RADIUS Realm

- RADIUS realms, on page 1
- Enable RADIUS realm, on page 2
- Configure realm to match the RADIUS server for authentication and accounting, on page 3
- Configure AAA policy for WLANs, on page 4
- Verify RADIUS-realm configuration, on page 6

RADIUS realms

A RADIUS realm is an AAA configuration element that

- enables assigning authentication and accounting requests to specific RADIUS servers based on user domain information
- uses the domain portion of a user's Network Access Identifier (NAI) to select the appropriate RADIUS server, and
- provides realm-based filtering and control for authentication and accounting requests within a WLAN.

Feature history

Table 1: Feature history for RADIUS realms

Feature name	Release information	Feature description
RADIUS realms	Cisco IOS XE 16.9.1	RADIUS realms are configuration elements in AAA (Authentication, Authorization, and Accounting) systems. They use the domain portion of a user's Network Access Identifier (NAI)—such as the part after "@" in an email address—to direct authentication and accounting requests to specific RADIUS servers. Realms help organizations manage user access and resource usage across different groups or domains.

When mobile clients connect to a WLAN, the RADIUS realm is included in the Extensible Authentication Protocol Method for UMTS Authentication and Key Agreement (EAP-AKA) identity response of the authentication request packet. For WLAN, the NAI format for EAP-AKA can be specified as

username@domain.com. In the NAI format, the realm follows the @ symbol and is specified as *example.com*. If the vendor-specific attribute "test" is added, the NAI format becomes *test@example.com*.

The RADIUS Realm feature can be enabled and disabled on a WLAN. If Realm is enabled on a WLAN, the corresponding user should send the username in the NAI format. The controller sends the authentication request to the AAA server only after it receives a realm in NAI format from the client and verifies that the realm complies with the required standards. Additionally, the controller sends accounting requests to the AAA server based on realm filtering.

Realm support on a WLAN

Each WLAN is configured to support NAI realms. Once the realm is enabled on a specific SSID, the system compares the received realms in the EAP identity response to those configured on the RADIUS server. If a username with the realm is not sent by the client, the WLAN uses the default RADIUS server for authentication. When the client's realm does not match the realms configured on the WLAN, the client is deauthenticated and dropped.

If the RADIUS Realm feature is not enabled on a WLAN, the controller uses the username received in the EAP identity request directly and authenticates the user using the configured RADIUS server. The RADIUS Realm feature is disabled on WLANs by default.

- **Realm match for authentication**: In dot1x with EAP methods (similar to EAP AKA), the username is received as part of an EAP identity response. A realm is derived from the username and is matched with the realms that are already configured in the corresponding RADIUS authentication server. If there is a match, the authentication requests are forwarded to the RADIUS server. If there is a mismatch, the client is deauthenticated.
- **Realm match for accounting**: After receiving a client's username through an access-accept message, the system derives the realm from the username when accounting messages are triggered. The realm is compared with the configured accounting realms on the RADIUS accounting server. When there is a match, the server receives the accounting requests. If there is no match, the system drops the accounting requests.

Enable RADIUS realm

Enable the RADIUS realm to allow the WLAN to use the RADIUS realm selection for AAA authentication.

Enabling the RADIUS realm is required when configuring wireless AAA policies that use RADIUS for authentication on your Cisco device.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Create a new AAA policy.**wireless aaa policy**

Example:

```
Device(config)# wireless aaa policy aaa-policy
```

Step 3 Enable AAA RADIUS realm selection.

Example:

```
Device(config-aaa-policy)# aaa-realm enable
```

Note
Use the **no aaa-realm enable** or the **default aaa-realm enable** command to disable the RADIUS realm.

The AAA RADIUS realm is now enabled and available for authentication purposes in the specified wireless AAA policy.

```
Device# configure terminal
Device(config)# wireless aaa policy policy-1
Device(config-aaa-policy)# aaa-realm enable
```

Configure realm to match the RADIUS server for authentication and accounting

Configure the realm to use your chosen RADIUS server group for authentication and accounting network access requests.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Create a AAA authentication model.

Example:

```
Device(config)# aaa new-model
```

Step 3 Set the authorization method.

Example:

```
Device(config)# aaa authorization network default group radius-server-group
```

Step 4 Indicate that 802.1x must use the realm group RADIUS server.

Example:

```
Device(config)# aaa authentication dot1x realm group radius-server-group
```

Step 5 Define the authentication method at login.

Example:

```
Device(config)# aaa authentication login realm group radius-server-group
```

Step 6 Enable accounting so the system sends a start record notice when a client is authorized and a stop record notice when the session ends.

Example:

```
Device(config)# aaa accounting identity realm start-stop group radius-server-group
```

Your device now uses the realm and RADIUS server group for authentication, authorization, and accounting.

```
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authorization network default group aaa_group_name
Device(config)# aaa authentication dot1x cisco.com group cisco1
Device(config)# aaa authentication login cisco.com group cisco1
Device(config)# aaa accounting identity cisco.com start-stop group v
```

Configure AAA policy for WLANs

Configure authentication, authorization, and accounting (AAA) policies to control and secure access for WLAN users.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Create a new AAA policy for wireless.

Example:

```
Device(config)# wireless aaa policy aaa-policy-name
```

Step 3 Enable AAA RADIUS server selection by realm.

Example:

```
Device(config-aaa-policy)# aaa-realm enable
```

Step 4 Return to global configuration mode.

Example:

```
Device(config-aaa-policy)# exit
```

Step 5 Configure a WLAN policy profile.

Example:

```
Device(config)# wireless profile policy wlan-policy-profile
```

Step 6 Map the AAA policy.**aaa-policy***aaa-policy*

Example:

```
Device(config-wireless-policy)# aaa-policy aaa-policy
```

Step 7 Set the accounting list.**accounting-list***acct-config-realm*

Example:

```
Device(config-wireless-policy)# accounting-list acct-config-realm
```

Step 8 Return to global configuration mode.

Example:

```
Device(config-wireless-policy)# exit
```

Step 9 Configure a WLAN.**wlan***wlan-namewlan-idssid*

Example:

```
Device(config)# wlan wlan-name wlan-id ssid
```

Step 10 Enable the security authentication list for IEEE 802.1x.

Example:

```
Device(config-wlan)# security dot1x authentication-list auth-list-realm
```

Step 11 Return to global configuration mode.

Example:

```
Device(config-wlan)# exit
```

Step 12 Configuresa policy tag.

Example:

```
Device(config)# wireless tag policy policy-name
```

Step 13 Map a policy profile to the WLAN.

Example:

```
Device(config-policy-tag)# wlan wlan-name policy policy-profile
```

Step 14 Return to global configuration mode.

Example:

```
Device(config-policy-tag)# exit
```

The AAA policy is successfully applied to the target WLAN, enabling centralized authentication and accounting for users connecting to that WLAN.

```
Device# configure terminal
Device(config)# wireless aaa policy aaa-policy-1
Device(config-aaa-policy)# aaa-realm enable
Device(config-aaa-policy)# exit
Device(config)# wireless profile policy wlan-policy-1
Device(config-wireless-policy)# aaa-policy aaa-policy-1
Device(config-wireless-policy)# accounting-list cisco.com
Device(config-wireless-policy)# exit
Device(config)# wlan wlan2 14 wlan-aaa
Device(config-wlan)# security dot1x authentication-list cisco.com
Device(config-wlan)# exit
Device(config)# wireless tag policy tag-policy-1
Device(config-policy-tag)# wlan Abc-wlan policy wlan-policy-a
Device(config-policy-tag)# exit
```

Verify RADIUS-realm configuration

Run this command to verify the RADIUS-realm configuration.

```
Device# show wireless client mac-address 14bd.61f3.6a24 detail
Client MAC Address : 14bd.61f3.6a24
Client IPv4 Address : 192.0.2.1
Client IPv6 Addresses : fe80::286e:9fe0:7fa6:8f4
Client Username : cisco-mac@cisco.com
AP MAC Address : 4c77.6d79.5a00
AP Name: AP4c77.6d53.20ec
AP slot : 1
Client State : Associated
Policy Profile : name-policy-profile
Flex Profile : N/A
Wireless LAN Id : 3
Wireless LAN Name: ha_realm_WLAN_WPA2_AES_DOT1X
BSSID : 4c77.6d79.5a0f
Connected For : 26 seconds
Protocol : 802.11ac
Channel : 44
Client IIF-ID : 0xa0000001
Association Id : 1
Authentication Algorithm : Open System
Client CCX version : No CCX support
Re-Authentication Timeout : 1800 sec (Remaining time: 1775 sec)
Input Policy Name  : None
Input Policy State : None
Input Policy Source : None
Output Policy Name  : None
Output Policy State : None
Output Policy Source : None
WMM Support : Enabled
U-APSD Support : Enabled
  U-APSD value : 0
  APSD ACs    : BK, BE, VI, VO
Fastlane Support : Disabled
Power Save : OFF
Supported Rates : 9.0,18.0,36.0,48.0,54.0
Mobility:
  Move Count                  : 0
  Mobility Role               : Local
  Mobility Roam Type          : None
  Mobility Complete Timestamp : 06/12/2018 19:52:35 IST
Policy Manager State: Run
NPU Fast Fast Notified : No
Last Policy Manager State : IP Learn Complete
Client Entry Create Time : 25 seconds
Policy Type : WPA2
Encryption Cipher : CCMP (AES)
Authentication Key Management : 802.1x
Encrypted Traffic Analytics : No
Management Frame Protection : No
Protected Management Frame - 802.11w : No
EAP Type : PEAP
VLAN : 113
Multicast VLAN : 0
Access VLAN : 113
Anchor VLAN : 0
WFD capable : No
Managed WFD capable : No
Cross Connection capable : No
```

```
Support Concurrent Operation : No
Session Manager:
  Interface        : capwap_9040000f
  IIF ID           : 0x9040000F
  Authorized       : TRUE
  Session timeout  : 1800
  Common Session ID: 097704090000000DF4607B3B
  Acct Session ID  : 0x00000fa2
  Aaa Server Details
  Server IP        : 192.0.2.2
  Auth Method Status List
       Method : Dot1x
              SM State         : AUTHENTICATED
              SM Bend State    : IDLE
  Local Policies:
       Service Template : wlan_svc_name-policy-profile_local (priority 254)
              Absolute-Timer   : 1800
              VLAN             : 113
  Server Policies:
  Resultant Policies:
              VLAN             : 113
              Absolute-Timer   : 1800
DNS Snooped IPv4 Addresses : None
DNS Snooped IPv6 Addresses : None
Client Capabilities
  CF Pollable : Not implemented
  CF Poll Request : Not implemented
  Short Preamble : Not implemented
  PBCC : Not implemented
  Channel Agility : Not implemented
  Listen Interval : 0
Fast BSS Transition Details :
  Reassociation Timeout : 0
11v BSS Transition : Not implemented
FlexConnect Data Switching : Central
FlexConnect Dhcp Status : Central
FlexConnect Authentication : Central
FlexConnect Central Association : No
.
.
.
Fabric status : Disabled
Client Scan Reports
Assisted Roaming Neighbor List
```