CHAPTER 4

802.1x 認証

802.1x 認証を使用すると、リモートの Cisco IOS ルータでは、常時稼働している VPN トンネルを介して、認証済みの VPN ユーザをセキュリティ保護されたネットワークに接続できます。Cisco IOS ルータは、セキュリティ保護されたネットワーク上の RADIUS サーバを通じてユーザを認証します。

802.1x 認証は、スイッチ ポートまたはイーサネット（ルーテッド）ポートのいずれかに適用され、両方のタイプのインターフェイスに適用されることはありません。802.1x 認証をイーサネット ポートに適用した場合、認証されていないユーザは、VPN トンネルを介さずにインターネットにルーティングされる可能性があります。

802.1x 認証をインターフェイスに設定するには、LAN ウィザードを使用します。ただし、インターフェイスで 802.1x を有効にするには、Cisco IOS ルータで AAA を有効にしておく必要があります。AAA を有効にする前に LAN ウィザードを使用しようとすると、AAA を有効にするかどうかを尋ねるウィンドウが表示されます。AAA を有効にすると答えると、LAN ウィザードの一手順として 802.1x の設定画面が表示されます。AAA を*有効にしない*と答えた場合は、802.1x の設定画面は*表示されません*。

LAN ウィザード：802.1x 認証（スイッチポート）

このウィンドウでは、LAN ウィザードで設定用に選択したスイッチ ポートに対して、802.1x 認証を有効にすることができます。

802.1x 認証の有効化

スイッチ ポートで 802.1x 認証を有効にするには、［802.1x 認証の有効化］を選択します。

ホスト モード

［単一］または［複数］を選択します。［単一］モードは、1 つの認証されたクライアントだけにアクセスを許可します。［複数］モードは、1 つのクライアントが認証された後、任意の数のクライアントにアクセスを許可します。

（注） Cisco 85x および Cisco 87x ルータのポートには、［複数］ホスト モードだけを設定できます。これらのルータには、［単一］モードは設定できません。

ゲスト VLAN

［ゲスト VLAN］を選択すると、802.1x がサポートされていないクライアントに対して VLAN を有効にできます。このオプションを有効にする場合は、［VLAN］ドロップダウン リストから［VLAN］を選択します。

Auth-fail VLAN

［Auth-fail VLAN］を選択すると、802.1x 認証に失敗したクライアントに対して VLAN を有効にできます。このオプションを有効にする場合は、［VLAN］ドロップダウン リストから［VLAN］を選択します。

定期的な再認証

［定期的な再認証］を選択すると、一定の間隔で 802.1x クライアントに再認証を強制できます。間隔をローカルに設定するか、または RADIUS サーバを使用して設定するかを選択します。再認証の間隔をローカルに設定する場合は、1 ～ 65,535 秒の範囲で値を入力します。デフォルト設定は 3600 秒です。

詳細オプション

［詳細オプション］をクリックすると、その他の 802.1x 認証パラメータを示すウィンドウが表示されます。

詳細オプション

このウィンドウでは、多数の 802.1x 認証パラメータのデフォルト値を変更できます。

RADIUS サーバ タイムアウト

RADIUS サーバへの接続がタイムアウトになるまでに Cisco IOS ルータが待機する時間（秒）を入力します。値の範囲は 1 ～ 65,535 秒です。デフォルト設定は 30 秒です。

サプリカントの応答タイムアウト

802.1x クライアントへの接続がタイムアウトになるまでに、Cisco IOS ルータがそのクライアントからの応答を待機する時間（秒）を入力します。値の範囲は 1 ～ 65,535 秒です。デフォルト設定は 30 秒です。

サプリカントの再試行タイムアウト

802.1x クライアントへの接続がタイムアウトになるまでに、Cisco IOS ルータがそのクライアントへの接続を再試行する時間（秒）を入力します。値の範囲は 1 ～ 65,535 秒です。デフォルト設定は 30 秒です。

待機時間

Cisco IOS ルータがクライアントに最初に接続してからログイン要求が送信されるまでに待機する時間（秒）を入力します。値の範囲は 1 ～ 65,535 秒です。デフォルト設定は 60 秒です。

レート制限時間

値の範囲は 1 ～ 65,535 秒です。ただし、デフォルト設定は 0 秒になっており、［レート制限時間］は無効になっています。

再認証の最大試行回数

Cisco IOS ルータが試行する 802.1x クライアントの再認証の最大回数を入力します。値の範囲は 1 ～ 10 です。デフォルト設定は 2 です。

最大試行回数

クライアントに送信できるログイン要求の最大回数を入力します。値の範囲は 1 ～ 10 です。デフォルト設定は 2 です。

デフォルトにリセット

［デフォルトにリセット］をクリックすると、すべての詳細オプションがデフォルト値にリセットされます。

LAN ウィザード：802.1x 認証用 RADIUS サーバ

802.1x 認証情報は、設定後、Cisco Secure ACS バージョン 3.3 を実行している RADIUS サーバ上のポリシー データベースに格納されます。ルータは、RADIUS サーバと通信して 802.1x クライアントのクレデンシャルを検証する必要があります。このウィンドウを使用して、ルータが 1 つ以上の RADIUS サーバに接続する際に必要となる情報を設定します。指定する各 RADIUS サーバでは、Cisco Secure ACS ソフトウェア バージョン 3.3 がインストールおよび設定されている必要があります。

（注） 802.1x 認証が有効になっているすべての Cisco IOS ルータ インターフェイスで、このウィンドウで設定された RADIUS サーバが使用されます。新しいインターフェイスを設定するときは、この画面が再び表示されますが、RADIUS サーバ情報を追加したり変更したりする必要はありません。

RADIUS クライアント ソースの選択

RADIUS のソースを設定すると、RADIUS サーバにバインドされた RADIUS パケットで送信されるように、送信元 IP アドレスを指定できます。インターフェイスの詳細については、インターフェイスを選択し、［詳細］ボタンをクリックして確認してください。

Cisco ACS バージョン 3.3 以降では、ルータ から送信される RADIUS パケットの送信元 IP アドレスを NAD IP アドレスとして設定する必要があります。

［ルータが送信元を選択します］を選択すると、RADIUS パケットの送信元 IP アドレスは、RADIUS パケットがルータから送り出されるときに通過するインターフェイスのアドレスになります。

インターフェイスを選択すると、RADIUS パケットの送信元 IP アドレスは、RADIUS クライアント ソースとして選択したインターフェイスのアドレスになります。

（注） Cisco IOS ソフトウェアを使用すると、単一 RADIUS ソースのインターフェイスをルータ上で設定できます。ルータにある設定済み RADIUS ソースとは別のソースを選択する場合、RADIUS サーバに送信されるパケットの送信元 IP アドレスは、新しいソースの IP アドレスに変わり、Cisco ACS で設定された NAD IP アドレスと一致しなくなる場合があります。

詳細

インターフェイスを選択する前に、インターフェイスに関する情報のクイックスナップショットが必要な場合は、［詳細］をクリックします。画面には、IP アドレスとサブネット マスク、インターフェイスに適用されるアクセス ルールとインスペクション ルール、適用された IPSec ポリシーと QoS ポリシー、およびインターフェイス上に Easy VPN 設定があるかどうかが表示されます。

サーバ IP/ タイムアウト / パラメータ カラム

［サーバ IP］、［タイムアウト］、および［パラメータ］カラムには、ルータから RADIUS サーバへの接続に使用される情報が含まれています。RADIUS サーバの情報が、選択されたインターフェイスに関連しない場合は、これらのカラムには何も表示されません。

802.1x 用に使用チェック ボックス

一覧表示された RADIUS サーバを 802.1x に使用する場合は、このチェック ボックスを選択します。802.1x を正常に使用するには、必要な 802.1x 認証情報がサーバに設定されている必要があります。

追加 / 編集 /Ping

RADIUS サーバの情報を入力するには、［追加］ボタンをクリックして、表示された画面に情報を入力します。RADIUS サーバの情報を変更するには、行を選択して［編集］をクリックします。ルータと RADIUS サーバ間の接続をテストするには、行を選択して［Ping］をクリックします。

（注）　Ping テストを実行するときは、［Ping］ダイアログ ボックスの［送信元］フィールドに、RADIUS ソース インターフェイスの IP アドレスを入力します。［ルータが送信元を選択します］を選択した場合は、［Ping］ダイアログ ボックスの［送信元］フィールドに値を入力する必要はありません。

選択されたインターフェイスで RADIUS サーバ情報を使用できない場合、［編集］ボタンと［Ping］ボタンは無効です。

802.1x 認証（スイッチポート）の編集

このウィンドウでは、802.1x 認証パラメータを有効化にしたり、設定したりできます。

802.1x 認証パラメータの代わりに、ポートがトランク モードで動作していることを示すメッセージが表示された場合は、そのスイッチで 802.1x 認証を有効にすることはできません。

802.1x 認証パラメータが表示されても、無効になっている場合は、次のいずれかが考えられます。

- AAA が有効になっていない。

  AAA を有効にするには、［設定］>［セキュリティ］>［AAA］>［概要］の順に選択します。次に、［AAA の有効化］をクリックします。
- AAA は有効になっているが、802.1x 認証ポリシーが設定されていない。

  802.1x 認証ポリシーを設定するには、［設定］>［セキュリティ］>［AAA］>［認証ポリシー］>［802.1x］の順に選択します。

802.1x 認証の有効化

対象のスイッチ ポートで 802.1x 認証を有効にするには、［802.1x 認証の有効化］を選択します。

ホスト モード

［単一］または［複数］を選択します。［単一］モードは、1 つの認証されたクライアントだけにアクセスを許可します。［複数］モードは、1 つのクライアントが認証された後、任意の数のクライアントにアクセスを許可します。

（注） Cisco 87x ルータのポートには、［複数］ホスト モードだけを設定できます。これらのルータには、［単一］モードは設定できません。

ゲスト VLAN

［ゲスト VLAN］を選択すると、802.1x がサポートされていないクライアントに対して VLAN を有効にできます。このオプションを有効にする場合は、［VLAN］ドロップダウン リストから［VLAN］を選択します。

Auth-fail VLAN

［Auth-fail VLAN］を選択すると、802.1x 認証に失敗したクライアントに対して VLAN を有効にできます。このオプションを有効にする場合は、［VLAN］ドロップダウン リストから［VLAN］を選択します。

定期的な再認証

［定期的な再認証］を選択すると、一定の間隔で 802.1x クライアントに再認証を強制できます。間隔をローカルに設定するか、または RADIUS サーバを使用して設定するかを選択します。再認証の間隔をローカルに設定する場合は、1 ～ 65,535 秒の範囲で値を入力します。デフォルト設定は 3600 秒です。

詳細オプション

［詳細オプション］をクリックすると、その他の 802.1x 認証パラメータを示すウィンドウが表示されます。

LAN ウィザード：802.1x 認証（VLAN/Ethernet）

このウィンドウでは、LAN ウィザードで設定用に選択したイーサネット ポートに対して、802.1x 認証を有効にすることができます。Cisco 87x ルータの場合、このウィンドウは、802.1x 認証を使用する VLAN を設定する場合に表示されます。

（注） VLAN に 802.1x を設定する前に、802.1x がいずれの VLAN スイッチ ポートにも*設定されていない*ことを確認してください。また、VLAN が DHCP に設定されていることも確認してください。

Use 802.1x Authentication to separate trusted and untrusted traffic on the interface

802.1x 認証を有効にするには、［Use 802.1x Authentication to separate trusted and untrusted traffic on the interface］を選択します。

例外リスト

例外リストを作成または編集するには、［例外リスト］をクリックします。例外リストは、特定のクライアントについて 802.1x 認証から除外する一方で VPN トンネルの使用を許可します。

802.1x 認証から Cisco IP 電話を除外

Cisco IP 電話を 802.1x 認証の対象から除外しながら、VPN トンネルの使用を許可する場合は、［802.1x 認証から Cisco IP 電話を除外］を選択します。

802.1x 例外リスト

例外リストは、特定のクライアントについて 802.1x 認証から除外する一方で VPN トンネルの使用を許可します。除外するクライアントは、MAC アドレスを使用して指定します。

追加

［追加］をクリックすると、クライアントの MAC アドレスを追加できるウィンドウが表示されます。MAC アドレスには、次のいずれかの例の形式を使用する必要があります。

- 0030.6eb1.37e4
- 00-30-6e-b1-37-e4

Cisco Router and Security Device Manager（Cisco CP）では、ここに示した例より短い MAC アドレスを除き、正しくない形式の MAC アドレスは拒否されます。例より短い MAC アドレスには、不足しているそれぞれの桁に 0（ゼロ）が埋め込まれます。

（注） Cisco CP の 802.1x 機能では、MAC アドレスにポリシーを関連付ける CLI オプションはサポートされていないため、例外リストには、ポリシーが関連付けられている MAC アドレスは含まれません。

削除

選択したクライアントを例外リストから削除するには、［削除］をクリックします。

レイヤ 3 インターフェイスでの 802.1x 認証

このウィンドウでは、レイヤ 3 インターフェイスに 802.1x 認証を設定できます。このウィンドウには、802.1x 認証が設定済みまたは設定可能なイーサネット ポートと VLAN インターフェイスが一覧表示され、信頼できないクライアントに仮想テンプレート インターフェイスを指定したり、802.1x 認証を回避させるクライアントの例外リストを作成したりできます。

（注） CLI を使用してポリシーが設定されている場合、それらのポリシーはこのウィンドウに読み取り専用情報として表示されます。その場合、このウィンドウで実行できる操作は、802.1x の有効化または無効化だけです。

必須タスク

このウィンドウに必須タスクが表示された場合は、802.1x 認証を設定する前に、それらのタスクを実行する必要があります。必須タスクを説明するメッセージと、タスクを実行できるウィンドウへのリンクが表示されます。

802.1x 認証をグローバルに有効化

［802.1x 認証をグローバルに有効化］を選択すると、すべてのイーサネット ポートで 802.1x 認証が有効になります。

インターフェイス表

［インターフェイス］表には、次のカラムがあります。

インターフェイス — イーサネットまたは VLAN インターフェイスの名前が表示されます。

802.1x 認証 — 対象のイーサネット ポートで 802.1x 認証が有効になっているかどうかが示されます。

編集

［編集］をクリックすると、編集可能な 802.1x 認証パラメータを示したウィンドウが表示されます。これらのパラメータは、［インターフェイス］表で選択したインターフェイスについての 802.1x 認証設定です。

外部ユーザポリシー

ドロップダウン リストから仮想テンプレート インターフェイスを選択します。選択した仮想テンプレート インターフェイスは、802.1x 認証に失敗したクライアントに適用するポリシーになります。

選択した仮想テンプレート インターフェイスの詳細を確認するには、［詳細］ボタンをクリックします。

例外リスト

例外リストの詳細については、「802.1x 例外リスト」を参照してください。

802.1x 認証から Cisco IP 電話を除外

Cisco IP 電話を 802.1x 認証の対象から除外しながら、VPN トンネルの使用を許可する場合は、［802.1x 認証から Cisco IP 電話を除外］を選択します。

変更の適用

行った変更を有効にするには、［変更の適用］をクリックします。

変更の破棄

適用しない変更を消去するには、［変更の破棄］をクリックします。

802.1x 認証の編集

このウィンウでは、多数の 802.1x 認証パラメータのデフォルト値を有効にしたり、変更したりできます。

802.1x 認証の有効化

イーサネット ポートで 802.1x 認証を有効にするには、[802.1x 認証の有効化] を選択します。

定期的な再認証

[定期的な再認証] を選択すると、一定の間隔で 802.1x クライアントに再認証を強制できます。間隔をローカルに設定するか、または RADIUS サーバを使用して設定するかを選択します。再認証の間隔をローカルに設定する場合は、1 ～ 65,535 秒の範囲で値を入力します。デフォルト設定は 3600 秒です。

詳細オプション

[詳細オプション] ボックスの各フィールドの説明を表示するには、[詳細オプション] をクリックします。

その他の手順

ここでは、LAN ウィザードで実行できないタスクの

手順を示します。

複数のイーサネット ポートに 802.1x 認証を設定する方法

いったん 1 つのインターフェイスに 802.1x 認証を設定すると、LAN ウィザードにはイーサネット ポート用の 802.1x オプションは表示されなくなります。これは、Cisco CP で、802.1x の設定がグローバルに使用されるためです。

イーサネット ポートの 802.lx 認証の設定を編集する場合は、［設定］>［セキュリティ］>［AAA］>［認証ポリシー］>［802.1x］の順に選択します。次に、認証ポリシーを選択して［編集］をクリックします。表示されるダイアログ ボックスでポリシーを編集します。