VLAN RADIUS Attributes in Access Requests

The VLAN RADIUS Attributes in Access Requests feature enhances the security for access switches with the use of VLAN RADIUS attributes (VLAN name and ID) in the access requests and with an extended VLAN name length of 128 characters.

This module describes how to create an attribute filter-list and how to bind an attribute filter-list with authentication and accounting requests.

- Finding Feature Information, page 1
- Restrictions for VLAN RADIUS Attributes in Access Requests, page 1
- Information About VLAN RADIUS Attributes in Access Requests, page 2
- How to Configure VLAN RADIUS Attributes in Access Requests, page 3
- Configuration Examples for VLAN RADIUS Attributes in Access Requests, page 6
- Additional References for VLAN RADIUS Attributes in Access Requests, page 6
- Feature Information for VLAN RADIUS Attributes in Access Requests, page 8

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.

Restrictions for VLAN RADIUS Attributes in Access Requests

- Dynamic VLAN assignment to critical authentication (inaccessible authentication bypass or AAA fail policy) VLAN is not supported.

- If the RADIUS server becomes unavailable during an 802.1x authentication exchange, the current exchange times out, and the switch uses critical access control lists (ACLs) during the next authentication attempt.
- In a scenario when the VLAN RADIUS Attributes in Access Requests feature is enabled on a Catalyst 4000 series switch, reloading the switch with an image that does not support the feature may lead to a crash. To recover the switch, erase the vlan.dat file by issuing the `erase cat4000_flash:` command. Once the vlan.dat file is erased, reboot the switch with the intended image.

Information About VLAN RADIUS Attributes in Access Requests

VLAN RADIUS attributes

Authentication prevents unauthorized devices (clients) from gaining access to the network by using different methods to define how users are authorized and authenticated for network access. To enhance security, you can limit network access for certain users by using VLAN assignment. Information available in the access-request packets sent to the authentication server (AAA or RADIUS server) validates the identity of the user and defines if a user can be allowed to access the network.

The VLAN RADIUS Attributes in Access Requests feature supports authentication using IEEE 802.1X, MAC authentication bypass (MAB), and web-based authentication (webauth). The default order for authentication methods is 802.1X, and then MAB, then web-based authentication. If required, you can change the order or disable any of these methods.

- If MAC authentication bypass is enabled, the network device relays the client's MAC address to the AAA server for authorization. If the client's MAC address is valid, the authorization succeeds and the network device grants the client access to the network.
- If web-based authentication is enabled, the network device sends an HTTP login page to the client. The network device relays the client's username and password to the AAA server for authorization. If the login succeeds, the network device grants the client access to the network.

While performing authentications, the VLAN RADIUS attributes (name and ID of the VLAN) assigned to the hosting port is included in the RADIUS access requests and accounting requests. The VLAN RADIUS Attributes in Access Requests feature supports VLAN names accommodating 128-character strings.

With the use of VLAN RADIUS attributes in authentication requests, clients are authorized based on existing VLAN segmented networks. The existing VLAN provisioning is used as an indication of the location.

Based on RFC 2868 (RADIUS Attributes for Tunnel Protocol Support), support is provided for standard RADIUS attributes that exist for specifying the tunnel-type, medium and identifier.

- Tunnel-Type (IEFT #64) = VLAN
- Tunnel-Medium-Type (IEFT #65) = 802 (6)
- Tunnel-Private-Group-ID (IEFT #81) = [tag, string]

Note The Tunnel-Private-Group-ID includes the VLAN ID or name and accommodates a string length of up to 253 characters.

How to Configure VLAN RADIUS Attributes in Access Requests

Configuring VLAN RADIUS Attributes in Access Requests

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **access-session attributes filter-list list** *list-name*
4. **vlan-id**
5. **exit**
6. **access-session accounting attributes filter-spec include list** *list-name*
7. **access-session authentication attributes filter-spec include list** *list-name*
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**access-session attributes filter-list list** *list-name* **Example:** `Device(config)# access-session attributes filter-list list mylist`	Adds access-session protocol data to accounting and authentication records and enters common filter list configuration mode. The **filter-list** keyword configures a sensor protocol filter list to accounting and authentication records.
Step 4	**vlan-id** **Example:** `Device(config-com-filter-list)# vlan-id`	Includes the VLAN ID for the attribute.

	Command or Action	Purpose
Step 5	**exit** **Example:** `Device(config-com-filter-list)# exit`	Exits common filter list configuration mode and returns to global configuration mode.
Step 6	**access-session accounting attributes filter-spec include list** *list-name* **Example:** `Device(config)# access-session accounting attributes filter-spec include list mylist`	Configures a sensor protocol filter specification, and binds an attribute filter list with accounting records.
Step 7	**access-session authentication attributes filter-spec include list** *list-name* **Example:** `Device(config)# access-session authentication attributes filter-spec include list mylist`	Configures a sensor protocol filter specification, and binds an attribute filter list with authentication records.

Step 8	**end**
	Example:
	`Device(config)# end`
		Exits global configuration mode and returns to privileged EXEC mode.

Verifying VLAN RADIUS Attributes in Access Requests

SUMMARY STEPS

1. **enable**
2. **debug radius**
3. **show authentication sessions interface**

DETAILED STEPS

Step 1 **enable**

Enables privileged EXEC mode.

- Enter your password if prompted.

Example:

```
Device> enable
```

Step 2 **debug radius**

Displays the RADIUS attributes.

Example:

```
Device# debug radius

19:01:33: RADIUS:  Tunnel-Private-Group[81]  5   01:"20"
19:01:33: RADIUS:  Tunnel-Type         [64]  6   01:VLAN     [13]
19:01:33: RADIUS:  Tunnel-Medium-Type  [65]  6   01:ALL_802  [6]
19:01:33: RADIUS:  Tunnel-Private-Group[81]  131
02:"aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa"
19:01:33: RADIUS:  Tunnel-Type         [64]  6   02:VLAN     [13]
19:01:33: RADIUS:  Tunnel-Medium-Type  [65]  6   02:ALL_802  [6]
19:01:33: RADIUS:  NAS-IP-Address      [4]   6   192.168.1.6
```

Step 3 **show authentication sessions interface**

Displays the detailed authentication session output for a specific interface.

Example:

```
Device# show authentication sessions interface GigabitEthernet3/0/2 details

            Interface:  GigabitEthernet3/0/2
          MAC Address:  xxxx.xxxx.xxxx
         IPv6 Address:  Unknown
         IPv4 Address:  192.0.2.1
            User-Name:  cisco1
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  multi-domain
     Oper control dir:  both
      Session timeout:  N/A
    Common Session ID:  CXXXXXX0000XXXXXXX
      Acct Session ID:  Unknown
               Handle:  0xDX0XXXX
       Current Policy:  POLICY_Gi3/0/2

Local Policies:
        Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
      Security Policy:  Should Secure
      Security Status:  Link Unsecure

Server Policies:
            SGT Value:  5


Method status list:
       Method           State
       dot1x            Authc Success

----------------------------------------
            Interface:  GigabitEthernet3/0/2
          MAC Address:  yyyy.yyyy.yyyy
         IPv6 Address:  Unknown
         IPv4 Address:  203.0.113.1
            User-Name:  cisco2
```

```
               Status:  Authorized
               Domain:  VOICE
       Oper host mode:  multi-domain
     Oper control dir:  both
      Session timeout:  N/A
    Common Session ID:  CXXXXXXX000
      Acct Session ID:  Unknown
               Handle:  0xDX0XXXX
       Current Policy:  POLICY_Gi3/0/2

Local Policies:
        Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
      Security Policy:  Should Secure

      Security Status:  Link Unsecure

Server Policies:
           Vlan Group:  Vlan: 11
            SGT Value:  5

Method status list:
       Method           State
       dot1x            Authc Success
```

Configuration Examples for VLAN RADIUS Attributes in Access Requests

Example: Configuring VLAN RADIUS Attributes in Access Requests

```
Device> enable
Device# configure terminal
Device(config)# access-session attributes filter-list list test-vlan-extension
Device(config-com-filter-list)# vlan-id
Device(config-com-filter-list)# exit
Device(config)# access-session accounting attributes filter-spec include list mylist
Device(config)# access-session authentication attributes filter-spec include list mylist
Device(config)# end
```

Additional References for VLAN RADIUS Attributes in Access Requests

Related Documents

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

Related Topic	Document Title
Security commands	• Cisco IOS Security Command Reference: Commands A to C • Cisco IOS Security Command Reference: Commands D to L • Cisco IOS Security Command Reference: Commands M to R • Cisco IOS Security Command Reference: Commands S to Z
802.1x Authentication with VLAN Assignment	"Configuring IEEE 802.1x Port-Based Authentication" chapter in *Catalyst 3750-X and 3560-X Switch Software Configuration Guide*
Configuring IEEE 802.1X authentication for access ports	"IEEE 802.1X VLAN Assignment" chapter in *802.1X Authentication Services Configuration Guide*

Standards and RFCs

Standard/RFC	Title
RFC 2868	*RADIUS Attributes for Tunnel Protocol Support*
RFC 2869	*RADIUS Extensions*
RFC 4675	*RADIUS Attributes for Virtual LAN and Priority Support*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for VLAN RADIUS Attributes in Access Requests

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 VLAN RADIUS Attributes in Access Requests

Feature Name	Releases	Feature Information
VLAN RADIUS Attributes in Access Requests	Cisco IOS XE 3.7E Cisco IOS XE Release 3.6E	The VLAN RADIUS Attributes in Access Requests feature enhances the security for access switches with the use of VLAN RADIUS attributes (VLAN name and ID) in the access requests and with an extended VLAN name length of 128 characters. In Cisco IOS XE Release 3.6E, this feature is supported on Cisco Catalyst 3850 Series Switches. The following commands were introduced or modified: **access-session attributes filter-list** *list*, **access-session accounting attributes filter-spec include** *list*, and **access-session authentication attributes filter-spec include** *list*.