Configuring Wireless QoS

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

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

Related Topics

Feature History and Information for Troubleshooting Software Configuration

Prerequisites for Wireless QoS

Before configuring wireless QoS, you must have a thorough understanding of these items:

- QoS concepts.
- Wireless concepts and network topologies.
- Classic Cisco IOS QoS.
- Modular QoS CLI (MQC).
- Understanding of QoS implementation.

- The types of applications used and the traffic patterns on your network.
- Traffic characteristics and needs of your network. For example, is the traffic on your network bursty? Do you need to reserve bandwidth for voice and video streams?
- Bandwidth requirements and speed of the network.
- Location of congestion points in the network.

Restrictions for Wireless QoS

General Restrictions

- A target is an entity where a policy is applied. You can apply a policy to either a wired or wireless target. A wired target can be either a port, client, or VLAN. A wireless target can be either a port, SSID, client, or radio. Wireless QoS policies for port, SSID, client, and radio are applied in the downstream direction. That is, when traffic is flowing from the switch to wireless client.

  Only port, SSID, and client (using AAA and Cisco IOS command-line interface) policies are user-configurable. Radio policies are set by the wireless control module and are not user-configurable.
- Port and radio policies are applicable only in the downstream direction (traffic flowing from a wired source to a wireless target).
- SSID and client support non-queuing policies in the upstream direction. SSID and client targets can be configured with marking and policing policies.
- One policy per target per direction is supported.
- For marking rules for access points associated with the switch, the following rules apply:
  - Policing at the access point is not supported.
  - Client policies that are passed to the access points in the upstream direction are not supported.
  - The following rules apply for QoS at the SSID:
    - One table map is supported at the ingress policy.
    - Up to three table maps can be configured in the egress direction for SSID when a QoS-group is involved.

    Note Table maps are not supported at the client targets.

  - IPv6 QoS for wireless clients is not supported.
- SSID policies are applicable for unicast downstream and upstream traffic. AFD policing support is supported only for downstream traffic.
- Client-based polices are supported in both upstream and downstream directions.
- Marking policies are applicable only at the SSID and client targets.
- SSID and client policies are applicable in the upstream direction.

- QoS policies are not supported on wired clients. To configure QoS on wired clients, configure the policy on the port. The UP values for wireless packets can be added when the ports are configured with the policies.
- By default, all wireless traffic is treated as untrusted. That is, in the absence of a table map on the SSID, the packets coming in and going out of the wireless targets are re-marked down to 0. To change the wireless traffic from being untrusted by default to being trusted, you must configure the table map to ensure appropriate packet markings are defined.

Wireless QoS Restrictions on Ports

The following are restrictions for applying QoS features on wireless port target:

- All wireless ports have similar parent policy with one class-default and one action shape under class-default. Shape rates are dependent on the 802.11a/b/g bands.
- You can create a maximum of four classes in a child policy.
- If there are four classes in the child policy at the port level, one must be a non-client-nrt class and one must be class-default.
- No two classes can have the same priority level. Only priority level 1 (for voice traffic and control traffic) and 2 (for video) are supported. Strict priority is supported on Q0.
- Priority is not supported in the multicast NRT class (non-client-nrt class).
- If four classes are configured, two of them have to be priority classes. If only three classes are configured, at least one of them should be a priority class. If three classes are configured and there is no non-client-nrt class, both priority levels must be present.
- Only match DSCP is supported.
- Multiple Multicast-NRT classes are not supported in the port level (that is, there can be only one non-client-nrt-class in the child policy)
- The port policy applied by the wireless control module cannot be removed using the CLI.
- Both Priority Rate and Police CIR (using MQC) in the same class is unsupported.
- Queue-limit is unsupported.

Wireless QoS Restrictions on SSID

The following are restrictions for applying QoS features on SSID:

- If a wireless port has a default policy with only two queues (one for multicast-NRT, one for default), the policy at SSID level cannot have voice and video class.
- Set and priority cannot coexist under the same class.
- Set (non-table map) policies at the SSID level will be restricted.
- Priority configuration at the SSID level is used only to configure the RT1 and RT2 policers (AFD for policer). Priority configuration does not include the shape rate. Therefore, priority is restricted for SSID policies without police.
- If **set** is not enabled in class-default, the classification at the SSID for voice or video must be a subset of the classification for the voice or video class at the port level.

- The mapping in the DSCP2DSCP and COS2COS table should be based on the classification mechanism for the voice and video classes in the port level policy.
- Two or three **set** commands with table-map related functionality is supported in the parent class-default policy.
- If one SSID policy has only voice class in a QoS configuration, for example:

```
SSID-1
  Class voice
  Priority level 1
  Class video (af11)
  Priority level 2
```

  And another SSID policy has both voice and video class, for example:

```
SSID-2
  Class voice
  Priority level 1
  Class video (af11)
  Priority level 2
```

  The table map for the SSID 1 must be configured so that the video DSCP is best effort marking. This action ensures that video packets for SSID1 are mapped to the NRT queue at the port level.
- The **set table-maps** configuration can only be applied in the parent class-default at the SSID level.
- Table map action is supported only in this class-default class.
- No action is allowed under the class-default of a child policy.
- For a flat policy (non-hierarchical):
  - In the ingress direction, the policy configuration must be a set or policing policy.
  - In the egress direction, the following is supported:
    - Aggregate policer

  For a hierarchical policy:
  - In the egress direction, the following is supported:
    - Table map in parent with only police allowed in child.
    - Table map and queuing configured in the parent policy—The parent policy will have a Bandwidth Remaining Ratio (BRR) or shape (either one can be configured), and the **set (table-map)** configuration command. The child policy should have a priority and police configuration, in which the priority matches the priority level configured at the AP port.

Wireless QoS Restrictions on Radio

The following are restrictions for applying QoS policies on radio targets:

- Ingress policies are not supported.
- For egress policies, only the shape and BRR queuing are supported on class-default.

Wireless QoS Restrictions on Clients

The following are restrictions for applying QoS policies on client targets:

- Queuing is not supported.
- Attaching or removing client policies on a WLAN in the up state is not supported. You must shut down the WLAN to apply or remove a policy.
- Table map based set is blocked at the client.
- Police in child policy class-default is not supported in the egress and ingress directions. For example, the following policy is not supported:

```
Policy-map parent-client
class class-default
police X
service-policy child-client

Policy-map child-client
class class-default
police Y
```

- Policing and set in class-default is blocked in both the upstream and downstream direction:

```
policy-map foo
class class-default
police X
set dscp Y
```

- The following policy configuration is not supported:

```
policy map foo
  class acl-101 (match on 3 tuple)
  Police X
  class acl-102
  (match on 5 tuple)
Police Y
```

- In a flat (nonhierarchical) policy, only police is supported. For user-defined classes, only the following filters are supported:
  - ACL
  - DSCP
  - COS
  - WLAN UP
- No child-policy support under class-default, if the parent policy contains other user-defined class maps in it.

Related Topics

Queuing in Wireless, on page 13
Port Policy Format, on page 11
Port, on page 8
Radio, on page 9
Restrictions for QoS on Wired Targets

Information about Wireless QoS

Wireless QoS Overview

Wireless QoS can be configured on the following wireless targets:

- Wireless ports, including all physical ports to which an access point can be associated.
- Radio
- SSID (applicable on a per-radio, per-AP, and per-SSID)
- Client

QoS policies are configured by using Modular QoS CLI (MQC). Port, SSID, and client policies are user configurable. Radio policies are controlled by the wireless control module.

A target is the entity where the policy is applied. Wireless QoS policies for port, SSID, client, and radio are applied in the downstream direction. That is, when traffic is flowing from the switch to wireless client.

Note SSID and client policies are supported only in the upstream direction.

The following are some of the specific features provided by wireless QoS:

- Policies on wireless QoS targets:
  - port
  - radio
  - SSID
  - client
- Queuing support
- Policing of wireless traffic
- Shaping of wireless traffic
- Rate limiting in both downstream and upstream direction
- Approximate Fair Drop (AFD)
- Mobility support for QoS
- Compatibility with precious metal QoS policies available on Cisco Unified Wireless Controllers.

User-Defined Policies

You can configure the following kinds of QoS policies:

- Port policies
- SSID policies

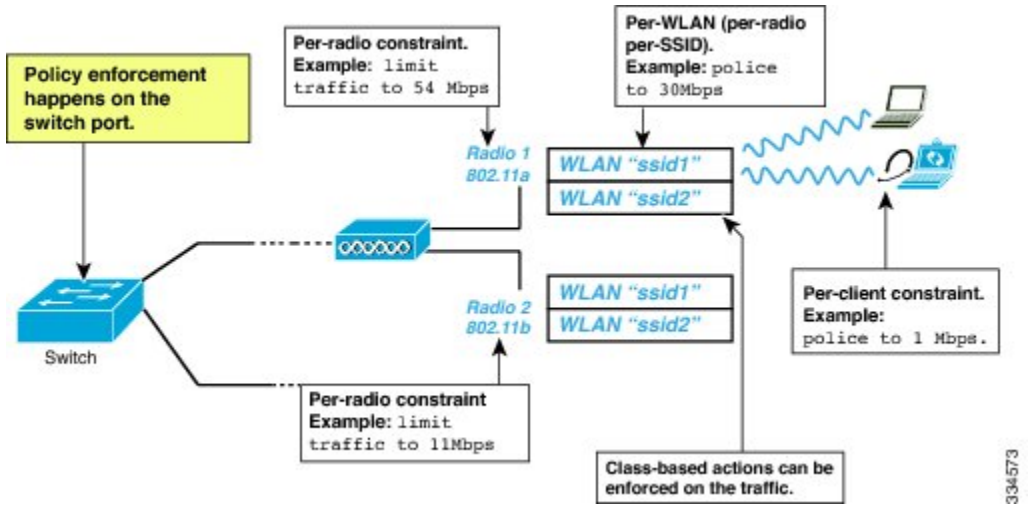
- Client policies
- Multidestination policers
- VLAN policies

Hierarchical Wireless QoS

The switch supports hierarchical QoS for wireless targets. Hierarchical QoS policies are applicable on port, radio, SSID, and client. QoS policies configured on the device (including marking, shaping, policing) can be applied across the targets. If the network contains non-realtime traffic, the non-realtime traffic is subject to approximate fair drop. Hierarchy refers to the process of application of the various QoS policies on the packets arriving to the device.

This figure shows the various targets available on a wireless network.

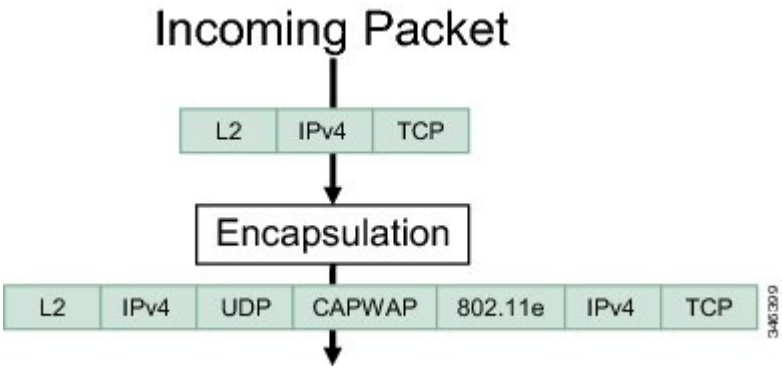
Figure 1: Hierarchical QoS



Wireless Packet Format

This figure describes the wireless packet flow. The incoming packet enters the switch. The switch encapsulates this incoming packet and adds the 802.11e and CAPWAP headers.

Figure 2: Wireless Packet Path in the Egress direction during first pass



Hierarchical AFD

Approximate Fair Dropping (AFD) is a feature provided by the QoS infrastructure in Cisco IOS. For wireless targets, AFD can be configured on SSID (via shaping) and clients (via policing). AFD shaping rate is only applicable for downstream direction. Unicast real-time traffic is not subjected to AFD drops.

Wireless QoS Targets

This section describes the various wireless QoS targets available on a switch.

Port

The switch supports port-based policies. The port policies includes port shaper and a child policy (port_child_policy).

Port shaper specifies the traffic policy between the device to the AP. This is the sum of the radio rates supported on the access point.

The child policy determines the mapping between packets and queues defined by the port-child policy. The child policy can be configured to include voice, video, and class-default classes where voice and video are based on DSCP value (which is the outer CAPWAP header DSCP value). The definition of class-default is known to the system as any value other than voice and video DSCP.

The DSCP value is assigned when the packet reaches the port. Before the packet arrives at the port, the SSID policies are applied on the packet. Port child policy also includes multicast percentage for a given port traffic. By default, the port child policy allocates up to 10 percent of the available rate.

Related Topics

Queuing in Wireless, on page 13

Restrictions for Wireless QoS, on page 2

Supported QoS Features on Wireless Targets, on page 10

Examples: Wireless QoS Policy Classified by Voice, Video, and Multicast Traffic, on page 22

Radio

The switch enables you to create policies. The radio policies are system defined and are not user configurable. Radio wireless targets are only applicable in the downstream direction.

Radio policies are applicable on a per-radio, per-access point basis. The rate limit on the radios is the practical limit of the AP radio rate.

Related Topics

Restrictions for Wireless QoS, on page 2

Supported QoS Features on Wireless Targets, on page 10

SSID

You can create QoS policies on SSID (BSSID) in both the upstream and downstream directions. By default, there is no SSID policy. All traffic is transmitted as best effort because the wireless traffic in untrusted. You can configure an SSID policy based on the SSID name. The policy is applicable on a per BSSID.

The types of policies you can create on SSID include marking by using table maps (table-maps), shape rate, and RT1 and RT2 policiers. If traffic is upstream, you usually configure a marking policy on the SSID. If traffic is downstream, you can configure marking and queuing.

There should be a one-to-one mapping between the policies configured on port and SSID. For example, if you configure class voice and class video on the port, you can have a similar policy on the SSID.

SSID priorities can be specified by configuring bandwidth remaining ratio. Queuing SSID policies are applied in the downstream direction.

Related Topics

Supported QoS Features on Wireless Targets, on page 10

Examples: SSID Policy, on page 23

Examples: Configuring Downstream BSSID Policy, on page 23

Client

Client policies are applicable in the upstream and downstream direction. The wireless control module of the switch applies the client policies when admission control is enabled for WMM clients. When admission control is disabled, there is no default client policy. You can configure policing and marking policies on clients.

You can configure client policies in the following ways:

- Using AAA—You can use a combination of AAA and TCLAS, AAA and SIP snooping when configuring via AAA.
- Using the IOS MQC CLI—You can use a combination of CLI and TCLAS and CLI and SIP snooping.
- Using the default configuration

Note When an installed policy gets modified on a WLAN, the WLAN must be restarted for the changes to take effect. For SSID policies, a restart is not required.

Note If you configured AAA by configuring the classic unified wireless controller procedure, and using the MQC QoS commands, the policy configuration performed through the MQC QoS commands takes precedence.

Related Topics

Supported QoS Features on Wireless Targets, on page 10
Examples: Client Policies, on page 24

Supported QoS Features on Wireless Targets

This table describes the various features available on wireless targets.

Table 1: QoS Features Available on Wireless Targets

Target	Features	Traffic	Direction Where Policies Are Applicable	Comments
Port	• Port Shaper • Priority Queuing • Shaping • Multicast Policing • HQF (Hierarchical QoS Framework) • BRR (Bandwidth Remaining Ratio)	Non-Real Time (NRT), Real Time (RT)	Downstream	
Radio	• Shaping	Non-Real Time	Downstream	Radio policies are not user configurable.

Target	Features	Traffic	Direction Where Policies Are Applicable	Comments
SSID	• Shaping • Police • Set • Table map • BRR **Note** Set without table map is not supported on SSID.	Non-Real Time, Real Time	Upstream and downstream	Queuing actions such as shaping and BRR are allowed only in the downstream direction.
Client	• Set • Police	Non-Real Time, Real time	Upstream and downstream	

Downstream Traffic

Traffic flows from a wired source to a wireless target.

Upstream Traffic

Traffic flows from a wireless source to a wired target.

Related Topics

Queuing in Wireless, on page 13
Port Policy Format, on page 11
Port, on page 8
Radio, on page 9
SSID, on page 9
Client, on page 9

Port Policy Format

This section describes the behavior of the port policies on a Catalyst 3850 switch. The ports on the switch do not distinguish between wired or wireless physical ports. Depending on the kind of device associated to the switch, the policies are applied. For example, when an access point is connected to a switch port, the switch detects it as a wireless device and applies the default hierarchical policy which is in the format of a parent-child policy. This policy is an hierarchical policy. The parent policy cannot be modified but the child policy (port-child policy) can be modified to suite the QoS configuration. The switch is pre configured with a default class map and a policy map.

Default class map:

```
Class Map match-any non-client-nrt-class
   Match non-client-nrt
```

The above port policy processes all network traffic to the Q2 queue. You can view the class map by executing the **show class-map** command.

Default policy map:

```
Policy Map port_child_policy
    Class non-client-nrt-class
      bandwidth remaining ratio 10
```

Note The class map and policy map listed are system-defined policies and cannot be changed.

The following is the system-defined policy map available on the ports on which wireless devices are associated. The format consists of a parent policy and a service child policy (**port_child_policy**). To customize the policies to suite your network needs, you must configure the port child policy.

```
Policy-map port policy_map_name
    Class class-default
         Shape average average_rate
         Service-policy port_child_policy
```

Note The parent policy is system generated and cannot be changed. You must configure the *port_child_policy* policy to suit the QoS requirements on your network.

Depending on the type of traffic in your network, you can configure the port child policy. For example, in a typical wireless network deployment, you can assign specific priorities to voice and video traffic. Here is an example:

```
Policy-map port_child_policy
     Class  voice-policy-name (match dscp ef)
          Priority level 1
         Police multicast-policer-name-voice Multicast Policer
    Class video-policy-name (match dscp af11)
        Priority level 2
        Police multicast-policer-name-video Multicast Policer
Class non-client-nrt-class traffic(match non-client-nrt)
        Bandwidth remaining ratio brr-value-nrt-q2
    Class class-default  (NRT Data)
        Bandwidth remaining ratio brr-value-q3
```

In the above port child policy:

- *voice-policy-name*: Refers to the name of the class that specifies rules for the traffic for voice packets. Here the DSCP value is mapped to a value of 46 (represented by the keyword ef). The voice traffic is assigned the highest priority of 1
- *video-policy-name*: Refers to the name of the class that specifies rules for the traffic for video packets. The DSCP value is mapped to a value of 34 (represented by the keyword af11)
- *multicast-policer-name-voice*: Multicast voice policy for video traffic. If you need to configure multicast voice traffic, you can configure policing for the voice class map
- *multicast-policer-name-video*: Multicast voice policy for video traffic. If you need to configure multicast voice traffic, you can configure policing for the video class map

In the above sample configuration, all voice and video traffic is directed to the Q0 and Q1 queues, respectively. These queues maintain a strict priority. The packets in Q0 and Q1 are processed in that order. The bandwidth remaining ratios *brr-value-nrt-q2* and *brr-value-q3l* are directed to the Q2 and Q3 respectively specified by the class maps *non-client-nrt* and *class-default*. The processing of packets on Q2 and Q3 are based on a weighted round robin approach. For example, if the *brr-value-nrtq2* has a value of 90 and *brr-value-nrtq3* is 10, the packets in queue 2 and queue 3 are processed in the ratio of 9:1.

Related Topics

Queuing in Wireless, on page 13
Restrictions for Wireless QoS, on page 2
Supported QoS Features on Wireless Targets, on page 10
Examples: Wireless QoS Policy Classified by Voice, Video, and Multicast Traffic, on page 22

Wireless QoS Rate Limiting

QoS per Client Rate Limit—Wireless

You can configure client rate limiting by the following means:

- AFD
- NetFlow policing

Note For client policy, the voice and video rate limits are applied at the same time.

QoS Downstream Rate Limit—Wireless

Downstream rate limiting is done using policing at the SSID level. AFD cannot drop real-time traffic, it can only be policed in the traffic queues. Real-time policing and AFD shaping is performed at the SSID level.

The radio has a default shaping policy. This shaping limit is the physical limit of the radio itself. For example, the 802.11b/g/n radio can shape up to 100 Mbps on a 2.4 GHz frequency. You can check the policy maps on the radio by using the **show policy-map interface wireless radio** command.

Wireless QoS Multicast

You can configure multicast shaping and policing rate at the port level.

Related Topics

Configuring QoS Policy for Multicast Traffic

Queuing in Wireless

Queuing in the wireless component is performed based on the port policy and is applicable only in the downstream direction. The wireless module supports the following four queues:

- Voice—This is a strict priority queue. Represented by Q0, this queue processes control traffic and multicast or unicast voice traffic. All control traffic (such as CAPWAP packets) is processed through the voice queue. The QoS module uses a different threshold within the voice queue to process control and voice packets to ensure that control packets get higher priority over other non-control packets.
- Video—This is a strict priority queue. Represented by Q1, this queue processes multicast or unicast video traffic.
- Data NRT—Represented by Q2, this queue processes all non-real-time unicast traffic.
- Multicast NRT—Represented by Q3, this queue processes Multicast NRT traffic. Any traffic that does not match the traffic in Q0, Q1, or Q2 is processed through Q3.

Note By default, the queues Q0 and Q1 are not enabled.

Note A weighted round-robin policy is applied for traffic in the queues Q2 and Q3.

For upstream direction only one queue is available. Port and radio policies are applicable only in the downstream direction.

Note The queues on the switch is different from the queues on the access points.

Note The wired ports support eight queues.

Related Topics

Port Policy Format, on page 11
Port, on page 8
Restrictions for Wireless QoS, on page 2
Supported QoS Features on Wireless Targets, on page 10
Examples: Wireless QoS Policy Classified by Voice, Video, and Multicast Traffic, on page 22

Wireless QoS Mobility

Wireless QoS Mobility enables you to configure QoS policies so that the network provides the same service anywhere in the network. A wireless client can roam from one location to another and as a result the client can get associated to different access points associated with a different switch. Wireless client roaming can be classified into two types:

- Intra-switch roaming
- Inter-switch roaming

Note The client policies must be available on all of the switches in the mobility group. The same SSID and port policy must be applied to all switches in the mobility group so that the clients get consistent treatment.

Inter-Switch Roaming

When a client roams from one location to another, the client can get associated to access points either associated to the same switch (anchor switch) or a different switch (foreign switch). Inter-switch roaming refers to the scenario where the client gets associated to an access point that is not associated to the same device before the client roamed. The host device is now foreign to the device to which the client was initially anchored.

In the case of inter-switch roaming, the client QoS policy is always executed on the foreign controller. When a client roams from anchor switch to foreign switch, the QoS policy is uninstalled on the anchor switch and installed on the foreign switch. In the mobility handoff message, the anchor device passes the name of the policy to the foreign switch. The foreign switch should have a policy with the same name configured for the QoS policy to be applied correctly.

In the case of inter-switch roaming, all of the QoS policies are moved from the anchor device to the foreign device. While the QoS policies are in transition from the anchor device to the foreign device, the traffic on the foreign device is provided the default treatment. This is comparable to a new policy installation on the client target.

Note If the foreign device is not configured with the user-defined physical port policy, the default port policy is applicable to all traffic is routed through the NRT queue, except the control traffic which goes through RT1 queue. The network administrator must configure the same physical port policy on both the Anchor and Foreign devices symmetrically.

Intra-Switch Roaming

With intra-switch roaming, the client gets associated to an access point that is associated to the same switch before the client roamed, but this association to the device occurs through a different access point.

Note QoS policies remain intact in the case of intra-switch roaming.

Precious Metal Policies for Wireless QoS

Wireless QoS is backward compatible with the precious metal policies offered by the unified wireless controller platforms. The precious metal policies are system-defined policies that are available on the controller.

The following policies are available:

- Platinum—Used for VoIP clients.
- Gold—Used for video clients.
- Silver— Used for traffic that can be considered best-effort.

- Bronze—Used for NRT traffic.

These policies (also known as profiles) can be applied to a WLAN based on the traffic. We recommend the configuration via the Cisco IOS MQC configuration. The policies are available in the system based on the precious metal policy required.

Based on the policies applied, the 802.11p, 802.11e (WMM) and DSCP fields in the packets are affected. These values are pre configured and installed when the switch is booted.

Note Unlike the precious metal policies that were applicable in the Cisco Unified Wireless controllers, the attributes `rt-average-rate`, `nrt-average-rate`, and peak rates are not applicable for the precious metal policies configured on this switch platform.

Related Topics

Configuring Precious Metal Policies, on page 16

How to Configure Wireless QoS

Configuring Precious Metal Policies

You can configure precious metal QoS policies on a per-WLAN basis.

Note Upstream policies differ from downstream policies. The upstream policies have a suffix of -up.

Before You Begin

SUMMARY STEPS

1. **configure terminal**
2. **wlan** *wlan-name*
3. **service-policy** [**client**] **output** *policy-name*
4. **end**
5. **show wlan** {*wlan-id* | *wlan-name*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global command mode.

	Command or Action	Purpose
Step 2	**wlan** *wlan-name* **Example:** `Switch(config)# wlan test4`	Enters the WLAN configuration sub-mode.
Step 3	**service-policy** [**client**] **output** *policy-name* **Example:** `Switch(config-wlan)# service-policy output platinum`	Configures the WLAN with the QoS policy. To configure the WLAN with precious metal policies, you must enter one of the following keywords: **platinum**, **gold**, **silver**, or **bronze**.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit the global configuration mode.

Step 5	**show wlan** {*wlan-id* | *wlan-name*}
	
	Example:
	`Switch# show wlan qos-wlan`
		Verifies the configured QoS policy on the WLAN.
		
		`Switch# show wlan qos-wlan`
		`. . .`
		`. . .`
		`. . .`
		`QoS Service Policy - Output`
		`  Policy Name : platinum`
		`  Policy State : Validation Pending`
		`QoS Client Service Policy`
		`  Input  Policy Name : gold`
		`  Output Policy Name :`
		`qos-wlan-client-service-policy`
		`. . .`
		`. . .`

Related Topics

Precious Metal Policies for Wireless QoS, on page 15

Configuring Class Maps for Voice and Video

To configure class maps for voice and video traffic, follow these steps:

SUMMARY STEPS

1. **configure terminal**
2. **class-map** *class-map-name*
3. **match dscp** *dscp-value-for-voice*
4. **end**
5. **configure terminal**
6. **class-map** *class-map-name*
7. **match dscp** *dscp-value-for-video*
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**class-map** *class-map-name* **Example:** `Switch(config)# class-map voice`	Creates a class map.
Step 3	**match dscp** *dscp-value-for-voice* **Example:** `Switch(config-cmap)# match dscp 46`	Matches the DSCP value in the IPv4 and IPv6 packets. Set this value to 46.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-z** to exit global configuration mode.
Step 5	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 6	**class-map** *class-map-name* **Example:** `Switch(config)# class-map video`	Configures a class map.
Step 7	**match dscp** *dscp-value-for-video* **Example:** `Switch(config-cmap)# match dscp 34`	Matches the DSCP value in the IPv4 and IPv6 packets. Set this value to 34.

	Command or Action	Purpose
Step 8	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-z** to exit global configuration mode.

Configuring Client Policies

Before You Begin

You must have the following features configured before configuring client policies:

- Access lists
- Access group name

SUMMARY STEPS

1. **configure terminal**
2. **ip access-list extended** *ext-name*
3. **permit ip host** *host-ip-address*
4. **end**
5. **configure terminal**
6. **class map** *acl-name*
7. **match access-group name** *access-list-name*
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**ip access-list extended** *ext-name* **Example:** `Switch(config)# ip access-list extended`	Configures a named access list.

	Command or Action	Purpose
Step 3	**permit ip host** *host-ip-address* **Example:** `Switch(config-ext-nacl)# permit ip host 203.0.113.3 host 203.0.113.5`	Configures IP protocol traffic from a source address to a destination address.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-z** to exit global configuration mode.
Step 5	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 6	**class map** *acl-name* **Example:** `Switch(config)# class-map acl-a1`	Configures the class map name.
Step 7	**match access-group name** *access-list-name* **Example:** `Switch(config-cmap)# match access-group name a1`	Assigns the class map to an access group name.
Step 8	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-z** to exit global configuration mode.

Configuring Table Maps

SUMMARY STEPS

1. **configure terminal**
2. table-map *table-map-name*
3. **map from** *from-value* **to** *to-value*
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	table-map *table-map-name* **Example:** `Switch(config)# table-map mutate-dscp`	Create the table map.

Step 3	**map from** *from-value* **to** *to-value*
	
	Example:
	
	`Switch(config-tablemap)# map from 10 to 34`
	`Switch(config-tablemap)# map from 34 to 40`
	`Switch(config-tablemap)# map from 46 to 48`
		Map a to value to a from value.

Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-z** to exit global configuration mode.

Applying an SSID Policy

Before You Begin

You must have a service-policy map configured before applying it on an SSID.

SUMMARY STEPS

1. **configure terminal**
2. **wlan** *wlan-name*
3. **service-policy** [**client**] **qos** [**input** | **output**] *ssid-policy-name*
4. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**wlan** *wlan-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *wlan-name* is the profile name of the configured WLAN.
Step 3	**service-policy** [**client**] **qos** [**input** | **output**] *ssid-policy-name* **Example:** `Switch(config-wlan)# service-policy input policy-map-ssid`	Applies the policy. The following options are available: • **input**: Assigns the policy map to WLAN input traffic. • **output**: Assigns the policy map to WLAN output traffic. • **client**: Assigns the policy map to all clients on the WLAN.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-z** to exit global configuration mode.

What to Do Next

Proceed to configure client policies.

Configuration Examples

Examples: Wireless QoS Policy Classified by Voice, Video, and Multicast Traffic

The following example provides a template for creating a port child policy for managing quality of service for voice and video traffic.

```
Policy-map port_child_policy
    Class voice (match dscp ef)
            Priority level 1
            Police  Multicast Policer
    Class video (match dscp af11)
            Priority level 2
            Police  Multicast Policer
    Class mcast-data  (match non-client-nrt)
            Bandwidth remaining ratio <>
    Class class-default  (NRT Data)
            Bandwidth remaining ratio <>
Policy-map parent_port
    Class class-default
         Shape average    Port Shaper
         Service-policy port_child_policy
```

Note Multicast Policer in the example above is not a keyword. It refers to the policing policy configured.

Two class maps with name voice and video are configured with DSCP assignments of 46 and 34. The voice traffic is assigned the priority of 1 and the video traffic is assigned the priority level 2 and is processed using Q0 and Q1. If your network receives multicast voice and video traffic, you can configure multicast policers. The non-client NRT data and NRT data are processed using the Q2 and Q3 queues.

Related Topics

Queuing in Wireless, on page 13
Port Policy Format, on page 11
Port, on page 8

Examples: SSID Policy

SSID Policy 1

The following is an example of an SSID policy for voice and video:

```
Policy-map enterprise-ssid-1
     Class  voice (match dscp ef)
          Priority level 1
         Police Unicast Policer
Class video (match dscp af11)
        Priority level 2
        Police Unicast Policer
Policy-map ssid-shaper
Class class-default  (NRT Data)
        queue-buffer 0
        shape average 100000000
        set wlan-user-priority dscp table dscp2up
        set dscp dscp table dscp2dscp
        service-policy  enterprise-ssid-1
```

SSID Policy 2

The following is an example of SSID policy configured with an average SSID shaping rate:

```
Policy-map enterprise-ssid-2
     Class  voice (match dscp af11)
          Priority level 1
         Police Unicast Policer
Class video (match dscp  ef)
        Priority level 2
        Police Unicast Policer
Policy-map ssid-shaper
Class class-default  (NRT Data)
       shape average 1000000000
       service-policy enterprise-ssid-2
       set wlan-user-priority dscp table dscp2up
       set dscp dscp table dscp2dscp
```

Related Topics

SSID, on page 9

Examples: Configuring Downstream BSSID Policy

To configure a downstream BSSID policy, you must first configure a port child policy with priority level queuing.

Configuring a User-Defined Port Child Policy

The following is an example of configuring a user-defined port child policy:

```
policy-map port_child_policy
   class voice
     priority level 1 20000

   class video
     priority level 2 10000

   class non-client-nrt-class
     bandwidth remaining ratio 10

   class class-default
     bandwidth remaining ratio 15
```

Configuring Downstream BSSID Policy

The following configuration example displays how to configure a downstream BSSID policy:

```
policy-map bssid-policer
   class class-default
   shape average 30000000
set dscp dscp table dscp2dscp
set wlan user-priority dscp table dscp2up
service-policy ssid_child_qos
```

The SSID child QoS policy may be defined as below:

```
Policy Map ssid-child_qos
    Class voice
      priority level 1
      police cir 5m
      admit cac wmm-tspec
           UP 6,7  / tells WCM allow 'voice' TSPEC\SIP snoop for this ssid
            rate 4000 / must be police rate value is in kbps)
   Class video
      priority level 2
      police cir 60000
```

Related Topics

SSID, on page 9

Examples: Client Policies

The following example shows a default client policy in the downstream direction. Any incoming traffic contains the user-priority as 0:

```
Policy-map client-def-down
  class class-default
      set wlan user-priority 0
```

The following example shows the default client policy in the upstream direction. Any traffic that is sent to the wired network from wireless network will result in the DSCP value being set to 0.

```
Policy-map client-def-up
   class class-default
    set dscp 0
```

The following examples shows client policies that are generated automatically and applied to the client when the client authenticates to a profile in AAA with a QoS-level attribute configured.

```
Policy Map platinum-WMM
Class voice-plat
  set wlan user-priority 6
 Class video-plat
 set wlan user-priority 4
Class class-default
  set wlan user-priority 0

Policy Map gold-WMM
Class voice-gold
  set wlan user-priority 4
 Class video-gold
 set wlan user-priority 4
Class class-default
  set wlan user-priority 0
```

The following is an example of client precious metal policies:

```
Policy Map platinum
  set wlan user-priority 6
```

Any traffic matching class voice1 the user priority is set to a pre-defined value. The class can be set to assign a DSCP or ACL.

```
Policy Map client1-down
Class voice1     //match dscp, cos
  set wlan user-priority <>
Class voice2    //match acl
   set wlan user-priority <>
Class voice3
   set wlan user-priority <>
Class class-default
  set wlan user-priority 0
```

The following is an example of a client policy based on AAA and TCLAS:

```
Policy Map client2-down[ AAA+ TCLAS pol example]
Class      voice\\match dscp
      police <>
      set <>
Class class-default
    set <>
Class voice1|| voice2 [match acls]
      police <>
      class voice1
        set <>
      class voice2
        set <>
```

The following is an example of a client policy for voice and video for traffic in the downstream direction:

```
Policy Map client3-down
    class voice \\match dscp, cos
          police X
     class video
         police Y
    class default
        police Z
```

The following is an example of a client policy for voice and video for traffic in the upstream direction using policing:

```
Policy Map client1-up
    class voice     \\match dscp, up, cos
```

```
      police X
    class video
     police Y
  class class-default
    police Z
```

The following is an example of a client policy for voice and video based on DSCP:

```
Policy Map client2-up
    class voice     \\match dscp, up, cos
set dscp <>
    class video
     set dscp <>
  class class-default
    set dscp <>
```

Related Topics

Client, on page 9

Additional References

Related Documents

Related Topic	Document Title
QoS Command Reference	*QoS Command Reference (Catalyst 3850 Switches)*
Mobility Configuration Guide	*Mobility Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*
Quality of Service Solutions Configuration Guide (Cisco IOS Software)	*Quality of Service Solutions Configuration Guide Library, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*

MIBs

MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS 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/support