IEEE 802.1X Multidomain Authentication

Multidomain authentication (MDA) allows both a data device and voice device, such as an IP phone (Cisco or non-Cisco), to authenticate on the same switch 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 IEEE 802.1X Multidomain Authentication

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 Access Control System (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 IEEE 802.1X Multidomain Authentication

- In multidomain authentication mode, only multicast EAPOL packets are accepted by the port.
- Inactivity aging is not supported on Cisco integrated services routers (ISRs) or Integrated Services Routers Generation 2 (ISR-G2s) in multidomain authentication mode.
- In multidomain authentication mode, the CDP 2nd port disconnect feature is supported.
- This feature does not support standard ACLs on the switch port.
- Configuring the same VLAN ID for both access and voice traffic (using the **switchport access vlan** *vlan-id* and the **switchport voice vlan** *vlan-id* commands) will fail if authentication has already been configured on the port.
- Configuring authentication on a port on which you have already configured **switchport access vlan** *vlan-id* and **switchport voice vlan** *vlan-id* will fail if the access VLAN and voice VLAN have been configured with the same VLAN ID.

Information About IEEE 802.1X Multidomain Authentication

Guidelines for Configuring IEEE 802.1X Multidomain Authentication

MDA allows both a data device and voice device, such as an IP phone (Cisco or non-Cisco), to authenticate on the same switch port. The port is divided into a data domain and a voice domain.

MDA does not enforce the order-of-device authentication. However, for best results, we recommend that a voice device is authenticated before a data device on an MDA-enabled port.

When you connect IP phones to a dot1x secured port, we recommend that you use MDA, instead of Cisco Discovery Protocol (CDP) bypass.

Note Any traffic destined to an unauthenticated client will be dropped. Traffic originating from an unauthenticated device will not be dropped.

Follow these guidelines for configuring MDA:

- To configure a switch port for MDA, see the "Configuring the Host Mode" section of the "Configuring IEEE 802.1X Port-Based Authentication" chapter.
- You must configure the voice VLAN for the IP phone when the host mode is set to multi-domain. For more information, see the "Configuring VLANS" chapter of the *Catalyst 3750 Switch Software Configuration Guide, Release 12.2(58)SE*.
- To authorize a voice device, the AAA server must be configured to send a Cisco Attribute-Value (AV) pair attribute with a value of device-traffic-class=voice. Without this value, the switch treats the voice device as a data device.
- The guest VLAN and restricted VLAN features only apply to the data devices on an MDA-enabled port. The switch treats a voice device that fails authorization as a data device.
- If more than one device attempts authorization on either the voice or the data domain of a port, it is error disabled.
- Non-Cisco IP phones or voice devices are allowed into both the data and voice VLANs. The data VLAN allows the voice device to contact a DHCP server to obtain an IP address and acquire the voice VLAN information. After the voice device starts sending on the voice VLAN, its access to the data VLAN is blocked.
- A voice device MAC address that is binding on the data VLAN is not counted towards the port security MAC address limit.
- MDA can use MAC authentication bypass as a fallback mechanism to allow the switch port to connect to devices that do not support 802.1X authentication.
- When a data or a voice device is detected on a port, its MAC address is blocked until authorization succeeds. If the authorization fails, the MAC address remains blocked for five minutes.
- If more than five devices are detected on the data VLAN or more than one voice device is detected on the voice VLAN while a port is unauthorized, the port is error disabled.
- When a port host mode changes from single- or multihost to multidomain mode, an authorized data device remains authorized on the port. However, a Cisco IP phone on the port voice VLAN is automatically removed and must be reauthenticated on that port.
- Active fallback mechanisms such as guest VLAN and restricted VLAN remain configured after a port changes from single-host or multihost mode to multidomain mode.
- Switching a port host mode from multidomain to single-host or multiple-hosts mode removes all authorized devices from the port.

- If a data domain is authorized first and placed in the guest VLAN, non-802.1X-capable voice devices need their packets tagged on the voice VLAN to trigger authentication. The phone need not need to send tagged traffic. (The same is true for an 802.1X-capable phone.)
- It is not recommended to use per-user ACLs with an MDA-enabled port. An authorized device with a per-user ACL policy might impact traffic on both the port voice and data VLANs. You can use only one device on the port to enforce per-user ACLs.

How to Configure IEEE 802.1X Multidomain Authentication

Configuring IEEE 802.1X Multidomain Authentication

SUMMARY STEPS

1. **configure terminal**
2. **radius-server vsa send authentication**
3. **interface** *type slot/port*
4. **access-session host-mode multi-domain**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**radius-server vsa send authentication** **Example:** `Switch(config)# radius-server vsa send authentication`	Configures the network access server to recognize and use vendor-specific attributes (VSAs).
Step 3	**interface** *type slot/port* **Example:** `Switch(config)# interface gigabitethernet0/1`	Specifies the port to which multiple hosts are indirectly attached, and enters interface configuration mode.

	Command or Action	Purpose
Step 4	**access-session host-mode multi-domain** **Example:** `Switch(config-if)# access-session host-mode multi-domain`	Allows both a host and a voice device, such as an IP phone (Cisco or non-Cisco), to be authenticated on an 802.1X-authorized port. **Note** You must configure the voice VLAN for the IP phone when the host mode is set to multi-domain. See the "Configuring Voice VLAN" chapter of the *Catalyst 3750 Switch Software Configuration Guide, Release 12.2(58)SE* for more information. Make sure that the **authentication port-control** interface configuration command is set to **auto** for the specified interface.
Step 5	**exit** **Example:** `Switch(config)# exit`	Returns to privileged EXEC mode.

Configuring Critical Voice VLAN Support in Multidomain Authentication Mode

Perform this task on a port to configure critical voice VLAN support in multidomain authentication (MDA) mode.

Note To configure MDA mode, see the "Configuring the Host Mode" section of the "Configuring IEEE 802.1X Port-Based Authentication" chapter.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot/port*
4. **authentication event server dead action authorize vlan** *vlan-id*
5. **authentication event server dead action authorize voice**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type slot/port* **Example:** `Switch(config)# interface gigabitethernet 0/1`	Specifies the port to be configured and enters interface configuration mode.
Step 4	**authentication event server dead action authorize vlan** *vlan-id* **Example:** `Switch(config-if)# authentication event server dead action authorize vlan 40`	Configures a critical data VLAN. **Note** This step is only required if the **authentication event server dead action authorize vlan** *vlan-id* command is not configured on the port.
Step 5	**authentication event server dead action authorize voice** **Example:** `Switch(config-if)# authentication event server dead action authorize voice`	Enables the Critical Voice VLAN feature, which puts phone traffic into the configured voice VLAN of a port if the authentication server becomes unreachable.

Configuration Examples for IEEE 802.1X Multidomain Authentication

Example: Configuring IEEE 802.1X Multidomain Authentication

The following example shows how to enable MDA and to allow both a host and a voice device on the port:

```
Device(config)interface GigabitEthernet0/0/0
Device(config-if)# switchport access vlan 110
Device(config-if)# switchport voice vlan 110
Device(config-if)# no ip address
Device(config-if)# authentication host-mode multi-domain
Device(config-if)# authentication port-control auto
Device(config-if)# mab
Device(config-if)# dot1x pae authenticator
Device(config-if)# end
```

Example: Critical Voice VLAN Support in Multidomain Authentication Mode

The following example shows how to enable the Critical Voice VLAN feature in MDA host-mode:

```
Switch(config) interface GigabitEthernet 0/0/0
Switch(config-if)# switchport access vlan 110
Switch(config-if)# switchport voice vlan 110
Switch(config-if)# no ip address
Switch(config-if)# authentication event server dead action authorize vlan 12
Switch(config-if)# authentication event server dead action authorize voice
Switch(config-if)# authentication host-mode multi-domain
Switch(config-if)# authentication port-control auto
Switch(config-if)# mab
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# end
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
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 IEEE 802.1X Multidomain Authentication

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 IEEE 802.1X Multidomain Authentication

Feature Name	Releases	Feature Information
IEEE 802.1X Multidomain Authentication	Cisco IOS 15.2(2)T	Multi-domain authentication (MDA) allows both a data device and voice device, such as an IP phone (Cisco or non-Cisco), to authenticate on the same switch port.