Configuring VLAN RADIUS Attributes

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.

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.

Information About VLAN RADIUS Attributes in Access Requests

VLAN RADIUS Attributes

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.

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

To create an attribute filter-list and to bind an attribute filter-list with authentication and accounting requests, perform the following task:

Procedure

	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(config)# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
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	**configure terminal** **Example:** `Device(config-com-filter-list)# vlan-id`	Includes the VLAN ID for the attribute.
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 authentication attributes filter-spec include list mylist`	Configures a sensor protocol filter specification, and binds an attribute filter list with authentication records.
Step 7	**end** **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Verifying VLAN RADIUS Attributes in Access Requests

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**set platform software trace** *process slot module trace-level* **Example:** `Device# set platform software trace smd switch active R0 radius debug`	Sets the trace level to debug VLAN RADIUS.
Step 3	**end** **Example:** `Device# end`	Exits privileged exec mode.

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)# end
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
```

Example: Verifying VLAN RADIUS Attributes in Access Requests

The following is sample output from the **set platform software trace** command. The output provides debugging information used to verify VLAN RADIUS attributes in access requests.

```
Device# set platform software trace smd switch active R0 radius debug

2019/03/08 04:27:05.948 {smd_R0-0}{1}: [radius] [17946]: UUID: 0, ra: 0, TID: 0 (info):
RADIUS: Send Access-Request to 10.64.69.253:1812 id 1812/38, len 296
2019/03/08 04:27:05.948 {smd_R0-0}{1}: [radius] [17946]: UUID: 0, ra: 0, TID: 0 (info):
RADIUS:  authenticator 7b d2 a9 25 35 ba 1e 78 - 09 bb a8 83 02 11 b3 9d
2019/03/08 04:27:05.948 {smd_R0-0}{1}: [radius] [17946]: UUID: 0, ra: 0, TID: 0 (info):
RADIUS:  User-Name           [1]      6  "hack"
2019/03/08 04:27:05.948 {smd_R0-0}{1}: [radius] [17946]: UUID: 0, ra: 0, TID: 0 (debug):
RADIUS:  Service-Type        [6]      6  Framed                    [2]
2019/03/08 04:27:05.948 {smd_R0-0}{1}: [radius] [17946]: UUID: 0, ra: 0, TID: 0 (debug):
RADIUS:  Vendor, Cisco       [26]    27
2019/03/08 04:27:05.948 {smd_R0-0}{1}: [radius] [17946]: UUID: 0, ra: 0, TID: 0 (info):
RADIUS:   Cisco AVpair       [1]     21  "service-type=Framed"
2019/03/08 04:27:05.948 {smd_R0-0}{1}: [radius] [17946]: UUID: 0, ra: 0, TID: 0 (info):
RADIUS:  Framed-MTU          [12]     6  1468
2019/03/08 04:27:05.948 {smd_R0-0}{1}: [radius] [17946]: UUID: 0, ra: 0, TID: 0 (info):
RADIUS:  EAP-Message         [79]    11  ...
2019/03/08 04:27:05.948 {smd_R0-0}{1}: [radius] [17946]: UUID: 0, ra: 0, TID: 0 (debug):
RADIUS:  EAP-Message         [79]    11RADIUS:   02 01 00 09 01 68 61 63 6b             [
 hack]
2019/03/08 04:27:05.948 {smd_R0-0}{1}: [radius] [17946]: UUID: 0, ra: 0, TID: 0 (info):
RADIUS:  Message-Authenticator[80]    18  ...
2019/03/08 04:27:05.948 {smd_R0-0}{1}: [radius] [17946]: UUID: 0, ra: 0, TID: 0 (debug):
RADIUS:  Message-Authenticator[80]    18RADIUS:   ea c3 dd 57 ef c2 1d 4e 46 ca ea 24 ff
1d 01 aa             [ WNF$]
2019/03/08 04:27:05.948 {smd_R0-0}{1}: [radius] [17946]: UUID: 0, ra: 0, TID: 0 (info):
RADIUS:  EAP-Key-Name        [102]    2  *
2019/03/08 04:27:05.948 {smd_R0-0}{1}: [radius] [17946]: UUID: 0, ra: 0, TID: 0 (debug):
RADIUS:  EAP-Key-Name        [102]    2  *
2019/03/08 04:27:05.948 {smd_R0-0}{1}: [radius] [17946]: UUID: 0, ra: 0, TID: 0 (debug):
RADIUS:  Vendor, Cisco       [26]    49
2019/03/08 04:27:05.948 {smd_R0-0}{1}: [radius] [17946]: UUID: 0, ra: 0, TID: 0 (info):
RADIUS:   Cisco AVpair       [1]     43  "audit-session-id=09170C33000000145B8DFD4A"
2019/03/08 04:27:05.948 {smd_R0-0}{1}: [radius] [17946]: UUID: 0, ra: 0, TID: 0 (debug):
RADIUS:  Vendor, Cisco       [26]    20
```

```
2019/03/08 04:27:05.948 {smd_R0-0}{1}: [radius] [17946]: UUID: 0, ra: 0, TID: 0 (info):
RADIUS:   Cisco AVpair       [1]     14  "method=dot1x"
2019/03/08 04:27:05.949 {smd_R0-0}{1}: [radius] [17946]: UUID: 0, ra: 0, TID: 0 (debug):
RADIUS:  Vendor, Cisco       [26]    31
2019/03/08 04:27:05.949 {smd_R0-0}{1}: [radius] [17946]: UUID: 0, ra: 0, TID: 0 (info):
RADIUS:   Cisco AVpair       [1]     25  "client-iif-id=306305245"
2019/03/08 04:27:05.949 {smd_R0-0}{1}: [radius] [17946]: UUID: 0, ra: 0, TID: 0 (info): 01:
2019/03/08 04:27:05.949 {smd_R0-0}{1}: [radius] [17946]: UUID: 0, ra: 0, TID: 0 (info):
RADIUS:  Tunnel-Private-Group-Id[81]     6  "123"
2019/03/08 04:27:05.949 {smd_R0-0}{1}: [radius] [17946]: UUID: 0, ra: 0, TID: 0 (info): 01:
2019/03/08 04:27:05.949 {smd_R0-0}{1}: [radius] [17946]: UUID: 0, ra: 0, TID: 0 (info):
RADIUS:  Tunnel-Type         [64]     6  VLAN                  [13]
2019/03/08 04:27:05.949 {smd_R0-0}{1}: [radius] [17946]: UUID: 0, ra: 0, TID: 0 (info): 01:
2019/03/08 04:27:05.949 {smd_R0-0}{1}: [radius] [17946]: UUID: 0, ra: 0, TID: 0 (info):
RADIUS:  Tunnel-Medium-Type  [65]     6  ALL_802               [6]
2019/03/08 04:27:05.949 {smd_R0-0}{1}: [radius] [17946]: UUID: 0, ra: 0, TID: 0 (info): 02:
2019/03/08 04:27:05.949 {smd_R0-0}{1}: [radius] [17946]: UUID: 0, ra: 0, TID: 0 (info):
RADIUS:  Tunnel-Private-Group-Id[81]    11  "VLAN0123"
2019/03/08 04:27:05.949 {smd_R0-0}{1}: [radius] [17946]: UUID: 0, ra: 0, TID: 0 (info): 02:
2019/03/08 04:27:05.949 {smd_R0-0}{1}: [radius] [17946]: UUID: 0, ra: 0, TID: 0 (info):
RADIUS:  Tunnel-Type         [64]     6  VLAN                  [13]
2019/03/08 04:27:05.949 {smd_R0-0}{1}: [radius] [17946]: UUID: 0, ra: 0, TID: 0 (info): 02:
2019/03/08 04:27:05.949 {smd_R0-0}{1}: [radius] [17946]: UUID: 0, ra: 0, TID: 0 (info):
RADIUS:  Tunnel-Medium-Type  [65]     6  ALL_802               [6]
2019/03/08 04:27:05.949 {smd_R0-0}{1}: [radius] [17946]: UUID: 0, ra: 0, TID: 0 (info):
RADIUS:  NAS-IP-Address      [4]      6  9.23.12.51
2019/03/08 04:27:05.949 {smd_R0-0}{1}: [radius] [17946]: UUID: 0, ra: 0, TID: 0 (info):
RADIUS:  NAS-Port-Id         [87]    22  "GigabitEthernet1/0/6"
2019/03/08 04:27:05.949 {smd_R0-0}{1}: [radius] [17946]: UUID: 0, ra: 0, TID: 0 (info):
RADIUS:  NAS-Port-Type       [61]     6  Ethernet                [15]
2019/03/08 04:27:05.949 {smd_R0-0}{1}: [radius] [17946]: UUID: 0, ra: 0, TID: 0 (info):
RADIUS:  NAS-Port            [5]      6  50106
2019/03/08 04:27:05.949 {smd_R0-0}{1}: [radius] [17946]: UUID: 0, ra: 0, TID: 0 (info):
RADIUS:  Calling-Station-Id  [31]    19  "20-37-06-CF-B7-18"
2019/03/08 04:27:05.949 {smd_R0-0}{1}: [radius] [17946]: UUID: 0, ra: 0, TID: 0 (debug):
RADIUS(00000000): Sending a IPv4 Radius Packet
```

Feature History for VLAN RADIUS

This table provides release and related information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature	Feature Information
Cisco IOS XE 17.13.1	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.