QoS Management

This segment describes the Quality of Service (QoS) management on Cisco® ASR 5500 chassis and explains how it is configured.

The product Administration Guides provide examples and procedures for configuration of basic services on the system. You should select the configuration example that best meets your service model and configure the required elements for that model as described in the respective product Administration Guide, before using the procedures described below.

- Introduction, on page 1
- Dynamic QoS Renegotiation, on page 1
- Network Controlled QoS (NCQoS), on page 4
- Configuring Dynamic QoS Renegotiation, on page 5
- Configuring Network Controlled QoS (NCQoS), on page 7
- Monitoring Dynamic QoS Renegotiation Operation, on page 9

Introduction

The QoS Traffic Policing functionality supported by the GGSN implements QoS for subscribers based on the configuration of the APN template. As a result, all subscriber PDP contexts using the APN receive the same QoS level. This could lead to unused or under-utilized bandwidth by some subscribers thus reducing the amount of resources available to others.

Dynamic QoS Renegotiation

Dynamic QoS Renegotiation minimizes the risk of bandwidth mis-appropriation. This feature allows the GGSN to analyze application traffic, and trigger QoS renegotiation with the SGSN to optimize service performance.

In Dynamic QoS Renegotiation, the GGSN performs packet inspection of application traffic to detect the type of service being utilized and automatically renegotiates the QoS to the appropriate level with a maximum QoS level corresponding to the level granted by the HLR.

QoS renegotiation is performed by sending an Update PDP Context Request to the SGSN. This solution is optimal since the appropriate QoS level is always granted to the subscriber without any requirement on the handset or on the core network. The only prerequisite is QoS renegotiation support on the SGSN. In this

model, over reservation of radio resources is avoided, while maintaining the appropriate bandwidth for subscribers with real requirements.

The ASR 5500 supports L7 stateful analysis and QoS Renegotiation. These functions combine to become Dynamic QoS Renegotiation. The system also generates CDRs (or real time charging information) that includes the current QoS information and the service accessed. This enables intelligent application-based charging of services, taking into account the granted QoS. It also enables rebates when it was not possible to provide the QoS level required by an application.

Important For L7 traffic analysis an ECSv2 license is required.

How Dynamic QoS Renegotiation Works

Implementation of Dynamic QoS Renegotiation involves the following:

- Initial QoS
- Service Detection
- Classification of Application Traffic
- Quality of Service Renegotiation

Initial QoS

When the session is established, an initial level of QoS must be assigned to the subscriber. The GGSN may either grant the requested QoS, or grant a lower QoS level (minimum or intermediate level). The initial QoS remains in effect until the SGSN or GGSN requests a change. When Dynamic QoS Renegotiation is enabled, there are several conditions when the system would request a QoS change.

- Services detected that do not need high QoS: After a configurable time period of a subscriber having terminated services that require high QoS, the system could lower the QoS to a value more appropriate to the services actually being used.
- Services detected that require higher QoS: As soon as a subscriber begins using a service that needs a high QoS, the system immediately attempts to raise the QoS through its service detection capability.

Service Detection

The Application analysis approach to service detection uses application level (L7) information. In the ASR 5500 chassis, application analysis is stateful—keeping track of the application state.

Important For L7 traffic analysis ECSv2 license is required.

Classification of Application Traffic

Application traffic can be classified into the following: Conversational, Streaming, Interactive 1, Interactive 2, Interactive 3, or Background. Traffic class can be configured in the charging-action, but it does not take

direction as a parameter. However, you can configure a rule matching uplink-only or downlink-only packets and associate it with the charging-action.

QoS renegotiation requires knowing what kind of data packets are flowing through for a particular user to associate a given traffic class with the user's current usage pattern. This is done through packet inspection for a subscriber profile via an Access Control List (ACL). Limits for each traffic class can be configured in the APN. The same infrastructure is reused to perform Dynamic QoS Renegotiation.

After classification of traffic and if required by subscriber profile, Dynamic QoS Renegotiation takes place.

L4 Packet Inspection

L4 packet analysis has no or low impact on the system performance with very limited impact on system capacity. L4 packet inspection is fully supported by the system.

L7 Packet Inspection

L7 packet analysis has a greater impact on system performance with very limited impact on the system capacity. L7 packet inspection involves complete application layer analysis and copes with customized applications.

QoS Renegotiation for a Subscriber QoS Profile

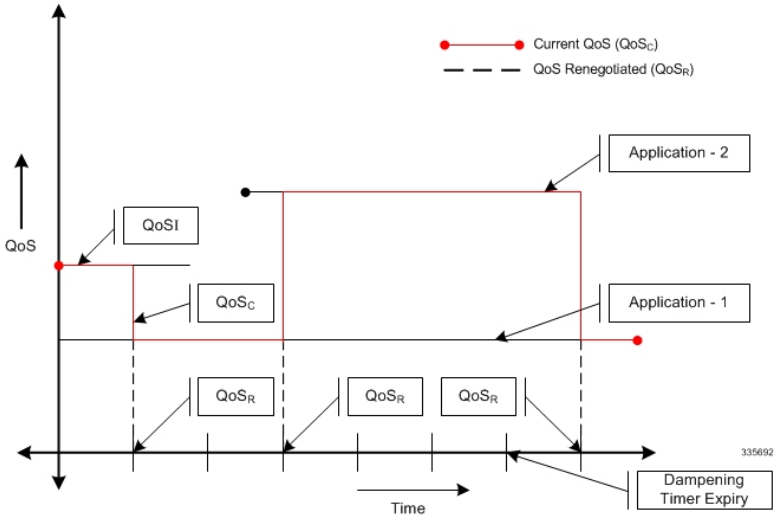
The following is the overall Dynamic QoS Renegotiation process.

1. When a subscriber attaches to the network, the following happens:
   - Dampening timer is started for the subscriber.
   - QoSI is assigned to the subscriber. This becomes the QoSC till a re-negotiation occurs, as shown in the figure below.
   - The traffic class bitfield is cleared.
2. As the subscriber starts using some applications, the traffic gets classified on the basis of type of data packets or traffic as mentioned in section *Classification of Application Traffic*. The corresponding bit in the Traffic-class-bitfield is set accordingly.
3. The mechanics of QoS renegotiation are as follows:
   - Examine traffic-class-bitfield to determine the highest bit that is set. This gives the desired QoS Traffic Class (QoSD). The associated uplink/downlink peak-data-rate and guaranteed-data-rate values are taken from the configured parameters for this traffic class in the subscriber APN.
   - If QoSC matches QoSD, no QoS renegotiation is required. Otherwise, send an Update PDP Context Request to the SGSN with the QoSD values and QoS renegotiation starts.
   - Reset the dampening timer.
   - Clear the traffic-class-bitfield.
4. QoS renegotiation happens under the following conditions:
   - When a higher priority traffic is detected, QoS is renegotiated immediately without waiting for the dampening time to expire. For example, if the current traffic has a QoS of Interactive and the system detects streaming traffic, QoS is immediately upgraded to Streaming.
   - When lower priority traffic is detected, the system waits for the expiry of the dampening timer before lowering the QoS.

- During "silence" or no-traffic, QoS renegotiation requests are not initiated.

As seen in the following figure, the QoS profile for the subscriber goes through three renegotiations to match the QoS profile of the highest priority application currently being used.

Figure 1: Dynamic QoS Renegotiations



When there is no traffic, traffic class drops to "Background" and the corresponding QoS profile is negotiated as described above.

Network Controlled QoS (NCQoS)

Network-controlled QoS is the method by which the system updates the QoS for a PDP context (primary or secondary) upon receipt of Network Requested Update PDP Context (NRUPC) messages from the GGSN. The system can also activate a new secondary PDP context upon receipt of a Network Requested Secondary PDP Context Activation (NRSPCA) message from the GGSN.

How Network Controlled QoS (NCQoS) Works

The GGSN activates or modifies a bearer whenever a service flow matches a statically provisioned Policy and Charging Control (PCC) rule. The network, based on QoS requirements of the application/service, determines what bearers are needed and either modifies an existing bearer or activates a new one.

Statically provisioned PCC rules, called Network Requested Operation (NRO) rules, are configured as charging rules in the Active Charging Service (ACS). As a part of charging action for such rules, QoS-needed and corresponding Traffic Flow Template (TFT) packet filters are configured. QoS-needed mainly consists of QoS Class Identifier (QCI) and data rates. Whereas, TFT mainly consists of uplink and downlink packet filter information.

Warning This feature does not work in conjunction with IMS-Authorization service.

When a packet arrives, the ACS analyzes it and performs rule matching based on the priority in the rulebase. If an NRO rule bound to the context on which the packet arrived matches, ACS applies the bandwidth limit and gating. If an NRO rule bound to some other context matches, ACS discards the packet.

If an unbound NRO rule matches, ACS finds a context with the same QCI as the NRO rule, where the context's Maximum Bit Rate (MBR) and matched rule's MBR (context's MBR + matched rule's MBR) is less than the MBR for that QCI in the APN. If such a context is found, NRUPC for that context is triggered. If the request succeeds, the rule will be bound to that context.

Important The packet that triggered the NRUPC request is discarded.

If no context satisfying the MBR limit is found, or if there is no context with the same QCI as the NRO rule, the system triggers NRSPCA. If the request succeeds, the rule is bound to that context.

Important The packet that triggered the NRSPCA request is discarded.

TFTs from the charging-action associated with the NRO rule are also sent as part of the NRUPC/NRSPCA request, and returned as part of the Create PDP Context Response.

Finally, if a non-NRO rule matches, ACS proceeds with the normal processing of that packet. Non-NRO charging-actions can still do "flow action" or ITC (limit-for-flow-type and limit-for-bandwidth).

ACS also does the following:

- Before making an NRUPC/NRSPCA Request, ACS checks if there is any outstanding request for the same QCI for the same subscriber. If there is, it will not process the new request and discards the packet.
- After a context is terminated, ACS unbinds all the rules bound to that context. Such a rule can later be bound to some other context when a packet matches that rule.

Important The packet that triggered the NRUPC/NRSPCA request is discarded.

Configuring Dynamic QoS Renegotiation

This section describes how to configure per-APN based Dynamic QoS Renegotiation.

Caution For Dynamic QoS Renegotiation, two RADIUS attributes are required for remote subscriber configuration. For a particular subscriber, these attributes can be overridden without considering the timeout for Dynamic QoS Renegotiation and whether Dynamic QoS Renegotiation is enabled or not.

To configure Dynamic QoS Renegotiation:

Step 1 Configure an Access Control List (ACL), as described in the Configuring ACL for Dynamic QoS Renegotiation, on page 6 section.

Step 2 Configure an APN for Dynamic QoS Renegotiation as described in the Configuring APNs for Dynamic QoS Renegotiation, on page 7 section.

Step 3 Save your configuration as described in *Verifying and Saving Your Configuration*.

Step 4 Monitor the operations as described in the Monitoring Dynamic QoS Renegotiation Operation, on page 9 section.

Important Commands used in the configuration examples in this section reflect base functionality (most common or likely commands and/or keyword options). In many cases, other commands and/or keyword options are available. Refer to the *ACS Configuration Mode Commands* and *APN Configuration Mode Commands* sections of the *Command Line Interface Reference* for complete information regarding all commands.

Configuring ACL for Dynamic QoS Renegotiation

Configuring an ACL and applying it to an APN template are required to specify permission and treatment levels for Dynamic QoS Renegotiation.

Use the following example to configure an ACL for Dynamic QoS Renegotiation:

```
configure
     context <context_name>
          ip access-list <acl_name>
               permit { tcp | udp } ........ treatment { background |
conversational | interactive-1 | interactive-2 | interactive-3 | streaming
 }
               end
```

Notes:

- *context_name* must be the name of the destination context in which you want to configure the ACL. The same context must be used for APN configuration.
- For information on configuring the rules that comprise the ACL, refer to *Access Control Lists*.

Configuring Charging Action for Dynamic QoS Renegotiation

Use the following example to configure charging action parameters for Dynamic QoS Renegotiation support:

```
configure
     active-charging service <service_name>
          charging-action <charging_action_name> -noconfirm
               qos-renegotiate traffic-class streaming
               flow action discard
              flow limit-for-bandwidth direction downlink peak-data-rate
 <bps> peak-burst-size <bytes> violate-action lower-ip-precedence
               end
```

Notes:

- A maximum of eight packet filters can be configured per charging action.
- The flow limit-for-bandwidth command contains other option than the example shown here. See *ACS Charging Action Configuration Mode Commands* in the *Command Line Interface Reference* for more information on this command.

Configuring Rulebase for Dynamic QoS Renegotiation

Use the following example to configure rulebase parameters for Dynamic QoS Renegotiation support:

```
configure
     active-charging service <service_name>
          rulebase <rulebase_name> [ -noconfirm ]
               qos-renegotiate timeout <timeout>
               end
```

Configuring APNs for Dynamic QoS Renegotiation

Use the following example to configure an APN template's QoS profile in support of Dynamic QoS Renegotiation:

```
configure
     context <context_name>
          apn <apn_name>
               ip access-group <acl_name> [ in | out ]
               end
```

Notes:

- *context_name* must be the name of the destination context in which you have already configured the ACL, and want to configure the APN template.
- <*acl_name*> must be the name of the ACL that you have already configured in the context.
- If the optional **in** or **out** keywords are not specified in the **ip access-group** command (APN Configuration Mode), the ACL will be applied to all inbound and outbound packets.

Configuring Network Controlled QoS (NCQoS)

To configure NCQoS:

Step 1 Configure packet filter parameters as described in the Configuring Packet Filter for NCQoS, on page 8 section.

Step 2 Configure charging rules and actions as described in the Configuring Charging Action for NCQoS, on page 8 section.

Step 3 Configure APN template and enable bearer control mode for NCQoS as described in the Configuring APN for NCQoS, on page 8 section.

Step 4 Save your configuration as described in *Verifying and Saving Your Configuration*.

Step 5 Monitor the operations as described in the Monitoring Dynamic QoS Renegotiation Operation, on page 9 section.

Important Commands used in the configuration examples in this section implement base functionality (most common or likely commands and/or keyword options). In many cases, other commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands.

Configuring Packet Filter for NCQoS

Use the following example to configure packet filter parameters for NCQoS support:

```
configure
     active-charging service <service_name>
          packet-filter <filter_name> [ -noconfirm ]
               ip local-port { = <port_num> | range <start_port_num> to
<end_port_num> }
               ip protocol { = <proto_num> | range <start_proto_num> to
<end_proto_num> }
               ip remote-address { = { <ip_address> | <ip_address/mask> } | {
range { <ip_address> | <ip_address/mask> } to { <ip_address> | <ip_address/mask> } }
               ip remote-port { = <port_num> | range <start_port_num> to
<end_port_num> }
               direction { bi-directional | download | upload }
               priority <priority>
               end
```

Configuring Charging Action for NCQoS

Use the following example to configure charging action parameters for NCQoS support:

```
configure
     active-charging service <service_name>
          charging-action <charging_action_name> [ -noconfirm ]
               qos-class-identifier <identifier>
               flow action discard [ downlink | uplink ]
               tft packet-filter <filter_name>
               flow limit-for-bandwidth direction { downlink | uplink }
peak-data-rate <bps> peak-burst-size <bytes> violate-action { discard |
lower-ip-precedence }
               end
```

Notes:

- A number of optional keywords and variable are available for the **flow limit-for-bandwidth direction** command. Refer to the *ACS Charging Action Configuration Mode Commands* section of the *Command Line Interface Reference* for more information regarding this command.

Configuring APN for NCQoS

Use the following example to enable Bearer Control Mode (BCM) for NCQoS support:

```
configure
     context <context_name>
          apn <apn_name>
               bearer-control-mode [ mixed | ms-only | none ]
               end
```

Notes:

- To enable NCQoS, bearer-control-mode in the APN Configuration Mode must be configured with **mixed** mode.

Monitoring Dynamic QoS Renegotiation Operation

Use the following steps to verify/monitor Dynamic QoS Renegotiation operations:

Step 1 Verify that your APNs were configured properly by entering the following command:

show apn { all | name *apn_name* **}**

The output is a listing of APN parameter settings.

Step 2 Verify that the ACLs have been properly applied by entering the following command:

show apn name *apn_name*

apn_name must be the name of the APN configured in the *Configuring APNs for Dynamic QoS Renegotiation* section.The output of this command displays the APN configuration. Examine the output for the **ip output access-group** and **ip input access-group** fields. For more details refer to the *Applying a Single ACL to Multiple Subscribers* section.

Step 3 Verify that your ACL was configured properly by entering the following command:

show ip access-list *acl_name*

The output is a concise listing of IP Access Control List parameter settings.

Step 4 Monitor your QoS renegotiation status for a subscriber by running the **show subscriber ggsn-only full** command (Exec mode).

The output is a concise listing of subscribers' settings.

Step 5 For L7 based QoS Renegotiation, view how many time QoS renegotiations have happened for that session by running the **show active-charging sessions full all** command (Exec mode).

Step 6 View the statistics of APN related to QoS renegotiation parameters by entering the following command:

show apn statistics { all | name *apn_name* **}**

The output is a listing of APN statistics related to QoS Renegotiation.

Event IDs Pertaining to Dynamic QoS Renegotiation

The Session Manager facility sources event IDs that can be useful for diagnosing errors that could occur when implementing of Dynamic QoS Renegotiation feature.

The following table displays information pertaining to these events.

Table 1: Event IDs in Session Manager Pertaining to Dynamic QoS Renegotiation

Event	Event ID	Type	Additional Information
QoS Renegotiation timer started for subscriber	10917	Info	"Indicates that the Dynamic QoS Renegotiation timer was started for the subscriber"
QoS Renegotiation timer stopped for subscriber	10918	Info	"Indicates that the Dynamic QoS Renegotiation timer was stopped for the subscriber"
QoS Renegotiation timer expired for subscriber	10919	Info	"Indicates that the Dynamic QoS Renegotiation timer was expired for the subscriber"
QoS Renegotiation message sent for subscriber	10920	Info	"Indicates that the Dynamic QoS Renegotiation message was sent for the subscriber"
L4 classification done for subscriber traffic	10921	Info	"Indicates the kind of L4 classification that was done for the subscriber traffic."

RADIUS Attributes

The RADIUS attributes listed in the following table are used to enable Dynamic QoS Renegotiation for subscribers configured on remote RADIUS servers.

For more information on these attributes, if you are using StarOS 12.3 or an earlier release, refer to the *AAA and GTPP Interface Administration and Reference*. If you are using StarOS 14.0 or a later release, refer to the *AAA Interface Administration and Reference*.

Table 2: RADIUS Attributes Required for Dynamic QoS Renegotiation Support

Attribute	Description
SN-Enable-QoS-Renegotiation (or SN1-Enable-QoS-Renegotiation)	Enables the Dynamic QoS Renegotiation for specific profile application. This attribute displays "enable qos renegotiation".
SN-QoS-Renegotiation-Timeout (or SN1-QoS-Renegotiation-Timeout)	Timeout duration for dampening time for QoS renegotiation to specific profile application. This attribute displays "qos renegotiation timeout".