Cisco Identity Services Engine のユニバーサル スイッチの設定

セキュア アクセスを実現するハウツー ガイド シリーズ

作成者:Hosuk Won

日付:2016 年 1 月

目次

はじめに

Cisco Identity Services Engine とは

Cisco Identity Services Engine（ISE）は、包括的でセキュアな、有線、ワイヤレスおよびバーチャル プライベート ネットワーク（VPN）アクセスを実現するオールインワン型エンタープライズ ポリシー制御製品です。

Cisco ISE は、RADIUS ベースの単一製品でありながら、ポリシーの包括的な管理と適用の集中制御ポイントとして機能します。Cisco ISE 固有のアーキテクチャにより、企業はネットワーク、ユーザ、およびデバイスから状況に応じた情報をリアルタイムで収集できるようになります。管理者は、プロアクティブなガバナンスの意思決定にその情報を使用できます。Cisco ISE は Cisco Secure Access の重要なコンポーネントです。

Cisco Secure Access は、ネットワーク インフラストラクチャに統合された高度なネットワーク アクセス コントロールとアイデンティティのソリューションです。ソリューション内のすべてのコンポーネントが統合システムとして十分に吟味かつ厳密にテストされた、実証済みの有効なソリューションです。

Cisco Catalyst スイッチ

オーバーレイ ネットワーク アクセス コントロール ソリューションとは異なり、Cisco Secure Access では、アクセス レイヤ デバイス（スイッチ、ワイヤレス コントローラなど）が適用時に使用されます。Web 認証用の URL リダイレクトなど、一般にはアプライアンスやその他のオーバーレイ デバイスによって処理されていた機能をアクセス デバイス自体が処理するようになりました。

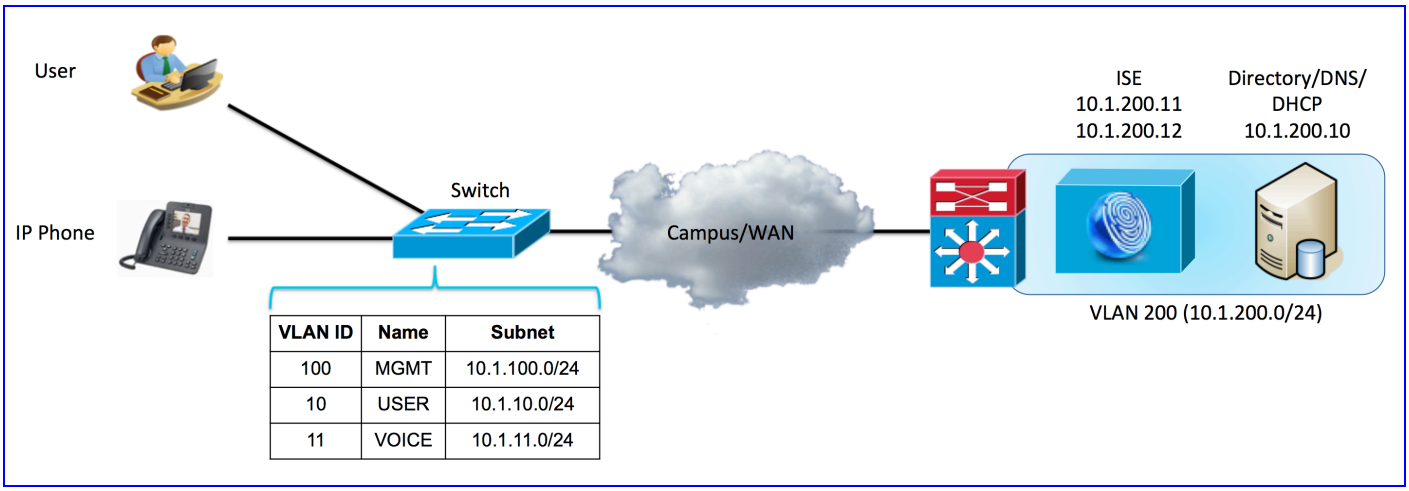
Cisco Secure Access は、IEEE 802.1X と VLAN 制御などの標準ベースのアイデンティティおよび適用モデルを組み合わせるだけでなく、柔軟な認証、ダウンロード可能アクセス コントロール リスト（dACL）、セキュリティ グループ タグ（SGT）、デバイス プロファイリング、ゲストと Web の認証サービス、ポスチャ評価、ネットワークへのアクセス前とアクセス時のモバイル デバイスのコンプライアンス検証を行うモバイル デバイス管理（MDM）の大手ベンダーとの統合など、さらに多くの高度なアイデンティティおよび適用機能も備えています。

このマニュアルについて

このドキュメントでは、Cisco Identity Services Engine と統合するための、Cisco Catalyst スイッチでのベスト プラクティスの設定を紹介しています。このドキュメントの主なセクションは 3 つのパートに分けられます。グローバル設定は、モニタ/ロー インパクト モードとクローズド モードの段階的な導入に適用されます。2 つのインターフェイス設定が提供されており、1 つ目はモニタ/ロー インパクト モード設定で、2 つ目はクローズド モード インターフェイス設定です。「オプション」と記載されている設定は、ISE 統合の観点からは不可欠ではありませんが、特定のユーザ エクスペリエンスに対応するためには重要となります。これには、RADIUS サーバが停止しているときのインターフェイスの動作や、HTTPS トラフィックのための URL リダイレクトの扱いなどが含まれます。

次の図は、コンポーネントの全体的なレイアウトを示します。アクセス VLAN は 2 つあります。従業員ユーザのための ACCESS VLAN と、IP フォンのための VOICE VLAN です。MGMT VLAN は、スイッチが管理ユーザおよび ISE ノードと通信するために使用されます。このドキュメントには BYOD、ポスチャ アセスメント、プロファイリングなどの ISE のポリシー設定は含まれていませんが、記載されている設定はこのような操作の基準を定めています。

図 1 コンポーネント



VLAN ID	Name	Subnet
100	MGMT	10.1.100.0/24
10	USER	10.1.10.0/24
11	VOICE	10.1.11.0/24

また、付録には最小限の変更を加えてコピー アンド ペーストができるサンプル設定が記載されています。

設定

グローバル設定

この設定では、2 つの ISE PSN ノードが冗長性のために定義されます。どの ISE ノードにもスイッチから到達できない場合には、ネットワークへのアクセスを許可するために重要な認証機能も使用されます。

注:IOS および IOS-XE のバージョンによっては、記載されているコマンドの一部がデフォルトで有効になっている可能性があります。

手順 1 システムの基本的な必須コマンドです。 ドメイン名は、https リダイレクトを有効にするときに必要です。

```
SWITCH(config)#ip domain-name EXAMPLE.COM
```

手順 2 (オプション)ISE の RADIUS テスト メッセージを生成するために、「RADIUS-TEST」アカウントが使用されます。

```
SWITCH(config)#username RADIUS-TEST password 0 PASSWORD
```

注:ユーザ名とパスワードは、ISE の ID データベースで有効なアカウントである必要はありません。ISE ノードが成功した認証のために ACCESS-ACCEPT を送り返す場合でも、失敗した認証のために ACCESS_REJECT を送り返す場合でも、スイッチは両方の応答を RADIUS デッド設定のためのライブ サーバからの有効な応答と見なします。ただし、スイッチがバックエンド ID ストアまでテストし、ISE ノードが外部 ID データベースへの接続性を持つことを確認できるように、MS Active Directory や LDAP などの外部 ID ストアの有効なアカウントを提供することを推奨します。

手順 3 (オプション)HTTPS サービスに使用するキーを生成します。

```
SWITCH(config)#crypto key generate rsa general-keys mod 2048
```

注:キーを生成する前に、「ip http secure-server」コマンドを実行しないでください。正しくない順序でコマンドを実行すると、スイッチは自動的に小さいキー サイズの証明書を生成します。HTTPS トラフィックをリダイレクトするときに、この証明書により、望ましくない動作が発生する可能性があります。

手順 4 AAA を有効化します。

```
SWITCH(config)#aaa new-model
```

手順 5 定義された RADIUS サーバで使用するネットワーク認証を有効にします。

```
SWITCH(config)#aaa authentication dot1x default group ISE
```

手順 6 802.1x 認証セッションの url リダイレクト、dVLAN（ダイナミック VLAN）、dACL（ダウンロード可能 ACL）などのネットワーク認証を有効にします。

```
SWITCH(config)#aaa authorization network default group ISE
```

手順 7 セッションが開始および停止されるたびに NAD から ISE にアカウント情報を送信します。

```
SWITCH(config)#aaa accounting dot1x default start-stop group ISE
```

手順 8 NAD のアクティブ セッションが ISE でも保持されるように、新しい更新があったときおよび 2 日ごとにアカウンティング更新を送信します。

```
SWITCH(config)#aaa accounting update newinfo periodic 2880
```

注：セッションに損傷がないことを示すために、中間 RADIUS アカウンティング メッセージが ISE に送信されます。指定されたエンドポイントで長期間 ISE が RADIUS アカウンティング メッセージの受信に失敗する場合、ISE はそのセッションをセッション テーブルから削除します。ISE はスイッチからエンドポイントを削除しません。どのセッションがアクティブかの観点から、スイッチと ISE 間を切断します。この切断は、エンドポイント アクセスを何らかの理由で再評価する必要がある場合に影響を与える可能性があります。デフォルトでは、ISE は認証セッションで 5 日間中間 RADIUS アカウンティング メッセージがないセッションを消去します。5 日間までに ISE ノードに RADIUS アカウンティング メッセージを定期的に送信することで、スイッチはそのセッションが ISE で保持されていることを確認します。ここでの 2 日間の理由は、RADIUS アカウンティング パケットが ISE ノードに到達できなかった場合に、5 日間以内に 2 つの更新を提供するためです。

手順 9 これにより、ISE から CoA 要求を受け入れるように NAD が設定されます。この NAD が CoA のためにも要求を送信する PSN を追加することを推奨します。これは、BYOD（NSP）、ポスチャ、CWA、MDM などの ISE の高度な使用例で必要となります。

```
SWITCH(config)#aaa server radius dynamic-author
SWITCH(config-locsvr-da-radius)# client 10.1.200.11 server-key RADIUS_KEY
SWITCH(config-locsvr-da-radius)# client 10.1.200.12 server-key RADIUS_KEY
```

手順 10 NAD は、異なる認証方式間で、共通するクライアントのセッション ID を使用します。このセッション ID は、レポート、CoA、ISE セッション管理のために使用されます。

```
SWITCH(config)#aaa session-id common
```

手順 11 （オプション）このオプションのコマンドは、同じスイッチの異なるポートの同じ MAC アドレスに既存のセッションがある場合に、ポートでの新しいセッションを許可します。これは、アンマネージド ハブまたはスイッチが使用されている場合や、サードパーティ製の IP フォンがエンド ユーザによって使用されている場合に役立ちます。

```
SWITCH(config)#authentication mac-move permit
```

注:この機能は、アンマネージド スイッチ/ハブまたはサードパーティ製の IP フォンが使用されている環境で特に役立ちます。これらのタイプのデバイスが使用されている場合、認証デバイスがインターフェイスから別のインターフェイスに移った場合に Catalyst スイッチに十分に通知されず、スイッチがアクセスを拒否する原因となる可能性があります。このコマンドを使用すると、スイッチはデバイスが最初に検出されたときの元のセッションを切断し、同じスイッチの異なるインターフェイスでデバイスを認証できるようになります。これは、シスコ IP フォンには必要ありません。シスコ IP フォンは CDP メッセージを使用して電話の背後のデバイスが切断されたときにスイッチに通知し、スイッチが効果的にセッションを削除できるようにします。

手順 12 (オプション)このコマンドにより、dACL のないセッションを ACL の有効なインターフェイスにフル アクセスで接続することができます。

```
SWITCH(config)#epm access-control open
```

注:この機能は、dACL を使用する認証プロファイルと使用しない認証プロファイルが組み合わさった環境で役立ちます。たとえば、ユーザ デバイスはネットワークへのアクセスを制限するために dACL を適用されていて、IP フォンでは dACL が使用されない場合です。IP フォンが接続されている場合、IP フォンは MAB/802.1X(dACL なし)により音声リソースに対して承認されます。ユーザのデバイスが IP フォンの背後に接続されている場合、スイッチはインターフェイス レベルで ACL を適用するユーザ デバイス dACL を適用します。これにより、IP フォンには認証のための dACL がないため、IP フォンへの IP アクセスが拒否されます。ただし、このコマンドがグローバルに入力された場合、スイッチは IP フォンを含む dACL を持たないセッションに動的に「permit ip any any」ACL を挿入します。これは、アンマネージド ハブを介して接続された複数のデバイスにも当てはまります。dACL を使用せずに複数のデバイスがすでに接続されているときに、dACL 認証を使用する新しいデバイスがアンマネージド ハブが接続されている同じインターフェイスに認証された場合、この機能は前に接続されたデバイスのセッションに「ip permit any any」ACL を適用します。

手順 13 802.1x をシステム全体で有効にします。

```
SWITCH(config)#dot1x system-auth-control
```

注:このコマンドを削除しても、すべてのポートで 802.1X が無効になるわけではありません。正確には、このコマンドがない場合、スイッチがエンドポイントからの EAP フレームを無視します。ポートで 802.1X を無効にすることが目的の場合には、インターフェイス範囲のコマンドを使用して認証関連のコマンドを削除します。

手順 14 (オプション)どの RADIUS サーバにも到達できない場合のポートのフェール オープン/フェール クローズ時に、定型 EAPoL 成功メッセージをクライアントに送信します。

```
SWITCH(config)#dot1x critical eapol
```

注:設定されたどの ISE ノードにも到達できない場合、スイッチに認証サービスを提供するために重要な認証が発生します。重要な認証に基づいてエンドポイントが承認される場合、エンドポイント サプリカントが認証を再起動し、これによりユーザ エクスペリエンスに影響が出る場合があります(認証中はネットワーク接続が中断されるため)。この機能はエンドポイント サプリカントに定型 EAPoL 成功メッセージを送信し、認証が再起動されないようにします。サプリカントが定型メッセージを受け取るかどうかは、サプリカント(サプリカントの設定、サプリカント ベンダー、EAP タイプなど)によって決まります。

手順 15 IP デバイストラッキングを有効にして、エンドポイント IP を見つけます。これは、プロファイリングや、セッションへの dACL、フィルタ ID、URL リダイレクトの適用のために不可欠です。

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

注:IP デバイストラッキングを有効にした後に Windows マシンで重複する IP メッセージが表示されるようになった場合には、次のコマンドを実行します。supplicant settings、supplicant vendor、EAP Types。

手順 16 (オプション)「IP デバイストラッキング」を有効にした後に Windows マシンで重複する IP メッセージが表示されるようになった場合には、次のコマンドを使用してこのメッセージを回避できます。IOS 15.2(2)E および IOS-XE 03.06.00E 以上を実行するスイッチ コードの場合は、次のコマンドを使用します。

```
SWITCH(config)#ip device tracking probe auto-source
```

注:IOS コードの以前のバージョンについては、次のコマンドを実行します。

```
SWITCH(config)#ip device tracking probe delay 10
```

注:上記のコマンドで問題が解決せず、スイッチが SVI を使用してエンドポイント VLAN のために設定されている場合には、次のコマンドを使用して重複する IP メッセージの問題に対処できます。

```
SWITCH(config)#ip device tracting probe use-svi
```

手順 17 VLAN を作成します。

```
SWITCH(config)#vlan 10
SWITCH(config-vlan)# name USER

SWITCH(config)#vlan 11
SWITCH(config-vlan)# name VOICE

SWITCH(config)#vlan 100
SWITCH(config-vlan)# name MGMT
```

手順 18 ユーザ VLAN 用の SVI 設定です。

```
SWITCH(config)#interface 10
SWITCH(config-if)# ip address 10.1.10.1 255.255.255.0
```

手順 19 DHCP サーバに DHCP パケットを送信します。

```
SWITCH(config-if)# ip helper-address 10.1.200.10
```

手順 20 (オプション)プロファイリングのために DHCP パケットを ISE に送信します。

```
SWITCH(config-if)#ip helper-address 10.1.200.11
```

注:ISE ノード間での複製トラフィックを減らすために、複数のノードではなく 1 つだけの ISE ノードに送信することを推奨します。また、デバイス センサーを使用する場合は、同時に「helper-address」を使用して DHCP を転送しないことを推奨します。プロファイリング情報が重複し、ISE ノード間の複製トラフィックが増える可能性があります。

手順 21 音声 VLAN 用の SVI 設定です。

```
SWITCH(config)#interface 11
SWITCH(config-if)#ip address 10.1.11.1 255.255.255.0
SWITCH(config-if)#ip helper-address 10.1.200.10
SWITCH(config-if)#! ip helper-address 10.1.200.11
```

手順 22 管理 VLAN 用の SVI 設定です。

```
SWITCH(config)#interface 100
SWITCH(config-if)#ip address 10.1.100.1 255.255.255.0
```

手順 23 スイッチの http リダイレクト機能を使用するために必要です。

```
SWITCH(config)#ip http server
```

手順 24 (オプション)スイッチの https リダイレクト機能を使用するために必要です。

```
SWITCH(config)#ip http secure-server
```

注:HTTPS リダイレクトの利用はスイッチの CPU に影響を与えるため、高密度スイッチで有効にする前にパフォーマンスをモニタすることを推奨します。

手順 25 (オプション)次のように設定して、URL リダイレクトを機能させながら、スイッチへの http ベースの管理者アクセスを無効にします。

```
SWITCH(config)#ip http active-session-modules none
SWITCH(config)#ip http secure-active-session-modules none
```

手順 26 （オプション）同時 URL リダイレクト セッションがいくつ存在できるかに影響します。高密度アクセス スイッチで、複数のユーザが URL リダイレクトを同時に使用するときにこの値を増やす必要がある場合があります。デフォルト値と最大値はコード バージョンとプラットフォームによって異なります。15.2(2)E3 を実行する 3560CG では、デフォルトは 16、最大は 48 です。

```
SWITCH(config)#ip http max-connections 48
```

注：IOS の旧バージョンでは使用できません。

手順 27 この ACL は、CWA、BYOD、ポスチャの間にどのトラフィックが ISE にリダイレクトされるかを定義します。ACL によって許可されているトラフィックがリダイレクトされます。暗黙の拒否によって、他のトラフィック タイプがリダイレクトされることが防がれます。このトラフィックはスイッチ CPU にプッシュされるため、ここでは HTTP（および HTTPS）のみが許可されるように指定することを推奨します。リダイレクト ACL と併せて追加のアクセス コントロールが必要な場合には、リダイレクト ACL と併せて dACL を使用することを推奨します。

```
SWITCH(config)#ip access-list extended ACL_WEBAUTH_REDIRECT
SWITCH(config-ext-nacl)#permit tcp any any eq www
SWITCH(config-ext-nacl)#permit tcp any any eq 443
```

注：上記で参照されている ACL 名は、新しい ISE 2.0 インストールで使用されているデフォルト リダイレクト ACL 名と同じです。別の名前を使用する場合は、スイッチと ISE 認証プロファイルの両方を新しいリダイレクト ACL 名で更新するようにします。

手順 28 この ACL は、ブラック リストに掲載されたデバイスのためにどのトラフィックが ISE にリダイレクトされるかを定義します。ACL によって許可されているトラフィックがリダイレクトされます。暗黙の拒否によって、他のトラフィック タイプがリダイレクトされることが防がれます。このトラフィックはスイッチ CPU にプッシュされるため、ここでは HTTP（および HTTPS）のみが許可されるように指定することを推奨します。リダイレクト ACL と併せて追加のアクセス コントロールが必要な場合には、リダイレクト ACL と併せて dACL を使用することを推奨します。

```
SWITCH(config)#ip access-list extended BLACKHOLE
SWITCH(config-ext-nacl)#permit tcp any any eq www
SWITCH(config-ext-nacl)#permit tcp any any eq 443
```

注：上記で参照されている ACL 名は、新しい ISE 2.0 インストールで使用されているデフォルト リダイレクト ACL 名と同じです。別の名前を使用する場合は、スイッチと ISE 認証プロファイルの両方を新しいリダイレクト ACL 名で更新するようにします。

手順 29 RADIUS 認証の前に適用される ACL です。有線アクセスのために段階的な導入のオープン モードまたはロー インパクト モードを使用する場合に必要です。

```
SWITCH(config)#ip access-list extended ACL-DEFAULT
SWITCH(config-ext-nacl)#permit udp any any eq domain
SWITCH(config-ext-nacl)#permit udp any eq bootpc any eq bootps
SWITCH(config-ext-nacl)#deny ip any any
```

注:ロー インパクト モードの導入では、この ACL はインターフェイスが重要な認証状態になったときに有効になります。これは、エンドポイントがどの ISE ノードにも到達できないときに接続を試みていて、エンドポイントがインターフェイス設定によって設定された重要な VLAN に配置されている場合でも、エンドポイントは重要な状態の間はこの ACL に制限されることを意味します。

手順 30 認証要求とアカウンティング更新の間に、定義されたベンダー固有属性(VSA)が ISE に送信されるように NAD を設定します。

```
SWITCH(config)#radius-server vsa send authentication
SWITCH(config)#radius-server vsa send accounting
```

手順 31 RADIUS サーバに追加の属性を送信します(ISE には必須)。

```
SWITCH(config)#radius-server attribute 6 on-for-login-auth
SWITCH(config)#radius-server attribute 8 include-in-access-req
SWITCH(config)#radius-server attribute 25 access-request include
```

手順 32 RADIUS サーバとして ISE PSN を追加します。

```
SWITCH(config)#radius server ISE01
SWITCH(config-radius-server)#address ipv4 10.1.200.11
```

手順 33 IOS 15.2(2)E および IOS-XE 03.06.00E 以上を実行するスイッチ コードで RADIUS ステータスをテストするためのメソッドとユーザ名を定義します。このコマンドは、RADIUS サーバがデッド基準によってデッドとしてマークされたときにのみ、サーバに RADIUS テスト メッセージを送信します。プローブはデッド時間が期限切れになると送信され、RADIUS サーバがまだ応答しない場合にはより頻繁に送信されます。このコマンドは、プローブが継続的に送信されないようにするために、多数の NAD を持つ大規模な組織で役立ちます。このコマンドと次のコマンドは相互に排他的な関係にあります。

```
SWITCH(config-radius-server)# automate-tester username RADIUS-TEST probe-on
```

注:次のコマンドは、前のバージョンの IOS でサポートされています。このコマンドは、サーバ ステータスにかかわらず、設定された間隔でサーバに RADIUS テスト メッセージを送信します。導入に多数の NAD がある場合は、プローブの間隔を大きくして RADIUS サーバへの影響を制限することを推奨します。アイドル時間値を大きくすると、プローブのアイドル時間がデッド時間よりも短くなるように、グローバル デッド時間値も大きくなります。これにより、デッド時間が期限切れになったときに重要な状態に承認されたエンドポイントは再初期化されず、重要な状態に再度承認されるだけになります。ここでは、値を 10 分に設定します(デフォルトは 60 分です)。

```
SWITCH(config-radius-server)# automate-tester username RADIUS-TEST ignore-acct-port idle-time 10
```

注:これらのプローブ メッセージは、通常のユーザ認証イベントとともに ISE RADIUS ライブログに表示されます。ISE では、コレクション フィルタを設定してプローブ メッセージをフィルタリングし、ユーザ認証イベントのみがライブログに表示されるようにすることができます。

手順 34 RADIUS キーを設定します。

```
SWITCH(config-radius-server)#key RADIUS_KEY
```

手順 35 RADIUS サーバとして追加 ISE PSN を設定します。

```
SWITCH(config)#radius server ISE02
SWITCH(config-radius-server)#address ipv4 10.1.200.12
SWITCH(config-radius-server)#automate-tester username RADIUS-TEST probe-on
SWITCH(config-radius-server)#! automate-tester username RADIUS-TEST idle-time 10
SWITCH(config-radius-server)#key RADIUS_KEY
```

手順 36 AAA 指令で参照される RADIUS サーバ グループを追加します。

```
SWITCH(config)#aaa group server radius ISE
SWITCH(config-sg-radius)#server name ISE01
SWITCH(config-sg-radius)#server name ISE02
```

手順 37 サーバが応答しない場合に NAD が RADIUS サーバをデッドとしてマークするためにかかる時間の長さを定義します。単一の ISE ノードが RADIUS サーバとして定義されている環境では、サーバがオンライン状態に戻った後にインターフェイス設定が再初期化されるように設定されている場合に、NAD がポートをフェール オープン/フェール クローズ(重要)状態のままにする時間の長さも定義されます。すべての ISE ノードが作動状態に戻った場合、スイッチはリストの最初の ISE ノードに復帰します。この例では、この値は 15 分に設定されています。

```
SWITCH(config-sg-radius)#deadtime 15
```

注:この値は、以前に設定されているどの RADIUS プローブに設定されたアイドル時間よりも大きくする必要があります。RADIUS サーバ グループでデッド時間を定義する代わりに、「radius-server deadtime 15」コマンドを使用してグローバルに設定することもできます。

手順 38 サーバをデッドとしてマークするための RADIUS デッド基準を設定します。

```
SWITCH(config)#radius-server dead-criteria time 10 tries 3
```

手順 39 (オプション)RADIUS 要求のソース元となるインターフェイスを定義します。

```
SWITCH(config)#ip radius source-interface vlan 100
```

注:上記の例では管理 SVI が使用されていますが、ループバック インターフェイスを利用して、RADIUS サーバへの複数のパスがある場合に RADIUS 要求のソース IP が同じソース IP から到着することを保証することを推奨します。

手順 40 （オプション）プロファイリングのために使用されます。ISE が NAD から CDP/LLDP/ARP テーブルに投票できるようにします。デバイス センサー機能が使用されている場合は、重複するプロファイリング データを減らすために SNMP を同時に使用しないことを推奨します。

```
SWITCH(config)#snmp-server community SNMP_COMMUNITY_STRING RO
```

注：カスタム SNMP コミュニティ文字列を除いて、ACL は ISE ノードと管理サーバが SNMP を介してスイッチにアクセスできるようにするためにのみ使用することも推奨します。

手順 41 （オプション）DHCP スヌーピングを有効にして、デバイス センサーを使用してプロファイリングのためにクライアントから DHCP 情報を収集します。これは、「ip helper-address」コマンドの使用とは対照的に、DHCP 情報を収集するために推奨される方法です。

```
SWITCH(config)#ip dhcp snooping
```

注：静的 IP アドレスがエンドポイント用に使用される場合は、この手順を省略します。

手順 42 （オプション）エンドポイントが存在する VLAN で DHCP スヌーピングを有効にします。

```
SWITCH(config)#ip dhcp snooping vlan 10, 11
```

注：静的 IP アドレスがエンドポイント用に使用される場合は、この手順を省略します。

手順 43 （オプション）DHCP 用のデバイス センサーを有効にします。

```
SWITCH(config)#device-sensor filter-list dhcp list TLV-DHCP
SWITCH(config-sensor-dhcplist)#option name host-name
SWITCH(config-sensor-dhcplist)#option name requested-address
SWITCH(config-sensor-dhcplist)#option name parameter-request-list
SWITCH(config-sensor-dhcplist)#option name class-identifier
SWITCH(config-sensor-dhcplist)#option name client-identifier
SWITCH(config)#device-sensor filter-spec dhcp include list TLV-DHCP
```

手順 44 （オプション）CDP をグローバルに有効にします。

```
SWITCH(config)#cdp run
```

手順 45 （オプション）CDP 用のデバイス センサーを有効にします。

```
SWITCH(config)#device-sensor filter-list cdp list TLV-CDP
SWITCH(config-sensor-cdplist)#tlv name device-name
SWITCH(config-sensor-cdplist)#tlv name address-type
SWITCH(config-sensor-cdplist)#tlv name capabilities-type
SWITCH(config-sensor-cdplist)#tlv name platform-type
SWITCH(config)#device-sensor filter-spec cdp include list TLV-CDP
```

手順 46　（オプション）LLDP をグローバルに有効にします。

```
SWITCH(config)#lldp run
```

手順 47　（オプション）LLDP 用のデバイス センサーを有効にします。

```
SWITCH(config)#device-sensor filter-list lldp list TLV-LLDP
SWITCH(config-sensor-lldplist)#tlv name system-name
SWITCH(config-sensor-lldplist)#tlv name system-description
SWITCH(config)#device-sensor filter-spec lldp include list TLV-LLDP
```

手順 48　（オプション）すべての変更を含む、センサー データが RADIUS アカウンティングで送信されるようにします。

```
SWITCH(config)#device-sensor accounting
SWITCH(config)#device-sensor notify all-changes
```

手順 49　（オプション）重複更新が ISE に送信されないようにローカル アナライザを無効にします。

```
SWITCH(config)#no macro auto monitor
SWITCH(config)#access-session template monitor
```

手順 50　設定モードを終了して設定を保存します。

```
SWITCH(config)#end
SWITCH#write memory
Building configuration…
[OK]
SWITCH#
```

インターフェイス レベル設定（モニタ モード / ロー インパクト モードの設定）

次のインターフェイス設定では、モニタ モードおよびロー インパクト モードの設定のキー コマンドである「authentication open」指令を有効にします。2 つのモードの主な違いは、ポート ACL が存在するかどうかです。通常、モニタ モードではポータル ACL は適用されず、ロー インパクト モードでは ACL が適用され、DHCP、DNS、場合によっては TFTP へのトラフィックが制限されます。この設定では、単一のインターフェイス上に無制限にホストを許可する「authentication host-mode multi-auth」を使用します。

手順 51　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。

```
SWITCH(config)#interface GigabitEthernetX/Y
SWITCH(config-if)#description ACCESS (Multi-Auth w/ Low-Impact Mode)
```

手順 52 ポートをアクセス モードにします。このコマンドがないと、インターフェイスは「authentication」関連のコマンドを受け取りません。

```
SWITCH(config-if)#switchport mode access
SWITCH(config-if)#switchport access vlan 10
SWITCH(config-if)#switchport voice vlan 11
```

手順 53 (オプション)デバイス センサーの CDP および LLDP を有効にします(デフォルトで有効になります)

```
SWITCH(config-if)#cdp enable
SWITCH(config-if)#lldp receive
```

手順 54 ロー インパクト モード用の事前認証 ACL を適用します。

```
SWITCH(config-if)#ip access-group ACL-DEFAULT in
```

手順 55 RADIUS の応答に関係なく、ネットワーク アクセスを許可します。上記の ACL と組み合わせて、認証に失敗したデバイスにどの程度のアクセス権を与えるかをコントロールする必要があります。

```
SWITCH(config-if)#authentication open
```

注: 上記のコマンドは、認証の前、および認証が失敗した場合(RADIUS が ACCESS-REJECT を送り返した場合)にアクセスを許可します。ただし、RADIUS サーバが dVLAN や dACL などの認証属性とともに ACCESS-ACCEPT を送り返した場合には、その認証がこのセッションで適用されます。これは、dACL がネットワークへの制限付きアクセスを提供する場合、「authentication open」指令に関係なく、エンドポイントが dACL による制限付きアクセスを持つことを意味します。

手順 56 (オプション)ネットワークから認証されていないポートにブロードキャスト トラフィックが入ることを許可します。これは WoL(Wake on LAN)プロセスに役立ち、ネットワーク管理サーバがオン デマンドでクライアントを起動できるようになります。また、別のホストからのネットワーク要求がなく、自身で多くのトラフィックを生成しない特定のタイプのデバイスの MAB プロセスにも役立ちます。

```
SWITCH(config-if)#authentication control-direction in
```

手順 57 802.1x 認証に失敗した後に MAB に移動することをポートに許可します。

```
SWITCH(config-if)#authentication event fail action next-method
```

手順 58 (オプション)認証中に RADIUS サーバが使用できない場合に、ポートのフェール オープン/フェール クローズを許可します。ポートをフェール オープンする必要がある場合には、同じ VLAN をアクセス VLAN として割り当てます。ポートをフェール クローズする必要がある場合には、SVI のないダミー VLAN を割り当てます。これは、どの RADIUS サーバにも到達できないときのデバイス接続にのみ影響します。このイベントの前にすでに接続されているデバイスは影響を受けません。このポートでは DEFAULT-ACL がまだ有効であることに注意してください。

```
SWITCH(config-if)#authentication event server dead action reinitialize vlan 10
```

注:VLAN ID は、ローカル スイッチで定義されている任意の VLAN に設定できます。どの ISE ノードも使用できず、そのような状況でフェール オープンが必要な場合には、通常のユーザ VLAN として同じ VLAN ID を設定することを推奨します。一方で、フェール クローズが必要な場合には、SVI のない VLAN ID に設定することができます。

手順 59 (オプション)どの RADIUS サーバも使用できない場合に、割り当てられた音声 VLAN に対して音声デバイスが承認されるようにします。

```
SWITCH(config-if)#authentication event server dead action authorize voice
```

手順 60 (オプション)RADIUS サーバが到達可能な場合、ポートが再初期化され、これによりインターフェイス上の各エンドポイントが再認証されます。このコマンドは、サーバが再び到達可能になった後もポートをフェール オープン/フェール クローズのままにする動作が必要な場合には省略できます。

```
SWITCH(config-if)#authentication event server alive action reinitialize
```

手順 61 ポートを、1 つの音声デバイスと無制限のデータ デバイスを許可するマルチ認証モードにします。スイッチング プラットフォームに応じて、このポートはすべてのデータ エンドポイントの同じ VLAN、または複数の VLAN に強制されます。

```
SWITCH(config-if)#authentication host-mode multi-auth
```

手順 62 (オプション)802.1x ポートを設定して、デバイスが 802.1x の有効なポートに接続されたときにデバイスに許可された最大数がすでにポートで認証されていた場合に、ポートをシャットダウンすることや、syslog エラーを生成すること、または新しいデバイスからのパケットを廃棄することができます。デフォルト設定は「shutdown」で、条件が満たされた場合にポートがエラー ディセーブルになります。「restrict」はポートを起動状態にしたままインシデントを記録します。通常、これは同じインターフェイスに複数のデバイスを許可するマルチ認証ポートでは問題になりませんが、複数の音声デバイスが接続されている場合や、インターフェイスがマルチドメインまたはシングル ホスト モードの場合には、ポートが違反となる可能性があります。

```
SWITCH(config-if)#authentication violation restrict
```

手順 63 (オプション)ポートの再認証と非アクティビティ タイマーを有効にします。このコマンドは、値がポートに静的に割り当てられている場合でも、RADIUS サーバから取得されている場合でも必要です。

```
SWITCH(config-if)#authentication periodic
```

手順 64 (オプション)再認証タイマー間隔(セッション タイマー)が RADIUS サーバからスイッチにダウンロードされるようにします。

```
SWITCH(config-if)#authentication timer reauthenticate server
```

注:属性 27(Session-Timeout)と 29(Terminate-Action)を RADIUS サーバで設定することができます。「RADIUS-Request」の属性 28 を使用すると、セッションが再認証されます。「Default」に設定するとセッションが終了され、再起動が強制されます。RADIUS サーバから値が送信されない場合は、セッションに再認証タイマーが適用されません。

手順 65 (オプション)非アクティビティ タイマー間隔が RADIUS サーバからスイッチにダウンロードされるようにします。「dynamic」というキーワードは、セッションを削除する前に ARP プローブを送信するように NAD に指示し、デバイスが実際に切断されるようにします。

```
SWITCH(config-if)#authentication timer inactivity server dynamic
```

注:RADIUS サーバからは、属性 28(Idle-Timeout)を設定できます。RADIUS サーバから値が送信されない場合は、セッションにアイドル タイムアウト タイマーが適用されません。

手順 66 ポート上で MAC(MAC 認証バイパス)を有効にします。

```
SWITCH(config-if)#mab
```

手順 67 スイッチからの EAPoL ID 要求フレームの間隔を削減します。再試行値と組み合わせた場合、ネットワークへのゲスト アクセスが 30 秒間待機されるようになります。tx-period のデフォルト値は 30 秒で、ゲスト デバイスの合計待機時間は 90 秒になります。待機時間が 90 秒の場合、多くのデバイスがネットワークからの IP アドレスの取得を諦めます。10 秒から開始し、必要に応じてより小さい値に削減してゲスト ユーザ エクスペリエンスを向上させることを推奨します。

```
SWITCH(config-if)#dot1x timeout tx-period 10
```

注:「authentication open」指令がインターフェイスで使用されている場合、802.1x 認証の前にネットワーク アクセスのためにポートがすでに開いているため、この値の影響は小さくなります。

手順 68 アクセス ポートのスパニング ツリー PortFast を有効にします。

```
SWITCH(config-if)#spanning-tree portfast
```

手順 69 このコマンドは、ポートで 802.1x を本質的に有効にします。このコマンドは、残りの 802.1x コマンドを入力した後に最後に実行することを推奨します。

```
SWITCH(config-if)#authentication port-control auto
```

インターフェイス レベル設定(クローズド モードの設定)

次のインターフェイス設定はクローズド モードの設定です。このモードでは、エンドポイントは 802.1X または MAB を介した認証が成功するまでトラフィックを渡すことができません。必須ではありませんが、この設定により単一のインターフェイス上に単一の音声デバイスと単一のデータ デバイスを許可する「authentication host-mode multi-domain」が活用されます。

手順 70 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。

```
SWITCH(config)#interface GigabitEthernetX/Y
SWITCH(config-if)#description ACCESS (Multi-Domain w/ Closed Mode)
```

手順 71 ポートをアクセス モードにします。このコマンドがないと、インターフェイスは「authentication」関連のコマンドを受け取りません。

```
SWITCH(config-if)#switchport mode access
SWITCH(config-if)#switchport access vlan 10
SWITCH(config-if)#switchport voice vlan 11
```

注:ユーザ名とパスワードは、ISE が利用している ID データベースで有効なアカウントである必要はありません。ISE ノードが成功した認証のために ACCESS-ACCEPT を送り返す場合でも、失敗した認証のために ACCESS_REJECT を送り返す場合でも、スイッチは両方の応答を RADIUS デッド設定のためのライブサーバからの有効な応答と見なします。MS Active Directory や LDAP などの外部 ID ストアを使用する場合には、ここで有効なアカウントを提供することに利点があります。有効なアカウントを使用すると、スイッチがバックエンド ID ストアまでテストし、ISE ノードが外部 ID データベースへの接続性を持つことを確認することができます。

手順 72 (オプション)デバイス センサーの CDP および LLDP を有効にします(デフォルトで有効になります)

```
SWITCH(config-if)#cdp enable
SWITCH(config-if)#lldp receive
```

手順 73 (オプション)ネットワークから認証されていないポートにブロードキャスト トラフィックが入ることを許可します。これは WoL プロセスに役立ち、ネットワーク管理サーバがオン デマンドでクライアントを起動できるようになります。また、別のホストからのネットワーク要求がなく、自身で多くのトラフィックを生成しない特定のタイプのデバイスの MAB プロセスにも役立ちます。

```
SWITCH(config-if)#authentication control-direction in
```

手順 74 802.1x 認証に失敗した後に MAB に移動することをポートに許可します。

```
SWITCH(config-if)#authentication event fail action next-method
```

手順 75 (オプション)認証中に RADIUS サーバが使用できない場合に、ポートのフェール オープン/フェール クローズを許可します。ポートをフェール オープンする必要がある場合には、同じ VLAN をアクセス VLAN として割り当てます。ポートをフェール クローズする必要がある場合には、SVI のないダミー VLAN を割り当てます。これは、どの RADIUS サーバにも到達できないときのデバイス接続にのみ影響します。このイベントの前にすでに接続されているデバイスは影響を受けません。このポートでは DEFAULT-ACL がまだ有効であることに注意してください

```
SWITCH(config-if)#authentication event server dead action authorize
```

注:コマンドの最後で VLAN ID を指定して、重要イベントが発生したときの VLAN ID を指定することができます。省略した場合、「switchport access vlan」コマンドで指定されている VLAN が使用されます。

手順 76 (オプション)どの RADIUS サーバも使用できない場合に、割り当てられた音声 VLAN に対して音声デバイスが承認されるようにします。

```
SWITCH(config-if)#authentication event server dead action authorize voice
```

手順 77 (オプション)RADIUS サーバが到達可能な場合、ポートが再初期化され、これによりインターフェイス上の各エンドポイントが再認証されます。このコマンドは、サーバが到達可能になった後もポートをフェール オープン/フェール クローズのままにする動作が必要な場合には省略できます。

```
SWITCH(config-if)#authentication event server alive action reinitialize
```

手順 78 ポートを、1 つの音声デバイスと 1 つのデータ デバイスを許可するマルチドメイン モードにします。

```
SWITCH(config-if)#authentication host-mode multi-domain
```

手順 79 (オプション)802.1x ポートを設定して、新しいデバイスが 802.1x の有効なポートに接続されたときにデバイスに許可された最大数がすでにそのポートで認証されていた場合に、シャットダウンすることや、syslog エラーを生成すること、またはパケットを廃棄することができます。デフォルト設定は「shutdown」で、条件が満たされた場合にポートがエラー ディセーブルになります。「restrict」はポートを起動状態にしたままインシデントを記録します。通常、これは同じインターフェイスに複数のデバイスを許可するマルチ認証ポートでは問題になりませんが、複数の音声デバイスが接続されている場合には、ポートが違反となる可能性があります。

```
SWITCH(config-if)#authentication violation restrict
```

手順 80 （オプション）ポートの再認証と非アクティビティ タイマーを有効にします。このコマンドは、値がポートに静的に割り当てられている場合でも、RADIUS サーバから取得されている場合でも必要です。

```
SWITCH(config-if)#authentication periodic
```

手順 81 （オプション）再認証タイマー間隔（セッション タイマー）が RADIUS サーバからスイッチにダウンロードされるようにします。

```
SWITCH(config-if)#authentication timer reauthenticate server
```

手順 82 （オプション）非アクティビティ タイマー間隔が RADIUS サーバからスイッチにダウンロードされるようにします。「dynamic」というキーワードは、セッションを削除する前に ARP プローブを送信するように NAD に指示し、デバイスが実際に切断されるようにします。

```
SWITCH(config-if)#authentication timer inactivity server dynamic
```

手順 83 ポート上で MAC（MAC 認証バイパス）を有効にします。

```
SWITCH(config-if)#mab
```

手順 84 スイッチからの EAPoL ID 要求フレームの間隔を削減します。再試行値と組み合わせた場合、ネットワークへのゲスト アクセスが 30 秒間待機されるようになります。tx-period のデフォルト値は 30 秒で、ゲスト デバイスの合計待機時間は 90 秒になります。多くのデバイスが、90 秒より前にネットワークからの IP アドレスの取得を試みることを止めます。10 秒から開始し、必要に応じてより小さい値に削減してゲスト ユーザ エクスペリエンスを向上させることを推奨します。

```
SWITCH(config-if)#dot1x timeout tx-period 10
```

手順 85 アクセス ポートのスパニング ツリー PortFast を有効にします。

```
SWITCH(config-if)#spanning-tree portfast
```

手順 86 ポート上で 802.1x を有効にします。このコマンドは、残りの 802.1x コマンドを入力した後に最後に実行することを推奨します。

```
SWITCH(config-if)#authentication port-control auto
```

付録 A: サンプル設定

デバイス センサーのあるグローバル設定

```
ip domain-name EXAMPLE.COM
username RADIUS-TEST password 0 PASSWORD
crypto key generate rsa general-keys mod 2048
aaa new-model
aaa authentication dot1x default group ISE
aaa authorization network default group ISE
aaa accounting dot1x default start-stop group ISE
aaa accounting update newinfo periodic 2880
aaa server radius dynamic-author
 client 10.1.200.11 server-key RADIUS_KEY
 client 10.1.200.11 server-key RADIUS_KEY
aaa session-id common
dot1x system-auth-control
dot1x critical eapol
ip device tracking
vlan 10
 name USER
vlan 11
 name VOICE
vlan 100
 name MGMT
interface 10
 ip address 10.1.10.1 255.255.255.0
ip helper-address 10.1.200.10
interface 11
 ip address 10.1.11.1 255.255.255.0
ip helper-address 10.1.200.10
interface 100
 ip address 10.1.100.1 255.255.255.0
ip http server
ip access-list extended ACL_WEBAUTH_REDIRECT
 permit tcp any any eq www
 permit tcp any any eq 443
ip access-list extended BLACKHOLE
 permit tcp any any eq www
 permit tcp any any eq 443
ip access-list extended ACL-DEFAULT
 permit udp any any eq domain
 permit udp any eq bootpc any eq bootps
 deny   ip any any
radius-server vsa send authentication
radius-server vsa send accounting
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius server ISE01
 address ipv4 10.1.200.11
 automate-tester username RADIUS-TEST probe-on
 # For IOS & IOS-XE without 'probe-on' feature use following command instead
 ! automate-tester username RADIUS-TEST idle-time 10
 key RADIUS_KEY
radius server ISE02
 address ipv4 10.1.200.11
 automate-tester username RADIUS-TEST probe-on
 # For IOS & IOS-XE without 'probe-on' feature use following command instead
 ! automate-tester username RADIUS-TEST idle-time 10
 key RADIUS_KEY
aaa group server radius ISE
 server name ISE01
 server name ISE02
 deadtime 15
```

```
radius-server dead-criteria time 10 tries 3
ip radius source-interface vlan 100
device-sensor filter-list dhcp list TLV-DHCP
 option name host-name
 option name requested-address
 option name parameter-request-list
 option name class-identifier
 option name client-identifier
device-sensor filter-spec dhcp include list TLV-DHCP
cdp run
device-sensor filter-list cdp list TLV-CDP
 tlv name device-name
 tlv name address-type Craig may not be needed
 tlv name capabilities-type
 tlv name platform-type
device-sensor filter-spec cdp include list TLV-CDP
lldp run
device-sensor filter-list lldp list TLV-LLDP
 tlv name system-name
 tlv name system-description
device-sensor filter-spec lldp include list TLV-LLDP
device-sensor accounting
device-sensor notify all-changes
no macro auto monitor
access-session template monitor
終了
write memory
```

デバイス センサーのないグローバル設定

```
ip domain-name EXAMPLE.COM
username RADIUS-TEST password 0 PASSWORD
crypto key generate rsa general-keys mod 2048
aaa new-model
aaa authentication dot1x default group ISE
aaa authorization network default group ISE
aaa accounting dot1x default start-stop group ISE
aaa accounting update newinfo periodic 2880
aaa server radius dynamic-author
 client 10.1.200.11 server-key RADIUS_KEY
 client 10.1.200.11 server-key RADIUS_KEY
aaa session-id common
dot1x system-auth-control
dot1x critical eapol
ip device tracking
vlan 10
 name USER
vlan 11
 name VOICE
vlan 100
 name MGMT
interface 10
 ip address 10.1.10.1 255.255.255.0
 ip helper-address 10.1.200.10
 ip helper-address 10.1.200.11
interface 11
 ip address 10.1.11.1 255.255.255.0
 ip helper-address 10.1.200.10
 ip helper-address 10.1.200.11
interface 100
 ip address 10.1.100.1 255.255.255.0
ip http server
ip access-list extended ACL_WEBAUTH_REDIRECT
 permit tcp any any eq www
 permit tcp any any eq 443
ip access-list extended BLACKHOLE
```

```
 permit tcp any any eq www
 permit tcp any any eq 443
ip access-list extended ACL-DEFAULT
 permit udp any any eq domain
 permit udp any eq bootpc any eq bootps
 deny   ip any any
radius-server vsa send authentication
radius-server vsa send accounting
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius server ISE01
 address ipv4 10.1.200.11
 automate-tester username RADIUS-TEST idle-time 10
 key RADIUS_KEY
radius server ISE02
 address ipv4 10.1.200.11
 automate-tester username RADIUS-TEST idle-time 10
 key RADIUS_KEY
aaa group server radius ISE
 server name ISE01
 server name ISE02
 deadtime 15
radius-server dead-criteria time 10 tries 3
ip radius source-interface vlan 100
snmp-server community SNMP_COMMUNITY_STRING RO
ip dhcp snooping
ip dhcp snooping vlan 10, 11
終了
write memory
```

ロー インパクト モードのインターフェイス レベル設定

```
description ACCESS (Multi-Auth w/ Low-Impact Mode)
switchport mode access
switchport access vlan 10
switchport voice vlan 11
ip access-group ACL-DEFAULT in
authentication open
authentication event fail action next-method
authentication event server dead action reinitialize vlan 10
authentication event server dead action authorize voice
authentication event server alive action reinitialize
authentication host-mode multi-auth
mab
authentication violation restrict
authentication periodic
authentication timer reauthenticate server
authentication timer inactivity server dynamic
dot1x timeout tx-period 10
spanning-tree portfast
authentication port-control auto
```

クローズド モードのインターフェイス レベル設定

```
description ACCESS (Closed Mode)
switchport mode access
switchport access vlan 10
switchport voice vlan 11
authentication event fail action next-method
authentication event server dead action authorize
authentication event server dead action authorize voice
authentication event server alive action reinitialize
authentication host-mode multi-domain
mab
authentication violation restrict
authentication periodic
authentication timer reauthenticate server
authentication timer inactivity server dynamic
dot1x timeout tx-period 10
spanning-tree portfast
authentication port-control auto
```