	**ip admission** *admission-name* **例：** `Router (config-if)# ip admission greentree`	名前付きのアドミッション コントロール ルールをインターフェイスに適用します。
ステップ 8	**exit** **例：** `Router (config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的

ステップ 9	**access-list** *access-list-number* {**permit** | **deny**} *protocol source destination*
	
	例：
	`Router (config)# access-list 105 permit udp any any`
	
	または
	
	`Router (config)# access-list 105 permit ip host 192.168.0.2 any`
	
	または
	
	`Router (config)# access-list 105 deny ip any any`
		番号付きのアクセス リストを定義します。
		
		（注） 「コマンドまたはアクション」の最初の 2 つの例では、ACL 「105」が UDP および 192.168.0.2（Cisco Secure ACS）へのアクセスを除くすべての IP トラフィックを拒否します。
		
		（注） 「コマンドまたはアクション」の 3 番めの例では、ACL「105」はネットワーク アドミッション コントロールに設定されたインターフェイスに適用され、EAPoUDP トラフィックおよび Cisco Secure ACS へのアクセス（この例では 192.168.0.2）を除くエンドポイント システムへのアクセスは、アンチウイルスの状態が検証されるまでブロックされます。この ACL（「105」）は「インターフェイス ACL」と呼ばれます。

ステップ 10	**ip access-group** {*access-list-number* | *access-list-name*} **in** **例：** `Router (config)# ip access-group 105 in`	インターフェイスへのアクセスを制御します。

グローバルな EAPoUDP の値の設定

グローバルな EAPoUDP の値を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **eou {allow | clientless | default | initialize | logging | max-retry | port | rate-limit | revalidate | timeout}**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `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 3	**eou** {**allow** | **clientless** | **default** | **initialize** | **logging** | **max-retry** | **port** | **rate-limit** | **revalidate** | **timeout**} **例：** `Router (config)# eou initialize`	EAPoUDP の値を指定します。 • **eou** コマンドで使用可能なキーワードと引数の詳細については、次のコマンドを参照してください。 – **eou allow** – **eou clientless** – **eou default** – **eou initialize** – **eou logging** – **eou max-retry** – **eou port** – **eou rate-limit** – **eou revalidate** – **eou timeout**

インターフェイス固有の EAPoUDP アソシエーションの設定

ネットワーク アドミッション コントロールに関連付けられた特定のインターフェイスに変更またはカスタマイズ可能な EAPoUDP アソシエーションを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type slot/port*
4. **eou** [**default** | **max-retry** | **revalidate** | **timeout**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `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 3	**interface** *type slot*/*port* **例：** `Router (config)# interface ethernet 2/1`	インターフェイスを定義し、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	**eou** [**default** | **max-retry** | **revalidate** | **timeout**] **例：** `Router (config-if)# eou revalidate`	特定の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ます。 • **eou** コマンドで使用可能なキーワードと引数の詳細については、次のコマンドを参照してください。 – **eou default** – **eou max-retry** – **eou revalidate** – **eou timeout**

EAPoUDP の AAA の設定

EAPoUDP の AAA を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication eou default enable group radius**
5. **aaa authorization network default group radius**
6. **radius-server host** {*hostname* | *ip-address*}
7. **radius-server key** {**0** *string* | **7** *string* | *string*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `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 3	**aaa new-model** **例：** `Router (config)# aaa new-model`	AAA アクセス コントロール モデルをイネーブルにします。
ステップ 4	**aaa authentication eou default enable group radius** **例：** `Router (config)# aaa authentication eou default enable group radius`	EAPoUDP アソシエーションの認証リストを設定します。
ステップ 5	**aaa authorization network default group radius** **例：** `Router (config)# aaa authorization network default group radius`	認証にすべての RADIUS サーバのリストを使用します。
ステップ 6	**radius-server host** {*hostname* | *ip-address*} **例：** `Router (config)# radius-server host 192.0.0.40`	RADIUS サーバ ホストを指定します。
ステップ 7	**radius-server key** {**0** *string* | **7** *string* | *string*} **例：** `Router (config)# radius-server key cisco`	ルータと RADIUS デーモンとの間におけるすべての RADIUS 通信用の認証および暗号化キーを設置得します。

アイデンティティ プロファイルとポリシーの設定

アイデンティティとは、ローカル プロファイルとポリシーの設定の指定に使用される共通のインフラストラクチャです。アイデンティティ プロファイルを使用すると、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、個々のデバイスをスタティックに認可または検証できます。スタティックに認証されたそれぞれのデバイスを、ネットワーク アクセス コントロール アトリビュートを指定したローカル ポリシーと関連付けることができます。**identity profile** コマンドを使用してホストを「例外リスト」に追加し、**identity policy** コマンドを使用して対応するポリシーをそのホストに関連付けます。

クライアントがアイデンティティに含まれる（つまり、クライアントが例外リストに記載されている）場合、そのクライアントのステータスはアイデンティティの設定に基づいて設定されます。クライアントではポスチャ検証処理を実行する必要はありません。また、関連するアイデンティティ ポリシーがそのクライアントに適用されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **identity profile eapoudp**
4. **device** {**authorize** {**ip address** *ip-address* {**policy** *policy-name*} | **mac-address** *mac-address* | **type** {**cisco** | **ip** | **phone**}} | **not-authorize**}
5. **exit**
6. **identity policy** *policy-name* [**access-group** *group-name* | **description** *line-of-description* | **redirect** *url* | **template** [**virtual-template** *interface-name*]]
7. **access-group** *group-name*
8. **exit**
9. **exit**
10. **ip access-list extended** *access-list-name*
11. {**permit** | **deny**} *source source-wildcard destination destination-wildcard*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `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 3	**identity profile eapoudp** **例：** `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 4	**device** {**authorize** {**ip address** *ip-address* {**policy** *policy-name*}	**mac-address** *mac-address*	**type** {**cisco**	**ip**	**phone**}}	**not-authorize**} **例：** `Router (config-identity-prof)# device authorize ip address 10.10.142.25 policy policyname1`	IP デバイス をスタティックに認可し、そのデバイスに関連するポリシーを適用します。
ステップ 5	**exit** **例：** `Router (config-identity-prof)# 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 モードを終了します。

	コマンドまたはアクション	目的
ステップ 6	**identity policy** *policy-name* [**access-group** *group-name* | **description** *line-of-description* | **redirect** *url* | **template** [**virtual-template** *interface-name*]] **例：** `Router (config-identity-prof)# identity policy policyname1`	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 7	**access-group** *group-name* **例：** `Router (config-identity-policy)# access-group exempt-acl`	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。
ステップ 8	**exit** **例：** `Router (config-identity-policy)# exit`	アイデンティティ ポリシー コンフィギュレーション モードを終了します。
ステップ 9	**exit** **例：** `Router (config-identity-prof)# 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 モードを終了します。
ステップ 10	**ip access-list extended** *access-list-name* **例：** `Router (config)# ip access-list extended exempt-acl`	スタティックに認証されたデバイスのアクセス コントロールを定義します（また、ネットワーク アクセス コントロール コンフィギュレーション モードを開始します）。
ステップ 11	{**permit** | **deny**} *source source-wildcard destination destination-wildcard* **例：** `Router (config-ext-nacl)# permit ip any 192.50.0.0. 0.0.0.255`	パケットが名前付きの IP アクセス リストを渡すことができる条件を設定します。

インターフェイスに関連付けられた EAPoUDP セッションのクリア

特定のインターフェイスに関連付けられた EAPoUDP セッション、または NAD の EAPoUDP セッションをクリアするには、次の手順を実行します。

手順の概要

1. **enable**
2. **clear eou all**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**clear eou all** **例：** `Router# clear eou all`	NAD の EAPoUDP セッションをすべてクリアします。

ネットワーク アドミッション コントロールの確認

EAP および EAPoUDP のメッセージまたはセッションを確認するには、次の手順を実行します。**show** コマンドは、他の **show** コマンドには依存せず、どんな順番でも使用できます。

手順の概要

1. **enable**
2. **show eou all**
3. **show ip admission eapoudp**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**show eou all** **例：** `Router# show eou all`	ネットワーク アクセス装置の EAPoUDP セッションに関する情報を表示します。
ステップ 3	**show ip admission eapoudp** **例：** `Router# show ip admission eapoudp`	ネットワーク アドミッション コントロールの設定、またはネットワーク アドミッションのキャッシュ エントリを表示します。

ネットワーク アドミッション コントロールのトラブルシューティング

次のコマンドを使用して、EAP および EAPoUDP のメッセージまたはセッションに関する情報を表示できます。**debug** コマンドは、他の **debug** コマンドには依存せず、どんな順番でも使用できます。

手順の概要

1. **enable**
2. **debug eap** {**all** | **errors** | **packets** | **sm**}

3. **debug eou {all | eap | errors | packets | sm}**
4. **debug ip admission eapoudp**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**debug eap {all	errors	packets	sm}** **例：** `Router# debug eap all`	EAP メッセージに関する情報を表示します。
ステップ 3	**debug eou {all	eap	errors	packets	sm}** **例：** `Router# debug eou all`	EAPoUDP メッセージに関する情報を表示します。
ステップ 4	**debug ip admission eapoudp** **例：** `Router# debug ip admission eapoudp`	IP アドミッション イベントに関する情報を表示します。

CISCO-NAC-NAD-MIB を使用した NAC のモニタおよび制御

ここでは、次の作業について説明します。

- 「cnnEouHostValidateAction テーブル オブジェクトに関連する CLI コマンド」（P.18）
- 「cnnEouIfConfigTable オブジェクトに関連する CLI コマンド」（P.18）
- 「cnnEouHostValidateAction テーブル オブジェクトに関連する CLI コマンド」（P.18）
- 「MIB クエリー テーブルの作成」（P.19）
- 「MIB クエリーの結果の表示」（P.22）

cnnEouGlobalObjectsGroup テーブル オブジェクトに関連する CLI コマンド

SNMP get または set 操作を実行して、cnnEouGlobalObjectsGroup テーブルにあるオブジェクトの値の範囲に関する情報を取得または変更できます。同じ情報は、**show eou** コマンドの出力でも表示できます。表 1 に、一部のグローバル設定オブジェクトと、その値を取得または変更するのに必要な SNMP get および set 操作の例を示します。

show eou コマンドの出力例については、「show eou」（P.25）を参照してください。

表 1　SNMP Get および Set 操作を使用したグローバル設定値の取得および変更

グローバル設定オブジェクト	SNMP の操作
EAPoUDP のバージョン	cnnEouVersion オブジェクトに対して get 操作を実行します（オブジェクトの値は「1」です）。

表 1　SNMP Get および Set 操作を使用したグローバル設定値の取得および変更（続き）

グローバル設定オブジェクト	SNMP の操作
EAPoUDP ポート	cnnEouPort オブジェクトに対して get 操作を実行します。
ロギングのイネーブル化（EOU ロギングのイネーブル化）	cnnEouLoggingEnable オブジェクトを設定します（オブジェクトの値は「true」です）。

cnnEouIfConfigTable オブジェクトに関連する CLI コマンド

cnnEouIfConfigTable にあるオブジェクトの値の範囲に関する情報を取得するには、SNMP get 操作を実行します。同じ情報は、**show eou** コマンドの出力でも表示できます。表 2 に、一部のインターフェイス固有の設定オブジェクトと、その値を取得するのに必要な SNMP get 操作の例を示します。

表 2　SNMP Get 操作を使用したインターフェイス固有の設定値の取得

インターフェイス固有のオブジェクト	SNMP の操作
AAA タイムアウト	cnnEouIfTimeoutAAA オブジェクトに対して get 操作を実行します。 • 形式：GET cnnEouIfTimeoutAAA.IfIndex • 特定のインターフェイスの対応するインデックス番号を指定する必要があります。
最大リトライ回数	cnnEouIfMaxRetry オブジェクトに対して get 操作を実行します。 • 形式：GET cnnEouIfMaxRetry.IfIndex

cnnEouHostValidateAction テーブル オブジェクトに関連する CLI コマンド

CLI を実行するか、cnnEouHostValidateAction テーブルに対して SNMP set 操作を使用すると、EOU セッションを初期化または再検証できます。

次に、MIB オブジェクトに関連する一部の例（CLI コマンドの一覧）を示します。

eou initialize all

すべてのセッションの EOU の初期化を実行するには、**eou initialize all** コマンドを使用するか、cnnEouHostValidateAction オブジェクトに対して SNMP set 操作を使用します。このオブジェクトには数値 2 を設定する必要があります。

eou initialize authentication clientless

認証タイプが「クライアントレス」のセッションの EOU の初期化を実行するには、**eou initialize authentication clientless** コマンドを使用するか、cnnEouHostValidateAction オブジェクトに対して SNMP set 操作を使用します。このオブジェクトには数値 3 を設定する必要があります。

eou initialize ip

特定のセッションの EOU の初期化を実行するには、**eou initialize ip** {*ip-address*} コマンドを使用します。

SNMP 操作を使用して同じ結果を得るには、cnnEouHostValidateAction MIB テーブルに次の 3 つのオブジェクトを設定する必要があります。

- cnnEouHostValidateAction：値の範囲を設定する必要があります。

- cnnEouHostValidateIpAddrType：IP アドレスのタイプを設定する必要があります。現在 NAC でサポートされているアドレス タイプは IPv4 のみであるため、この値を Ipv4 に設定する必要があります（この値は、cnnEouHostValidateIPAddr オブジェクトに設定されるアドレス タイプです）。
- cnnEouHostValidateIPAddr：IP アドレスを設定する必要があります。

（注） この 3 つの MIB オブジェクトは 1 回の SNMP set 操作で設定する必要があります。

eou initialize posturetoken

eou initialize posturetoken {*string*} コマンドを使用すると、特定の posturetoken を持つすべてのセッションを初期化できます。このコマンドのデフォルト値の範囲は 8 です。

SNMP set 操作を使用して同じ結果を得るには、次のオブジェクトを設定する必要があります。

- cnnEouHostValidateAction：この値を 8 に設定します。
- cnnEouHostValidatePostureTokenStr：文字列の値を設定します。

（注） この 2 つの MIB オブジェクトは 1 回の SNMP set 操作で設定する必要があります。

MIB クエリー テーブルの作成

MIB テーブル cnnEouHostQueryTable は、MIB クエリーの作成または構築に使用されます。

show eou all CLI コマンドに関連する MIB クエリー

show eou all コマンドを使用した場合と同じ結果が得られるクエリーを構築するには、次の SNMP get 操作を実行します。

cnnEouHostQueryTable テーブルの cnnEouHostQueryMask オブジェクトは、クエリーの種類を表しています。**show eou all** コマンドの出力に対応する cnnEouHostQueryMask オブジェクトの値は 8（整数値）です。

手順の概要

1. cnnEouHostQueryStatus オブジェクトに createandgo を設定します。
2. cnnEouHostQueryMask オブジェクトに 8 を設定します。
3. cnnEouHostQueryStatus オブジェクトをアクティブに設定して、クエリーの作成が完了したことを示します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	cnnEouHostQueryStatus オブジェクトに createandgo を設定します。	クエリーの行を作成します。
ステップ 2	cnnEouHostQueryMask オブジェクトに 8 を設定します。	**show eou all** コマンドの値に対応します。
ステップ 3	cnnEouHostQueryStatus オブジェクトをアクティブに設定します。	クエリーの構築が終了したことを示します。

（注） 前の表では例を示していません。これは、使用しているソフトウェアによって形式が異なるためです。

この次の手順

結果を表示します。「show eou all コマンドに関連する MIB クエリーの結果の表示」の項を参照してください。

show eou all コマンドに関連する MIB クエリーの結果の表示

MIB クエリーを構築し、「アクティブ」ステータスで終了したことを示したら、結果を表示できます。cnnEouHostQueryTable のクエリーは行で表されます。行番号はクエリー インデックスになります。同様に、cnnEouHostResultTable は結果の行で構成されます。cnnEouHostResultTable の各行は、クエリー インデックスと結果インデックスの組み合わせによって一意に識別されます。cnnEouHostQueryTable の結果のインデックスと cnnEouHostResultTable は一致する必要があります。クエリー テーブル内の 1 行を、結果テーブル内の複数行の 1 つに一致させます。たとえば、**show** コマンドに対応するクエリーの結果が 10 個のセッションになった場合、結果テーブルには 10 行存在し、各行が特定のセッションに対応します。結果テーブルの 1 番めの行は R1.1 です。2 番めの行は R1.2 となり、R1.10 まで続きます。クエリー テーブルに別のクエリーが作成され、その結果が 5 個のセッションになった場合、結果テーブルには 5 行作成されます（R2.1、R2.2、R2.3、R2.4、R2.5）。

表 3 に、クエリー テーブルのセッションが結果テーブルの行にマップされる方法を示します。

表 3　　クエリー テーブルと結果テーブルのマッピング

クエリー テーブル	結果テーブルの行
Q1（10 セッション）	R1.1、R1.2、R1.3、R1.4、R1.5、R1.6、R1.7、R1.8、R1.9、R1.10
Q2（5 セッション）	R2.1、R2.2、R2.3、R2.4、R2.5

SNMP クエリーの作成

show eou ip {*ip-address*} コマンドの出力と同じ情報を得られる SNMP クエリーを作成するには、次の手順を実行します。

手順の概要

1. cnnEouHostQueryStatus に createandgo を設定します。
2. cnnEouHostQueryIpAddrType に IPv4 および IP アドレス（たとえば 10.2.3.4）を設定します。
3. cnnEouHostQueryStatus をアクティブに設定します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	cnnEouHostQueryStatus に createandgo を設定します。	クエリーの行を作成します。
ステップ 2	cnnEouHostQueryIpAddrType に IPv4 および IP アドレス（たとえば 10.2.3.4）を設定します。	アドレス タイプを設定します。 • 現在 NAC でサポートされているアドレス タイプは IPv4 のみです。
ステップ 3	cnnEouHostQueryStatus をアクティブに設定します。	クエリーの構築が終了したことを示します。

（注） 前の表では例を示していません。これは、使用しているソフトウェアによって形式が異なるためです。

結果の表示

cnnEouHostResultTable の結果を表示するには、次の手順を実行します。

手順の概要

1. cnnEouHostQueryRows に対して get 操作を実行します。
2. resultTableObjectName.QueryIndex.ResultIndex の形式で、cnnEouHostResultTable オブジェクトに対して get 操作を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	cnnEouHostQueryRows に対して get 操作を実行します。	特定のクエリーで結果テーブルに作成された行数を検索します。 • クエリーの行がマイナスの数字である場合、そのクエリーはまだ処理中です。
ステップ 2	resultTableObjectName.QueryIndex.ResultIndex の形式で、cnnEouHostResultTable オブジェクトに対して get 操作を実行します。	結果テーブルで特定のクエリーに一致する特定のオブジェクトの値を検索します。 • 1 つのクエリーに対して結果テーブルに複数行がある場合、ResultIndex の範囲は 1 から cnnEouHostQueryRows の値までになります。

（注） 前述の表では例を示していません。これは、使用しているソフトウェアによって形式が異なるためです。

show eou ip コマンドに関連する MIB クエリー

show eou ip {*ip-address*} コマンドと同じ結果が得られる MIB クエリーを構築するには、次の SNMP get 操作を実行します。

手順の概要

1. cnnEouHostQueryStatus オブジェクトに createandgo を設定します。
2. cnnEouHostQueryIpAddrType オブジェクトに「IPv4」を設定します。
3. cnnEouHostQueryIpAddr オブジェクトに IP アドレス（たとえば 10.2.3.4）を設定します。
4. cnnEouHostQueryStatus オブジェクトをアクティブに設定します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	cnnEouHostQueryStatus オブジェクトに createandgo を設定します。	クエリーのステータスを設定します。
ステップ 2	cnnEouHostQueryIpAddrType オブジェクトに「IPv4」を設定します。	アドレス タイプを設定します。 （注） 現在 NAC でサポートされているアドレス タイプは IPv4 のみです。
ステップ 3	cnnEouHostQueryIpAddr オブジェクトに IP アドレス（たとえば 10.2.3.4）を設定します。	IP アドレスを設定します。
ステップ 4	cnnEouHostQueryStatus オブジェクトをアクティブに設定します。	クエリーの構築が終了したことを示します。

（注） 前の表では例を示していません。これは、使用しているソフトウェアによって形式が異なるためです。

MIB クエリーの結果の表示

MIB クエリーを構築したら、cnnEouHostResultTable の結果を表示できます。結果の確認方法の詳細については、「show eou all コマンドに関連する MIB クエリーの結果の表示」（P.20）を参照してください。

クエリーのサブクエリーへの分割

show eou all コマンドに関連する MIB クエリーを実行すると、2,000 もの行が出力される場合があります。MIB クエリーのすべての情報を確実に表示できるようにするために、そのクエリーをサブクエリーに分割することができます。たとえば、クエリーの出力が 2,000 行になる場合、クエリーを 4 つのサブクエリーに分割して、結果を 1 ページずつの形式で表示できます。1 番めのサブクエリーには 1 ～ 500 行め（最初の 500 セッション）が含まれ、2 番めのサブクエリーには 501 ～ 1,000 行め、3 番めのサブクエリーには 1,001 ～ 1,500 行め、4 番めのサブクエリーには 1,501 ～ 2,000 行めまでが含まれるようにします。

（注） cnnEouHostQueryTotalHosts オブジェクトは、クエリーの条件に一致するホストの合計数（行数）を提供します。この数字を調べると、必要なサブクエリーの数を判断できます。ただし、最初のクエリーを構築するまでは、cnnEouHostQueryTotalHosts オブジェクトの数字を取得できません。

クエリーを構築するには次の手順を実行します。

手順の概要

1. cnnEouHostQueryStatus オブジェクトに createandgo を設定します。
2. cnnEouHostQueryMask オブジェクトに 8 を設定します。
3. cnnEouHostQueryRows に 500 を設定します。
4. cnnEouHostQuerySkipNHosts に 0 を設定します。
5. cnnEouHostQueryStatus オブジェクトをアクティブに設定します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	cnnEouHostQueryStatus オブジェクトに createandgo を設定します。	クエリーのステータスを設定します。
ステップ 2	cnnEouHostQueryMask オブジェクトに 8 を設定します。	**show eou all** コマンドのデフォルトに関連付けます。
ステップ 3	cnnEouHostQueryRows に 500 を設定します。	このクエリーで結果テーブルに構築される最大行数を識別します。
ステップ 4	cnnEouHostQuerySkipNHosts に 0 を設定します。	作成される結果の行に対応します。
ステップ 5	cnnEouHostQueryStatus オブジェクトをアクティブに設定します。	クエリーの構築が終了したことを示します。

（注） 前の表では例を示していません。これは、使用しているソフトウェアによって形式が異なるためです。この表は、2,000 セッション（行）を返すクエリーに基づいています。

この次の手順

前述のタスクを実行したら、最初の 500 ホスト（行）の情報のクエリーが実行されます。次の 500 ホスト（行）のクエリー情報を表示するには同じ 5 つの手順を実行しますが、ステップ 4 の cnnEouHostQuerySkipNHosts オブジェクトの値を 500 に変更します。このタスクによって、501 ～ 1000 行めのクエリー情報を取得できます。同じ方法で、残りのホスト（2000 まで）のクエリー情報を取得するには、もう一度同じ 5 つの手順を実行し、ステップ 4 の cnnEouHostQuerySkipNHosts オブジェクトの値をそれぞれ 1000 と 1500 に変更します。

ネットワーク アドミッション コントロールの設定例

ここでは、次の例について説明します。

ネットワーク アドミッション コントロール：例

次の出力例では、IP アドミッション コントロールが Cisco IOS ルータに設定されています。

```
Router# show running-config

Building configuration...

Current configuration: 1240 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
aaa new-model
!
!
aaa authentication eou default group radius
aaa session-id common
ip subnet-zero
ip cef
!
! The following line creates a network admission rule. A list is not specified; therefore,
! the rule intercepts all traffic on the applied interface.
ip admission name avrule eapoudp
!
eou logging
!
!
interface FastEthernet0/0
 ip address 10.13.11.106 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 10.0.0.1 255.255.255.0
 ip access-group 102 in
! The following line configures an IP admission control interface.
 ip admission avrule
 duplex auto
 speed auto
!
ip http server
no ip http secure-server
ip classless
!
!
```

```
! The following lines configure an interface access list that allows EAPoUDP traffic
! and blocks the rest of the traffic until it is validated.
access-list 102 permit udp any any eq 21862
access-list 102 deny   ip any any
!
!
! The following line configures RADIUS.
radius-server host 10.13.11.105 auth-port 1645 acct-port 1646 key cisco
!
control-plane
!
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
!
!
end
```

NAC MIB の出力：例

次に、MIB オブジェクト情報を表示する **show** コマンドの出力例を示します。

show eou

show eou コマンドは、さまざまな CISCO-NAC-NAD-MIB テーブルでも表示可能な情報を出力します。**show eou** コマンドを実行した結果の情報は cnnEouGlobalObjectsGroup テーブルにもあり、**show eou all** コマンドを実行した結果の情報は cnnEouIfConfigTable にもあります。

```
Router# show eou

Global EAPoUDP Configuration
----------------------------
EAPoUDP Version     = 1
EAPoUDP Port        = 0x5566
Clientless Hosts    = Enabled
IP Station ID       = Disabled
Revalidation        = Enabled
Revalidation Period = 36000 Seconds
ReTransmit Period   = 3 Seconds
StatusQuery Period  = 300 Seconds
Hold Period         = 30 Seconds
AAA Timeout         = 60 Seconds
Max Retries         = 3
EAP Rate Limit      = 20
EAPoUDP Logging     = Enabled
Clientless Host Username = clientless
Clientless Host Password = clientless

Router# show eou all

Interface Specific EAPoUDP Configurations
-----------------------------------------
Interface Vlan333
AAA Timeout         = 60 Seconds
Max Retries         = 3
eou initialize interface {interface-name}
```

```
eou revalidate interface {interface-name}
```

show ip device tracking all

show ip device tracking all コマンドは、cnnIpDeviceTrackingObjectsGroup MIB テーブルでも表示可能な情報を出力します。次に、その **show** コマンドの出力例を示します。

```
Router# show ip device tracking all

IP Device Tracking = Enabled
Probe Count: 2
Probe Interval: 10
```

その他の参考資料

ここでは、ネットワーク アドミッション コントロールに関する関連資料について説明します。

関連資料

内容	参照先
ACL の設定	「IP Access List Overview」フィーチャ モジュール
認証、認可、およびアカウンティング	『*Cisco IOS Security Configuration Guide: Securing User Services*, Release 12.4T』の「Authentication, Authorization, and Accounting」
インターフェイス、設定	『*Cisco IOS Configuration Fundamentals Configuration Guide,* Release 12.4T』
SNMP、および SNMP get 操作と set 操作	

規格

規格	タイトル
この機能によってサポートされる新しい規格や変更された規格はありません。	—

MIB

MIB	MIB リンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によってサポートされる新しい RFC や変更された RFC はありません。	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/techsupport

ネットワーク アドミッション コントロールの機能情報

表 4 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

（注） 表 4 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 4　ネットワーク アドミッション コントロールの機能情報

機能名	リリース	機能情報
ネットワーク アドミッション コントロール	12.3(8)T	ネットワーク アドミッション コントロール機能は、増大するワームやウイルスがネットワーク化されたビジネスに与える脅威や影響に対応します。この機能は、顧客がセキュリティの脅威を認識して防御し、適合するのに役立つ Cisco Self-Defending Network Initiative（自己防衛型ネットワーク構想）の一部です。 Cisco Network Admission Control 機能は、その初期段階で、エンドポイントがネットワークに接続しようとしたときに Cisco ルータがアクセス権限を制限できるようにします。 この機能に関する詳細については、次の各項を参照してください。 • 「ネットワーク アドミッション コントロールの前提条件」（P.2） • 「ネットワーク アドミッション コントロールの制約事項」（P.2） • 「ネットワーク アドミッション コントロールの概要」（P.2） • 「ネットワーク アドミッション コントロールの設定方法」（P.7） • 「ネットワーク アドミッション コントロールの設定例」（P.24） この機能により、次のコマンドが導入または変更されました。**aaa authentication eou default enable group radius**、**access-group**（アイデンティティ ポリシー）、**auth-type**、**clear eou**、**clear ip admission cache**、**debug eap**、**debug eou**、**debug ip admission eapoudp**、**description**（アイデンティティ ポリシー）、**description**（アイデンティティ プロファイル）、**device**（アイデンティティ プロファイル）、**eou allow**、**eou clientless**、**eou default**、**eou initialize**、**eou logging**、**eou max-retry**、**eou port**、**eou rate-limit**、**eou revalidate**、**eou timeout**、**identity policy**、**identity profile eapoudp**、**ip admission**、**ip admission name**、**redirect**（アイデンティティ ポリシー）、**show eou**、**show ip admission**、**template**（アイデンティティ ポリシー）

表 4　ネットワーク アドミッション コントロールの機能情報（続き）

機能名	リリース	機能情報
NAC MIB	12.4(15)T	CISCO-NAC-NAD-MIB のサポートが追加されました。この MIB モジュールは、Cisco NAC システムの NAD のモニタおよび設定に使用されます。 この機能に関する詳細については、次の各項を参照してください。 • 「NAC MIB」（P.5） • 「CISCO-NAC-NAD-MIB を使用した NAC のモニタおよび制御」（P.17） この機能により、次のコマンドが導入または変更されました。**show ip device tracking**。
	12.2(33)SXI	この機能は、Cisco IOS Release 12.2(33)SXI に統合されました。

用語集

EAPoUDP : Extensible Authentication Protocol over User Datagram Protocol の略です。EAP は、PPP で複数の任意の認証メカニズムをサポートするフレームワークで、クリアテキスト パスワード、チャレンジとレスポンス、任意のダイアログ シーケンスなどがあります。UDP は、TCP/IP プロトコル スタックのコネクションレス トランスポート レイヤ プロトコルです。UDP は、確認応答または保証された配信を使用せずにデータグラムを交換するシンプルなプロトコルで、他のプロトコルでエラー処理や再送信を実行する必要があります。UDP は RFC 768 で定義されています。

IP アドミッション ルール : IP アドミッション コントロールを適用する方法を定義した名前付きのルールです。IP アドミッション ルールはインターセプト ACL に関連付けられ、IP アドミッション機能を使用できるホストを制御します。IP アドミッション コントロール ルールを作成するには、ip admission name コマンドを使用します。

デフォルト アクセス ポリシー : AAA サーバがクレデンシャルを検証するまで、クライアント デバイスに適用される ACL を設定します。

ポスチャ トークン : ポスチャ クレデンシャルの評価結果の伝達に使用されるステータスです。AAA サーバは、ポスチャ トークン（ステータスには Healthy、Checkup、Quarantine、Infected、または Unknown を使用できます）を、クライアントが到達するピアのネットワーク アクセス ポリシー（ACL、URL、リダイレクト、またはステータス クエリー タイマー）にマップします。
