Congestion Control

This chapter describes the Congestion Control feature. It covers the following topics:

Overview

Congestion Control monitors the system for conditions that could potentially degrade performance when the system is under heavy load. Typically, these conditions are temporary (for example, high CPU or memory utilization) and are quickly resolved. However, continuous or large numbers of these conditions within a specific time interval may impact the system's ability to service subscriber sessions. Congestion control helps identify such conditions and invokes policies for addressing the situation.

Congestion control operation is based on configuring the following:

- **Congestion Condition Thresholds:** Thresholds dictate the conditions for which congestion control is enabled and establishes limits for defining the state of the system (congested or clear). These thresholds function in a way similar to operation thresholds that are configured for the system as described in the *Thresholding Configuration Guide*. The primary difference is that when congestion thresholds are reached, a service congestion policy and an SNMP trap (starCongestion) are generated.

  A threshold tolerance dictates the percentage under the configured threshold that must be reached in order for the condition to be cleared. An SNMP trap, starCongestionClear, is then triggered.

  - **Port Utilization Thresholds**: If you set a port utilization threshold, when the average utilization of all ports in the system reaches the specified threshold, congestion control is enabled.
  - **Port-specific Thresholds**: If you set port-specific thresholds, when any individual port-specific threshold is reached, congestion control is enabled system-wide.

- **Service Congestion Policies:** Congestion policies are configurable for each service. These policies dictate how services respond when the system detects that a congestion condition threshold has been crossed.

Important This section provides the minimum instruction set for configuring congestion control. Commands that configure additional interface or port properties are provided in *Subscriber Configuration Mode* in the *Command Line Interface Reference*. Always refer to the Administration Guides for all of the licensed products running on this platform for additional configuration information with respect to congestion control. Congestion control functionality varies based on product and StarOS version.

For the MME three levels of congestion control thresholds are supported – critical, major and minor. By default only the critical threshold is supported for other products. SNMP traps also support major and minor congestion control thresholds. A set of **congestion-action-profile** commands allows an operator to establish additional actions to be taken for specific thresholds and threshold levels.

Configuring Congestion Control

To configure Congestion Control functionality:

Step 1 Configure congestion control thresholds as described in Configuring the Congestion Control Threshold, on page 2

Step 2 Configure service congestion policies as described in Configuring Service Congestion Policies, on page 3

Step 3 Enable redirect overload policies as described in Enabling Congestion Control Redirect Overload Policy, on page 4

Step 4 Configure disconnecting subscribers based on call or inactivity time as described in Disconnecting Subscribers Based on Call or Inactivity Time, on page 6

Step 5 Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

Configuring the Congestion Control Threshold

To configure congestion control threshold, apply the following example configuration in the Global Configuration mode of the CLI:

```
configure
   congestion-control threshold max-sessions-per-service-utilization percent

   congestion-control threshold tolerance percent
   end
```

Notes:

- There are numerous threshold parameters. See *Global Configuration Mode Commands* in the *Command Line Interface Reference* for more information.
- The tolerance is the percentage under a configured threshold that dictates the point at which the condition is cleared.
- Multiple levels of congestion thresholds – critical, major and minor – a re supported for various types of congestion control thresholds. If a threshold level is not specified, the default is critical. Currently, major and minor thresholds are only supported for the MME and ePDG. The **congestion-action-profile** command under **lte-policy** defines the action to be taken when thresholds are exceeded. See *Global*

Configuration Mode Commands, *LTE Policy Configuration Mode Commands* and *Congestion Action Profile Configuration Mode Commands* in the *Command Line Interface Reference* for more information.

- Repeat this configuration as needed for additional thresholds.

Configuring Service Congestion Policies

To create a congestion control policy, apply the following example configuration in the Global Configuration mode of the CLI:

```
configure
      congestion-control policy service action { drop | none | redirect |
reject }
      end
```

Notes:

- When the redirect action occurs for PDSN services, the PDSN responds to the PCF with a reply code of 136, "unknown PDSN address" along with the IP address of an alternate PDSN.
- **redirect** is not available for PDIF. The default action for PDIF is "none."
- When the redirect action occurs for HA services, the system responds to the FA with a reply code of 136, "unknown home agent address".
- **redirect** cannot be used in conjunction with GGSN services.
- **redirect** is not available for the Local Mobility Anchor (LMA) service.
- When setting the action to **reject**, the reply code is 130, "insufficient resources".
- For the GGSN, the reply code is 199, "no resources available".
- For the SaMOG, MME and ePDG, **redirect** is not available.
- For the MME and ePDG, create action profiles for optional major and minor thresholds using the **congestion-action-profile** command under **lte-policy** in the Global Configuration mode.
- For the MME and ePDG, you can specify *service* as **critical**, **major** or **minor** to set a policy and associate an action-profile for the respective threshold. See *Global Configuration Mode Commands* in the *Command Line Interface Reference* for more information.

Configuring Overload Reporting on the MME and ePDG

When an overload condition is detected on an MME and ePDG and the report-overload keyword is enabled in the **congestion-control policy** command, the system reports the condition to a specified percentage of eNodeBs and proceeds to take the configured action on incoming sessions. To create a congestion control policy with overload reporting, apply the following example configuration:

```
configure
   congestion-control policy mme-service action report-overload
reject-new-sessions enodeb-percentage percentage
   end
```

Notes:

- Other overload actions include **permit-emergency-sessions** and **reject-non-emergency-sessions**.

Enabling Congestion Control Redirect Overload Policy

To create a congestion control policy and configure a redirect overload policy for the service, apply the following example configuration:

```
configure
   congestion-control
      context context_name
        {service_configuration_mode}
             policy overload redirect address
             end
```

Notes:

- *Optional:* If the congestion control policy action was configured to **redirect**, then a redirect overload policy must be configured for the service(s) that are affected.
- There are several service configuration modes that you can configure. See the *Command Line Interface Reference* for a complete list of modes.
- You can set various options for redirection. See the *Command Line Interface Reference* for more information.
- Repeat this configuration example to configure overload policies for additional services configured in the same context.

Verify the Service Overload Policies

To verify that the service overload policies were properly configured enter the following command in the Exec Mode:

```
[local]host_name# show service_type name service_name
```

This command lists the entire service configuration. Verify that the information displayed for the "Overload Policy" is accurate.

Repeat this configuration example to configure additional services in other contexts.

Verify the Congestion Control Configuration

To verify Congestion Control Configuration enter the following **show** command in the Exec Mode.

```
[local]host_name# show congestion-control configuration
```

The following output is a concise listing of all threshold and policy configurations showing multi-level Critical, Major and Minor threshold parameters:

```
Congestion-control: enabled

Congestion-control Critical threshold parameters
    system cpu utilization:              80%      exclusion: demux
    service control cpu utilization:     80%
    system memory utilization:           80%
    message queue utilization:           80%
    message queue wait time:             10 seconds
    port rx utilization:                 80%
```

```
    port tx utilization:                80%
    license utilization:                100%
    max-session-per-service utilization: 100%
    tolerence limit:                    10%
Congestion-control Critical threshold parameters
    system cpu utilization:             80%
    service control cpu utilization:    80%
    system memory utilization:          80%
    message queue utilization:          80%
    message queue wait time:            10 seconds
    port rx utilization:                80%
    port tx utilization:                80%
    license utilization:                100%
    max-session-per-service utilization: 100%
    tolerence limit:                    10%
Congestion-control Major threshold parameters
    system cpu utilization:             0%
    service control cpu utilization:    0%
    system memory utilization:          0%
    message queue utilization:          0%
    system memory utilization:          0%
    message queue wait time:            0 seconds
    port rx utilization:                0%
    port tx utilization:                0%
    license utilization:                0%
    max-session-per-service utilization: 0%
    tolerence limit:                    0%
Congestion-control Minor threshold parameters
    system cpu utilization:             0%
    service control cpu utilization:    0%
    system memory utilization:          0%
    message queue utilization:          0%
    message queue wait time:            0 seconds
    port rx utilization:                0%
    port tx utilization:                0%
    license utilization:                0%
    max-session-per-service utilization: 0%
    tolerence limit:                    0%
Overload-disconnect: disabled
Overload-disconnect threshold parameters
    license utilization:                80%
    max-session-per-service utilization: 80%
    tolerance:                          10%
    session disconnect percent:         5%
    iterations-per-stage:               8
Congestion-control Policy
    pdsn-service: none
    hsgw-service: none
    ha-service:   none
    ggsn-service: none
    closedrp-service: none
    lns-service: none
    pdif-service: none
  wsg-service: none
  pdg-service: none
    epdg-service: none
    fng-service: none
    sgsn-service: none
    mme-service: drop
  henbgw-network-service: none
    asngw-service: none
    asnpc-service: none
    phsgw-service: none
    phspc-service: none
```

```
    mipv6ha-service: none
    lma-service: none
    saegw-service: none
    sgw-service: none
    pgw-service: none
    hnbgw-service: none
    pcc-policy-service: none
    pcc-quota-service: none
    pcc-af-service: none
    ipsg-service: none
  samog-service: none
```

The primary threshold to observe is *license utilization*. This threshold is defaulted to 80%. Overload controls on the system enables the Congestion-control Policy when the system has only 80% of the licenses used. The overload condition will not clear until the utilization drops below the tolerance limit setting. The tolerance limit is defaulted to 10%. If the system goes into overload due to license utilization (threshold at 80%), the overload condition will not clear until the license utilization reaches 70%.

The system may go into overload if threshold settings are set too low and congestion control is enabled. You will need to review all threshold values and become familiar with the settings.

Since the recommendation for license utilization overload threshold is 100%, you should enable a license threshold alarm at 80%. An alarm is then triggered when the license utilization hits 80%. When the congestion-control policy setting is set to **drop**, the system drops incoming packets containing new session requests.

Important For additional information on configuring the alarm threshold, refer to the *Threshold Configuration Guide*.

Verify MME and ePDG Congestion Action Profiles

To verify MME and ePDG multilevel congestion action profiles, run the following Exec mode command:

```
[local]host_name# show lte-policy congestion-action-profile { name profile_name
 | summary }
```

Disconnecting Subscribers Based on Call or Inactivity Time

During periods of heavy system load, it may be necessary to disconnect subscribers in order to maintain an acceptable level of system performance. You can establish thresholds to select subscribers to disconnect based on the length of time that a call has been connected or inactive.

To enable overload disconnect for the currently selected subscriber, use the following configuration example:

```
configure
   context context_name
      subscriber name subscriber_name
         default overload-disconnect threshold inactivity-time dur_thresh
         default overload-disconnect threshold connect-time dur_thresh
         end
```

To disable the overload disconnect feature for this subscriber, use the following configuration example:

```
configure
  context context_name
    subscriber subscriber_name
    no overload-disconnect { [threshold inactivity-time] | [threshold
```

```
connect-time] }
     end
```