Client Roaming Across Policy Profile

Information about Client Roaming Policy Profile

In Cisco Catalyst 9800 Series Wireless controller, each WLAN must be associated to a policy profile using a policy tag. Since the policy profile represent the policy defined by the administrator, the general rule is that the controller will not allow seamless roaming between same WLAN associated with different policy profile. The client will be disconnected hence disrupting seamless roaming and client will be required to join again and the new policy can be evaluated and implemented.

When you enable roaming across policy profile, if the two policy profiles differ only in the settings as listed, then client seamless roaming is allowed to same wlan associated to different policy profiles.

A typical use case is when clients roaming across two APs that belong to different policy tag and have WLAN associated with different policy profiles with different VLAN setting for each policy profile. If roaming across policy profile is enabled, the controller allows seamless roaming to another policy profile even if the VLAN is different and the client retains the original IP address. The controller applies all other attributes except VLAN from the new policy profile to which client has joined.

Client roaming across policy profiles is not allowed if there are different policy profile configurations. However; the following are the exceptions:

- Accounting list
- CTS
- DHCP-TLV-caching
- Dot11 5 Ghz airtime-fairness
- Dot11 24 Ghz airtime-fairness
- ET-analytics enable
- http-TLV-caching
- Idle-threshold
- Idle-timeout

- MDnS-SD service policy
- IPv4 ACL
- IPv6 ACL
- QBSS load
- RADIUS profiling
- Session timeout
- SIP CAC disassociation client
- SIP CAC send-486busy
- VLAN

You must execute the configuration in the global configuration mode. When a client roam across policy profile is attempted, the roam is either a success or a failure. However; the total roam across policy profiles counter under client global statistics section increments. But when the roam across policy profile is denied then roam across policy profile deny delete reason counter is incremented.

Note This feature is not supported on fabric and on Cisco 9800 FlexConnect.

The following is an example in which case a client roams across policy profiles PP1 and PP2 will be denied.

```
wireless profile policy PP1
vlan 42
no shutdown
wireless profile policy PP2
aaa-override
vlan 43
no shutdown
```

Configuring Client Roaming Across Policy Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enables configuration mode
Step 2	**wireless client vlan-persistent** **Example:** `Device(config) # wireless client vlan-persistent`	Enables client roaming across different policy profiles.
Step 3	**end** **Example:**	Ends the session.

	Command or Action	Purpose
	Device(config) # end	

Verifying Client Roaming Across Policy Profiles

The following shows the client roaming from policy profile PP1 configured with VLAN 42 to policy profile PP2 configured with VLAN 43.

The following is the sample output of the **show wireless client mac-address xxxx.xxxx.xxxx detail** command that shows the client is connected to policy profile PP1.

```
Device#show wireless client mac-address xxxx.xxxx.xxxx detail

Client MAC Address : xxxx.xxxx.xxxx
Client MAC Type : Universally Administered Address
Client IPv4 Address : 169.254.189.170
Client Username : cisco
AP MAC Address : xxxx.xxxx.xxxx
AP Name: vinks_ios
AP slot : 1
Client State : Associated
Policy Profile : PP1
Flex Profile : N/A
Wireless LAN Id: 3
WLAN Profile Name: prateekk_dot1x
Wireless LAN Network Name (SSID): prateekk_dot1x
BSSID : 0081.c4f6.6bfb
Connected For : 688 seconds
Protocol : 802.11ac
Channel : 161
Client IIF-ID : 0xa0000001
Association Id : 1
Authentication Algorithm : Open System
Idle state timeout : N/A
Re-Authentication Timeout : 1800 sec (Remaining time: 1112 sec)
Session Warning Time : Timer not running
Input Policy Name  : client-default
Input Policy State : Installed
Input Policy Source : QOS Internal Policy
Output Policy Name  : client-default
Output Policy State : Installed
Output Policy Source : QOS Internal Policy
WMM Support : Enabled
U-APSD Support : Enabled
  U-APSD value : 0
  APSD ACs    : BK, BE, VI, VO
Fastlane Support : Disabled
Client Active State : Active
Power Save : OFF
Current Rate : m8 ss1
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 : 07/13/2020 02:00:22 UTC
Client Join Time:
  Join Time Of Client : 07/13/2020 02:00:22 UTC
Client State Servers : None
```

```
Client ACLs : None
Policy Manager State: Run
Last Policy Manager State : IP Learn Complete
Client Entry Create Time : 688 seconds
Policy Type : WPA2
Encryption Cipher : CCMP (AES)
Authentication Key Management : 802.1x
User Defined (Private) Network : Disabled
User Defined (Private) Network Drop Unicast : Disabled
Encrypted Traffic Analytics : No
Protected Management Frame - 802.11w : No
EAP Type : EAP-FAST
VLAN Override after Webauth : No
VLAN : 42
Multicast VLAN : 0
WiFi Direct Capabilities:
  WiFi Direct Capable           : No
Central NAT : DISABLED
Session Manager:
  Point of Attachment : capwap_90400006
  IIF ID              : 0x90400006
  Authorized          : TRUE
  Session timeout     : 1800
  Common Session ID: 3C2A09090000000E45E6D59E
  Acct Session ID  : 0x00000000
  Last Tried Aaa Server Details:
   Server IP : 9.10.8.247
  Auth Method Status List
   Method : Dot1x
    SM State          : AUTHENTICATED
    SM Bend State     : IDLE
  Local Policies:
   Service Template : wlan_svc_PP1_local (priority 254)
    VLAN              : 42
    Absolute-Timer    : 1800
  Server Policies:
  Resultant Policies:
    VLAN Name         : VLAN0042
    VLAN              : 42
    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
11v DMS Capable : No
QoS Map Capable : No
FlexConnect Data Switching : N/A
FlexConnect Dhcp Status : N/A
FlexConnect Authentication : N/A
FlexConnect Central Association : N/A
Client Statistics:
  Number of Bytes Received from Client : 19442
  Number of Bytes Sent to Client : 3863
  Number of Packets Received from Client : 197
  Number of Packets Sent to Client : 36
  Number of Policy Errors : 0
```

```
  Radio Signal Strength Indicator : -39 dBm
  Signal to Noise Ratio : 55 dB
Fabric status : Disabled
Radio Measurement Enabled Capabilities
  Capabilities: None
Client Scan Report Time : Timer not running
Client Scan Reports
Assisted Roaming Neighbor List
Nearby AP Statistics:
EoGRE : Pending Classification
Device Type      : Apple-Device
Device Name      : APPLE, INC.
Protocol Map     : 0x000001  (OUI)
Max Client Protocol Capability: 802.11ac Wave 2
Cellular Capability : N/A
Apple Specific Requests(ASR) Capabilities/Statistics Summary
  Regular ASR support: : DISABLED
```

The following is the sample output of the **show wireless client mac-address xxxx.xxxx.xxxx detail** command after client has roamed to a policy profile PP2.

```
Client MAC Address : xxxx.xxxx.xxxx
Client MAC Type : Universally Administered Address
Client IPv4 Address : 9.9.42.236
Client Username : cisco
AP MAC Address : xxxx.xxxx.xxxx
AP Name: prateekk_cos_1
AP slot : 1
Client State : Associated
Policy Profile : PP2
Flex Profile : N/A
Wireless LAN Id: 3
WLAN Profile Name: prateekk_dot1x
Wireless LAN Network Name (SSID): prateekk_dot1x
BSSID : a0f8.4985.0029
Connected For : 11 seconds
Protocol : 802.11ac
Channel : 36
Client IIF-ID : 0xa0000001
Association Id : 1
Authentication Algorithm : Open System
Idle state timeout : N/A
Re-Authentication Timeout : 1800 sec (Remaining time: 1789 sec)
Session Warning Time : Timer not running
Input Policy Name  : client-default
Input Policy State : Installed
Input Policy Source : QOS Internal Policy
Output Policy Name  : client-default
Output Policy State : Installed
Output Policy Source : QOS Internal Policy
WMM Support : Enabled
U-APSD Support : Enabled
  U-APSD value : 0
  APSD ACs    : BK, BE, VI, VO
Fastlane Support : Disabled
Client Active State : Active
Power Save : OFF
Current Rate : m9 ss3
Supported Rates : 9.0,18.0,36.0,48.0,54.0
Mobility:
  Move Count                  : 0
  Mobility Role               : Local
  Mobility Roam Type          : L2
  Mobility Complete Timestamp : 07/13/2020 02:12:19 UTC
```

```
Client Join Time:
  Join Time Of Client : 07/13/2020 02:12:19 UTC
Client State Servers : None
Client ACLs : None
Policy Manager State: Run
Last Policy Manager State : IP Learn Complete
Client Entry Create Time : 728 seconds
Policy Type : WPA2
Encryption Cipher : CCMP (AES)
Authentication Key Management : 802.1x
User Defined (Private) Network : Disabled
User Defined (Private) Network Drop Unicast : Disabled
Encrypted Traffic Analytics : No
Protected Management Frame - 802.11w : No
EAP Type : EAP-FAST
VLAN Override after Webauth : No
VLAN : 43
Multicast VLAN : 0
WiFi Direct Capabilities:
  WiFi Direct Capable           : No
Central NAT : DISABLED
Session Manager:
  Point of Attachment : capwap_90000005
  IIF ID              : 0x90000005
  Authorized          : TRUE
  Session timeout     : 1800
  Common Session ID: 3C2A09090000000E45E6D59E
  Acct Session ID  : 0x00000000
  Last Tried Aaa Server Details:
   Server IP : 9.10.8.247
  Auth Method Status List
   Method : Dot1x
    SM State          : AUTHENTICATED
    SM Bend State     : IDLE
  Local Policies:
   Service Template : vlan-42-template (priority 200)
    VLAN              : 42
   Service Template : wlan_svc_PP2_local (priority 254)
    Absolute-Timer    : 1800
  Server Policies:
  Resultant Policies:
    VLAN Name         : VLAN0042
    VLAN              : 42
    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
11v DMS Capable : No
QoS Map Capable : No
FlexConnect Data Switching : N/A
FlexConnect Dhcp Status : N/A
FlexConnect Authentication : N/A
FlexConnect Central Association : N/A
Client Statistics:
  Number of Bytes Received from Client : 23551
```

```
  Number of Bytes Sent to Client : 12588
  Number of Packets Received from Client : 239
  Number of Packets Sent to Client : 71
  Number of Policy Errors : 0
  Radio Signal Strength Indicator : -28 dBm
  Signal to Noise Ratio : 60 dB
Fabric status : Disabled
Radio Measurement Enabled Capabilities
  Capabilities: None
Client Scan Report Time : Timer not running
Client Scan Reports
Assisted Roaming Neighbor List
Nearby AP Statistics:
  prateekk_cos_1 (slot 1)
   antenna 0: 13 s ago ........ -25  dBm
   antenna 1: 13 s ago ........ -25  dBm
EoGRE : No/Simple client
Device Type      : Apple-Device
Device Name      : APPLE, INC.
Protocol Map     : 0x000001  (OUI)
Protocol         : DHCP
Type             : 0    0
Data             : 00

Max Client Protocol Capability: 802.11ac Wave 2
Cellular Capability : N/A
Apple Specific Requests(ASR) Capabilities/Statistics Summary
  Regular ASR support: : DISABLED
```

The following is the sample output of the **show wireless stats client detail** command that displays that client roam across policy profile is attempted and roam across policy is not denied.

```
Device #show wireless stats client detail | in Roam
Total Roam Across Policy Profiles : 1
Roam across policy profile deny : 0
```