EoGRE Deployment Guide for Cisco Catalyst 9800 Series Wireless Controllers, Cisco IOS XE Amsterdam 17.1

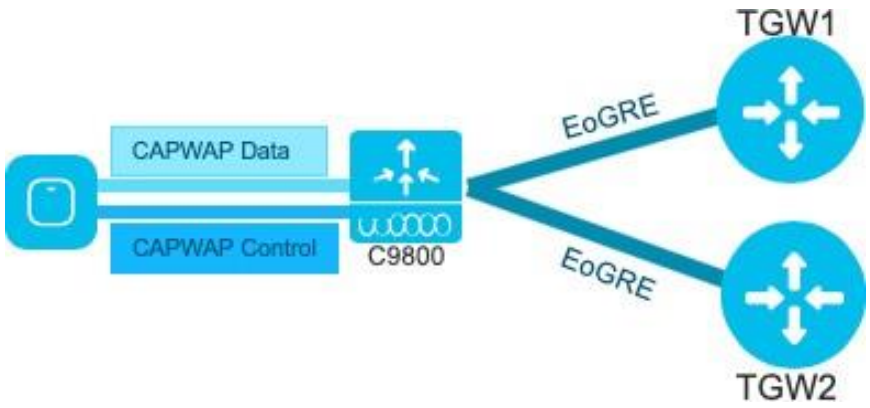
First Published: March 12, 2020

Table of Contents

EoGRE Tunneling Overview

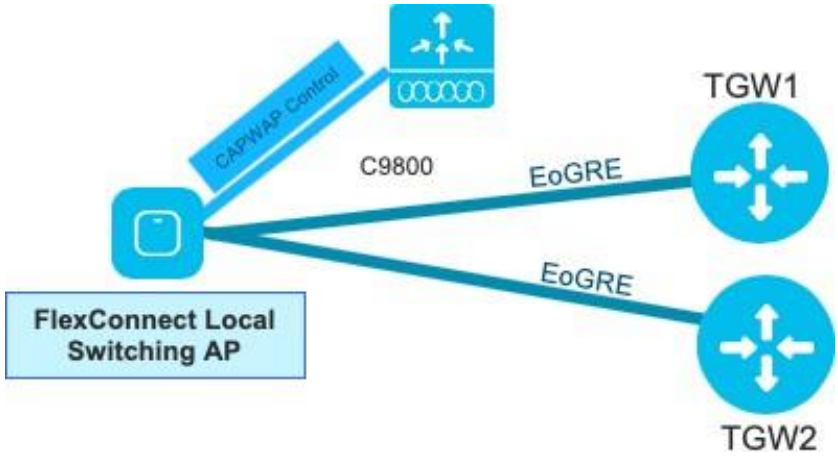
Ethernet over GRE (EoGRE) is a new aggregation solution for aggregating Wi-Fi traffic from hotspots. This solution enables customer premises equipment (CPE) devices to bridge the Ethernet traffic coming from an end host, and encapsulate the traffic in Ethernet packets over an IP GRE tunnel. When the IP GRE tunnels are terminated on a service provider broadband network gateway, the end host's traffic is terminated and subscriber sessions are initiated for the end host.

C9800 EoGRE Tunnel in Local Mode



- CAPWAP Control (AP-WLC) - encrypted
- CAPWAP Data (AP-WLC) – optional as encrypted
- EoGRE Data (C9800-TGW)-not encrypted

C9800 EoGRE Tunnel in FlexConnect Mode



- CAPWAP Control (Flex AP-C9800)
- EoGRE Data (Flex AP-TGW)
- Once tunnel is established – data flows from FC AP directly to the TGW

Benefits of EoGRE Tunneling

- Client can maintain IP address and policy across heterogeneous access networks with different technologies and/or vendors.
- Bypass MAC address scaling limitation of the L2 switch connecting to the WLC.

The EoGRE Tunneling offers the following benefits for mobile operators:

- Reduces network congestion by reducing OpEx and increasing network efficiency by offloading 3G and 4G traffic.
- Provides access to 3G and 4G core in spite of a lack of weak cell signal, leading to subscriber retention.
- Lowers CapEx on per user basis or bandwidth basis in dense metro environments.

The EoGRE tunneling offers the following benefits for wireline and Wi-Fi operators:

- Provides Wi-Fi security and subscriber control.
- Delivers scalable, manageable, and secure wireless connectivity.
- Enables new revenue-sharing business models.
- Delivers a Wi-Fi platform that offers new location-based services.

The EoGRE tunneling offers the following benefits for subscribers:

- Provides enhanced quality of experience to subscribers on Wi-Fi networks.
- Provides unified billing across access networks.
- Provides mobility across radio access technologies—3G or 4G to Wi-Fi and Wi-Fi to Wi-Fi.
- Provides multiple options within the Wi-Fi platform, thereby enabling location-based services.
- EoGRE Tunnels support IPv4 and IPv6 in Local and Flex Connect Modes
- EoGRE supports primary and secondary TGWs Failover and Redundancy
- Support EoGRE tunnels for 802.1x and open WLANs
- Support IPv4 and IPv6 wireless clients
- Support DHCP option 82 insertion on EOGRE Tunnel
- Support AAA override for EoGRE users
- Support for Tunnel Gateway as Radius-proxy
- Support up to 10 Tunnel Gateways
- Support Accounting ad-interim updates

- Support definition of EoGRE Domains
- Support per-realm filters to choose target domain per user
- Support VLAN tagging in per-realm filters
- Support VLAN override per WLAN
- Support for Wave-1 and Wave-2 APs
- Enhanced number (4094) of EoGRE VLANs support
- AAA-proxy Gateway configuration enhancement

Platform Support

Catalyst wireless platforms 9800-40, 9800-80, 9800-CL and C9800-L

11ac Wave 1 and Wave 2 Access Points: AP18xx, 2802, 3802, 4800, 1540, 1560, 1700, 2700, 3700, 1570

All WiFi6 or Catalyst 9100 series Access Points.

Supported releases IOS-XE -17.1 in CLI and WebUI modes.

EoGRE Tunnel Design Options

C9800 Controller EoGRE Tunnel configuration

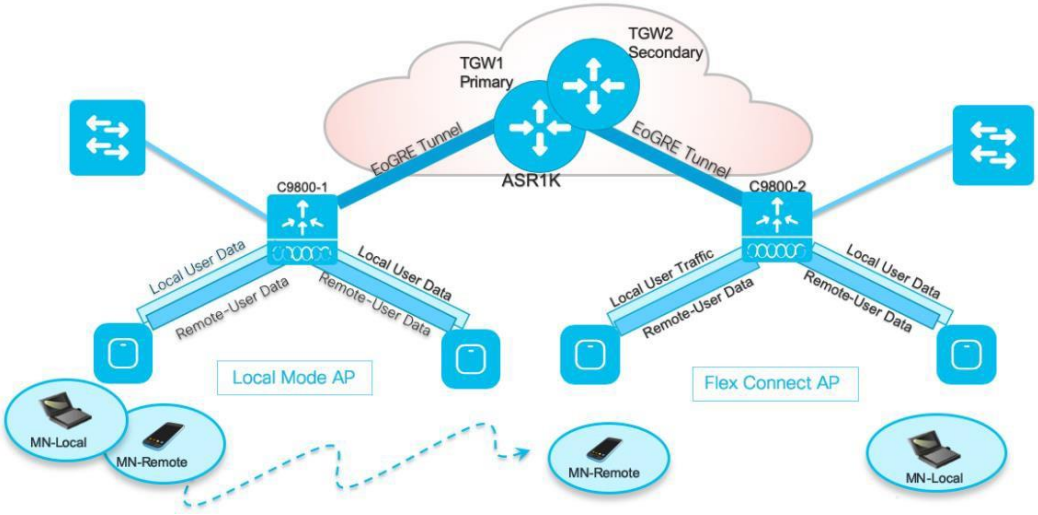
- CAPWAP Control Path (AP-WLC)
- CAPWAP Data Path (AP-WLC)
- EoGRE Data Flow (WLC-TGW)

In this design model, a tunnel gets generated from WLC to the tunnel gateway such as ASR 1000. Begin with IOS-XE release 16.12, controllers support up to10 tunnel Gateway configurations and 10 EoGRE Tunnel Domains. Each configured Tunnel profile is applied per Domain. Each profile can also be configured with a realm. When realms are configured, it will be a username followed by "@". Realm is a string after @, for example, in user_name@cisco.com the realm is "cisco.com". Two or more tunnels can be configured for redundancy, so that when the primary or active tunnel fails, the secondary or standby tunnel will take over the operation of the EoGRE tunnel. Intra-controller and Inter-controller mobility are also supported with the EoGRE tunnel configuration.

Tunnels can be configured to be part of a single VLAN- only single VLAN tag supported in the Ethernet frame.

- Tunnel Domains are redundancy grouping of tunnels. Configuration specifies a primary and a secondary tunnel, together with redundancy model.
- Tunnel Rules are in charge of realm filtering, each client has a realm assigned in its username for instance, for username mike@cisco.com, hence "cisco.com" is the realm.
- Rules allow user to define what domain to use for each realm. Also, they allow to define the VLAN tagging for client traffic going toward that TGW.

- Filters cannot have wildcards (*) in the realm configuration to catch all.



Only one type of tunnel is supported per WLAN. EoGRE is supported on either Open or 802.1x based WLANs. Other authentication modes including PSK are not supported in the present release by the tunneled clients.

When open SSID WLAN is used, either all local/simple or all tunneled clients are supported but cannot be mixed on the same WLAN. However, 802.1x authenticated simple or tunneled EoGRE clients are supported on the same WLAN.

It is now possible to assign EoGRE Tunnel Profiles to WLANs based on authentication if configured with AAA override; clients will be separated into local or tunneled mode. The WLC supports two types of user's traffic such as:

- Remote-Tunneled and Local on the same WLAN.
- Local users' traffic is defined as traffic that is locally bridged by the Controller. Remote-Tunneled user traffic is defined as traffic of remote-tunnel users and is tunneled by the Controller to a TGW. AAA override for EoGRE users is supported. Tunnel gateway can also act as Authentication/Authorization and/or Accounting proxy. AAA-proxy option allows for forwarding AAA requests to tunnel gateways

If AAA Override is enabled on the controller for EoGRE 802.1x authenticated clients:

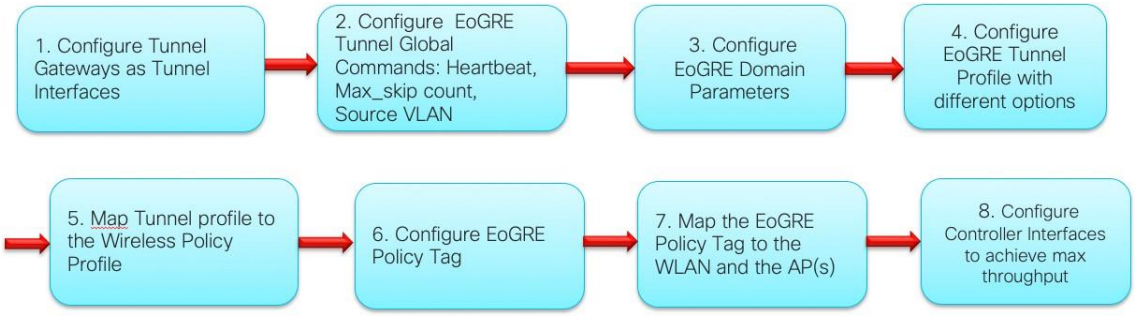
- AAA override is enabled, the above rule-filtering is overridden by AAA reply for a given client. Radius server will provide in its reply what Domain and what VLAN to use for the client
- Controller parses Access Accept and looks for MPC-Protocol-Type, such as EoGRE
- If the Protocol-Type AV Pair exists, Controller looks for all parameters related to that tunnel-type. The static profile is ignored and the AAA provided parameters are used to setup tunnel.
- If AVP is not present, Controller uses static profile on WLC to determine tunnel type based on the realm extracted from username.
- If some of the parameters are not present, the authentication fails. For example, if everything is present except T-GW IP, then the client authentication fails.
- If the MPC-Protocol-Type is None, then it will be simple IP.

Some of the attributes that can be returned by the AAA server are:

- User-Name
- Calling-Station-Id
- gw-domain-name
- mn-service
- cisco-mpc-protocol-interface
- eogre_vlan_id
- Primary or Secondary TGW

Configuring EoGRE Tunneling

Below are EoGRE Tunnel configuration steps on the C9800 controller



Note: In release IOS-XE 17.1 CLI and WebUI configuration options are available.

Step 1: On the C9800 EoGRE Tunnel Global Interface configure EoGRE Tunnel “heartbeat interval”, “heartbeat max-skip- Heartbeats (simple ping packets) are the way tunnel connectivity is checked. The heartbeat timeout (interval between heartbeats)

The max-skip-count (maximum number of heartbeats that can be dropped before declaring a tunnel down and perform failover)

```
Cat9800(config)#tunnel eogre heartbeat interval ?
<60-600> heartbeat interval (seconds)

Cat9800(config)#tunnel eogre heartbeat max-skip-count?
<3-10> Tolerable dropped heartbeats count” and Source VLAN

C9800(config)#tunnel eogre source vlan?
<1-4094> Vlan interface number
```

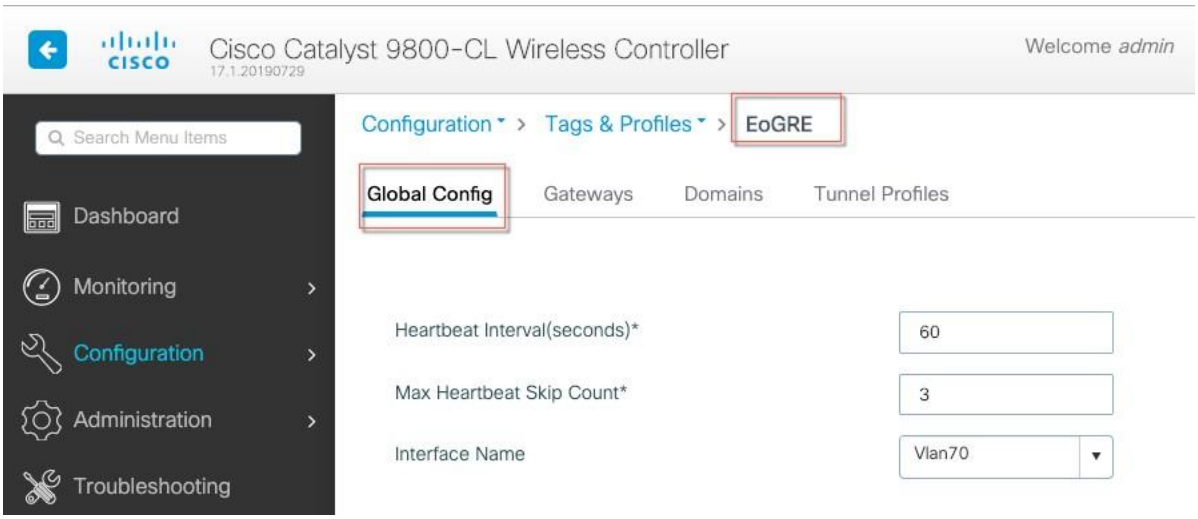
Note: Global Source interface can be overridden by specific per-tunnel source interface The client VLAN will be resolved in this order:

The one returned in AAA if there is an aaa-override and an eogre vlan parameter in AAA data. The one configured in tunnel profile

The one configured in rules

```
Vlan < wireless management interf>
```

Same configuration done from the WebUI



Verify the heartbeat configuration with the show command as shown in the example below:

```
spwifi-ewlc-11#sh tunnel eogre global-configuration
Heartbeat interval          : 60
Max Heartbeat skip count    : 3
Source Interface            : Vlan11
```

Verify the configured tunnel details with the following show command as shown in the example below:

```
spwifi-ewlc-11#sh tunnel eogre gateway det
spwifi-ewlc-11#sh tunnel eogre gateway detailed
Gateway : Tunnel1
 Mode    : IPv4
 IP      : 179.0.0.50
 Source  : Vlan11 / 180.11.0.11
 State   : Up
 SLA ID  : 17
 MTU     : 1480
 Up Time: 2 days 12 hours 58 minutes 35 seconds

 Clients
  Total Number of Wireless Clients      : 501
 Traffic
  Total Number of Received Packets      : 10342557
  Total Number of Received Bytes        : 1858775842
  Total Number of Transmitted Packets   : 10390636
  Total Number of Transmitted Bytes     : 1684960382
 Keepalives
  Total Number of Lost Keepalives       : 0
  Total Number of Received Keepalives   : 3659
  Total Number of Transmitted Keepalives: 3660
  Windows                               : 1219
  Transmitted Keepalives in last window : 3
  Received Keepalives in last window    : 3

Event history
Timestamp               #Times   Event               RC Context
----------------------- -------- ------------------- -- ----------------------------------------
03/06/2019 16:15:05.135 21879    UPDATE               0 stats update
03/06/2019 16:14:30.838 3659     SLA_RX               0 rx:3 in window:1219
03/06/2019 16:14:30.836 3660     SLA_TX               0 tx:3 in window:1219
03/06/2019 15:57:11.758 84       CLIENT_COUNT_UPD     0 501 local clients
03/02/2019 02:40:28.660 1        ADD_TO_DOMAIN        0 primary GW in:dom1
03/02/2019 02:40:14.397 1        HA_RECOVER           0 Status:Up,Admin-Status:Up,SrcAddrChanged
                                                        ,SrcIntfChanged
03/02/2019 02:39:21.140 2        SLA_RESET            0 dst, Window:0
03/02/2019 02:39:21.138 1        CREATE               0
```

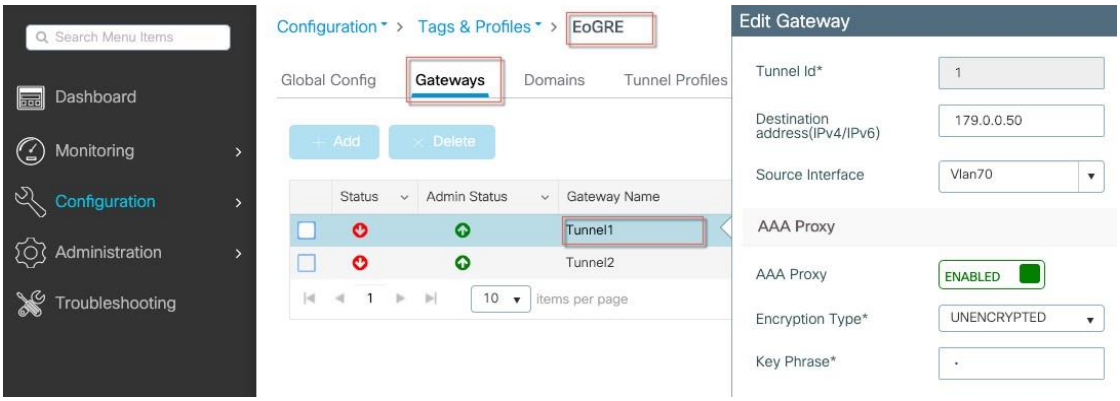
Step 2: Configure Tunnel Gateways as Tunnel Interfaces

```
interface Tunnel1
tunnel eogre source Vlan70 no ip address
```

```
tunnel source Vlan70
tunnel mode ethernet gre ipv4 p2p tunnel destination 179.0.0.50
!

interface Tunnel2 no ip address
tunnel source Vlan70
tunnel mode ethernet gre ipv4 p2p tunnel destination 179.0.0.54
```

Same configuration from the WebUI



Step 2a: AAA-proxy related Gateway specific configuration, see WebUI configuration in the screen shot example above.

When Tunnel Gateway is behaving as AAA proxy server, the only piece of configuration needed is the server key:

```
tunnel eogre interface Tunnel <tunnel_id> aaa proxy key 0 <key>
```

Note: No other piece of AAA config is needed, and this simplifies configuration of the overall EoGRE features in the IOS-XE deployments.

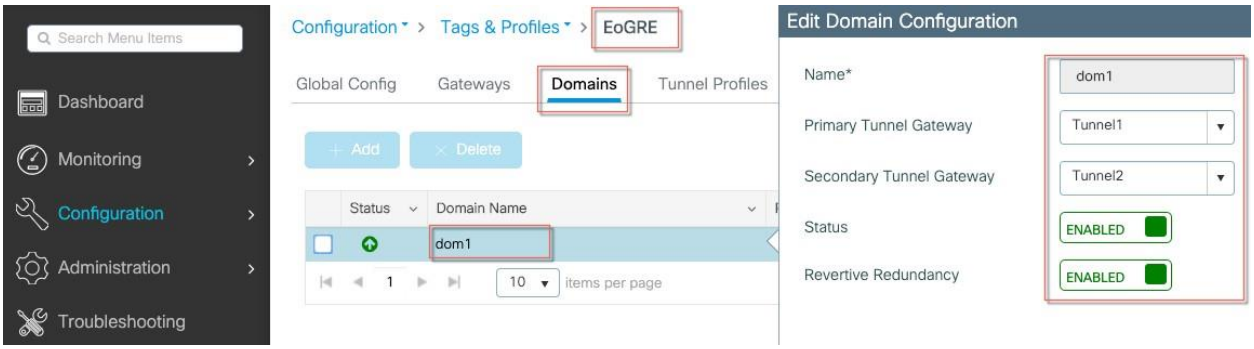
After tunnel configuration is done verify with the show command:

```
spwifi-ewlc-11#sh tunnel eogre gateway summary
Name              Type  Address                                   AdminState  State  Clients
-------------------------------------------------------------------------------------------
Tunnel1           IPv4  179.0.0.50                                Up          Up     501
Tunnel2           IPv4  179.0.0.54                                Up          Up     0
Tunnel3           IPv4  179.0.0.58                                Up          Up     500
Tunnel4           IPv4  179.0.0.62                                Up          Up     0
Tunnel5           IPv4  179.0.0.66                                Up          Up     500
Tunnel6           IPv4  179.0.0.70                                Up          Up     0
Tunnel7           IPv4  179.0.0.74                                Up          Up     501
Tunnel8           IPv4  179.0.0.78                                Up          Up     0
```

Step 3: On the C9800 EoGRE Tunnel Global Interface configure domain Ex: tunnel eogre domain dom1

```
primary Tunnel1 secondary Tunnel2
redundancy revertive (If primary is UP, primary will be the active GW, no matter the state of
secondary)
Cat9800(config)#tunnel eogre domain dom1 Cat9800(config-eogre-domain)# Cat9800(config-eogre-domain)#?
default     Set a command to its defaults
exit        Exit sub-mode
no          Negate a command or set its defaults
primary     primary gateway
redundancy  redundancy model
secondary   secondary gateway
shutdown    Disable the tunnel profile
```

Same configuration done from the WebUI



Verify the configured tunnel details with the following show command as shown in the example below:

```
spwifi-ewlc-11#sh tunnel eogre domain summary
Domain Name          Primary GW    Secondary GW          Active GW      Redundancy       AdminState
-------------------------------------------------------------------------------------------------
dom1                 Tunnel1       Tunnel2               Tunnel1        Revertive        Up
dom2                 Tunnel3       Tunnel4               Tunnel3        Revertive        Up
dom3                 Tunnel5       Tunnel6               Tunnel5        Revertive        Up
dom4                 Tunnel7       Tunnel8               Tunnel7        Revertive        Up
```

Step 4: On the C9800 EoGRE Tunnel Global Interface configure EoGRE Profile with DHCP options, Rules and Realm filters.

```
Cat9800(config)#wireless profile tunnel eogre-sp-basic Cat9800(config-tunnel-profile)#?
aaa-override                    AAA Policy Override
default                         Set a command to its defaults
dhcp-opt82                      Configure DHCP Option 82 for tunneled clients
exit                            Exit sub-mode
gateway-accounting-radius-proxy Gateway Accounting Radius Proxy gateway-radius-proxy Gateway Radius
Proxy
no                              Negate a command or set its defaults
rule                            Rule to choose domain
shutdown                        Disable tunnel profile
```

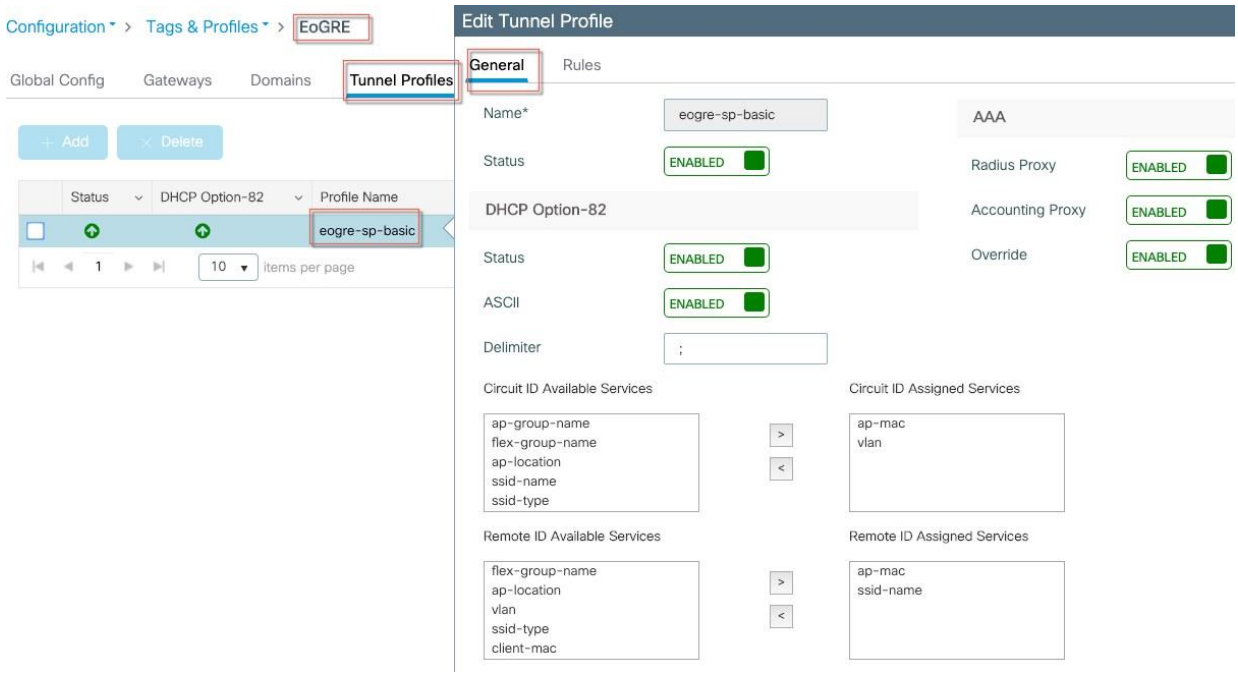
Note: Open-Authentication: only wildcard rule is acceptable.

Dot1X: NAI = <user>@<realm> (Realm e.g. = cisco.com)

Example:

```
wireless profile tunnel eogre-sp-basic
dhcp-opt82 circuit-id ap-ethmac,vlan
dhcp-opt82 delimiter ;
dhcp-opt82 enable
dhcp-opt82 remote-id ap-mac,ssid-nam
```

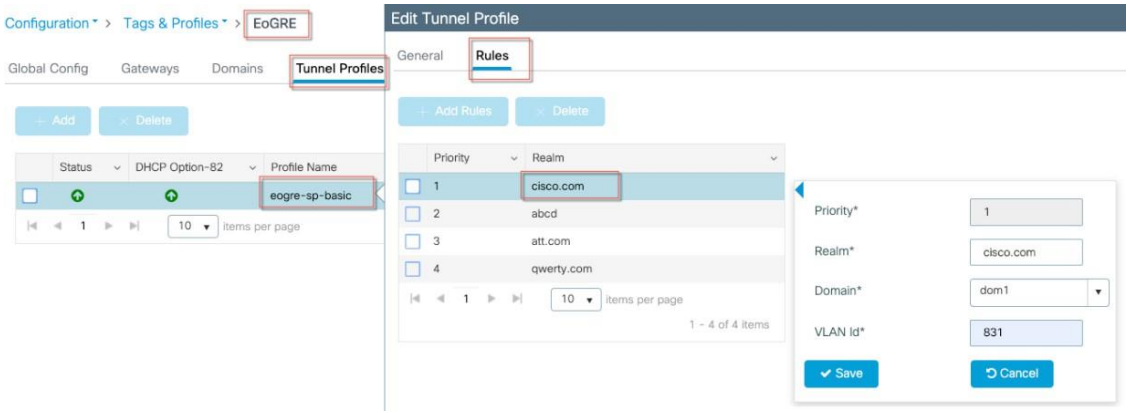
Same Configuration done from the WebUI interface



Step 5: On the C9800 EoGRE Tunnel Global Interface configure EoGRE Profile with Rules and Realm filters.

```
Rule 1 realm-filter cisco.com domain dom1 vlan 831
rule 2 realm-filter abcd.com domain dom2 vlan 833
rule 3 realm-filter att.com domain dom3 vlan 835
rule 4 realm-filter qwerty.com domain dom1 vlan 831
```

Same configuration done from the WebUI interface

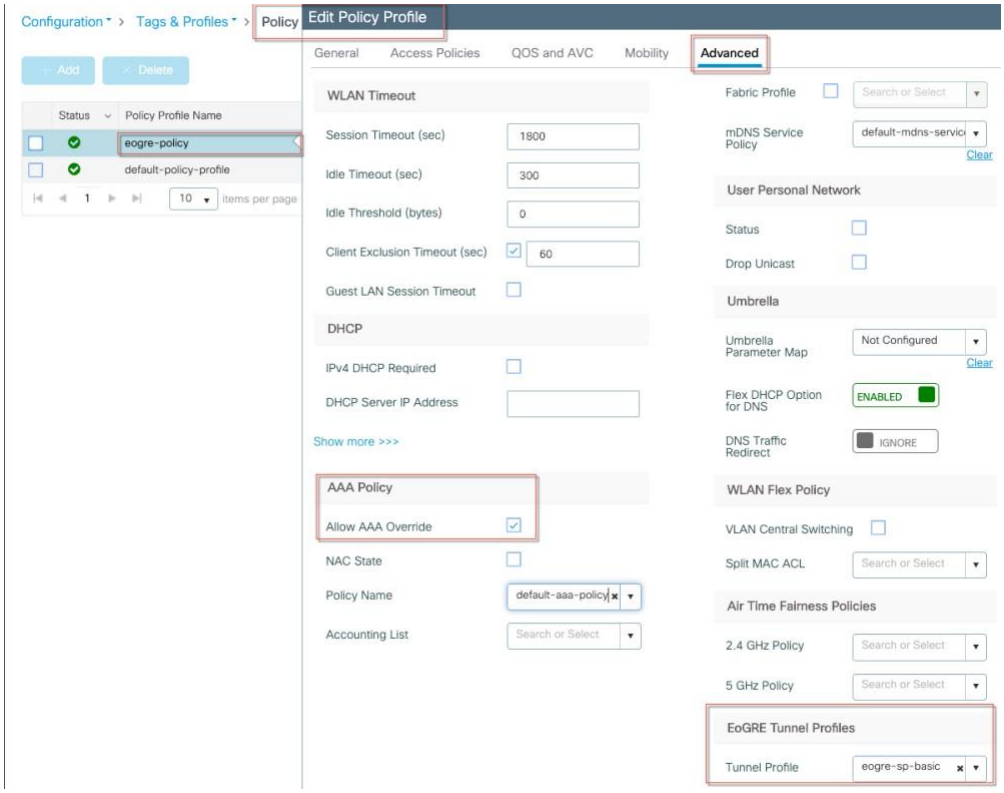


Step 6: Map the earlier created Tunnel Profile to the Wireless Policy Profile wireless profile

```
policy eogre-sp-local-basic
aaa-override
```

```
no central switchin
session-timeout 86400
tunnel-profile eogre-sp-basic
vlan 135
no shutdown
```

Same configuration can be done on the WebUI interface

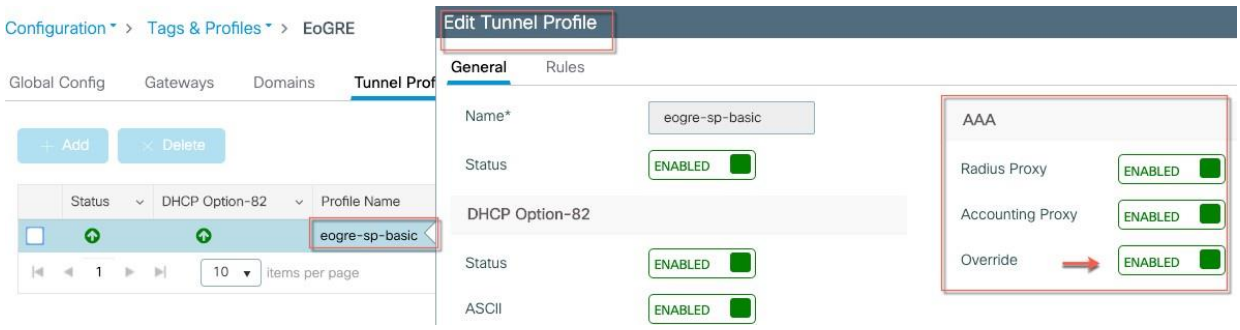


Use Show command as in the example below to display the profile mapping

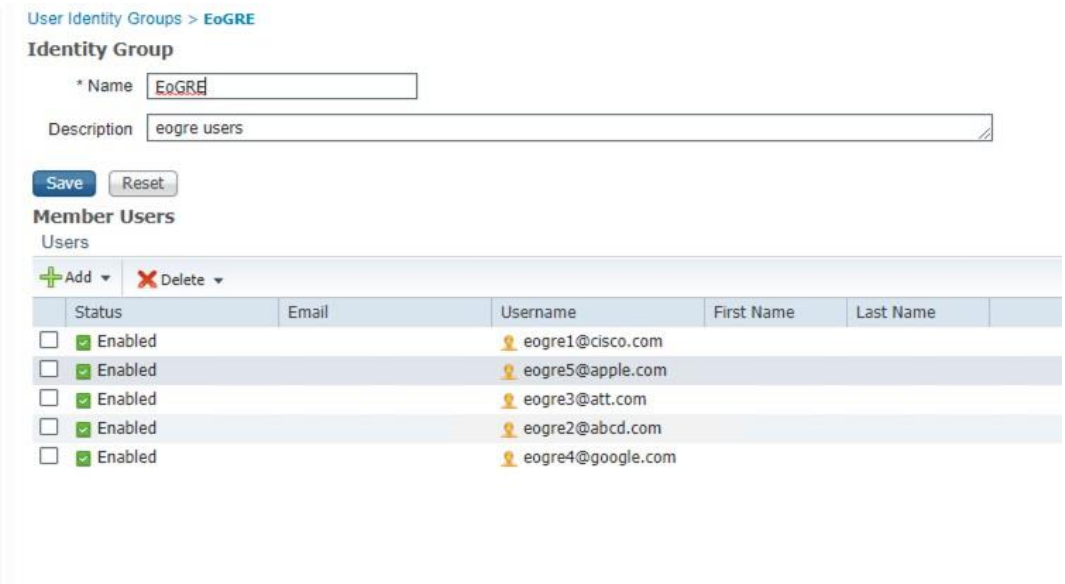
```
spwifi-ewlc-11#sh wireless profile policy detailed eogre-sp-local-basic

Policy Profile Name                          : eogre-sp-local-basic
Description                                  :
Status                                       : ENABLED
VLAN                                         : 135
Multicast VLAN                               : 0
Passive Client                               : DISABLED
ET-Analytics                                 : DISABLED
StaticIP Mobility                            : DISABLED
WLAN Switching Policy
  Flex Central Switching                     : ENABLED
  Flex Central Authentication                : ENABLED
  Flex Central DHCP                          : ENABLED
  Flex NAT PAT                               : DISABLED
  Flex Central Assoc                         : ENABLED
WLAN Flex Policy
  VLAN based Central Switching               : DISABLED
WLAN ACL
  IPv4 ACL                                   : Not Configured
  IPv6 ACL                                   : Not Configured
  Layer2 ACL                                 : Not Configured
  Preauth urlfilter list                     : Not Configured
  Postauth urlfilter list                    : Not Configured
WLAN Timeout
  Session Timeout                            : 86400
  Idle Timeout                               : 300
  Idle Threshold                             : 0
WLAN Local Profiling
  Subscriber Policy Name                     : Not Configured
  RADIUS Profiling                           : DISABLED
  HTTP TLV caching                           : DISABLED
  DHCP TLV caching                           : DISABLED
CTS Policy
  Inline Tagging                             : DISABLED
  SGACL Enforcement                          : DISABLED
  Default SGT                                : 0
WLAN Mobility
  Anchor                                     : DISABLED
AVC VISIBILITY                               : Enabled
IPv4 Flow Monitors
  Ingress
      wireless-avc-basic
  Egress
```

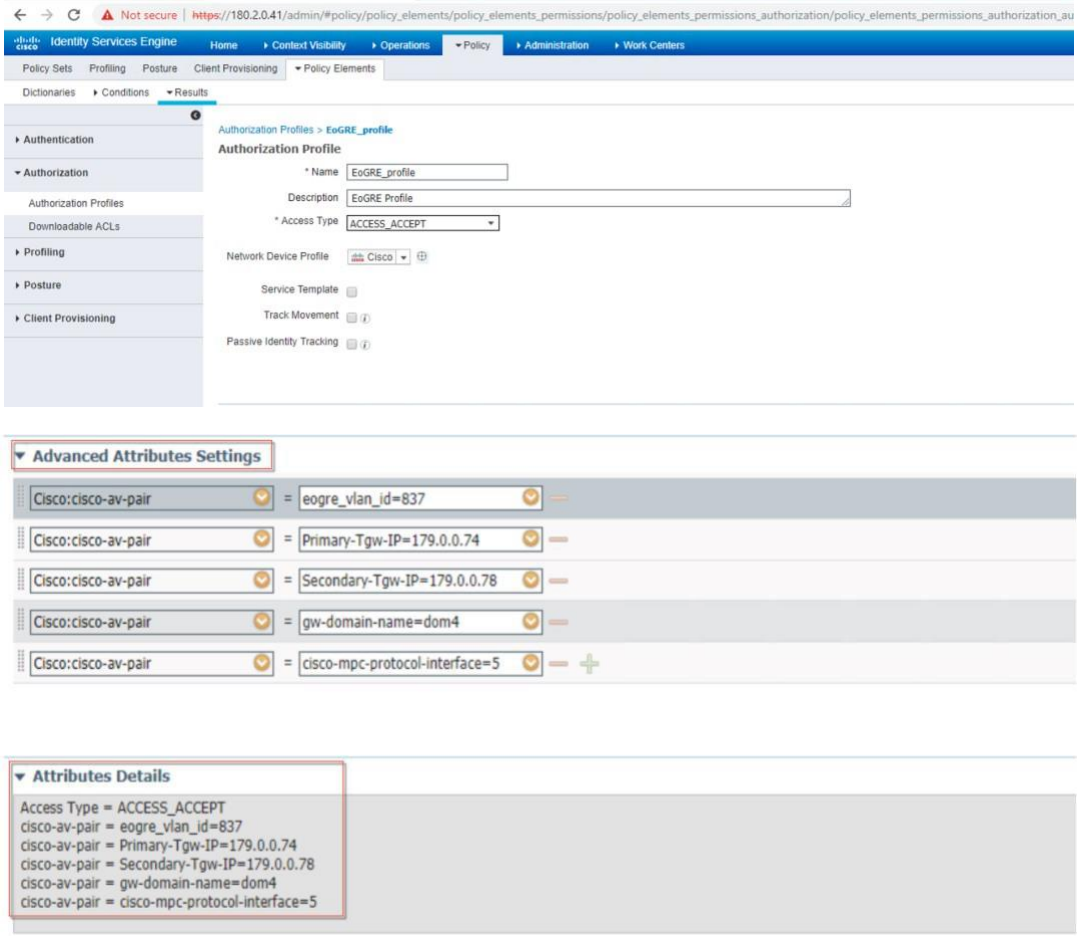
Step 7: (Optional) Configure EoGRE profile with AAA override.



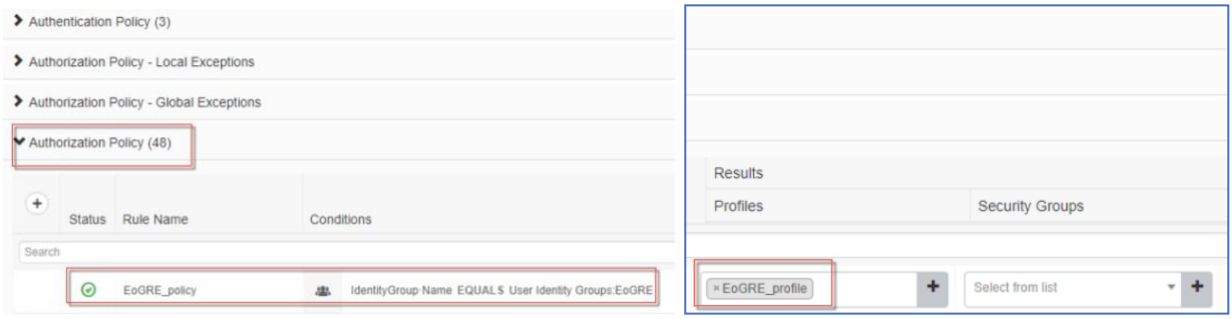
Examples 1: On ISE Create Users NAI (Name@realm) and Identity Group:



Example 2: Create Authorization profile with EoGRE specific attributes to be returned to Controller:



Example 3: Create Authorization Policy mapping user Identity Group to EoGRE Authorization profile



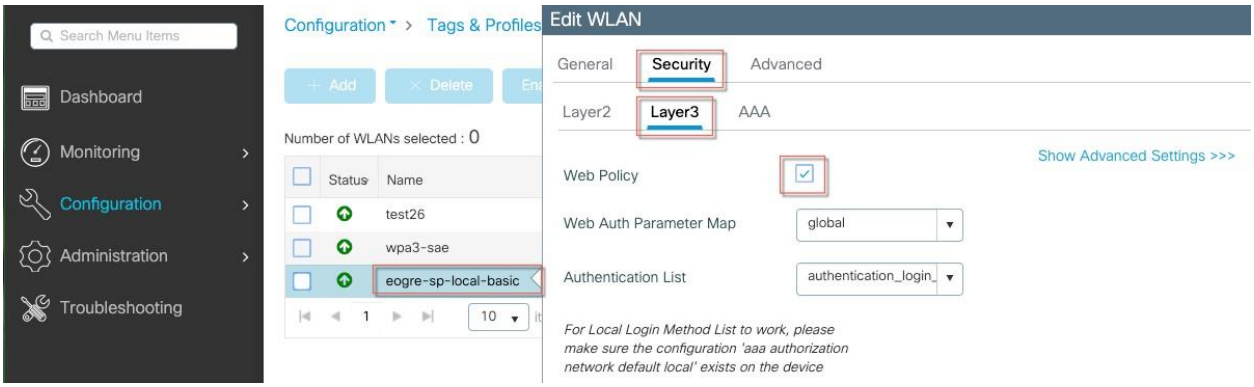
Step 8: On the C9800 create WLAN and Map Policy Tag to WLAN and AP

```
Cat9800(config)#wireless tag policy eogre-sp-tag-local
Cat9800(config-policy-tag)#?
default Set a command to its defaults
description Add a description for the policy tag
exit        Exit sub-mode
no      Negate a command or set its defaults
remote-lan  Map a Remote-Lan profile to a policy profile
wlan    Map a WLAN profile to a policy profile
```

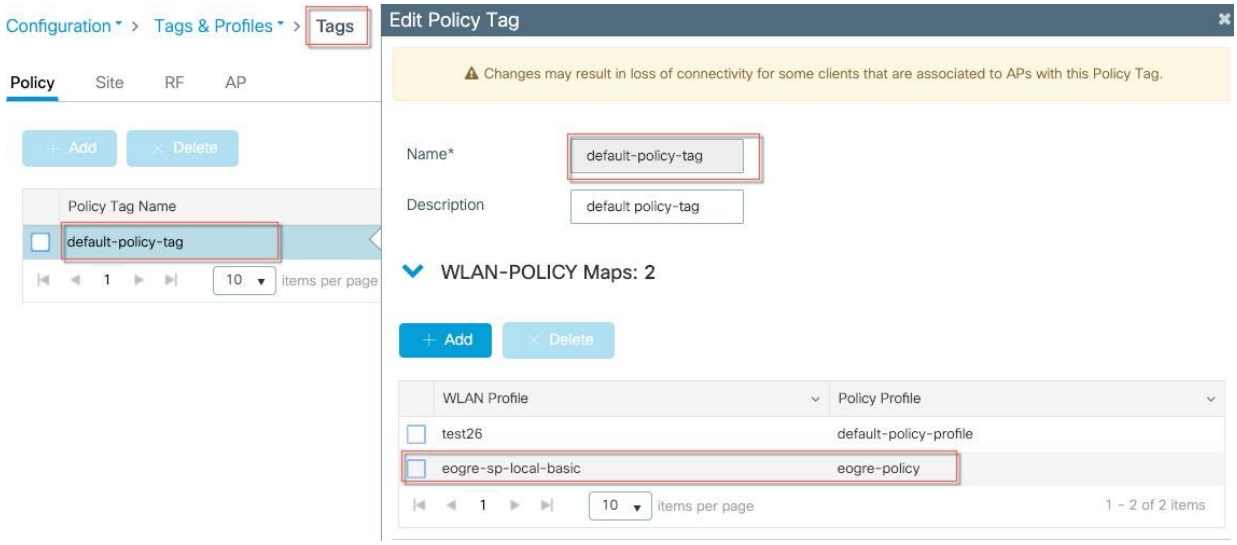
Example:

```
wlan eogre-webauth 9 eogre-webauth
wlan eogre-sp-local-basic 8 eogre-sp-local-basic
tag policy eogre-sp-tag-local
tag site eogre-sp-local-site1
tag policy eogre-sp-tag-local
security web-auth
security web-auth authentication-list lwa_external
security web-auth parameter-map lwa_external
no shut
```

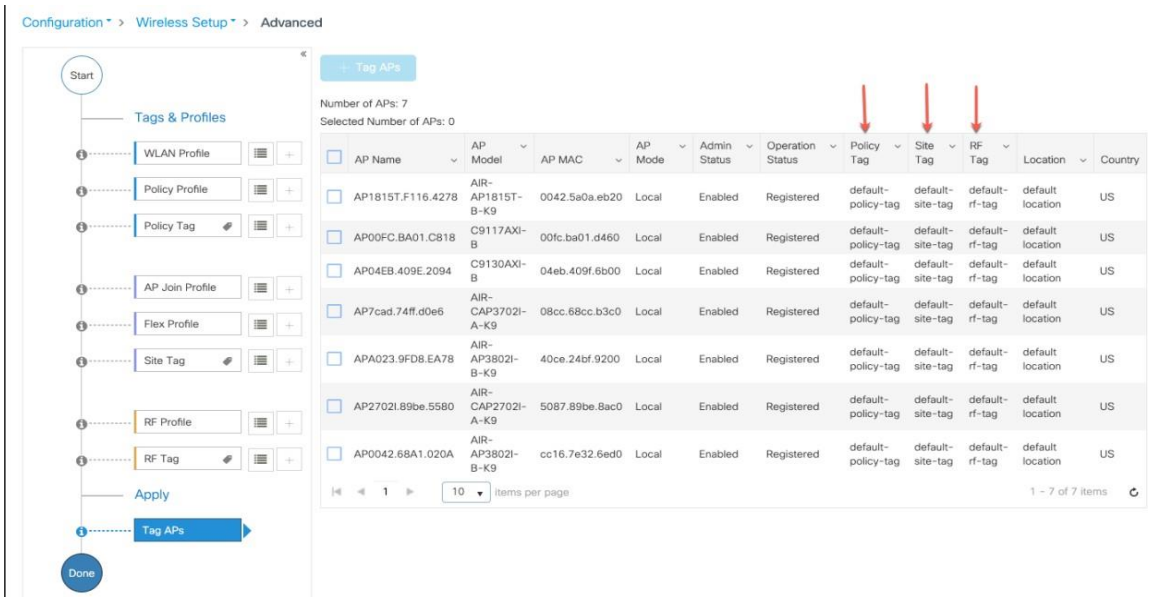
Same configuration done from the WebUI interface



After WLAN is created with policy profile tag the default-policy-tag or any other Policy Tag created with the WLAN and Policy Profiles as shown in the example below.



Also verify that all appropriate tags are mapped to the all desired APs as shown in the example below under Configuration>Wireless Setup>Advanced>Tag APs.



Verify Policy Mapping with the following show Command:

```
spwifi-ewlc-11#sh wireless tag policy detailed eogre-sp-tag-local

Policy Tag Name : eogre-sp-tag-local
Description     :

Number of WLAN-POLICY maps: 3
WLAN Profile Name                Policy Name
------------------------------------------------------------------------
eogre-avc                        eogre-avc
eogre-webauth                    eogre-sp-local-basic
eogre-sp-local-basic             eogre-sp-local-basic

Number of RLAN-POLICY maps: 0
```

Step 9: (Optional Recommended Configuration) On the C9800 configure source interfaces for a better throughput

Step 9a: C9800 4 ports bundled in Ether-channel on the Controller and switch side. Enable load balancing based on source destination IP.

```
conf t
port-channel load-balance src-dst-ip
```

Step 9b: Use different source interfaces on each tunnel as shown in the example below:

```
interface Tunnel1
no ip address
tunnel source Vlan1443
tunnel mode ethernet gre ipv4 p2p
tunnel destination 40.253.0.2
interface Tunnel2
no ip address
tunnel source Vlan1446
tunnel mode ethernet gre ipv4 p2p
tunnel destination 40.253.0.6
interface Tunnel3
no ip address
tunnel source Vlan1447
tunnel mode ethernet gre ipv4 p2p
tunnel destination 40.253.0.10
interface Tunnel4
no ip address
tunnel source Vlan1448
tunnel mode ethernet gre ipv4 p2p
tunnel destination 40.253.0.14
```

Step 9c: Choose IP of source interface, such that, the traffic flows will take different links for each src-dest IP pair.

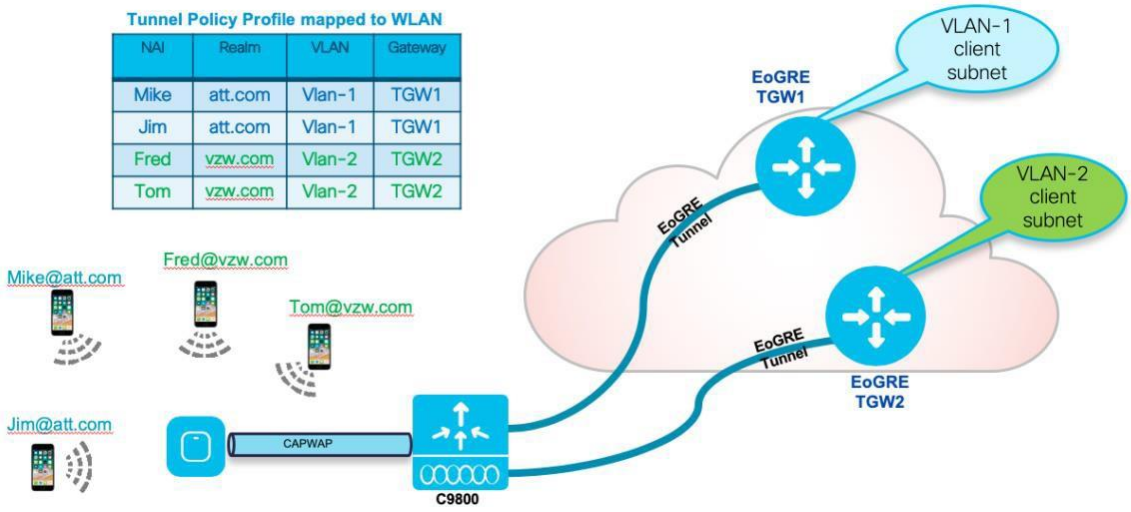
Ex: Hash result for following three flows are bucket 2, 10, 2, one member link. This will not give max throughput, as all flows go through link 2.
Client traffic on Tunnel1 – Src IP: 40.143.0.72 Dest IP: 40.253.0.2
Client traffic on Tunnel2 – Src IP: 40.146.0.72 Dest IP: 40.253.0.6
Client traffic on Tunnel3 – Src IP: 40.147.0.72 Dest IP: 40.253.0.10

Ex: Hash result for following three flows are bucket 2, 1, 3, three member links. This will maximize throughput achieved. Note the Source IPs are different from above
Client traffic on Tunnel1 – Src IP: 40.143.0.72 Dest IP: 40.253.0.2
Client traffic on Tunnel2 – Src IP: 40.146.0.94 Dest IP: 40.253.0.6
Client traffic on Tunnel3 – Src IP: 40.147.0.74 Dest IP: 40.253.0.10

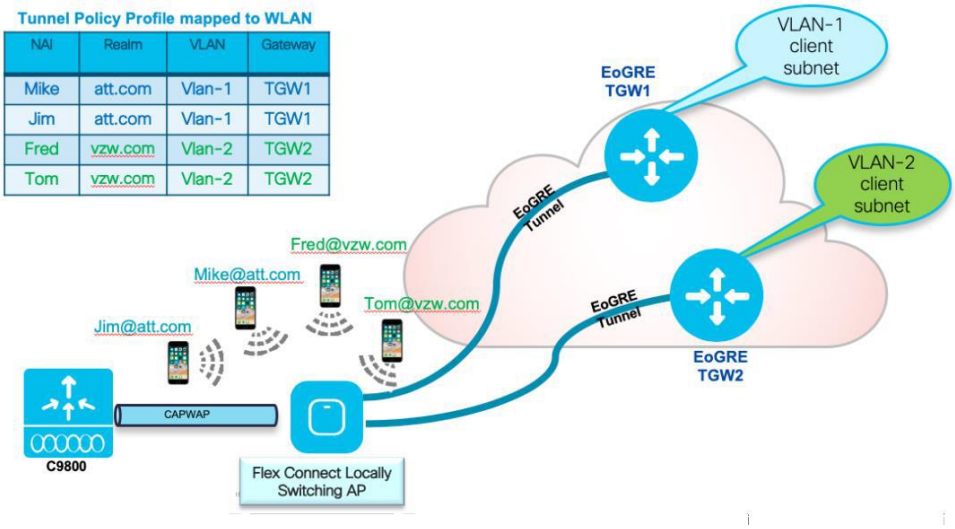
Step 9d: Use CLI command to determine the link a particular flow would take. CLI is available in IOS-XE 17.1 code. CLI will plug in arbitrary source and destination IP addresses, and the output will be the best link the traffic flow will take. This command is applicable for Local Mode APs with EoGRE tunnel only.

```
sh platform software port-channel link-select interface port-channel 4 ipv4 <src_ip>
<dest_ip> "
```

Typical Deployment C9800 – Local Mode EoGRE Topology



Typical Deployment FC-AP – FlexConnect Mode EoGRE Topology



In case of Flex, the Access Point creates the EoGRE tunnels towards Tunnel Gateways and EoGRE module in WLC takes care of handling the control path for wireless clients and manageability for tunnels. When Flex Connect AP joins the controller the Tunnel Manager on the controller will push the global EoGRE parameters and the whole set of the Domains and Tunnel configurations to the FC AP.

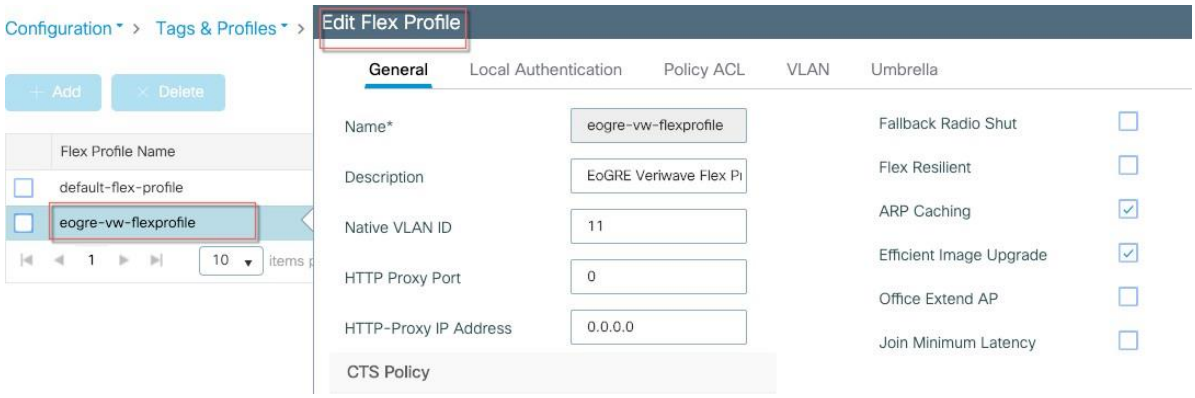
For Flex Connect mode, C9800 controller does the following:

- Pass Domain and TGW configuration to APs
- Allow Tunnel creation on Access Points
- Implement (or proxy) AAA functionalities for APs

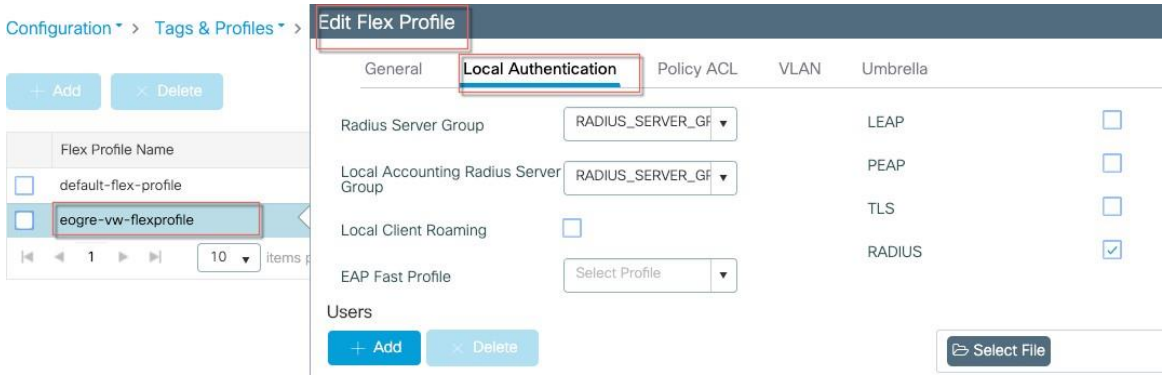
EoGRE with FlexConnect sample configuration is below:

Below please see FlexConnect example configurations in both CLI and also followed by the WebUI modes.

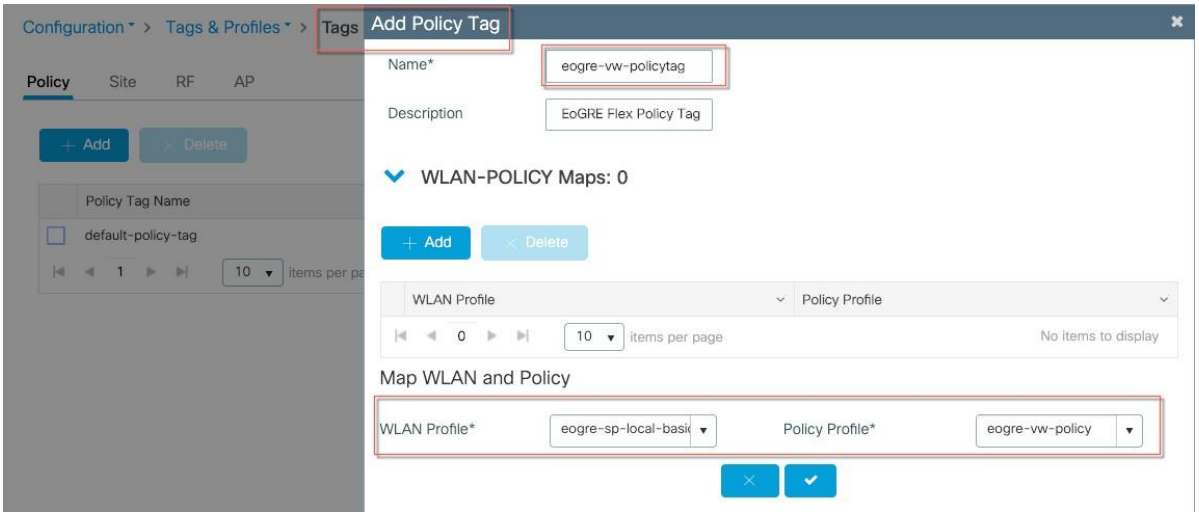
```
wireless tag site eogre-vw-sitetag
flex-profile eogre-vw-flexprofile
no local-site
```



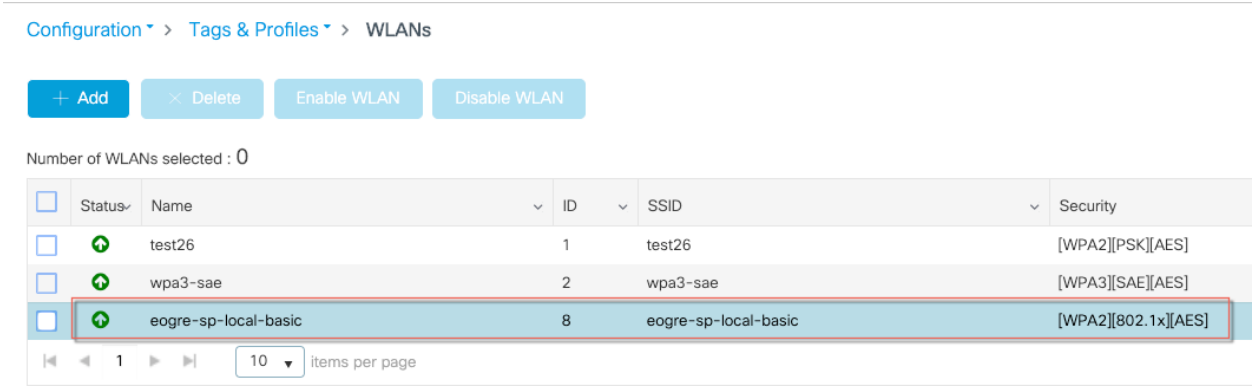

```
wireless profile flex eogre-vw-flexprofile
local-auth radius-server-group vw
native-vlan-id 11
vlan-name flexvlan
vlan-id 140
```




```
wireless tag policy eogre-vw-policytag
wlan eogre-sp-local-basic policy eogre-vw-policy
```



```
wlan eogre-sp-local-basic 8 eogre-sp-local-basic
no security ft over-the-ds
no security ft adaptive
security dot1x authentication-list spwifi_dot1x
no shutdown
```




```
wireless profile policy eogre-vw-policy
no central association
no central dhcp
no central switching session-timeout 86400
tunnel-profile eogre-sp-basic
vlan 140

no shutdown

Note: Ensure that central authentication is configured
```

Local mode EoGRE Show Configuration Details

```
Tunnel Gateways
show tunnel eogre gateway summary
show tunnel eogre gateway detailed <tunnel-intf> show tunnel eogre gateway detailed
Domain
show tunnel eogre domain summary
show tunnel eogre domain detailed <domain-name> show tunnel eogre domain detailed
Flex Connect Mode EoGRE Show Configuration details Tunnel Gateways
show ap tunnel eogre gateway summary
show ap tunnel eogre gateway detailed <tunnel-intf> show ap tunnel eogre gateway detailed
show ap name <ap-name> tunnel eogre gateway summary
show ap name <ap-name> tunnel eogre gateway detailed <tunnel-intf>
Domain
show ap tunnel eogre domain summary
show ap tunnel eogre domain detailed <domain-name> show ap tunnel eogre domain detailed
show ap name <ap-name> tunnel eogre domain summary
show ap name <ap-name> tunnel eogre domain detailed <domain-name>
EoGRE Events on APs
show ap tunnel eogre events
show ap name <ap-name> tunnel eogre events
```

EoGRE configuration summary from running config

```
interface Tunnel1
tunnel eogre source Vlan70 no ip address
tunnel source Vlan70
tunnel mode ethernet gre ipv4 p2p tunnel destination 179.0.0.50
!
interface Tunnel2 no ip address
tunnel source Vlan70
tunnel mode ethernet gre ipv4 p2p tunnel destination 179.0.0.54
!
wireless profile tunnel eogre-sp-basic aaa-override
dhcp-opt82 ascii
dhcp-opt82 circuit-id ap-mac,vlan dhcp-opt82 delimiter ;
dhcp-opt82 enable
dhcp-opt82 remote-id ap-mac,ssid-name gateway-accounting-radius-proxy gateway-radius-proxy
rule 1 realm-filter cisco.com domain dom1 vlan 831 rule 2 realm-filter abcd domain dom2 vlan 833
rule 3 realm-filter att.com domain dom3 vlan 835 rule 4 realm-filter qwerty.com domain dom1 vlan 831 no
shutdown
!
vlan-name flexvlan vlan-id 11
description "EoGRE Veriwave Flex Profile"
local-accounting radius-server-group RADIUS_SERVER_GROUP_<...> local-auth radius-server-group
RADIUS_SERVER_GROUP_<. >
native-vlan-id 11 vlan-name flexvlan vlan-id 140
!
wireless profile policy eogre-policy aaa-override
description "EoGRE Policy Profile" tunnel-profile eogre-sp-basic
no shutdown
wireless profile policy eogre-vw-policy
no central association
no central dhcp
no central switching
description "EoGRE policy tag FC" no shutdown
!
wireless tag site eogre-vw-sitetag description "EoGRE sitetag"
!
wlan eogre-sp-local-basic policy eogre-policy wireless tag policy eogre-vw-policytag description "EoGRE
Flex Policy Tag"
wlan eogre-sp-local-basic policy eogre-vw-policy
!
tunnel eogre domain dom1 primary Tunnel1 redundancy revertive secondary Tunnel2
no shutdown
tunnel eogre domain dom2 primary Tunnel1 redundancy revertive secondary Tunnel2
no shutdown
tunnel eogre domain dom3 primary Tunnel2
redundancy revertive secondary Tunnel1 no shutdown
tunnel eogre source Vlan70
tunnel eogre interface Tunnel1 aaa proxy key 0 0 tunnel eogre interface Tunnel2 aaa proxy key 0 1
!
wlan eogre-sp-local-basic 8 eogre-sp-local-basic ccx aironet-iesupport
no security ft adaptive security pmf mandatory
security web-auth authentication-list authentication_login_day0 security web-auth parameter-map global
```

Legal Information

Cisco Trademark

Cisco Copyright