



QoS Commands

- [class](#), on page 1
- [class-map](#), on page 4
- [match \(class-map configuration\)](#), on page 5
- [match non-client-nrt](#), on page 8
- [match wlan user-priority](#), on page 8
- [policy-map](#), on page 9
- [priority](#), on page 11
- [queue-buffers ratio](#), on page 13
- [queue-limit](#), on page 14
- [qos wireless-default untrust](#), on page 15
- [service-policy \(Wired\)](#), on page 16
- [service-policy \(WLAN\)](#), on page 17
- [set](#), on page 18
- [show ap name service-policy](#), on page 24
- [show ap name dot11](#), on page 25
- [show class-map](#), on page 28
- [show platform hardware fed switch](#), on page 28
- [show platform software fed switch qos](#), on page 31
- [show platform software fed switch qos qsb](#), on page 32
- [show wireless client calls](#), on page 34
- [show wireless client dot11](#), on page 35
- [show wireless client mac-address \(Call Control\)](#), on page 36
- [show wireless client mac-address \(TCLAS\)](#), on page 36
- [show wireless client voice diagnostics](#), on page 37
- [show policy-map](#), on page 38
- [show wlan](#), on page 40
- [trust device](#), on page 42

class

To define a traffic classification match criteria for the specified class-map name, use the **class** command in policy-map configuration mode. Use the **no** form of this command to delete an existing class map.

```
class {class-map-name | class-default}
no class {class-map-name | class-default}
```

Syntax Description

class-map-name The class map name.

class-default Refers to a system default class that matches unclassified packets.

Command Default

No policy map class-maps are defined.

Command Modes

Policy-map configuration

Command History**Release****Modification**

Cisco IOS XE 3.2SE Cisco IOS XE 3.3SE Cisco IOS XE 3.3SE This command was introduced.

Usage Guidelines

Before using the **class** command, you must use the **policy-map** global configuration command to identify the policy map and enter policy-map configuration mode. After specifying a policy map, you can configure a policy for new classes or modify a policy for any existing classes in that policy map. You attach the policy map to a port by using the **service-policy** interface configuration command.

After entering the **class** command, you enter the policy-map class configuration mode. These configuration commands are available:

- **admit**—Admits a request for Call Admission Control (CAC)
- **bandwidth**—Specifies the bandwidth allocated to the class.
- **exit**—Exits the policy-map class configuration mode and returns to policy-map configuration mode.
- **no**—Returns a command to its default setting.
- **police**—Defines a policer or aggregate policer for the classified traffic. The policer specifies the bandwidth limitations and the action to take when the limits are exceeded. For more information about this command, see *Cisco IOS Quality of Service Solutions Command Reference* available on Cisco.com.
- **priority**—Assigns scheduling priority to a class of traffic belonging to a policy map.
- **queue-buffers**—Configures the queue buffer for the class.
- **queue-limit**—Specifies the maximum number of packets the queue can hold for a class policy configured in a policy map.
- **service-policy**—Configures a QoS service policy.
- **set**—Specifies a value to be assigned to the classified traffic. For more information, see [set, on page 18](#)
- **shape**—Specifies average or peak rate traffic shaping. For more information about this command, see *Cisco IOS Quality of Service Solutions Command Reference* available on Cisco.com.

To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

The **class** command performs the same function as the **class-map** global configuration command. Use the **class** command when a new classification, which is not shared with any other ports, is needed. Use the **class-map** command when the map is shared among many ports.

You can configure a default class by using the **class class-default** policy-map configuration command. Unclassified traffic (traffic that does not meet the match criteria specified in the traffic classes) is treated as default traffic.

You can verify your settings by entering the **show policy-map** privileged EXEC command.

Examples

This example shows how to create a policy map called policy1. When attached to the ingress direction, it matches all the incoming traffic defined in class1, sets the IP Differentiated Services Code Point (DSCP) to 10, and polices the traffic at an average rate of 1 Mb/s and bursts at 20 KB. Traffic exceeding the profile is marked down to a DSCP value gotten from the policed-DSCP map and then sent.

```
Device(config)# policy-map policy1
Device(config-pmap)# class class1
Device(config-pmap-c)# set dscp 10
Device(config-pmap-c)# police 1000000 20000 exceed-action policed-dscp-transmit
Device(config-pmap-c)# exit
```

This example shows how to configure a default traffic class to a policy map. It also shows how the default traffic class is automatically placed at the end of policy-map pm3 even though **class-default** was configured first:

```
Device# configure terminal
Device(config)# class-map cm-3
Device(config-cmap)# match ip dscp 30
Device(config-cmap)# exit

Device(config)# class-map cm-4
Device(config-cmap)# match ip dscp 40
Device(config-cmap)# exit

Device(config)# policy-map pm3
Device(config-pmap)# class class-default
Device(config-pmap-c)# set dscp 10
Device(config-pmap-c)# exit

Device(config-pmap)# class cm-3
Device(config-pmap-c)# set dscp 4
Device(config-pmap-c)# exit

Device(config-pmap)# class cm-4
Device(config-pmap-c)# set precedence 5
Device(config-pmap-c)# exit
Device(config-pmap)# exit

Device# show policy-map pm3
Policy Map pm3
  Class cm-3
    set dscp 4
  Class cm-4
    set precedence 5
  Class class-default
    set dscp af11
```

Related Topics

- [class-map](#), on page 4
- [policy-map](#), on page 9
- [show policy-map](#), on page 38
- [set](#), on page 18

class-map

To create a class map to be used for matching packets to the class whose name you specify and to enter class-map configuration mode, use the **class-map** command in global configuration mode. Use the **no** form of this command to delete an existing class map and to return to global or policy map configuration mode.

class-map [{*match-anytype*}] *class-map-name*
no class-map [{*match-anytype*}] *class-map-name*

| Syntax Description | |
|-----------------------|--|
| match-any | (Optional) Perform a logical-OR of the matching statements under this class map. One or more criteria must be matched. |
| type | (Optional) Configures the CPL class map. |
| <i>class-map-name</i> | The class map name. |

Command Default No class maps are defined.

Command Modes Global configuration
 Policy map configuration

| Command History | Release | Modification |
|-----------------|--|------------------------------------|
| | Cisco IOS XE 3.2SE Cisco IOS XE 3.3SE Cisco IOS XE 3.3SE | This command was introduced. |
| | Cisco IOS XE 3.3SE | The type keyword was added. |

Usage Guidelines Use this command to specify the name of the class for which you want to create or modify class-map match criteria and to enter class-map configuration mode.

The **class-map** command and its subcommands are used to define packet classification, marking, and aggregate policing as part of a globally named service policy applied on a per-port basis.

After you are in quality of service (QoS) class-map configuration mode, these configuration commands are available:

- **description**—Describes the class map (up to 200 characters). The **show class-map** privileged EXEC command displays the description and the name of the class map.
- **exit**—Exits from QoS class-map configuration mode.
- **match**—Configures classification criteria.
- **no**—Removes a match statement from a class map.

If you enter the **match-any** keyword, you can only use it to specify an extended named access control list (ACL) with the **match access-group** class-map configuration command.

To define packet classification on a physical-port basis, only one **match** command per class map is supported.

The ACL can have multiple access control entries (ACEs).

Examples

This example shows how to configure the class map called class1 with one match criterion, which is an access list called 103:

```
Device(config)# access-list 103 permit ip any any dscp 10
Device(config)# class-map class1
Device(config-cmap)# match access-group 103
Device(config-cmap)# exit
```

This example shows how to delete the class map class1:

```
Device(config)# no class-map class1
```

You can verify your settings by entering the **show class-map** privileged EXEC command.

Related Topics

[policy-map](#), on page 9

[show policy-map](#), on page 38

match (class-map configuration)

To define the match criteria to classify traffic, use the **match** command in class-map configuration mode. Use the **no** form of this command to remove the match criteria.

```
match {access-group{nameacl-name acl-index} | class-map class-map-name | cos cos-value | dscp
dscp-value | [ip] dscp dscp-list | [ip] precedence ip-precedence-list | precedence
precedence-value1...value4 | qos-group qos-group-value | vlan vlan-id}
no match {access-group{nameacl-name acl-index} | class-map class-map-name | cos cos-value | dscp
dscp-value | [ip] dscp dscp-list | [ip] precedence ip-precedence-list | precedence
precedence-value1...value4 | qos-group qos-group-value | vlan vlan-id}
```

Syntax Description

| | |
|--|---|
| access-group | Specifies an access group. |
| name <i>acl-name</i> | Specifies the name of an IP standard or extended access control list (ACL) or MAC ACL. |
| <i>acl-index</i> | Specifies the number of an IP standard or extended access control list (ACL) or MAC ACL. For an IP standard ACL, the ACL index range is 1 to 99 and 1300 to 1999. For an IP extended ACL, the ACL index range is 100 to 199 and 2000 to 2699. |
| class-map <i>class-map-name</i> | Uses a traffic class as a classification policy and specifies a traffic class name to use as the match criterion. |

| | |
|---|--|
| cos <i>cos-value</i> | Matches a packet on the basis of a Layer 2 class of service (CoS)/Inter-Switch Link (ISL) marking. The cos-value is from 0 to 7. You can specify up to four CoS values in one match cos statement, separated by a space. |
| dscp <i>dscp-value</i> | Specifies the parameters for each DSCP value. You can specify a value in the range 0 to 63 specifying the differentiated services code point value. |
| ip dscp <i>dscp-list</i> | Specifies a list of up to eight IP Differentiated Services Code Point (DSCP) values to match against incoming packets. Separate each value with a space. The range is 0 to 63. You also can enter a mnemonic name for a commonly used value. |
| ip precedence <i>ip-precedence-list</i> | Specifies a list of up to eight IP-precedence values to match against incoming packets. Separate each value with a space. The range is 0 to 7. You also can enter a mnemonic name for a commonly used value. |
| precedence <i>precedence-value1...value4</i> | Assigns an IP precedence value to the classified traffic. The range is 0 to 7. You also can enter a mnemonic name for a commonly used value. |
| qos-group <i>qos-group-value</i> | Identifies a specific QoS group value as a match criterion. The range is 0 to 31. |
| vlan <i>vlan-id</i> | Identifies a specific VLAN as a match criterion. The range is 1 to 4095. |

Command Default

No match criteria are defined.

Command Modes

Class-map configuration

Command History

| Release | Modification |
|--|--|
| Cisco IOS XE 3.2SE Cisco IOS XE 3.3SE Cisco IOS XE 3.3SE | This command was introduced. |
| Cisco IOS XE 3.3SE | The class-map <i>class-map-name</i> , cos <i>cos-value</i> , qos-group <i>qos-group-value</i> , and vlan <i>vlan-id</i> keywords were added. |

Usage Guidelines

The **match** command is used to specify which fields in the incoming packets are examined to classify the packets. Only the IP access group or the MAC access group matching to the Ether Type/Len are supported.

If you enter the **class-map match-any** *class-map-name* global configuration command, you can enter the following **match** commands:

- **match access-group** *name acl-name*



Note The ACL must be an extended named ACL.

- **match ip dscp** *dscp-list*
- **match ip precedence** *ip-precedence-list*

The **match access-group** *acl-index* command is not supported.

To define packet classification on a physical-port basis, only one **match** command per class map is supported. In this situation, the **match-any** keyword is equivalent.

For the **match ip dscp** *dscp-list* or the **match ip precedence** *ip-precedence-list* command, you can enter a mnemonic name for a commonly used value. For example, you can enter the **match ip dscp af11** command, which is the same as entering the **match ip dscp 10** command. You can enter the **match ip precedence critical** command, which is the same as entering the **match ip precedence 5** command. For a list of supported mnemonics, enter the **match ip dscp ?** or the **match ip precedence ?** command to see the command-line help strings.

Use the **input-interface** *interface-id-list* keyword when you are configuring an interface-level class map in a hierarchical policy map. For the *interface-id-list*, you can specify up to six entries.

Examples

This example shows how to create a class map called class2, which matches all the incoming traffic with DSCP values of 10, 11, and 12:

```
Device(config)# class-map class2
Device(config-cmap)# match ip dscp 10 11 12
Device(config-cmap)# exit
```

This example shows how to create a class map called class3, which matches all the incoming traffic with IP-precedence values of 5, 6, and 7:

```
Device(config)# class-map class3
Device(config-cmap)# match ip precedence 5 6 7
Device(config-cmap)# exit
```

This example shows how to delete the IP-precedence match criteria and to classify traffic using acl1:

```
Device(config)# class-map class2
Device(config-cmap)# match ip precedence 5 6 7
Device(config-cmap)# no match ip precedence
Device(config-cmap)# match access-group acl1
Device(config-cmap)# exit
```

This example shows how to specify a list of physical ports to which an interface-level class map in a hierarchical policy map applies:

```
Device(config)# class-map match-any class4
Device(config-cmap)# match cos 4
Device(config-cmap)# exit
```

This example shows how to specify a range of physical ports to which an interface-level class map in a hierarchical policy map applies:

```
Device(config)# class-map match-any class4
Device(config-cmap)# match cos 4
```

```
Device(config-cmap) # exit
```

You can verify your settings by entering the **show class-map** privileged EXEC command.

match non-client-nrt

To match non-client NRT (non-real-time), use the **match non-client-nrt** command in class-map configuration mode. Use the **no** form of this command to return to the default setting.

```
match non-client-nrt  
no match non-client-nrt
```

| | | |
|---------------------------|--|------------------------------|
| Syntax Description | This command has no arguments or keywords. | |
| Command Default | None | |
| Command Modes | Class-map | |
| Command History | Release | Modification |
| | Cisco IOS XE 3.2SE Cisco IOS XE 3.3SE Cisco IOS XE 3.3SE | This command was introduced. |
| Usage Guidelines | None | |

This example show how you can configure non-client NRT:

```
Device(config) # class-map test_1000  
Device(config-cmap) # match non-client-nrt
```

match wlan user-priority

To match 802.11 specific values, use the **match wlan user-priority** command in class-map configuration mode. Use the **no** form of this command to return to the default setting.

```
match wlan user-priority wlan-value [wlan-value] [wlan-value] [wlan-value]  
no match wlan user-priority wlan-value [wlan-value] [wlan-value] [wlan-value]
```

| | |
|---------------------------|---|
| Syntax Description | <i>wlan-value</i> The 802.11-specific values. Enter the user priority 802.11 TID user priority (0-7). (Optional) Enter up to three user priority values separated by white-spaces. |
| Command Default | None |
| Command Modes | Class-map |
| Command History | Release |
| | Cisco IOS XE 3.2SE Cisco IOS XE 3.3SE Cisco IOS XE 3.3SE |
| | Modification |
| | This command was introduced. |

Usage Guidelines None

This example show how you can configure user-priority values:

```
Device(config)# class-map test_1000
Device(config-cmap)# match wlan user-priority 7
```

policy-map

To create or modify a policy map that can be attached to multiple physical ports or switch virtual interfaces (SVIs) and to enter policy-map configuration mode, use the **policy-map** command in global configuration mode. Use the **no** form of this command to delete an existing policy map and to return to global configuration mode.

policy-map *policy-map-name*
no policy-map *policy-map-name*

Syntax Description *policy-map-name* Name of the policy map.

Command Default No policy maps are defined.

Command Modes Global configuration

| Command History | Release | Modification |
|-----------------|--------------------|------------------------------|
| | Cisco IOS XE 3.2SE | Cisco IOS XE 3.3SE |
| | Cisco IOS XE 3.3SE | This command was introduced. |

Usage Guidelines After entering the **policy-map** command, you enter policy-map configuration mode, and these configuration commands are available:

- **class**—Defines the classification match criteria for the specified class map.
- **description**—Describes the policy map (up to 200 characters).
- **exit**—Exits policy-map configuration mode and returns you to global configuration mode.
- **no**—Removes a previously defined policy map.
- **sequence-interval**—Enables sequence number capability.

To return to global configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

Before configuring policies for classes whose match criteria are defined in a class map, use the **policy-map** command to specify the name of the policy map to be created, added to, or modified. Entering the **policy-map** command also enables the policy-map configuration mode in which you can configure or modify the class policies for that policy map.

You can configure class policies in a policy map only if the classes have match criteria defined for them. To configure the match criteria for a class, use the **class-map** global configuration and **match** class-map configuration commands. You define packet classification on a physical-port basis.

Only one policy map per ingress port is supported. You can apply the same policy map to multiple physical ports.

You can apply a nonhierarchical policy maps to physical ports. A nonhierarchical policy map is the same as the port-based policy maps in the device.

A hierarchical policy map has two levels in the format of a parent-child policy. The parent policy cannot be modified but the child policy (port-child policy) can be modified to suit the QoS configuration.

In VLAN-based QoS, a service policy is applied to an SVI interface. All physical interfaces belonging to a VLAN policy map then need to be configured to refer to the VLAN-based policy maps instead of the port-based policy map.



Note Not all MQC QoS combinations are supported for wired and wireless ports. For information about these restrictions, see chapters "Restrictions for QoS on Wired Targets" and "Restrictions for QoS on Wireless Targets" in the QoS configuration guide.

Examples

This example shows how to create a policy map called policy1. When attached to the ingress port, it matches all the incoming traffic defined in class1, sets the IP DSCP to 10, and polices the traffic at an average rate of 1 Mb/s and bursts at 20 KB. Traffic less than the profile is sent.

```
Device(config)# policy-map policy1
Device(config-pmap)# class class1
Device(config-pmap-c)# set dscp 10
Device(config-pmap-c)# police 1000000 20000 conform-action transmit
Device(config-pmap-c)# exit
```

This example show you how to configure hierarchical polices:

```
Switch# configure terminal
Device(config)# class-map c1
Device(config-cmap)# exit

Device(config)# class-map c2
Device(config-cmap)# exit

Device(config)# policy-map child
Device(config-pmap)# class c1
Device(config-pmap-c)# priority level 1
Device(config-pmap-c)# police rate percent 20 conform-action transmit exceed action drop
Device(config-pmap-c-police)# exit
Device(config-pmap-c)# exit

Device(config-pmap)# class c2
Device(config-pmap-c)# bandwidth 20000
Device(config-pmap-c)# exit

Device(config-pmap)# class class-default
Device(config-pmap-c)# bandwidth 20000
Device(config-pmap-c)# exit
Device(config-pmap)# exit

Device(config)# policy-map parent
Device(config-pmap)# class class-default
Device(config-pmap-c)# shape average 1000000
Device(config-pmap-c)# service-policy child
```

```
Deviceconfig-pmap-c) # end
```

This example shows how to delete a policy map:

```
Device(config) # no policy-map policymap2
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

Related Topics

[class](#), on page 1

[class-map](#), on page 4

[service-policy \(Wired\)](#), on page 16

[show policy-map](#), on page 38

priority

To assign priority to a class of traffic belonging to a policy map, use the **priority** command in policy-map class configuration mode. To remove a previously specified priority for a class, use the **no** form of this command.

```
priority [Kbps [burst -in-bytes] ] | level level-value [Kbps [burst -in-bytes] ] | percent
percentage [Kb/s [burst -in-bytes] ] ]
no priority [Kb/s [burst -in-bytes] ] | level level value [Kb/s [burst -in-bytes] ] | percent
percentage [Kb/s [burst -in-bytes] ] ]
```

| Syntax Description | |
|----------------------------------|---|
| <i>Kb/s</i> | (Optional) Guaranteed allowed bandwidth, in kilobits per second (kbps), for the priority traffic. The amount of guaranteed bandwidth varies according to the interface and platform in use. Beyond the guaranteed bandwidth, the priority traffic will be dropped in the event of congestion to ensure that the nonpriority traffic is not starved. The value must be between 1 and 2,000,000 kbps. |
| <i>burst -in-bytes</i> | (Optional) Burst size in bytes. The burst size configures the network to accommodate temporary bursts of traffic. The default burst value, which is computed as 200 milliseconds of traffic at the configured bandwidth rate, is used when the burst argument is not specified. The range of the burst is from 32 to 2000000 bytes. |
| level <i>level-value</i> | (Optional) Assigns priority level. Available values for <i>level-value</i> are 1 and 2. Level 1 is a higher priority than Level 2. Level 1 reserves bandwidth and goes first, so latency is very low. Reserve the bandwidth even if you do not use it. Both levels 1 and 2 can reserve bandwidth. |
| percent <i>percentage</i> | (Optional) Specifies the amount of guaranteed bandwidth to be specified by the percent of available bandwidth. |

Command Default No priority is set.

Command Modes Policy-map class configuration

| Command History | Release | Modification |
|-----------------|--|---|
| | Cisco IOS XE 3.2SE Cisco IOS XE 3.3SE Cisco IOS XE 3.3SE | This command was introduced. |
| | Cisco IOS XE 3.3SE | The <i>Kbps</i> , <i>burst -in-bytes</i> , and percent percentage keywords were added. |

Usage Guidelines This command configures low latency queuing (LLQ), providing strict priority queuing (PQ) for class-based weighted fair queuing (CBWFQ). Strict PQ allows delay-sensitive data such as voice to be dequeued and sent before packets in other queues are dequeued.



Note You can configure a priority only with a level.

Only one strict priority or priority with levels is allowed in one policy-map. Multiple priorities with same priority levels without kbps/percent are allowed in a policy-map only if all of them are configured with police.

The priority command allows you to set up classes based on a variety of criteria (not just User Datagram Ports [UDP] ports) and assign priority to them, and is available for use on serial interfaces and ATM permanent virtual circuits (PVCs). A similar command, the **ip rtp priority** command, allows you to stipulate priority flows based only on UDP port numbers and is not available for ATM PVCs.

When the device is not congested, the priority class traffic is allowed to exceed its allocated bandwidth. When the device is congested, the priority class traffic above the allocated bandwidth is discarded.

The bandwidth and priority commands cannot be used in the same class, within the same policy map. However, these commands can be used together in the same policy map.

Within a policy map, you can give one or more classes priority status. When multiple classes within a single policy map are configured as priority classes, all traffic from these classes is queued to the same, single, priority queue.

When the policy map containing class policy configurations is attached to the interface to stipulate the service policy for that interface, available bandwidth is assessed. If a policy map cannot be attached to a particular interface because of insufficient interface bandwidth, the policy is removed from all interfaces to which it was successfully attached.

Example

The following example shows how to configure the priority of the class in policy map policy1:

```
Device(config)# class-map cml
Device(config-cmap)#match precedence 2
Device(config-cmap)#exit

Device(config)#class-map cm2
Device(config-cmap)#match dscp 30
Device(config-cmap)#exit

Device(config)# policy-map policy1
Device(config-pmap)# class cml
Device(config-pmap-c)# priority level 1
```

```

Device(config-pmap-c) # police 1m
Device(config-pmap-c-police) #exit
Device(config-pmap-c) #exit
Device(config-pmap) #exit

Device(config) #policy-map policy1
Device(config-pmap) #class cm2
Device(config-pmap-c) #priority level 2
Device(config-pmap-c) #police 1m

```

queue-buffers ratio

To configure the queue buffer for the class, use the **queue-buffers ratio** command in policy-map class configuration mode. Use the **no** form of this command to remove the ratio limit.

```

queue-buffers ratio ratio limit
no queue-buffers ratio ratio limit

```

| Syntax Description | <i>ratio limit</i> (Optional) Configures the queue buffer for the class. Enter the queue buffers ratio limit (0-100). | | | | |
|---------------------------|--|---------|--------------|--------------------|---|
| Command Default | No queue buffer for the class is defined. | | | | |
| Command Modes | Policy-map class configuration (config-pmap-c) | | | | |
| Command History | <table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.2SE</td> <td>Cisco IOS XE 3.3SE This command was introduced.</td> </tr> </tbody> </table> | Release | Modification | Cisco IOS XE 3.2SE | Cisco IOS XE 3.3SE This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE 3.2SE | Cisco IOS XE 3.3SE This command was introduced. | | | | |
| Usage Guidelines | <p>Either the bandwidth, shape, or priority command must be used before using this command. For more information about these commands, see <i>Cisco IOS Quality of Service Solutions Command Reference</i> available on Cisco.com</p> <p>The <code>queue-buffers ratio</code> allows you to allocate buffers to queues. If buffers are not allocated, then they are divided equally amongst all queues. You can use the queue-buffer ratio to divide it in a particular ratio. The buffers are soft buffers because Dynamic Threshold and Scaling (DTS) is active on all queues by default.</p> | | | | |

Example

The following example sets the queue buffers ratio to 10 percent:

```

Device(config) # policy-map policy_queuebuf01
Device(config-pmap) # class-map class_queuebuf01
Device(config-cmap) # exit
Device(config) # policy policy_queuebuf01
Device(config-pmap) # class class_queuebuf01
Device(config-pmap-c) # bandwidth percent 80
Device(config-pmap-c) # queue-buffers ratio 10
Device(config-pmap) # end

```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

Related Topics

[show policy-map](#), on page 38

queue-limit

To specify or modify the maximum number of packets the queue can hold for a class policy configured in a policy map, use the **queue-limit** policy-map class configuration command. To remove the queue packet limit from a class, use the **no** form of this command.

```
queue-limit queue-limit-size [{packets}] {cos cos-value | dscp dscp-value} percent percentage-of-packets
no queue-limit queue-limit-size [{packets}] {cos cos-value | dscp dscp-value} percent
percentage-of-packets
```

| Syntax Description | | |
|---|--|---|
| <i>queue-limit-size</i> | | The maximum size of the queue. The maximum varies according to the optional unit of measure keyword specified (bytes, ms, us, or packets). |
| cos <i>cos-value</i> | | Specifies parameters for each cos value. CoS values are from 0 to 7. |
| dscp <i>dscp-value</i> | | Specifies parameters for each DSCP value. You can specify a value in the range 0 to 63 specifying the differentiated services code point value for the type of queue limit . |
| percent <i>percentage-of-packets</i> | | A percentage in the range 1 to 100 specifying the maximum percentage of packets that the queue for this class can accumulate. |

Command Default None

Command Modes Policy-map class configuration

| Command History | Release | Modification |
|-----------------|--|------------------------------|
| | Cisco IOS XE 3.2SE Cisco IOS XE 3.3SE Cisco IOS XE 3.3SE | This command was introduced. |

Usage Guidelines Although visible in the command line help-strings, the **packets** unit of measure is not supported; use the **percent** unit of measure.



Note This command is supported only on wired ports in the egress direction.

Weighted fair queuing (WFQ) creates a queue for every class for which a class map is defined. Packets satisfying the match criteria for a class accumulate in the queue reserved for the class until they are sent, which occurs when the queue is serviced by the fair queuing process. When the maximum packet threshold you defined for the class is reached, queuing of any further packets to the class queue causes tail drop.

You use queue limits to configure Weighted Tail Drop (WTD). WTD ensures the configuration of more than one threshold per queue. Each class of service is dropped at a different threshold value to provide for QoS differentiation.

You can configure the maximum queue thresholds for the different subclasses of traffic, that is, DSCP and CoS and configure the maximum queue thresholds for each subclass.

Example

The following example configures a policy map called port-queue to contain policy for a class called dscp-1. The policy for this class is set so that the queue reserved for it has a maximum packet limit of 20 percent:

```
Device(config)# policy-map policy11
Device(config-pmap)# class dscp-1
Device(config-pmap-c)# bandwidth percent 20
Device(config-pmap-c)# queue-limit dscp 1 percent 20
```

qos wireless-default untrust

To configure the default trust behavior to untrust wireless packets, use the **qos wireless-default untrust** command. To configure the default trust behavior of wireless traffic to trust, use the **no** form of the command.

```
qos wireless-default-untrust
no qos wireless-default-untrust
```

Syntax Description

This command has no arguments or keywords.

Command Default

By default, the wireless traffic is trusted.

By default, the wireless traffic is untrusted.

To check the trust behavior on the device, use the **show running-config | sec qos** or the **show run | include untrust** command.

Command Modes

Configuration

Command History

| Release | Modification |
|--------------------|------------------------------|
| Cisco IOS XE 3.3SE | This command was introduced. |

Usage Guidelines



Note The default trust behavior of wireless traffic was untrusted in the Cisco IOS XE 3.2 SE release.



Note If you upgrade from Cisco IOS XE 3.2 SE Release to a later release, the default behavior of the wireless traffic is still untrusted. In this situation, you can use the **no qos wireless-default untrust** command to enable trust behavior for wireless traffic. However, if you install Cisco IOS XE 3.3 SE or a later release on the device, the default QoS behavior for wireless traffic is trust. Starting with Cisco IOS XE 3.3 SE Release and later, the packet markings are preserved in both egress and ingress directions for new installations (not upgrades) for wireless traffic.

The Cisco IOS XE 3.2 Release supported different trust defaults for wired and wireless ports. The trust default for wired ports was the same as for this software release. For wireless ports, the default system behavior was non-trust, which meant that when the came up, all markings for the wireless ports were defaulted to zero and no traffic received priority treatment. For compatibility with an existing wired , all traffic went to the best-effort queue by default. The access point performed priority queuing by default. In the downstream direction, the access point maintained voice, video, best-effort, and background queues for queuing. The access selected the queuing strategy based on the 11e tag information. By default, the access point treated all wireless packets as best effort.

The following command changes the default behavior for trusting wireless traffic to untrust.

```
Device(config)# qos wireless-default-untrust
```

service-policy (Wired)

To apply a policy map to a physical port or a switch virtual interface (SVI), use the **service-policy** command in interface configuration mode. Use the **no** form of this command to remove the policy map and port association.

```
service-policy {input | output} policy-map-name
no service-policy {input | output} policy-map-name
```

| Syntax Description | |
|--------------------------------------|--|
| input <i>policy-map-name</i> | Apply the specified policy map to the input of a physical port or an SVI. |
| output <i>policy-map-name</i> | Apply the specified policy map to the output of a physical port or an SVI. |

Command Default No policy maps are attached to the port.

Command Modes WLAN interface configuration

| Command History | Release | Modification |
|-----------------|--|--|
| | Cisco IOS XE 3.2SE Cisco IOS XE 3.3SE | Cisco IOS XE 3.3SE This command was introduced. |

Usage Guidelines A policy map is defined by the **policy map** command.

Only one policy map is supported per port, per direction. In other words, only one input policy and one output policy is allowed on any one port.

You can apply a policy map to incoming traffic on a physical port or on an SVI. *QoS Configuration Guide (Cisco WLC 5700 Series)*/*QoS Configuration Guide (Catalyst 3650 Switches)*.



Note Though visible in the command-line help strings, the **history** keyword is not supported, and you should ignore the statistics that it gathers.

Examples

This example shows how to apply plcmap1 to an ingress port:

```
Device(config)# interface gigabitEthernet2/0/1
Device(config-if)# service-policy input plcmap1
```

This example shows how to remove plcmap2 from a physical port:

```
Device(config)# interface gigabitEthernet2/0/2
Device(config-if)# no service-policy input plcmap2
```

The following example displays a VLAN policer configuration. At the end of this configuration, the VLAN policy map is applied to an interface for QoS:

```
Device# configure terminal
Device(config)# class-map vlan100
Device(config-cmap)# match vlan 100
Device(config-cmap)# exit
Device(config)# policy-map vlan100
Device(config-pmap)# policy-map class vlan100
Device(config-pmap-c)# police 100000 bc conform-action transmit exceed-action drop
Device(config-pmap-c-police)# end
Device# configure terminal
Device(config)# interface gigabitEthernet1/0/5
Device(config-if)# service-policy input vlan100
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

Related Topics

[policy-map](#), on page 9

[show policy-map](#), on page 38

service-policy (WLAN)

To configure the WLAN quality of service (QoS) service policy, use the **service-policy** command. To disable a QoS policy on a WLAN, use the **no** form of this command.

```
service-policy [client] {input | output} policy-name
no service-policy [client] {input | output} policy-name
```

Syntax Description

| | |
|---------------|---|
| client | (Optional) Assigns a policy map to all clients in the WLAN. |
|---------------|---|

input Assigns an input policy map.

output Assigns an output policy map.

policy-name The policy name.

Command Default No policies are assigned and the state assigned to the policy is None.

Command Modes WLAN configuration

| Command History | Release | Modification |
|-----------------|--------------------|------------------------------|
| | Cisco IOS XE 3.2SE | Cisco IOS XE 3.3SE |
| | Cisco IOS XE 3.3SE | This command was introduced. |

Usage Guidelines You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

Examples

This example shows how to configure the input QoS service policy on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# service-policy input policy-test
```

This example shows how to disable the input QoS service policy on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no service-policy input policy-test
```

This example shows how to configure the output QoS service policy on a WLAN to platinum (precious metal policy):

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# service-policy output platinum
```

Related Topics

[wlan](#)

set

To classify IP traffic by setting a Differentiated Services Code Point (DSCP) or an IP-precedence value in the packet, use the **set** command in policy-map class configuration mode. Use the **no** form of this command to remove traffic classification.

set

cos | dscp | precedence | ip | qos-group | wlan

set cos

{*cos-value*} | {**cos | dscp | precedence | qos-group | wlan**} [{**table** *table-map-name*}]

```

set dscp
  {dscp-value } | {cos | dscp | precedence | qos-group | wlan} [{table table-map-name}]
set ip {dscp | precedence}
set precedence {precedence-value } | {cos | dscp | precedence | qos-group} [{table table-map-name}]
set qos-group
  {qos-group-value | dscp [{table table-map-name}] | precedence [{table table-map-name}] }
set wlan user-priority
  user-priority-value | costable table-map-name | dscptable table-map-name | qos-grouptable table-map-name
  | wlantable table-map-name

```

Syntax Description**cos**

Sets the Layer 2 class of service (CoS) value or user priority of an outgoing packet. You can specify these values:

- *cos-value*—CoS value from 0 to 7. You also can enter a mnemonic name for a commonly used value.
- Specify a packet-marking category to set the CoS value of the packet. If you also configure a table map for mapping and converting packet-marking values, this establishes the "map from" packet-marking category. Packet-marking category keywords:
 - **cos**—Sets a value from the CoS value or user priority.
 - **dscp**—Sets a value from packet differentiated services code point (DSCP).
 - **precedence**—Sets a value from packet precedence.
 - **qos-group**—Sets a value from the QoS group.
 - **wlan**—Sets the WLAN user priority values.
- (Optional) **table** *table-map-name*—Indicates that the values set in a specified table map are used to set the CoS value. Enter the name of the table map used to specify the CoS value. The table map name can be a maximum of 64 alphanumeric characters.

If you specify a packet-marking category but do not specify the table map, the default action is to copy the value associated with the packet-marking category as the CoS value. For example, if you enter the **set cos precedence** command, the precedence (packet-marking category) value is copied and used as the CoS value.

dscp

Sets the differentiated services code point (DSCP) value to mark IP(v4) and IPv6 packets. You can specify these values:

- *cos-value*—Number that sets the DSCP value. The range is from 0 to 63. You also can enter a mnemonic name for a commonly used value.
 - Specify a packet-marking category to set the DSCP value of the packet. If you also configure a table map for mapping and converting packet-marking values, this establishes the "map from" packet-marking category. Packet-marking category keywords:
 - **cos**—Sets a value from the CoS value or user priority.
 - **dscp**—Sets a value from packet differentiated services code point (DSCP).
 - **precedence**—Sets a value from packet precedence.
 - **qos-group**—Sets a value from the QoS group.
 - **wlan**—Sets a value from WLAN.
 - (Optional) **table** *table-map-name*—Indicates that the values set in a specified table map will be used to set the DSCP value. Enter the name of the table map used to specify the DSCP value. The table map name can be a maximum of 64 alphanumeric characters.
- If you specify a packet-marking category but do not specify the table map, the default action is to copy the value associated with the packet-marking category as the DSCP value. For example, if you enter the **set dscp cos** command, the CoS value (packet-marking category) is copied and used as the DSCP value.

ip

Sets IP values to the classified traffic. You can specify these values:

- **dscp**—Specify an IP DSCP value from 0 to 63 or a packet marking category.
 - **precedence**—Specify a precedence-bit value in the IP header; valid values are from 0 to 7 or specify a packet marking category.
-

precedence

Sets the precedence value in the packet header. You can specify these values:

- *precedence-value*— Sets the precedence bit in the packet header; valid values are from 0 to 7. You also can enter a mnemonic name for a commonly used value.
- Specify a packet marking category to set the precedence value of the packet.
 - **cos**—Sets a value from the CoS or user priority.
 - **dscp**—Sets a value from packet differentiated services code point (DSCP).
 - **precedence**—Sets a value from packet precedence.
 - **qos-group**—Sets a value from the QoS group.
- (Optional)**table** *table-map-name*—Indicates that the values set in a specified table map will be used to set the precedence value. Enter the name of the table map used to specify the precedence value. The table map name can be a maximum of 64 alphanumeric characters.

If you specify a packet-marking category but do not specify the table map, the default action is to copy the value associated with the packet-marking category as the precedence value. For example, if you enter the **set precedence cos** command, the CoS value (packet-marking category) is copied and used as the precedence value.

qos-group

Assigns a QoS group identifier that can be used later to classify packets.

- *qos-group-value*—Sets a QoS value to the classified traffic. The range is 0 to 31. You also can enter a mnemonic name for a commonly used value.
- **dscp**—Sets the original DSCP field value of the packet as the QoS group value.
- **precedence**—Sets the original precedence field value of the packet as the QoS group value.
- (Optional)**table** *table-map-name*—Indicates that the values set in a specified table map will be used to set the DSCP or precedence value. Enter the name of the table map used to specify the value. The table map name can be a maximum of 64 alphanumeric characters.

If you specify a packet-marking category (**dscp** or **precedence**) but do not specify the table map, the default action is to copy the value associated with the packet-marking category as the QoS group value. For example, if you enter the **set qos-group precedence** command, the precedence value (packet-marking category) is copied and used as the QoS group value.

wlan user-priority *wlan-user-priority*

Assigns a WLAN user-priority to the classified traffic. You can specify these values:

- *wlan-user-priority*—Sets a WLAN user priority to the classified traffic. The range is 0 to 7.
- **cos**—Sets the Layer 2 CoS field value as the WLAN user priority.
- **dscp**—Sets the DSCP field value as the WLAN user priority.
- **precedence**—Sets the precedence field value as the WLAN user priority.
- **wlan**—Sets the WLAN user priority field value as the WLAN user priority.
- (Optional) **table** *table-map-name*—Indicates that the values set in a specified table map will be used to set the WLAN user priority value. Enter the name of the table map used to specify the value. The table map name can be a maximum of 64 alphanumeric characters.

If you specify a packet-marking category but do not specify the table map, the default action is to copy the value associated with the packet-marking category as the WLAN user priority. For example, if you enter the **set wlan user-priority cos** command, the cos value (packet-marking category) is copied and used as the WLAN user priority.

Command Default

No traffic classification is defined.

Command Modes

Policy-map class configuration

Command History

| Release | Modification |
|--|--|
| Cisco IOS XE 3.2SE Cisco IOS XE 3.3SE | Cisco IOS XE 3.3SE Cisco IOS XE 3.3SE This command was introduced. |
| Cisco IOS XE 3.3SE | The cos , dscp , qos-group , wlan table <i>table-map-name</i> , keywords were added. |

Usage Guidelines

For the **set dscp** *dscp-value* command, the **set cos** *cos-value* command, and the **set ip precedence** *precedence-value* command, you can enter a mnemonic name for a commonly used value. For example, you can enter the **set dscp af11** command, which is the same as entering the **set dscp 10** command. You can enter the **set ip precedence critical** command, which is the same as entering the **set ip precedence 5** command. For a list of supported mnemonics, enter the **set dscp ?** or the **set ip precedence ?** command to see the command-line help strings.

When you configure the **set dscp cos** command, note the following: The CoS value is a 3-bit field, and the DSCP value is a 6-bit field. Only the three bits of the CoS field are used.

When you configure the **set dscp qos-group** command, note the following:

- The valid range for the DSCP value is a number from 0 to 63. The valid value range for the QoS group is a number from 0 to 99.
- If a QoS group value falls within both value ranges (for example, 44), the packet-marking value is copied and the packets is marked.
- If QoS group value exceeds the DSCP range (for example, 77), the packet-marking value is not be copied and the packet is not marked. No action is taken.

The **set qos-group** command cannot be applied until you create a service policy in policy-map configuration mode and then attach the service policy to an interface or ATM virtual circuit (VC).

To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

Examples

This example shows how to assign DSCP 10 to all FTP traffic without any policers:

```
Device(config)# policy-map policy_ftp
Device(config-pmap)# class-map ftp_class
Device(config-cmap)# exit
Device(config)# policy policy_ftp
Device(config-pmap)# class ftp_class
Device(config-pmap-c)# set dscp 10
Device(config-pmap)# exit
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

Related Topics

- [class](#), on page 1
- [policy-map](#), on page 9
- [show policy-map](#), on page 38

show ap name service-policy

To display service-policy information for a specific Cisco lightweight access point, use the **show ap name service-policy** command.

show ap name *ap-name* **service-policy**

| | |
|---------------------------|--|
| Syntax Description | <i>ap-name</i> Name of the Cisco lightweight access point. |
| Command Default | None |
| Command Modes | Any command mode |

| Command History | Release | Modification |
|-----------------|--|------------------------------|
| | Cisco IOS XE 3.2SE Cisco IOS XE 3.3SE Cisco IOS XE 3.3SE | This command was introduced. |

This example shows how to display service-policy information for a specific Cisco lightweight access point:

```
Device# show ap name 3502b service-policy

NAME: Cisco AP      , DESCR: Cisco Wireless Access Point
PID: 3502I   , VID: V01, SN: FTX1525E94A

NAME: Dot11Radio0   , DESCR: 802.11N 2.4GHz Radio
PID: UNKNOWN, VID:   , SN: FOC1522BLNA

NAME: Dot11Radio1   , DESCR: 802.11N 5GHz Radio
PID: UNKNOWN, VID:   , SN: FOC1522BLNA
```

show ap name dot11

To display 802.11a or 802.11b configuration information that corresponds to specific Cisco lightweight access points, use the **show ap name dot11** command.

```
show ap name ap-name dot11 {24ghz | 5ghz} {ccx | cdp | profile | service-policy output | stats | tsm}
{allclient-mac}}
```

| Syntax Description | | |
|------------------------------|--|---|
| <i>ap-name</i> | | Name of the Cisco lightweight access point. |
| 24ghz | | Displays the 2.4 GHz band. |
| 5ghz | | Displays the 5 GHz band. |
| ccx | | Displays the Cisco Client eXtensions (CCX) radio management status information. |
| cdp | | Displays Cisco Discovery Protocol (CDP) information. |
| profile | | Displays configuration and statistics of 802.11 profiling. |
| service-policy output | | Displays downstream service policy information. |
| stats | | Displays Cisco lightweight access point statistics. |
| tsm | | Displays 802.11 traffic stream metrics statistics. |
| all | | Displays the list of all access points to which the client has associations. |
| <i>client-mac</i> | | MAC address of the client. |

Command Default None

Command Modes

Any command mode

Command History**Release****Modification**

| Release | Modification |
|--|------------------------------|
| Cisco IOS XE 3.2SE Cisco IOS XE 3.3SE Cisco IOS XE 3.3SE | This command was introduced. |

This example shows how to display the service policy that is associated with the access point:

```
Device# show ap name test-ap dot11 24ghz service-policy output

Policy Name   : test-ap1
Policy State  : Installed
```

This example shows how to display the CCX RRM 802.11 configuration for a specific access point:

```
Device# show ap name AP01 dot11 24ghz ccx
```

This example show how to display CDP information for a specific access point:

```
Device# show ap name AP01 dot11 24ghz cdp

AP Name          AP CDP State
-----          -
AP03             Disabled
```

This example show how to display the configuration and statistics of 802.11b profiling for a specific access point:

```
Device# show ap name AP01 dot11 24ghz profile

802.11b Cisco AP performance profile mode      : GLOBAL
802.11b Cisco AP Interference threshold       : 10 %
802.11b Cisco AP noise threshold              : -70 dBm
802.11b Cisco AP RF utilization threshold      : 80 %
802.11b Cisco AP throughput threshold         : 1000000 bps
802.11b Cisco AP clients threshold            : 12 clients
```

This example show how to display downstream service policy information for a specific access point:

```
Device# show ap name AP01 dot11 24ghz service-policy output

Policy Name   : def-11gn
Policy State  : Installed
```

This example show how to display statistics for a specific access point:

```
Device# show ap name AP01 dot11 24ghz stats

Number of Users.....: 0
TxFragmentCount.....: 0
MulticastTxFrameCnt.....: 0
FailedCount.....: 0
RetryCount.....: 0
MultipleRetryCount.....: 0
FrameDuplicateCount.....: 0
RtsSuccessCount.....: 0
RtsFailureCount.....: 0
AckFailureCount.....: 0
```

```

RxIncompleteFragment.....: 0
MulticastRxFrameCnt.....: 0
FcsErrorCount.....: 0
TxFrameCount.....: 0
WepUndecryptableCount.....: 0
TxFramesDropped.....: 0

Call Admission Control (CAC) Stats
  Voice Bandwidth in use(% of config bw).....: 0
  Video Bandwidth in use(% of config bw).....: 0
  Total BW in use for Voice(%).....: 0
  Total BW in use for SIP Preferred call(%).....: 0

Load based Voice Call Stats
  Total channel MT free.....: 0
  Total voice MT free.....: 0
  Na Direct.....: 0
  Na Roam.....: 0

WMM TSPEC CAC Call Stats
  Total num of voice calls in progress.....: 0
  Num of roaming voice calls in progress.....: 0
  Total Num of voice calls since AP joined.....: 0
  Total Num of roaming calls since AP joined.....: 0
  Total Num of exp bw requests received.....: 0
  Total Num of exp bw requests admitted.....: 0
  Num of voice calls rejected since AP joined.....: 0
  Num of roam calls rejected since AP joined.....: 0
  Num of calls rejected due to insufficient bw....: 0
  Num of calls rejected due to invalid params....: 0
  Num of calls rejected due to PHY rate.....: 0
  Num of calls rejected due to QoS policy.....: 0

SIP CAC Call Stats
  Total Num of calls in progress.....: 0
  Num of roaming calls in progress.....: 0
  Total Num of calls since AP joined.....: 0
  Total Num of roaming calls since AP joined.....: 0
  Total Num of Preferred calls received.....: 0
  Total Num of Preferred calls accepted.....: 0
  Total Num of ongoing Preferred calls.....: 0
  Total Num of calls rejected(Insuff BW).....: 0
  Total Num of roam calls rejected(Insuff BW)....: 0

Band Select Stats
  Num of dual band client .....: 0
  Num of dual band client added.....: 0
  Num of dual band client expired .....: 0
  Num of dual band client replaced.....: 0
  Num of dual band client detected .....: 0
  Num of suppressed client .....: 0
  Num of suppressed client expired.....: 0
  Num of suppressed client replaced.....: 0

```

This example show how to display the traffic stream configuration for all clients that correspond to a specific access point:

```
Device# show ap name AP01 dot11 24ghz tsm all
```

show class-map

To display quality of service (QoS) class maps, which define the match criteria to classify traffic, use the **show class-map** command in EXEC mode.

```
show class-map [class-map-name | type control subscriber {all | class-map-name}]
```

Syntax Description

| | |
|--------------------------------|---|
| <i>class-map-name</i> | (Optional) Class map name. |
| type control subscriber | (Optional) Displays information about control class maps. |
| all | (Optional) Displays information about all control class maps. |

Command Modes

User EXEC
Privileged EXEC

Command History

| Release | Modification |
|--|--|
| Cisco IOS XE 3.2SE Cisco IOS XE 3.3SE | Cisco IOS XE 3.3SE This command was introduced. |

Examples

This is an example of output from the **show class-map** command:

```
Device# show class-map
Class Map match-any videowizard_10-10-10-10 (id 2)
  Match access-group name videowizard_10-10-10-10

Class Map match-any class-default (id 0)
  Match any
Class Map match-any dscp5 (id 3)
  Match ip dscp 5
```

Related Topics

[class-map](#), on page 4

show platform hardware fed switch

To display device-specific hardware information, use the **show platform hardware fed switch** *switch_number* command.

This topic elaborates only the QoS-specific options, that is, the options available with the **show platform hardware fed switch** *{switch_num | active | standby} qos* command.

```
show platform hardware fed switch {switch_num | active | standby} qos {afd | {config type type | [{asic
asic_num}]} | stats clients {all | bssid id | wlanid id}} | dscp-cos counters {iifd_id id | interface type number}
| le-info | {iifd_id id | interface type number} | policer config {iifd_id id | interface type number} | queue
| {config | {iifd_id id | interface type number | internal port-type type {asic number [{port_num}]}} |
```

label2qmap | [**{aqmreqpostbl | iqslabtable | sqslabtable}**] | **{asicnumber}** | **stats** | **{iifd_id id | interface type number | internal {cpu policer | port-type type asic number} {asicnumber [{port_num}]}}** | **resource}**

Syntax Description

switch {*switch_num* | **active** | **standby** }

Switch for which you want to display information. You have the following options:

- *switch_num*—ID of the switch.
- **active**—Displays information relating to the active switch.
- **standby**—Displays information relating to the standby switch, if available.

qos

Displays QoS hardware information. You must choose from the following options:

- **afd** —Displays Approximate Fair Drop (AFD) information in hardware.
- **dscp-cos**—Displays information dscp-cos counters for each port.
- **leinfo**—Displays logical entity information.
- **policer**—Displays QoS policer information in hardware.
- **queue**—Displays queue information in hardware.
- **resource**—Displays hardware resource information.

afd {**config type** | **stats client** }

You must choose from the options under **config type** or **stats client** :

config type:

- **client**—Displays wireless client information
- **port**—Displays port-specific information
- **radio**—Displays wireless radio information
- **ssid**—Displays wireless SSID information

stats client :

- **all**—Displays statistics of all client.
- **bssid**—Valid range is from 1 to 4294967295.
- **wlanid**—Valid range is from to 1 4294967295

asicasic_num

(Optional) ASIC number. Valid range is from 0 to 255.

dscp-cos counters { **iifd_id id | interface type number** }

Displays per port dscp-cos counters. You must choose from the following options under **dscp-cos counters**:

- **iifd_id id**—The target interface ID. Valid range is from 1 to 4294967295.
- **interface type number**—Target interface type and ID.

leinfo

You must choose from the following options under **dscp-cos counters**:

- **iifd_id id**—The target interface ID. Valid range is from 1 to 4294967295.
- **interface type number**—Target interface type and ID.

| | |
|---|--|
| policer config | Displays configuration information related to policers in hardware. You must choose from the following options: <ul style="list-style-type: none"> • iif_id <i>id</i>—The target interface ID. Valid range is from 1 to 4294967295. • interface <i>type number</i>—Target interface type and ID. |
| queue { config { iif_id <i>id</i> interface <i>type number</i> internal } label2qmap stats } | Displays queue information in hardware. You must choose from the following options: <ul style="list-style-type: none"> • config—Configuration information. You must choose from the following options: <ul style="list-style-type: none"> • iif_id <i>id</i>—The target interface ID. Valid range is from 1 to 4294967295. • interface <i>type number</i>—Target interface type and ID. • internal—Displays internal queue related information. • label2qmap—Displays hardware label to queue mapping information. You can choose from the following options: <ul style="list-style-type: none"> • (Optional) aqmrepqostbl— AQM REP QoS label table lookup. • (Optional) iqslabeltable—IQS QoS label table lookup. • (Optional) sqslabeltable—SQS and local QoS label table lookup. • stats—Displays queue statistics. You must choose from the following options: <ul style="list-style-type: none"> • iif_id <i>id</i>—The target interface ID. Valid range is from 1 to 4294967295. • interface <i>type number</i>—Target interface type and ID. • internal { cpu policer port_type <i>port_type</i> asic <i>asic_num</i> [port_num <i>port_num</i>] }—Displays internal queue related information. |
| resource | Displays hardware resource usage information. You must enter the following keyword: usage |

Command Modes

User EXEC

Privileged EXEC

Command History

| Release | Modification |
|--------------------|------------------------------|
| Cisco IOS XE 3.2SE | This command was introduced. |

This is an example of output from the **show platform hardware fed switch switch_number qos queue stats internal cpu policer** command

```
Device#show platform hardware fed switch 3 qos queue stats internal cpu policer
```

```

                                (default) (set)
QId PlcIdx Queue Name           Enabled Rate Rate Drop
-----
```

| | | | | | | |
|----|----|--------------------------|-----|-------|-------|---|
| 0 | 11 | DOT1X Auth | No | 1000 | 1000 | 0 |
| 1 | 1 | L2 Control | No | 500 | 500 | 0 |
| 2 | 14 | Forus traffic | No | 1000 | 1000 | 0 |
| 3 | 0 | ICMP GEN | Yes | 200 | 200 | 0 |
| 4 | 2 | Routing Control | Yes | 1800 | 1800 | 0 |
| 5 | 14 | Forus Address resolution | No | 1000 | 1000 | 0 |
| 6 | 3 | ICMP Redirect | No | 500 | 500 | 0 |
| 7 | 6 | WLESS PRI-5 | No | 1000 | 1000 | 0 |
| 8 | 4 | WLESS PRI-1 | No | 1000 | 1000 | 0 |
| 9 | 5 | WLESS PRI-2 | No | 1000 | 1000 | 0 |
| 10 | 6 | WLESS PRI-3 | No | 1000 | 1000 | 0 |
| 11 | 6 | WLESS PRI-4 | No | 1000 | 1000 | 0 |
| 12 | 0 | BROADCAST | Yes | 200 | 200 | 0 |
| 13 | 10 | Learning cache ovfl | Yes | 100 | 100 | 0 |
| 14 | 13 | Sw forwarding | Yes | 1000 | 1000 | 0 |
| 15 | 8 | Topology Control | No | 13000 | 13000 | 0 |
| 16 | 12 | Proto Snooping | No | 500 | 500 | 0 |
| 17 | 16 | DHCP Snooping | No | 1000 | 1000 | 0 |
| 18 | 9 | Transit Traffic | Yes | 500 | 500 | 0 |
| 19 | 10 | RPF Failed | Yes | 100 | 100 | 0 |
| 20 | 15 | MCAST END STATION | Yes | 2000 | 2000 | 0 |
| 21 | 13 | LOGGING | Yes | 1000 | 1000 | 0 |
| 22 | 7 | Punt Webauth | No | 1000 | 1000 | 0 |
| 23 | 10 | Crypto Control | Yes | 100 | 100 | 0 |
| 24 | 10 | Exception | Yes | 100 | 100 | 0 |
| 25 | 3 | General Punt | No | 500 | 500 | 0 |
| 26 | 10 | NFL SAMPLED DATA | Yes | 100 | 100 | 0 |
| 27 | 2 | SGT Cache Full | Yes | 1800 | 1800 | 0 |
| 28 | 10 | EGR Exception | Yes | 100 | 100 | 0 |
| 29 | 16 | Show frwd | No | 1000 | 1000 | 0 |
| 30 | 9 | MCAST Data | Yes | 500 | 500 | 0 |
| 31 | 10 | Gold Pkt | Yes | 100 | 100 | 0 |

show platform software fed switch qos

To display device-specific software information, use the **show platform hardware fed switch** *switch_number* command.

This topic elaborates only the QoS-specific options available with the **show platform software fed switch** {*switch_num* | **active** | **standby** } **qos** command.

show platform software fed switch {*switch number* | **active** | **standby**} **qos** {**avc** | **internal** | **label2qmap** | **nflqos** | **policer** | **policy** | **qsb** | **tablemap** | **wireless**}

Syntax Description

| | |
|---|---|
| switch { <i>switch_num</i> active standby } | The device for which you want to display information. |
| <ul style="list-style-type: none"> • <i>switch_num</i>—Enter the switch ID. Displays information for the specified switch. • active—Displays information for the active switch. • standby—Displays information for the standby switch, if available. | |

| | |
|------------|---|
| qos | <p>Displays QoS software information. Choose one the following options:</p> <ul style="list-style-type: none"> • avc—Displays Application Visibility and Control (AVC) QoS information. • internal—Displays internal queue-related information. • label2qmap—Displays label to queue map table information. • nflqos—Displays NetFlow QoS information. • policer—Displays QoS policer information in hardware. • policy—Displays QoS policy information. • qsb—Displays QoS sub-block information. • tablemap—Displays table mapping information for QoS egress and ingress queues. • wireless—Displays wireless QoS information. |
|------------|---|

Command Modes

User EXEC

Privileged EXEC

Command History**Release**

Cisco IOS XE Denali 16.1.1

Modification

This command was introduced.

show platform software fed switch qos qsb

To display QoS sub-block information, use the **show platform software fed switch** *switch_number* **qos qsb** command.

```
show platform software fed switch {switch number | active | standby} qosqsb {brief | [{all | type |
clientclient_id | port port_number | radioradio_type | ssidssid}] | iif_idid | interface |
{Auto-Templateinterface_number | BDIinterface_number | Capwapinterface_number |
GigabitEthernetinterface_number | InternalInterfaceinterface_number | Loopbackinterface_number |
Nullinterface_number | Port-channelinterface_number | TenGigabitEthernetinterface_number |
Tunnelinterface_number | Vlaninterface_number}}
```

Syntax Description

| | |
|---|---|
| switch { <i>switch_num</i> active standby } | <p>The switch for which you want to display information.</p> <ul style="list-style-type: none"> • <i>switch_num</i>—Enter the ID of the switch. Displays information for the specified switch. • active—Displays information for the active switch. • standby—Displays information for the standby switch, if available. |
|---|---|

| | |
|----------------|--|
| qos qsb | Displays QoS sub-block software information. |
|----------------|--|

qsb {brief | iif_id | brief interface}

- **all**—Displays information for all client.
- **type**—Displays qsb information for the specified target type:
 - **client**—Displays QoS qsb information for wireless clients
 - **port**—Displays port-specific information
 - **radio**—Displays QoS qsb information for wireless radios
 - **ssid**—Displays QoS qsb information for wireless networks

iif_id—Displays information for the iif_ID

interface—Displays QoS qsb information for the specified interface:

- **Auto-Template**—Auto-template interface between 1 and 999.
- **BDI**—Bridge-domain interface between 1 and 16000.
- **Capwap**—CAPWAP interface between 0 and 2147483647.
- **GigabitEthernet**—GigabitEthernet interface between 0 and 9.
- **InternalInterface**—Internal interface between 0 and 9.
- **Loopback**—Loopback interface between 0 and 2147483647.
- **Null**—Null interface 0-0
- **Port-Channel**—Port-channel interface between 1 and 128.
- **TenGigabitEthernet**—TenGigabitEthernet interface between 0 and 9.
- **Tunnel**—Tunnel interface between 0 and 2147483647.
- **Vlan**—VLAN interface between 1 and 4094.

Command Modes

User EXEC

Privileged EXEC

Command History

| Release | Modification |
|----------------------------|------------------------------|
| Cisco IOS XE Denali 16.1.1 | This command was introduced. |

This is an example of the output for the **show platform software fed switch switch_number qos qsb** command

```
Device#sh pl so fed sw 3 qos qsb interface g3/0/2
```

```
QoS subblock information:
Name:GigabitEthernet3/0/2 iif_id:0x00000000000007b iif_type:ETHER(146)
qsb ptr:0xffd8573350
Port type = Wired port
asic_num:0 is_uplink:false init_done:true
FRU events: Active-0, Inactive-0
```

```

def_qos_label:0 def_le_priority:13
trust_enabled:false trust_type:TRUST_DSCP ifm_trust_type:1
LE priority:13 LE trans_index(in, out): (0,0)
Stats (plc,q) export counters (in/out): 0/0
Policy Info:
  Ingress Policy: pmap::{(0xffd8685180,AutoQos-4.0-CiscoPhone-Input-Policy,1083231504,)}
    tcg::{0xffd867ad10,GigabitEthernet3/0/2 tgt(0x7b,IN) level:0 num_tccg:4 num_child:0},
status:VALID,SET_INHW
  Egress Policy: pmap::{(0xffd86857d0,AutoQos-4.0-Output-Policy,1076629088,)}
    tcg::{0xffd8685b40,GigabitEthernet3/0/2 tgt(0x7b,OUT) level:0 num_tccg:8 num_child:0},
status:VALID,SET_INHW
  TCG(in,out):(0xffd867ad10, 0xffd8685b40) le_label_id(in,out):(2, 1)
Policer Info:
  num_ag_policers(in,out)[1r2c,2r3c]: ([0,0],[0,0])
  num_mf_policers(in,out): (0,0)
  num_afd_policers:0
  [ag_plc_handle(in,out) = (0xd8688220,0)]
  [mf_plc_handle(in,out)=(nil),(nil)] num_mf_policers:(0,0)
  base:(0xffffffff,0xffffffff) rc:(0,0)]
Queueing Info:
  def_queueing = 0, shape_rate:0 interface_rate_kbps:1000000
  Port shaper:false
  lbl_to_qmap_index:1
Physical qparams:
  Queue Config: NodeType:Physical Id:0x40000049 parent:0x40000049 qid:0 attr:0x1 defq:0

PARAMS: Excess Ratio:1 Min Cir:1000000 QBuffer:0
Queue Limit Type:Single Unit:Percent Queue Limit:44192
SHARED Queue

```

show wireless client calls

To display the total number of active or rejected calls on the device, use the **show wireless client calls** command in privileged EXEC mode.

show wireless client calls {active | rejected}

| Syntax Description | active Displays active calls. | | | | | | |
|---------------------------|---|---------|--------------|--------------------|--------------------|--------------------|------------------------------|
| | rejected Displays rejected calls. | | | | | | |
| Command Default | No default behavior or values. | | | | | | |
| Command Modes | Privileged EXEC | | | | | | |
| Command History | <table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.2SE</td> <td>Cisco IOS XE 3.3SE</td> </tr> <tr> <td>Cisco IOS XE 3.3SE</td> <td>This command was introduced.</td> </tr> </tbody> </table> | Release | Modification | Cisco IOS XE 3.2SE | Cisco IOS XE 3.3SE | Cisco IOS XE 3.3SE | This command was introduced. |
| Release | Modification | | | | | | |
| Cisco IOS XE 3.2SE | Cisco IOS XE 3.3SE | | | | | | |
| Cisco IOS XE 3.3SE | This command was introduced. | | | | | | |

The following is sample output from the **show wireless client calls** command:

```

device# show wireless client calls active

TSPEC Calls:

```

```

-----
MAC Address      AP Name          Status           WLAN  Authenticated
-----
0000.1515.000f   AP-2             Associated       1    Yes

SIP Calls:
-----
Number of Active TSPEC calls on 802.11a and 802.11b/g: 1
Number of Active SIP calls on 802.11a and 802.11b/g: 0

```

show wireless client dot11

To display the total number of active or rejected calls for a specific band (2.4 Ghz or 5 Ghz), use the **show wireless client dot11** command in privileged EXEC mode.

```
show wireless client dot11 {24ghz | 5ghz} calls {active | rejected}
```

| Syntax Description | 24ghz Displays the 802.11b/g network. | | | | |
|--|--|---------|--------------|--|------------------------------|
| | 5ghz Displays the 802.11a network. | | | | |
| | calls Displays the wireless client calls. | | | | |
| | active Displays active calls. | | | | |
| | rejected Displays rejected calls. | | | | |
| Command Default | No default behavior or values. | | | | |
| Command Modes | Privileged EXEC | | | | |
| Command History | <table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.2SE Cisco IOS XE 3.3SE Cisco IOS XE 3.3SE</td> <td>This command was introduced.</td> </tr> </tbody> </table> | Release | Modification | Cisco IOS XE 3.2SE Cisco IOS XE 3.3SE Cisco IOS XE 3.3SE | This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE 3.2SE Cisco IOS XE 3.3SE Cisco IOS XE 3.3SE | This command was introduced. | | | | |

The following is sample output from the **show wireless client dot11** command:

```

Device# show wireless client dot11 5ghz calls active

TSPEC Calls:
-----

SIP Calls:
-----
Number of Active TSPEC calls on 802.11a: 0
Number of Active SIP calls on 802.11a: 0

```

show wireless client mac-address (Call Control)

To view call control information related to clients, use the **show wireless client mac-address** command in privileged EXEC mode.

show wireless client mac-address *mac-address* **call-control call-info**

| | | |
|---------------------------|--|--|
| Syntax Description | <i>mac-address</i> | The client MAC address. |
| | call-control call-info | Displays the call control and IP-related information about a client. |
| Command Default | None | |
| Command Modes | Privileged EXEC | |
| Command History | Release | Modification |
| | Cisco IOS XE 3.2SE Cisco IOS XE 3.3SE Cisco IOS XE 3.3SE | This command was introduced. |

This example shows how to display call control and IP-related information about a client:

```
Device# show wireless client mac-address 30e4.db41.6157 call-control call-info
Client MAC Address      : 30E4DB416157

Call 1 Statistics

Uplink IP Address      : 209.165.200.225
Downlink IP Address    : 209.165.200.226
Uplink Port            : 29052
Downlink Port          : 27538
Call ID                : c40acb4d-3b3b0.3d27da1e-356bed03
Called Party           : sip:1011
Calling Party          : sip:1012
Priority                : 6
Call On Hold           : false
Call Duration          : 30

Call 2 Statistics

No Active Call
```

show wireless client mac-address (TCLAS)

To view information about TCLAS and user priority, use the **show wireless client mac-address** command in privileged EXEC mode.

show wireless client mac-address *mac-address* **tclas**

| | | |
|---------------------------|--------------------|--|
| Syntax Description | <i>mac-address</i> | The client MAC address. |
| | tclas | Displays TCLAS and user priority-related information about a client. |

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|--------------------|------------------------------|
| | Cisco IOS XE 3.2SE | Cisco IOS XE 3.3SE |
| | Cisco IOS XE 3.3SE | This command was introduced. |

This example shows how to display the TCLAS and user priority-related information about a client:

```
Device# show wireless client mac-address 30e4.db41.6157 tclas
MAC Address      UP TID Mask Source IP Addr  Dest IP Addr  SrcPort DstPort Proto
-----
30e4.db41.6157   4  4  95 167838052  2164326668   5060    5060    6
30e4.db41.6157   6  1  31 0          2164326668    0       27538   17
```

show wireless client voice diagnostics

To display wireless client voice diagnostic parameters, use the **show wireless client voice diagnostics** command in privileged EXEC mode.

show wireless client voice diagnostics { qos-map | roam-history | rssi | status | tspec }

| Syntax Description | | |
|---------------------|--|--|
| qos-map | Displays information about the QoS and DSCP mapping and packet statistics in each of the four queues: VO, VI, BE, BK. The different DSCP values are also displayed. | |
| roam-history | Displays information about the last 3 roaming histories for each known client. The output contains the timestamp, access point associated with roaming, roaming reason, and if there is a roaming failure, a reason for the roaming failure. | |
| rssi | Displays the client's RSSI values in the last 5 seconds when voice diagnostics are enabled. | |
| status | Displays status of voice diagnostics for clients. | |
| tspec | Displays voice diagnostics that are enabled for TSPEC clients. | |

Command Default No default behavior or values.

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|--------------------|------------------------------|
| | Cisco IOS XE 3.2SE | Cisco IOS XE 3.3SE |
| | Cisco IOS XE 3.3SE | This command was introduced. |

Usage Guidelines Debug voice diagnostics must be enabled for voice diagnostics to work.

The following is sample output from the **show wireless client voice diagnostics status** command:

```
Device# show wireless client voice diagnostics status
Voice Diagnostics Status: FALSE
```

show policy-map

To display quality of service (QoS) policy maps, which define classification criteria for incoming traffic, use the **show policy-map** command in EXEC mode.

```
show policy-map [{policy-map-name | interface interface-id}]
```

```
show policy-map interface {Auto-template | Capwap | GigabitEthernet | GroupVI |
InternalInterface | Loopback | Lspvif | Null | Port-channel | TenGigabitEthernet | Tunnel
| Vlan | brief | class | input | output}
```

```
show policy-map type control subscriber detail
```

```
show policy-map interface wireless {ap name ap_name | client mac mac_address | radio type {24ghz
| 5ghz} ap name ap_name | ssid name ssid_name {ap name ap_name | radio type {24ghz |
5ghz} ap name ap_name}}
```

| Syntax Description | | |
|--------------------|--|--|
| | <i>policy-map-name</i> | (Optional) Name of the policy-map. |
| | interface <i>interface-id</i> | (Optional) Displays the statistics and the configurations of the input and output policies that are attached to the interface. |
| | type control subscriber detail | (Optional) Identifies the type of QoS policy and the statistics. |
| | ap name <i>ap_name</i> | Displays SSID policy configuration of an access point. |
| | client mac <i>mac_address</i> | Displays information about the policies for all the client targets. |
| | radio type { 24ghz 5ghz } | Displays policy configuration of the access point in the specified radio type. |
| | ssid name <i>ssid_name</i> | Displays policy configuration of an SSID. |

| Command Modes | |
|---------------|-----------------|
| | User EXEC |
| | Privileged EXEC |

| Command History | Release | Modification |
|-----------------|--|---|
| | Cisco IOS XE 3.2SE Cisco IOS XE 3.3SE Cisco IOS XE 3.3SE | This command was introduced. |
| | Cisco IOS XE 3.3SE | The interface <i>interface-id</i> keyword was added. |

| Usage Guidelines | |
|------------------|--|
| | Policy maps can include policers that specify the bandwidth limitations and the action to take if the limits are exceeded. |



Note Though visible in the command-line help string, the **control-plane**, **session**, and **type** keywords are not supported, and the statistics shown in the display should be ignored.

This is an example of the output for the **show policy-map interface** command.

```
Device# show policy-map interface gigabitethernet1/0/48GigabitEthernet1/0/48
```

```
Service-policy output: port_shape_parent

Class-map: class-default (match-any)
 191509734 packets
 Match: any
 Queueing

 (total drops) 524940551420
 (bytes output) 14937264500
 shape (average) cir 2500000000, bc 2500000, be 2500000
 target shape rate 250000000

Service-policy : child_trip_play

  queue stats for all priority classes:
    Queueing
    priority level 1

    (total drops) 524940551420
    (bytes output) 14937180648

  queue stats for all priority classes:
    Queueing
    priority level 2

    (total drops) 0
    (bytes output) 0

Class-map: dscp56 (match-any)
 191508445 packets
 Match: dscp cs7 (56)
    0 packets, 0 bytes
    5 minute rate 0 bps
 Priority: Strict,

 Priority Level: 1
 police:
   cir 10 %
   cir 25000000 bps, bc 781250 bytes
   conformed 0 bytes; actions: >>>>counters not supported
   transmit
   exceeded 0 bytes; actions:
     drop
     conformed 0000 bps, exceeded 0000 bps >>>>counters not supported
```

Related Topics

[policy-map](#), on page 9

show wlan

To view WLAN parameters, use the **show wlan** command.

```
show wlan {all | id wlan-id | name wlan-name | summary}
```

| Syntax Description | | |
|------------------------------|--|---|
| all | | Displays a summary of parameters of all configured WLANs. The list is ordered by the ascending order of the WLAN IDs. |
| id <i>wlan-id</i> | | Specifies the wireless LAN identifier. The range is from 1 to 512. |
| name <i>wlan-name</i> | | Specifies the WLAN profile name. The name is from 1 to 32 characters. |
| summary | | Displays a summary of the parameters configured on a WLAN. |
| Command Default | None | |
| Command Modes | Global configuration | |
| Command History | Release | Modification |
| | Cisco IOS XE 3.2SE Cisco IOS XE 3.3SE Cisco IOS XE 3.3SE | This command was introduced. |

This example shows how to display a summary of the WLANs configured on the device:

```
Device# show wlan summary
Number of WLANs: 1

WLAN Profile Name          SSID                      VLAN Status
-----
45 test-wlan                test-wlan-ssid            1    UP
```

This example shows how to display a summary of parameters configured on a particular WLAN:

```
Device# show wlan name test-wlan
WLAN Identifier              : 45
Profile Name                 : test-wlan
Network Name (SSID)         : test-wlan-ssid
Status                       : Enabled
Broadcast SSID              : Enabled
Maximum number of Associated Clients : 0
AAA Policy Override         : Disabled
Network Admission Control
  NAC-State                  : Disabled
Number of Active Clients     : 0
Exclusionlist Timeout        : 60
Session Timeout              : 1800 seconds
CHD per WLAN                : Enabled
Webauth DHCP exclusion      : Disabled
Interface                   : default
Interface Status            : Up
```



```

Multicast Interface                : test
WLAN IPv4 ACL                     : test
WLAN IPv6 ACL                     : unconfigured
DHCP Server                       : Default
DHCP Address Assignment Required  : Disabled
DHCP Option 82                   : Disabled
DHCP Option 82 Format             : ap-mac
DHCP Option 82 Ascii Mode        : Disabled
DHCP Option 82 Rid Mode          : Disabled
QoS Service Policy - Input
  Policy Name                     : unknown
  Policy State                    : None
QoS Service Policy - Output
  Policy Name                     : unknown
  Policy State                    : None
QoS Client Service Policy
  Input Policy Name               : unknown
  Output Policy Name              : unknown
WifiDirect                        : Disabled
WMM                               : Disabled
Channel Scan Defer Priority:
  Priority (default)              : 4
  Priority (default)              : 5
  Priority (default)              : 6
Scan Defer Time (msecs)          : 100
Media Stream Multicast-direct    : Disabled
CCX - AironetIe Support          : Enabled
CCX - Gratuitous ProbeResponse (GPR) : Disabled
CCX - Diagnostics Channel Capability : Disabled
Dot11-Phone Mode (7920)         : Invalid
Wired Protocol                   : None
Peer-to-Peer Blocking Action     : Disabled
Radio Policy                     : All
DTIM period for 802.11a radio    : 1
DTIM period for 802.11b radio    : 1
Local EAP Authentication         : Disabled
Mac Filter Authorization list name : Disabled
Accounting list name             : Disabled
802.1x authentication list name  : Disabled
Security
  802.11 Authentication           : Open System
  Static WEP Keys                 : Disabled
  802.1X                          : Disabled
  Wi-Fi Protected Access (WPA/WPA2)
    WPA (SSN IE)                  : Disabled
    WPA2 (RSN IE)                 : Enabled
    TKIP Cipher                   : Disabled
    AES Cipher                    : Enabled
    Auth Key Management
      802.1x                      : Enabled
      PSK                         : Disabled
      CCKM                        : Disabled
  IP Security                     : Disabled
  IP Security Passthru            : Disabled
  L2TP                            : Disabled
  Web Based Authentication        : Disabled
  Conditional Web Redirect        : Disabled
  Splash-Page Web Redirect       : Disabled
  Auto Anchor                     : Disabled
  Sticky Anchoring               : Enabled
  Cranite Passthru               : Disabled
  Fortress Passthru              : Disabled
  PPTP                           : Disabled
  Infrastructure MFP protection   : Enabled

```

```

Client MFP : Optional
Webauth On-mac-filter Failure : Disabled
Webauth Authentication List Name : Disabled
Webauth Parameter Map : Disabled
Tkip MIC Countermeasure Hold-down Timer : 60
Call Snooping : Disabled
Passive Client : Disabled
Non Cisco WGB : Disabled
Band Select : Disabled
Load Balancing : Disabled
IP Source Guard : Disabled
Netflow Monitor : test
    Direction : Input
    Traffic : Datalink

Mobility Anchor List
IP Address
-----

```

trust device

To configure trust for supported devices connected to an interface, use the **trust device** command in interface configuration mode. Use the **no** form of this command to disable trust for the connected device.

```

trust device {cisco-phone | cts | ip-camera | media-player}
no trust device {cisco-phone | cts | ip-camera | media-player}

```

| Syntax Description | cisco-phone Configures a Cisco IP phone | | | | |
|--|--|---------|--------------|--|------------------------------|
| | cts Configures a Cisco TelePresence System | | | | |
| | ip-camera Configures an IP Video Surveillance Camera (IPVSC) | | | | |
| | media-player Configures a Cisco Digital Media Player (DMP) | | | | |
| Command Default | Trust disabled | | | | |
| Command Modes | Interface configuration | | | | |
| Command History | <table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.2SE Cisco IOS XE 3.3SE Cisco IOS XE 3.3SE</td> <td>This command was introduced.</td> </tr> </tbody> </table> | Release | Modification | Cisco IOS XE 3.2SE Cisco IOS XE 3.3SE Cisco IOS XE 3.3SE | This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE 3.2SE Cisco IOS XE 3.3SE Cisco IOS XE 3.3SE | This command was introduced. | | | | |

Usage Guidelines Use the **trust device** command on the following types of interfaces:

- **Auto**— auto-template interface
- **Capwap**—CAPWAP tunnel interface
- **GigabitEthernet**—Gigabit Ethernet IEEE 802
- **GroupVI**—Group virtual interface
- **Internal Interface**—Internal interface

- **Loopback**—Loopback interface
- **Null**—Null interface
- **Port-channel**—Ethernet Channel interface
- **TenGigabitEthernet**—10-Gigabit Ethernet
- **Tunnel**—Tunnel interface
- **Vlan**—Catalyst VLANs
- **range**—**interface range** command

Example

The following example configures trust for a Cisco IP phone in Interface GigabitEthernet 1/0/1:

```
Device(config)# interface GigabitEthernet1/0/1  
Device(config-if)# trust device cisco-phone
```

You can verify your settings by entering the **show interface status** privileged EXEC command.

