Network Edge Access Topology（NEAT）

Network Edge Access Topology を使用した 802.1x サプリカントおよびオーセンティケータスイッチ

802.1x 規格では、一般の人がアクセス可能なポートから不正なクライアントが LAN に接続しないように規制する（適切に認証されている場合を除く）、クライアント/サーバ型のアクセス コントロールおよび認証プロトコルを定めています。認証サーバーがスイッチ ポートに接続する各クライアントを認証したうえで、スイッチまたは LAN が提供するサービスを利用できるようにします。設定情報を含む、802.1x の詳細については、「Configuring IEEE 802.1x Port-Based Authentication」を参照してください。

Network Edge Access Topology（NEAT）機能は、ワイヤリングクローゼット外の領域まで識別を拡張します。これにより、任意のタイプのデバイスをポートで認証できます。NEAT では、サプリカントスイッチとオーセンティケータ間でクライアントの MAC と VLAN 情報を伝播するために Client Information Signalling Protocol（CISP）が使用されます。CISP および NEAT は L2 ポートでのみサポートされ、L3 ポートではサポートされません。Cisco Catalyst IE9300 高耐久性シリーズ スイッチで NEAT を設定できます。

- 802.1x スイッチ サプリカント：802.1x サプリカント機能を使用することで、別のスイッチのサプリカントとして機能するようにスイッチを設定できます。この設定は、たとえば、スイッチがワイヤリング クローゼット外にあり、トランク ポートを介してアップストリーム スイッチに接続される場合に役に立ちます。802.1x スイッチ サプリカント機能を使用して設定されたスイッチは、セキュアな接続のためにアップストリーム スイッチで認証します。サプリカント スイッチが認証に成功すると、オーセンティケータ スイッチでポー

トモードがアクセスからトランクに変更されます。サプリカントスイッチでは、CISP を有効にするときに手動でトランクを設定する必要があります。

- アクセス VLAN は、オーセンティケータ スイッチで設定されている場合、認証が成功した後にトランク ポートのネイティブ VLAN になります。

デフォルトでは、BPDU ガードが有効にされたオーセンティケータ スイッチにサプリカントのスイッチを接続する場合、オーセンティケータのポートはサプリカント スイッチが認証する前にスパニングツリー プロトコル（STP）のブリッジ プロトコル データ ユニット（BPDU）を受信した場合、errdisable 状態になる可能性があります。認証中にサプリカントのポートから送信されるトラフィックを制御できます。**dot1x supplicant controlled transient** グローバル コンフィギュレーション コマンドを入力すると、認証が完了する前にオーセンティケータ ポートがシャットダウンすることがないように、認証中に一時的にサプリカントのポートをブロックします。認証に失敗すると、サプリカントのポートが開きます。**no dot1x supplicant controlled transient** グローバル コンフィギュレーション コマンドを入力すると、認証期間中にサプリカント ポートが開きます。これはデフォルトの動作です。

BPDU ガードが **spanning-tree bpduguard enable** インターフェイス コンフィギュレーション コマンドによりオーセンティケータのスイッチ ポートで有効になっている場合、サプリカント スイッチで **dot1x supplicant controlled transient** コマンドを使用することを強く推奨します。

（注） **spanning-tree portfast bpduguard default** グローバル コンフィギュレーション コマンドを使用して、グローバルにオーセンティケータスイッチで BPDU ガードを有効にした場合、サプリカントスイッチで **dot1x supplicant controlled transient** コマンドを入力すると、BPDU の違反が避けられなくなります。

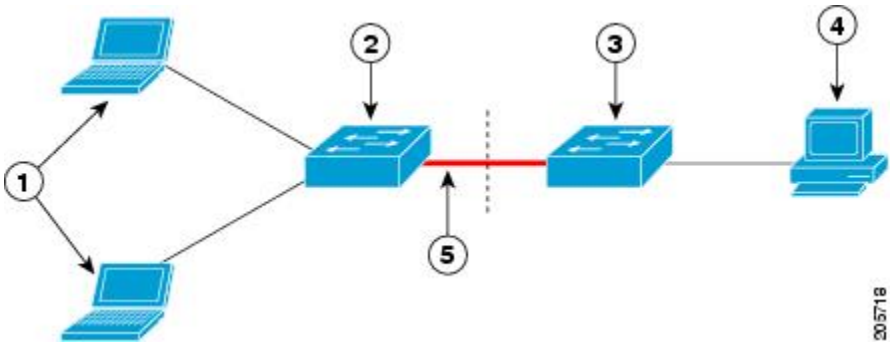
1 つ以上のサプリカントスイッチに接続するオーセンティケータ スイッチ インターフェイスで MDA または multiauth モードを有効にできます。マルチホスト モードはオーセンティケータ スイッチ インターフェイスではサポートされていません。

インターフェイスで有効になっているシングルホスト モードでオーセンティケータ スイッチをリブートすると、インターフェイスが認証前に err-disabled 状態に移行する場合があります。err-disabled 状態から回復するには、オーセンティケータ ポートをフラップしてインターフェイスを再度アクティブにし、認証を開始します。

すべてのホストモードで機能するように **dot1x supplicant force-multicast** グローバル コンフィギュレーション コマンドを NEAT のサプリカントスイッチで使用します。

- ホスト許可：許可済み（サプリカントでスイッチに接続する）ホストからのトラフィックだけがネットワークで許可されます。これらのスイッチは、CISP を使用して、サプリカントスイッチに接続する MAC アドレスをオーセンティケータスイッチに送信します。
- 自動有効化：オーセンティケータ スイッチでのトランク コンフィギュレーションを自動的に有効化します。これにより、サプリカント スイッチから着信する複数の VLAN のユーザー トラフィックが許可されます。ISE で cisco-av-pair を *device-traffic-class=switch* として設定します（この設定は *group* または *user* 設定で行うことができます）。

図 *1 : CISP* を使用したオーセンティケータまたはサプリカントスイッチ



1	ワークステーション（クライアント）
2	サプリカントスイッチ（ワイヤリングクローゼット外）
3	オーセンティケータ スイッチ
4	Cisco ISE
5	トランク ポート

（注） **switchport nonegotiate** コマンドは、NEAT を使用したサプリカントおよびオーセンティケータスイッチではサポートされません。このコマンドは、トポロジのサプリカント側で設定しないでください。オーセンティケータ サーバ側で設定した場合は、内部マクロによってポートからこのコマンドが自動的に削除されます。

注意事項と制約事項

次に、NEAT の設定および使用に関する注意事項と制約事項を示します。

- シスコの Identity Server Engine（ISE）などの RADIUS サーバーが必要です。
- CISP および NEAT は L2 ポートでのみサポートされ、L3 ポートではサポートされません。
- NEAT および 802.1x は、EtherChannel ポートではサポートされません。
- NEAT はダイナミックポートではサポートされません。
- MACsec は NEAT でサポートされます。
- NEAT は PTP と併用できます。

- MAB と NEAT は相互に排他的です。インターフェイス上で NEAT が有効の場合は、MAB を有効にすることはできません。また、インターフェイス上で MAB が有効の場合は、NEAT を有効にすることはできません。

NEAT を使用したオーセンティケータスイッチの設定

この機能を設定するには、ワイヤリング クローゼット外の 1 つのスイッチがサプリカントとして設定され、オーセンティケータ スイッチに接続されている必要があります。

（注）

- *cisco-av-pairs* は、ISE で *device-traffic-class=switch* として設定されている必要があります。これにより、サプリカントが正常に認証された後でトランクとしてインターフェイスが設定されます。

スイッチをオーセンティケータに設定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **cisp enable**
4. **interface** *interface-id*
5. **switchport mode access**
6. **authentication port-control auto**
7. **dot1x pae authenticator**
8. **spanning-tree portfast**
9. **end**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例：	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。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 3	**cisp enable** 例： `Device(config)# cisp enable`	CISP を有効にします。
ステップ 4	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/2`	設定するポートを指定し、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 5	**switchport mode access** 例： `Device(config-if)# switchport mode access`	ポートモードを **access** に設定します。
ステップ 6	**authentication port-control auto** 例： `Device(config-if)# authentication port-control auto`	ポート認証モードを auto に設定します。
ステップ 7	**dot1x pae authenticator** 例： `Device(config-if)# dot1x pae authenticator`	インターフェイスをポート アクセス エンティティ（PAE）オーセンティケータとして設定します。
ステップ 8	**spanning-tree portfast** 例： `Device(config-if)# spanning-tree portfast trunk`	インターフェイスを、複数の VLAN のメンバーであるインターフェイスのスパニングツリー フォワーディング ステートにすばやく移行できるようにします。このコマンドは、スイッチ間接続がレイヤ 2 ループの一部ではないことが確実な場合にのみ使用します。
ステップ 9	**end** 例： `Device(config-if)# end`	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、特権 EXEC モードに戻ります。

NEAT を使用したサプリカントスイッチの設定

スイッチをサプリカントに設定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **cisp enable**
4. **eap profile** *profile-name*
5. **method** *type*
6. **exit**
7. **dot1x credentials** *profile*
8. **username** *suppswitch*
9. **password** *password*
10. **dot1x supplicant force-multicast**
11. **interface** *interface-id*
12. **switchport trunk encapsulation dot1q**
13. **switchport mode trunk**
14. **dot1x pae supplicant**
15. **dot1x credentials** *profile-name*
16. **dot1x supplicant eap profile** *profile-name*
17. **end**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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	**cisp enable** 例：	CISP を有効にします。

	コマンドまたはアクション	目的
	`Device(config)# cisp enable`	
ステップ 4	**eap profile** *profile-name* 例： `Device(config)# eap profile CISP`	Extensible Authentication Protocol（EAP）プロファイルを作成し、EAP プロファイル コンフィギュレーション モードを開始します。
ステップ 5	**method** *type* 例： `Device(config-eap-profile)# method md5`	EAP 認証方式を指定します。
ステップ 6	**exit** 例： `Device(config-eap-profile)# exit`	EAP 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 7	**dot1x credentials** *profile* 例： `Device(config)# dot1x credentials test`	802.1x クレデンシャル プロファイルを作成します。これは、サプリカントとして設定されるポートに接続する必要があります。
ステップ 8	**username** *suppswitch* 例： `Device(config)# username suppswitch`	ユーザ名を作成します。
ステップ 9	**password** *password* 例： `Device(config)# password myswitch`	新しいユーザ名のパスワードを作成します。
ステップ 10	**dot1x supplicant force-multicast** 例： `Device(config)# dot1x supplicant force-multicast`	ユニキャストまたはマルチキャスト パケットのいずれかを受信した場合にスイッチに強制的にマルチキャスト EAPOL だけを送信させます。 これにより、NEAT がすべてのホスト モードでのサプリカント スイッチで機能できるようにもなります。
ステップ 11	**interface** *interface-id* 例：	設定するポートを指定し、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。

	コマンドまたはアクション	目的
	`Device(config)# interface gigabitethernet1/0/1`	
ステップ 12	**switchport trunk encapsulation dot1q** 例： `Device(config-if)# switchport trunk encapsulation dot1q`	ポートをトランク モードに設定します。
ステップ 13	**switchport mode trunk** 例： `Device(config-if)# switchport mode trunk`	インターフェイスを VLAN トランク ポートとして設定します。
ステップ 14	**dot1x pae supplicant** 例： `Device(config-if)# dot1x pae supplicant`	インターフェイスをポート アクセス エンティティ（PAE）サプリカントとして設定します。
ステップ 15	**dot1x credentials** *profile-name* 例： `Device(config-if)# dot1x credentials test`	802.1x クレデンシャルプロファイルをインターフェイスに対応付けます。
ステップ 16	**dot1x supplicant eap profile** *profile-name* 例： `Device(config-if)# dot1x supplicant eap profile cisp`	EAP-TLS プロファイルを 802.1X インターフェイスに割り当てます。
ステップ 17	**end** 例： `Device(config-if)# end`	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、特権 EXEC モードに戻ります。

設定の確認

Client Information Signaling Protocol（CISP）および Network Edge Access Topology（NEAT）の設定に関する情報を確認するには、次の show コマンドを使用します。

- show cisp interface <interface name>

- show cisp clients
- show cisp summary
- show cisp registrations

次に、**show cisp** コマンドの出力例を示します。GigabitEthernet 1/0/1 はオーセンティケータとして設定され、GigabitEthernet 1/0/2 はサプリカントとして設定されます。

```
Auth# show cisp interface Gi1/0/2

CISP Status for interface Gi1/0/2
 -------------------------------------
Version: 1
Mode: Supplicant Peer
Mode: Authenticator
Supp State: Idle

Auth# show cisp clients

Authenticator Client Table:
 ------------------------
 MAC Address VLAN Interface
 ---------------------------------
 0050.5695.4de8 1 Gi1/0/10
6c03.09e7.3947 1 Gi1/0/10
6c03.09e7.3954 11 Gi1/0/10
6c03.09e7.4485 1 Gi1/0/10
 9077.ee4a.8567 1 Gi1/0/10
e41f.7ba1.bbd4 1 Gi1/0/10

Supplicant Client Table:
------------------------
MAC Address VLAN Interface
---------------------------------
9077.ee4a.856b 11 Vl11
9077.ee4a.8572 1 Ap1/1
e41f.7bc7.2f03 1 Gi1/0/9

Auth# show cisp summary

CISP is running on the following interface(s):
---------------------------------------------
Gi1/0/2 (Authenticator)

Supp# show cisp summary

CISP is running on the following interface(s):
---------------------------------------------
Gi1/0/1 (Supplicant)

Auth# show cisp registrations

Interface(s) with CISP registered user(s):
-----------------------------------------
Gi1/0/2
Auth Mgr (Authenticator)

Supp# show cisp registration

Interface(s) with CISP registered user(s):
-----------------------------------------
```

```
Gi1/0/1
802.1x Sup (Supplicant)
```

CISP および NEAT をトラブルシューティングするには、次の debug コマンドを使用します。

- debug access-session errors
- debug access-session event
- debug dot1x errors
- debug dot1x packets
- debug dot1x events

機能の履歴

機能名	リリース	機能情報
Network Edge Access Topology（NEAT）	Cisco IOS XE 17.8.1	Cisco Catalyst IE9300 高耐久性シリーズ スイッチでの最初のサポート

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。