Application Traffic Management Command Reference

MANUAL PAGE

190 80-CRA 119 1170/1-V1 Uen J

Copyright

© Ericsson AB 2009–2011. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

SmartEdge	is a registered trademark of Telefonaktiebolaget LM Ericsson.
NetOp	is a trademark of Telefonaktiebolaget LM Ericsson.

Contents

1 Commands

This document provides command syntax and usage guidelines for commands used in the configuration and operation of application traffic management. For an overview of application traffic management, see Reference [1]. For configuration tasks, see Reference [2].

1.1 access-group

access-group ***acl-name***

no access-group

1.1.1 Command Mode

DPI policy configuration

1.1.2 Syntax Description

acl-name	Name of the DPI traffic management ACL policy created using the dpi access-list command (in global configuration mode).

1.1.3 Default

None

1.1.4 Usage Guidelines

Associates a DPI traffic management policy with a DPI access control list.

1.1.5 Examples

```
[local]Redback(config-policy-dpi)#access-group myacl
```

1.2 accounting

accounting [class | protocol]

no accounting [class | protocol]

1.2.1 Command Mode

DPI traffic-management policy configuration

1.2.2 Syntax Description

`class`	Depending on whether the policy you are configuring is associated with a subscriber or subscriber group, enables per subscriber per class or per subscriber group per class statistics reporting.
`protocol`	Enables per subscriber per protocol statistics reporting.

1.2.3 Default

Statistics reporting is disabled by default.

1.2.4 Usage Guidelines

Enables statistics reporting. The **no** form of this command disables reporting.

1.2.5 Examples

The following example shows how to enable per subscriber per protocol statistics reporting:

```
[local]Redback(config)#dpi traffic-management policy p1
[local]Redback(config-dpi-policy)#accounting protocol
```

The following example shows how to enable per subscriber group per class statistics reporting:

```
[local]Redback(config)#dpi traffic-management policy p1agg aggregate
[local]Redback(config-dpi-policy)#accounting class
```

1.3 action policy

action policy ***action-policy-name*** [**aggregate**]

no action policy [***action-policy-name***] [**aggregate**]

1.3.1 Command Mode

DPI policy configuration

1.3.2 Syntax Description

action-policy-name	Name of the action policy.
aggregate	Optional. Specifies that the action policy is used for per class per subscriber group or per class per SmartEdge® router level traffic management configuration.

1.3.3 Default

No DPI traffic management action policy is configured.

1.3.4 Usage Guidelines

Associates a DPI traffic management policy with a DPI traffic management action policy.

1.3.5 Examples

The following example shows how to configure a DPI traffic management policy with the DPI traffic management action policy, a1.

```
[local]Redback(config-policy-dpi)#action policy a1
```

1.4 application

[**seq** *sequence-number*] **application** *application-name* [**network** *network-prefix/prefix-length* | **any**] **class** *class-name*

no seq *sequence-number*

1.4.1 Command Mode

DPI access control list configuration

1.4.2 Syntax Description

seq *sequence-number*	Optional. Sequence number for the statement. Range: 1 to 4,294,967,295.
application *application-name*	Application name.
network *network-prefix*	Optional. Source or destination IP address to be included in the criteria. Destination IP address when the traffic direction is from subscriber to Internet; source IP address when the traffic direction is from Internet to subscriber.
prefix-length	Optional. Number of prefix bits. Range: 0 to 32.
any	Optional Indicates that IP traffic from all IP addresses is to be included in the criteria.
class *class-name*	Policy-based class name.

1.4.3 Default

None

1.4.4 Usage Guidelines

Creates an ACL statement to allow packets that meet the specified criteria. Use the CLI help with this command (**application** ?) or issue the **show dpi traffic-management application** command in any mode for a list of application names. If the **seq** *sequence-number* construct is not specified, the system assigns a sequence number.

1.4.5 Examples

```
[local]Redback(dpi-acl)#seq 10 application bittorrent class c1
```

```
[local]Redback(dpi-acl)#seq 40 application skype class c3
```

```
[local]Redback(dpi-acl)#application youtube class c5
```

1.5 category

[**seq** *sequence-number*] **category** *category-name* [**network** *network-prefix/prefix-length* | **any**] **class** *class-name*

no seq *sequence-number*

1.5.1 Command Mode

DPI access control list configuration

1.5.2 Syntax Description

seq *sequence-number*	Optional. Sequence number for the statement. Range: 1 to 4,294,967,295.
category *category-name*	Category name according to one of the keywords listed in Table 1.
network *network-prefix*	Optional. Source or destination IP address to be included in the criteria. Destination IP address when the traffic direction is from subscriber to Internet; source IP address when the traffic direction is from Internet to subscriber.
prefix-length	Optional. Number of prefix bits. Range: 0 to 32.
any	Optional. Indicates that IP traffic from all IP addresses is to be included in the criteria.
class *class-name*	Policy-based class name.

1.5.3 Default

None

1.5.4 Usage Guidelines

Creates an ACL statement to allow packets that meet the specified criteria. If **seq** *sequence-number* is not specified, the system assigns a sequence number.

Table 1 lists the valid keyword substitutions for the *category-name* argument.

Table 1 Valid Keyword Substitutions for the category-name Argument

Keyword	Definition
`all`	All categories.
`file-transfer`	File transfer applications.
`gaming`	Gaming applications.
`instant-messaging`	Instant messaging applications.
`p2p`	All P2P applications.
`streaming`	Audio or video streaming applications.

Keyword	Definition
`transport`	Transport applications.
`voip`	Voice over IP applications.

1.5.5 Examples

```
[local]Redback(dpi-acl)#seq 20 category streaming network 1.1.1.0/24 class c1
[local]Redback(dpi-acl)#category gaming network 4.1.1.0/24 class c2
```

1.6 class

`class` ***`class-name`***

`no class` ***`class-name`***

1.6.1 Command Mode

DPI action configuration

1.6.2 Syntax Description

`class-name`	Class name for a class of traffic to which the policy applies an action.

1.6.3 Default

None

1.6.4 Usage Guidelines

Creates a class entry that defines actions applied to traffic mapped to a class. Allows different QoS policies to be applied to different sets (classes) of flows that are defined in the applied policy Access Control List (ACL).

If the ***`class-name`*** argument referenced by an ACL rule matches the class name in an action policy, the classified traffic is processed according to the class definition. If a rule for the ***`class-name`*** argument is not specified in the ACL policy, the class-based policy considers the class to be dormant and takes no action. If a rule for the ***`class-name`*** argument is specified in the ACL, but you do not include the class in the action policy (using this command), the SmartEdge® OS considers those packets to be in the default class.

1.6.5 Examples

```
[local]Redback(config-dpi-action)#class c0
```

1.7 clear dpi card traffic-management statistics

clear dpi card ***slot/port*** **traffic-management statistics**

1.7.1 Command Mode

Eec

1.7.2 Syntax Description

slot	Chassis slot number for a particular ASE card.
asp-id	The ID of the ASP on the ASE card: 1 or 2.

1.7.3 Usage Guidelines

Clears all peak counters and all packet/byte counters.

1.7.4 Examples

```
[local]Redback#clear dpi card 2/1 traffic-management statistics
```

1.8 clear dpi circuit traffic-management sessions

clear dpi circuit {**agent-circuit-id** ***agent-circuit-id*** | **agent -remote-id** ***agent-remote-id*** | ***slot/port***[**:** ***chan-num***[**:** ***sub-chan-num***] ***circuit-id*** | **username** ***subscriber***} **traffic-management sessions**

1.8.1 Command Mode

Exec

1.8.2 Syntax Description

agent-circuit-id *agent-circuit-id*
Subscriber session identifier, where the *agent-circuit-id* argument is the value of the agent circuit ID in a subscriber record. Enter the *agent-circuit-id* argument as a structured subscriber username in the form subscriber@context.

agent-remote-id *agent-remote-id*
Subscriber session identifier, where the *agent-remote-id* argument is the value of the agent remote ID in a subscriber record. Enter the *agent-remote-id* argument as a structured subscriber username in the form subscriber@context.

slot
Chassis slot number for a particular card.

port
Port number on the specified card.

circuit-id
Subscriber session identifier. See Table 2 for information about the *circuit-id* argument.

username *subscriber*
Subscriber session identifier. Enter the subscriber argument as a structured subscriber username in the form subscriber@context.

1.8.3 Usage Guidelines

Clears all the traffic management sessions for the specified subscriber.

The *circuit-id* argument represents the following keywords and arguments; see Table 2.

clips [*clips-session*] | **pppoe** [*pppoe-session*] | **vlan-id** *vlan-id* [**pppoe** [*pppoe-session*] | **clips** [*clips-session*]] | **vpi-vci** *vpi vci* [**pppoe** [*pppoe-session*] | **clips** [*clips-session*]]

Table 2 Building Blocks of the circuit-id Argument

Construct	Description
clips *clips-session*	A filter that limits the command to a specified CLIPS circuit on a port, channel, 802.1Q PVC, or ATM PVC. If the CLIPS circuit is on an 802.1Q or ATM PVC, also specify the circuit identifier for the 802.1Q or ATM PVC. If the session is not specified, the command applies to all CLIPS sessions in the context. The range of values for the clips-session argument is 1 to 262,144.

Construct	Description
`pppoe` *`pppoe-session`*	A filter that limits the command to a specified PPPoE session. If the *`pppoe-session`* argument is not specified, the command applies to all PPPoE sessions in the context.
`vlan-id` *`vlan-id`*	A filter that limits the command to a specified virtual LAN (VLAN) 802.1Q tunnel or PVC. The *`vlan-id`* argument is one of the following constructs: • `vlan-id` *`pvc-vlan-id`* — VLAN tag value of a PVC that is not within an 802.1Q tunnel. • `vlan-id` *`pvc-vlan-id tunl-vlan-id`* — VLAN tag value of an 802.1Q tunnel. • `vlan-id` *`pvc-vlan-id tunl-vlan-id`*`:`*`pvc-vlan-id`* — VLAN tag value of an 802.1Q tunnel followed by the VLAN tag value for the PVC within the tunnel. If you specify the VLAN tag value for an 802.1Q tunnel, this command clears subscriber sessions on all the PVCs within the tunnel. The range of values for either VLAN tag value is 1 to 4,095.
`vpi-vci` *`vpi vci`*	A filter that limits the command to a specified ATM PVC. The ATM PVC is specified by the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI). The range of values is 0 to 255 and 1 to 65,534, respectively.

1.8.4 Examples

```
[local]Redback#clear dpi circuit username joe@local traffic-management sessions
```

1.9 clear dpi circuit traffic-management statistics

`clear dpi circuit` {**`agent-circuit-id`** *`agent-circuit-id`* | **`agent-remote-id`** *`agent-remote-id`* | *`slot`*/*`port`*[:*`chan-num`*[:*`sub-chan-num`*] *`circuit-id`* | **`username`** *`subscriber`*} **`traffic-management statistics`**

1.9.1 Command Mode

Exec

1.9.2 Syntax Description

agent-circuit-id *agent-circuit-id*	Subscriber session identifier, where the *agent-circuit-id* argument is the value of the agent circuit ID in a subscriber record. Enter the *agent-circuit-id* argument as a structured subscriber username in the form subscriber@context.
agent-remote-id *agent-remote-id*	Subscriber session identifier, where the *agent-remote-id* argument is the value of the agent remote ID in a subscriber record. Enter the *agent-remote-id* argument as a structured subscriber username in the form subscriber@context.
slot	Chassis slot number for a particular card.
port	Port number on the specified card.
circuit-id	Subscriber session identifier. See Table 2 for information about the *circuit-id* argument.
username *subscriber*	Subscriber session identifier. Enter the subscriber argument as a structured subscriber username in the form subscriber@context.

1.9.3 Usage Guidelines

Clears all peak counters and all packet/byte counters for the specified subscriber.

1.9.4 Examples

```
[local]Redback#clear dpi circuit username joe@local traffic-management statistics
```

1.10 conform mark dscp

conform mark dscp *dscp-class*

no conform mark dscp

1.10.1 Command Mode

DPI QoS profile rate configuration

1.10.2 Syntax Description

dscp-class — Priority with which packets conforming to the rate are marked. Values can be:

- An integer from 0 to 63.
- One of the keywords listed in Table 3.

1.10.3 Default

No action is taken on packets that conform to the configured rate.

1.10.4 Usage Guidelines

Marks packets that conform to the configured Quality of Service (QoS) rate with a Differentiated Services Code Point (DSCP) value.

You can configure the rate using the **rate** command. Only one mark instruction can be in effect at a time. To change the mark instruction, enter the **conform mark dscp** command, specifying a new value for the *dscp-class* argument, which supersedes the one previously configured.

Table 3 lists the keywords for the *dscp-class* argument.

Table 3 DSCP Class Keywords

DSCP Class	Keyword	DSCP Class	Keyword
Assured Forwarding (AF) Class 1/Drop precedence 1	**af11**	Class Selector 0 (same as default forwarding)	cs0 (same as **df**)
AF Class 1/Drop precedence 2	**af12**	Class Selector 1	cs1
AF Class 1/Drop precedence 3	**af13**	Class Selector 2	cs2
AF Class 2/Drop precedence 1	**af21**	Class Selector 3	cs3
AF Class 2/Drop precedence 2	**af22**	Class Selector 4	cs4
AF Class 2/Drop precedence 3	**af23**	Class Selector 5	cs5
AF Class 3/Drop precedence 1	**af31**	Class Selector 6	cs6

DSCP Class	Keyword	DSCP Class	Keyword
AF Class 3/Drop precedence 2	`af32`	Class Selector 7	`cs7`
AF Class 3/Drop precedence 3	`af33`	Default Forwarding (same as Class Selector 0)	`df` (same as `cs0`)
AF Class 4/Drop precedence 1	`af41`	Expedited Forwarding	`ef`
AF Class 4/Drop precedence 2	`af42`		
AF Class 4/Drop precedence 3	`af43`		

For more information about DSCP values, see RFC 2474, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*.

Caution!

Risk of packet reordering. Packets can be reordered into a different major DSCP class. To reduce the risk, ensure that the marking of conforming packets and exceeding packets differ only within a major DSCP class. Major DSCP classes are identified by the Class Selector code, and include CS0=DF, CS1=AF11, AF12, AF13, CS2=AF21, AF22, AF23, CS3=AF31, AF32, AF33, CS4=AF41, AF42, AF43, and CS5=EF. For example, if you mark conforming packets with AF11 and you want to avoid reordering, mark exceeding packets with AF11, AF12, or AF13 only.

1.10.5 Examples

The following example shows how to configure the DPI, `qos_prof_01`, to mark all packets that conform to the configured rate with a DSCP value representing a high priority of expedited forwarding (ef):

```
[local]Redback(config)#dpi qos profile qos_prof_01
[local]Redback(dpi-qos)#rate 64 burst 3000
[local]Redback(dpi-qos-rate)#conform mark dscp ef
```

1.11 conform mark precedence

`conform mark precedence` ***`prec-value`***

`no conform mark precedence`

1.11.1 Command Mode

DPI QoS profile rate configuration

1.11.2 Syntax Description

`prec-value`	Drop precedence value. Range: 1 to 3.

1.11.3 Default

No action is taken on packets that conform to the configured rate.

1.11.4 Usage Guidelines

Marks packets that conform to the configured QoS rate with a drop precedence value corresponding to the Assured Forwarding (AF) class of the packet.

You configure the QoS rate by using the **`rate`** command.

In general, the level of forwarding assurance of an IP packet is based on:

- Resources allocated to the AF class to which the packet belongs
- Current load of the AF class, and, in case of congestion within the class
- Drop precedence of the packet. In case of congestion, the drop precedence of a packet determines the relative importance of the packet within the AF Differentiated Services Code Point (DSCP) class

Packets with a lower drop precedence value are preferred and protected from being lost, and packets with a higher drop precedence value are discarded.

With AF classes AF1 (AF11, AF12, AF13), AF2 (AF21, AF22, AF23), AF3 (AF31, AF32, AF33), and AF4 (AF41, AF42, AF43), the second integer represents a drop precedence value. Table 4 shows how the AF drop precedence value of an incoming packet is changed when it exits the SmartEdge router after being tagged with a new drop precedence. (See also RFC 2597, *Assured Forwarding PHB Group*.)

Table 4 Drop Precedence Value

DSCP Value of an Incoming Packet	Packet is Tagged with a Drop Precedence Value	DSCP Value of the Outgoing Packet
AF11, AF12, AF13	1	AF11
AF21, AF22, AF23		AF21
AF31, AF32, AF33		AF31
AF41, AF42, AF43		AF41
AF11, AF12, AF13	2	AF12
AF21, AF22, AF23		AF22
AF31, AF32, AF33		AF32
AF41, AF42, AF43		AF42
AF11, AF12, AF13	3	AF13
AF21, AF22, AF23		AF23
AF31, AF32, AF33		AF33
AF41, AF42, AF43		AF43

Only one mark instruction can be in effect at a time. To change the mark instruction, enter the **conform mark precedence** command, specifying a new value for the ***prec-value*** argument, which supersedes the one previously configured.

1.11.5 Examples

The following example shows how to configure the DPI QoS profile qos_prof_01 to mark all packets that conform to the configured rate with a drop precedence value of 1 and drops all packets that exceed the rate:

```
[local]Redback(config)#dpi qos profile qos_prof_01
[local]Redback(dpi-qos)#rate 64 burst 3000
[local]Redback(dpi-qos-rate)#conform mark precedence 1
```

1.12 conform mark priority

```
conform mark priority {group-num | ignore} [{drop-precedence
{group-num | ignore} | af-drop drop-value}]
```

```
no conform mark priority
```

1.12.1 Command Mode

DPI QoS profile rate configuration

1.12.2 Syntax Description

group-num	Packet descriptor (PD) QoS priority group number. The range of values is 0 to 7. The scale used by this command for packet priority, from 0 (highest priority) to 7 (lowest priority), is the relative inverse of the scale used by QoS classification map and classification definition commands.
ignore	Specifies that the internal PD QoS priority or drop-precedence value is not modified.
drop-precedence	Optional. Enables you to specify a setting for either the drop-precedence portion of the PD QoS field or the priority group, or both.
af-drop *drop-value*	Optional. Target internal drop-precedence value in two-bit format; leaves the least significant bit unmodified. The range of values is 1 to 3.

1.12.3 Default

No action is taken on packets that conform to the configured rate. Default mapping of priority groups to queues is listed in Table 5.

1.12.4 Usage Guidelines

Marks packets that conform to the configured QoS rate with a PD QoS priority group number, a drop-precedence value, or both, while leaving the packet's IP header DSCP value unmodified. To configure the QoS rate **rate**, enter the **rate** command.

A PD QoS priority group is an internal value used by the SmartEdge OS to determine into which egress queue the inbound packet is placed. The Type of Service (ToS) value, DSCP value, and Multiprotocol Label Switching (MPLS) experimental (EXP) bits are unchanged by this command. The actual queue number depends on the number of queues configured on the egress circuit.

The SmartEdge OS uses the factory preset or default mapping of a PD QoS priority group to queue, according to the number of queues configured on a circuit; see Table 5.

Table 5 Default Mapping of Priority Groups

PD QoS priority group	8 Queues	4 Queues	2 Queues	1 Queue
0	queue 0	queue 0	queue 0	queue 0
1	queue 1	queue 1	queue 1	queue 0
2	queue 2	queue 1	queue 1	queue 0
3	queue 3	queue 2	queue 1	queue 0
4	queue 4	queue 2	queue 1	queue 0
5	queue 5	queue 2	queue 1	queue 0
6	queue 6	queue 2	queue 1	queue 0
7	queue 7	queue 3	queue 1	queue 0

Only one mark instruction can be in effect at a time. To change the mark instruction, enter the **conform mark priority** command, specifying a new value for the ***group-num*** argument. This supersedes the value previously configured.

1.12.5 Examples

The following example shows how to configure the policy to mark all packets that conform to the configured rate with PD QoS priority group number 3 and drops all packets that exceed the rate:

```
[local]Redback(config)#dpi qos profile qos_prof_01
[local]Redback(dpi-qos)#rate 64 burst 3000
[local]Redback(dpi-qos-rate)#conform mark priority 3
```

1.13 debug dpi card traffic-management

debug dpi card ***slot/asp-id*** **traffic-management** ***message-type*** **trace** {**buffer** | **console** | **external**} [**level** ***level***]

1.13.1 Command Mode

Exec

1.13.2 Syntax Description

`slot` Chassis slot number for a particular ASE card.

`asp-id` The ID of the ASP on the ASE card: 1 or 2.

`message-type` Type of messages to debug, where ***`message-type`*** is one of the following:

- **`all`**
- **`classification`**— Packet classification messages
- **`config`**—Configuration messages
- **`dispatcher`**—Dispatcher messages
- **`forwarding`**—Packet forwarding messages
- **`inspection`**—Packet inspection messages
- **`packet`**—Packet processing messages
- **`qos`**—QoS processing messages
- **`signature`**—Signature matching messages
- **`statistics`**—Statistics collection messages

`trace` Enables trace and sends debug information to buffer, console, or external.

`buffer` Configures debug information for the circular buffer on the ASE.

`console` Configures debug information for the console.

`external`	Configures debug information for the external log server.
`level` *`level`*	Specifies the debug logging level, where *`level`* is one of the following (in descending severity order): • **`emergency`**—Only emergency events. • **`alert`**—Alert and more severe events. • **`critical`**—Critical and more severe events. • **`error`**—Error and more severe events. • **`warning`**—Warning and more severe events. • **`notice`**—Notice and more severe events. • **`informational`**—Informational and more severe events. • **`debug`**–All events, including debug events. • **`all`**

1.13.3 Usage Guidelines

Enables the generation of debug messages for the traffic management application on a specific ASE card.

Separate levels and message-types can be configured for the console and an external log server.

Caution!

Risk of performance loss. Enabling the generation of debug messages can severely affect system performance. To reduce the risk, exercise caution when enabling the generation of debug messages on a production system.

1.13.4 Examples

```
[local]Redback#debug dpi card 1 / 2 traffic-management all log console level alert
```

1.14 default-class

`default-class` *`class-name`*

`no default-class`

1.14.1 Command Mode

DPI action configuration

DPI access control list configuration

1.14.2 Syntax Description

class-name	Name of the default class.

1.14.3 Default

No default class is configured.

1.14.4 Usage Guidelines

Specifies a class to use to map all traffic that is not otherwise classified. The default class defined in the DPI ACL policy is used to map all traffic that was not classified into one of the classes defined in the DPI ACL policy. The default class defined in the DPI action policy is used to map all traffic assigned to a class that is not defined in the action policy.

1.14.5 Examples

```
[local]Redback(config-dpi-action)#default-class default
```

1.15 dpi access-list

dpi access-list *acl-name*

no dpi access-list *acl-name*

1.15.1 Command Mode

Global configuration

1.15.2 Syntax Description

acl-name	DPI ACL policy name; must be unique.

1.15.3 Default

No DPI ACL policy is configured.

1.15.4 Usage Guidelines

Creates or selects a DPI ACL policy and enters DPI access control list configuration mode.

1.15.5 Examples

```
[local]Redback(config)#dpi access-list b1
```

1.16 dpi qos profile

dpi qos profile ***profile-name*** [**policing** | **metering**]

no dpi qos profile ***profile-name*** [**policing** | **metering**]

1.16.1 Command Mode

Global configuration

1.16.2 Syntax Description

profile-name	Name of the QoS profile.
policing	Optional. Specifies a QoS profile used to rate-limit traffic in the ingress direction.
metering	Optional. Specifies a QoS profile used to rate-limit traffic in the egress direction.

1.16.3 Default

No DPI is configured.

1.16.4 Usage Guidelines

Creates or selects a DPI QoS profile and enters DPI QoS profile configuration mode. If policing or metering is not specified, a bidirectional QoS profile is implied.

1.16.5 Examples

```
[local]Redback(config)#dpi qos profile q1
```

```
[local]Redback(config)#dpi qos profile q2 policing
```

1.17 dpi traffic-management action policy

dpi traffic-management action policy ***name*** [**aggregate**]

no dpi traffic-management action policy ***name*** [**aggregate**]

1.17.1 Command Mode

Global configuration

1.17.2 Syntax Description

name	Name of the DPI traffic management action policy.
aggregate	Optional. Specifies that the DPI traffic management action policy is used for per class per subscriber group or per class per SmartEdge router level traffic management configuration.

1.17.3 Default

No DPI traffic management action policy is configured.

1.17.4 Usage Guidelines

Creates or selects a DPI traffic management action policy and enters DPI action configuration mode.

1.17.5 Examples

```
[local]Redback(config)#dpi traffic-management action policy a1
```

1.18 dpi traffic-management group

dpi traffic-management group ***group-name***

no dpi traffic-management group ***group-name***

1.18.1 Command Mode

- Global configuration
- Subscriber configuration

1.18.2 Syntax Description

group-name	Name of the DPI traffic management group.

1.18.3 Default

No DPI traffic management group is configured.

1.18.4 Usage Guidelines

If used in global configuration mode, creates a DPI traffic management group and enters DPI traffic management group configuration mode. When used in subscriber configuration mode, associates a subscriber with the DPI traffic management group.

1.18.5 Examples

```
[local]Redback(config)#dpi traffic-management group g1

[local]Redback(config)#context local
[local]Redback(config-ctx)#subscriber joe
[local]Redback(config-sub)#dpi traffic-management group g1
```

1.19 dpi traffic-management maximum sessions

dpi traffic-management maximum sessions ***max-sessions*** [**exceed class** ***class-name***]

no dpi traffic-management maximum sessions ***max-sessions*** [**exceed class** ***class-name***]

1.19.1 Command Mode

Global configuration

1.19.2 Syntax Description

max-sessions	Maximum number of allowed sessions per subscriber. Range: 16 to 4096.
exceed class *class-name*	Optional. Specifies the action policy class used to map all traffic associated with subscriber sessions that exceed the allowed maximum value.

1.19.3 Default

Session limiting is disabled by default. When session limiting is enabled, the default action is to drop all packets associated with sessions that exceed the allowed maximum value.

1.19.4 Usage Guidelines

Enables subscriber session limiting and specifies the maximum number of allowed sessions per subscriber. In addition, specifies whether packets associated with sessions that exceed the session limit are dropped, or mapped to an action policy class. The **no** form of this command disables subscriber session limiting.

1.19.5 Examples

```
[local]Redback(config)#dpi traffic-management maximum sessions 300 exceed class cl_01
```

1.20 dpi traffic-management policy

dpi traffic-management policy {**default** | *policy-name*} [**aggregate**]

no dpi traffic-management policy {**default** | *policy-name*} [**aggregate**]

no dpi traffic-management policy

1.20.1 Command Mode

- Global configuration
- Subscriber configuration

1.20.2 Syntax Description

`default`	Global default traffic management policy applied to traffic when the specified policy is not configured. Only applies in global configuration mode.
`policy-name`	Name of the DPI traffic management policy.
`aggregate`	Optional. Specifies that the DPI traffic management policy is used for per class per subscriber group or per class per SmartEdge router level traffic management.

1.20.3 Default

No DPI traffic management policy is configured.

1.20.4 Usage Guidelines

In global configuration mode, creates or selects a DPI traffic management policy and enters DPI policy configuration mode.

In subscriber configuration mode, applies a DPI traffic management policy to a subscriber, default subscriber, or subscriber profile.

1.20.5 Examples

The following examples shows how to create the DPI traffic management policy `p1`.

```
(config)#dpi traffic-management policy p1
```

The following example shows how to apply the DPI traffic management policy `p1` to subscriber `joe`.

```
[isp1]Redback(config-ctx)#subscriber name joe
[isp1]Redback(config-sub)#dpi traffic-management policy p1
```

1.21 dpi traffic-management resource-failure-action

`dpi traffic-management resource-failure-action drop`

`no dpi traffic-management resource-failure-action`

1.21.1 Command Mode

Global configuration

1.21.2 Syntax Description

`drop`	Drop application traffic in the event of a resource failure.

1.21.3 Default

Application traffic bypasses the failed ASP and continues to forward subscriber traffic.

1.21.4 Usage Guidelines

Drops application traffic when a resource fails. Use the no form of the command to bypass the ASP and continue to forward subscriber traffic in the event of a resource failure.

1.21.5 Examples

```
[local]Redback(config)#dpi traffic-management resource-failure-action drop
```

1.22 dpi traffic-management signature-file

`dpi traffic-management signature-file` ***`sig-filename`***

`no dpi traffic-management signature-file`

1.22.1 Command Mode

Global configuration

1.22.2 Syntax Description

`sig-filename`	Signature-file name or path and filename. To specify a file in the secure directory in /flash (the default signature-file directory), use only the filename. To specify a signature file in another location, use a path and filename.

1.22.3 Default

The SmartEdge uses the built-in signature file.

1.22.4 Usage Guidelines

Use the **dpi traffic-management signature-file** command to configure a signature file to use for DPI traffic-management. You cannot configure a signature-file, if it does not support the rules in an existing DPI access-list.

Use the **no** form of the command to use the default (built-in) signature file.

Signature-file names are in the format, ***App-Name-Major-Minor*.sdf**

Where:

App-Name is the Application name, such as P2P.

Major is the DPI Engine Major Number; the value must be equal to or less than the current installed DPI Engine version.

Minor is the signature-file release number.

sdf is the file extension, which stands for Signature Definition File.

For example, `P2P-3-1.sdf` is a signature file about P2P applications for DPI engine 3, release 1.

1.22.5 Examples

```
[local]Redback(config)#dpi traffic-management signature-file p2p-3-1.sdf
```

1.23 dpi traffic-management statistics

dpi traffic-management statistics [**interim-interval** ***minutes***]

default dpi traffic-management statistics

1.23.1 Command Mode

Global configuration

1.23.2 Syntax Description

interim-interval ***minutes***	Optional. Frequency with which reporting statistics are sent to an external server. Range: 15 to 4,294,967,295; default: 15.

1.23.3 Default

Statistics reporting is disabled by default. When statistics reporting is enabled, the default interim-interval is 15 minutes.

1.23.4 Usage Guidelines

Configures the frequency to send statistics to an external server.

1.23.5 Examples

```
[local]Redback(config)#dpi traffic-management statistics interim-interval 30
```

1.24 dpi traffic-management subscriber

dpi traffic-management subscriber load-balancing intra-asp adaptive

no dpi traffic-management subscriber load-balancing intra-asp adaptive

1.24.1 Command Mode

Global configuration

1.24.2 Default

Round-robin subscriber distribution is enabled by default.

1.24.3 Usage Guidelines

With **adaptive** subscriber allocation, subscribers are distributed based on adaptive instance load computation. The weighted average packet latency reflects current system load conditions. A new subscriber is allocated to the instance with the lightest load. Given equal loads, the new subscriber is assigned to the instance with the least subscriber count.

Use the **no** form of this command to use **round-robin** subscriber allocation.

1.25 exceed drop

exceed drop

no exceed drop

1.25.1 Command Mode

DPI QoS profile rate configuration

1.25.2 Default

All packets exceeding the QoS rate and burst tolerance are dropped.

1.25.3 Usage Guidelines

Specifies how packets are dropped when the traffic rate exceeds the QoS rate and burst tolerance.

Configure the traffic rate and burst tolerance with the **rate** command.

1.25.4 Examples

The following example shows how to drop packets that exceed the traffic rate and burst tolerance:

```
[local]Redback(config)#dpi qos profile qos_prof_01
[local]Redback(dpi-qos)#rate 64 burst 3000
[local]Redback(dpi-qos-rate)#exceed drop
```

1.26 exceed mark dscp

exceed mark dscp ***dscp-class***

no exceed mark dscp

1.26.1 Command Mode

DPI QoS profile rate configuration

1.26.2 Syntax Description

dscp-class	Priority with which packets exceeding the rate are marked. Values can be: • An integer from 0 to 63. • One of the keywords listed in Table 3.

1.26.3 Default

Packets that exceed the configured rate are dropped.

1.26.4 Usage Guidelines

Marks packets that exceed the configured QoS rate and burst tolerance with a DSCP value.

To configure the rate, enter the **rate** command. Only one mark instruction can be in effect at a time. To change the mark instruction, enter the **exceed mark dscp** command, specifying a new value for the *dscp-class* argument. This supersedes the one previously configured.

Table 3 lists the keywords for the *dscp-class* argument.

For more information about DSCP values, see RFC 2474, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*.

Caution!

Risk of packet reordering. Packets can be reordered into a different major DSCP class. To reduce the risk, ensure that the marking of conforming packets and exceeding packets differ only within a major DSCP class. Major DSCP classes are identified by the Class Selector code, and include CS0=DF, CS1=AF11, AF12, AF13, CS2=AF21, AF22, AF23, CS3=AF31, AF32, AF33, CS4=AF41, AF42, AF43, and CS5=EF. For example, if you mark conforming packets with AF11 and you want to avoid reordering, mark exceeding packets with AF11, AF12, or AF13 only.

Use the **no** or **default** form of this command to return to the default behavior of not taking any action on packets that conform to the configured rate.

1.26.5 Examples

The following example shows how to configure the DPI, `qos_prof_01`, to mark all packets that exceed the configured rate with a DSCP value representing a high priority of expedited forwarding (ef):

```
[local]Redback(config)#dpi qos profile qos_prof_01
[local]Redback(dpi-qos)#rate 64 burst 3000
[local]Redback(dpi-qos-rate)#exceed mark dscp ef
```

1.27 exceed mark precedence

exceed mark precedence*prec-value*

no exceed

1.27.1 Command Mode

DPI QoS profile rate configuration

1.27.2 Syntax Description

prec-value	Drop precedence bits value. Range: 1 to 3.

1.27.3 Default

Packets that exceed the configured rate are dropped.

1.27.4 Usage Guidelines

Marks packets that exceed the configured QoS rate with a drop precedence value corresponding to the AF class of the packet.

To configure the rate, enter the **rate** command.

In general, the level of forwarding assurance of an IP packet is based on: (1) the resources allocated to the AF class to which the packet belongs, (2) the current load of the AF class, and, in case of congestion within the class, (3) the drop precedence of the packet. In case of congestion, the drop precedence of a packet determines the relative importance of the packet within the AF class. Packets with a lower drop precedence value are preferred and protected from being lost, and packets with a higher drop precedence value are discarded.

With AF classes AF1 (AF11, AF12, AF13), AF2 (AF21, AF22, AF23), AF3 (AF31, AF32, AF33), and AF4 (AF41, AF42, AF43), the second integer represents a drop precedence value. Table 4 shows how the AF drop precedence value of an incoming packet is changed when it exits the SmartEdge router after being tagged with a new drop precedence. (See also RFC 2597, *Assured Forwarding PHB Group*.)

Only one mark instruction can be in effect at a time. To change the mark instruction, enter the **exceed mark precedence** command, specifying a new value for the *prec-value* argument, which supersedes the one previously configured.

Use the no or default form of this command to return to the default behavior of dropping packets that exceed the rate.

1.27.5 Examples

The following example shows how to configure the DPI, `qos_prof_01`, to mark all packets that exceed the configured rate with an IP precedence value of 3.

```
[local]Redback(config)#dpi qos profile qos_prof_01
[local]Redback(dpi-qos)#rate 64 burst 3000
[local]Redback(dpi-qos-rate)#exceed mark precedence 3
```

1.28 exceed mark priority

exceed mark priority {*group-num* | **ignore**} [{**drop-precedence** {*group-num* | **ignore**} | **af-drop** *drop-value*}]

no exceed mark priority

1.28.1 Command Mode

DPI QoS profile rate configuration

1.28.2 Syntax Description

group-num

Packet descriptor (PD) QoS priority group number. The range of values is 0 to 7.

The scale used by this command for packet priority, from 0 (highest priority) to 7 (lowest priority), is the relative inverse of the scale used by QoS classification map and classification definition commands.

ignore

Specifies that the internal PD priority or drop-precedence value is not modified.

drop-precedence

Optional. Enables you to specify a setting for either the drop-precedence portion of the PD QoS field or the priority group, or both.

af-drop *drop-value*

Optional. Target internal drop-precedence value in two-bit format; leaves the least significant bit unmodified. Range: 1 to 3.

1.28.3 Default

Packets that exceed the configured rate are dropped.

1.28.4 Usage Guidelines

Marks packets that exceed the QoS rate and burst tolerance with a PD QoS priority group number, a drop-precedence value, or both, while leaving the packet's IP header DSCP value unmodified.

To configure the QoS rate, enter the **rate** command.

A PD QoS priority group is an internal value used by the SmartEdge OS to determine into which egress queue the inbound packet is placed. The ToS value, DSCP value, and MPLS EXP bits are unchanged by this command. The actual queue number depends on the number of queues configured on the circuit. For more information, see the **num-queues** command in Reference [3].

The SmartEdge OS uses the factory preset or default mapping of a PD QoS priority group to queue, according to the number of queues configured on a circuit; see Table 5.

Only one mark instruction can be in effect at a time. To change the mark instruction, enter the **exceed mark priority** command, specifying a new value for the ***group-num*** argument. This supersedes the value previously configured.

Caution!

Risk of overriding configurations. The SmartEdge OS checks for and applies marking in a specific order. To reduce the risk, remember the following guidelines: Circuit-based marking overrides class-based marking; Border Gateway Protocol (BGP) destination-based marking, through route maps, overrides both circuit-based and class-based marking.

Note: By default, the SmartEdge OS assigns a PD QoS priority group to each egress queue, according to the number of queues configured on a circuit. You can override the default mapping of packets into egress queues by creating a customized queue priority map using the **qos queue-map** command (in global configuration mode).

Use the **no** or **default** form of this command to return to the default behavior.

1.28.5 Examples

The following example shows how to configure the policy to mark all packets that exceed the configured rate with PD QoS priority group number 3:

```
[local]Redback(config)#dpi qos profile qos_prof_01
[local]Redback(dpi-qos)#rate 64 burst 3000
[local]Redback(dpi-qos-rate)#exceed mark priority 3
```

1.29 log detection

`log detection`

`no log detection`

1.29.1 Command Mode

DPI action class configuration

1.29.2 Default

Log detection is not enabled by default.

1.29.3 Usage Guidelines

Generates a log entry when application or protocol traffic is detected in traffic mapped to the class. Enabling logging may impact performance.

1.29.4 Examples

```
[local]Redback(config-dpi-action-class)#log detection
```

1.30 mark dscp

`mark dscp` ***`dscp-class`***

`no mark dscp` ***`dscp-class`***

1.30.1 Command Mode

DPI QoS profile configuration

1.30.2 Syntax Description

`dscp-class` Priority with which packets are marked. Values can be:

- An integer from 0 to 63.
- One of the keywords listed in Table 3.

1.30.3 Default

Packets are not assigned a DSCP priority.

1.30.4 Usage Guidelines

Assigns a QoS DSCP priority to packets.

Caution!

Risk of overriding configurations. The SmartEdge OS checks for and applies marking in a specific order. To reduce the risk, remember the following guidelines: Circuit-based marking overrides class-based marking; Border Gateway Protocol (BGP) destination-based marking, through route maps, overrides both circuit-based and class-based marking.

For more information about DSCP values, see RFC 2474, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*.

1.30.5 Examples

The following example shows how to configure the DPI `qos_prof_02`, to mark all packets as high-priority packets:

```
[local]Redback(config)#dpi qos profile qos_prof_02
[local]Redback(dpi-qos)#mark dscp ef
```

1.31 mark precedence

`mark precedence` ***`prec-value`***

`no mark precedence` ***`prec-value`***

1.31.1 Command Mode

DPI QoS profile configuration

1.31.2 Syntax Description

`prec-value`	Drop precedence value. Range: 1 to 3.

1.31.3 Default

Packets are not marked with an explicit drop precedence value.

1.31.4 Usage Guidelines

Assigns a QoS drop precedence value to packets corresponding to the AF class of the packets.

In general, the level of forwarding assurance of an IP packet is based on:

- Resources allocated to the AF class to which the packet belongs
- Current load of the AF class, and, in case of congestion within the class
- Drop precedence of the packet. In case of congestion, the drop precedence of a packet determines the relative importance of the packet within the AF DSCP class

Packets with a lower drop precedence value are preferred and protected from being lost, while packets with a higher drop precedence value are discarded.

For more information, see RFC 2597, *Assured Forwarding PHB Group*.

With AF classes AF1 (AF11, AF12, AF13), AF2 (AF21, AF22, AF23), AF3 (AF31, AF32, AF33), and AF4 (AF41, AF42, AF43), the second integer represents a drop precedence value. Table 4 shows how the AF drop precedence value of an incoming packet is changed when it exits the SmartEdge router after being tagged with a new drop precedence. (See also RFC 2597, *Assured Forwarding PHB Group*.)

Only one mark instruction can be in effect at a time. To change the mark instruction, enter the **mark precedence** command, specifying a new value for the ***prec-value*** argument, which supersedes the one previously configured.

1.31.5 Examples

The following example shows how to configure the DPI, qos_prof_02, to mark all packets as preferred packets.

```
[local]Redback(config)#dpi qos profile qos_prof_02
[local]Redback(dpi-qos)#mark precedence 1
```

1.32 mark priority

mark priority {***group-num*** | **ignore**} [{**drop-precedence** {***group-num*** | **ignore**} | **af-drop** ***drop-value***}]

no mark priority

1.32.1 Command Mode

DPI QoS profile configuration

1.32.2 Syntax Description

group-num	Packet descriptor (PD) QoS priority group number. Range: 0 to 7. The scale used by this command for packet priority, from 0 (highest priority) to 7 (lowest priority), is the relative inverse of the scale used by QoS classification map and classification definition commands.
ignore	Specifies that the internal PD QoS priority or drop-precedence value is not modified.
drop-precedence	Optional. Enables you to specify a setting for either the drop-precedence portion of the PD QoS field, or the priority group, or both.
af-drop ***drop-value***	Optional. Target internal drop-precedence value in two-bit format; leaves the least significant bit unmodified. Range: 1 to 3.

1.32.3 Default

The PD QoS values for a packet are not modified.

1.32.4 Usage Guidelines

Sets the internal Packet Descriptor (PD) QoS classification value for specified packets, while preserving the packet's IP header DSCP value.

A PD QoS priority group is an internal value used by the SmartEdge OS to determine into which egress queue the inbound packet is placed. The ToS value, DSCP value, and MPLS EXP bits are unchanged by this command. The actual queue number depends on the number of queues configured on the egress circuit. For more information, see the **num-queues** command in Reference [3].

The SmartEdge OS uses the factory preset or default mapping of a PD QoS priority group to queue, according to the number of queues configured on a circuit; see Table 5.

Only one mark instruction can be in effect at a time. To change the mark instruction, enter the **mark priority** command, specifying a new value for the ***group-num*** argument. This supersedes the value previously configured.

Note: By default, the SmartEdge OS assigns a PD QoS priority group to each egress queue, according to the number of queues configured on a circuit. You can override the default mapping of packets into egress queues by creating a customized queue priority map using the **qos queue-map** command (in global configuration mode).

If neither the **drop-precedence** nor the **af-drop** keyword is specified, the priority bits are set to the specified value and the drop-precedence bits are cleared.

1.32.5 Examples

The following example shows how to configure the DPI, qos_prof_02, to mark all packets as high-priority packets:

```
[local]Redback(config)#dpi qos profile qos_prof_01
[local]Redback(dpi-qos)#mark priority 2
```

1.33 protocol

For UDP and TCP:

[**seq** *sequence-number*] **protocol** {**udp** | **tcp**} {**network** *network-prefix/prefix-length* | **any**} {**cond** *source-port* | **range** *source-start-port source-end-port* | **any**} {**cond** *dest-port* | **range** *dest-start-port dest-end-port* | **any**} **class** *class-name*

no seq *sequence-number*

For other protocols:

[**seq** *sequence-number*] **protocol** *protocol* {**network** *network-prefix/prefix-length* | **any**} **class** *class-name*

no seq *sequence-number*

1.33.1 Command Mode

DPI access control list configuration

1.33.2 Syntax Description

seq *sequence-number*	Optional. Sequence number for the statement. Range: 1 to 4,294,967,295.
tcp	Transmission Control Protocol.
udp	User Datagram Protocol.

protocol

Protocol name or number indicating a protocol as specified in RFC 1700, *Assigned Numbers*. Range: 0 to 255 or one of the keywords listed in Table 6.

network *network-prefix*

Source or destination IP address to be included in the criteria. Destination IP address when the traffic direction is from subscriber to Internet; source IP address when the traffic direction is from Internet to subscriber.

prefix-length

Optional. Number of prefix bits. Range: 0 to 32.

any

Optional. Indicates that IP traffic from all IP addresses or ports is to be included in the criteria.

cond

One of the following expressions:

- **gt**—greater than
- **lt**—less than
- **eq**—equal to
- **neq**—not equal to

source-port

Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) source port. This argument is only available if you specified TCP or UDP as the protocol. Range: 1 to 65,535 or one of the keywords listed in Table 7 and Table 8.

range *source-start-port source-end-port*

Beginning and ending TCP or UDP source ports that define a range of port numbers. A packet's port must fall within the specified range to match the criteria. This construct is only available if you specified TCP or UDP as the protocol. Range: 1 to 65,535 or one of the keywords listed in Table 7 and Table 8.

dest-port

TCP or UDP destination port. This argument is only available if you specified TCP or UDP as the protocol. Range: 1 to 65,535 or one of the keywords listed in Table 7 and Table 8.

range ***dest-start-port dest-end-port***	Beginning and ending TCP or UDP destination ports that define a range of port numbers. A packet's port must fall within the specified range to match the criteria. This construct is only available if you specified TCP or UDP as the protocol. Range: 1 to 65,535 or one of the keywords listed in Table 7 and Table 8.
class ***class-name***	Class name.

1.33.3 Default

None

1.33.4 Usage Guidelines

Creates an ACL statement to allow packets that meet the specified criteria. If **seq** ***sequence-number*** is not specified, the system assigns a sequence number.

The ***cond source-port*** and ***cond dest-port*** constructs are mutually exclusive with the **range** ***source-start-port source-end-port*** and **range** ***dest-start-port dest-end-port*** constructs.

Table 6 lists the valid keyword substitutions for the ***protocol*** argument.

Table 6 Valid Keyword Substitutions for the protocol Argument

Keyword	Definition
ahp	Authentication Header Protocol.
esp	Encapsulation Security Payload.
gre	Generic Routing Encapsulation.
icmp	Internet Control Message Protocol.
igmp	Internet Group Management Protocol.
ip	Any IP protocol.
ipinip	IP-in-IP tunneling.
ospf	Open Shortest Path First.
pcp	Payload Compression Protocol.
pim	Protocol Independent Multicast.

Table 7 lists the valid keyword substitutions for the ***source-port***, ***source-start-port***, ***source-end-port***, ***dest-port***, ***dest-start-port***, or ***dest-end-port*** argument when it is used to specify a TCP port.

Table 7 Valid Keyword Substitutions for the Port Argument (TCP Port)

Keyword	Definition	Corresponding Port Number
`bgp`	Border Gateway Protocol	179
`chargen`	Character generator	19
`cmd`	Remote commands (rcmd)	514
`daytime`	Daytime	13
`discard`	Discard	9
`domain`	Domain Name System	53
`echo`	Echo	7
`exec`	Exec (rsh)	512
`finger`	Finger	79
`ftp`	File Transfer Protocol	21
`ftp-data`	FTP data connections (used infrequently)	20
`gopher`	Gopher	70
`hostname`	Network Interface Card (NIC) hostname server	101
`ident`	Identification protocol	113
`irc`	Internet Relay Chat	194
`klogin`	Kerberos login	543
`kshell`	Kerberos Shell	544
`login`	Login (rlogin)	513
`lpd`	Printer service	515
`nntp`	Network News Transport Protocol	119
`pim-auto-rp`	Protocol Independent Multicast Auto-RP	496
`pop2`	Post Office Protocol Version 2	109
`pop3`	Post Office Protocol Version 3	110
`shell`	Remote command shell	514
`smtp`	Simple Mail Transport Protocol	25
`ssh`	Secure Shell	22
`sunrpc`	Sun Remote Procedure Call	111
`syslog`	System logger	514

Keyword	Definition	Corresponding Port Number
`tacacs`	Terminal Access Controller Access Control System	49
`talk`	Talk	517
`telnet`	Telnet	23
`time`	Time	37
`uucp`	UNIX-to-UNIX Copy Program	540
`whois`	Nickname	43
`www`	World Wide Web (HTTP)	80

Table 8 lists the valid keyword substitutions for the ***source-port***, ***source-start-port***, ***source-end-port***, ***dest-port***, ***dest-start-port***, or ***dest-end-port*** argument when it is used to specify a UDP port.

Table 8 Valid Keyword Substitutions for the port Argument (UDP Port)

Keyword	Definition	Corresponding Port Number
`biff`	Biff (Mail Notification, Comsat)	512
`bootpc`	Bootstrap Protocol client	68
`bootps`	Bootstrap Protocol server	67
`discard`	Discard	9
`dnsix`	DNSIX Security Protocol Auditing	195
`domain`	Domain Name System	53
`echo`	Echo	7
`isakmp`	Internet Security Association and Key Management Protocol (ISAKMP)	500
`mobile-ip`	Mobile IP Registration	434
`nameserver`	IEN116 Name Service (obsolete)	42
`netbios-dgm`	NetBIOS Datagram Service	138
`netbios-ns`	NetBIOS Name Service	137
`netbios-ss`	NetBIOS Session Service	139
`ntp`	Network Time Protocol	123
`pim-auto-rp`	Protocol Independent Multicast Auto-RP	496

Keyword	Definition	Corresponding Port Number
`rip`	Router Information Protocol	520
`snmp`	Simple Network Management Protocol	161
`snmptrap`	SNMP traps	162
`sunrpc`	Sun Remote Procedure Call	111
`syslog`	System logger	514
`tacacs`	Terminal Access Controller Access Control System	49
`talk`	Talk	517
`tfpt`	Trivial File Transfer Protocol	69
`time`	Time	37
`who`	Who Service (rwho)	513
`xdmcp`	X Display Manager Control Protocol	177

1.33.5 Examples

```
[local]Redback(dpi-acl)#seq 20 udp any eq echo class c5
[local]Redback(dpi-acl)#tcp any any any class c6
```

1.34 qos profile

qos profile ***profile-name*** **[policing | metering]**

no qos profile ***profile-name*** **[policing | metering]**

1.34.1 Command Mode

- DPI action class configuration
- DPI traffic-management policy configuration

1.34.2 Syntax Description

`profile-name`	Name of the QoS profile.
`policing`	Optional. Specifies a QoS profile used to rate-limit traffic in the ingress direction.
`metering`	Optional. Specifies a QoS profile used to rate-limit traffic in the egress direction.

1.34.3 Default

No QoS profile is configured.

1.34.4 Usage Guidelines

Creates or selects a QoS profile and enters DPI QoS profile configuration mode. One policing and one metering QoS profile can be applied to a single DPI action class or traffic management policy. Neither policing nor metering QoS profiles can be applied together with a bidirectional QoS profile. When used in DPI traffic-management policy configuration mode, applies traffic control actions to all traffic associated with a specified subscriber.

1.34.5 Examples

```
[local]Redback(config-dpi-action-class)#qos profile q1
```

```
[local]Redback(config-dpi-action-class)#qos profile q2 policing
```

```
[local]Redback(config-dpi-policy)#dpi qos profile sub_qos1
```

1.35 rate

`rate` *`kbps`* {**`burst`** *`bytes`* | **`time-burst`** *`msec`*}

1.35.1 Command Mode

DPI QoS profile configuration

1.35.2 Syntax Description

kbps	Rate in kilobits per second. Range: 5 to 1,000,000,000.
burst *bytes*	Burst tolerance in bytes. Range: 1 to 4,250,000,000.
time-burst *msec*	Burst tolerance in milliseconds. Range: 1 to 10000.

1.35.3 Default

Rate is calculated based on the default values for the *kbps*, *bytes*, and *msec* arguments.

1.35.4 Usage Guidelines

Sets the rate and burst tolerance for traffic on the subscriber record to which the QoS policy is attached.

Rate limits apply to an aggregate of inbound and outbound directions.

1.35.5 Examples

```
[local]Redback(config)#dpi qos profile qos_prof_01
[local]Redback(dpi-qos)#rate 64 burst 3000
```

1.36 show dpi card access-list

show dpi card *slot/asp-id* **access-list** [*list-name*]

1.36.1 Command Mode

All modes

1.36.2 Syntax Description

slot	Chassis slot number for a particular ASE card.
asp-id	The ID of the ASP on the ASE card: 1 or 2.
list-name	Detailed configuration information from the ASP for the ACL with the specified name.

1.36.3 Usage Guidelines

Displays information about one or all ACLs configured on the ASE card in the specified slot and port.

1.36.4 Examples

```
[local]Redback#show dpi card 2/1 access-list
  acl_01
  acl_02

[local]Redback# show dpi card 2/1 access-list acl_01
  Default Class: cc
    seq 10 application bit-torrent class dd
    seq 20 application bit-torrent class dd
    seq 30 application bit-torrent class dd
    seq 40 application bit-torrent class dd
    seq 50 category p2p class cc
    seq 60 protocol tcp any range 1 65535 range 1 65535 class dd
    seq 70 application bit-torrent network 1.2.3.4/0
    class hh
    seq 80 application bit-torrent network 1.2.3.4/1
    class hh
```

1.37 show dpi card qos profile

show dpi card ***slot/asp-id*** **qos profile** [***profile-name***]

1.37.1 Command Mode

All modes

1.37.2 Syntax Description

slot	Chassis slot number for a particular ASE card.
asp-id	The ID of the ASP on the ASE card: 1 or 2.
profile-name	Name of the profile.

1.37.3 Usage Guidelines

Displays information about one or all QoS profiles configured on the ASE card in the specified slot and port.

1.37.4 Examples

```
[local]Redback#show dpi card 2/1 qos profile
  q1
  q2
  q34

[local]Redback#show dpi card 2/1 qos profile q1
  Rate:  12312 kbps    Burst: 23 bytes
  Time-burst: 0 milli-seconds
  Conf-mark-priority   Conf-mark-prec  Conf-mark-
  dscp
      0xff                0xff                0x16
  Exceed-mark-priority   Exceed-mark-prec  Exceed-mark-
  dscp
      0xff                 0x2                0xff

    Jitter : 0
  Delay  : 123123
  Reorder: 12 (random)
```

1.38 show dpi card traffic-management action policy

show dpi card ***slot/asp-id*** **traffic-management action policy** [***policy-name***]

1.38.1 Command Mode

All modes

1.38.2 Syntax Description

slot	Chassis slot number for a particular ASE card.
asp-id	The ID of the ASP on the ASE card: 1 or 2.
policy-name	Name of the DPI traffic management action policy

1.38.3 Usage Guidelines

Displays information about one or all DPI traffic management action policies configured on the ASE card in the specified slot and port.

1.38.4 Examples

```
[local]Redback#show dpi card 2/1 traffic-management action policy
  apol_01
  apol_02

[local]Redback#show dpi card 2/1 traffic-management action policy apol_01
  Default Class:
  class c1
    Qos Profile: q1 [Bidirectional]
    Statistics: Enable
    Log Events: Detection
  class c2
    Qos Profile: q2 [Policing]
    Qos Profile: q3 [Metering]
    Statistics: Enable
    Log Events: Detection
```

1.39 show dpi card traffic-management application

show dpi card ***slot/asp-id*** **traffic-management application**

1.39.1 Command Mode

All modes

1.39.2 Syntax Description

slot	Chassis slot number for a particular ASE card.
asp-id	The ID of the ASP on the ASE card: 1 or 2.

1.39.3 Usage Guidelines

Displays a list of applications supported by the current signature file on an ASE card.

1.39.4 Examples

```
[local]Redback#show dpi card 4/2 traffic-management application
bit-torrent
fast-track
edonkey
gnutella
open-fast-track
skype
yahoo-messenger
google-talk
windows-live-messenger
rtp
rtsp
blackberry
imap
microsoft-media-services
shoutcast
netbios
quick-time
syncml
wap2
quake
half-life-2
doom-3
world-of-warcraft
tencent-qq
aol-instant-messenger
wireless-village
all-peers
direct-connect
ares
mxit
hamachi
fring
paltalk
http
sip
itunes
cool-streaming
max-tv
ppmate
apple-juice
100-bao
go-boogy
hot-line
kugoo
poco
tesla
soribada
baidu
citrix
imesh
kad-network
manolito
soulseek
warez
```

1.40 show dpi card traffic-management category

show dpi card ***slot/asp-id*** **traffic-management category** [***category-name***]

1.40.1 Command Mode

All modes

1.40.2 Syntax Description

slot Chassis slot number for a particular ASE card.

asp-id The ID of the ASP on the ASE card: 1 or 2.

category Displays a list of categories supported by the signature-file in use.

category-name Optional with the **category** keyword. Category name according to one of the keywords listed in Table 1. Displays the applications in the specified category.

1.40.3 Usage Guidelines

Displays a list of categories supported by the current signature file or the applications included in a specified category.

1.40.4 Examples

The following example provides a list of the application categories supported by the signature file in use:

```
[local]Redback#show dpi card 4/2 traffic-management category
all
file-transfer
gaming
instant-messaging
p2p
social-networks
streaming
transport
voip
```

1.41 show dpi card traffic-management group

show dpi card ***slot/asp-id*** **traffic-management group** [***group-name*** | **global**]

1.41.1 Command Mode

All modes

1.41.2 Syntax Description

slot Chassis slot number for a particular ASE card.

asp-id The ID of the ASP on the ASE card: 1 or 2.

group-name Optional. Displays only the DPI traffic management policy associated with the specified DPI traffic management group.

global Optional. Displays only the DPI traffic management policy associated with the global DPI traffic management group.

1.41.3 Usage Guidelines

Displays the DPI traffic management policy associated with all DPI traffic management groups configured on a SmartEdge router.

1.41.4 Examples

```
[local]Redback#show dpi card traffic-management group
  global
    policy: global_p_a3
  group1
    policy: p1_a3
  group2
    policy: p2_a3
```

1.42 show dpi card traffic-management policy

show dpi card ***slot/asp-id*** **traffic-management policy** [***policy-name***]

1.42.1 Command Mode

All modes

1.42.2 Syntax Description

slot Chassis slot number for a particular ASE card.

asp-id The ID of the ASP on the ASE card: 1 or 2.

policy-name Name of the DPI traffic management policy.

1.42.3 Usage Guidelines

Displays information about one or all DPI traffic management policies configured on the ASE card in the specified slot and port.

1.42.4 Examples

```
[local]Redback#show dpi card 2/1 traffic-management policy
  pol_01
    Access Group: acl_01
    Action Policy: apol_01

[local]Redback#show dpi card 2/2 traffic-management policy
  p1
    Access Group: acl1
    Action Policy: ap1
    qos profile sub_01

  p1_a3 aggregate
    Action Policy: ap1_a3
```

1.43 show dpi card traffic-management signature-file

show dpi card ***slot/asp-id*** **traffic-management signature-file**

1.43.1 Command Mode

All modes

1.43.2 Syntax Description

slot Chassis slot number for a particular ASE card.

asp-id The ID of the ASP on the ASE card: 1 or 2.

1.43.3 Usage Guidelines

Displays information about the signature file for the specified ASP; it could be the configured signature-file or the built-in one.

1.43.4 Examples

The following example displays information about the built-in signature file, configures a new signature file, and then displays information about the configured signature-file.

```
[local]Redback#show dpi card 6/1 traffic-management signature-file
  Signature Configured: [Built-in]
  Signature Applied: [Built-in]
  Error: None
  Signature-file Version: 4-25
  DPI Engine Version: 4-25
[local]Redback#configuration
Enter configuration commands, one per line, 'end' to exit
[local]Redback(config)#dpi traffic-management signature-file /md/P2P-4-35.sdf
[local]Redback#show dpi card 6/1 traffic-management signature-file
  Signature Configured: P2P-4-35.sdf
  Signature Applied: P2P-4-35.sdf
  Error: None
  Signature-file Version: 4-35
  DPI Engine Version: 4-25
```

1.44 show dpi card traffic-management statistics

show dpi card ***slot/asp-id*** **traffic-management statistics** {**packet** [**in** | **out**] | **protocol** [***protocol-name***] | **sessions** | **signature-file** | **subscriber instance**| **group** ***group-name*** [**class** ***class-name***] }

1.44.1 Command Mode

All modes

1.44.2 Syntax Description

slot	Chassis slot number for a particular ASE card.
asp-id	The ID of the ASP on the ASE card: 1 or 2.
packet	Displays traffic-management statistics for packets.
in	Optional. Limits packet statistics to inbound packets.
out	Optional. Limits packet statistics to outbound packets.
protocol	Displays ASP counters per application. If you include the optional ***protocol-name*** argument, displays ASP counters for that application.
sessions	Displays traffic-management statistics for sessions.
signature-file	Displays traffic-management statistics for the signature-file in use.
subscriber instance	Displays the total number of subscribers including the current and peak values.

`group` Displays traffic-management statistics for a DPI traffic management group that you specify with the ***`group-name`*** argument.

`class` Optional. Displays traffic management statistics for a class of traffic configured for a DPI traffic management group that you specify with the ***`class-name`*** argument.

1.44.3 Usage Guidelines

Use the **`show dpi card traffic-management statistics`** command to display traffic management statistics. Use the **`packet`** keyword to display traffic-management statistics for packets.

Use the **`in`** | **`out`** keywords to limit the display by direction.

Use the **`protocol`** keyword to display ASP counters per application; for example, the total number of packets and bytes received, dropped, and so on.

Use the **`signature-file`** keyword to display signature-file statistics for the configured or built-in signature-file for an ASP.

Use the **`subscriber`** keyword to display the current number of active subscribers, maximum subscriber count (historical), number of subscribers being processed with the specified profile, number of subscribers being processed with the default profile, and other subscriber statistics.

Use the **`group`** keyword to display statistics for a specified DPI traffic management group.

1.44.4 Examples

```
[local]Redback#show dpi card 2/1 traffic-management statistics protocol bit-torrent
Protocol: bit-torrent
      Direction: Egress
       Packets Received: 4110091
       Bytes Received: 2747344474
       Packets Dropped: 0
       Bytes Dropped: 0
       Flow Count: 1000
       Packets Inspected: 1000
       Packets Rate Limited: 0
       Packets Sent: 4110091
       Bytes Sent: 2747344474

      Direction: Ingress
       Packets Received: 18
       Bytes Received: 15238
       Packets Dropped: 10
       Bytes Dropped: 14720
       Flow Count: 1
       Packets Inspected: 1
       Packets Rate Limited: 10
       Packets Sent: 8
       Bytes Sent: 518
```

```
[local]Redback#show dpi card 2/1 traffic-management statistics subscriber
  Current Subscriber Count: 1000
  Maximum Subscriber Count: 1000
  Subscribers Exceeding Session Limit: 100
  Subscribers Per Profile:
           Profile-Name                  Subscriber-Count
               dpi_pol_1                  1000

  Subscribers Per Group:
           Group-Name                    Subscriber-Count
               dpi_grp_1                  500
               dpi_grp_2                  500


[local]Redback#show dpi card 9/1 traffic-management statistics packet
                                    Total           TCP             UDP      Non-TCP/UDP
   Packets Received:                  0              0               0             0
   Bytes Received:                    0              0               0             0
   Packets Dropped:                   0
       Queue limit:                   0
       Policy enforcement:            0
       Memory overload:               0
   Bytes Dropped:                     0
       Queue limit:                   0
       Policy enforcement:            0
       Memory overload:               0
   Packets Inspected:                 0              0               0
   Bytes Inspected:                   0              0               0
   Packets Rate Limited:              0
   Packets Sent:                      0
   Bytes Sent:                        0
   Packets Bypassed:                  0


[local]Redback#show dpi card 9/1 traffic-management statistics packet in
                                    Total           TCP             UDP      Non-TCP/UDP
   Packets Received:                  0              -             -             -
   Bytes Received:                    0              -             -             -
   Packets Dropped:                   0
       Queue limit:                   0
       Policy enforcement:            0
       Memory overload:               0
   Bytes Dropped:                     0
       Queue limit:                   0
       Policy enforcement:            0
       Memory overload:               0
   Packets Inspected:                 0              -             -
   Bytes Inspected:                   0              -             -
   Packets Rate Limited:              0
   Packets Sent:                      0
   Bytes Sent:                        0
   Packets Bypassed:                  0

[local]Redback#show dpi card 2/1 traffic-management statistics sessions
Sessions:
   TCP:
     Current:
       Pending Classification: 0
         Setup-rate:  (5s     1m     5m)
                       0      0      0
         Peak Setup-rate (1s): 0
         Total: 0
     Cumulative (since ASP Startup):
         Created: 0
         Terminated:  0

   UDP:
     Current:
         DNS: 0
         Pending Classification: 0
         Setup-rate:  (5s     1m     5m)
                       0      0      0
         Peak Setup-rate (1s): 0
         Total: 0
     Cumulative (since ASP Startup):
         Created: 0
         Terminated:  0
```

```
[local]Redback#show dpi card 2/1 traffic-management statistics group dpi_grp_1
  Class: c1_01
         Direction: Egress
         Packets Received: 79858
         Bytes Received: 3242513
         Packets Dropped: 784
         Bytes Dropped: 35154
         Packets Sent: 79074
         Bytes Sent: 3207359

  Class: c1_01
         Direction: Ingress
         Packets Received: 123261
         Bytes Received: 176663951
         Packets Dropped: 35323
         Bytes Dropped: 51222346
         Packets Sent: 87938
         Bytes Sent: 125441605
```

1.45 show dpi circuit

show dpi circuit {**agent-circuit-id** ***agent-circuit-id*** | **agent-remote-id** ***agent-remote-id*** | ***slot***/***port***[**:** ***chan-num***[**:** ***sub-chan-num***] [***circuit-id***] | **username** ***subscriber***} **traffic-management** [**sessions** | **statistics sessions** | **statistics** [**packet** [**in** | **out**]] {**class** | **protocol**}]

1.45.1 Command Mode

All modes

1.45.2 Syntax Description

agent-circuit-id ***agent-circuit-id***

Subscriber session identifier, where the ***agent-circuit-id*** argument is the value of the agent circuit ID in a subscriber record. Enter the ***agent-circuit-id*** argument as a structured subscriber username in the form subscriber@context.

agent-remote-id ***agent-remote-id***

Subscriber session identifier, where the ***agent-remote-id*** argument is the value of the agent remote ID in a subscriber record. Enter the ***agent-remote-id*** argument as a structured subscriber username in the form subscriber@context.

slot

Chassis slot number for a particular card.

port

Port number on the specified card.

circuit-id

Subscriber session identifier. See Table 2 for information about the ***circuit-id*** argument.

username ***subscriber***

Subscriber session identifier. Enter the subscriber argument as a structured subscriber username in the form subscriber@context.

`sessions`	Displays a summary of all active (TCP, UDP) sessions for the specified subscriber.
`statistics sessions`	Displays subscriber session statistics from the ASP.
`packet` [`in` | `out`]	Displays directional traffic statistics per subscriber.
`class`	Displays subscriber statistics per class.
`protocol`	Displays subscriber statistics per application or protocol.

1.45.3 Usage Guidelines

Displays security service specific information per subscriber, including:

- The service enabled for the subscriber
- Whether the subscriber is receiving the specified service
- Whether the service is being bypassed
- Whether traffic for this subscriber is being dropped due to a lack of operational ASPs
- The specific ASP that is providing the service

Use the **`sessions`** keyword to display a summary of all active (TCP, UDP) sessions for the specified subscriber, including the standard 5-tuple and the class applied to the flow; one line is displayed per subscriber session. Use the **`statistics`** keyword to display the subscriber statistics, including session statistics.

1.45.4 Examples

```
[local]Redback#show dpi circuit username p2_1@local
  Assigned-ASP 2/1
  ASP-State: Up
  Services Configured: P2P-Traffic-Management[test]
  Services Applied: P2P-Traffic-Management[test]
  Service State: Normal

[local]Redback#show dpi circuit username p2_1@local traffic-management sessions
Source-IP  Source-  Transport      Dest-        Dest-IP
           Port                    Port
12.1.0.1   32768    tcp        6881     112.1.1.1
P2P-Protocol       Class-Protocol
bit-torrent          c34

[local]Redback#show dpi circuit username p2_1@local traffic-management statistics class
  Class: c100
        Direction: Egress
        Packets Received: 2
        Bytes Received: 80
        Packets Dropped: 0
        Bytes Dropped: 0
        Flow Count: 0
        Packets Inspected: 2
        Packets Rate Limited: 0
        Packets Sent: 2
        Bytes Sent: 80
  Class: c100
        Direction: Ingress
        Packets Received: 1
        Bytes Received: 40
        Packets Dropped: 0
        Bytes Dropped: 0
        Flow Count: 0
        Packets Inspected: 1
        Packets Rate Limited: 0
        Packets Sent: 1
        Bytes Sent: 40
  Class: c34
        Direction: Egress
        Packets Received: 58
        Bytes Received: 3390

[local]Redback#show dpi circuit username p2_1@local traffic-management statistics protocol
  Protocol: bit-torrent
        Direction: Egress
        Packets Received: 106
        Bytes Received: 6166
        Packets Dropped: 0
        Bytes Dropped: 0
        Flow Count: 1
        Packets Inspected: 1
        Packets Rate Limited: 0
        Packets Sent: 106
        Bytes Sent: 6166
  Protocol: bit-torrent
        Direction: Ingress
        Packets Received: 283
        Bytes Received: 266422
        Packets Dropped: 177
        Bytes Dropped: 260544
        Flow Count: 1
        Packets Inspected: 0
        Packets Rate Limited: 177
        Packets Sent: 106
        Bytes Sent: 5878
```

```
[local]Redback#show dpi circuit username user1@domain.com traffic-management statistics packet
        Packets Received: 6144
        Bytes Received: 4479456
        Packets Dropped: 856
        Bytes Dropped: 34240
        Packets Inspected: 64
        Packets Rate Limited: 0
        Packets Exceeding Session Limit: 1100
        Bytes Exceeding Session Limit: 187592
        Packets Sent: 6144
        Bytes Sent: 4479456
        TCP Resets Originated: 0
```

```
[local]Redback#show dpi circuit username user1@domain.com traffic-management statistics session
 Sessions:
   TCP:
     Pending Classification: 1
     Total: 2
   UDP:
     DNS: 0
     Pending Classification: 1
     Total: 1
```

1.46 show dpi traffic-management

show dpi traffic-management {**signature-file** [***sig-filename*** {**application** | **category**}] | **application** | **category** [***category-name***]}

1.46.1 Command Mode

All modes

1.46.2 Syntax Description

signature-file

Optional. Display the configured and applied signature-file, version of DPI Engine, active signature-file, and any errors.

sig-filename

Name of a signature file on the XCRP controller card.

A signature filename is optional with the **signature-file** keyword. If you do not specify a filename, the built-in file is used. To specify a file in the secure directory in /flash (the default signature file directory), use only the filename. To specify a signature file in another location, use a path and filename.

application

Optional. Displays all supported applications or the applications supported by a specific signature file.

`category`

Optional. Displays all supported categories or the applications supported by a specific category.

`category-name`

Optional with the **`category`** keyword. Category name according to one of the keywords listed in Table 1. Displays all applications in the specified category.

1.46.3 Usage Guidelines

Displays traffic management applications or categories supported by the current or built-in signature file.

With the **`signature-file`** keyword, displays the configured and applied signature-file, version of DPI Engine, active signature-file, and any errors. With the **`signature-file`** ***`sig-filename`*** construct, displays the applications or categories supported by the signature file.

1.46.4 Examples

The following example displays the categories supported by the current signature-file on the XCRP card.

```
[local]Redback#show dpi traffic-management category
all
file-transfer
gaming
instant-messaging
p2p
social-networks
streaming
transport
voip
```

The following example displays the applications supported by the `p2p-3-1.sdf` signature file.

```
 [local]Redback#show dpi traffic-management signature-file p2p-3-1.sdf application
bit-torrent
fast-track
edonkey
gnutella
open-fast-track
skype
yahoo-messenger
google-talk
windows-live-messenger
rtp
rtsp
blackberry
imap
microsoft-media-services
shoutcast
netbios
quick-time
syncml
wap2
quake
half-life-2
doom-3
world-of-warcraft
```

```
tencent-qq
aol-instant-messenger
wireless-village
all-peers
direct-connect
ares
mxit
hamachi
fring
paltalk
http
sip
itunes
cool-streaming
max-tv
ppmate
apple-juice
100-bao
go-boogy
hot-line
kugoo
poco
tesla
soribada
baidu
citrix
imesh
kad-network
manolito
soulseek
warez
joost
orb
peercasting
pplive
slingbox
windows-media-player
youtube
zattoo
winny
flashstreaming
zrtp
ants-p2p
rdp
sopcast
veetle
zepp
nntp
rtmp
your-freedom
spotify
audition
facebook
hulu
opera-mini
```

1.47 show dpi traffic-management group distribution

`show dpi traffic-management group` [*`group-name`*] **`distribution`**

1.47.1 Command Mode

All modes

1.47.2 Syntax Description

group-name Optional. Displays only the subscriber distribution per ASP for the specified DPI traffic management group.

1.47.3 Usage Guidelines

Displays subscriber distribution per subscriber group per ASP for all DPI traffic management groups configured on a SmartEdge router.

1.47.4 Examples

```
[local]Redback#show dpi traffic-management group distribution
  Group-Name              Subscriber-Count
    g3                            0

    g5                           4000
      ASP 1/1                      2000
      ASP 2/2                      2000

    global                       4000
      ASP 1/1                      2000
      ASP 1/2                      2000
```

1.48 show security card statistics

show security card ***slot/asp-id*** **statistics** {**packet** ***slot*** | **system**}

1.48.1 Command Mode

All modes

1.48.2 Syntax Description

slot Chassis slot number for a particular ASE card.

asp-id The ID of the ASP on the ASE card: 1 or 2.

packet Statistics output lists the Rx/Tx counters, including packets and bytes received, error packet and byte counts, packets and bytes sent, and packets and bytes dropped.

slot Chassis slot number.

system Statistics output lists memory usage of an ASP, including the number of ATM APS packets processed that were replicated.

1.48.3 Usage Guidelines

Displays statistics for the ASP on the specified ASE card.

1.48.4 Examples

```
[local]Redback#show security card 2/1 statistics system

Data Plan CPU % usage: (5s,      1m,      5m)
                       18.36    15.45    12.57

Memory Information :
  Total Dynamic Memory: 1226803784 Bytes
  Memory Allocated: 502920800 Bytes
  Memory Available: 723882984 Bytes
  Allocation Failures: 0 Bytes

Packet Statistics :
  Bypassed packets:
    Unknown Subscribers:  0
    Memory Overload: 0
  Replicated packets
    slot 1: 19108908
    slot 5: 817923
    slot 6: 817923
    slot 10: 19108908
```

1.49 show security card system

show security card ***slot/asp-id*** **system**

1.49.1 Command Mode

All modes

1.49.2 Syntax Description

slot	Chassis slot number for a particular ASE card.
asp-id	The ID of the ASP on the ASE card: 1 or 2.

1.49.3 Usage Guidelines

Displays system-level information stored on the ASP, such as a list of slots populated with cards, card type and PPA type of traffic cards installed, and the state of each populated slot.

1.49.4 Examples

```
[local]Redback#show security card 2/1 system

Control Plane :
     Slot          Card-Type           State
      2            ase                   Up
      4            ge-20-port            Up

Data Plane :
     Slot          Card-Type           State
      2            ase                   Up
      4            ge-20-port            Up
```

1.50 statistics

statistics [class | protocol |]

no statistics [class | protocol]

1.50.1 Command Mode

DPI traffic-management policy configuration

1.50.2 Syntax Description

class	Depending on whether the policy you are configuring is associated with a subscriber or subscriber group, enables per subscriber per class or per subscriber group per class statistics collection.
protocol	Enables per subscriber per protocol statistics collection.

1.50.3 Default

Statistics collection is disabled by default.

1.50.4 Usage Guidelines

Enables per subscriber per class and per subscriber per protocol statistics collection. The **no** form of this command disables statistics collection.

Note: The keyword statistics

1.50.5 Examples

The following example shows how to enable per subscriber per protocol statistics collection:

```
[local]Redback(config)#dpi traffic-management policy p1
[local]Redback(config-dpi-policy)#statistics protocol
```

The following example shows how to enable per subscriber group per class statistics collection:

```
[local]Redback(config)#dpi traffic-management policy p1agg aggregate
[local]Redback(config-dpi-policy)#statistics class
```

1.51 traffic-management policy

traffic-management policy ***policy-name***

no traffic-management policy ***policy-name***

1.51.1 Command Mode

DPI traffic management group configuration

1.51.2 Syntax Description

policy-name	The name of the DPI traffic management policy.

1.51.3 Default

No DPI traffic management policy is configured.

1.51.4 Usage Guidelines

Associates a DPI traffic management policy with a DPI traffic management group.

1.51.5 Examples

```
[local]Redback(config)#dpi traffic-management group g1
[local]Redback(config-dpi-group)#traffic-management policy p3_a
```

Glossary

ACL
Access Control List

AF
Assured Forwarding

DSCP
Differentiated Services Code Point

ISAKMP
Internet Security Association and Key Management Protocol

MPLS
Multiprotocol Label Switching

NIC
Network Interface Card

PD
Packet Descriptor

QoS
Quality of Service

TCP
Transmission Control Protocol

ToS
Type of Service

UDP
User Datagram Protocol

VCI
Virtual Circuit Identifier

VPI
Virtual Path Identifier

Reference List

[1] *Application Traffic Management Overview*, 221 02-CRA 119 1170/1-V1

[2] *Application Traffic Management Configuration and Operation*, 1543-CRA 119 1170/1-V1

[3] *Command List*, 1/190 77-CRA 119 1170/1-V1