Cisco Identity Services Engine での NEAT の設定例

目次

概要

この資料は簡単なシナリオでネットワークエッジ 認証 トポロジーの設定および動作を（端正な）記述したものです。 端正クライアント の 情報シグナリング プロトコル（CISP）をサプリカントとオーセンティケータ スイッチ間のクライアントのMACアドレスおよび VLAN 情報を伝搬するために利用します。

この設定例では、両方ともオーセンティケータ スイッチ（またオーセンティケータと呼ばれる）およびサプリカント スイッチ（またサプリカントと呼ばれる） 802.1X 認証を行います; オーセンティケータはサプリカントを認証します、それから、テスト PC を認証する。

前提条件

要件

Cisco は IEEE 802.1x 認証規格のナレッジがあることを推奨します。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco IOS ® ソフトウェアの 2 つの Cisco Catalyst 3560 シリーズ スイッチ、リリース 12.2(55)SE8; 1 スイッチはオーセンティケータとして機能し、他人はサプリカントとして機能します。
- Cisco Identity Services Engine （ ISE ）、リリース 1.2。
- Microsoft Windows XP がある PC、サービスパック 3。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

設定

この例はのための設定 例をカバーします:

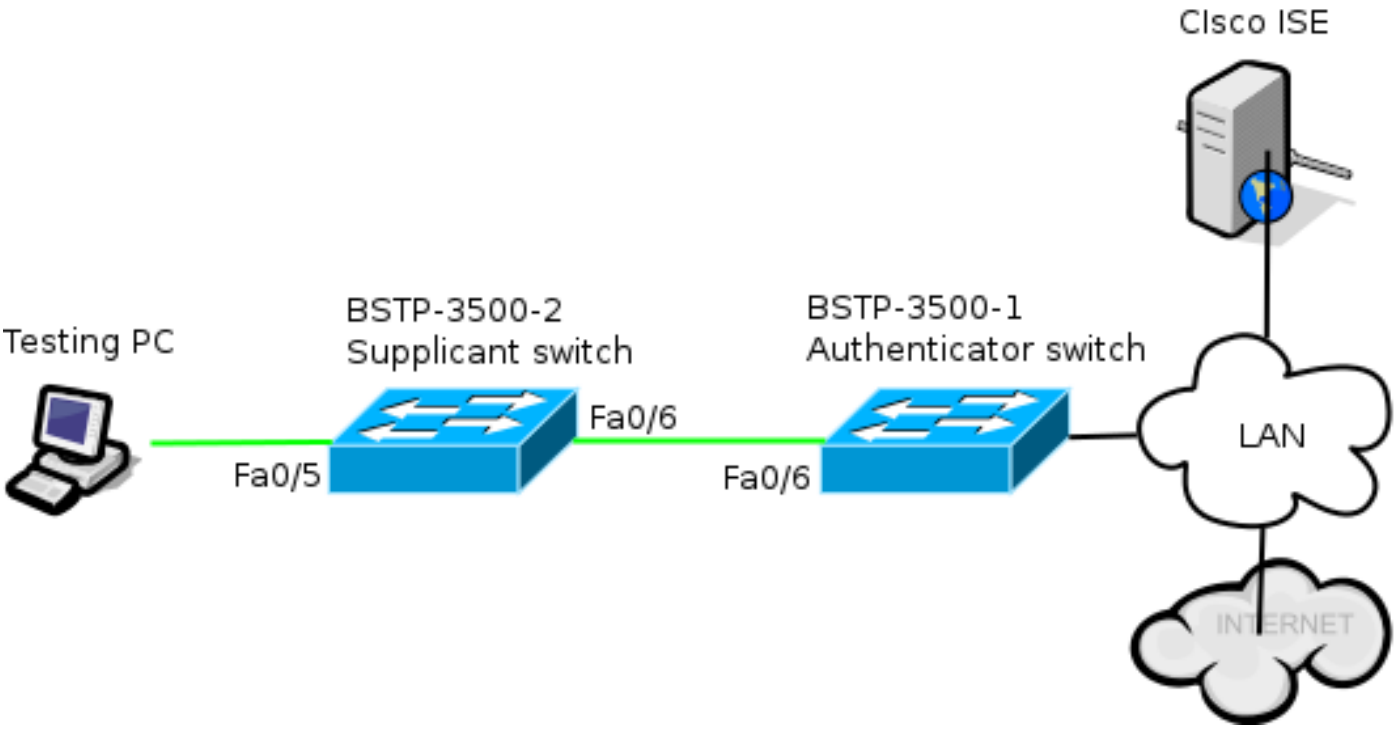
- オーセンティケータ スイッチ
- サプリカント スイッチ
- Cisco ISE

コンフィギュレーションは必要とされた perfom 最小のこのラボ演習です; それらは最適のためにですまたは他の必要を達成しないかもしれません。

> **注:** このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

このネットワークダイアグラムはこの例で使用される接続を説明します。 黒い行は論理的か物理的接続性を示し、緑の線は 802.1X の使用によって認証されるリンクを示します。



オーセンティケータ スイッチ設定

オーセンティケータは dot1x のために必要とされる基本的な要素が含まれています。 この例では、端正に特定のまたは CISP は太字ですコマンド。

これは基本的な認証、許可および会計（AAA）設定です:

```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius

radius-server host 10.48.66.107 auth-port 1812 acct-port 1813 key cisco

! Enable authenticator switch to authenticate the supplicant switch.
dot1x system-auth-control
! Enable CISP framework.
cisp enable

! configure uplink port as access and dot1x authentication.
interface FastEthernet0/6
switchport mode access
authentication port-control auto
dot1x pae authenticator
spanning-tree portfast
```

CISP はグローバルに 有効に なり、相互接続ポートはオーセンティケータおよびアクセス モードで設定されます。

サプリカント スイッチ設定

正確なサプリカント 設定は予想通りはたらいてが全体のセットアップ用の重大です。 この設定例は典型的な AAA および dot1x 設定が含まれています。

これは基本的な AAA設定です:

```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius

radius-server host 10.48.66.107 auth-port 1812 acct-port 1813 key cisco

! Enable supplicant switch to authenticate devices connected
dot1x system-auth-control

! Forces the switch to send only multicast EAPOL packets when it receives either
unicast or multicast packets, which allows NEAT to work on the supplicant
switch in all host modes.
dot1x supplicant force-multicast

! Enable CISP framework operation.
cisp enable
```

サプリカントは資格情報を設定し、使用されるべき Extensible Authentication Protocol（EAP）方式を供給する必要があります。

サプリカントはセキュアなプロトコル（ファースト）（他の EAP タイプの間で）によって CISP の場合には認証のために EAP メッセージ ダイジェスト 5（MD5）および EAP 適用範囲が広い認証を使用できます。 ISE 設定を最低限に保つために、この例はオーセンティケータにサプリカントの認証のために EAP-MD5 を使用します。（保護されたアクセス クレデンシャル[PAC]プロビジョニングを必要とするデフォルトは EAP-FAST の使用を強制します、; この資料はそのシナリオを取り扱っていません。）

```
! configure EAP mode used by supplicant switch to authenticate itself to
authenticator switch eap profile EAP_PRO
method md5

! Configure credentials use by supplicant switch during that authentication.
dot1x credentials CRED_PRO
 username bsnsswitch
password 0 C1sco123
```

オーセンティケータへのサプリカントの接続はトランク ポートであるために既に設定されています（オーセンティケータのアクセス ポート 設定と対照をなして）。 この段階では、これは期待されます; 設定は動的に ISE が正しいアトリビュートを戻す場合変更されます。

```
interface FastEthernet0/6
switchport trunk encapsulation dot1q
 switchport mode trunk
dot1x pae supplicant
 dot1x credentials CRED_PRO
 dot1x supplicant eap profile EAP_PRO
```

Windows PC に接続するポートに最小コンフィギュレーションがあり、参照だけ用にここに示されています。

```
interface FastEthernet0/5
switchport access vlan 200
switchport mode access
authentication port-control auto
dot1x pae authenticator
```

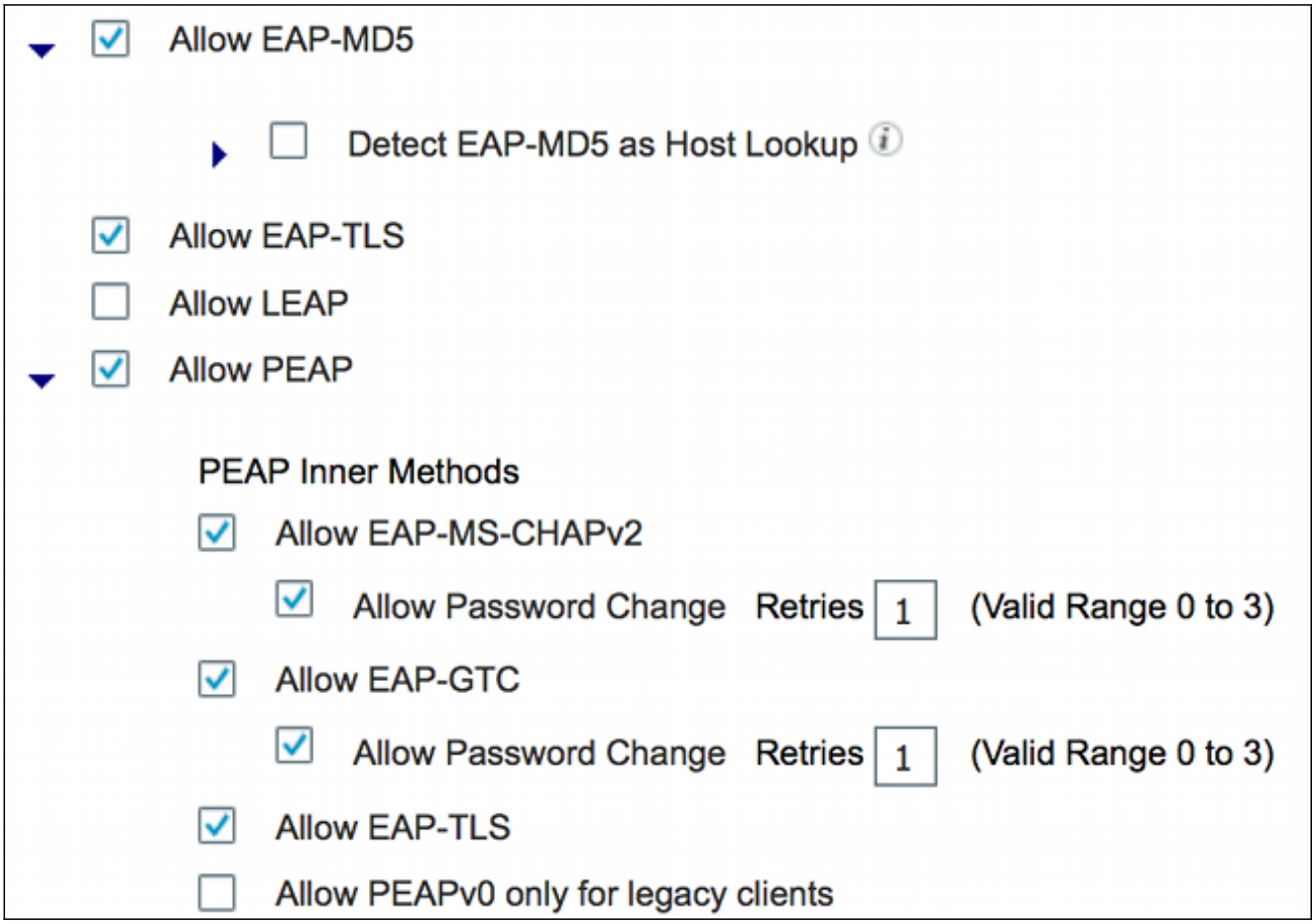
ISE 設定

このプロシージャは基本 ISE 設定を設定する方法を記述します。

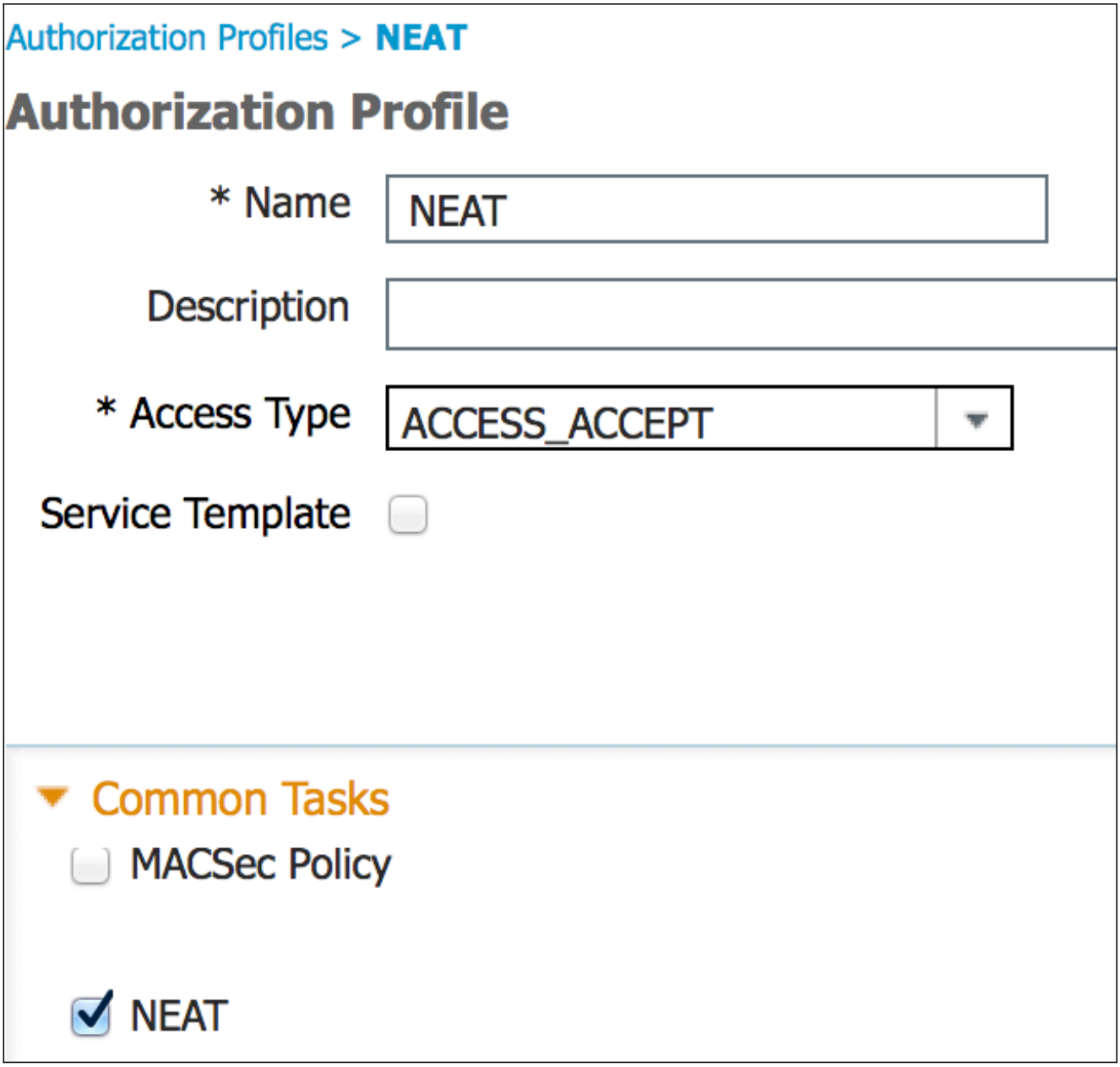
1. 要求された認証プロトコルを有効に して下さい。

   この例では、配線された dot1x は EAP-MD5 がオーセンティケータにサプリカントを認証するようにし、Protected Extensible Authentication Protocol （ PEAP ）が- Microsoft Challenge Handshake Authentication Protocol バージョン 2 （ MSCHAPv2 ）サプリカントに Windows PC を認証するようにします。

   > 許可されたプロトコルはポリシー > 結果 > 認証にナビゲート し、配線された dot1x によって使用される**プロトコル Service リストを**選択しこのステップのプロトコルを有効に なります確認します。



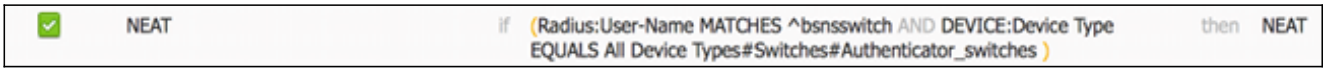
2. 承認ポリシーを作成して下さい。 **ポリシー > 結果 > 許可 > 承認ポリシー**にナビゲート し、ポリシーを作成するか、またはアップデートして下さいそうすれば端正がように戻されたアトリビュート含まれています。 このようなポリシーの例を次に示します。



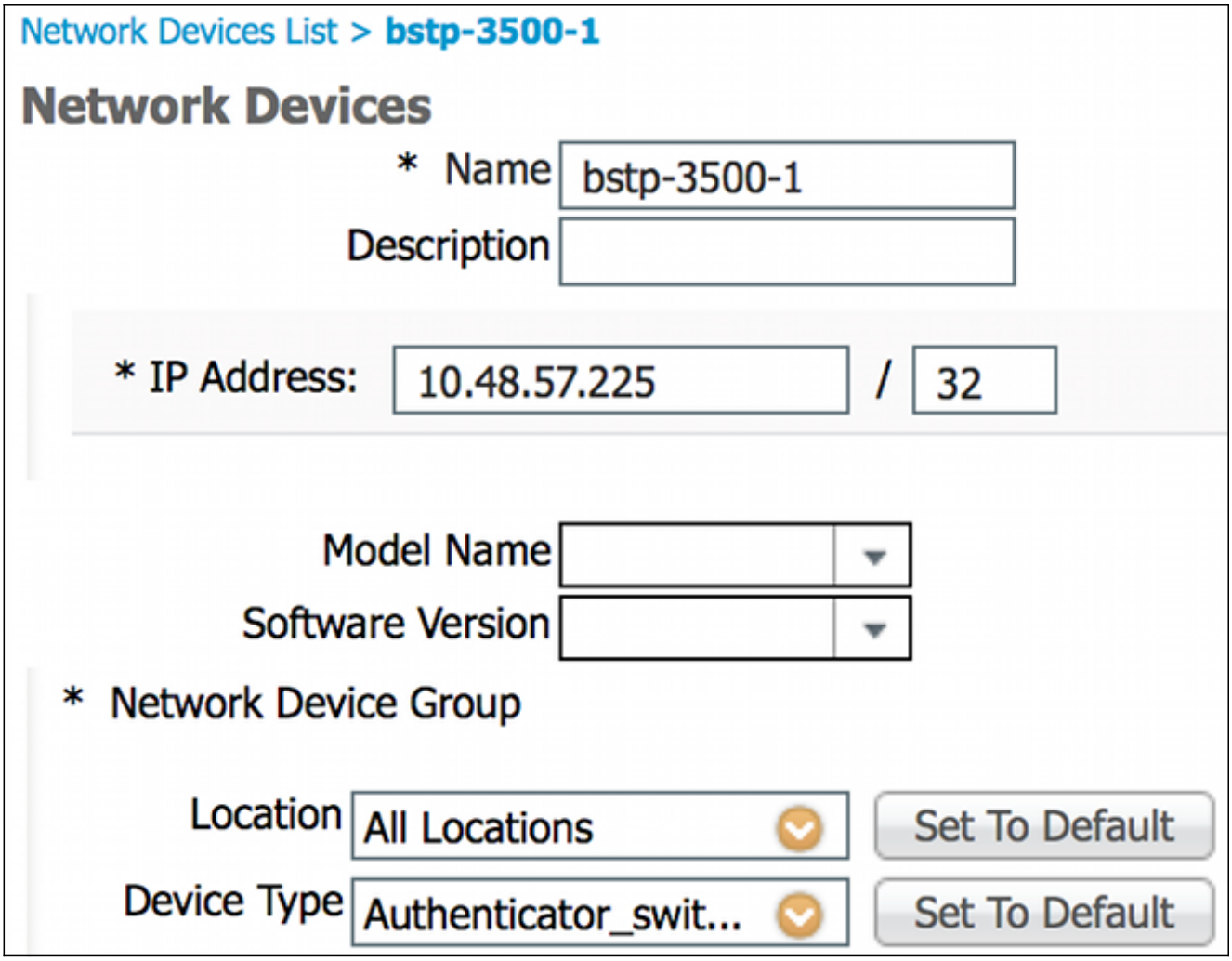
端正なオプションがつくとき、ISE は許可の一部として device-traffic-class=switch を戻します。 このオプションはトランキングするためにアクセスからオーセンティケータのポートモードを変更して必要です。

3. このプロファイルを使用する承認規則を作成して下さい。 **ポリシー > 許可**にナビゲート し、ルールを作成するか、またはアップデートして下さい。

   この例では、Authenticator_switches と問い合わせられる特別なデバイス グループは作成され、すべての要求元は bsnsswitch から始まるユーザ名を送信 します。



4. 適切なグループにスイッチを追加して下さい。 **Administration > ネットワークリソース > ネットワークデバイス**にナビゲート し、『Add』 をクリック して下さい。



この例では、BSTP-3500-1（オーセンティケータ）は Authenticator_switches グループの一部です; BSTP-3500-2（サプリカント）はこのグループの一部である必要はありません。

確認

ここでは、設定が正常に動作していることを確認します。 このセクションは 2 つの動作を記述します:

- スイッチ間の認証
- Windows PC とサプリカント間の認証

それはまた 3 つの追加状況を説明します:

- ネットワークからの認証されたクライアントの削除
- サプリカントの削除
- サプリカントの dot1x のないポート

注：

特定の show コマンドがアウトプット インタープリタ ツール（登録ユーザ専用）でサポートされています。 show コマンド出力の分析を表示するには、アウトプット インタープリタ ツールを使用します。

debug コマンドを使用する前に、『**debug コマンドの重要な情報**』を参照してください。

オーセンティケータ スイッチへのサプリカント スイッチ 認証

この例では、サプリカントはオーセンティケータに認証します。 プロセスのステップは次のとおりです:

1. サプリカントはポート fastethernet0/6 に設定され、プラグインされます。 dot1x 交換によりサプリカントはオーセンティケータに前もって構成されたユーザ名 および パスワードを送信 するために EAP を使用します。
2. オーセンティケータは RADIUS 交換を行い、ISE 検証に資格情報を提供します。
3. 資格情報が正しい場合、ISE が端正によって必要な属性を（device-traffic-class=switch）戻し、オーセンティケータはアクセスからトランキングするためにスイッチポートモードを変更します。

この例はスイッチ間の CISP 情報の交換を示したものです:

```
bstp-3500-1#debug cisp all
Oct 15 13:51:03.672: %AUTHMGR-5-START: Starting 'dot1x' for client
(001b.0d55.2187) on Interface Fa0/6 AuditSessionID 0A3039E10000000600757ABB
Oct 15 13:51:03.723: %DOT1X-5-SUCCESS: Authentication successful for client
(001b.0d55.2187) on Interface Fa0/6 AuditSessionID
Oct 15 13:51:03.723: %AUTHMGR-7-RESULT: Authentication result 'success' from
'dot1x' for client (001b.0d55.2187) on Interface Fa0/6 AuditSessionID
0A3039E10000000600757ABB
Oct 15 13:51:03.723: Applying command... 'no switchport access vlan 1' at Fa0/6
Oct 15 13:51:03.739: Applying command... 'no switchport nonegotiate' at Fa0/6
Oct 15 13:51:03.748: Applying command... 'switchport trunk encapsulation dot1q'
at Fa0/6
Oct 15 13:51:03.756: Applying command... 'switchport mode trunk' at Fa0/6
Oct 15 13:51:03.756: Applying command... 'switchport trunk native vlan 1' at
Fa0/6
Oct 15 13:51:03.764: Applying command... 'spanning-tree portfast trunk' at Fa0/6
Oct 15 13:51:04.805: %AUTHMGR-5-SUCCESS: Authorization succeeded for client
(001b.0d55.2187) on Interface Fa0/6 AuditSessionID 0A3039E10000000600757ABB

Oct 15 13:51:04.805: CISP-EVENT (Fa0/6): Received action Run Authenticator
Oct 15 13:51:04.805: CISP-EVENT (Fa0/6): Authenticator received event Start in
state Not Running
Oct 15 13:51:04.805: CISP-EVENT (Fa0/6): Authenticator state changed to Waiting
link UP
Oct 15 13:51:04.805: CISP-EVENT (Fa0/6): Sync supp_id: 0
Oct 15 13:51:05.669: %LINK-3-UPDOWN: Interface FastEthernet0/6, changed state to
up
Oct 15 13:51:06.793: CISP-EVENT (Fa0/6): Received action Run Authenticator
Oct 15 13:51:06.793: CISP-EVENT (Fa0/6): Authenticator received event Start in
state Waiting link UP (no-op)
Oct 15 13:51:07.799: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/6, changed state to up
Oct 15 13:51:07.799: CISP-EVENT (Fa0/6): Authenticator received event Link UP in
state Waiting link UP
Oct 15 13:51:07.799: CISP-EVENT (Fa0/6): Transmitting a CISP Packet
Oct 15 13:51:07.799: CISP-TXPAK (Fa0/6): Code:RESPONSE ID:0x20 Length:0x0018
Type:HELLO
Oct 15 13:51:07.799: CISP-EVENT (Fa0/6): Proposing CISP version: 1
Oct 15 13:51:07.799: CISP-EVENT (Fa0/6): Started 'hello' timer (5s)
Oct 15 13:51:07.799: CISP-EVENT (Fa0/6): Authenticator state changed to Idle
Oct 15 13:51:07.799: CISP-EVENT (Fa0/6): Sync supp_id: 0
Oct 15 13:51:07.799: CISP-EVENT: Received action Start Tick Timer
Oct 15 13:51:07.799: CISP-EVENT: Started CISP tick timer
Oct 15 13:51:12.942: CISP-EVENT (Fa0/6): 'hello' timer expired
```

```
Oct 15 13:51:12.942: CISP-EVENT (Fa0/6): Authenticator received event Timeout in
state Idle
Oct 15 13:51:12.942: CISP-EVENT (Fa0/6): Transmitting a CISP Packet
Oct 15 13:51:12.942: CISP-TXPAK (Fa0/6): Code:RESPONSE ID:0x20 Length:0x0018
Type:HELLO
Oct 15 13:51:12.942: CISP-EVENT (Fa0/6): Proposing CISP version: 1
Oct 15 13:51:12.942: CISP-EVENT (Fa0/6): Started 'hello' timer (5s)
Oct 15 13:51:18.084: CISP-EVENT (Fa0/6): 'hello' timer expired
Oct 15 13:51:18.084: CISP-EVENT (Fa0/6): Authenticator received event Timeout in
state Idle
Oct 15 13:51:18.084: CISP-EVENT (Fa0/6): Transmitting a CISP Packet
Oct 15 13:51:18.084: CISP-TXPAK (Fa0/6): Code:RESPONSE ID:0x20 Length:0x0018
Type:HELLO
Oct 15 13:51:18.084: CISP-EVENT (Fa0/6): Proposing CISP version: 1
Oct 15 13:51:18.084: CISP-EVENT (Fa0/6): Started 'hello' timer (5s)
Oct 15 13:51:23.226: CISP-EVENT (Fa0/6): 'hello' timer expired
Oct 15 13:51:23.226: CISP-EVENT (Fa0/6): Authenticator received event Timeout in
state Idle
Oct 15 13:51:23.226: CISP-EVENT (Fa0/6): Transmitting a CISP Packet
Oct 15 13:51:23.226: CISP-TXPAK (Fa0/6): Code:RESPONSE ID:0x20 Length:0x0018
Type:HELLO
Oct 15 13:51:23.226: CISP-EVENT (Fa0/6): Proposing CISP version: 1
Oct 15 13:51:23.226: CISP-EVENT (Fa0/6): Started 'hello' timer (5s)
Oct 15 13:51:28.377: CISP-EVENT (Fa0/6): 'hello' timer expired
Oct 15 13:51:28.377: CISP-EVENT (Fa0/6): Authenticator received event Timeout in
state Idle
Oct 15 13:51:29.400: CISP-EVENT: Stopped CISP tick timer
Oct 15 13:51:36.707: CISP-RXPAK (Fa0/6): Code:REQUEST ID:0x22 Length:0x001C
Type:REGISTRATION
Oct 15 13:51:36.707: Payload: 0200E84B
Oct 15 13:51:36.707: CISP-EVENT (Fa0/6): Authenticator received event Receive
Packet in state Idle
Oct 15 13:51:36.707: CISP-EVENT (Fa0/6): Proposed CISP version: 1
Oct 15 13:51:36.707: CISP-EVENT (Fa0/6): Negotiated CISP version: 1
Oct 15 13:51:36.707: CISP-EVENT (Fa0/6): Sync supp_id: 59467
Oct 15 13:51:36.707: CISP-EVENT (Fa0/6): Transmitting a CISP Packet
Oct 15 13:51:36.707: CISP-TXPAK (Fa0/6): Code:RESPONSE ID:0x22 Length:0x001C
Type:REGISTRATION
Oct 15 13:51:36.707: Payload: 01000000
Oct 15 13:51:36.724: CISP-RXPAK (Fa0/6): Code:REQUEST ID:0x23 Length:0x003A
Type:ADD_CLIENT
Oct 15 13:51:36.724: Payload: 010011020009001B0D5521C10300050 ...
Oct 15 13:51:36.724: CISP-EVENT (Fa0/6): Authenticator received event Receive
Packet in state Idle
Oct 15 13:51:36.724: CISP-EVENT (Fa0/6): Adding client 001b.0d55.21c1 (vlan: 200)
to authenticator list
Oct 15 13:51:36.724: CISP-EVENT (Fa0/6): Notifying interest parties about new
downstream client 001b.0d55.21c1 (vlan: 200)
Oct 15 13:51:36.724: CISP-EVENT (Fa0/6): Adding client info at Authenticator
Oct 15 13:51:36.724: CISP-EVENT (Fa0/6): Adding client 001b.0d55.21c0 (vlan: 1)
to authenticator list
Oct 15 13:51:36.724: CISP-EVENT (Fa0/6): Notifying interest parties about new
downstream client 001b.0d55.21c0 (vlan: 1)
Oct 15 13:51:36.724: CISP-EVENT (Fa0/6): Adding client info at Authenticator
Oct 15 13:51:36.724: CISP-EVENT (Fa0/6): Transmitting a CISP Packet
Oct 15 13:51:36.724: CISP-TXPAK (Fa0/6): Code:RESPONSE ID:0x23 Length:0x0018
Type:ADD_CLIENT
```

認証 および 権限が成功すれば、CISP 交換は行われます。 各交換にサプリカントによって返される、およびオーセンティケータからの応答および確認応答として動作する応答があります REQUEST。

2 つの個別の交換は実行された: 登録および ADD_CLIENT。 登録交換の間に、サプリカントは

CISP 可能である、オーセンティケータはそしてこのメッセージを確認しますことオーセンティケータを知らせ。 ADD_CLIENT 交換が要求元のローカルポートに接続されるデバイスについてのオーセンティケータを知らせるのに使用されています。 登録と同様に、ADD-CLIENT はサプリカントで始められ、オーセンティケータによって確認されます。

コミュニケーション、役割およびアドレスを確認するためにこれらの show コマンドを入力して下さい:

```
bstp-3500-1#show cisp clients

Authenticator Client Table:
---------------------------
MAC Address VLAN Interface
--------------------------------
001b.0d55.21c1 200 Fa0/6
001b.0d55.21c0 1 Fa0/6

bstp-3500-1#show cisp registrations

Interface(s) with CISP registered user(s):
----------------------------------------
Fa0/6
Auth Mgr (Authenticator)
```

この例では、オーセンティケータのロールは正しいインターフェイス (fa0/6) に正しく割り当てられ、2 つの MAC アドレスは登録されています。 MAC アドレスは VLAN1 と VLAN200 のポート fa0/6 のサプリカントです。

dot1x 認証 セッションの確認は今実行されたことができます。 アップストリーム スイッチの fa0/6 ポートは既に認証されています。 これは BSTP-3500-2 （ サプリカント ）がで差し込まれるとき引き起こされる dot1x 交換です:

```
bstp-3500-1#show authentication sessions

Interface MAC Address Method Domain Status Session ID
Fa0/6 001b.0d55.2187 dot1x DATA Authz Success 0A3039E10000000700FB3259
```

予想通りこの段階で、サプリカントにセッションがありません:

```
bstp-3500-2#show authentication sessions
No Auth Manager contexts currently exist
```

サプリカント スイッチへの Windows PC 認証

この例では、Windows PC はサプリカントに認証します。 プロセスのステップは次のとおりです:

1. Windows PC は FastEthernet に BSTP-3500-2 （ サプリカント ）の 0/5 のポート プラグインされます。
2. サプリカントは ISE と認証 および 権限を行います。
3. サプリカントは新しいクライアントがポートで接続されることオーセンティケータを知らせます。

これはサプリカントからの通信です:

```
Oct 15 14:19:37.207: %AUTHMGR-5-START: Starting 'dot1x' for client
(c464.13b4.29c3) on Interface Fa0/5 AuditSessionID 0A3039E200000013008F77FA
Oct 15 14:19:37.325: %DOT1X-5-SUCCESS: Authentication successful for client
(c464.13b4.29c3) on Interface Fa0/5 AuditSessionID
Oct 15 14:19:37.325: %AUTHMGR-7-RESULT: Authentication result 'success' from
```

```
'dot1x' for client (c464.13b4.29c3) on Interface Fa0/5 AuditSessionID
0A3039E200000013008F77FA
Oct 15 14:19:37.341: CISP-EVENT (Fa0/5): Received action Add Client
Oct 15 14:19:37.341: CISP-EVENT (Fa0/5): Adding client c464.13b4.29c3 (vlan: 200)
to supplicant list
Oct 15 14:19:37.341: CISP-EVENT (Fa0/6): Supplicant received event Add Client in
state Idle
Oct 15 14:19:37.341: CISP-EVENT (Fa0/6): Adding client c464.13b4.29c3 (vlan: 200)
to the ADD list
Oct 15 14:19:37.341: CISP-EVENT (Fa0/6): Adding client c464.13b4.29c3 (vlan: 200)
to ADD CLIENT req
Oct 15 14:19:37.341: CISP-EVENT (Fa0/6): Transmitting a CISP Packet
Oct 15 14:19:37.341: CISP-TXPAK (Fa0/6): Code:REQUEST ID:0x24 Length:0x0029
Type:ADD_CLIENT
Oct 15 14:19:37.341: Payload: 010011020009C46413B429C30300050 ...
Oct 15 14:19:37.341: CISP-EVENT (Fa0/6): Started 'retransmit' timer (30s)
Oct 15 14:19:37.341: CISP-EVENT: Started CISP tick timer
Oct 15 14:19:37.341: CISP-EVENT (Fa0/6): Supplicant state changed to Request
Oct 15 14:19:37.341: CISP-RXPAK (Fa0/6): Code:RESPONSE ID:0x24 Length:0x0018
Type:ADD_CLIENT
Oct 15 14:19:37.350: CISP-EVENT (Fa0/6): Supplicant received event Receive Packet
in state Request
Oct 15 14:19:37.350: CISP-EVENT (Fa0/6): Stopped 'retransmit' timer
Oct 15 14:19:37.350: CISP-EVENT (Fa0/6): All Clients implicitly ACKed
Oct 15 14:19:37.350: CISP-EVENT (Fa0/6): Supplicant state changed to Idle
Oct 15 14:19:38.356: %AUTHMGR-5-SUCCESS: Authorization succeeded for client
(c464.13b4.29c3) on Interface Fa0/5 AuditSessionID 0A3039E200000013008F77FA
Oct 15 14:19:38.356: CISP-EVENT (Fa0/5): Received action Run Authenticator
Oct 15 14:19:38.356: CISP-EVENT (Fa0/5): Authenticator received event Start in
state Not Running
Oct 15 14:19:38.356: CISP-EVENT (Fa0/5): Authenticator state changed to Waiting
link UP
Oct 15 14:19:38.356: CISP-EVENT (Fa0/5): Sync supp_id: 0
Oct 15 14:19:38.373: CISP-EVENT: Stopped CISP tick timer
Oct 15 14:19:39.162: %LINK-3-UPDOWN: Interface FastEthernet0/5, changed state to
up
```

ADD_CLIENT 交換は行われますが、登録交換は必要ではないです。

サプリカントの動作を確認するために、**提示 cisp 登録** コマンドを入力して下さい:

```
bstp-3500-2#show cisp registrations

Interface(s) with CISP registered user(s):
----------------------------------------
Fa0/5
Auth Mgr (Authenticator)
Fa0/6
802.1x Sup (Supplicant)
```

サプリカントにオーセンティケータ（fa0/6 インターフェイス）の方のサプリカントのロールおよび Windows PC （fa0/5 インターフェイス）の方のオーセンティケータのロールがあります。

オーセンティケータの動作を確認するために、**提示 cisp クライアントを**コマンド入力して下さい:

```
bstp-3500-1#show cisp clients

Authenticator Client Table:
---------------------------
MAC Address VLAN Interface
--------------------------------
001b.0d55.21c1 200 Fa0/6
```

```
001b.0d55.21c0 1 Fa0/6
c464.13b4.29c3 200 Fa0/6
```
新しい MAC アドレスは VLAN 200 の下でオーセンティケータで現われます。 サプリカントの AAA 要求で観察されたのは MAC アドレスです。

認証 セッションは同じデバイスがサプリカントの fa0/5 ポートで接続されることを示す必要があります:

```
bstp-3500-2#show authentication sessions

Interface MAC Address Method Domain Status Session ID
Fa0/5 c464.13b4.29c3 dot1x DATA Authz Success 0A3039E20000001501018B58
```

ネットワークからの認証されたクライアントの削除

クライアントが (たとえば) 取除かれる時ポートがシャットダウンされる場合、オーセンティケータは DELETE_CLIENT 交換によって知らせられます。

```
Oct 15 15:54:05.415: CISP-RXPAK (Fa0/6): Code:REQUEST ID:0x25 Length:0x0029
Type:DELETE_CLIENT
Oct 15 15:54:05.415: Payload: 010011020009C46413B429C30300050 ...
Oct 15 15:54:05.415: CISP-EVENT (Fa0/6): Authenticator received event Receive
Packet in state Idle
Oct 15 15:54:05.415: CISP-EVENT (Fa0/6): Removing client c464.13b4.29c3
(vlan: 200) from authenticator list
Oct 15 15:54:05.415: CISP-EVENT (Fa0/6): Notifying interest parties about
deletion of downstream client c464.13b4.29c3 (vlan: 200)
Oct 15 15:54:05.415: CISP-EVENT (Fa0/6): Transmitting a CISP Packet
Oct 15 15:54:05.415: CISP-TXPAK (Fa0/6): Code:RESPONSE ID:0x25 Length:0x0018
Type:DELETE_CLIENT
```

サプリカント スイッチの削除

サプリカントがプラグを抜かれるか、または取除かれるとき、オーセンティケータはポートに戻ってセキュリティ上の問題を避けるためにオリジナル設定をもたらします。

```
Oct 15 15:57:31.257: Applying command... 'no switchport nonegotiate' at Fa0/6
Oct 15 15:57:31.273: Applying command... 'switchport mode access' at Fa0/6
Oct 15 15:57:31.273: Applying command... 'no switchport trunk encapsulation
dot1q' at Fa0/6
Oct 15 15:57:31.290: Applying command... 'no switchport trunk native vlan 1' at
Fa0/6
Oct 15 15:57:31.299: Applying command... 'no spanning-tree portfast trunk' at
Fa0/6
Oct 15 15:57:31.307: Applying command... 'switchport access vlan 1' at Fa0/6
Oct 15 15:57:31.315: Applying command... 'spanning-tree portfast' at Fa0/6
Oct 15 15:57:32.247: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/6, changed state to down
Oct 15 15:57:32.247: CISP-EVENT (Fa0/6): Authenticator received event Link DOWN
in state Idle
Oct 15 15:57:32.247: CISP-EVENT (Fa0/6): Removing client 001b.0d55.21c1
(vlan: 200) from authenticator list
Oct 15 15:57:32.247: CISP-EVENT (Fa0/6): Notifying interest parties about
deletion of downstream client 001b.0d55.21c1 (vlan: 200)
Oct 15 15:57:32.247: CISP-EVENT (Fa0/6): Removing client 001b.0d55.21c0 (vlan: 1)
from authenticator list
Oct 15 15:57:32.247: CISP-EVENT (Fa0/6): Notifying interest parties about
deletion of downstream client 001b.0d55.21c0 (vlan: 1)
Oct 15 15:57:32.247: CISP-EVENT (Fa0/6): Authenticator state changed to Not
```

```
Running
Oct 15 15:57:32.247: CISP-EVENT (Fa0/6): Sync supp_id: 0
Oct 15 15:57:33.262: %LINK-3-UPDOWN: Interface FastEthernet0/6, changed state
to down
```

同時に、サプリカントは CISP 表からのサプリカントを表す取除き、そのインターフェイスの CISP を無効にしますクライアントを。

サプリカント スイッチの dot1x のないポート

CISP 情報は適用の別の層としてだけサプリカントからオーセンティケータへの伝搬する動作します。 サプリカントはそれに接続される許可された MAC アドレスすべてについてのオーセンティケータを知らせます。

シナリオは一般的に誤解されるこれです: デバイスが有効に なる dot1x がないポートで差し込まれれば MAC アドレスは CISP によってアップストリーム スイッチに学習され、伝搬させて。

オーセンティケータは CISP によって学ばれるすべてのクライアントから来る通信を可能にします。

要するに、それはデバイスのアクセスを、dot1x か他のメソッドによって制限し、オーセンティケータへの MAC アドレスおよび VLAN 情報を伝搬するサプリカントの口ールです。 オーセンティケータは情報の執行者がそれらの更新で提供したように機能します。

一例として、新しい VLAN （ VLAN300 ）はサプリカントのポート fa0/4 に両方のスイッチおよびデバイスでプラグインされました作成されました。 ポート fa0/4 は dot1x のために設定されない簡単なアクセス ポートです。

サプリカントからのこの出力は新しい登録済みのポートを示したものです:

```
bstp-3500-2#show cisp registrations

Interface(s) with CISP registered user(s):
----------------------------------------
Fa0/4
Fa0/5
Auth Mgr (Authenticator)
Fa0/6
802.1x Sup (Supplicant)
```

オーセンティケータで、新しい MAC アドレスは VLAN 300 で目に見えます。

```
bstp-3500-1#show cisp clients

Authenticator Client Table:
---------------------------
MAC Address VLAN Interface
---------------------------------
001b.0d55.21c1 200 Fa0/6
001b.0d55.21c0 1 Fa0/6
001b.0d55.21c2 300 Fa0/6
c464.13b4.29c3 200 Fa0/6
 68ef.bdc7.13ff 300 Fa0/6
```

トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

> **注:**
>
> 特定の show コマンドがアウトプット インタープリタ ツール（登録ユーザ専用）でサポートされています。 show コマンド出力の分析を表示するには、アウトプット インタープリタ ツールを使用します。
>
> debug コマンドを使用する前に、『**debug コマンドの重要な情報**』を参照してください。

これらのコマンドは端正および CISP を解決するのを助けます; この資料は殆んどのための例が含まれています:

- **全デバッグ cisp は**スイッチ間の CISP 情報の交換を示します。
- **cisp 概略を表示して下さい**-スイッチの CISP インターフェイス ステータスの概略を表示する。
- **cisp 登録を示して下さい**- CISP 交換に、それらのインターフェイスのロール加わる、そしてかどうかインターフェイスは端正の一部であるインターフェイス示します。
- **cisp クライアントを表示して下さい**-既知のクライアント MAC アドレスおよび位置の表を表示する（VLAN およびインターフェイス）。 これはオーセンティケータから役立ちます主に。