

Traffic Policy-Map Configuration Mode Commands

A Policy-Map imposes a flow-based traffic policy for Traffic Policy feature within a destination context. It designates the flow treatment based on the classification rules configured in Class-Map mode for a subscriber session flow.

Command Modes

Exec > Global Configuration > Context Configuration > Traffic Policy Map Configuration

configure > context *context_name* **> policy-map name** *map_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-policy-map)#`

Important The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

- 3gpp2 data-over-signaling, on page 2
- access-control, on page 2
- accounting suppress, on page 3
- accounting trigger, on page 4
- class-map, on page 6
- description, on page 7
- do show, on page 7
- end, on page 8
- exit, on page 8
- flow-tp-trigger, on page 8
- ip header-compression, on page 9
- qos encaps-header, on page 10
- qos traffic-police, on page 11
- qos user-datagram dscp-marking, on page 13
- sess-tp-trigger, on page 14
- type, on page 15

3gpp2 data-over-signaling

Configures 3GPP2-related flow treatment policy for the flow-based traffic policing of subscriber sessions.

Product

HA

HSGW

PDSN

P-GW

SAEGW

SCM

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Traffic Policy Map Configuration

configure > context *context_name* **> policy-map name** *map_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-policy-map)#
```

Syntax Description

3gpp2 data-over-signaling marking [class-map *class_name* **]**
no 3gpp2 data-over-signaling marking

no

Disables configured 3GPP2-related flow treatment policy.

class-map *class_name*

Associates class map to be used for selective data over signaling (DOS) marking. *class_name* is an alphanumeric string of 1 through 15 characters.

marking

Indicates 3GPP2-related traffic flow for data over signaling channel.

Usage Guidelines

Use this command to mark traffic flows for 3GPP2-related policy.

Example

3gpp2 data-over-signaling marking

access-control

Configures the access control action for traffic flows matching the Class-Map rules.

Product

ASN-GW

HA

HSGW

PDSN

P-GW

SAEGW

SCM

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Traffic Policy Map Configuration

configure > context *context_name* **> policy-map name** *map_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-policy-map)#
```

Syntax Description

access-control { allow | discard }

allow

Allows the packets, if the policy matches with the criteria defined in the Class-Map assigned to the specific traffic policy.

discard

Discards the packets, if the policy matches with the criteria defined in the Class-Map assigned to the specific traffic policy.

Usage Guidelines

Configures the action or treatment for traffic flows match criteria specified in the assigned Class-Map.

Example

The following command allows the packets or traffic flow on matching with criteria specified in assigned Class-Map for specific traffic policy.

access-control allow

accounting suppress

Suppresses accounting action for traffic flows matching the policy map.

Product

ASN-GW

HA

HSGW

PDSN

P-GW

SAEGW

SCM

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Traffic Policy Map Configuration

configure > context *context_name* **> policy-map name** *map_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-policy-map)#`

Syntax Description

`[ no ] accounting suppress`

no

Removes the suppression of accounting for traffic flow matching this policy map.

Usage Guidelines

Use this command to suppress accounting action on traffic flow matching this policy map.

Policy maps configured for accounting suppression are used to implement the QChat Billing Suppression feature that selectively starts and terminates accounting sessions based on the categorization of traffic as being interesting or non-interesting. See the **accounting trigger** command.

Example

The following command configures suppression of accounting on traffic flows matching this policy map:

`accounting suppress`

accounting trigger

Configures an accounting trigger policy map to selectively start and terminate accounting sessions based on the categorization of traffic as being interesting or non-interesting. This command supports the QCHAT Billing Suppression feature.

Product

HSGW

PDSN

P-GW

SAEGW

SCM

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Traffic Policy Map Configuration

configure > **context** *context_name* > **policy-map name** *map_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-policy-map)#
```

Syntax Description

[no | default] accounting trigger { inactivity-timeout | interesting-traffic | intra-service-handoff }

default

Sets or restores the default value assigned for specified parameter.

no

Disables previously configured triggers.

inactivity-timeout

Generates an accounting Stop message if there has been no data activity on the session for the interim accounting timeout interval.

Default: disabled

interesting-traffic

Generates an accounting Start message upon arrival of interesting traffic.

Default: disabled

intra-service-handoff

Generates accounting Start and Stop messages during intra-service handoffs.

Default: enabled

If disabled, the messages are suppressed during the handoffs. The current accounting session continues and no Stop or Start messages are generated during the intra-service handoff.

Usage Guidelines

Use this command to configure an accounting trigger policy map (ATPM) to selectively start and terminate accounting sessions based on the categorization of traffic as being interesting or non-interesting. This command supports the QChat Billing Suppression feature.

Interesting traffic is identified as traffic that does not match any of the other Accounting Policy Maps (APMs) configured for accounting suppression. See the **accounting suppress** command.

An ATPM is similar to an APM, but without the class map rules. The ATPM is configured as of type accounting using the **type accounting** command.

Optionally, timeout can be triggered when there is no data traffic for the interim accounting timeout interval using the **accounting trigger inactivity-timeout stop** command. On timeout, the accounting session is terminated and an Accounting Stop message is sent. A new accounting session is created if interesting traffic resumes.

In the ATPM, the trigger to start accounting for interesting traffic is configured using the **accounting trigger interesting-traffic** command. Accounting Start is triggered on arrival of interesting traffic, or change in airlink parameters conveyed through active-start airlink record. If an active-start record was included in the initial

connection setup, Accounting Start is not triggered. But if the active-start comes separately and is the first one for the session, it is treated as airlink change and an Accounting Start is sent.

The ATPM should have the lowest precedence among the APMs.

As the airlink events are generated on the ingress side, the ATPM must be included in a policy group that is applied to the ingress direction in the subscriber profile. The configuration is applicable only for standard trigger policy and session based accounting mode.

Example

The following command sets the trigger to generate accounting start message upon arrival of interesting traffic:

```
accounting trigger interesting-traffic
```

class-map

Assigns a traffic classification rule (Class-Map) to the policy map.

Product

ASN-GW

HA

HSGW

PDSN

P-GW

SAEGW

SCM

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Traffic Policy Map Configuration

configure > context *context_name* **> policy-map name** *map_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-policy-map)#
```

Syntax Description

[no] class-map *name*

no

Enables or disables **class-map**.

name

Specifies the name of the class map assigned for this policy map. The class map should have been preconfigured via the Class Map Configuration Mode.

name must be an alphanumeric a string of 1 through 15 characters.

Usage Guidelines Use this command to assign a class map to the policy map for traffic policing. The class map is configured in the Class Map Configuration Mode.

Example

The following command assigns the class map *classification1* to the current policy map:

```
class classification1
```

description

Allows you to enter descriptive text for this configuration.

Product All

Privilege Security Administrator, Administrator

Syntax Description

```
description text
no description
```

no

Clears the description for this configuration.

text

Enter descriptive text as an alphanumeric string of 1 to 100 characters.

If you include spaces between words in the description, you must enclose the text within double quotation marks (" "), for example, "AAA BBBB".

Usage Guidelines The description should provide useful information about this configuration.

do show

Executes all **show** commands while in Configuration mode.

Product All

Privilege Security Administrator, Administrator

Syntax Description

```
do show
```

Usage Guidelines Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.

Caution There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

end

Exits the current configuration mode and returns to the Exec mode.

Product All

Privilege Security Administrator, Administrator

Syntax Description **end**

Usage Guidelines Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product All

Privilege Security Administrator, Administrator

Syntax Description **exit**

Usage Guidelines Use this command to return to the parent configuration mode.

flow-tp-trigger

This command specifies that the traffic volume will be calculated based on the traffic on the flow.

Product ASN-GW

HA

HSGW

PDSN

P-GW

SAEGW

SCM

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Traffic Policy Map Configuration

configure > context *context_name* **> policy-map name** *map_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-policy-map)#`

Syntax Description

flow-tp-trigger volume *traffic_volume_threshold*
no flow-tp-trigger volume

traffic_volume_threshold

Specifies the volume threshold to trigger traffic policing. *volume* must be an integer from 1 through 4294967295.

Usage Guidelines

This command is available if you have purchased and installed the Intelligent Traffic Control License on your system. Use this command to calculate the traffic volume based on the traffic on the flow.

Example

flow-tp-trigger volume 500

ip header-compression

Enables the system to mark IP flows for Robust Header Compression (RoHC).

Product

ASN-GW

HA

HSGW

PDSN

P-GW

SAEGW

SCM

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Traffic Policy Map Configuration

configure > context *context_name* **> policy-map name** *map_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-policy-map)#`

Syntax Description

[no] ip header-compression rohc flow-marking

no

Disables the setting.

rohc flow-marking

Marks the IP flow for SO67 and PPP RoHC.

Usage Guidelines

Use this command to mark IP flows for SO67 and PPP RoHC.

Example

```
ip header-compression rohc flow-marking
```

qos encaps-header

Enables and configures Quality of Service (QoS) policy to use Differentiated Service Code Point (DSCP) marking in IP header fields for the flow-based traffic policing to subscriber session flow.

Product

ASN-GW

HA

HSGW

PDSN

P-GW

SAEGW

SCM

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Traffic Policy Map Configuration

configure > context *context_name* **> policy-map name** *map_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-policy-map)#
```

Syntax Description

```
qos encaps-header dscp-marking { dscp_code | copy-from-user-datagram [
ignore-pcf-signaled-dscp ] | user-datagram }
no qos encaps-header dscp-marking { dscp_code | copy-from-user-datagram [
ignore-pcf-signaled-dscp ] }
```

no

Enables/Disables the **qos encaps-header**.

The value must be expressed as a hexadecimal value from 0x00 through 0x3F.

dscp-marking *dscp_code*

Uses the DSCP code value marked in the IP header of packet/flow to determine the QoS for traffic policing. *dscp_code* must be expressed as a hexadecimal number from 0x00 through 0x3F.

copy-from-user-datagram

Uses the DSCP code value from the user datagram (UDP header) to determine the QoS for traffic policing.

ignore-pcf-signaled-dscp

Overrides the highest priority DSCP value signaled by the PCF.

user-datagram

Uses the DSCP value copied from the user datagram.

Usage Guidelines

Use this command to apply the QoS policy based on the DSCP value encapsulated in the IP packet header to police subscriber session traffic flows.



Important For more information on the QoS traffic policing, see the *System Administration Guide*.

Example

The following command sets QoS policy with DSCP code value to *0x0C* for Class 1, silver (AF12):

```
qos encaps-header dscp-marking 0x0c
```

qos traffic-police

Enables and configures Quality of Service (QoS) policy for flow-based traffic policing of subscriber session flows on a per-flow basis.

Product

ASN-GW

HA

HSGW

PDSN

P-GW

SAEGW

SCM

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Traffic Policy Map Configuration

configure > context *context_name* **> policy-map name** *map_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-policy-map)#
```

Syntax Description

qos traffic-police committed *bps* **peak** *bps* **burst-size** *byte* **exceed-action { drop | lower-ip-precedence | allow } violate-action { drop | lower-ip-precedence | allow }**
no qos traffic-police

no

Enables/Disables the **qos traffic-police**



Important This parameter should be configured to be greater than the following two values: 1) three times greater than packet MTU for the subscriber connection, OR 2) three seconds worth of token accumulation within the "bucket" for the configured peak-data-rate.

burst-size *bytes*

Default: 3000

Specifies the allowed peak burst size in bytes. *bytes* must be an integer from 0 through 4294967295.



Important This parameter should be configured to be greater than the following two values: 1) three times greater than the packet MTU for the subscriber connection, OR 2) three seconds worth of token accumulation within the "bucket" for the configured peak-data-rate.

committed *bps*

Default: 144000

Specifies the committed data rate (guaranteed-data-rate) in bits per second (bps).

bps must be an integer from 0 through 4294967295.

exceed-action { drop | lower-ip-precedence | allow }

Default: **lower-ip-precedence**

Specifies the action to take on packets that exceed the committed-data-rate but do not violate the peak-data-rate. The following actions are supported:

drop: Drops the packet

lower-ip-precedence: Transmits the packet after lowering the ip-precedence

allow: Transmits the packet

peak *bps*

Default: 256000

Specifies the peak data-rate for the subscriber in bits per second (bps).

bps must be an integer from 0 through 4294967295.

violate-action { drop | lower-ip-precedence | allow }

Default: drop

Specifies the action to take on the packets that exceed both the committed-data-rate and the peak-data-rate. The following actions are supported:

drop: Drops the packet

lower-ip-precedence: Transmits the packet after lowering the IP precedence

allow: Transmits the packet

Usage Guidelines

Use this command to apply the QoS policy to a subscriber session flow for flow-based traffic policing.

Important For additional information on the QoS traffic policing, see the *System Administration Guide*.

Example

The following command sets the committed data rate to *102400* bps with a peak data rate of *128000* bps and a burst size of *2048* bytes. This lowers the IP precedence when the committed-data-rate is exceeded and drops the packets when the peak-data-rate are violated:

```
qos traffic-police commited 102400 peak 128000 burst-size 2048
exceed-action lower-ip-precedence violate-action drop
```

qos user-datagram dscp-marking

Enables and configures Quality of Service (QoS) policy related to differentiated service code point (DSCP) marking in the user datagrams of subscriber session flows on a per-flow basis.

Product

ASN-GW

HA

HSGW

PDSN

P-GW

SAEGW

SCM

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Traffic Policy Map Configuration

configure > context *context_name* **> policy-map name** *map_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-policy-map)#
```

Syntax Description

qos user-datagram dscp-marking *dscp_code*
no qos user-datagram dscp-marking

dscp_code

Specifies the use of the DSCP code value marked in the IP header of packet/flow to determine the QoS for traffic policing. *dscp_code* must be expressed as a hexadecimal number from 0x00 through 0x3F.

Usage Guidelines

Use this command to apply the QoS policy to subscriber session flow by DSCP marking in user datagram.

Example

The following command sets DSCP marking for user datagram as *0x01* for QoS to subscriber session flow:

qos user-datagram dscp-marking 0x01

sess-tp-trigger

Configures the trigger for traffic policing based on the traffic volume for a subscriber session.

Product

ASN-GW

HA

HSGW

PDSN

P-GW

SAEGW

SCM

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Traffic Policy Map Configuration

configure > **context** *context_name* > **policy-map name** *map_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-policy-map)#
```

Syntax Description

sess-tp-trigger volume *volume* **direction { both | downlink | uplink }**
no sess-tp-trigger

no

Enables or disables the **sess-tp-trigger**

volume

Specifies the traffic volume threshold (in bytes) that triggers traffic control. *volume* is an integer from 1 through 4294967295.

Usage Guidelines

Use this command to trigger traffic control based on the traffic volume for a subscriber session. This command requires the purchase and installation of a license.

Example

```
sess-tp-trigger 500
```

type

Specifies the type of traffic policy within a specific Policy-Map.

Product

ASN-GW

HA

HSGW

PDSN

P-GW

SAEGW

SCM

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Traffic Policy Map Configuration

configure > context *context_name* **> policy-map name** *map_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-policy-map)#
```

Syntax Description

type { accounting | dynamic { three-gpp2 rev-A profile-id { any | id *profile_id* **| range** *low_value* **to** *high_value* **} flow-id { any | id** *flow_id* **| range** *low_value* **to** *high_value* **} | pre-provisioned wimax asn-service-profile-id { any | id** *service_id* **} asn-pdfid { any | id** *pdf_id* **} | static | template }**

accounting

Specifies the type of traffic policing as accounting for this specific policy map. This configuration is used for enabling/disabling the accounting of different flows matching conditions within this Policy-Map.

dynamic

Identifies the type of policy map as dynamic.

three-gpp2 rev-A

Configures the dynamic policy map type for CDMA2000-3GPP2 RevA service.

profile-id { any | id *profile_id* | range *low_hex* to *high_hex* }

Specifies the profile id matching within this policy map.

any: allows any profile identifier matching this policy map.

id *profile_id*: allows specific profile identifier matching with in this policy map. *profile_id* must be a hexadecimal number from 0x0 to 0xFFFF.

range *low_value* **to** *high_value*: identifies a range in which a profile identifier must fall within to be considered a match. *low_value* and *high_value* must be either a hexadecimal number from 0x0 to 0xFFFF, or an integer from 0 through 65535 characters.

flow-id { any | id *flow_id* | range *low_hex* to *high_hex* }

Specifies the flow id matching in this policy map.

any allows any flow identifier matching with in this policy map.

id *flow_id* allows specific flow identifier matching with in this policy map. *flow_id* must be either a a hexadecimal number from 0x0 to 0xFFFF, or an integer from 0 to 65535.

range *low_value* **to** *high_value*: identifies a range in which a flow identifier must fall within to be considered a match. *low_value* and *high_value* must be either a hexadecimal number from 0x0 to 0xFFFF, or an integer 0 to 65535.

pre-provisioned

Identifies the type of policy map as pre-provisioned.

wimax

Configures WiMAX service policy map in an ASN-GW service.

asn-service-profile { any | id *service_id* }

Specifies the ASN Service profile identifier to match with in this policy map.

any: Allows any ASN Service Profile Identifier matching within this policy map.

id *service_id*: Allows specific Service Profile matching to a specified identifier. *service_id* must be an integer from 1 to 65535 that matches a service ID that was configured in the Subscriber Configuration Mode.

asn-pdfid { any | id *pdf_id* }

Specifies the ASN Packet Data Flow Identifier to match with in this policy map.

any: Allows any ASN Packet Data Flow Identifier matching within this policy map.

id *pdf_id*: Allows specific Packet Data Flow matching to a specified identifier. *pdf_id* must be an integer from 1 to 255 that matches a PDF ID that was configured in the Subscriber Configuration Mode.

static

Specifies the type of traffic policing as static for this specific Policy Map. In this type of policy, the traffic flow classification and flow treatment is pre-defined with classification rules through Class-Map configuration.

This is the detailed type of policy map.

template

Specifies the type of traffic policy to as a template to all subscribers associated with this policy map.

Usage Guidelines

Specifies the type of traffic policy within the specific Policy-Map.

Example

The following commands configures the traffic policy for this Policy-Map as static:

```
type static
```

The following commands configures the traffic policy for this Policy-Map as pre-provisioned for WiMAX service requiring a match of any service profile and PDF id of *3*:

```
type pre-provisioned wimax asn-service-profile any asn-pdfid id 3
```