RADIUS Realm

Information About RADIUS Realm

The RADIUS Realm feature is associated with the domain of the user. Using this feature, a client can choose the RADIUS server through which authentication and accounting is to be processed.

When mobile clients are associated with a WLAN, RADIUS realm is received as a part of Extensible Authentication Protocol Method for UMTS Authentication and Key Agreement (EAP-AKA) identity response request in the authentication request packet. The Network Access Identifier (NAI) format (EAP-AKA) for WLAN can be specified as *username@domain.com*. The realm in the NAI format is represented after the @ symbol, which is specified as domain.com. If vendor-specific attributes are added as *test*, the NAI format is represented as test@domain.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 when the realm, which is in the NAI format and is received from the client, is compiled as per the given standards. Apart from authentication, accounting requests are also required to be sent to the AAA server based on realm filtering.

Realm Support on a WLAN

Each WLAN is configured to support NAI realms. After the realm is enabled on a particular SSID, the lookup is done to match the realms received in the EAP identity response against the configured realms on the RADIUS server. If the client does not send a username with the realm, the default RADIUS server that is configured on the WLAN is used for authentication. If the realm that is received from the client does not match the configured realms on the WLAN, the client is deauthenticated and dropped.

If the RADIUS Realm feature is not enabled on a WLAN, the username that is received as part of the EAP identity request is directly used as the username and the configured RADIUS server is used for authentication and accounting. By default, the RADIUS Realm feature is disabled on WLANs.

- **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 are 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**: A client's username is received through an access-accept message. When accounting messages are triggered, the realm is derived from the corresponding client's username and compared with the accounting realms configured on the RADIUS accounting server. If there is a match, accounting requests are forwarded to the RADIUS server. If there is a mismatch, accounting requests are dropped.

Enabling RADIUS Realm

Follow the procedure given below to enable RADIUS realm:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless aaa policy** *aaa-policy* **Example:** `Device(config)# wireless aaa policy policy-1`	Creates a new AAA policy.
Step 3	**aaa-realm enable** **Example:** `Device(config-aaa-policy)# aaa-realm enable`	Enables AAA RADIUS realm selection. **Note** Use the **no aaa-realm enable** or the **default aaa-realm enable** command to disable the RADIUS realm.

Configuring Realm to Match the RADIUS Server for Authentication and Accounting

Follow the procedure given below to configure the realm to match the RADIUS server for authentication and accounting:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Device# configure terminal`	
Step 2	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Creates a AAA authentication model.
Step 3	**aaa authorization network default group** *radius-server-group* **Example:** `Device(config)# aaa authorization network default group aaa_group_name`	Sets the authorization method.
Step 4	**aaa authentication dot1x** *realm* **group** *radius-server-group* **Example:** `Device(config)# aaa authentication dot1x cisco.com group cisco1`	Indicates that dot1x must use the realm group RADIUS server.
Step 5	**aaa authentication login** *realm* **group** *radius-server-group* **Example:** `Device(config)# aaa authentication login cisco.com group cisco1`	Defines the authentication method at login.
Step 6	**aaa accounting identity** *realm* **start-stop group** *radius-server-group* **Example:** `Device(config)# aaa accounting identity cisco.com start-stop group cisco1`	Enables accounting to send a start-record accounting notice when a client is authorized, and a stop-record at the end.

Configuring the AAA Policy for a WLAN

Follow the procedure given below to configure the AAA policy for a WLAN:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless aaa policy** *aaa-policy-name* **Example:** `Device(config)# wireless aaa policy aaa-policy-1`	Creates a new AAA policy for wireless.

	Command or Action	Purpose
Step 3	**aaa-realm enable** **Example:** `Device(config-aaa-policy)# aaa-realm enable`	Enables AAA RADIUS server selection by realm.
Step 4	**exit** **Example:** `Device(config-aaa-policy)# exit`	Returns to global configuration mode.
Step 5	**wireless profile policy** *wlan-policy-profile* **Example:** `Device(config)# wireless profile policy wlan-policy-a`	Configures a WLAN policy profile.
Step 6	**aaa-policy** *aaa-policy* **Example:** `Device(config-wireless-policy)# aaa-policy aaa-policy-1`	Maps the AAA policy.
Step 7	**accounting-list** *acct-config-realm* **Example:** `Device(config-wireless-policy)# accounting-list cisco.com`	Sets the accounting list.
Step 8	**exit** **Example:** `Device(config-wireless-policy)# exit`	Returns to global configuration mode.
Step 9	**wlan** *wlan-name wlan-id ssid* **Example:** `Device(config)# wlan wlan2 14 wlan-aaa`	Configures a WLAN.
Step 10	**security dot1x authentication-list** *auth-list-realm* **Example:** `Device(config-wlan)# security dot1x authentication-list cisco.com`	Enables the security authentication list for IEEE 802.1x.
Step 11	**exit** **Example:** `Device(config-wireless-policy)# exit`	Returns to global configuration mode.
Step 12	**wireless tag policy** *policy* **Example:** `Device(config)# wireless tag policy tag-policy-1`	Configures a policy tag.

	Command or Action	Purpose
Step 13	**wlan** *wlan-name* **policy** *policy-profile* **Example:** `Device(config-policy-tag)# wlan Abc-wlan policy wlan-policy-a`	Maps a policy profile to the WLAN.
Step 14	**exit** **Example:** `Device(config-policy-tag)# exit`	Returns to global configuration mode.

Verifying the RADIUS-Realm Configuration

Use the following 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 : 9.4.113.103
Client IPv6 Addresses : fe80::286e:9fe0:7fa6:8f4
Client Username : sacthoma@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        : 9.4.23.50
  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
```