Configuring ME 3400E QoS Classification for QinQ-Based Service, Release 12.2(53)SE

December 15, 2009

An ME 3400E switch supports port-based 802.1Q tunneling (QinQ) on tunnel or trunk ports and selective (VLAN-based) QinQ on trunk ports. This enhancement in Cisco IOS Release 12.2(53)SE allows you to apply an ingress QoS classification on the customer packet that is tunneled into a service-provider 802.1Q tag (S-tag) and on the imposed S-tag on the QinQ port.

You can classify on the customer packet tunneled into the S-tag based on the customer VLAN-ID (C-VLAN), the customer class of service (CoS) priority (C-CoS), the customer DSCP priority (C-DSCP), or multifield parameters (MAC-ACL and IP-ACL) in the incoming packet. You can also classify on the S-tag based on the service-provider VLAN (S-VLAN) or the service-provider CoS priority (S-CoS) of the packet.

As with any QoS classification, you create a class map by entering the **class-map** global configuration command and enter class-map configuration mode, where you use the **match** command to define the match criteria for the traffic. The incoming packets are compared to the class match criteria; packets matching the criteria are part of the class and are forwarded according to the QoS specifications in the traffic policy.

After classification, you can apply the ingress QoS functions of policing and marking to these packets. You create and name a policy map by using the **policy-map** global configuration command, naming the traffic class associated with the traffic policy, and specifying the action to take on all traffic in the class. You use the **service-policy** interface configuration command to attach the traffic policy to the port on which QinQ is configured.

Note This document covers only configuration with commands for the QoS classification enhancement for QinQ. For all other information about QoS or tunneling, refer to the *ME 3400E Software Configuration Guide for Cisco IOS Release 12.2(52)SE*: http://www.cisco.com/en/US/docs/switches/metro/me3400e/software/release/12.2_52_se/configuration/guide/ME3400e_scg.html

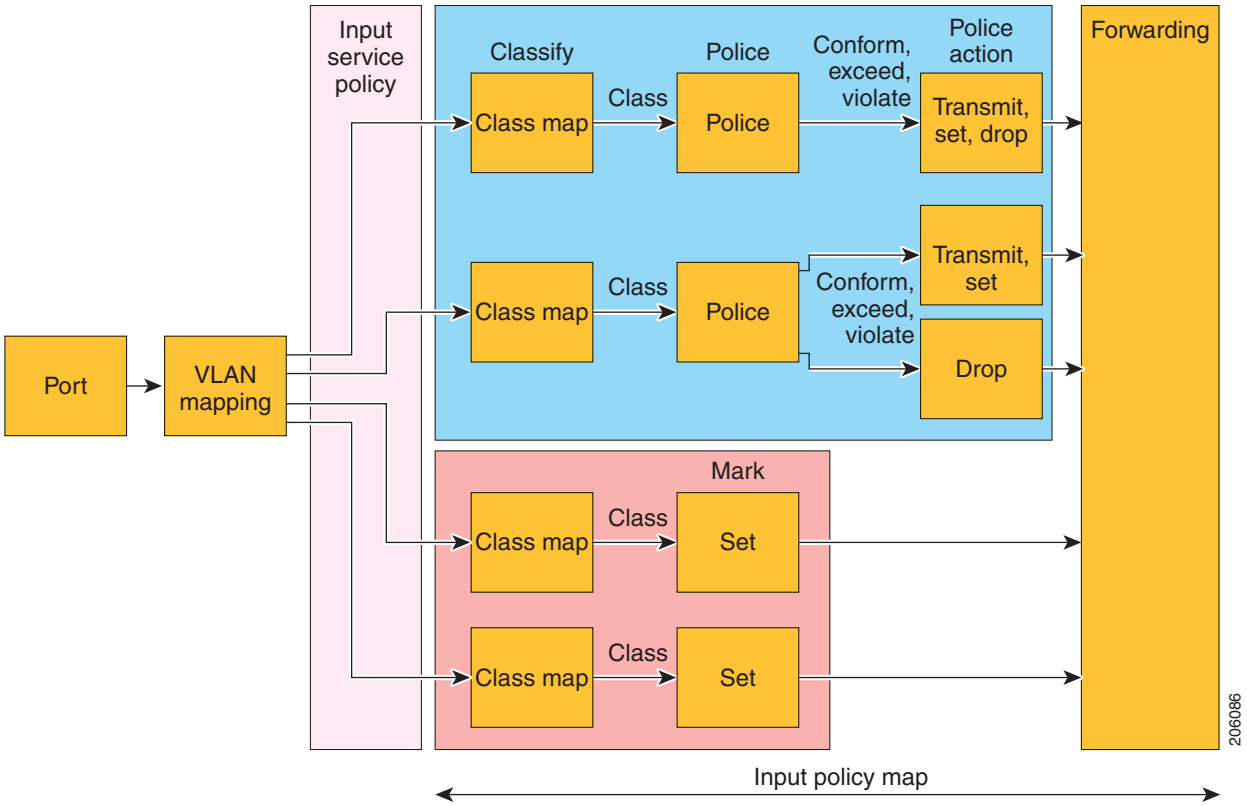
Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Note that the procedures in this document for configuring class maps replace the procedures in the software configuration guide for this release.

Guidelines for Configuring QoS Classification for QinQ

- This document uses the terms C-VLAN for customer VLAN (inner VLAN), S-VLAN for service-provider VLAN (outer VLAN), C-CoS for customer CoS value, and S-CoS for service-provider CoS value.
- For VLAN-based classification on a port, you must apply a hierarchical QoS policy on the port. The hierarchical policy map supports a parent level and a child level. With the QoS parent-child structure, you can reference a child policy in a parent policy to specify that the classification and actions defined in the child policy should be executed within the context of the corresponding class in the parent policy map.
- For classification based only on a port (and not on VLAN-IDs), you can apply a nonhierarchical QoS policy on the port. The nonhierarchical policy has the same structure as a child policy.
- Classification based on C-VLAN and C-CoS applies only to QinQ packets formed as a result of the configured QinQ ports (see “Configuring the QinQ Ports” section on page 5). For other ports, the configurations are allowed but do not function; that is, no packets match those classes.
- Ingress QoS classification of the packet occurs after VLAN-mapping operations, such as VLAN tunneling and translation, are performed. QoS actions, such as policing and marking of the packet, occur after QoS classification. See Figure 1.

Figure 1 Ingress QoS Process



Parent Policy-Map Guidelines

- You must specify classification based on S-VLAN and C-VLAN in the parent-level classes of the parent policy map. You can specify the VLAN match criteria only in parent-level-classes.
- A parent-level VLAN class specifies the VLANs on which to execute the corresponding child policy. Therefore, a child policy *must* be associated with the parent-level class. A parent-level (VLAN) class cannot exist without an associated child policy. Actions, such as policing and marking, cannot be directly associated with a parent-level class.
- In a parent-level class map, when you configure classification based only on the S-VLAN (the parent class map is configured with the logical-operation **match-any** and one or more **match vlan** commands), all packets matching *any* of those S-VLANs are associated with the corresponding child policy.
- In a parent-level class map, when you configure classification based only on the C-VLAN (the parent class map is configured with the logical-operation **match-any** and one or more **match vlan inner** commands), all packets matching *any* of those C-VLANs are associated with the corresponding child policy.
- In a parent-level class map, when you configure classification based on S-VLAN *and* C-VLAN (the parent class map is configured with the logical-operation **match-all** with one **match vlan** command and one **match vlan inner** command), all packets matching *both* of those VLANs (matching the S-VLAN and C-VLAN pair) are associated with the corresponding child policy.

In this case, both the **match vlan** and **match vlan inner** commands can match on single VLANs or a set of VLANs. When either or both of these commands are configured with a set of VLANs, the class map represents all combinations of S-VLAN-and-C-VLAN pairs possible with the configured S-VLANs and C-VLANs. For example, when a **match vlan** for a single VLAN is configured with a **match vlan inner** for a set of VLANs in a class map with the logical operation **match-all**, the class map matches all packets with the configured C-VLANs tunneled into the same S-VLAN.

- Classification based on multiple S-VLANs, C-VLANs, or S-VLAN-and-C-VLAN-pairs in a parent-level class map with the logical-operation **match-all** is *not* allowed because it is not a legitimate packet classification criterion.

Child-Level and Nonhierarchical Policy-Map Guidelines

- A child-level policy map in a hierarchical policy map has the same structure and configuration guidelines as a nonhierarchical policy map. Both of these kinds of policy maps are called *child policy maps*, and the classes in these policy maps are called *child-level* classes.
- You must specify classification based on parameters (C-CoS, S-CoS, C-DSCP, and multifield flow classification) in the child-level classes. You *cannot* specify VLAN match criteria in the child-level-classes.
- Actions such as policing and marking are directly associated with a child-level class and are performed only on packets already classified by the associated parent class (if any) and child class.

Note QoS classification occurs after the VLAN-mapping operation (for example, tunneling) on the post-VLAN-mapped packet. During VLAN-mapping tunneling operation, the C-CoS is copied into the S-CoS. Therefore, classifying on an S-CoS-and-C-CoS pair in the post-VLAN-mapped packet is the same as classifying on either S-CoS or C-CoS.

- A child policy can include either Layer 2 classification criteria (**match cos**, **match cos inner**, and **match access-group** for a MAC-ACL) *or* Layer 3 classification criteria (**match ip dscp**, **match ip precedence**, and **match access-group** for an IP-ACL). If you specify both Layer 2 and Layer 3 classification criteria in a child policy map, the configuration is rejected.
- In a child-level class map, when you configure classification based only on S-CoS (the child class map is configured with the logical-operation **match-any** with one or more **match cos** commands), all packets matching *any* of the S-CoS values are associated with the corresponding action.
- In a child-level class map, when you configure classification based only on C-CoS (the child class map is configured with the logical-operation **match-any** with one or more **match cos inner** commands), all packets matching *any* of the C-CoS values are associated with the corresponding action.
- In a child-level class map, when you configure classification based on S-CoS and C-CoS (the child class map is configured with the logical-operation **match-all** with one **match cos** command and one **match cos inner** command), all packets matching *both* of the COS values (matching the S-CoS-and-C-CoS pair) are associated with the corresponding child policy.
- In a child-level class map, configuring classification based on multiple S-CoS or C-CoS values or S-CoS-and-C-CoS-pairs with the logical-operation **match-all** is *not* allowed because it is not a legitimate packet classification criteria.
- When a per-port policy or child-level policy in a per-port, per-VLAN policy is applied to QinQ packets on QinQ ports, you cannot configure the policy map with a MAC-ACL classification matching on a Layer 2 protocol.

- When a per-port policy or child-level policy in a per-port, per-VLAN policy is applied to QinQ packets on QinQ ports, you cannot configure the policy with an IP-ACL classification matching on Layer 4 ports, such as transport protocol TCP/UDP ports, or on any Layer 3 protocol types except TCP, UDP, and Stream Control Transmission Protocol (SCTP).
- You cannot associate a particular S-VLAN (**match vlan**) with these combinations of child policies at the same time across the switch:
  - A Layer 2 child policy (classifying on S-COS, C-COS, or MAC access group) *and* a Layer 3 child policy (classifying on DSCP, precedence, or IP access group).
  - A **class-default** child-policy *and* a Layer 3 child policy (classifying on DSCP, precedence, or IP access group).
- You cannot associate classes matching on only C-VLAN (**match vlan inner**) with these combinations of child policies at the same time across the switch:
  - A Layer 2 child policy (classifying on S-COS, C-COS, or MAC access group) *and* a Layer 3 child policy (classifying on DSCP, precedence, or IP access group).
  - A **class-default** child-policy *and* a Layer 3 child policy (classifying on DSCP, precedence, or IP access group),

Configuring the QinQ Ports

You can configure port-based QinQ on an ingress port in one of two ways:

- Configuring an 802.1Q Tunneling Port (All-to-One Bundling), page 5
- Configuring Traditional QinQ (All-to-One Bundling) on a Trunk Port, page 6

You can also configure VLAN-based QinQ, or selective QinQ, on a trunk port:

- Configuring Selective QinQ on a Trunk Port, page 7

For more information about configuring tunnel ports, see the chapter on "Configuring IEEE 802.1Q Tunneling, VLAN Mapping, and Layer 2 Protocol Tunneling" in the ME 3400E software configuration guide.

Configuring an 802.1Q Tunneling Port (All-to-One Bundling)

Beginning in privileged EXEC mode, follow these steps to configure a port as an 802.1Q tunnel port:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter interface configuration mode for the interface to be configured as a tunnel port. This should be the edge port in the service-provider network that connects to the customer switch. Valid interfaces include physical interfaces and port-channel logical interfaces (port channels 1 to 48).
Step 3	**no shutdown**	Enable the port, if necessary. By default, UNIs and ENIs are disabled, and NNIs are enabled.

	Command	Purpose
Step 4	**switchport access vlan** *vlan-id*	Specify the default VLAN, which is used if the interface stops trunking. This VLAN ID is specific to the particular customer. **Note** The access VLAN becomes the S-VLAN when **switchport mode dot1q-tunnel** is configured on the port. If the VLAN is a UNI-ENI isolated VLAN, local switching does not occur between UNIs and ENIs. If the VLAN is a UNI-ENI community VLAN, local switching can occur.
Step 5	**switchport mode dot1q-tunnel**	Set the interface as an 802.1Q tunnel port.
Step 6	**exit**	Return to global configuration mode.
Step 7	**vlan dot1q tag native**	(Optional) Set the switch to enable tagging of native VLAN packets on all 802.1Q trunk ports. When not set, and a customer VLAN ID is the same as the native VLAN, the trunk port does not apply a metro tag (outer tag with the customer VLAN ID), and packets could be sent to the wrong destination.
Step 8	**end**	Return to privileged EXEC mode.
Step 9	**show running-config**	Display the ports configured for 802.1Q tunneling.
	show dot1q-tunnel	Display the ports that are in tunnel mode.
Step 10	**show vlan dot1q tag native**	Display 802.1Q native VLAN tagging status.
Step 11	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Configuring Traditional QinQ (All-to-One Bundling) on a Trunk Port

Beginning in privileged EXEC mode, follow these steps to configure VLAN mapping for traditional QinQ on a trunk port. By default, configuring tunneling bundles all packets on the port into the configured S-VLAN.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter interface configuration mode for the interface connected to the service-provider network. You can enter a physical interface or an EtherChannel port channel.
Step 3	**switchport mode trunk**	Configure the interface as a trunk port.
Step 4	**switchport trunk allowed vlan** *vlan-id*	Configure the outer VLAN of the service provider network (S-VLAN) to to be allowed on the interface. This should be the same outer VLAN ID entered in the next step.
Step 5	**switchport vlan mapping default dot1q-tunnel** *outer vlan-id*	Configure VLAN mapping so that all packets entering the port are bundled into the specified S-VLAN: *outer-vlan-id*—Enter the outer VLAN ID (S-VLAN) of the service-provider network. The range is from 1 to 4094.
Step 6	**end**	Return to privileged EXEC mode.

	Command	Purpose
Step 7	**show interfaces** *interface-id* **vlan mapping**	Verify the configuration.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Configuring Selective QinQ on a Trunk Port

Beginning in privileged EXEC mode, follow these steps to configure VLAN mapping for selective QinQ on a trunk port. Note that you can configure one-to-one mapping and selective QinQ on the same interface, but you cannot use the same C-VLAN IDs in both configurations. You can use the **default drop** keywords to specify that traffic is dropped unless the specified C-VLAN ID and S-VLAN ID combination is explicitly mapped.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter interface configuration mode for the interface connected to the service-provider network. You can enter a physical interface or an EtherChannel port channel.
Step 3	**switchport mode trunk**	Configure the interface as a trunk port.
Step 4	**switchport vlan mapping** *vlan-id* **dot1q-tunnel** *outer vlan-id*	Enter the VLAN IDs to be mapped: • *vlan-id*—the customer VLAN ID (C-VLAN) entering from the customer network. The range is from 1 to 4094. You can enter a string of VLAN-IDs. • *outer-vlan-id*—Enter the outer VLAN ID (S-VLAN) of the service-provider network. The range is from 1 to 4094.
Step 5	**switchport vlan mapping default drop**	(Optional) Specify that all packets on the port are dropped if they do not match the VLANs specified in Step 4.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show interfaces** *interface-id* **vlan mapping**	Verify the configuration.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Using Class Maps to Define a Traffic Class

You use the **class-map** global configuration command to name and to isolate a specific traffic flow or class from all other traffic. A class map defines the criteria to match against a specific traffic flow to further classify it. Match statements can include an ACL, CoS value, DSCP value, IP precedence values QoS group values, or VLAN IDs. You define match criterion with one or more **match** statements entered in the class-map configuration mode.

Configuring Class Maps for Input Policy Maps

Follow these guidelines when configuring class maps for an input policy map:

- A **match-all** or **match-any** class map with ACL match criteria (**match access-group**) cannot have more than one classification criterion (one match statement).
- A **match-all** class with DSCP or IP precedence match criteria cannot have more than one classification criterion (one match statement).
- You can use **match vlan** or **match vlan inner** match statements to match VLAN IDs. A **match-all** class map cannot have more than one **match vlan** classification criterion (match statement) or more than one **match vlan inner** classification criterion. However, a **match-all** class map can have one **match vlan** classification criterion and one **match vlan inner** classification criterion.
- You can use **match cos** or **match cos inner** match statements to match CoS values. A **match-all** class map cannot have more than one **match cos** classification criterion (match statement) or more than one **match cos inner** classification criterion. However, a **match-all** class map can have one **match cos** classification criterion and one **match cos inner** classification criterion.
- A **match-any** class map can have multiple match statements.
- You use a class map with the **match vlan** or **match vlan inner** command in the parent policy in input hierarchical policy maps for per-port, per-VLAN QoS on ports. A policy is considered a parent policy map when it has one or more of its classes associated with a child policy map. Each class within a parent policy map is called a parent class. You can configure only the **match vlan** or **match vlan inner** command in parent classes. You cannot configure the **match vlan** or **match vlan inner** command in classes within the child policy map.
- You use a class map with the **match ip dscp, match ip precedence, match access-group, match cos**, or **match cos inner** commands in a nonhierarchical policy or in the child policy of an input hierarchical policy map for per-port, per-VLAN QoS on ports. You cannot configure the **match ip dscp, match ip precedence, match access-group, match cos,** or **match cos inner** commands in the parent class of an input hierarchical policy map.
- For an input policy map, you cannot configure an IP classification (**match ip dscp**, **match ip precedence**, **match access-group** for an IP ACL) and a Layer 2 classification (**match cos, match cos inner,** or **match access-group** for a MAC ACL) in the same policy map or class map. For a per-port, per-VLAN hierarchical policy map, this applies to the child policy map.
- When a child policy is associated with a parent class that is classifying on the C-VLAN by using the **match vlan inner** command, you cannot configure the policy with a MAC-ACL classification matching on a Layer 2 protocol type.
- When a child policy is associated with a parent class that is classifying on the C-VLAN by using the **match vlan inner** command, you cannot configure the policy with an IP-ACL classification matching on Layer 4 ports, such as Transport protocol TCP/UDP ports, or on any Layer 3 protocol types except TCP, UDP and Stream Control Transmission Protocol (SCTP).
- You cannot configure **match qos-group** for an input policy map.
- The maximum number of class maps on the switch is 1024.

Beginning in privileged EXEC mode, follow these steps to create a class-level class-map and to define the match criteria to classify traffic for an input policy map. This procedure is required.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**class-map** [**match-all** | **match-any**] *class-map-name*	Create a class map, and enter class-map configuration mode. By default, no class maps are defined. • (Optional) Use the **match-all** keyword to perform a logical-AND of all matching statements under this class map. All criteria in the class map must be matched. • (Optional) Use the **match-any** keyword to perform a logical-OR of all matching statements under this class map. One or more criteria must be matched. • For *class-map-name*, specify the name of the class map. If neither the **match-all** nor the **match-any** keyword is specified, the default is **match-all**.
Step 3	**match** {**vlan** *vlan-id* | **vlan inner** *vlan-id*}	Define the match criterion to classify traffic by VLAN. You can configure these match criteria only in the parent class map of a hierarchical policy-map. By default, no match criterion is defined. • Enter **vlan** *vlan-id* to match a packet based on the service-provider VLAN ID (S-VLAN). For QinQ, where an incoming customer packet is tunneled into an S-tag, this is the VLAN value in the imposed S-tag. For all other cases, this is the VLAN value in the incoming packet. • Enter **vlan inner** *vlan-id* to match a packet based on the C-VLAN, the inner customer VLAN ID of an 802.1Q tunnel. For QinQ, where an incoming customer packet is tunneled into an S-tag, this is the VLAN value in the incoming customer packet. For all other cases, this command has no effect. For *vlan-id*, you can specify a single VLAN identified by a VLAN number or a range of VLANs separated by a hyphen. The range is 1 to 4094.
or		

	Command	Purpose
Step 3b	**match** {**access-group** *acl-number-or-name* | **cos** *cos-list* | **cos inner** *cos-list* | **ip dscp** *dscp-list* | **ip precedence** *ip-precedence-list*}	Define the match criterion to classify traffic by QoS per-hop-behavior markings (CoS and DSCP) or flows. You can configure these match criterion only in the child class map of a hierarchical policy map or in classes of a nonhierarchical policy map. By default, no match criterion is defined. • Enter **access-group** *acl-number-or-name* for multifield flow classification based on the IP ACL or MAC ACL of the incoming customer packet, regardless of whether the packet is tunneled into an S-tag (QinQ) or not. Enter the number or name of the ACL access group. • Enter **cos** *cos-list* to match a packet based on the service-provider CoS value (S-CoS). For QinQ, where an incoming packet is tunneled into an S-tag, this is the CoS value in the imposed S-tag. For all other cases, this is the CoS value in the incoming packet. You can specify up to four Layer 2 CoS values to match against the packet. Separate each value with a space. The range is 0 to 7. • Enter **cos inner** *cos-list* to match a packet based on the C-CoS, the inner (customer) CoS value of an 802.1Q tunnel. For QinQ, where an incoming packet is tunneled into an S-tag, this is the CoS value in the incoming customer packet. For all other cases, this command has no effect. You can spe*cify* up to four Layer 2 CoS values to match against the packet. Separate each value with a space. The range is 0 to 7. • Enter **ip dscp** *dscp-list* to match the DSCP value in the incoming customer packet, whether the packet is tunneled into an S-tag (QinQ) or not. You can specify up to eight IP DSCP values to match against the packet. Separate each value with a space. The range is 0 to 63. • Enter **ip precedence** *ip-precedence-list* to match the IP-precedence value in the incoming customer packet, whether the packet is tunneled into an S-tag (QinQ) or not. You can specify up to eight IP-precedence values to match against the packet. Separate each value with a space. The range is 0 to 7. **Note** You cannot mix combinations of VLAN match criteria, per-hop-behavior match criteria, and flow match criteria within a class map.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show class-map**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To apply QoS policing and marking actions to the class, create and name a policy map by using the **policy-map** global configuration command to enter policy-map configuration mode. In this mode, enter the **class** command with the QinQ class map name, and then specify the action to take on all traffic in the class. See the “Configuring QoS” chapter in the ME 3400E software configuration guide for configuration details.

Then enter interface configuration mode for the ingress port on which QinQ is configured, and use the **service-policy input** interface configuration command to attach the traffic policy to the interface.

Configuring Class Maps for Output Policy Maps

Follow these guidelines when configuring class maps for an output policy map:

- You cannot configure **match access-group**, **match vlan**, **match vlan inner**, or **match cos inner** in an output policy map.
- A **match-all** class map containing DSCP, IP precedence, CoS, or qos-group match criteria cannot have more than one classification criterion (one match statement).
- A **match-any** class map can have multiple match statements.
- No two class maps can have the same classification criteria, that is, the same match qualifiers and values.
- The maximum number of class maps on the switch is 1024.

Beginning in privileged EXEC mode, follow these steps to create a class-level class-map and to define the match criterion to classify traffic for an output policy map. This procedure is required.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**class-map** [**match-all** | **match-any**] *class-map-name*	Create a class map, and enter class-map configuration mode. By default, no class maps are defined. • (Optional) Use the **match-all** keyword to perform a logical-AND of all matching statements in this class map. All criteria in the class map must be matched. • (Optional) Use the **match-any** keyword to perform a logical-OR of all matching statements in this class map. One or more criteria must be matched. • For *class-map-name*, specify the name of the class map. If neither the **match-all** nor the **match-any** keyword is specified, the default is **match-all**.

	Command	Purpose
Step 3b	**match** {**cos** *cos-list* | **ip dscp** *dscp-list* | **ip precedence** *ip-precedence-list* | **qos-group** *value*}	Define the match criteria to classify traffic by QoS per-hop-behavior markings (CoS and DSCP). You can configure these match criteria only in the child class map of a hierarchical policy map or in classes of a nonhierarchical policy map. By default, no match criterion is defined. • Enter **cos** *cos-list* to match a packet based on the CoS value in the outgoing packet. You can specify up to four Layer 2 CoS values. Separate each value with a space. The range is 0 to 7. • Enter **ip dscp** *dscp-list* to match the DSCP value in the outgoing packet. You can specify up to eight IP DSCP values. Separate each value with a space. The range is 0 to 63. • Enter **ip precedence** *ip-precedence-list* to match the IP-precedence value in the outgoing packet. You can specify up to eight IP-precedence values. Separate each value with a space. The range is 0 to 7. • Enter **qos-group** *value* to specify the QoS group number. The range is 0 to 99. QoS group matching is supported only in output policy maps.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show class-map**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

As with input policies, you then create and name a policy map by using the **policy-map** global configuration command to enter policy-map configuration mode. In this mode, enter the **class** command with the QinQ class map name, and then specify the action to be taken on all traffic in the class. See the "Configuring QoS" chapter in the ME 3400E software configuration guide for configuration details.

Then enter interface configuration mode for the egress port on which QinQ is configured and use the **service-policy output** interface configuration command to attach the traffic policy to the interface.

Configuration Examples

Example 1: C-DSCP-Based QoS Classification for Port-Based QinQ

This configuration produces these results:

- All customer traffic on Fast Ethernet port 0/1 is tunneled into an S-TAG with VLAN 100.
- The policy-map *uni-parent-policy* acts on all tagged and untagged customer traffic.
- Packets with a DSCP value of *ef* are classified by the class *voice-L3* and policed to 5 Mb.
- Packets with a DSCP value of *af41* are classified by the class *video-L3* and policed to 40 Mb to color the packets without dropping excess traffic.
- The DSCP value of all other packets is reset to *default* 0.

Child Class

```
Switch(config)# class-map match-any video-L3
Switch(config-cmap)# match ip dscp af41
Switch(config-cmap)# exit
Switch(config)# class-map match-any voice-L3
Switch(config-cmap)# match ip dscp ef
Switch(config-cmap)# exit
```

Child Policy

```
Switch(config)# policy-map child-policy-3
Switch(config-pmap)# class voice-L3
Switch(config-pmap-c)# police cir 5000000
Switch(config-pmap-c-police)# conform-action set-dscp-transmit 5
Switch(config-pmap-c-police)# exceed-action drop
Switch(config-pmap-c-police)# exit
Switch(config-pmap-c)# exit
Switch(config-pmap)# class video-L3
Switch(config-pmap-c)# police cir 40000000
Switch(config-pmap-c-police)# conform-action set-dscp-transmit 4
Switch(config-pmap-c-police)# exceed-action set-dscp-transmit 1
Switch(config-pmap-c-police)# exit
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set dscp 0
Switch(config-pmap-c)# exit
```

Parent Class

```
Switch(config)# class-map match-any internet-access
Switch(config-cmap)# match vlan 100
Switch(config-cmap)# exit
```

Parent Policy

```
Switch(config)# policy-map uni-parent-policy
Switch(config-pmap)# class internet-access
Switch(config-pmap-c)# service-policy child-policy-3
Switch(config-pmap-c)# exit
```

Interface

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport access vlan 100
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# service-policy input uni-parent-policy
Switch(config-pmap-c)# exit
```

Example 2: C-DSCP and C-CoS-Based QoS Classification for VLAN-Based QinQ

This configuration produces these results:

- Customer traffic on Fast Ethernet port 0/1 with C-VLAN 200 is tunneled into an S-TAG with S-VLAN 100.
- Customer traffic on Fast Ethernet port 0/1 with C-VLANs 210 to 220 is tunneled into an S-TAG with S-VLAN 110.
- Customer traffic on Fast Ethernet port 0/1 with C-VLANs 230 and 240 is tunneled into an S-TAG with S-VLAN 130.
- Customer traffic on Fast Ethernet port 0/1 with C-VLAN 241 is tunneled into an S-TAG with S-VLAN 131.
- Customer traffic on Fast Ethernet port 0/1 with C-VLAN 242 is tunneled into an S-TAG with S-VLAN 132.
- Customer traffic on Fast Ethernet port 0/1 with VLANs 133 to 150 is bridged normally with the same VLAN.
- After the above VLAN-mapping operation, policy-map *uni-parent-policy* acts on all single-tagged, double-tagged, and untagged packets.
- All packets with an S-VLAN of 100 *and* a C-VLAN of 200 (packets with C-VLAN 200 tunneled into S-VLAN 100) are classified by the class *L2-vpn* and subject to *child-policy-1*. In *child-policy-1*, the packets are classified by C-CoS in classes *voice-L2* and *video-L2,* and the specified policing and marking actions occur.
- All packets with an S-VLAN of 110 *and* a C-VLAN in the range of 210 to 220 (packets with C-VLANs 210 to 220 tunneled into S-VLAN 110) are classified by the class *voice-gateway* and subject to *child-policy-2*. In *child-policy-1*, the packets are classified by C-CoS in the classes *voice-L2* and *video-L2,* and the specified policing and marking actions occur.
- All packets with an S-VLAN in the range 130 to 132 and a C-VLAN of 230 or in the range of 240 to 242 (packets with C-VLANs 230, 240 to 242 tunneled into any one of the S-VLANs 130, 131, 132) are classified by the class *internet-access* and subject to *child-policy-3*. In *child-policy-3*, the packets are classified by C-DSCP in the classes *voice-L3* and *video-L3,* and the specified policing and marking actions occur.

Child Class

```
Switch(config)# class-map match-any video-L2
Switch(config-cmap)# match cos inner 3
Switch(config-cmap)# exit

Switch(config)# class-map match-any voice-L2
Switch(config-cmap)# match cos inner 5
Switch(config-cmap)# exit

Switch(config)# class-map match-any video-L3
Switch(config-cmap)# match ip dscp af41
Switch(config-cmap)# exit

Switch(config)# class-map match-any voice-L3
Switch(config-cmap)# match ip dscp ef
Switch(config-cmap)# exit
```

Child Policy

```
Switch(config)# policy-map child-policy-1
Switch(config-pmap)# class voice-L2
Switch(config-pmap-c)# police cir 10000000 bc 50000
Switch(config-pmap-c-police)# conform-action set-cos-transmit 5
Switch(config-pmap-c-police)# exceed-action drop
Switch(config-pmap-c-police)# exit
Switch(config-pmap-c)# exit
Switch(config-pmap)# class video-L2
Switch(config-pmap-c)# set cos 4
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set cos 0
Switch(config-pmap-c)# exit

Switch(config)# policy-map child-policy-2
Switch(config-pmap)# class voice-L2
Switch(config-pmap-c)# police cir 5000000 bc 50000
Switch(config-pmap-c-police)# conform-action set-cos-transmit 6
Switch(config-pmap-c-police)# exceed-action drop
Switch(config-pmap-c-police)# exit
Switch(config-pmap-c)# exit
Switch(config-pmap)# class video-L2
Switch(config-pmap-c)# set cos 3
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set cos 0
Switch(config-pmap-c)# exit

Switch(config)# policy-map child-policy-3
Switch(config-pmap)# class voice-L3
Switch(config-pmap-c)# police cir 5000000
Switch(config-pmap-c-police)# conform-action set-dscp-transmit 5
Switch(config-pmap-c-police)# exceed-action drop
Switch(config-pmap-c-police)# exit
Switch(config-pmap-c)# exit
Switch(config-pmap)# class video-L3
Switch(config-pmap-c)# police cir 40000000
Switch(config-pmap-c-police)# conform-action set-dscp-transmit 4
Switch(config-pmap-c-police)# exceed-action set-dscp-transmit 1
Switch(config-pmap-c-police)# exit
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set dscp 0
Switch(config-pmap-c)# exit
```

Parent Class

```
Switch(config)# class-map match-all L2-vpn
Switch(config-cmap)# match vlan 100
Switch(config-cmap)# match vlan inner 200
Switch(config-cmap)# exit

Switch(config)# class-map match-all voice-gateway
Switch(config-cmap)# match vlan 110
Switch(config-cmap)# match vlan inner 210-220
Switch(config-cmap)# exit

Switch(config)# class-map match-all internet-access
Switch(config-cmap)# match vlan 130-132
Switch(config-cmap)# match vlan inner 230, 240-242
Switch(config-cmap)# exit
```

Parent Policy

```
Switch(config)# policy-map uni-parent-policy
Switch(config-pmap)# class L2-vpn
Switch(config-pmap-c)# service-policy child-policy-1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class voice-gateway
Switch(config-pmap-c)# service-policy child-policy-2
Switch(config-pmap-c)# exit
Switch(config-pmap)# class internet-access
Switch(config-pmap-c)# service-policy child-policy-3
Switch(config-pmap-c)# exit
```

Interface

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan 100, 110, 130-150
Switch(config-if)# switchport vlan mapping 200 dot1q-tunnel 100
Switch(config-if)# switchport vlan mapping 210-220 dot1q-tunnel 110
Switch(config-if)# switchport vlan mapping 230 dot1q-tunnel 130
Switch(config-if)# switchport vlan mapping 240 dot1q-tunnel 130
Switch(config-if)# switchport vlan mapping 241 dot1q-tunnel 131
Switch(config-if)# switchport vlan mapping 242 dot1q-tunnel 132
Switch(config-if)# service-policy input uni-parent-policy
Switch(config-pmap-c)# exit
```

Commands

These commands have been modified to implement this feature:

- match cos, page 17
- match vlan, page 19

match cos

Use the **match cos** class-map configuration command to match a packet based on a Layer 2 class of service (CoS) marking. Use the **no** form of this command to remove the CoS match criteria.

match cos [**inner**] *cos-list*

no match cos [**inner**] *cos-list*

Syntax Description

inner	(Optional) Match a packet based on the C-CoS, the inner (customer) CoS value of an 802.1Q tunnel. If you do not enter the **inner** keyword, the packet is matched based on service-provider CoS value (S-CoS).
cos-list	List of up to four CoS values to match against incoming packets. Separate each value with a space. The range is 0 to 7.

Defaults

No match criteria are defined.

Command Modes

Class-map configuration

Command History

Release	Modification
12.2(44)EY	This command was introduced.
12-2(53)SE	The **inner** keyword was added.

Usage Guidelines

The **match cos** command specifies a CoS value to use as the match criteria to determine if packets belong to the class specified by the class map.

Before using the **match cos** command, you must enter the **class-map** global configuration command to specify the name of the class whose match criteria you want to establish.

- Enter **cos** *cos-list* to match a packet based on the service-provider CoS value (S-CoS). For QinQ, where an incoming packet is tunneled into an S-tag, this is the CoS value in the imposed S-tag. For all other cases, this is the CoS value in the incoming packet.

  You can specify up to four Layer 2 CoS values to match against the packet. Separate each value with a space. The range is 0 to 7.

- Enter **cos inner** *cos-list* to match a packet based on the C-CoS, the inner (customer) CoS value of an 802.1Q tunnel. For QinQ, where an incoming packet is tunneled into an S-tag, this is the CoS value in the incoming customer packet. For all other cases, this command has no effect.

You can spe*cify* up to four Layer 2 CoS values to match against the packet. Separate each value with a space. The range is 0 to 7.

Matching of CoS values is supported only on ports carrying Layer 2 VLAN-tagged traffic. That is, you can use the **cos** classification only on IEEE 802.1Q trunk ports.

You can use **match cos** classification in input and output policy maps.

Examples

This example shows how to create a class map called *in-class*, which matches all the incoming traffic with service provider CoS values of 1 and 4:

```
Switch(config)# class-map match-any in-class
Switch(config-cmap)# match cos 1 4
Switch(config-cmap)# exit
```

This example shows how to create a class map called *video-L2*, which matches all the incoming traffic with customer CoS value of 3:

```
Switch(config)# class-map match-any video-L2
Switch(config-cmap)# match cos inner 3
Switch(config-cmap)# exit
```

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

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to the class whose name you specify.
show class-map	Displays quality of service (QoS) class maps.

match vlan

Use the **match vlan** class-map configuration command in the parent policy of a hierarchical policy map to apply QoS policies to frames carried on a user-specified VLAN for a given interface. You can use hierarchical policy maps for per-VLAN classification on trunk ports Use the **no** form of this command to remove the match criteria.

match vlan [inner] *vlan-list*

no match vlan [inner] *vlan-list*

Syntax Description

inner	(Optional) Match a packet based on the C-VLAN, the inner customer VLAN ID of an 802.1Q tunnel. If you do not enter the **inner** keyword, the packet is matched based on the service-provider VLAN ID (S-VLAN).
vlan-list	Specify a VLAN ID or a range of VLANs to match against incoming packets in a parent policy map for per-port, per-VLAN QoS on a trunk port. You can enter up to 30 VLAN IDs. Use a hyphen for a range of VLANs. A VLAN range is counted as two VLAN IDs. Use a space to separate individual VLANs. The range is 1 to 4094.

Defaults

No match criteria are defined.

Command Modes

Class-map configuration

Command History

Release	Modification
12.2(44)EY	This command was introduced.
12-2(53)SE	The **inner** keyword was added.

Usage Guidelines

The feature is supported only using a 2-level hierarchical input policy map, where the parent-level defines the VLAN-based classification, and the child-level defines the QoS policy to be applied to the corresponding VLAN(s).

You can configure multiple service classes at the parent-level to match different combinations of VLANs, and you can apply independent QoS policies to each parent-service class using any child-policy map

A policy is considered a parent policy map when it has one or more of its classes associated with a child policy-map. Each class within a parent policy map is called a parent class. You can configure only the **match vlan** command in parent classes. You cannot configure the **match vlan** command in classes within the child policy map.

- Enter **vlan** *vlan-id* to match a packet based on the service-provider VLAN ID (S-VLAN). For QinQ, where an incoming customer packet is tunneled into an S-tag, this is the VLAN value in the imposed S-tag. For all other cases, this is the VLAN value in the incoming packet.

- Enter **vlan inner** *vlan-id* to match a packet based on the C-VLAN, the inner customer VLAN ID of an 802.1Q tunnel. For QinQ, where an incoming customer packet is tunneled into an S-tag, this is the VLAN value in the incoming customer packet. For all other cases, this command has no effect.

A per-port, per-VLAN parent-level class map supports only a child-policy association; it does not allow any actions to be configured. In addition, for a parent-level class map, you cannot configure an action or a child-policy association for the class **class-default**.

You cannot configure a mixture of Layer 2 and Layer 3 class maps in a child policy map. When you attempt to associate such a child policy map with a parent policy, the configuration is rejected. However, you can associate Layer 2 child policies and Layer 3 child policies with different parent-level class maps.

Per-port, per-VLAN QoS is supported only on IEEE 802.1Q trunk ports.

Once a per-port, per-vlan hierarchical policy-map is attached to an interface, a parent-class with vlan-based classification can not be dynamically added or removed. The service policy needs to be detached from the interface before making this configuration change.

When the child policy map attached to a VLAN or set of VLANs contains only Layer 3 classification (**match ip dscp**, **match ip precedence**, **match IP ACL**), you must be careful to ensure that these VLANs are not carried on any port other than the one on which this per-port, per-VLAN policy is attached. Not following this restriction could result in improper QoS behavior for traffic ingressing the switch on these VLANs.

We also recommend that you restrict VLAN membership on the trunk ports to which the per-port, per-VLAN is applied by using the **switchport trunk allowed vlan** interface configuration command. Overlapping VLAN membership between trunk ports that have per-port, per-VLAN policies with Layer 3 classification could also result in unexpected QoS behavior.

Before using the **match vlan** command, you must enter the **class-map** global configuration command to specify the name of the class whose match criteria you want to establish.

Examples

In this example, the class maps in the child-level policy map specify matching criteria for voice and video traffic, and the child policy map sets the action for input policing each type of traffic. The parent-level policy map specifies the VLANs to which the child policy maps are applied on the specified port.

```
Switch(config)# class-map match-any dscp-23 video
Switch(config-cmap)# match ip dscp 23
Switch(config-cmap)# exit
Switch(config)# class-map match-any dscp-63 voice
Switch(config-cmap)# match ip dscp-63
Switch(config-cmap)# exit
Switch(config)# class-map match-any customer-1-vlan
Switch(config-cmap)# match vlan 100
Switch(config-cmap)# match vlan 200
Switch(config-cmap)# match vlan 300
Switch(config-cmap)# exit
```


Note You can also enter the match criteria as **match vlan 100 200 300** with the same result.

```
Switch(config)# policy-map child policy-1
Switch(config-pmap)# class dscp-63 voice
Switch(config-pmap-c)# police cir 10000000 bc 50000
Switch(config-pmap-c)# conform-action set-cos-transmit 5
Switch(config-pmap-c)# exceed-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# class dscp-23 video
Switch(config-pmap-c)# set cos 4
```

```
Switch(config-pmap-c)# set ip precedence 4
Switch(config-pmap-c)# exit

Switch(config)# policy-map parent-customer-1
Switch(config-pmap)# class customer-1-vlan
Switch(config-pmap-c)# service-policy ingress-policy-1
Switch(config-pmap-c)# exit
```

In this example, all packets with an S-VLAN of 100 *and* a C-VLAN of 200 (packets with C-VLAN 200 tunneled into S-VLAN 100) are classified by the class *L2-vpn* and packets with an S-VLAN of 110 *and* a C-VLAN in the range of 210 to 220 (packets with C-VLANs 210 to 220 tunneled into S-VLAN 110) are classified by the class *voice-gateway.*

```
Switch(config)# class-map match-all L2-vpn
Switch(config-cmap)# match vlan 100
Switch(config-cmap)# match vlan inner 200
Switch(config-cmap)# exit

Switch(config)# class-map match-all voice-gateway
Switch(config-cmap)# match vlan 110
Switch(config-cmap)# match vlan inner 210-220
Switch(config-cmap)# exit
```

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

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class name.
show class-map	Displays quality of service (QoS) class maps.

Related Documents

Documents with complete information about the Cisco ME 3400 are available from this Cisco.com site. For information about the latest released features, refer to the release notes, software configuration guides, and command references for Cisco IOS Release 12.2(50)SE.

http://www.cisco.com/en/US/products/ps9637/tsd_products_support_series_home.html

These are combined documents for the switches:

- *Cisco ME 3400E, ME 3400, and ME 2400 Ethernet Access Switches System Message Guide*

These documents are available for the Cisco ME 3400E switch:

- *Release Notes for the Cisco ME 3400E and ME 3400 Ethernet Access Switch*
- *Cisco ME 3400E Ethernet Access Switch Software Configuration Guide*
- *Cisco ME 3400E Ethernet Access Switch Command Reference*
- *Cisco ME 3400E Ethernet Access Switch Hardware Installation Guide*
- *Cisco ME 3400E Ethernet Access Switch Getting Started Guide*
- *Regulatory Compliance and Safety Information for the Cisco ME 3400E Ethernet Access Switch*

Other related documents:

- *Cisco Small Form-Factor Pluggable Modules Installation Notes*
- *Cisco CWDM GBIC and CWDM SFP Installation Note*
- These compatibility matrix documents are available from this Cisco.com site:

http://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html

- Cisco Gigabit Ethernet Transceiver Modules Compatibility Matrix
- Cisco 100-Megabit Ethernet SFP Modules Compatibility Matrix
- Cisco Small Form-Factor Pluggable Modules Compatibility Matrix
- Compatibility Matrix for 1000BASE-T Small Form-Factor Pluggable Modules

For information about the latest released features, refer to the release notes, software configuration guides, and command references for Cisco IOS Release 12.2(50)SE.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

This document is to be used in conjunction with the documents listed in the "Related Documents" section.