VLAN ID Based Policy Control

The VLAN ID based policy control feature is used to segregate subscribers based on VLAN IDs. Service Set Identifier (SSID) is mapped to virtual local area network (VLAN), and hence VLAN-based segregation allows Intelligent Services Gateway(ISG) and Intelligent Wireless Access Gateway (iWAG) to detect subscribers connecting to open and secure SSID efficiently. In case of sessions where a NAS port ID is not available for segregation of the subscribers, (e.g. - Walk-By users), the VLAN ID can be used to segregate subscribers. This feature is specifically designed for Ethernet over Generic Routing Encapsulation (EoGRE) access where multiple VLANs get terminated on the same Tunnel Interface.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for VLAN ID Based Policy Control

The VLAN ID Based Policy Control feature is applicable only to session-start and session-restart events in the control policy.

Information About VLAN ID Based Policy Control

With VLAN-based control policies, subscribers connecting through specific SSIDs can be identified with any packet (DHCP, ARP, Data Packet) based on VLANs, and respective policies or features can be applied during session start and restart. Multiple VLANs can be mapped to the same SSID with specific IP pools and subnets. IP address is allocated to WiFi subscriber device connecting through specific SSID/VLAN from respective subnet.

Multipoint Generic Routing Encapsulation (mGRE) Tunnels can map to multiple VLANs and all the VLAN may be terminated in the single EoGRE Tunnel. As a result, subscribers connecting to VLAN1 and VLAN2 will reach iWAG on the same access interface. It is necessary to identify such subscribers and apply a different control policy based on the VLAN IDs.

Configuring VLAN ID Based Policy Control

Perform this task to configure VLAN ID Based Policy Control feature.

SUMMARY STEPS

1. enable
2. configure terminal
3. match vlan *vlan_id*
4. end

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password when prompted.
Step 2	configure terminal **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	match vlan *vlan_id* **Example:** `Router(config)# match vlan 200`	Segregates subscribers based on VLAN IDs. When the VLAN ID-based control policy is applied under condition class map, different control policies are applied for different subscribers. **Note** The **no** form of this command unconfigures the VLAN ID based control policy feature.
Step 4	end **Example:** `Router(config)# end`	Returns the device to privileged EXEC mode.

Configuration Examples for VLAN ID Based Policy Control

Example: Defining a Default Control Policy

```
policy-map type control EOGRE_WALKBY_RULE
 class type control SECURE_SSID_VLAN event session-start
  10 default-exit
 !
 class type control always event session-start
  .......
 !
 class type control always event timed-policy-expiry
  1 service disconnect
 !
!
```

Example: Defining a Regular Control Policy

```
policy-map type control EOGRE_POLICY_RULE
 class type control IP_UNAUTH_COND event timed-policy-
expiry
  10 service disconnect
 !
class type control SECURE_SSID_VLAN event session-start
  ......
 !
 class type control SECURE_SSID_VLAN event session-restart
...... !

 class type control always event session-start
  ....
 !
 class type control always event session-restart
...... !
```

Example: Defining a Condition Map

```
class-map type control match-any SECURE_SSID_VLAN
 match vlan 200
 match vlan 201
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases

Related Topic	Document Title
iWAG commands	Cisco IOS Intelligent Wireless Access Gateway Command Reference

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for VLAN ID Based Policy Control

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for VLAN ID Based Policy Control

Feature Name	Releases	Feature Information
VLAN ID Based Policy Control	Cisco IOS XE Release 3.15	In Cisco IOS XE Release 3.15, this feature was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.