Queue Sharing and Redirection

In This Section

This section provides information to configure queue groups using the command line interface.

Topics in this section include:

Queue Sharing and Redirection

Queue groups are objects created on access or network Ethernet port or ingress forwarding plane of an IOM/IMM/XMA that allow SAP or IP interface forwarding classes to be redirected from the normal type of queue mapping to a shared queue. Queue groups may contain queues, policers, or a combination or the two depending on the type of queue group.The following types of queue groups are supported:

- Access ingress supports a single queue group instance per ingress port, or multiple queue groups created at the ingress forwarding plane level of the IOM/IMM/XMA. Access ingress port queue groups may only contain queues, whereas access ingress forwarding plane queue groups may only contain policers.
- Access egress supports the creation of multiple queue groups per egress port. These queue groups may only contain queues.
- Network ingress supports the creation of multiple queue groups at the ingress forwarding plane level of the IOM/IMM/XMA. These queue groups may only contain policers.
- Network egress supports the creation of multiple queue groups per egress port. These queue groups may contain queues, only, or queues and policers.

Supported Platforms

Queue sharing and redirection is supported on the SR and ESS platforms with the following IOM types:

- Access SAP port queue group supported on IOM-1 of types the iom-10g, iom-20g, and iom- 20g-b. Network queue groups are not supported.
- Access SAP port and network port queue group are supported on IOM-2s. Up to 20K SAPs per MDA can be configured with any supported Ethernet MDA.
- Access SAP port and ingress forwarding plane and network port and ingress forwarding plane queue groups are supported on IOM-3s.

Queue sharing and redirection are also supported in conjunction with the use of existing Ethernet MDA, Ethernet CMA, HS-MDA and the VSM MDA.

Queue Group Applications

Access SAP Queue Group Applications

Normally, each SAP (Service Access Point) has dedicated ingress and egress queues that are only used by that particular SAP. The SAP queues are created based on the queue definitions within the SAP ingress and SAP egress QoS policy applied to the SAP. Each packet that enters or egresses the SAP has an associated forwarding class. The QoS policy is used to map the forwarding class to one of the SAP's local queue IDs. This per-SAP queuing has advantages over a shared queuing model in that it allows each SAP to have a unique scheduling context per queue. During congestion, SAPs operating within their conforming bandwidth will experience little impact since they do not need to compete for queue buffer space with misbehaving or heavily loaded SAPs.

The situation is different for a shared or port-queuing model that is based on policing color packets that conform or exceed a static rate before the single queue and that use WRED or drop tail functions to essentially reserve room for the conforming packets.

In this model, there is no way for the conforming packets to go to the head of line in the view of the port scheduler. Another advantage of per-SAP queuing is the ability for the SAP queues to perform shaping to control burst sizes and forwarding rates based on the SAPs defined SLA. This is especially beneficial when a provider is enforcing a sub-line rate bandwidth limit and the customer does not have the ability to shape at the CE.

However, there are cases where per-SAP queuing is not preferred. Per SAP queuing requires a more complex provisioning model in order to properly configure the SAPs ingress and egress SLAs. This requires service awareness at some points in the network where an aggregation function is being performed. In this case, a shared queuing or per-port queuing model will suffice. Creating ingress and egress access queue groups and mapping the SAPs forwarding classes to the queues within the queue group provides this capability.

A further use case is where a set of ingress SAPs, which may represent a subset of the total number of ingress SAPs, is to be shaped or policed on an aggregate per-forwarding class basis when those SAPs are spread across a LAG on multiple ingress ports, and where color-aware treatment is required so that explicitly in-profile traffic is honored up to CIR, but above which it is marked as out of profile

The above scenarios can be supported with access queue groups. A single ingress queue group is supported per access port, while multiple ingress queue group instances are supported per IOM/IMM/XMA forwarding plane. To provide more flexibility on the egress side of the access port, multiple egress access queue group queue-group instances are supported per egress access port.

Since queue redirection is defined per forwarding class, it is possible to redirect some forwarding classes to a queue group while having others on the SAP use the SAP local queues. This is helpful when shared queuing is only desired for a few applications such as VOIP or VOD while other applications still require queuing at the SAP level.

Network Port Queue Groups for IP Interfaces

Queue groups may be created on egress network ports in order to provide network IP interface queue redirection. A single set of egress port based forwarding class queues are available by default and all IP interfaces on the port share the queues. Creating a network queue group allows one or more IP interfaces to selectively redirect forwarding classes to the group in order to override the default behavior. Using network egress queue groups it is possible to provide dedicated queues for each IP interface.

Note that non-IPv4/IPv6/MPLS packets will remain on the regular network port queues. Therefore, when using an egress port-scheduler it is important to parent the related regular network port queues to appropriate port-scheduler priority levels to ensure the desired operation under port congestion. This is particularly important for protocol traffic such as LACP, EFM-OAM, ETH-CFM, ARP and IS-IS, which by default use the FC NC regular network port queue.

Pseudowire Shaping for Layer 2 and Layer 3 Services

This feature allows the user to perform ingress and egress data path shaping of packets forwarded within a spoke-sdp (PW). It applies to a VLL service, a VPLS/B-VPLS service, and an IES/VPRN spoke-interface.

The ingress PW rate-limiting feature uses a policer in the queue-group provisioning model. This model allows the mapping of one or more PWs to the same instance of policers that are defined in a queue-group template.

Operationally, the provisioning model in the case of the ingress PW shaping feature consists of the following steps:

1. Create an ingress queue-group template and configure policers for each FC that needs to be redirected and optionally for each traffic type (unicast or multicast).
2. Apply the queue-group template to the network ingress forwarding plane where there exists a network IP interface that the PW packets can be received on. This creates one instance of the template on the ingress of the FP. One or more instances of the same template can be created.
3. Configure FC-to-policer mappings together with the policer redirect to a queue-group in the ingress context of a network QoS policy. No queue-group name is specified in this

step, which means the same network QoS policy can redirect different PWs to different queue-group templates.

4. Apply this network QoS policy to the ingress context of a spoke-sdp inside a service, or to the ingress context of a PW template and specify the redirect queue-group name.

One or more spoke-sdps can have their FCs redirected to use policers in the same policer queue-group instance.

The egress PW shaping provisioning model allows the mapping of one or more PWs to the same instance of queues, or policers and queues, that are defined in the queue-group template.

Operationally, the provisioning model consists of the following steps:

1. Create an egress queue-group template and configure queues only, or policers and queues for each FC which needs to be redirected.
2. Apply the queue-group template to the network egress context of all ports where there exists a network IP interface which the PW packets can be forwarded on. This creates one instance of the template on the egress of the port. One or more instances of the same template can be created.
3. Configure FC-to-policer or FC-to-queue mappings together with the redirect to a queue-group in the egress context of a network QoS policy. No queue-group name is specified in this step, which means the same network QoS policy can redirect different PWs to different queue-group templates.
4. Apply this network QoS policy to the egress context of a spoke-sdp inside a service, or to the egress context of a PW template and specify the redirect queue-group name.

One or more spoke-sdps can have their FCs redirected to use queues only, or queues and policers in the same queue-group instance.

Queue Group Templates and Port Queue Groups

Queue Group Templates

Before a queue group with a specific name may be created on a port or an IOM/IMM/XMA ingress forwarding plane, a queue group template with the same name must first be created. The template is used to define each queue, scheduling attributes and its default parameters. When a queue or policer is defined in a queue group template, that queue will exist in every instance of a port or forwarding plane queue group with that template name. The default queue or policer parameters (such as rate or mbs values) may be overridden with a specific value in each queue group. This works in a similar manner to SAP ingress or SAP egress QoS policies.

Queue sharing is also supported if the High Scale MDA (HSMDA) is used. On ingress, HSMDA queues are bypassed, and the queue group on the IOM forwarding plane is used. On egress, it is possible to redirect forwarding classes from multiple SAPs to an HSMDA queue group. Note that the HSMDA also uses the term *queue group* to describe a group of 8 pre-configured hardware queues on its egress port. When queue sharing and redirection is configured on egress, a set of 8 HSMDA queues could be configured as a part of the queue group template. These correspond to 8 hardware queues on the HSMDA. When all eight (8) egress fcs are mapped to the queue-group instantiated in the egress port, the per-sap hsmda queue-group resource is freed.

Port Queue Groups

Once an ingress or egress queue group template is defined, a port based queue group with the same name may be created. Port queue groups are named objects that act as a container for a group of queues. The queues are created based on the defined queue IDs within the associated queue group template. Port queue groups must be created individually on the ingress and egress sides of the port, but multiple port queue groups of the same template name may be created on egress ports if they have a different instance identifier. These are termed ‘queue group instances’. Each instance of a named queue group created on a port is an independent set of queues structured as per the queue group template. Port queue groups are only supported on Ethernet ports and may be created on ports within a LAG.

Forwarding Plane Queue Groups

Ingress forwarding plane queue groups allow groups of SAPs on one or more ports, or on a LAG on the IOM/IMM/XMA, to be bundled together from a QoS enforcement perspective with an aggregate rate limit to be enforced across all SAPs of a bundle. Multiple queue groups are supported per IOM/IMM/XMA or port on access ingress. These are implemented at the forwarding plane level on the ingress IOM so that SAPs residing on different ingress ports or SAPs on a LAG spread across ports on a given IOM can be redirected to the same queue group

Once an ingress queue group template is defined, a forwarding plane queue group with the same name may be created on an ingress forwarding plane of an IOM/IMM/XMA. Forwarding plane queue groups are named objects that act as a container for a group of policers. Queues are not supported in forwarding plane queue groups. Only hierarchical policers are supported in the forwarding plane queue group, rather than queues. These policers may be configured to use profile-aware behavior. The policers are created based on the defined policer IDs within the associated queue group template. Multiple forwarding plane queue groups of the same template name may be created on ingress if they have a different instance identifier. These are termed *queue group instances*. Each instance of a named queue group created on a forwarding plane is an independent set of policers structured as per the queue group template. Forwarding plane queue groups are only supported with Ethernet ports and may be created on IOM/IMM/XMAs with ports in a LAG.

Redirection Models

Two models are supported for forwarding class redirection. In the first, the actual instance of a queue group to use for forwarding class redirection is named in the QoS policy. This is termed *policy-based redirection*.

In the second model, the forwarding class queue or policers to apply redirection to are identified in the ingress or egress QoS policy. However, the specific named queue group instance is not identified until a QoS policy is applied to a SAP. This is termed *SAP-based redirection*.

Policy-based redirection allows different forwarding classes in the same QoS policy to be redirected to different queue groups, but it requires at least one QoS policy to be configured per queue group instance.

SAP-based redirection can require less QoS policies to be configured since the policy does not have to name the queue group. However, if redirected, all forwarding classes of a given SAP must use the same named queue group instance.

Policy based redirection is applicable to port queue groups on access ingress and access and network egress, while SAP based redirection is applicable to forwarding plane queue groups on access and network ingress, and port queue groups on access and network egress.

Access SAP Forwarding Class Based Redirection

Forwarding class redirection is provisioned within the SAP ingress or SAP egress QoS policy. In each policy, the forwarding class to queue ID mapping may optionally specify a named queue group instance (policy-based redirection) or may simply tag the forwarding class for redirection (SAP-based redirection). When the name is specified, the defined queue ID must exist in the queue group template with the same name.

Redirecting a SAP forwarding class to a queue within a port based queue group using policy-based redirection requires four steps:

1. Create an ingress or egress queue group template. If the forwarding class redirection is in the ingress SAP path, an ingress queue group template must be created. Similarly, an egress queue group template must be created for egress forwarding class redirection. Optionally, you can create the queues in a template by using default parameters. Individual queues must be created before they are associated with a forwarding class. The default queue parameters may be overridden on each port based queue group.
2. Create an ingress or egress queue group instance with the same name as the template on the port associated with the SAP. Examples are as follows:

   On ingress ports:
   config>port>ethernet>access>ingress>queue-group *queue-group-name*

   On egress ports:
   config>port>ethernet>access>egress>queue-group *queue-group-name* [**instance** *instance-id*]

   Queue parameter overrides can also be applied at this time.
3. Redirect the SAP ingress or SAP egress QoS policy forwarding class policer or queue to the queue group name and desired queue ID (Steps 2 and 3 may be done in opposite order). Examples are as follows:

   On ingress:
   config>qos>sap-ingress *policy-id*
       fc *fc-name*
           queue *queue-id* **group** *queue-group-name*

   On egress:
   config>qos>sap-egress *policy-id*
       fc *fc-name*
           queue *queue-id* **group** *queue-group-name* **instance** *instance-id*

config>qos>sap-egress *policy-id*
    fc *fc-name*
        policer *policer-id* **group** *queue-group-name* **instance** *instance-id*

4. Finally, the SAP ingress or SAP egress QoS policy must be applied to the SAP.

Redirecting a SAP forwarding class to a queue within an egress port based or ingress forwarding plane queue group using SAP-based redirection requires four steps:

1. Create an ingress or egress queue group template. If the forwarding class redirection is in the ingress SAP path, an ingress queue group template must be created. Similarly, an egress queue group template must be created for egress forwarding class redirection. Optionally, you can create the queues in a template by using default parameters. Individual queues must be created before they are associated with a forwarding class. The default queue parameters may be overridden on each port based queue group.
2. Create an ingress queue group instance on the forwarding plane of the IOM/IMM/XMA, or an egress port queue group with the same name as the template on the port associated with the SAP.

   On ingress:
   config>card>fp>ingress>access>queue-group *queue-group-name* **instance** *instance-id* [**create**]

   On egress:
   config>port>ethernet>access>egress>queue-group *queue-group-name* [**instance** *instance-id*]
3. Redirect the SAP ingress forwarding class policer in the SAP-ingress QoS policy using the keyword **fp-redirect-group** keyword on the policer, or SAP egress forwarding class queue or policer using the **port-redirect-group** keyword. (Steps 2 and 3 may be done in opposite order.)

   On ingress:
   config>qos>sap-ingress *policy-id*
       fc *fc-name*
           queue *queue-id* **fp-redirect-group**

   On egress:
   config>qos>sap-egress *policy-id*
       fc *fc-name*
           queue *queue-id* **port-redirect-group-queue**

   config>qos>sap-egress *policy-id*
       fc *fc-name*
           policer *policer-id* **port-redirect-group-queue**

4. Finally, the SAP ingress or SAP egress QoS policy must be applied to the SAP. The named queue group instance that was created on the ingress forwarding plane or the egress port must be specified at this time.

   On ingress:

   ```
   config>service>epipe>sap sap-id
           ingress
                   qos sap-ingress-policy-id fp-redirect-group queue-group-name instance instance-id
   ```

   On egress:

   ```
   config>service>epipe>sap sap-id
           egress
                   qos sap-egress-policy-id port-redirect-group queue-group-name instance instance-id
   ```

Note that redirection to a queue group on the HSMDA supports the SAP-based provisioning model, only.

Ingress and Egress SAP Forwarding Class Redirection Association Rules

Policy Based Provisioning Model

The association rules between SAP ingress and egress QoS policies and queue group templates are simple since both the target queue group name and queue ID within the group are explicitly stated within the access QoS policies.

The following association rules apply when the policy based provisioning model is applied with port queue groups.

When a SAP ingress QoS policy forwarding class is redirected to a queue group queue ID:

- If the queue group name does not exist as an ingress queue group template, the forwarding class redirection will fail.
- If a redirection queue ID does not exist within the ingress queue group template, the forwarding class redirection will fail.
- If the SAP ingress QoS policy is currently applied to a non-Ethernet port or an Ethernet port where the specified ingress queue group does not exist, the forwarding class redirection will fail.

When a SAP ingress QoS policy forwarding class redirection is removed from a queue group queue ID:

- If the forwarding class is being moved to another queue group queue ID that does not exist within an ingress queue group template, the redirection removal from the current queue group queue ID will fail.
- If the forwarding class is being moved to a local queue ID within the SAP ingress QoS policy and the local queue ID does not exist, the redirection removal from the current queue group queue ID will fail.
- If the forwarding class is being moved to a local queue ID within the SAP ingress QoS policy and it is the first forwarding class to be mapped to the queue ID the system will attempt to instantiate the queue on each ingress SAP where the SAP ingress QoS policy is applied. If the queue cannot be created on any of the SAPs, the redirection removal from the current queue group ID will fail.

When a SAP egress QoS policy forwarding class is redirected to a queue group queue ID:

- If the queue group name does not exist as an egress queue group template, the forwarding class redirection will fail.
- If a redirection queue ID does not exist within the egress queue group template, the forwarding class redirection will fail.

- If the SAP egress QoS policy is currently applied to a non-Ethernet port or an Ethernet port where the specified egress queue group does not exist, the forwarding class redirection will fail.

When a SAP egress QoS policy forwarding class redirection is removed from a queue group queue ID:

- If the forwarding class is being moved to another queue group queue ID that does not exist within an egress queue group template, the redirection removal from the current queue group queue ID will fail.
- If the forwarding class is being moved to a local queue ID within the SAP egress QoS policy and the local queue ID does not exist, the redirection removal from the current queue group queue ID will fail.
- If the forwarding class is being moved to a local queue ID within the SAP egress QoS policy and it is the first forwarding class to be mapped to the queue ID the system will attempt to instantiate the queue on each egress SAP where the SAP egress QoS policy is applied. If the queue cannot be created on any of the SAPs, the redirection removal from the current queue group ID will fail.

If the above operation is successful then:

- The system decrements the association counter for the egress queue group template with the same name as the queue group previously specified in the forwarding class redirection.
- The system decrements the queue ID association counter within the queue group template for the queue ID previously specified in the forwarding class redirection.
- The system decrements the port queue group association counter for each egress port queue group where the SAP egress QoS policy is applied to a SAP.

When a SAP ingress QoS policy with a forwarding class redirection to a queue group queue ID is applied to a SAP:

- If the queue group specified in any forwarding class redirection does not exist as an ingress port queue group on the port associated with the SAP, the SAP ingress QoS policy application will fail.

If the operation above is successful, then:

- The system increments the port queue group association counter for each ingress port queue group referenced in a forwarding class redirection on the port associated with the SAP. The ingress port queue group association counter is incremented for each forwarding class redirected to the queue group within the added policy.

When a SAP ingress QoS policy with a forwarding class redirection to a queue group queue ID is removed from a SAP:

- If removing the SAP ingress QoS policy from the SAP results in the need to instantiate an ingress queue for the SAP that cannot be created, the SAP ingress QoS policy removal action will fail.

If the operation above is successful, then:

- The system decrements the port queue group association counter for each egress port queue group referenced in a forwarding class redirection within the removed SAP egress QoS policy. The egress port queue group association counter is decremented for each forwarding class redirected to the queue group within the removed policy.

SAP-Based Provisioning Model

When a redirection to a named forwarding plane queue group instance is applied to a SAP on ingress:

- If the queue group name does not exist as an ingress queue group template, the redirection will fail.
- If a queue group name does exist as an ingress queue group template, but the specified instance-id has not been instantiated on the same forwarding plane as used by the SAP, the redirection will fail.
- If a redirected policer ID in the SAP ingress QoS policy does not match a policer ID in the named ingress queue group template, the redirection will fail.
- If the SAP ingress QoS policy is currently applied to a non-Ethernet port or an Ethernet port where the specified ingress queue group instance does not exist on the forwarding plane, the redirection will fail.

If the operation above is successful, then:

- The system increments the association counter for the ingress queue group template with the same name as the queue group specified in the SAP redirection for each forwarding class redirected to the template.
- The system increments the policer ID association counter within the queue group template for each forwarding class redirected to a policer ID.
- The system increments the forwarding plane queue group instance association counter for each ingress queue group instance where a SAP ingress QoS policy specifying redirection is applied to a SAP.

When redirection to a named queue group is removed from an ingress SAP:

- If the forwarding class is being moved to another queue group policer ID that does not exist within the ingress FP queue group, the redirection removal from the current queue group policer ID will fail.

- If the forwarding class is being moved to a local policer ID within the SAP ingress QoS policy and the local policer ID does not exist, the redirection removal from the current queue group policer ID will fail.
- If the forwarding class is being moved to a local policer ID within the SAP ingress QoS policy and it is the first forwarding class to be mapped to the policer ID the system will attempt to instantiate the policer on each ingress SAP where the SAP ingress QoS policy is applied. If the policer cannot be created on any of the SAPs, the redirection removal from the current queue group policer ID will fail.

If the operation above is successful, then:

- The system decrements the association counter for the ingress queue group template with the same name as the queue group previously specified in the forwarding class redirection.
- The system decrements the policer ID association counter within the queue group template for the policer ID previously specified in the forwarding class redirection.

The system decrements the forwarding plane queue group template association counter for each ingress queue group where redirection is applied to the ingress SAP.

For the SAP-based provisioning model, the rules for redirecting a forwarding class queue to an egress port queue group are similar to those on ingress.

- If an egress QoS policy containing one or more redirections is applied to a SAP, but either no queue group instance is specified at association time, or a named queue group instance is specified and either the queue group name or the instance identifier does not correspond to a queue group that has been created on the egress port, then the association will be rejected.
- If all of the redirections in an egress QoS policy are to queue ids that do not exist in the named queue group istance, then the association will be rejected.
- Note that if a policer local to a SAP feeds into a SAP based queue group queue instance, and the queue ID to use is not explicitly specified in the egress QoS policy (through the command policer policer-id port-redirect-group-queue) and is instead inferred from the forwarding class of the policer, but that forwarding class does not exist in the queue group template, then no error is generated. Instead, the queue with the lowest queue ID is used in the queue group instance. If at a later time, a user attempts to add a queue with a given queue-id to a policer redirect for a given forwarding class in the egress QoS template, then the system will check that the corresponding queue-id exists in any queue group instances associated with any SAPs using the QoS policy.

Access Queue Group Statistics

Port Queue Groups

When a forwarding class is redirected to a ingress or egress port queue group queue, the packets sent to the queue are statistically tracked by a set of counters associated with the queue group queue and not with any of the counters associated with the SAP.

This means that it is not possible to perform accounting within a queue group based on the source SAPs feeding packets to the queue. The statistics associated with the SAP will not reflect packets redirected to a port queue group queue.

The set of statistics per queue are eligible for collection in a similar manner as SAP queues. The collect-stats command enables or disables statistics collection in to a billing file based on the accounting policy applied to the queue group.

Forwarding Plane Queue Groups

When a forwarding class is redirected to a forwarding plane queue group queue or policer, the packets sent to the queue or policer are statistically tracked by a set of counters associated with the queue group queue/policer and not with any of the counters associated with the SAP.

This means that it is not possible to perform accounting within a queue group based on the source SAPs feeding packets to the queue. That is, the statistics associated with the SAP will not include packets redirected to a queue group queue.

Note that if the user enables the **packet-byte-offset** {**add** *bytes* | **subtract** *bytes*} option under the ingress queue-group policer, the byte counters of that policer will reflect the adjusted packet size.

The set of statistics per queue are eligible for collection in a similar manner to SAP queues. The **collect-stats** command enables or disables statistics collection in to a billing file based on the accounting policy applied to the queue group.

Network IP Interface Forwarding Class-Based Redirection

Forwarding class redirection for a network IP interface is defined in a four step process.

1. Create an ingress or egress queue group template with the appropriate queues or policers.
2. Apply an instance of an ingress queue-group template created in step 1 (containing only policers) to the FP ingress network configuration context of card X. In addition, or alternatively, apply an instance of an egress queue-group template created in step 1 to the network egress configuration context of port Y.
3. Configure the network QoS policy used on the IP interface to redirect ingress traffic to a policer ID (defined in the ingress queue-group template created in step 1) on the basis of forwarding-class and forwarding-type (unicast vs. multicast). In addition, or alternatively, configure the network QoS policy to redirect egress traffic to a queue ID and/or a policer ID based on forwarding-class.
4. Apply the network QoS policy to the network IP interface and at the same time specify the ingress and/or egress queue-group instances associated with the interface.

Egress Network Forwarding Class Redirection Association Rules

The association rules work differently for network egress IP interfaces than they do for access SAPs. Since the network QoS policy does not directly reference the queue group names, the system is unable to check for queue group template existence or queue ID existence when the forwarding class queue redirection is defined. Configuration verification can only be checked at the time the network QoS policy is applied to a network IP interface.

The system keeps an association counter for each queue group template and an association counter for each queue ID within the template. The system also keeps an association counter for each queue group created on a port.

When a network QoS policy is applied to an IP interface with the queue group parameter specified:

- If the queue group name does not exist as an egress queue group template, the QoS policy application will fail.
- If a redirection queue ID within the policy does not exist within the egress queue group template, the QoS policy application will fail.
- If the IP interface is bound to a port (or LAG) and the specified queue group name does not exist on the port, the QoS policy application will fail.

If the operation above is successful, then:

- The system increments the association counter for the queue group template with the same name as the queue group specified when the QoS policy is applied.
- The system increments the queue ID association counter within the queue group template for each forwarding class redirected to the queue ID.
- If the IP interface is currently bound to a port (or LAG), the association counter for the queue group on the port is incremented.

When the queue group parameter is removed from an IP interface:

- The system decrements the association counter for the queue group template with the same queue group name that was removed from the IP interface.
- The system decrements the queue ID association counter within the queue group template for each forwarding class that had previously been redirected to the queue ID.
- If the IP interface is currently bound to a port (or LAG), the association counter for the removed queue group on the port is decremented.

When a network QoS policy egress forwarding class redirection to a queue ID is removed or added:

- If a redirection is being added to a forwarding class and the queue ID does not exist on the queue groups for IP interfaces where the QoS policy is applied, the redirection will fail.

If the operation above is successful, then:

- The system finds all IP interfaces where the policy is applied.
- Finds all affected queue group templates based on the queue group associated with the QoS policy on each interface.
- If removing, the queue ID association counter is decremented within each queue group template based on the queue ID removed from the policy.
- If adding, the queue ID association counter is incremented within each queue group template based on the queue ID added to the policy.

When an IP interface associated with a queue group is bound to a port:

- If the specified egress queue group does not exist on the port, the port binding will fail.

If the operation above is successful, then:

- The system increments the association counter for the queue group on the port.

When an IP interface associated with a queue group is unbound from a port:

- The system decrements the association counter for the queue group on the unbound port

Egress Network IP Interface Statistics

The statistics for network interfaces work differently than statistics on SAPs. Counter sets are created for each egress IP interface and not per egress queue. When a forwarding class for an egress IP interface is redirected from the default egress port queue to a queue group queue, the system continues to use the same counter set.

Separate Ingress IPv4 and IPv6 Statistics

This feature adds support for separate ingress IPv4 and IPv6 statistics on IP interfaces. IES and VPRN interfaces, and subscriber group interfaces on IES and VPRN,as well as for uRPF. In previous release, the ingress statistics for IPv4 and IPv6 traffic was combined into a single set of packet and bytes counters. The existing counters will now only count IPv4 traffic, while new separate counters are available to IPv6 traffic.

The feature introduces a new CLI command to explicitly enable ingress statistics on IP interfaces, changing the default to disabled.

Ingress PW Shaping Using Spoke-SDP Forwarding Class-Based Redirection

Feature Configuration

The user applies a network QoS policy to the ingress context of a spoke-SDP[1] to redirect the mapping of a Forwarding Class (FC) to a policer defined in a queue-group template which is instantiated on the ingress Forwarding Plane (FP) where the PW packets are received.

config>service>vprn>interface>spoke-sdp>ingress>qos *network-policy-id* **fp-redirect-group** *queue-group-name* **instance** *instance-id*

Let us refer to a queue-group containing policers as a *policer queue-group*. The user must instantiate this queue-group by applying the following command:

config>card>fp>ingress>network>queue-group *queue-group-name* **instance** *instance-id*

The policers are instantiated at ingress FP, one instance per destination tap, and are used to service packets of this spoke-SDP which are received on any port on the FP to support a network IP interface on LAG and on any network IP interface to support ECMP on the network IP interface and LSP reroutes to a different network IP interface on the same FP.

In the ingress context of the network QoS policy, the user defines the mapping of a FC to a policer-id and instructs the code to redirect the mapping to the policer of the same ID in some queue-group:

config>qos>network>ingress>fc>fp-redirect-group policer *policer-id*
config>qos>network>ingress>fc>fp-redirect-group multicast-policer *policer-id*

The user can redirect the Unicast and multicast packets of a FC to two different policers to allow for different policing rates for these packet types. However, the queue-group is explicitly named only at the time the network QoS policy is applied to the spoke-SDP as shown above with the example of the VPRN service.

When the FC of a PW is redirected to use a policer in the named queue-group, the policer feeds the existing per-FP ingress shared queues referred to as *policer-output-queues*. These queues are shared by both access and network policers configured on the same ingress FP. The shared queue parameters are configurable using the following command:

configure>qos>shared-queue policer-output-queues

[1] This feature applies to both spoke-SDP and mesh-SDP. Spoke-SDP is used throughout for ease of reading.

The CLI configuration in this section uses a spoke-SPD defined in the context of a VPRN interface. However the PW shaping feature is supported with all PW based services including the PW template.

Provisioning Model

Operationally, the provisioning model in the case of the ingress PW shaping feature consists of the following steps:

1. Create an ingress queue-group template and configure policers for each FC which needs to be redirected and optionally for each traffic type (Unicast or multicast).
2. Apply the queue-group template to the network ingress context of all IOM3/IMM FPs where there exists a network IP interface which the PW packets can be received on. This creates one instance of the template on the ingress of the FP. One or more instances of the same template can be created.
3. Configure FC-to-policer mappings together with the policer redirect to a queue-group in the ingress context of a network QoS policy. No queue-group name is specified in this step which means the same network QoS policy can redirect different PWs to different queue-group templates.
    a. Apply this network QoS policy to the ingress context of a spoke-SDP inside a service or to the ingress context of a PW template and specify the redirect queue-group name.
    b. One or more spoke-SDPs can have their FCs redirected to use policers in the same policer queue-group instance.

The following are the constraints and rules of this provisioning model when used in the ingress PW shaping feature:

1. Only a queue-group containing policers, can be instantiated in the network ingress context of an IOM3/IMM FP. If the queue-group template contains policers and queues, the queues are not instantiated.
2. If the queue-group contains queues only, the instantiation in the data path is failed.
3. One or more instances of the same policer queue-group name and/or a different policer queue-group name can be created on network ingress context of an IOM3/IMM FP.
4. The queue-group-name must be unique within all network ingress and access ingress queue groups in the system.
5. The instantiated FP policer queue-group can be used by PW packets received on a network IP interface configured on both Ethernet ports and POS ports of that IOM3/IMM.

6. When a PW FC is redirected to use a policer in a named policer queue-group and the queue-group name does not exist, the association is failed at the time the user associates the ingress context of a spoke-SDP to the named queue-group. In such a case, the PW packet feeds directly the ingress network shared queue for that FC defined in the network-queue policy applied to the ingress of the MDA/FP.

7. When a PW FC is redirected to use a policer in a named policer queue-group and the queue-group name exists but the policer-id is not defined in the queue-group template, the association is failed at the time the user associates the ingress context of a spoke-SDP to the named queue-group. In such a case, the PW packet feeds directly the ingress network shared queue for that FC defined in the network-queue policy applied to the ingress of the MDA/FP.

8. When a PW FC is redirected to use a policer in a named policer queue-group and the queue-group name exists and the policer-id is defined in the queue-group template, it is not required to check that an instance of that queue-group exists in all ingress FPs which have network IP interfaces. The handling of this is dealt with in the data path as follows:
   a. When a PW packet for that FC is received and an instance of the referenced queue-group name exists on that FP, the packet is processed by the policer and is then feed the per-FP ingress shared queues referred to as *policer-output-queues*.
   b. When a PW packet for that FC is received and an instance of the referenced queue-group name does not exist on that FP, the PW packets are fed directly into the corresponding ingress network shared queue for that FC defined in the network-queue policy applied to the ingress of the MDA/FP.

9. If a network QoS policy is applied to the ingress context of a PW, any PW FC, which is not explicitly redirected in the network QoS policy, has the corresponding packets feed directly the ingress network shared queue for that FC defined in the network-queue policy applied to the ingress of the MDA/FP.
   a. This behavior is the same regardless if the ingress network IP interface from which the PW packet is received is redirected or not to a policer queue-group.

10. If no network QoS policy is applied to the ingress context of the PW, then all packets of the PW feed:
    a. the ingress network shared queue for the packet FC defined in the network-queue policy applied to the ingress of the MDA/FP. This is the default behavior.
    b. a queue-group policer followed by the per-FP ingress shared queues referred to as *policer-output-queues* if the ingress context of the network IP interface from which the packet is received is redirected to a queue-group. The only exceptions to this behavior are for packets received from a IES/VPRN spoke interface and from a R-VPLS spoke-SDP, which is forwarded to the R-VPLS IP interface. In these two cases, the ingress network shared queue for the packet FC defined in the network-queue policy applied to the ingress of the MDA/FP is used.

Ingress Packet Classification

When a PW is redirected to use a policer queue-group, the classification of the packet for the purpose of FC and profile determination is performed according to default classification rule or the QoS filters defined in the ingress context of the network QoS policy applied to the PW. This is true regardless if an instance of the named policer queue-group exists on the ingress FP the PW packet is received on. The user can apply a QoS filter matching the dot1.p in the VLAN tag corresponding to the Ethernet port encapsulation, the EXP in the outer label when the tunnel is an LSP, the DSCP in the IP header if the tunnel encapsulation is GRE, and the DSCP in the payload's IP header if the user enabled the **ler-use-dscp** option and the PW terminates in IES or VPRN service (spoke-interface).

When the policer queue-group name the PW is redirected does not exist, the redirection command is failed. In this case, the packet classification is performed according to default classification rule or the QoS filters defined in the ingress context of the network QoS policy applied to the network IP interface the PW packet is received on.

Egress PW Shaping using Spoke-SDP Forwarding Class-Based Redirection

Feature Configuration

The user applies a network QoS policy to the egress context of a spoke-sdp to redirect the mapping of a Forwarding Class (FC) to a policer and/or a queue part of a queue-group instance created in the egress of a network port.

config>service>vprn>interface>spoke-sdp>egress>qos *network-policy-id* **port-redirect-group** *queue-group-name* **instance** *instance-id*

The queue-group queues or policers are instantiated at egress port, one instance per network port and per link of LAG network port and are used to service packets of this spoke-SDP, which are forwarded over any network IP interface on this port.

config>port>ethernet>network>egress>queue-group *queue-group-name* **instance** *instance-id*

In the egress context of the network QoS policy, the user defines the mapping of a FC to a policer-id or a queue-id and instructs the code to redirect the mapping to the queue or policer of the same ID in some queue-group. However, the queue-group is explicitly named only at the time the network QoS policy is applied to the spoke-SDP as shown above with the example of the VPRN service. The command is as follows:

config>qos>network>egress>fc>port-redirect-group {**queue** *queue-id* | **policer** *policer-id* [**queue** *queue-id]*}

There are three possible outcomes when executing this command.

- The user can redirect a FC to use a queue in a queue-group and in which case there are no policers used.
  config>qos>network>egress>fc>port-redirect-group queue *queue-id*
- The user can redirect a FC to use a policer-id in a queue-group without specifying a queue-id and in which case the policer is feeding the egress shared queue for that FC defined in the network-queue policy applied to the egress of this port.
  config>qos>network>egress>fc>port-redirect-group policer *policer-id*
- The user can redirect a FC to use a policer feeding a queue both of which are defined in the named queue-group.
  config>qos>network>egress>fc>port-redirect-group policer *policer-id* **queue** *queue-id*

The CLI configuration in this section uses a spoke-sdp defined in the context of a VPRN interface. However the PW shaping feature is supported with all PW based services and PW template.

Provisioning Model

This provisioning model allows the mapping of one ore more PWs to the same instance of queues, or policers and queue, which are defined in the queue-group template.

Operationally, the provisioning model consists of the following steps:

1. Create an egress queue-group template and configure queues only or policers and queues for each FC which needs to be redirected.
2. Apply the queue-group template to the network egress context of all IOM3/IMM ports where there exists a network IP interface which the PW packets can be forwarded on. This creates one instance of the template on the egress of the port. One or more instances of the same template can be created.
3. Configure FC-to-policer or FC-to-queue mappings together with the redirect to a queue-group in the egress context of a network QoS policy. No queue-group name is specified in this step which means the same network QoS policy can redirect different PWs to different queue-group templates.
    a. Apply this network QoS policy to the egress context of a spoke-sdp inside a service or to the egress context of a PW template and specify the redirect queue-group name.
    b. One or more spoke-sdp's can have their FCs redirected to use queues only or queues and policers in the same queue-group instance.

The following are the constraints and rules of this provisioning model:

1. Queue-groups containing queues only or policers and queues can be instantiated in the network egress context of an Ethernet port on IOM3/IMM.
2. When a port is a LAG, one instance of the queue-group is instantiated on each member link.
3. One or more instances of the same queue-group name and/or a different queue-group name can be created in the network egress context of an Ethernet port.
4. The queue-group-name must be unique within all network egress and access egress queue groups in the system.
5. A user attempt to instantiate the queue-group on the network egress context of a POS port or a TDM port will fail.
6. When a PW FC is redirected to use a queue or a policer and a queue in a queue-group and the queue-group name does not exist, the association is failed at the time the user associates the egress context of a spoke-SDP to the named queue-group. In such a case, the PW packet is fed directly to the corresponding egress queue for that FC used by the IP network interface the PW packet is forwarded on. This queue can be a queue-group

queue or the egress shared queue for that FC defined in the network-queue policy applied to the egress of this port. This is the existing implementation and default behavior for a PW packet.

7. When a PW FC is redirected to use a queue or a policer and a queue in a queue-group and the queue-group name exists but the policer-id and/or the queue-id is not defined in the queue-group template, the association is failed at the time the user associates the egress context of a spoke-SDP to the named queue-group. In such a case, the PW packet is fed directly to the corresponding egress queue for that FC used by the IP network interface the PW packet is forwarded on.

8. When a PW FC is redirected to use a queue or a policer and a queue in a queue-group and the queue-group name exists and the policer-id or policer-id plus queue-id exist, it is not required to check that an instance of that queue-group exists in all egress network ports which have network IP interfaces. The handling of this is dealt with in the data path as follows:

    a. When a PW packet for that FC is forwarded and an instance of the referenced queue-group name exists on that egress port, the packet is processed by the queue-group policer and is fed to the queue-group queue. If only a policer is specified in the redirection command, then the packet is processed by the queue-group policer and is then fed into the corresponding egress shared queue for that FC defined in the network-queue policy applied to the egress of this port. If only a queue is specified in the redirection command, the packet is fed to the queue-group queue.

    b. When a PW packet for that FC is forwarded and an instance of the referenced queue-group name does not exist on that egress port, the PW packet is fed directly to the corresponding egress shared queue for that FC defined in the network-queue policy applied to the egress of this port.

    c. If a network QoS policy is applied to the egress context of a PW, any PW FC, which is not explicitly redirected in the network, QoS policy has the corresponding packets feed directly the corresponding the egress shared queue for that FC defined in the network-queue policy applied to the egress of this port.

Egress Marking of PW Packet Header

When the queue-group name the PW is redirected to exists and the redirection succeeds, the marking of the packet's DEI/dot1.p/DSCP and the tunnel's DEI/dot1.p/DSCP/EXP is performed according to the relevant mappings of the {FC, profile} in the egress context of the network QoS policy applied to the PW. This is true if an instance of the queue-group exists on the egress port the PW packet is forwarded to. If the packet's profile value changed due to egress child policer CIR profiling, the new profile value is used to mark the packet's DEI/dot1.p and the tunnel's DEI/dot1.p/EXP but the DSCP is not modified by the policer's operation.

When the redirection command succeeds but there is no instance of the queue-group on the egress port, or when the redirection command fails due to an inexistent queue-group name, the marking of the packet's DEI/dot1.p/DSCP and the tunnel's DEI/dot1.p/DSCP/EXP fields is performed according to the relevant commands in the egress context of the network QoS policy applied to the network IP interface the PW packet is forwarded to.

Egress Packet Re-Classification Based on IPv4/IPv6 Criteria

The user enables IP precedence or DSCP based egress re-classification by applying the following command in the context of the network QoS policy applied to the egress context of a spoke-SDP.

config>qos>network>egress>prec *ip-prec-value* [**fc** *fc-name*] [**profile** {**in** | **out**}]
config>qos>network>egress>dscp *dscp-name* [**fc** *fc-name*] [**profile** {**in** | **out**}]

The IP precedence bits used to match against DSCP reclassification rules come from the Type of Service (ToS) field within the IPv4 header or the Traffic Class field from the IPv6 header.

The IP DSCP bits used to match against DSCP reclassification rules come from the Type of Service (ToS) field within the IPv4 header or the Traffic Class field from the IPv6 header.

If the packet does not have an IP header, DSCP or IP-precedence based matching is not performed.

Note that the IP precedence and DSCP based re-classification are only supported on a PW used in an IES or VPRN spoke-interface. The CLI blocks the application of a network QoS policy with the egress re-classification commands to a network IP interface or to a spoke-SDP part of L2 service. Conversely, the CLI does not allow the user to add the egress re-classification commands to a network QoS policy if it is being used by a network IP interface or a L2 spoke-SDP.

In addition, the egress re-classification commands only take effect if the redirection of the spoke-SDP to use an egress port queue-group succeeds; for example, the following CLI commands succeed:

config>service>vprn>interface>spoke-sdp>egress>qos *network-policy-id* **port-redirect-group** *queue-group-name* **instance** *instance-id*

config>service>ies>interface>spoke-sdp>egress>qos *network-policy-id* **port-redirect-group** *queue-group-name* **instance** *instance-id*

Reclassification will however occur regardless of whether the queue group instance exists or not on a given egress network port. When the redirection command fails in CLI, the PW uses the network QoS policy assigned to the network IP interface. Since the network QoS policy applied to a network IP interface does not support re-classification, the PW packets do not undergo re-classification.

Ingress and Egress PW Statistics

The PW forwarded packet and octet statistics (SDP binding statistics) are currently supported for both ingress and egress and are available via show command, monitor command, and accounting file. These statistics consist of the ingress-forwarded and ingress-dropped packet and octet counters, as well as the egress-forwarded packet and octet counters. However, they do not include discards in the ingress network queues. The latter are counted in the stats of the queues defined in the network-queue policy applied to the ingress of the MDA/FP.

Note the ingress and egress SDP binding stats do not count the label stack of the PW packet but count the PW Control Word (CW) if included in the packet.

With the introduction of the PW shaping feature—the ingress or egress queue-group policer—a PW FC is redirected to also provide packet and octet forwarded and dropped-statistics by means of the show command, monitor command, and accounting file of the ingress or egress queue-group instance.

Similar to the SDP binding stats, the ingress policer stats for a spoke-SDP does not count the label stack. When the spoke-SDP is part of a L2-service, they will count the L2-encapsulation, minus CRC and VLAN tag if popped out, and they also count the PW CW, if included in the packet. When the spoke-SDP is part of a L3-service, the policer stats only count the IP payload and do not count the PW CW. Unlike the ingress SDP binding stats, if the user enables the **packet-byte-offset** {**add** *bytes* | **subtract** *bytes*} option under the queue-group policer, then the policer stats reflect the adjusted packet size in both L2 and L3-spoke-SDPs.

The egress queue-group policer and/or queue counts the full label stack of the PW packet including the CW. If the user enables the **packet-byte-offset** {**add** *bytes* | **subtract** *bytes*} option under the queue-group policer and queue-group queue, then the policer and queue stats reflect the adjusted packet size.

The SDP binding and queue-group statistics does however remain separate as one or more PWs can have FCs redirected to the same policer ID in the queue-group instance.

Queue Group Behavior on LAG

Queue Group Queue Instantiation Per Link

When a port queue group is created on a Link Aggregation Group (LAG) context, it is individually instantiated on each link in the LAG.

Per Link Queue Group Queue Parameters

The queue parameters for a queue within the queue group are used for each port queue and are not divided or split between the port queues representing the queue group queue. For instance, when a queue rate of 100Mbps is defined on a queue group queue, each instance of the queue group (on each LAG port) will have a rate of 100Mbps.

Adding a Queue Group to an Existing LAG

A queue group must be created on the primary (lowest port ID) port of the LAG. If an attempt is made to create a queue group on a port other than the primary, the attempt will fail. When the group is define on the primary port, the system will attempt to create the queue group on each port of the LAG. If sufficient resources are not available on each port, the attempt to create the queue group will fail.

Any queue group queue overrides defined on the primary port will be automatically replicated on all other ports within the LAG.

Removing a Queue Group from a LAG

A queue group must be removed from the primary port of the LAG. The queue group will be deleted by the system from each of the port members of the LAG.

Adding a Port to a LAG

When adding a port to a LAG group, the port must have the same queue groups defined as the existing ports on the LAG before it will be allowed as a member. This includes all queue group override parameters.

Basic Configurations

Configuring an Ingress Queue Group Template

The following displays an ingress queue group template configuration example:

```
*A:Dut-T>cfg>qos>qgrps# info
----------------------------------------------
            ingress
                queue-group "QG_ingress_1" create
                    queue 1 best-effort create
                        mbs 100
                    exit
                    queue 2 best-effort create
                        mbs 100
                    exit
                    queue 3 best-effort create
                        mbs 100
                    exit
                    queue 4 best-effort create
                        mbs 100
                    exit
                exit
            exit
----------------------------------------------
*A:Dut-T>cfg>qos>qgrps#
```

NOTE: To fully use the queue group feature to save queues, you must explicitly map all forwarding classes to queue group queues. This rule is applicable to SAP ingress, SAP egress and network QoS policies.

Configuring Egress Queue Group Template

The following displays an egress queue group template configuration example:

```
*A:Dut-T>cfg>qos>qgrps# info
----------------------------------------------
...
            egress
                queue-group "QG_egress_1" create
                    description "Egress queue group"
                    queue 1 best-effort create
                        mbs 100
                    exit
                    queue 2 best-effort create
                        mbs 100
                    exit
                    queue 3 best-effort create
                        mbs 100
                    exit
                    queue 4 best-effort create
                        mbs 100
                    exit
                exit
            exit
----------------------------------------------
*A:Dut-T>cfg>qos>qgrps#
```

Applying Ingress Queue Group to SAP Ingress Policy

The following display a SAP ingress policy configuration with **group** *queue-group-name* specified:

```
*A:Dut-T>config>qos>sap-ingress# info
----------------------------------------------
            queue 1 create
            exit
            queue 11 multipoint create
            exit
            fc "af" create
                queue 2 group "QG_ingress_1"
            exit
            fc "be" create
                queue 1 group "QG_ingress_1"
            exit
            fc "ef" create
                queue 3 group "QG_ingress_1"
            exit
            fc "nc" create
                queue 4 group "QG_ingress_1"
            exit
            dot1p 0 fc "be"
            dot1p 2 fc "af"
            dot1p 4 fc "ef"
            dot1p 6 fc "nc"
----------------------------------------------
*A:Dut-T>config>qos>sap-ingress#
```

Applying Egress Queue Group to SAP Egress Policy

The following display a SAP egress policy configuration with **group** *queue-group-name* specified:

```
A:Dut-T>config>qos>sap-egress# info
----------------------------------------------
            queue 1 create
            exit
            fc af create
                queue 2 group "QG_egress_1"
            exit
            fc be create
                queue 1 group "QG_egress_1"
            exit
            fc ef create
                queue 3 group "QG_egress_1"
            exit
            fc nc create
                queue 4 group "QG_egress_1"
            exit
----------------------------------------------
A:Dut-T>config>qos>sap-egress#
```

SAP-based Egress Queue Re-direction

The following displays a SAP egress policy configuration with port-redirect-group-queue construct (shown for both regular and HS-MDA egress queues) and the actual queue-group-name is determined by the SAP egress QoS configuration:

```
*A:Dut-A# configure qos sap-egress 3
*A:Dut-A>config>qos>sap-egress# info
----------------------------------------------
            queue 1 create
            exit
            queue 2 create
            exit
            policer 8 create
                rate 50000
            exit
            fc af create
                queue 3 port-redirect-group-queue
                hsmda
                    queue 3 port-redirect-group-queue
                exit
            exit
            fc be create
                queue 3 port-redirect-group-queue
                hsmda
                    queue 3 port-redirect-group-queue
                exit
            exit
            fc ef create
                policer 8 port-redirect-group-queue
                hsmda
                    queue 3 port-redirect-group-queue
                exit
            exit
            fc h1 create
                queue 3 port-redirect-group-queue
                hsmda
                    queue 3 port-redirect-group-queue
                exit
            exit
            fc h2 create
                queue 3 port-redirect-group-queue
                hsmda
                    queue 3 port-redirect-group-queue
                exit
            exit
            fc l1 create
                queue 3 port-redirect-group-queue
                hsmda
                    queue 3 port-redirect-group-queue
                exit
            exit
            fc l2 create
                queue 3 port-redirect-group-queue
                hsmda
```

```
                    queue 3 port-redirect-group-queue
                exit
            exit
            fc nc create
                queue 3 port-redirect-group-queue
                hsmda
                    queue 3 port-redirect-group-queue
                exit
            exit
----------------------------------------------
```

This is to be in-conjunction with:

```
*A:Dut-A# configure service vpls 1
*A:Dut-A>config>service>vpls# info
----------------------------------------------
            stp
                shutdown
            exit
            sap 9/1/2:1 create
                egress
                    qos 3 port-redirect-group qg1 instance 101
                exit
            exit
```

Configuring Queue Group on Ethernet Access Ingress Port

The provisioning steps involved in using a queue-group queue on an ingress port are:

- Queue Group Template Creation
  - → Create the queue group template in the ingress context
  - → Create the queue within the queue group template
- Queue Group Creation
  - → Identify the ingress port (or ports) for which the queue group will be needed (for LAG use the primary port member)
  - → Create a queue group with the same name as the template on the port or ports
- Map a Forwarding Class to the queue-id within the queue group
  - → Map forwarding classes to queue-group queues.
  - → Identify or create the SAP ingress QoS policy that will be used on the ingress SAP where queue redirection is desired
  - → Map the desired forwarding classes to the queue group name and the specific queue ID within the group
- Apply the SAP ingress QoS policy
  - → Identify or create the ingress SAP requiring forwarding class redirection to the queue group
  - → Assign the QoS policy to the SAP

The following displays an Ethernet access ingress port queue-group configuration example :

```
*A:Dut-T>config>port# /configure port 9/2/1
*A:Dut-T>config>port# info
----------------------------------------------
        ethernet
            mode access
            access
                ingress
                    queue-group "QG_ingress_1" create
                    exit
                exit
                egress
                    queue-group "QG_egress_1" create
                    exit
                exit
            exit
        exit
        no shutdown
----------------------------------------------
*A:Dut-T>config>port#
```

```
*A:Dut-T>config>port# /configure port 9/2/2
*A:Dut-T>config>port# info
----------------------------------------------
        ethernet
            mode access
            access
                ingress
                    queue-group "QG_ingress_1" create
                    exit
                exit
                egress
                    queue-group "QG_egress_1" create
                    exit
                exit
            exit
        exit
        no shutdown
----------------------------------------------
*A:Dut-T>config>port#
```

Configuring Overrides

The following output display a port queue group queue override example.

```
*A:Dut-T>config>port>ethernet>access# /configure port 9/2/1
*A:Dut-T>config>port# info
----------------------------------------------
        ethernet
            mode access
            access
                ingress
                    queue-group "QG_ingress_1" create
                        queue-overrides
                            queue 2 create
                                rate 800000 cir 20000
                            exit
                        exit
                    exit
                exit
                egress
                    queue-group "QG_egress_1" create
                    exit
                exit
            exit
        exit
        no shutdown
----------------------------------------------
*A:Dut-T>config>port# /configure port 9/2/2
*A:Dut-T>config>port# info
----------------------------------------------
        ethernet
            mode access
            access
                ingress
                    queue-group "QG_ingress_1" create
                    exit
                exit
                egress
                    queue-group "QG_egress_1" create
                        queue-overrides
                            queue 3 create
                                rate 1500000 cir 2000
                            exit
                        exit
                    exit
                exit
            exit
        exit
        no shutdown
----------------------------------------------
*A:Dut-T>config>port#
```

Configuring Queue Group on Ethernet Access Egress Port

The provisioning steps involved in using a queue-group queue on an egress access port are:

- Queue Group Template Creation
  - → Create the queue group template in the egress context
  - → Create the queue within the queue group template
- Queue Group Creation
  - → Identify which egress port (or ports) on which the queue group will be needed (for LAG use the primary port member)
  - → Create a queue group instance with the same name as the template on the port or ports
- From this point, there are two methods for regular ethernet based SAPs to have port access egress re-direction. a). Policy based re-direction and, b). SAP based re-direction. For Policy based redirection:
- Map a Forwarding Class to the queue-id within the queue group
  - → Identify or create the SAP egress QoS policy that will be used on the egress SAP where policy-based queue re-direction is desired
  - → Map the desired forwarding classes to the queue group name and the specific queue ID within the group with the “group” keyword
- Apply the SAP egress QoS policy
  - → Identify or create the egress SAP requiring forwarding class redirection to the queue group
  - → Assign the QoS policy to the SAP
- For SAP based redirection:
- Map a Forwarding Class to the queue-id within the queue group
  - → Identify or create the SAP egress QoS policy that will be used on the egress SAP where SAP-based queue re-direction redirection is desired
  - → Map the desired forwarding classes to the queue group specific queue-id, and the keyword "port-redirect-group-queue". The actual queue-group template name is determined by the sap instance's configuration which associated the sap-egress qos policy in conjunction with the port-redirect-group's instance.
- Apply the SAP egress QoS policy and the queue-group template's instance under the SAP.
  - → Identify or create the egress SAP requiring forwarding class redirection to the queue group
  - → Assign the QoS policy and the egress queue-group template's instance to the SAP.

Configuring Queue Group for Network Egress Traffic on Port

The provisioning steps involved in using a queue-group queue on an egress network port are:

- Queue Group Template Creation:
  - → Create the egress queue group template.
  - → Create the queues and/or policers within the queue group template.
- Queue Group Creation:
  - → Identify the egress port (or ports) on which the queue group will be needed (for LAG use the primary port member).
  - → Create a queue group with the same name as the template on the port or ports. The instance ID is optional.
- Map a Forwarding Class to the queue-id within the queue group:
  - → Identify or create the network QoS policy that will be used on the egress IP interface where queue redirection is desired.
  - → Map the desired egress forwarding classes within the network QoS policy to the specific queue IDs and/or policer IDs within the group (the group name will be supplied when the QoS policy is applied to the IP interface).
- Apply the network QoS policy:
  - → Identify or create the IP interface requiring forwarding class redirection to the queue group.
  - → Assign the QoS policy to the IP interface and specify the queue group name (and optionally instance ID) for redirection of egress traffic.

Once a queue within a template is mapped by a forwarding class on any object, the queue may be edited, but not deleted.

Configuring Queue Group for Network Ingress Traffic on Forwarding Plane

The provisioning steps involved in using a queue-group for ingress traffic on a network interface are:

- Queue Group Template Creation:
  - → Create the ingress queue group template.
  - → Create the policers within the queue group template.
- Queue Group Creation:
  - → Identify the ingress forwarding plane on which the queue group will be needed.
  - → Create a queue group with the same name as the template in the FP ingress network configuration context. An instance ID is mandatory.
- Map a Forwarding Class to the policer-id within the queue group:
  - → Identify or create the network QoS policy that will be used on the ingress IP interface where queue redirection is desired.
  - → Map the desired ingress forwarding classes within the network QoS policy to the specific policer IDs within the group (the group name will be supplied when the QoS policy is applied to the IP interface).
- Apply the network QoS policy:
  - → Identify or create the IP interface requiring forwarding class redirection to the queue group.
  - → Assign the QoS policy to the IP interface and specify the queue group name and instance ID for redirection of ingress traffic.

Using Queue Groups to Police Ingress/Egress Traffic on Network Interface

```
config
     qos
          queue-group-templates
               ingress
                    queue-group "Ingress_QG_1" create
                         policer 2 create
                              rate 9000
                         exit
                    exit
               exit
               egress
                    queue-group "Egress_QG_1" create
                         queue 1 best-effort create
                         exit
                         policer 2 create
                              rate 9000
                         exit
                    exit
               exit
          exit

          network 2 create
               ingress
                    fc be
                         fp-redirect-group policer 2
                    exit
               exit
               egress
                    fc be
                         port-redirect-group policer 2
                    exit
               exit
          exit


     card 1
          card-type xcm-x20
               mda 1             mda-type cx20-10g-sfp no shutdown
               exit
          fp 1
               ingress
                    network
                         queue-group "Ingress_QG_1" instance 550 create
                         exit
                    exit
               exit
          exit
          no shutdown

     port 1/1/3
          ethernet
                    mtu 1514
                    network
                         egress
                              queue-group "Egress_QG_1" instance 550 create
                              exit
                         exit
                    exit
               exit
          no shutdown
     exit

     router
          interface “to-D”
          address 10.10.11.3/24
          port 1/1/3
          qos 2 egress-port-redirect-group "Egress_QG_1" egress-instance
          550 ingress-fp-redirect-group "Ingress_QG_1" ingress-instance
          550
          no shutdown
```

Configuring Ingress/Egress PW Shaping Using Spoke-SDP Forwarding Class-Based Redirection

```
configure
#--------------------------------------------------
echo "QoS Policy Configuration"
#--------------------------------------------------
    qos
        queue-group-templates
            ingress
                queue-group "QGIng1" create
                    policer 1 create
                    exit
                    policer 2 create
                    exit
                    policer 3 create
                    exit
                    policer 4 create
                    exit
                exit
            exit
            egress
                queue-group "QGEgr1" create
                    queue 1 best-effort create
                    exit
                    policer 1 create
                    exit
                    policer 2 create
                    exit
                    policer 3 create
                    exit
                    policer 4 create
                    exit
                exit
            exit
        exit
    exit
        network 10 create
            ingress
                lsp-exp 0 fc be profile out
                lsp-exp 1 fc be profile out
                lsp-exp 2 fc be profile out
                lsp-exp 3 fc be profile out
                lsp-exp 4 fc be profile out
                lsp-exp 5 fc be profile out
                lsp-exp 6 fc be profile out
                lsp-exp 7 fc be profile out
                fc af
                    fp-redirect-group policer 4
                exit
                fc be
                    fp-redirect-group policer 1
                exit
                fc l1
                    fp-redirect-group policer 2
                exit
                fc l2
```

```
                    fp-redirect-group policer 3
                exit
            exit
            egress
                fc af
                    port-redirect-group policer 4
                exit
                fc be
                    port-redirect-group policer 1
                exit
                fc l1
                    port-redirect-group policer 2
                exit
                fc l2
                    port-redirect-group policer 3
                exit
            exit
        exit
    exit
#--------------------------------------------------
echo "Card Configuration"
#--------------------------------------------------
    card 3
        fp 1
            ingress
                network
                    queue-group "QGIng1" instance 1 create
                    exit
                    queue-group "QGIng1" instance 2 create
                    exit
                exit
            exit
        exit
    exit
#--------------------------------------------------
echo "Port Configuration"
#--------------------------------------------------
    port 3/2/1
        ethernet
            encap-type dot1q
            network
                egress
                    queue-group "QGEgr1" instance 1 create
                    exit
                    queue-group "QGEgr1" instance 2 create
                    exit
                exit
            exit
        exit
        no shutdown


*A:Dut-T>config>service#
        customer 1 create
            description "Default customer"
        exit
        sdp 1 mpls create
            description "Default sdp description"
            far-end 2.2.2.2
            ldp
            path-mtu 9000
            keep-alive
                shutdown
            exit
            no shutdown
        exit
        vpls 1 customer 1 vpn 1 create
            description "Default tls description for service id 1"
            service-mtu 9000
            stp
                shutdown
            exit
            service-name "XYZ Vpls 1"
            sap 9/2/1:1.* create
                description "Default sap description for service id 1"
                static-mac 00:00:1e:00:01:02 create
                ingress
                    qos 10
                exit
            exit
            spoke-sdp 1:101 vc-type vlan create
                description "Description for Sdp Bind 1 for Svc ID 1"
                ingress
                    qos 10 fp-redirect-group "QGIng1" instance 1
                exit
                egress
                    qos 10 port-redirect-group "QGEgr1" instance 1
                exit
                static-mac 00:00:28:00:01:02 create
                no shutdown
            exit
            no shutdown
        exit


    router
        interface "ip-12.1.1.1"
            address 12.1.1.1/24
            port 3/2/1:1
        exit
        interface "system"
            address 1.1.1.1/32
        exit
#---------------------------------------------
```

Specifying QoS Policies on Service SAPs

The following output displays a VPLS service configuration example.

```
*A:Dut-T>config>service>vpls# info
----------------------------------------------
            stp
                shutdown
            exit
            sap 9/2/1 create
                ingress
                    qos 10
                exit
                egress
                    qos 10
                exit
            exit
            sap 9/2/2 create
                ingress
                    qos 10
                exit
                egress
                    qos 10
                exit
            exit
            no shutdown
----------------------------------------------
*A:Dut-T>config>service>vpls#
```