Network Edge Authentication Topology

The Network Edge Access Topology (NEAT) feature enables extended secure access in areas outside the wiring closet (such as conference rooms). This secure access allows any type of device to authenticate on the port.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Network Edge Authentication Topology

IEEE 802.1X—Port-Based Network Access Control

You should understand the concepts of port-based network access control and have an understanding of how to configure port-based network access control on your Cisco platform. For more information, see the *Configuring IEEE 802.1X Port-Based Authentication* module.

The switch must be connected to a Cisco secure ACS and RADIUS authentication, authorization, and accounting (AAA) must be configured for Web authentication. If appropriate, you must enable ACL download.

If the authentication order includes the 802.1X port authentication method, you must enable IEEE 802.1X authentication on the switch.

If the authentication order includes web authentication, configure a fallback profile that enables web authentication on the switch and the interface.

Note The web authentication method is not supported on Cisco integrated services routers (ISRs) or Integrated Services Routers Generation 2 (ISR G2s) in Cisco IOS Release 15.2(2)T.

RADIUS and ACLs

You should understand the concepts of the RADIUS protocol and have an understanding of how to create and apply access control lists (ACLs). For more information, see the documentation for your Cisco platform and the *Cisco IOS Security Configuration Guide: Securing User Services*.

The switch must have a RADIUS configuration and be connected to the Cisco secure access control server (ACS). For more information, see the *Configuration Guide for CISCO Secure ACS.*

Restrictions for Network Edge Authentication Topology

- NEAT is not supported on an EtherChannel port.
- It is recommended that NEAT is only deployed with auto-configuration.
- This feature does not support standard ACLs on the switch port.

Information About Network Edge Authentication Topology

Authenticator and Supplicant Switch with Network Edge Authentication Topology

The NEAT feature enables extended secure access in areas outside the wiring closet (such as conference rooms). NEAT allows you to configure a switch to act as a supplicant to another switch. Thus, with NEAT enabled, the desktop switch can become a supplicant switch and authenticate itself to the access switch.

- 802.1X supplicant switch: You can configure a switch to act as a supplicant to another switch by using the 802.1X supplicant feature. This configuration is helpful in a scenario where, for example, a switch is outside a wiring closet and is connected to an upstream switch through a trunk port. A switch configured with the 802.1X switch supplicant feature authenticates with the upstream switch for secure connectivity. Once the supplicant switch authenticates successfully the port mode changes from access to trunk.

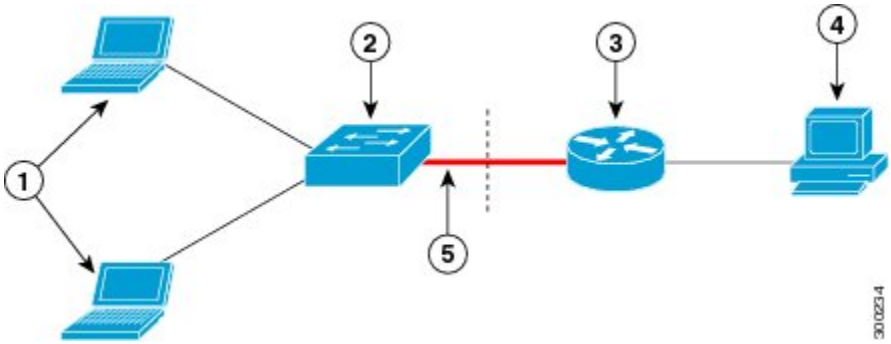
- If the access VLAN is configured on the authenticator, it becomes the native VLAN for the trunk port after successful authentication.

You can enable multidomain authentication (MDA) or multiple-authentication mode on the authenticator interface that connects to one or more supplicant switches. Multihost mode is not supported on the authenticator interface. Additional information about the authenticator can be found in the "IEEE 802.1X Authenticator" section of the "Configuring IEEE 802.1X Port-Based Authentication" chapter.

Use the **dot1x supplicant force-multicast** global configuration command on the supplicant switch for NEAT to work in all host modes.

- Host Authorization: Ensures that only traffic from authorized hosts (connecting to the switch with supplicant) is allowed on the network. The switches use Client Information Signalling Protocol (CISP) to send the MAC addresses connecting to the supplicant switch to the authenticator, as shown in the figure below.
- Auto enablement: Automatically enables trunk configuration on the authenticator switch, allowing user traffic from multiple VLANs coming from supplicant switches. Configure the Cisco Attribute-Value (AV) pair as device-traffic-class=switch at the ACS. (You can configure this under the group or the user settings.)

Figure 1: Authenticator and Supplicant Switch Using CISP



1	Workstations (clients)	2	Supplicant switch (outside wiring closet)
3	ISR G2 as an Authenticator	4	Access control server (ACS)
5	Trunk port		

Guidelines for Configuring Network Edge Access Topology

- You can configure NEAT ports with the same configurations as the other authentication ports. When the supplicant switch authenticates, the port mode is changed from access-based to trunk-based on the switch vendor-specific attributes (VSAs) (device-traffic-class=switch).
- The VSA changes the authenticator switch port mode from access to trunk and enables 802.1X trunk encapsulation and the access VLAN (if any) would be converted to a native trunk VLAN. VSA does not change any of the port configurations on the supplicant.

- To change the host mode and apply a standard port configuration on the authenticator switch port, you can also use Auto Smartports user-defined macros, instead of the switch VSA. This allows you to remove unsupported configurations on the authenticator switch port and to change the port mode from access to trunk. For information, see the *AutoSmartports Configuration Guide*.

Note NEAT does not support redundant links between authenticator and supplicant switches.

How to Configure Network Edge Authentication Topology

Configuring an Authenticator with Network Edge Authentication Topology

SUMMARY STEPS

1. **configure terminal**
2. **cisp enable**
3. **interface** *type slot/port*
4. **switchport mode access**
5. **authentication port-control auto**
6. **dot1x pae authenticator**
7. **end**
8. **show authentication interface** *interface-id*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**cisp enable** **Example:** `Switch(config)# cisp enable`	Enables CISP.
Step 3	**interface** *type slot/port* **Example:** `Switch(config)# interface gigabitethernet0/1`	Specifies the port to be configured, and enters interface configuration mode.

	Command or Action	Purpose
Step 4	**switchport mode access** **Example:** `Switch(config-if)# switchport mode access`	Sets the port mode to access.
Step 5	**authentication port-control auto** **Example:** `Switch(config-if)# authentication port-control auto`	Sets the port-authentication mode to auto.
Step 6	**dot1x pae authenticator** **Example:** `Switch(config-if)# dot1x pae authenticator`	Configures the interface as a port access entity (PAE) authenticator.
Step 7	**end** **Example:** `Switch(config-if)# end`	Returns to privileged EXEC mode.
Step 8	**show authentication interface** *interface-id* **Example:** `Switch# show authentication interface gigabitethernet0/1`	Verifies your entries.

Configuring a Supplicant Switch with Network Edge Authentication Topology

SUMMARY STEPS

1. **configure terminal**
2. **cisp enable**
3. **dot1x credentials** *profile*
4. **username** *name*
5. **password** *password*
6. **exit**
7. **dot1x supplicant force-multicast**
8. **interface** *type slot/port*
9. **switchport trunk encapsulation dot1q**
10. **switchport mode trunk**
11. **dot1x pae supplicant**
12. **dot1x credentials** *profile-name*
13. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**cisp enable** **Example:** `Switch(config)# cisp enable`	Enables CISP.
Step 3	**dot1x credentials** *profile* **Example:** `Switch(config)# dot1x credentials test`	Creates a 802.1X credential profile. This must be attached to the port that is configured as supplicant.
Step 4	**username** *name* **Example:** `Switch(config-dot1x-creden)# username suppswitch`	Creates a username.

	Command or Action	Purpose
Step 5	**password** *password* **Example:** `Switch(config-dot1x-creden)# password secret`	Creates a password for the new username.
Step 6	**exit** **Example:** `Switch(config-dot1x-creden)# exit`	Returns to global configuration mode.
Step 7	**dot1x supplicant force-multicast** **Example:** `Switch(config)# dot1x supplicant force-multicast`	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.
Step 8	**interface** *type slot/port* **Example:** `Switch(config)# interface gigabitethernet0/1`	Specifies the port to be configured, and enters interface configuration mode.
Step 9	**switchport trunk encapsulation dot1q** **Example:** `Switch(config-if)# switchport trunk encapsulation dot1q`	Sets the port to trunk mode.
Step 10	**switchport mode trunk** **Example:** `Switch(config-if)# switchport mode trunk`	Configures the interface as a VLAN trunk port.
Step 11	**dot1x pae supplicant** **Example:** `Switch(config-if)# dot1x pae supplicant`	Configures the interface as a port access entity (PAE) supplicant.
Step 12	**dot1x credentials** *profile-name* **Example:** `Switch(config-if)# dot1x credentials test`	Attaches the 802.1X credentials profile to the interface.

	Command or Action	Purpose
Step 13	**end** **Example:** `Switch(config-if)# end`	Returns to privileged EXEC mode.

Configuration Examples for Network Edge Authentication Topology

Example: Configuring an Authenticator with NEAT

The following example shows how to configure a switch as an 802.1X authenticator:

```
Switch# configure terminal
Switch(config)# cisp enable
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport mode access
Switch(config-if)# authentication port-control auto
Switch(config-if)# dot1x pae authenticator
```

Example: Configuring a Supplicant Switch with NEAT

This example shows how to configure a switch as a supplicant:

```
Switch# configure terminal
Switch(config)# cisp enable
Switch(config)# dot1x credentials test
Switch(config)# username suppswitch
Switch(config)# password myswitch
Switch(config)# dot1x supplicant force-multicast
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# dot1x pae supplicant
Switch(config-if)# dot1x credentials test
Switch(config-if)# end
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases

Related Topic	Document Title
IEEE 802.1X commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	• *Catalyst 4500 Series Switch Cisco IOS Command Reference, Release 12.2(25)SGA* • *Catalyst 3750 Switch Command Reference, Cisco IOS Release 12.2(25)SEE*

Standards and RFCs

Standard/RFC	Title
IEEE 802.1X	*Port Based Network Access Control*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Network Edge Authentication Topology

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for NEAT

Feature Name	Releases	Feature Information
NEAT (Network Edge Authentication Topology)	Cisco IOS 15.2(1)SY	The NEAT feature enables extended secure access in areas outside the wiring closet (such as conference rooms). This secure access allows any type of device to authenticate on the port.