



Policy Traffic Switch CLI Reference Guide, Release 6.40

**05-00263 B01
2014-5-12**

Contents

1 CLI Overview	12
1.1 Command Line Interface.....	13
1.1.1 The CLI Shell.....	13
1.1.2 Available CLI Commands.....	16
1.1.3 Output Filtering.....	18
1.1.4 Commands Entered Incorrectly.....	19
1.1.5 Waiting for Completion.....	20
1.1.6 Configuration versus Operational show Commands.....	21
1.2 CLI Command Structure.....	22
1.2.1 Command Class.....	22
2 CLI Commands.....	24
2.1 Management Commands.....	25
2.1.1 Waiting for Completion.....	25
2.1.2 clear.....	25
2.1.3 commit.....	25
2.1.4 configure.....	25
2.1.5 edit.....	25
2.1.6 exit.....	26
2.1.7 history.....	26
2.1.8 load config.....	26
2.1.9 ping.....	26
2.1.10 reboot.....	26
2.1.11 reload.....	26
2.1.12 reload.....	27
2.1.13 restart service.....	27
2.1.14 save config.....	28
2.1.15 shutdown.....	28
2.1.16 start service.....	28
2.1.17 stop service.....	29
2.1.18 techsupport.....	30
2.1.19 traceroute.....	31
2.1.20 update.....	31
2.1.21 set user default-shell.....	31
2.2 Adding, Setting, and Deleting Users.....	31
2.2.1 add user.....	31
2.2.2 set user.....	32

2.2.3 delete user.....	32
2.3 add/set/delete config.....	32
2.3.1 add/set/delete config interface mac-ip-mapping.....	33
2.3.2 add/set/delete config service bgp peer.....	33
2.3.3 add/set/delete config policy divert vlan.....	34
2.3.4 add/set/delete config policy vlan-label.....	35
2.3.5 add/set/delete config service protocol voip provider.....	35
2.3.6 add/set/delete config service session-qualifier bridge-group.....	36
2.3.7 add/set/delete config service session-qualifier s-vlan.....	37
2.3.8 add/set/delete config service session-qualifier vlan.....	37
2.3.9 add/set/delete config service tunneling.....	38
2.3.10 add/set/delete config system log remote-server	39
2.3.11 add/set/delete service udp-prioritization prioritized-port.....	39
2.4 Overview of clear commands.....	40
2.4.1 clear alarms bridge-group.....	40
2.4.2 clear alarms counters.....	40
2.4.3 clear alarms ip-overload-management.....	40
2.4.4 clear interface counters.....	41
2.4.5 clear policy controller key-translation cache.....	41
2.4.6 clear service bgp routing-table.....	41
2.4.7 clear service ip-overload-management interval-stats.....	41
2.4.8 clear service ip-overload-management subnet.....	41
2.4.9 clear service load-balancer.....	41
2.4.10 clear service protocol voip unknown-providers.....	42
2.4.11 clear service subscriber-management.....	42
2.5 delete subscriber ip.....	42
2.6 delete service nat mappings all.....	43
2.7 edit policy.....	43
2.8 edit service ip-overload-management subnets.....	43
2.9 edit system motd.....	43
2.10 set config.....	44
2.10.1 set config cli prompt.....	44
2.10.2 set config cli session-limit.....	44
2.10.3 set config cli text-editor.....	44
2.10.4 set config cluster.....	45
2.10.5 set config deployment mode.....	45
2.10.6 set config files.....	46
2.10.7 set config interface <cluster-interface>.....	46
2.10.8 set config interface <data-interface>.....	49

2.10.9 set config interface address-tracking.....	51
2.10.10 set config interface <interface> media	52
2.10.11 set config interface <interface> shunt-tos.....	52
2.10.12 set config interface bridge-group monitoring.....	52
2.10.13 set config interface bypass.....	53
2.10.14 set config interface cluster vlan external-service.....	54
2.10.15 set config interface external-service ip-address primary.....	54
2.10.16 set config interface internal-service ip-address primary.....	54
2.10.17 set config interface internal-routeability.....	55
2.10.18 set config interface link-group.....	55
2.10.19 set config interface management redundancy.....	55
2.10.20 set config interface max-inspect-frame-size.....	56
2.10.21 set config interface <lag-interface>.....	56
2.10.22 set config interface mac-logging-rate.....	56
2.10.23 set config interface spanning-tree cst bridge-priority.....	56
2.10.24 set config interface trunk-distribution	57
2.10.25 set config interface vlan.....	57
2.10.26 set config network-protection.....	57
2.10.27 set config policy arp interval.....	58
2.10.28 set config policy destination file default-path.....	59
2.10.29 set config policy divert max-divert-errors	59
2.10.30 set config policy ipv6 hash-mask.....	59
2.10.31 set config policy measurement max-subscriber-instances.....	59
2.10.32 set config policy optimization flow-statistics.....	60
2.10.33 set config policy session-management.....	60
2.10.34 set config policy shaper burst-absorption scaling-factor	60
2.10.35 set config policy shaper shape-traffic-before-recognition.....	60
2.10.36 set config policy table max-row-bytes.....	60
2.10.37 set config service bgp.....	61
2.10.38 set config service control-center authentication.....	62
2.10.39 set config service diameter connection ip-dscp.....	62
2.10.40 set config service diameter messages pts application-common.....	62
2.10.41 set config service id-allocation.....	63
2.10.42 set config service ip-overload-management.....	64
2.10.43 set config service ip-overload-management alarms.....	66
2.10.44 set config service load-balancer.....	66
2.10.45 set config service nat enabled.....	67
2.10.46 set config service protocol.....	68
2.10.47 set config service protocol flow reassembly.....	68

2.10.48 set config service session-qualifier cluster-number	68
2.10.49 set config service session-qualifier mode	68
2.10.50 set config service session-qualifier warn-ip-policy.....	69
2.10.51 set config service spb.....	69
2.10.52 set config service statistics log-interval.....	70
2.10.53 set config service statistics skip-headers.....	70
2.10.54 set config service statistics subscriber minimum-bytes.....	71
2.10.55 set config service statistics tunnel-fragment-extrapolation.....	71
2.10.56 set config service streaming analyzer hds.....	71
2.10.57 set config service streaming analyzer hls.....	72
2.10.58 set config service streaming analyzer smooth-streaming video-state	72
2.10.59 set config streaming analyzer hls video-state.....	72
2.10.60 set config service subscriber-management auto-remap.....	73
2.10.61 set config service subscriber-management end-session-event end-flows.....	74
2.10.62 set config service subscriber-management login-events handle-notification.....	74
2.10.63 set config service subscriber-management lookup.....	74
2.10.64 set config service subscriber-management new-session-event require-activity.....	75
2.10.65 set config service subscriber-management timeout.....	75
2.10.66 set config service switch-fabric workfarm.....	76
2.10.67 set config service switch-fabric core-fabric.....	77
2.10.68 set config service tunneling.....	78
2.10.69 set config service udp-prioritization.....	80
2.10.70 set config support notification-email-address.....	80
2.10.71 set config system accounting.....	81
2.10.72 set config system accounting tacacs+.....	81
2.10.73 set config system authentication tacacs+.....	82
2.10.74 set config system authentication.....	82
2.10.75 set config system reload bridge-mode alarm timeout.....	82
2.10.76 set config system services last-reload.....	83
2.10.77 set config traffic flow-limit.....	83
2.11 Operational set Commands.....	83
2.11.1 set interface shunt.....	83
2.11.2 set policy destination.....	83
2.11.3 set service load-balancer.....	84
2.12 monitor.....	84
2.12.1 monitor interface counters.....	84
2.12.2 monitor interface rate.....	86
2.12.3 monitor system overview.....	87
2.12.4 monitor traffic.....	88

2.13 show.....	88
2.13.1 show alarms.....	88
2.13.2 show alarms history.....	89
2.13.3 show alarms model.....	90
2.13.4 show cli sessions.....	91
2.13.5 show config pending.....	91
2.13.6 show interface bridge-group.....	91
2.13.7 show interface bypass.....	92
2.13.8 show interface bypass-chassis.....	93
2.13.9 show interface configuration.....	94
2.13.10 show interface counters.....	95
2.13.11 show interface divert-vlan.....	99
2.13.12 show interface drops.....	99
2.13.13 show interface internal-mac-lookup.....	102
2.13.14 show interface ip-address-tracking.....	102
2.13.15 show interface link-group.....	103
2.13.16 show interface mac-address-table.....	103
2.13.17 show interface management.....	104
2.13.18 show interface modules.....	105
2.13.19 show interface neighbors.....	106
2.13.20 show interface network.....	106
2.13.21 show interface npu assignment.....	106
2.13.22 show interface rate.....	106
2.13.23 show interface spanning-tree instance.....	107
2.13.24 show interface spanning-tree instance cst.....	107
2.13.25 show interface spanning-tree port.....	108
2.13.26 show interface spanning-tree vlans.....	108
2.13.27 show interface vlan-tagging.....	109
2.13.28 show log.....	109
2.13.29 show log authentication.....	109
2.13.30 show log cli.....	109
2.13.31 show log control-center.....	110
2.13.32 show log install.....	110
2.13.33 show log mac-movement	110
2.13.34 show policy.....	110
2.13.35 show policy attacks.....	110
2.13.36 show policy attacks detections.....	111
2.13.37 show policy attacks detections stats.....	111
2.13.38 show policy attacks rules.....	111

2.13.39 show policy attacks rules counts.....	112
2.13.40 show policy attacks rules <id>.....	112
2.13.41 show policy attacks rules patterns.....	113
2.13.42 show policy attacks rules stats.....	113
2.13.43 show policy attacks rules status.....	113
2.13.44 show policy attacks signature-match.....	114
2.13.45 show policy attacks spam.....	114
2.13.46 show policy classifier.....	114
2.13.47 show policy classifier stats.....	115
2.13.48 show policy controller.....	115
2.13.49 show policy count.....	116
2.13.50 show policy count demographic.....	117
2.13.51 show policy count port.....	118
2.13.52 show policy count subscriber.....	119
2.13.53 show policy destination.....	119
2.13.54 show policy divert.....	122
2.13.55 show policy dpm.....	122
2.13.56 show policy errors.....	122
2.13.57 show policy flow-detector.....	123
2.13.58 show policy healthcheck.....	123
2.13.59 show policy histogram.....	125
2.13.60 show policy inspection.....	126
2.13.61 show policy limiter.....	127
2.13.62 show policy map.....	128
2.13.63 show policy measurement.....	129
2.13.64 show policy publish.....	131
2.13.65 show policy shaper.....	132
2.13.66 show policy subnets.....	134
2.13.67 show policy table.....	135
2.13.68 show policy timer.....	136
2.13.69 show policy timer instances.....	136
2.13.70 show policy timer stats.....	137
2.13.71 show policy whitelist.....	137
2.13.72 show service bgp attributes.....	137
2.13.73 show service bgp errors.....	137
2.13.74 show service bgp peer.....	138
2.13.75 show service bgp peer <ipv4-address>.....	138
2.13.76 show service bgp peer all.....	139
2.13.77 show service bgp route.....	140

2.13.78 show service bgp route-distribution.....	141
2.13.79 show service bgp status.....	141
2.13.80 show service bgp subnet.....	142
2.13.81 show service cluster-discovery.....	142
2.13.82 show service control-center stats.....	144
2.13.83 show service diameter.....	144
2.13.84 show service election.....	153
2.13.85 show service election feature.....	153
2.13.86 show service election master.....	153
2.13.87 show service election master peer.....	154
2.13.88 show service election random.....	154
2.13.89 show service election random peer.....	154
2.13.90 show service id-allocation.....	154
2.13.91 show service ip-overload-management never-shunted-subnets.....	156
2.13.92 show service ip-overload-management shunted-subnets.....	156
2.13.93 show service ip-overload-management stats.....	157
2.13.94 show service ip-overload-management usage-detection.....	157
2.13.95 show service load-balancer bundle.....	158
2.13.96 show service load-balancer cluster compatibility.....	158
2.13.97 show service load-balancer ip.....	159
2.13.98 show service load-balancer element status.....	160
2.13.99 show service load-balancer master.....	160
2.13.100 show service load-balancer modules.....	161
2.13.101 show service load-balancer preload.....	162
2.13.102 show service load-balancer stats.....	162
2.13.103 show service nat.....	163
2.13.104 show service protocol voip.....	164
2.13.105 show service protocol parsed-fields.....	164
2.13.106 show service route.....	164
2.13.107 show service statistics tunnel-fragment-extrapolation.....	165
2.13.108 show service session-management config.....	165
2.13.109 show service shaping stats.....	166
2.13.110 show service spb config.....	166
2.13.111 show service spb connections.....	167
2.13.112 show service spb.....	168
2.13.113 show service spb connections diagnostics.....	168
2.13.114 show service spb messages.....	169
2.13.115 show service spb stats.....	170
2.13.116 show service spb subscribers.....	171

2.13.117 show service streaming analyzer.....	172
2.13.118 show service streaming analyzer smooth-streaming	173
2.13.119 show service streaming errors.....	174
2.13.120 show service streaming stats.....	174
2.13.121 show service subscriber-management stats.....	175
2.13.122 show service subscriber-management dashboard.....	177
2.13.123 show service tunneling config.....	178
2.13.124 show service udp-prioritization.....	178
2.13.125 show subscriber all.....	179
2.13.126 show subscriber ip.....	179
2.13.127 show subscriber name.....	180
2.13.128 show subscriber all file.....	181
2.13.129 show system accounting.....	182
2.13.130 show system blades.....	182
2.13.131 show system environmental.....	183
2.13.132 show system environmental fans.....	183
2.13.133 show system environmental power.....	183
2.13.134 show system environmental temperature.....	184
2.13.135 show system environmental voltage.....	184
2.13.136 show system firewall.....	184
2.13.137 show system hardware.....	185
2.13.138 show system hardware machine-check.....	185
2.13.139 show system history enable.....	185
2.13.140 show system history login.....	186
2.13.141 show system history reload.....	186
2.13.142 show system indicators.....	186
2.13.143 show system information.....	187
2.13.144 show system licenses.....	187
2.13.145 show system modules.....	188
2.13.146 show system nat.....	189
2.13.147 show system overview.....	189
2.13.148 show system processes.....	189
2.13.149 show system resources.....	190
2.13.150 show system services.....	193
2.13.151 show system services last-reload.....	193
2.13.152 show system storage container.....	194
2.13.153 show system storage controller.....	195
2.13.154 show system storage disk.....	195
2.13.155 show system version.....	197

2.13.156 show traffic.....	197
2.13.157 show user.....	200



1

CLI Overview

- ["Command Line Interface" on page 13](#)
- ["CLI Command Structure" on page 22](#)

1.1 Command Line Interface

The Command Line Interface (CLI) available on Sandvine software or hardware elements provides:

- Operational and configuration modes
- Output filtering
- Tab completion
- Online help



Note:

Commands are updated and/or deprecated with Sandvine product releases. See the product release notes in conjunction with this guide.

1.1.1 The CLI Shell

Run CLI commands within the CLI shell (the CLI prompt).

You can run CLI commands directly on a Sandvine element or from an SSH session that logs onto an element. When on an element, at the default command prompt, enter `svcli`. You can also access the CLI using the command `cli`.

The CLI shell appears, with the prompt indicating the platform you are logged onto, such as PTS, SRP or SDE. For example:

```
Sandvine CLI.  
Copyright 20XX Sandvine Incorporated. All rights reserved.
```

```
SRP>
```

```
Sandvine CLI.  
Copyright 20XX Sandvine Incorporated. All rights reserved.
```

```
PTS>
```

```
Sandvine CLI.  
Copyright 20XX Sandvine Incorporated. All rights reserved.
```

```
SDE>
```

The CLI defaults to operational mode, which is used to administer the system, display status and perform operations. To enter configuration mode type `configure`. The CLI shell changes:

```
SRP> configure
```

```
The CLI is now in CONFIGURATION mode.
```

```
SRP#
```

```
PTS> configure
```

```
The CLI is now in CONFIGURATION mode.
```

```
PTS#
```

```
SDE> configure
```

```
The CLI is now in CONFIGURATION mode.
```

```
SDE#
```

To compare the modes:

	Operational Mode	Configuration Mode
prompt	The platform name followed by the "greater than" sign. For example: SRP> PTS>SDE>.	The platform name followed by the hash sign. For example:SRP#PTS#SDE#.
purpose	Administering the system.	Configuring the system.
available commands	show, clear, and some set commands, typically to do with SandScript or the database.	All operational commands and add, delete, commit, save, reset, restart, and set config commands.
allowed sessions	Unlimited. 1000 sessions maximum.	Only one session allowed. Session times out after 10 minutes of inactivity.
permissions	This is command-specific.	sv_admin only

1.1.1.1 Operational Mode

You can use the CLI operational mode to run basic operational commands. Common commands include:

- ?—Displays online help.
- add—Adds a configuration.
- clear—Clears the terminal or a service.
- configure—Enters configuration mode.
- delete—Deletes a configuration.
- exit—Exits the CLI.
- history—Displays command history.
- monitor—Auto-refreshes operational data.
- reload—Reloads a configuration or SandScript.
- restore—Restores counters to pre-cleared values.
- set—Sets an operational variable which typically triggers some action.
- show—Displays operational data.
- techsupport—Collects system/service level information useful for debugging the machine.

1.1.1.2 Configuration Mode

You can use the CLI configuration mode to configure the system.

Run the `configure` command from the operational mode to enter the configuration mode. The prompt changes to the name of the platform, with the hash symbol. The commands available in the configuration mode include all operational mode commands in addition to commands for configuring the system.

To prevent conflicts, only one user can enter configuration mode on an element at a time. If a user is already in configuration mode, an error message appears when trying to switch between modes. If the configuration mode is inactive for 10 minutes, the CLI exits the configuration mode to revert to the operational mode. An output similar to this appears:

```
PTS> configure
The CLI is now in CONFIGURATION mode.
This configuration session will expire after 10 minutes of inactivity.
PTS#
The inactivity timer has expired, exiting configuration mode...
The CLI is now in OPERATIONAL mode.
PTS>
```

```
SRP> configure
The CLI is now in CONFIGURATION mode.
This configuration session will expire after 10 minutes of inactivity.
SRP#
The inactivity timer has expired, exiting configuration mode...
```

```
The CLI is now in OPERATIONAL mode.  
SRP>
```

```
SDE> configure  
The CLI is now in CONFIGURATION mode.  
This configuration session will expire after 10 minutes of inactivity.  
SDE#  
The inactivity timer has expired, exiting configuration mode...  
The CLI is now in OPERATIONAL mode.  
SDE>
```

Forcing Configuration Mode

Run this CLI command to force another user out of the configuration mode. The user who is forced out of the configuration mode loses any pending changes.

```
PTS> configure force  
The CLI is now in CONFIGURATION mode. This configuration session will expire after 10 minutes  
of inactivity  
SRP> configure force  
The CLI is now in CONFIGURATION mode. This configuration session will expire after 10 minutes  
of inactivity  
SDE> configure force  
The CLI is now in CONFIGURATION mode. This configuration session will expire after 10 minutes  
of inactivity
```

A notification similar to this appears:

```
PTS#  
The CLI was forced out of configuration mode by another user and is now in OPERATIONAL mode.  
PTS>
```

```
SRP#  
The CLI was forced out of configuration mode by another user and is now in OPERATIONAL mode.  
SRP>
```

```
SDE#  
The CLI was forced out of configuration mode by another user and is now in OPERATIONAL mode.  
SDE>
```



Note:

The `configure force` notification appears only when you try to run a new command or press **Tab**.

Configuration tables

Some configurations are stored in tables. Run the appropriate `add config ...` CLI command to add a row to a table and also to add the specified configuration to the table. You must specify a value for every non-optional entry in the table.

Applying configuration changes

The CLI saves configuration changes that you make using `set`, `add`, `delete`, or `reset config` CLI commands, but does not apply the changes. Run the `show config pending` command to view the pending changes. Run the `show config *` command to view specific pending configuration changes. The `->` symbol indicates the pending changes.

This example changes the subname:

```
name: SANDVINE-1  
sub-name: SANDVINE-1 -> subname  
stat-name:
```

This example shows change in a cluster name:

```
name: SANDVINE-SDE-1 -> cluster123
```

Run the `commit` CLI command to apply the configuration changes. The element automatically reloads, restarts, or reboots any required processes or elements, depending on the configuration change.

**Note:**

Schedule the system configuration during standard maintenance windows to prevent service impact or performance degradation.

After applying the configuration changes, the CLI switches to operational mode. If the configuration fails, the system rolls back to the previous configuration, restoring the system to its operational state.

In the event of roll back failure, Alarm Model 79—Last reload failed— is raised and the system is in an indeterminate state.

Run the `exit` command to undo your changes or to exit the configuration mode.

An output similar to this appears if you exit the CLI with pending changes:

```
Exit configuration mode without committing changes? (y/n)
```

Reset config

Run the `reset` CLI commands to reset a configuration variable to its default value. For example:

```
reset config service diameter messages message-maximums incoming-queued
reset config service message-broker max-connections
```

Show config

Every `add config` and `set config` command has a corresponding `show config` command. For example:

```
set config service spb servers
show config service spb servers
```

See the CLI reference documentation for the corresponding `add config` or `set config` command for information about the command output.

1.1.2 Available CLI Commands

Press **Tab** at the CLI prompt to see which CLI commands are available.

The top level of the command structure appears with a brief description for each command. For example, these commands are available to **sv_operator** users:

```
PTS>
?                Display online help
add              Add a user or some operational state
clear           Clear the terminal or a service
exit            Exit the CLI
help            Display help and documentation
history         Display command history
monitor         Auto-refreshing operational data
ping            Ping a host (send an ICMP echo request)
restore         Restore counters to pre-cleared values
set             Change operational settings/state or trigger an action
show           Display operational data
techsupport     Collect system/service level information useful for debugging this machine
traceroute      Display the route packets take to reach a host
```

These commands are available to **sv_admin** users :

```
PTS>
?                Display online help
add              Add a user or some operational state
clear           Clear the terminal or a service
```


edit	Edit a file
exit	Exit the CLI
help	Display help and documentation
history	Display command history
monitor	Auto-refreshing operational data
ping	Ping a host (send an ICMP echo request)
reload	Reload configuration and policy
restore	Restore counters to pre-cleared values
set	Change operational settings/state or trigger an action
show	Display operational data techsupport Collect system/service level information useful for debugging this machine
traceroute	Display the route packets take to reach a host

To refine the output, enter a command and then press **Tab** twice. For example, if you refine the `show` command:

alarms	Alarm status, history and information
cli	Information related to the Command Line Interface
cluster	Information about the SPB cluster
config	System configuration
interface	Information about network interfaces
network-element	SPB, PTS, or other elements on the network
network-element-cluster	Clusters on the network
service	Information about system services
subscriber	Information about subscribers
system	System version, status and resources

alarms	Alarm status, history and information
cli	Information related to the Command Line Interface
config	System configuration
log	The primary log file for the system
policy	Rules and constructs defined in policy
service	Information about system services
subscriber	Information about subscribers
system	System version, status and resources
usage-management	Information about Usage Management products
user	A list of users and privilege levels



Note:

See the appropriate Usage Management User Guide for information about the `show usage-management` commands.

1.1.2.1 Auto-complete Commands

Type part of a CLI command, then press **Tab**. The system auto-completes the last word based on the letters you entered. You can do this for each word of a command. If the command takes a parameter, such as an enumerated value or a range of integers, the system lists the valid inputs.

1.1.2.2 Accessing Online Help

Online help is accessible via the '?' node provided by the CLI grammar and tab-complete. The system displays the online help for the command. For example, this CLI command displays the help for the `show system version` command.

```
show system version ?
```

If you want to use a literal question mark to set a configuration, and it is the only character at the end of the command, you must add the question mark with a backslash. For example:

```
set config my variable \?  
set config service message-broker max-connections \?
```



Note:

In cases where the displayed help text is too long, press **q** to return to the command line.

1.1.2.3 ID Parameters

Some commands have an ID parameter that applies the command upon a single instance of the information you request, such as a specific alarm model ID instead of all alarms. If you use an ID with a command, more detailed information is available.

1.1.2.4 Permissions

There are three levels of permission associated with CLI commands:

- **sv_operator**—Standard permission level with restricted ability to change the system
- **sv_service**—Standard permissions, with the ability to change some aspects of the system
- **sv_admin**—Full permissions to use any command and commit any changes through the CLI that the system allows

1.1.3 Output Filtering

To filter the output of any **show** command, run the command with a pipe character (**|**), a filter option and, in some cases, a regular expression to filter each line of output. The CLI allows only one level of filtering. You cannot use more than one pipe (**|**) symbol to string multiple filters together. The syntax is:

```
PTS> show <command> | {non-zero | include <regex> | exclude <regex> | begin <regex> | grep  
[-v] regex}
```

```
SRP> show <command> | {non-zero | include <regex> | exclude <regex> | begin <regex> | grep  
[-v] regex}
```

Where:

- **non-zero**—This is used for tables, specifies to only show output that has a value other than zero. You can optionally specify to filter non-zero output by column or row, so that either rows or columns that only contain zeroes are not output. This option does not take a regular expression.
- **include**—This specifies the inclusion of output matching the regular expression.
- **exclude**—This specifies the exclusion of output matching the regular expression.
- **begin**—This specifies to display the first line of output that matches the regular expression and also display all lines after the first matching line.
- **grep**—This searches for output that matches the regular expression, which is the same as using the include filter option. Using the **-v** option with **grep** has the same effect as using the exclude filter option.
- **regex**—This is the regular expression to search for. Do not enclose the regular expression in quotes or double quotes and do not include trailing white spaces as these are taken as part of the regular expression.

```
SDE> show <command> | begin <regex>  
SDE> show <command> | exclude <regex>  
SDE> show <command> | grep [-v] <regex>  
SDE> show <command> | include <regex>  
SDE> show <command> | non-zero
```

Filter	Description
begin	Displays all lines after and including the first that matches a regular expression.
exclude	Displays lines that do not match a regular expression.

Filter	Description
grep	Displays lines that match a regular expression, which is the same as using the <code>include</code> filter option. Using the <code>-v</code> option with <code>grep</code> has the same effect as using the <code>exclude</code> filter option.
include	Displays lines that match a regular expression.
non-zero	Displays only table columns and rows with at least one value other than zero. You can optionally specify to filter non-zero output by column or row, so that either rows or columns that only contain zeroes do not appear in the output. This option does not take a regular expression.

Press the **Tab** key after the pipe symbol (|) to display a list of the available commands.

You can use any alphanumeric character to create regular expressions. To use these special characters as single-character patterns, precede the character with a backslash (\). These characters have special meaning when used in a regular expression:

Character	Name	Description
.	Period	Matches any single character, including whitespace
*	Asterisk	Matches zero or more sequences of the pattern
+	Plus	Matches one or more sequences of the pattern
?	Question mark	Matches zero or one sequence of the pattern
^	Caret	Matches the beginning of the input string
\$	Dollar	Matches the end of the input string
_	Underscore	Matches a comma (,), left brace ({), right brace (}), left parenthesis, right parenthesis, the beginning of the input string, the end of the input string, or a space
[]	Square brackets	Designates a range of single-character patterns
-	Hyphen	Separates the end points of a range

1.1.4 Commands Entered Incorrectly

The CLI displays error messages for commands that you enter incorrectly.

This section contains these sub-sections:

- [Invalid Commands](#) on page 20
- [Invalid Configuration Value](#) on page 20
- [Permission denied](#) on page 20
- [Incomplete command](#) on page 20

1.1.4.1 Invalid Commands

When you run an invalid command, the CLI displays an error message and indicates the first invalid character with a caret symbol. For example:

```
PTS> show alarns
      ^
Invalid command
SRP> show alarns
      ^
Invalid command
SDE > show alarns
      ^
Invalid command
```

1.1.4.2 Invalid Configuration Value

While running the `set config` commands, if you provide a value that is not valid, an invalid command message appears at the first invalid character. For example:

```
PTS# set config interface vlan
Incomplete command, try one of:
<vlan-id-list-or-none>  A comma-separated or dash-separated list vlan id or none, e.g. 200,
or 200,201,202 or 200-202
PTS# set config interface vlan a
      ^
Invalid command.  Value must be a comma or dash-separated list of integers in the range 150 to
3499 or none, e.g. 200, or 200,201,202 or 200-202.

SRP# set config service database port
Incomplete command, try one of:
<int:0..>  Port to connect to the database
SRP# set config service database port a
      ^
Invalid command. Value must be a 32-bit integer.

SDE# set config service dhcp max-active-transactions abc
                                           ^
Invalid command. Value must be a 32-bit integer.
```

1.1.4.3 Permission denied

If the CLI command exists, but you do not have permission to run it, a permission denied message appears.

1.1.4.4 Incomplete command

If you run an incomplete CLI command, the system displays an error message and possible options to complete the command.

1.1.5 Waiting for Completion

Any command that requires services to start, stop, or restart has a "wait for completion" logic that shows the CLI is waiting for the service to achieve the requested state. A scrolling dot displays for every two seconds of elapsed time while waiting. The CLI will time out after 30 seconds for stops and 3 minutes for starts or restarts.

1.1.6 Configuration versus Operational show Commands

The CLI includes two different types of `show` commands: `show config` command and `show` command, both of which are supported for the same feature or subsystem.

It is important to understand the difference between the two, as they display different types of information.

show config

Shows global configurations for a feature or subsystem. You can display the full configuration or refine the command to display a configuration group or a single configuration parameter.

Run the `show config policy` CLI command to display the SandScript policy configuration. For example:

```
SDE> show config policy
measurements
  max-subscriber-instances: 32
publish
  max-published-expression-rows: 200
  max-published-expressions    : 200
tables
  maximum-total-rows: 100000000
  max-row-bytes      : 20000000000
subsystem
  events-per-second: 100000
```

Run the `show config service top-talker` CLI command to display the full Top Talkers configuration. For example:

```
SRP> show config service top-talker
enabled      : false
policy-file: /usr/local/sandvine/etc/policy.conf
transaction
  timeout: 1440
schedule: 0 0 0 * * ?
```

Run the `show config policy publish` CLI command to display the configured values for publishing SandScript. For example:

```
SDE> show config policy publish
max-published-expression-rows: 200
max-published-expressions    : 200
```

Run the `show config service top-talker transaction` CLI command to display the Top Talkers configured transaction settings. For example:

```
SRP> show config service top-talker transaction

timeout: 1440
```

Run the `show config policy publish max-published-expressions` CLI command to display a specific configured value for SandScript measurements and publishing. For example:

```
SDE> show config policy publish max-published-expressions
max-published-expressions: 200
```

Run the `show config service top-talker transaction timeout` CLI command to display a specific configured transaction timeout for a single execution of the Top Talker search. For example:

```
SRP> show config service top-talker transaction timeout
timeout: 1440
```

show command

Displays operational data, such as live statistical data for the feature or subsystem. For example:

```
SDE> show policy measurement

UNIQUE-BY    MEASUREMENTS
```

```
=====
Name           Instances Average Peak Units
-----
counterTier      0         0     1 [none]
```

SRP> show subscriber attribute-definitions

```
Name Audited Reported Visible Notifiable IpNotifiable
-----
abc  [true]  [false]  [true]  [true]    [true]
```

1.2 CLI Command Structure

The CLI provides a textual interface to view the operational metrics of Sandvine elements and to configure the system.

1.2.1 Command Class

The first word in a CLI command defines the command class.

Press the **Tab** key, at the CLI prompt, to view top-level command classes:

```
PTS>
?          Display online help
add        Add a user or some operational state
clear      Clear the terminal or a service
configure  Enter configuration mode
delete     Clear run-time state
edit       Edit a file
exit       Exit the CLI
history    Display command history
monitor    Auto-refreshing operational data
ping       Ping a host (send an ICMP echo request)
reboot     Reboot the system immediately
reload     Reload configuration and policy
restart    Restart a service or application
restore    Restore counters to pre-cleared values
set        Set an operational variable which typically triggers some actions
shell      Exit the CLI to the shell
show       Display operational data
shutdown   Shutdown the system immediately
start      Start a service or application
stop       Stop a service or application
techsupport Collect system/service level information useful for debugging this machine
traceroute Display the route packets take to reach a host

SRP>
?          Display online help
add        Add a row to a configuration table
clear      Clear the terminal or a service
commit     Commit configuration changes
delete     Delete a row from a configuration table
exit       Exit configuration mode without committing changes
history    Display command history
load       Load a previously saved configuration
ping       Ping a host (send an ICMP echo request)
reboot     Reboot the system immediately
reload     Reload configuration and policy
reset      Reset a configuration variable back to its default value
restart    Restart a service or application
```

```
save          Save the running configuration
set           Set a configuration variable
show          Show configuration
shutdown      Shutdown the system immediately
start         Start a service or application
stop          Stop a service or application
traceroute    Display the route packets take to reach a host

SDE>

?             Display online help
add           Add a user or some operational state
clear         Clear the terminal or a service
configure     Enter configuration mode
delete        Delete an operational record
exit          Exit the CLI
history       Display command history
monitor       Auto-refreshing operational data
reload        Reload configuration and policy
restore       Restore counters to pre-cleared values
set           Set an operational variable which typically triggers some action
show          Display operational data
techsupport   Collect system/service level information useful for debugging this machine
```

A command class has a descendant structure built on command foundations, attribute(s), and parameter(s).

In this document, each command class is in a section and special commands appear in separate sections. Special commands are not considered as command classes because they have no descendant commands.

1.2.1.1 Command Foundation

The command foundation is a minimum of one word at the CLI prompt that combines at least one attribute and resolves to a command, whether or not there are more optional attributes or parameters available.

Section	Description
Syntax	The syntax section lists all the variations of the command foundation with available attributes and parameters. For example: <pre>show alarms show alarms <id:0...> show alarms all show alarms history show alarms model <id:1...></pre>
Attributes	The CLI concatenates the attributes with the command foundation and lists them in a table.
Subattributes	The CLI concatenates the subattributes with the attributes and lists them in a table.
Parameters	The CLI concatenates parameters with attributes, sub-attributes, and other parameters and lists them in a table.
Output	The output section lists and defines the output columns that the command foundation provides.
Reference	The reference section provides references for terminology expressed in command output. This is usually in the form of: <ul style="list-style-type: none">• Request for Comments (RFC)• A Sandvine internal management information base (MIB)• An industry-standard specification



2

CLI Commands

- ["Management Commands" on page 25](#)
- ["Adding, Setting, and Deleting Users" on page 31](#)
- ["add/set/delete config" on page 32](#)
- ["Overview of clear commands" on page 40](#)
- ["delete subscriber ip" on page 42](#)
- ["delete service nat mappings all" on page 43](#)
- ["edit policy" on page 43](#)
- ["edit service ip-overload-management subnets" on page 43](#)
- ["edit system motd" on page 43](#)
- ["set config" on page 44](#)
- ["Operational set Commands" on page 83](#)
- ["monitor" on page 84](#)
- ["show" on page 88](#)

2.1 Management Commands

Management commands are those commands that operate without application specific parameters.

2.1.1 Waiting for Completion

Any command that requires services to start, stop, or restart has a "wait for completion" logic that shows the CLI is waiting for the service to achieve the requested state. A scrolling dot displays for every two seconds of elapsed time while waiting. The CLI will time out after 30 seconds for stops and 3 minutes for starts or restarts.

2.1.2 clear

Clears the terminal or a service.

```
clear
```

2.1.3 commit

Available only in configuration mode, this command commits configuration changes and initiates a reload, restart, or reboot (as required) to activate the changes.

```
commit
```



Note:

Running the `commit` command can impact service. Therefore, perform configuration changes during a maintenance window.

2.1.4 configure

Puts the CLI into configuration mode.

Only one user can enter configuration mode at a time.



Note:

The `configure force` command can forcefully expel another user if run by someone with administrative privileges.

2.1.5 edit

The edit command launches a text editor that allows you to modify text-based configuration files, such as the `policy.conf` file. Options include `edit` or `vi`.

These changes occur outside the standard CLI configuration mode. Changes to the text files takes place immediately when they are saved, but usually an `svreload` must take place before the changes take affect in operations.

2.1.6 exit

In configuration mode, this command returns the CLI to operation mode. In operational mode, this command exits the CLI.

```
exit
```

2.1.7 history

Lists the history of the commands that you executed with a timestamp for each command.

```
history
```

2.1.8 load config

Loads a previously saved local configuration.

This command is only available in configuration mode. The changes are pending until you run `commit` and can be seen by running `show config pending`. Any configuration changes made in the same session, before or after running the `load` command, overwrite the pending changes from the configuration file.

This command uses tab completion to show the available saved configuration names.

```
load config <configuration name>
```

2.1.9 ping

Used with IPv4 only, this command pings a specified host or IP address. Count is an optional integer that specifies the number of ping requests to send. This command sends ICMP echo requests to a specified destination.

```
ping <host> [count <count>]
```



Example:

```
PTS> ping localhost count 1
```

2.1.10 reboot

Reboots the system immediately.

You are prompted to confirm the reboot.

```
Confirm 'reboot'? (y/n):
```

2.1.11 reload

Although you can validate configurations with this command, you can also use it to reload configurations, SandScript, or maps.

```
reload
reload ip-overload-management-subnets
reload maps
```

```
reload validate
reload validate policy <file-path>
reload validate policy <file-path> subnets <file-path>
reload validate subnets <file-path>
reload validate subnets <file-path> policy <file-path>
```

Attribute	Description
ip-overload-management-subnets	Reloads AlwaysShuntIpList and NeverShuntIpList.
maps	Reloads maps.
validate	Validates a reload.
validate policy	Validates SandScript policy.
validate subnets	Validates subnets.

2.1.12 reload


Reloads configuration and policy.

```
reload
```

2.1.13 restart service

Runs the required command to restart the specified service. The service is stopped and then starts up again.

```
restart service cnd
restart service msd
restart service ptsd
restart service ptsm
restart service scdpd
restart service sfcd
restart service svbgpd
```

 **Note:** It is expected that when scdpd is restarted it may lead to dropped packets.

Service	Impact of restarting service...
ptsm	The element stops inspecting traffic and shunts traffic until the service restarts. During the restart short periods can pass where packets are dropped.
ptsd	The element stops inspecting traffic and shunts traffic until the service restarts. During the restart short periods can pass where packets are dropped.
cnd	<p>The element temporarily stops:</p> <ul style="list-style-type: none">• Mapping subscribers, but existing subscriber mappings remain active.• Sending statistics records. Any statistics that would have been transmitted to the SPB while cnd is down will be lost. This includes published expressions and other data available in NDS reports.• Dynamically adjusting shaping and session management rates. The element retains the last rate(s) from before the cnd was stopped. <p>If this element is the load-balancer master, the load-balancing state is cleared.</p>

Service	Impact of restarting service...
	Some, or all, dynamic shapers in the cluster will reset to the configured maximum rate.
scdpd	SNMP temporarily gets a timeout; the element doesn't send traps or poll values. The element cannot detect if an element is added to, or removed from, the cluster. Some cluster communication will work but not all.
sfcd	External data ports go down, and the element drops all traffic. Communication between the element and the cluster does not function. Traffic bound to this element from other elements in the cluster is shunted.
svbgpd	The BGP connection between the PTS and its neighboring router goes down while the service is down or is in the process of restarting. Any SandScript under evaluation against BGP attributes is not performed correctly during these times.

2.1.14 save config

Saves the running configuration. This command is only available in the configuration mode. The command creates a local backup of the current configuration, so that you can revert the changes, if required. The command does not save pending changes.

```
save config
save config <name>
```

Command	Description
save config	Saves the configuration with a date and timestamp. For example, 2012-08-02T10:45:26-0400.
save config <name>	Saves the configuration with a name you specify.

Run the `load config` command to revert to a saved configuration. This command supports tab completion and lists the available saved configurations. The command can take a few seconds to run. This command does not overwrite any changes that are pending in the session when you run the command.

2.1.15 shutdown

Shuts down the system immediately. The system halts and does not reboot.

2.1.16 start service

Run on of these commands to start the required service. All services start automatically when the system is started; you should only have to run these commands after administratively stopping a service.

```
PTS> start service

start service cnd
start service msd
start service ptsd
start service ptsm
start service scdpd
start service sfcd
start service svbgpd
```

Service	Impact of restarting service...
ptsm	The element stops inspecting traffic and shunts traffic until the service restarts. During the restart short periods can pass where packets are dropped.
ptsd	The element stops inspecting traffic and shunts traffic until the service restarts. During the restart short periods can pass where packets are dropped.
cnd	<p>The element temporarily stops:</p> <ul style="list-style-type: none"> Mapping subscribers, but existing subscriber mappings remain active. Sending statistics records. Any statistics that would have been transmitted to the SPB while cnd is down will be lost. This includes published expressions and other data available in NDS reports. Dynamically adjusting shaping and session management rates. The element retains the last rate(s) from before the cnd was stopped. <p>If this element is the load-balancer master, the load-balancing state is cleared. Some, or all, dynamic shapers in the cluster will reset to the configured maximum rate.</p>
scdpd	SNMP temporarily gets a timeout; the element doesn't send traps or poll values. The element cannot detect if an element is added to, or removed from, the cluster. Some cluster communication will work but not all.
sfcd	External data ports go down, and the element drops all traffic. Communication between the element and the cluster does not function. Traffic bound to this element from other elements in the cluster is shunted.
svbgpd	The BGP connection between the PTS and its neighboring router goes down while the service is down or is in the process of restarting. Any SandScript under evaluation against BGP attributes is not performed correctly during these times.

2.1.17 stop service

Run one of these commands to stop the required service. Many CLI commands will not work when any service is stopped.

```
PTS> stop service
```

```
stop service cnd
stop service msd
stop service ptsd
stop service ptsm
stop service scdpd
stop service sfcd
stop service svbgpd
```



Note:

It is expected that when scdpd is restarted it may lead to dropped packets.

Service	Impact of restarting service...
ptsm	The element stops inspecting traffic and shunts traffic until the service restarts. During the restart short periods can pass where packets are dropped.
ptsd	The element stops inspecting traffic and shunts traffic until the service restarts. During the restart short periods can pass where packets are dropped.

Service	Impact of restarting service...
cnd	<p>The element temporarily stops:</p> <ul style="list-style-type: none"> Mapping subscribers, but existing subscriber mappings remain active. Sending statistics records. Any statistics that would have been transmitted to the SPB while cnd is down will be lost. This includes published expressions and other data available in NDS reports. Dynamically adjusting shaping and session management rates. The element retains the last rate(s) from before the cnd was stopped. <p>If this element is the load-balancer master, the load-balancing state is cleared. Some, or all, dynamic shapers in the cluster will reset to the configured maximum rate.</p>
scdpd	SNMP temporarily gets a timeout; the element doesn't send traps or poll values. The element cannot detect if an element is added to, or removed from, the cluster. Some cluster communication will work but not all.
sfcd	External data ports go down, and the element drops all traffic. Communication between the element and the cluster does not function. Traffic bound to this element from other elements in the cluster is shunted.
svbgpd	The BGP connection between the PTS and its neighboring router goes down while the service is down or is in the process of restarting. Any SandScript under evaluation against BGP attributes is not performed correctly during these times.

2.1.18 techsupport

Collects logs and system information from a Sandvine element into a tarball, which you can send to Sandvine Customer Support or its authorized partner for analysis.



Note:

To run this command, you must log in as an administrative user.

In the default operating mode, the `techsupport` command collects the basic set of information that you or the support team need to debug most common issues. In default mode, the command completes in less than 5 minutes and does not impact service. While the command runs, it displays the completion percentage. When the command completes, it displays the output file destination.

The element automatically removes output files from the destination directory after 3 days, therefore you should copy the files to another location.

```
techsupport
techsupport extended
techsupport extended private
techsupport extended verbose
techsupport extended verbose private
techsupport private
techsupport verbose
techsupport verbose private
```

Attribute	Description
extended	Collects an extended set of data. This mode usually takes 30 minutes to complete, but can complete anywhere in the range of 10 minutes to 2 hours. This mode can impact service.
private	Masks information such as configurable IP addresses, usernames, and passwords.
verbose	Displays the commands that are running and any error messages encountered during the process.

2.1.19 traceroute

Used with IPv4 only, traces the route or routes against or to a specified host or IP address. This command prints the route that packets take to the specified destination and provides information on bad transport.

```
traceroute <host>
```

2.1.20 update

Runs the svupdate command to install or upgrade software.

```
update  
update uri <uri>
```

Where <uri> specifies an alternate site. Useful when the files to install are already downloaded.

2.1.21 set user default-shell

This a CLI command is used by an administrative user to change their default shell. Can be used by an administrative user to change any user's default shell.

```
set user default-shell <bash|cli>
```

```
set user <name> default-shell <bash|cli>
```

Attribute	Description
default-shell <bash cli>	The default shell to use for new terminal sessions.


2.2 Adding, Setting, and Deleting Users

This section describes the CLI commands used to create, set, and delete a user on the system.

2.2.1 add user

Creates a new user on the system and assigns them to the specified group. The group determines the user's permissions on the system.

```
add user <name> group <admin|service|operator>
```

 **Note:**
To run this command, you must log in as a root user.

Attribute	Description
user	The name of the user.
group	The group to assign this user to. Possible values include:

Attribute	Description
	<ul style="list-style-type: none">admin—This is the highest privilege level and gives administrative users full access. These users can start or stop any application and edit files.service—Service users can start or stop some applications and edit run-time configuration files.operator—Operators have read-only privileges for accessing log files.

2.2.2 set user

This command allows users and administrators to set or configure items such as password. Administrative users have access to all the user accounts and they can set passwords for everyone.

```
set user password
set user <name> password
set user <name> default-shell
```

Attribute	Description
password	This is used to set your password.
<name> password	This is used when an administrator changes or sets password for another user.
default-shell	Set the default shell for a specific user.
bash cli	The default shell to use for new terminal sessions.

2.2.3 delete user

This command deletes the specified user.

```
delete user <name>
```



Note:

To run this command, you must log in as a root user.

2.3 add/set/delete config

The add/set/delete configuration commands are used with configuration tables.

Each row of the table is one set of configurations. The row key is a unique identifier for the row, which could be an IP address or a unique ID. The row key is a mandatory parameter.

You must be in configuration mode to run these commands.

2.3.1 add/set/delete config interface mac-ip-mapping

This command adds or deletes IP/port mappings.

```
add/set/delete config interface mac-ip-mapping <mac> ip <ip> interface <port>
```

Option	Description
mac	Must be a valid MAC address.
ip	Must be a valid IPv4 address.
interface	Must be a service, switch, divert, or cluster interface.

2.3.2 add/set/delete config service bgp peer

These commands configure the BGP peers.

2.3.2.1 add config service bgp peer

Adds a BGP peer configuration to a table of BGP peer configurations.

```
add config service bgp peer <ipv4-address> as <int:0..65535>
add config service bgp peer <ipv4-address> as <int:0..4294967295> port <int:0..65535>
add config service bgp peer <ipv4-address> as <int:0..4294967295> port <int:0..65535> password
  <password>
add config service bgp peer <ipv4-address> as <int:0..4294967295> port <int:0..65535> password
  <password> hold-time <int:3..65535>
add config service bgp peer <ipv4-address> as <int:0..4294967295> port <int:0..65535> password
  <password> hold-time <int:3..65535> priority <<int:0..65535>
```

You must specify a value for every non-optional parameter. The IP address for the peer is the unique identifier for the row.

Parameter	Description
peer	The IP address of the router. This must be unique among all rows. Required. Takes an IPv4 address only.
as	BGP AS number of the connected peer router. Required.
port	The port the router is listening on. Optional. Default is 179.
password	The peer's MD5 password. Optional. Default is none.
hold-time	The maximum number of seconds that may elapse between the receipt of successive KEEPALIVE and/or UPDATE messages from the sender. Set to 0 if no hold-time is to be used in BGP sessions. Optional.
priority	The route-selection priority to assign to this peer. Optional. Where 1 is highest priority and 65534 is the lowest. Set to 0 to use the IP address. By default a random priority is assigned to the peer based on its IP address. The lower the IP address, the lower the priority value.

2.3.2.2 set config service bgp peer

Adds to or alters the BGP peer router configuration created with the `add config service bgp peer <ip-address>` CLI command.

```
set config service bgp peer <ipv4-address> as <int:0..4294967295>
set config service bgp peer <ipv4-address> port <int:0..65535>
```

```
set config service bgp peer <ipv4-address> password <password>
set config service bgp peer <ipv4-address> hold-time <int:3..65535>
set config service bgp peer <ipv4-address> hold-time <int:3..65535> priority <int:0..65535>
```

Attribute	Description
peer	The IP address of the router. Acts as the identifier for this BGP peer's configuration. Takes an IPv4 address only.
as	The BGP AS number.
port	The port the router is listening on.
password	The peer's MD5 password
hold-time	If KEEPALIVE or UPDATE messages from the peer are not detected within this time (in seconds), the connection will be reestablished. Set to 0 for no timeout.
priority	The route-selection priority to assign to this peer. Optional. Where 1 is highest priority and 65534 is the lowest. Set to 0 to use the IP address. By default a random priority is assigned to the peer based on its IP address. The lower the IP address, the lower the priority value.

2.3.2.3 delete config service bgp peer

Deletes a BGP peer configuration. Takes an IPv4 address that is a row key into the BGP peer configuration table. This command deletes the row from the table.

```
delete config service bgp peer <ip-address>
```

2.3.3 add/set/delete config policy divert vlan

This group of commands configures divert using VLANs.

Using Sandvine **divert** policy action, selected traffic can be redirected for targeted advertising, caching (both HTTP and P2P), and URL filtering.

2.3.3.1 add config policy divert vlan

Adds a divert action configuration to a table of divert actions.

```
add config policy divert vlan <int:150..3499> ip-address <ip-address> mask <ip-address>
```

You must specify a value for every non-optional parameter. The VLAN tag is the unique identifier for the row.

Attribute	Description
vlan	VLAN tag. This must be unique among all rows. Required.
ip-address	The IP address of the management interface
mask	IP address mask

2.3.3.2 set config policy divert vlan <vlan>

Adds to or alters a row of the divert action table configuration created with the `add config policy divert vlan` CLI command.

```
set config policy divert vlan <int:150..3499> ip-address <ip-address>
set config policy divert vlan <int:150..3499> mask <ip-address>
```

2.3.3.3 delete config policy divert vlan

Deletes a divert action configuration.

Takes a VLAN tag that is a row key into the divert action configuration table. This command deletes the row from the table.

2.3.4 add/set/delete config policy vlan-label

These commands configure labels for VLAN numbers.

2.3.4.1 add config policy vlan-label

Creates an association between a VLAN number and a VLAN name

```
add config policy vlan-label <vlan-label> vlan-number <int:150..3500>
```

Parameter	Description
vlan-label	A symbolic representation of the VLAN number over which to send diverted traffic. Use a <code>vlan_label</code> when different elements in a cluster are executing the same policy but wish to use different VLANs for diverted traffic. The maximum number of VLANs that can be configured is 400.
vlan-number	The number over which to send diverted traffic. There are no defaults.

2.3.4.2 set config policy vlan-label

Modifies an association between a VLAN number and a VLAN name created using the `add config policy vlan-label` command.

```
set config policy vlan-label <vlan-label> vlan-number <int:150..3500>
```

2.3.4.3 delete config policy vlan-label

Deletes the label for a previously configured VLAN number.

```
delete config policy vlan-label <vlan-label>
```

2.3.5 add/set/delete config service protocol voip provider

Sandvine provides a list of recognized VoIP providers. This group of commands configure additional VoIP service providers.

2.3.5.1 add config service protocol voip provider

Adds a new VoIP provider to the list of recognized providers.

```
add config service protocol voip provider <name> uri <uri>
```

Attribute	Description
name	The name of the VoIP provider.
uri	The URI for the VoIP provider. Can use a regular expression for character matching.

2.3.5.2 set config service protocol voip provider

Changes the URI of an existing provider that was added using the `add config service protocol voip provider <name> uri <uri>` CLI. Default providers cannot be changed.

```
set config service protocol voip provider <name> uri <uri>
```

2.3.5.3 delete config service protocol voip provider

Deletes the specified VoIP provider that was added using the CLI. Default providers cannot be deleted.

```
delete config service protocol voip provider <name>
```

2.3.6 add/set/delete config service session-qualifier bridge-group

These commands configure bridge-group traffic mapping for session-qualifiers.

2.3.6.1 add config service session-qualifier bridge-group

Creates a row in the bridge-group to site mapping table. This command assigns a mapping for traffic entering the PTS through a particular bridge-group to a configured site number. The PTS, when receiving a packet through the specified bridge-group, maps it to a site number and uses it to uniquely identify subscriber traffic throughout the Sandvine system.

While the bridge-group number is specific to the local PTS, it can be enforced by any PTS in the cluster. Therefore, if a packet is originally received on bridge-group 2 of PTS A, but is balanced to PTS B for processing, it will still be processed under the site assigned to PTS A, bridge-group 2. Note that bridge-group rules take precedence over VLAN-tag rules, so if you have a flow which matches both a bridge-group-based site rule, and a VLAN-based site rule, the bridge-group-based rule is applied.

```
add config service session-qualifier bridge-group <int:1..16> site <int:1..2147483647>
```

Attribute	Description
bridge-group	A valid bridge-group ID is a number from 1-16. It directly maps onto the bridge groups configured using <code>set config interface <interface-id> bridge-group <id></code> .
site	The site number.

2.3.6.2 set config service session-qualifier bridge-group

Modifies a row in the bridge-group to site mapping table. The bridge-group must reference a configuration previously created with the `add config service session-qualifier bridge-group` command.

```
set config service session-qualifier bridge-group <int:1..16> site <int:1..2147483647>
```

2.3.6.3 delete config service session-qualifier bridge-group

Deletes a bridge-group mapping. This command deletes the row from the table.

```
delete config service session-qualifier bridge-group <int:1..16>
```

2.3.7 add/set/delete config service session-qualifier s-vlan

These commands configure mapping an 802.1ad QinQ nested VLAN tag to a site number to be used with session qualifiers.

add config service session-qualifier s-vlan

Assigns a mapping from a particular pair of QinQ nested VLAN tags (as seen on a packet entering the PTS) to a configured site number. The PTS, when receiving a packet with the given QinQ VLAN tags, translates this tag pair to a site-number and uses it to uniquely identify subscriber traffic throughout the Sandvine system.

```
add config service session-qualifier s-vlan <int:0..4095> c-vlan <int:0..4095> site  
<int:0..2147483647>
```

This command is used to configured in site-number mode. See [set config service session-qualifier mode](#) on page 68 for more information.

Attribute	Description
s-vlan	802.1ad QinQ service VLAN tag of the tag pair that is to be mapped to the provided site number. Specifying 0 is equivalent to "no service tag." Specifying the keyword "any" is permitted, and wildcards the service tag.
c-vlan	802.1Q client VLAN tag of the tag pair that is to be mapped to the provided site number. Specifying 0 is equivalent to "no client tag." Specifying the keyword "any" is permitted, and wildcards the client tag.
site	The site number used to qualify all traffic that arrives in the provided vlan.



Note:

Only one of s-vlan or c-vlan is specified as "any", not both. This allows a single rule to apply to every client vlan within a given service vlan, or every service vlan with a given client vlan. When rules containing "any" are present, packets are matched in this priority order:

1. If both service VLAN id and client VLAN id exactly match a rule, use that rule.
2. If the service VLAN id matches a rule with client VLAN "any", use that rule.
3. If the client VLAN id matches a rule with service VLAN "any", use that rule.

2.3.7.1 set config service session-qualifier s-vlan

Modifies an existing entry in the QinQ VLAN mapping table. See also `add config service session-qualifier s-vlan`.

2.3.7.2 delete config service session-qualifier s-vlan

Removes an entry from the QinQ VLAN mapping table.

```
delete config service session-qualifier s-vlan <row> c-vlan <row>
```

2.3.8 add/set/delete config service session-qualifier vlan

These commands configure mapping a VLAN tag to a site number to be used with session qualifiers.

2.3.8.1 add config service session-qualifier vlan

Assigns a mapping from a particular VLAN tag (as seen on a packet entering the PTS) to a configured site number. The PTS, when receiving a packet with the given VLAN tag, translates this tag to a site-number and uses it to uniquely identify subscriber traffic throughout the Sandvine system.

```
add config service session-qualifier vlan <int:0..4095> site <int:0..2147483647>
```

This command is to be used when configured in site-number mode. See [set config service session-qualifier mode](#) on page 68.

Attribute	Description
vlan	VLAN tag that to be mapped to the provided site number.
site	The site number used to qualify all traffic that arrives in the provided vlan.

2.3.8.2 set config service session-qualifier vlan

Modifies an existing entry in the VLAN mapping table. See also `add config service session-qualifier vlan`.

2.3.8.3 delete config service session-qualifier vlan

Removes an entry from the VLAN mapping table.

2.3.9 add/set/delete config service tunneling

This group of commands configure how tunneled traffic is handled.

2.3.9.1 add config service tunneling mpls

Configures how MPLS encapsulated traffic is handled.

```
add config service tunneling mpls rule <int:16..1048575> type <inner|outer> action  
<shunt|discard|ip|eompls>
```

The rule ID is the unique identifier for the row.

Parameter	Description
rule	The MPLS label. This must be unique among all rows. Required.
type	The MPLS label type
action	The action to apply to the MPLS label

2.3.9.2 add config service tunneling vlan

Configures how VLAN-tagged traffic is handled.

```
add config service tunneling vlan rule <int:1..4095> depth <int:1..8> action <shunt|discard|ip>
```

The rule ID is the unique identifier for the row.

Parameter	Description
rule	The VLAN tag. This must be unique among all rows. Required.
depth	The depth of the VLAN tag
action	Action to apply to the VLAN tag

2.3.9.3 delete config service tunneling

Deletes a row from the tunneling configuration table.

```
delete config service tunneling vlan rule <row> depth <depth>  
delete config service tunneling mpls rule <row> type <type>
```

2.3.10 add/set/delete config system log remote-server

These commands configure whether or not logs are sent to a remote server.

2.3.10.1 add config system log remote-server

Adds the configuration that sends logs to a remote server.

```
add config system log remote-server <server>[:<port>] type <alarms|snmp|svlog>
```

The IP, port, and type uniquely identifies the row.

Attribute	Description
remote-server	IPv4 address or hostname of the remote server; with an optional port number (default 514).
type	<p>These types are available:</p> <ul style="list-style-type: none">alarms—Sends a human-readable version of SNMP notifications to a remote server. Each message consists of the alarm model name and number, and a description.snmp—Sends SNMP notifications to a remote server as syslog messages, using the format defined in RFC 5675.svlog—Sends svlog messages to a remote server in addition to the local file <p>Note: SNMP and alarm severities map to the syslog priorities outlined in section 2 of RFC 5674.</p>

2.3.10.2 set config system log remote-server

Modifies the configuration created using the `add config system log remote-server` command.

```
set config system log remote-server <server>[:<port>] type <alarms|snmp|svlog>
```

2.3.10.3 delete config system log remote-server

Deletes the configuration that sends log messages to a remote server.

```
delete config system log remote-server <server>[:port] type <alarms|snmp|svlog>
```

2.3.11 add/set/delete service udp-prioritization prioritized-port

The group of commands configure the UDP prioritization matching rules.

2.3.11.1 add config service udp-prioritization prioritized-port

This command adds a new UDP prioritization matching rule. These rules are uniquely identified using the prioritized UDP port number.

```
add config service udp-prioritization prioritized-port <int:1..65535> priority <int:0..7>
```

Parameter	Description
prioritized-port	This is the internet-side UDP port whose matching packets are set to the given priority.
priority	The Assigned priority of the UDP port.

2.3.11.2 set config service udp-prioritization prioritized-port

This command modifies the rule created using the " add config service udp-prioritization prioritized-port" command.

```
set config service udp-prioritization prioritized-port <already created prioritized-port number>
priority <new priority>
```

2.3.11.3 delete config service udp-prioritization prioritized-port

This command deletes rules that the add config service udp-prioritization prioritized-port command creates.

```
delete config service udp-prioritization prioritized-port <already created prioritized-port
number>
```

2.4 Overview of clear commands

The clear suite of commands clears aggregated data and services from the Sandvine environment.

When these clear commands are called:

```
clear alarms bridge-group
clear alarms counters
clear alarms ip-overload-management ip-shunt-failure
```

they set up a checkpoint so that subsequent calls to the same command are measured relative to the previous call to clear.

2.4.1 clear alarms bridge-group

Forcibly clears all inline bridge-group alarms. If a defect persists then an alarm is triggered again.

2.4.2 clear alarms counters

Forcibly clears all threshold-based alarms.

```
clear alarms counters
```

2.4.3 clear alarms ip-overload-management

Clears active IP overload management alarms.

```
clear alarms ip-overload-management ip-shunt-failure
```

Attribute	Description
ip-shunt-failure	Forcibly clears the abusive IPs shunt failure alarm (model 134)

2.4.4 clear interface counters

Resets the counters used by `show interface counters` to zero. Use this command to analyze traffic or troubleshoot the system.

2.4.5 clear policy controller key-translation cache

Clears the name-to-ID mapping stored in Quality Guard that is obtained using the ID allocation subsystem. Once this is cleared, any name translation requires a message to the SPB requesting an ID corresponding to the name.

```
clear policy controller key-translation cache
```

2.4.6 clear service bgp routing-table

Discards the existing BGP routing table. The table will be reconstructed by the BGP service as it gathers information from the AS peers.

2.4.7 clear service ip-overload-management interval-stats

Resets all of the IP overload management request interval counters to zero. The interval counters are incremental counts that are initialized to zero whenever the system is started. The counts are reset to zero when cleared by this command. Use this command in conjunction with the `show ip-overload-management stats` command.

2.4.8 clear service ip-overload-management subnet

Clears subnets dynamically shunted by IP overload management.

```
clear service ip-overload-management subnet <ip-address-or-all>
```

Attribute	Description
subnet	An IPv4 or IPv6 address. To clear all subnets, enter "all".

2.4.9 clear service load-balancer

Clears the current state of the load balancer.

This command only applies to centralized load balancing and can only be run from the element that is elected as the load balancing master. If centralized load-balancing is configured the `show config service load-balancer mode` command will return "policy". For more information about load-balancing see the *PTS Network Configuration Guide*.

2.4.10 clear service protocol voip unknown-providers

VoIP providers are identified by matching a certain tag in the VoIP packet with a list of regular expressions. If a regular expression matches against the packet, the corresponding call is attributed to the provider.

In the event that the provider tag within the packet does not match a regular expression, that is to say a known provider, the provider tag substring is stored on the PTS. A provider logged to the unknown list can be made known by adding a regular expression that matches the unknown text and the name of the provider to the configuration. In the event that unknown providers remain in the system, this command clears the list.

2.4.11 clear service subscriber-management

Clears the cached subscriber and IP-assignment records from the network element.

2.5 delete subscriber ip

Deletes a mapped subscriber by IP address from the PTS. If traffic is still flowing for the IP addresses that were unmapped, the PTS quickly looks these mappings up once again.

```
delete subscriber ip <strict-ip-address>
delete subscriber ip <strict-ip-address> port <int:0..65535>
delete subscriber ip <strict-ip-address> site-number <site:0..>
```

Attribute	Description
ip	User-specified IP address (IPv4 format only).
port	The port number for which to show subscriber information.
site	Session qualifier site number to use for lookup of subscriber session. Default is 0.

Output	Description
IpAddress IP	Address assigned.
PrefixLength	Size of the IP prefix of the assignment.
Name	The subscriber's name.
Status	[deleting] - The element is attempting to delete this subscriber.
NetworkClass	Network class of the IP address, as defined in subnets.txt.
PolicyClass	Policy class of the IP address, as defined in subnets.txt.
Module	Processing module on which this IP assignment is active.
SiteNumber	Session qualifier site number of the displayed session.
Session ID	Unique identifier of this session in the sandvine system.

2.6 delete service nat mappings all

Clears the cached NAT mappings from the current element. Afterward, any active traffic for removed mappings will cause lookup requests to be sent to the SPB and may cause NAT mappings to be recreated.

```
delete service nat mappings all
```

2.7 edit policy

Edits `/usr/local/sandvine/etc/policy.conf` or `/usr/local/sandvine/etc/subnets.txt` files. These commands start either vi or edit, depending on the configuration of the CLI or editor. When specifying a policy file name, press TAB for the system to list out the available files.

```
edit policy
edit policy <policy-file>
edit policy subnets
```

For example, if the `policy.conf` file contains

```
include "/usr/local/sandvine/etc/policy.talktalk.conf"
```

and you execute `edit policy <TAB>` it would return:

```
PTS> edit policy

<ENTER>      Run the specified command
?            Display online help for the specified command
subnets      Edit the subnets.txt file
              Edit an included policy or map file
/usr/local/sandvine/etc/policy.talktalk.conf

PTS>
```

2.8 edit service ip-overload-management subnets

Launches a text editor so you can edit the files that determine which (if any) subnets are always or never shunted during overload conditions by the IP overload management feature if it is enabled.

The default editor can be configured using the `set config cli text-editor` command.

The files contain a list of subnet definitions, in CIDR notation, one per line. Comments are preceded by #.

```
edit service ip-overload-management subnets always-shunt
edit service ip-overload-management subnets never-shunt
```

2.9 edit system motd

The message-of-the-day or MOTD displays when a user logs into the system. This message can consist of any message network operators want to display at log in.

```
edit system motd
show system motd
```

The `edit system motd` command launches a text editor with which to edit the message-of-the-day. The `show system motd` command shows the message contents immediately.

2.10 set config

The `set config` commands are used to configure the system and are only available in configuration mode. Additional configuration commands are available under `add config`.

2.10.1 set config cli prompt

Configures the prompt shown by Sandvine's CLI.

You can configure the prompt to contain these special character patterns, which are substituted with the corresponding values:

- `%h`—A short version of the host name of the machine
- `%H`—The full host name of the machine
- `%u`—The user name
- `%g`—The group to which the user belongs
- `%p`—The name of the platform

For example, given a user named Pat, committing this command on a PTS: `set config cli prompt "%u on a %p"` changes the CLI prompt to be: `Pat on a PTS`.

For example, given a user named Pat, committing this command on the SDE: `set config cli prompt "%u on an %p"` changes the CLI prompt to be: `Pat on an SDE`.

```
set config cli prompt <prompt>
```

2.10.2 set config cli session-limit

Configures the maximum number of concurrent active CLI sessions. The range is 1 to 1000 and the default is 10.

```
set config cli session-limit <int:1..1000>
```

2.10.3 set config cli text-editor

Configures the text-editor to use when editing files through the CLI.

```
set config cli text-editor <vi|edit>
```

Attribute	Description
text-editor	The text-editor to use. Can be one of: <ul style="list-style-type: none">• <code>vi</code>—To use the vi editor (the default)• <code>edit</code>—To use the easy editor (the UNIX text-based command-line editor)

2.10.4 set config cluster

Configure the cluster compatibility version in a PTS contributing to cluster.



Warning:

Committing the `set config cluster compatibility version` command requires SFCD restart. Changing the cluster sub-name will restart SFCD automatically, but all other changes require a PTS reload to restart SFCD.

```
set config cluster compatibility version <1|2>
```

```
set config cluster name <name>
```

```
set config cluster log-default
```

```
set config cluster stat-name <stat-name>
```

```
set config cluster sub-name <sub-name>
```



Note:

You can validate some of your SPB configurations with these commands:

- In case of a configured SPB cluster, make sure that you first run these commands on the domain manager node. Run the `show config cluster domain-manager` CLI command to find the node that is designated as the domain-manager:
- In case of a new SPB cluster configuration, run the `set config cluster domain-manager <ip-address>` CLI command to set the domain manager and then run the other commands:
- When compatibility version 2 is set, you need to configure the internal-service IP.

Attribute	Description
compatibility version	Configures the PTS to use a different IP subnet for internal service (PTS to PTS) and external service (PTS to non-PTS) traffic.
log-default	Enable/disable the logging of statistics and heartbeats when the system is configured with the default cluster name.
name	Group PTS elements by name.
sub-name	Elements are considered local to one another if they are in the same sub-cluster.
stat-name	The name used to represent the cluster when writing stats.

Attribute	Description
domain-manager	IP of the domain manager message broker.
name	The cluster name of the SPB servers.
servers	Space separated list of server IP addresses in the cluster. Use this configuration on a database-only server.

2.10.5 set config deployment mode

Configures the PTS's deployment mode.

```
set config deployment mode <inline|offline>
```

The PTS can be deployed in these modes:

- inline - the PTS is deployed between communicating network devices and intersects the data flow.
- offline - the PTS is deployed outside the path of the data flow and is provided a copy of the data passing between the communicating network devices.

Committing this change requires restarting PTSM, PTSD and SFCD.

See the *PTS Network Configuration Guide* for more information.

2.10.6 set config files

Configures the location of files.

```
set config files policy <file|url>
set config files remote-config <url>
set config files subnets <file|url>
```

Attribute	Description
policy	Configures the location of the policy file. Command takes either a file name or a URL that points to the policy.conf file. The default path is /usr/local/sandvine/etc/policy.conf.
remote-config	Configures the location of the remote configuration file.
subnets	Configures the location of the subnets file. Command takes either a filename or a URL that points to subnets.txt. The default location is /usr/local/sandvine/etc/subnets.txt

2.10.7 set config interface <cluster-interface>

```
set config interface <cluster-interface> alias <alias>
set config interface <cluster-interface> auto-negotiation <all|disabled>

set config interface <cluster-interface> bridge-group <bridge-group-or-none>

set config interface <cluster-interface> divert-vlan <vlan-id-list-or-none>

set config interface <cluster-interface> enabled <true|false>

set config interface <cluster-interface> external-service-tagged <true|false>

set config interface <cluster-interface> function
<none|subscriber|internet|cluster|service|switch|divert>

set config interface <cluster-interface> mac-logging-enabled <true|false>

set config interface <cluster-interface> link-aggregation-group <int:1..8|none>

set config interface <cluster-interface> link-group <link-group-or-none>

set config interface <cluster-interface> speed-duplex
<10-full-duplex|100-full-duplex|10-half-duplex|100-half-duplex>
```

```
set config interface <cluster-interface> vlan-port-id <port-vlan-or-none>
```

```
set config interface <cluster-interface> vlan-priority <vlan-priority-or-none>
```

Alias: Provides a non-volatile handle for the interface that is displayed in the MIB, on SNMP walks, and by the `show interface configuration` CLI command.

Attribute	Description
interface	The interface to configure in the form n-n. For example: 1-1.
alias	An alias for the interface. Defaults to a zero length string. The maximum length is 64 characters and any character is valid.

Auto-negotiation: Configures the interface to auto-negotiate the media type.

Attribute	Description
interface	The interface to configure. May be a cluster or data interface in the form n-n. For example: 1-1.
auto-negotiation	The type of auto-negotiation, including: <ul style="list-style-type: none">all - Enables auto-negotiation on copper and fiber.disabled - Disables auto-negotiation on copper and fiber.

Bridge-Group: Configures an interface to a specific user-defined bridge group

Parameter	Description
interface	The interface to configure in the form n-n. For example: 1-1.
bridge-group	The ID of the bridge group. Set this to "none" to unset the bridge-group.

Divert-vlan: Sets the VLANs that will be on each port for interfaces with a function divert. This CLI command is intended for use on a PTS where multi-divert is configured. Multi-divert is not supported on the PTS 8210.

Attribute	Description
interface	The data interface to configure in the form n-n. For example: 1-1.
divert-vlan	A comma- and/or hyphen-separated list of VLAN IDs or none. For example: <ul style="list-style-type: none">200,201,202200-202200,202,205-207 The PTS supports VLAN tags in the range of 150-3500, and a maximum of 400 VLAN tags. Set this to "none" to unset all divers.

Enabled: Enables an interface.

Attribute	Description
interface	The interface to configure in the form n-n. For example: 1-1.
enabled	True to enable the interface; false to disable it

External-service-tagged: Used to enable external service vlan tagging on service and switch interfaces.

Attribute	Description
false true	Whether traffic is tagged with external-service VLAN on this port.

Function: Configures the function of the interface. Some interfaces only allow a sub-set of the full list of functions. For example, data-only interfaces can only be configured with function subscriber or internet.

Parameter	Description
interface	The interface to configure in the form n-n. For example: 1-1.
function-type	<p>The function options are:</p> <ul style="list-style-type: none"> • subscriber - interface is used to intersect data traffic, facing subscribers; in other words the interface's Rx is upstream traffic. • internet - interface is used to intersect data traffic, facing the internet; in other words the interface's Rx is downstream traffic. • cluster - interface is connected to another PTS element in a cluster. • service - interface is connected to a non-PTS service device (such as OCS, SRP). Spanning-tree is disabled. • switch - interface is connected to a non-PTS service device (such as OCS, SRP). Spanning-tree is enabled. • divert - interface is connected to a third-party divert host. • none - interface is not used. An interface cannot be enabled if the function is none. Use when transitioning an interface between functions.

Mac-logging-enabled: To enable or disable the logs for MAC movement on external non-data ports. You can view this log file using the `show log mac-movement` CLI command.

Attribute	Description
interface	The external non-data port can be in the form of n-n or lag-n for example 1-1 or lag-2.
mac-logging-enabled	Status of the mac-logging, true means logging is enabled and being captured, false means logging is disabled and no logs are being captured.

Link-Aggregation-Group

Enables up to two Link Aggregation Groups (LAG) on a specified interface

Set the link-aggregation-group ID to none to disable LAG on a port. For example:

```
set config interface 1-5 link-aggregation-group none
```

Link-Group

Configures the link-group of the data or cluster interface.

Speed-Duplex: Configures the speed for the interface. Valid on PTS 14000 only.

Parameter	Description
interface	The interface to configure. May be a cluster or data interface in the form n-n. For example: 1-1.
speed-duplex	<p>Speed/duplex if auto-negotiation is disabled on 1421x/1451x. Can be one of:</p> <ul style="list-style-type: none"> • 10-full-duplex - sets the speed to 10 megabit duplex. • 10-half-duplex - sets the speed to 10 megabit half-duplex. • 100-full-duplex - sets the speed to 100 megabit duplex. • 100-half-duplex - sets the speed to 100 megabit half-duplex.

Vlan-port-id: Configures a VLAN ID for this port.

Parameter	Description
interface	The interface to configure in the form n-n. For example: 1-1.
vlan-port-id	The VLAN ID. To unset the VLAN ID, set to none. For example: set config interface 1-1 vlan-port-id none

Vlan-priority: Configures the VLAN priority for this port.

Parameter	Description
interface	The interface to configure in the form n-n. For example: 1-1.
vlan-priority	The VLAN priority of the port. To unset the VLAN priority, set to none. For example: set config interface 1-1 vlan-priority none

2.10.8 set config interface <data-interface>

```
set config interface <data-interface> alias <alias>
set config interface <data-interface> auto-negotiation <all|disabled>
set config interface <data-interface> bridge-group <bridge-group-or-none>
set config interface <data-interface> enabled <true|false>
set config interface <data-interface> function
<none|subscriber|internet|subscriber-internet|cluster|service|switch|divert>
set config interface <data-interface> layer3-hairpin-mac <mac-address-or-none>
set config interface <data-interface> link-group <link-group-or-none>
set config interface <data-interface> npu <npu>
set config interface <data-interface> npu-link <0|1|auto>
set config interface <data-interface> shunt-tos <shunt-tos-or-none>
set config interface <data-interface> vlan-port-id <port-vlan-or-none>
set config interface <data-interface> vlan-priority <vlan-priority-or-none>
```

Alias: Provides a non-volatile handle for the interface that is displayed in the MIB, on SNMP walks, and by the show interface configuration CLI command.

Attribute	Description
interface	The interface to configure in the form n-n. For example: 1-1.
alias	An alias for the interface. Defaults to a zero length string. The maximum length is 64 characters and any character is valid.

Auto-negotiation: Configures the interface to auto-negotiate the media type.

Attribute	Description
interface	The interface to configure. May be a cluster or data interface in the form n-n. For example: 1-1.

Attribute	Description
auto-negotiation	The type of auto-negotiation, including: <ul style="list-style-type: none">all - Enables auto-negotiation on copper and fiber.disabled - Disables auto-negotiation on copper and fiber.

Bridge-Group: Configures an interface to a specific user-defined bridge group.

Parameter	Description
interface	The interface to configure in the form n-n. For example: 1-1.
bridge-group	The ID of the bridge group. Set this to "none" to unset the bridge-group.

Enabled: Enables an interface.

Attribute	Description
interface	The interface to configure in the form n-n. For example: 1-1.
enabled	True to enable the interface; false to disable it

Function: Configures the function of the interface. Some interfaces only allow a sub-set of the full list of functions. For example, data-only interfaces can only be configured with function subscriber or internet.

Parameter	Description
interface	The interface to configure in the form n-n. For example: 1-1.
function-type	The function options are: <ul style="list-style-type: none">subscriber - interface is used to intersect data traffic, facing subscribers; in other words the interface's Rx is upstream traffic.internet - interface is used to intersect data traffic, facing the internet; in other words the interface's Rx is downstream traffic.cluster - interface is connected to another PTS element in a cluster.service - interface is connected to a non-PTS service device (such as OCS, SRP). Spanning-tree is disabled.switch - interface is connected to a non-PTS service device (such as OCS, SRP). Spanning-tree is enabled.divert - interface is connected to a third-party divert host.none - interface is not used. An interface cannot be enabled if the function is none. Use when transitioning an interface between functions.

Layer3-hairpin-mac: Configures the destination MAC address for a hairpin deployment of the PTS in which the network device is a layer 3 device, such as a router.

Parameter	Description
interface	The interface to configure in the form n-n. For example: 1-1.
mac	The destination MAC address. Set to 'none' to unset the MAC address.

Link-Group

Configures the link-group of the data or cluster interface.

NPU/NPU-link: Configures the NPU or NPU-link to assign the data interface to. Valid for PTS 22000 and 24000 only.

Parameter	Description
list	The interface to configure
npu	The NPU to assign the interface to. Defaults to auto.
npu-link	The NPU link to assign the interface to. Defaults to auto.

Shunt-tos: Configures the PTS to shunt packets with the given TOS marker. Shunted traffic passes through the PTS with no inspection, no actions performed, and no statistics collected.

Attribute	Description
interface	The interface to configure in the form n-n. For example: 1-1.
tos-id-list	A comma- or hyphen-separated list of TOS values to shunt, or none. For example, 100 or 100,101,150. Set to "none" to unset the list.

Vlan-port-id: Configures a VLAN ID for this port.

Parameter	Description
interface	The interface to configure in the form n-n. For example: 1-1.
vlan-port-id	The VLAN ID. To unset the VLAN ID, set to none. For example: <code>set config interface 1-1 vlan-port-id none</code>

Vlan-priority: Configures the VLAN priority for this port.

Parameter	Description
interface	The interface to configure in the form n-n. For example: 1-1.
vlan-priority	The VLAN priority of the port. To unset the VLAN priority, set to none. For example: <code>set config interface 1-1 vlan-priority none</code>

2.10.9 set config interface address-tracking

Configures sanity checking on port and subnets configuration.

```
set config interface address-tracking enabled <false|true>
set config interface address-tracking network-mask width ipv4 <int:0..32>
set config interface address-tracking network-mask width ipv6 <int:0..128>
```

Output	Description
enabled	Enables or disables tracking of external addresses on internal ports.
network-mask width ipv4	Configures the net mask size when aggregating IPv4 IPs. The default is 24.
network-mask width ipv6	Configures the net mask size when aggregating IPv6 IPs. The default is 56.

2.10.10 set config interface <interface> media

Sets the interface media type for interfaces that have a fiber port and a copper port (for example, ports 2-3 through 3-9 on PTS 1421x, 1451x). Valid for PTS 14000 only.

```
set config interface <interface> media <copper|fiber|auto>
```

Parameter	Description
interface	The interface to configure in the form n-n. For example: 1-1.
media	Can be one of: <ul style="list-style-type: none">copper - a copper media typefiber - a fiber media type. Takes priority over copper.auto - the media type is detected automatically. The PTS selects the media type based on the presence of a signal.

2.10.11 set config interface <interface> shunt-tos

Configures the PTS to shunt packets with the given TOS marker. Shunted traffic passes through the PTS with no inspection, no actions performed, and no statistics collected.

```
set config interface <interface> shunt-tos <shunt-tos-or-none>
```

To unset all shunt-tos, set to none. For example:

```
set config interface 1-1 shunt-tos none
```

Attribute	Description
interface	The interface to configure in the form n-n. For example: 1-1.
tos-id-list	A comma- or hyphen-separated list of TOS values to shunt, or none. For example, 100 or 100,101,150.

2.10.12 set config interface bridge-group monitoring

The PTS can be configured to monitor the received and transmitted data rates on every configured bridge-group, triggering an alarm if the ratio of data transmitted over the data received is below a certain threshold. Not valid for PTS 8210 only.

```
set config interface bridge-group monitoring alarm-threshold <float:0..0.99>
```

```
set config interface bridge-group monitoring enabled <true|false>
```

```
set config interface bridge-group monitoring failure-threshold <int:1..100>
```

```
set config interface bridge-group monitoring min-rx-threshold <int:0..>
```

```
set config interface bridge-group monitoring period <int:1..3600>
```

**Note:**

Changing this configuration will likely interrupt traffic for any existing bridge groups being modified.

Attribute	Description
alarm-threshold	The transmit-to-receive threshold for the alarm.
enabled	Enables or disables bridge-group monitoring.
failure-threshold	Number of consecutive failed intervals before the alarm is triggered. A failed interval is an interval where the transmit to receive ratio does not meet the threshold, and the amount of received data is greater than the minimum received threshold. Defaults to 3.
min-rx-threshold	Minimum amount of received data (in bytes) required over a given sample interval. This threshold prevents the alarm from triggering during installation or startup conditions. Defaults to 100000.
period	Alarm threshold is checked this often (in seconds). Defaults to 5.

2.10.13 set config interface bypass

Configures the bypass settings for the interface. The bypass module causes all traffic to bypass the PTS. No inspection or policies are applied.

```
set config interface bypass external admin-status <active|bypass|down|software>
set config interface bypass external description <description>
set config interface bypass external comm-port <com1|com2>
set config interface bypass <list> admin-status <active|bypass|software>
set config interface bypass software-timeout <int:1600..3200>
set config interface bypass sticky <true|false>
```

Where <list> is the index of the bypass group.

Attribute	Description
admin-status	<ul style="list-style-type: none"> active - The PTS only drops into bypass mode when power is lost. Other system failures, such as an upgrade or component failure, do not result in the PTS dropping into bypass mode. bypass - This causes all traffic to bypass the PTS; no inspection or policies are applied. down - This is the default mode and, when configured, indicates that the bypass is disabled. software - The bypass module will flip into bypass mode upon power loss, component failure, or system unresponsiveness. Bypass mode is not activated for a software upgrade or in case of link failure.
description	The description of the external bypass chassis, in a quoted string.
comm-port	The serial port used to communicate with the external bypass.
software-timeout	Bypass software watchdog timeout in milliseconds. Valid values are in the range 1600 - 3200. The default is 3200.
sticky	Configures software bypass mode to remain in effect until it is manually removed. True to enable bypass stickiness; false (the default) to disable.

2.10.14 set config interface cluster vlan external-service

This command is used to set external service Vlan on the cluster interface

```
set config interface cluster vlan external-service
set config interface cluster vlan external-service enabled
```

Attribute	Description
false true	Configure the external-service VLAN on all cluster ports.

Reset command

```
reset config interface cluster vlan external-service enabled
```

**Note:**

If external-service vlan is disabled on cluster port in cluster compatibility version 1 then PTS cluster will not form and cluster will form in cluster compatibility version 2.

2.10.15 set config interface external-service ip-address primary

Configure the IP Address for the External-Service interface. External-Service interface is used to send external service traffic. When cluster compatibility version '1' is selected, cluster traffic uses External-Service Interface. The cluster will not form if each PTS does not have its appropriate service interface in the same subnet.

Use this command to change or verify the IP address assigned to the external-service interface (cluster compatibility version is 1). For example:

```
set config interface external-service ip-address primary 1.0.0.1/8
```

You must enter the IP address in CIDR format. To clear the IP address, enter the keyword 'none'.

**Note:**

You cannot use the chosen IP address on any other interfaces in the system.

Attribute	Description
External-service	External service interface. It is used to transmit/receive the external service traffic. In cluster compatibility version 1 it is also used for internal service traffic.
Primary	Configures the primary IPV4 address for the interface.
IP Address	The IP Address in CIDR notation that is X.Y.Z.W/mask OR none.

2.10.16 set config interface internal-service ip-address primary

Configures the IP Address for Internal-Service interface. Internal-Service interface is used to send cluster traffic to other elements in the cluster when compatibility version 2 is selected.

Use this command to change or verify the IP address assigned to the internal-service interface (cluster compatibility version is 2). For example:

```
set config interface internal-service ip-address primary 2.0.0.1/8
```

You must enter the IP address in CIDR format and can enter none to reset the IP address to none.

Attribute	Description
Internal-service	Internal service interface. It is used to transmit or receive the internal service traffic in cluster compatibility version 2.
Primary	Configures the primary IPV4 address for the interface.
IP Address	The IP Address in CIDR notation i.e. X.Y.Z.W/mask or none.

2.10.17 set config interface internal-routeability

This command chooses whether the diameter traffic from the PPU's is sent out of the management port, or the external service port.

```
set config interface internal-routeability enabled <true|false>
```

Attribute	Description
true false	Enable/disable cluster interface internal routeability. If false – management port If true – external service port

2.10.18 set config interface link-group

Configures link group properties.

```
set config interface link-group <int:1..16> enabled <true|false>
```

```
set config interface link-group <int:1..16> online-delay <int:0..60>
```

Attribute	Description
link-group	The link group ID.
enabled	True to enable the link group, false to disable it.
online-delay	Delay between receiving carrier sense and turning on transmitter.

2.10.19 set config interface management redundancy

Configures how link redundancy is handled on the platform.

```
set config interface management redundancy protocol <none|failback>
```

```
set config interface management redundancy primary <mgmt1|mgmt2>
```

Attribute	Description
protocol	Configures link redundancy. Set to failback to enable the hardware to failover to a secondary link. Set to none to disable this feature. Default is none.
primary	If link redundancy is enabled, configures which port is to be used for primary communication. Default is mgmt1.

2.10.20 set config interface max-inspect-frame-size

Sets the maximum inspected packet size. The PTS shunts without inspection packets with a frame size larger than the configured maximum.

```
set config interface max-inspect-frame-size <int:1518..1980>
```

Committing this change requires restarting the SFCD.

2.10.21 set config interface <lag-interface>

To enable or disable the logs for MAC movement on external non-data ports. You can view this log file using the `show log mac-movement` CLI command.

```
set config interface <port> mac-logging-enabled  
set config interface <port> mac-logging-enabled <true|false>
```



Note:

If an interface for example; ports 1-10 is already assigned to a LAG, then enabling the mac-logging for port 1-10 does not have any impact. Mac logs for the ports 1-10 are not visible because, it is part of a LAG.

Attribute	Description
interface	The external non-data port can be in the form of n-n or lag-n for example 1-1 or lag-2.
mac-logging-enabled	Status of the mac-logging, true means logging is enabled and being captured, false means logging is disabled and no logs are being captured.

2.10.22 set config interface mac-logging-rate

To configure the rate at which logs are recorded and stored. Logs are stored at the rate of logs/sec.

```
set config interface mac-logging-rate 1001
```

Attribute	Description
mac-logging-rate	Configure the rate at which MAC movement logs are captured on external non data interfaces.

2.10.23 set config interface spanning-tree cst bridge-priority

This command lets you change the CST bridge priority of the PTS. You can also set the priority as primary or secondary, where primary makes the PTS the root of the CST. Bridge priority input can take values from 0 to 61440, in steps of 4096.

```
set config interface spanning-tree cst bridge-priority <primary|secondary|bridge-priority>
```

Attribute	Description
CST	Configure parameters for Common Spanning Tree protocol
Bridge-priority	0 to 61440 in steps of 4094. Primary is special bridge priority value(0), which increases the probability of PTS to become CST root.

Attribute	Description
	Secondary is special bridge priority value(16384), which will reduce probability of PTS to become root of CST

reset-config-interface-spanning-tree-cst-bridge-priority

This command lets you reset the CST bridge priority of the PTS. The default value is 32768.

2.10.24 set config interface trunk-distribution

Sets the trunk distribution algorithm for cluster interfaces. You must first configure the cluster interfaces in link aggregation groups for the trunk distribution algorithm to have effect on the interfaces.

```
set config interface trunk-distribution <trunk-distribution-method>
```

Trunk distribution ensures that for any particular flow, all packets use the same port, so that packet order is guaranteed to be preserved.



Note:

All elements within a cluster must be configured to the same mode.

Set trunk-distribution to one of:

- `simple` - PTS hashes the destination module number to distribute data traffic across cluster interfaces.
- `sv-mpls` – PTS hashes the source and destination IPs in the packet and applies an MPLS label to each packet. The PTS uses the hash value in this MPLS label to distribute traffic across cluster interfaces.

2.10.25 set config interface vlan

Configures VLAN(s) allowed by cluster interfaces.

```
set config interface vlan <vlan-id-list-or-none>
```

Accepts a comma-separated or dash-separated list of VLAN IDs or none. For example 200, or 200,201,202 or 200-202.

To unset the VLAN IDs, set to none. For example:

```
set config interface vlan none
```

2.10.26 set config network-protection

Configuration related to network protection.

```
set config network-protection dns outstanding-sessions-period <int:1..30>
set config network-protection email-alert rate-limit <int:0..>
set config network-protection email-alert rate-period <int:1..>
set config network-protection email-alert report-server <server>
set config network-protection max-actions <int:0..>
set config network-protection max-ports-per-smtp-host <int:0..>
set config network-protection max-smtp-hosts <int:0..>
set config network-protection minimum-rule-priority <int:0..>
set config network-protection mitigation enable <false|true>
```

Parameter	Description
dns outstanding-sessions-period	The number of seconds after which a DNS session is considered outstanding.
rate-limit	The maximum number of emails that can be sent in rate-period seconds.
rate-period	The period, in seconds, in which a maximum of rate-limit emails can be sent.
report-server	The report server the PTS will notify to send the email alerts (usually the Network Demographics Server).
max-actions	The maximum number of mitigation actions to be implemented per module. Default is 1000.
max-ports-per-smtp-host	The maximum number of ports per SMTP host to be monitored for spam. Default is 5.
max-smtp-hosts	The maximum number of SMTP hosts for which spam detection will track and maintain mitigation state. Default is 7500.
minimum-rule-priority	Rules with a priority that is greater than or equal to this value will be active.
mitigation enable	Enables or disables the deployment of mitigation actions.

2.10.27 set config policy arp interval

Configures the period, in seconds, in which PTS will send ARP requests for IP addresses on the service network.

```
set config policy arp interval <int:1..600>
```

set config policy

Attributes	Description
arp	Configuration related to determining next hop and ethernet address
destination	Configuration related to policy destinations
divert	Configuration related to the divert action
ipv6	Configuration related to unique by IPv6 clauses
measurement	Configuration related to policy measurements
optimization	Configuration related to policy optimization
session-management	Configuration related to session management
table	Configuration related to policy tables
vlan-label	Create an association between a VLAN number and a VLAN name

2.10.28 set config policy destination file default-path

Configures the directory where capture files are stored. The packet capture files are specified in SandScript policy with the keywords `destination "<name>" file`. The value must start with `/d2/var/captures/` and must contain only alphanumeric characters, `'_'`, `'/'` or `'.'`. It must not exceed 64 characters.

```
set config policy destination file default-path <default-path>
```

2.10.29 set config policy divert max-divert-errors

Configures the maximum number of current errors a divert destination may accumulate before PTS sets the destination operation status as down.

Divert destination's current error count increases when it fails to respond to TCP handshake. In addition, the current error count increases if the divert host modifies data that had already been received by the endpoint.

Divert destination's current error count is decreased when PTS successfully connects with the divert host.

```
set config policy divert max-divert-errors <int:0..>
```

Attribute	Description
max-divert-errors	The maximum number of current errors a divert destination may accumulate. The default value is 20.

2.10.30 set config policy ipv6 hash-mask

This command provides a means of fine tuning the uniqueness calculation when unique by IPv6 is used.

```
set config policy ipv6 hash-mask <strict-ipv6-address>
```

Attribute	Description
<strict-ipv6-address>	IPv6 address.



Note:

Unique-by clause holding IPv6 addresses may not guarantee uniqueness.

2.10.31 set config policy measurement max-subscriber-instances

Configures the maximum number of unique-by subscriber measurements published to the SPB for reporting purposes. The default is 64.

Note that each measurement can have thousands of instances. Increasing the amount of measurements published results can result in an increase in the amount of system resources used.

```
set config policy measurement max-subscriber-instances <int:32..128>
```



Note:

Each incremental 32 sum classifiers, or 6 peak classifiers published by a network element requires an additional full database row to store. Consequently, if a single network element, publishes 66 sum classifiers and 8 peak classifiers, 3 total database rows are created. Additional database rows will result in increased storage, report processing duration,

memory and CPU requirements. If the number of additional rows required exceeds the maximum record writing threshold, the SPB can no longer summarize data in a timely manner which results in a system outage.

2.10.32 set config policy optimization flow-statistics

Enables or disables optimization of measurements based on flow-statistics.

```
set config policy optimization flow-statistics <true|false>
```

2.10.33 set config policy session-management

Configuration related to session management.

```
set config policy session-management next-hop-router <ip-address>
```

```
set config policy session-management offline enabled <true|false>
```

Parameter	Description
next-hop-router	The IP address of the next-hop router.
enabled	Enables or disables off line session management

2.10.34 set config policy shaper burst-absorption scaling-factor

This command defines the percentage of modules that will see bursts within the level distribution interval.

```
set config policy shaper burst-absorption scaling-factor <n>
```

2.10.35 set config policy shaper shape-traffic-before-recognition

When this command is set to **true**, SandScript shapes all traffic, regardless of whether the protocol is detected.

```
set config policy shaper shape-traffic-before-recognition <true|false>
```

2.10.36 set config policy table max-row-bytes

Configures the maximum amount of memory that can be used for policy table data, per row, in bytes.

```
set config policy table max-row-bytes <int:0..>
```

Parameter	Description
max-row-bytes	The maximum amount of memory in bytes

2.10.37 set config service bgp

Configures the Border Gateway Protocol (BGP) service.

The BGP service gathers information about external IP routing and enables policy decisions on a per packet basis that consider the route the packet will take after it heads upstream from the PTS.

```
set config service bgp 4byte-as enabled <true|false>
set config service bgp as-path-limit <int:1..255>
set config service bgp enabled <true|false>
set config service bgp holdoff <int:10..300>

set config service bgp local-as <local-as>
set config service bgp local-id <ipv4-address>
set config service bgp peering-lost-timeout <int:30..9000>
set config service bgp rib-memory-limit <int:1..300>

set config service bgp route-retention enabled <true|false>
set config service bgp route-retention timeout <int:1..>
set config service bgp subnet-limit <int:1..10000000>
```

Attribute	Description
4byte-as	Configures whether or not the PTS will use 4 byte AS numbers and advertise them through policy and subnets.txt. Note: Changing whether 4-byte AS numbers are enabled can drop and reset peer connections. You will receive a confirmation message through the CLI before proceeding.
enabled	Enables or disables the BGP service. Set to true to enable the BGP service, false to disable it. BGP service is disabled by default. Committing changes to this command requires restarting the BGP daemon.
local-as	Local Autonomous System (AS) number of BGP connection to peer router. Note: Changing the AS will drop and reset peer connections. You will receive a confirmation message through the CLI before proceeding.
local-id	Sets the IP address of the interface connected to the BGP peer(s). The routing information from the peer is obtained over this interface. The command takes an IPv4 address only. Note: Changing the local-id will drop and reset peer connections. You will receive a confirmation message through the CLI before proceeding.
route-retention enabled	Configures the BGP service to retain subnets when a peer fails. Set this to true to enable route-retention, false to disable it. If not specified, the default (route-retention) is enabled.
route-retention timeout	Configures the timeout for the BGP service route-retention. Default is 7200 seconds (2 hours).
subnet-limit	Maximum number of subnets tracked. Default on a PTS 24000 or PTS 22000 is 10,000,000 and on a PTS 14000 the default is 100,000.
as-path-limit	Maximum number of AS numbers retained from an update packet. If a packet contains more than the maximum configured number of AS numbers, the information in it will be ignored. Committing a change that increases the limit causes the PTS to drop the peer connections and then reconnect.

Attribute	Description
peering-lost-timeout	Wait time (in seconds) after total peer connectivity is lost before another BGPD will be elected as master. Default is 600 seconds or 10 minutes.
rib-memory-limit	Maximum allowable Routing Information Base (RIB) memory in MB.
holdoff	The time to wait for BGP updates for specified AS, in seconds.

2.10.38 set config service control-center authentication

Configures user authentication for Control Center. The element authenticates requests that Control Center sends to make sure that the users who are logged into Control Center have the proper credentials to interact with the element.

```
set config service control-center authentication cache-time <int:0..>  
set config service control-center authentication enabled <true|false>
```

Attribute	Description	Default
cache-time	Configures the amount of time for which to cache the result of the local authentication. Caching the result improves performance and avoids placing a heavy load on centralized authentication servers. The value is in seconds.	3600 secs
enabled	Enables or disables local authentication. Generally, you do not need to use this command , except in cases where the element uses a multifactor authentication scheme (such as RSA SecurID) and passwords work only once or expire after a short duration.	false

2.10.39 set config service diameter connection ip-dscp

This command configures the Differentiated Services Code Point (DSCP) value used for diameter traffic originating from the PTS. This value ensures the Quality of Service (QoS) for diameter traffic.

```
set config service diameter connection ip-dscp <int:0..63>
```

Where `ip-dscp` is the DSCP value to use in the IP header of Diameter packets.

2.10.40 set config service diameter messages pts application-common

This command configures messages that the Diameter stack processes. Diameter messages enable SandScript decisions in the PTS to take into account information about per-subscriber account status and service plans.

```
set config service diameter messages pts application-common max-blocked-messages-per-session
```

```
set config service diameter messages pts application-common max-avp-instances
set config service diameter messages pts application-common max-message-size
set config service diameter messages pts application-common retransmission-interval
set config service diameter messages pts application-common retransmission-attempts
set config service diameter messages pts application-common retransmission-attempts incoming
set config service diameter messages pts application-common retransmission-attempts peer-failover

set config service diameter messages pts application-common retransmission-attempts
session-tracking
```

Attribute	Description
max-blocked-messages-per-session	Maximum number of Diameter messages that the Diameter stack can queue while awaiting an answer for a pending request
max-avp-instances	Maximum number of instances that the Diameter stack allows for an AVP in SandScript
max-message-size	Maximum size of a Diameter message
retransmission-interval	Timeout in milliseconds before the Diameter stack resends an outgoing request message as an outgoing retransmitted message (in cases where the Diameter stack does not receive a corresponding answer/error message)
retransmission-attempts	Maximum number of outgoing retransmitted messages that the Diameter stack sends if it does not receive a corresponding incoming answer/error message
incoming	Incoming request, answer, error, or retransmitted message
peer-failover	Peer failover if a secondary peer is configured and the primary peer is unavailable, according to RFC3539
session-tracking	When enabled, the Diameter stack blocks outgoing request messages if it sent another outgoing request message with the same session-id and did not receive a corresponding message

2.10.41 set config service id-allocation

Configures the ID allocation subsystem. Corresponding `show config` and `reset config` commands are also available.

```
set config service id-allocation batch-interval <int:1..>
set config service id-allocation latency-histogram-lookback <int:1..>
set config service id-allocation max-batch-size <int:1..1000>
set config service id-allocation max-retry-attempts <int:1..20>
set config service id-allocation policy-to-subsystem-queue-size <int:1..>
set config service id-allocation retry-interval <int:1..>
set config service id-allocation retry-queue-size <int:1..>
set config service id-allocation subsystem-to-policy-immediate-queue-size <int:1..>
set config service id-allocation subsystem-to-policy-queue-size <int:1..>
```

Parameter	Description	Default
batch-interval	The interval (in milliseconds) that the subsystem waits before sending a bulk request to the SPB.	20 milliseconds
latency-histogram-lookback	The time (in seconds) for which the subsystem retains the latency histogram.	1000 seconds
max-batch-size	The maximum number of requests that the subsystem processes simultaneously and sends to the SPB. The maximum value is 1000.	1000
max-retry-attempts	The maximum number of retries that the subsystem attempts for completing an action. The maximum number of attempts is 20.	3
policy-to-subsystem-queue-size	The size of the queue containing SandScript action requests between the policy engine on the SDE and the subsystem.	100000
retry-interval	The interval (in minutes) that the subsystem waits before resending an action that had failed previously because the SPB was not working.	1 minute
retry-queue-size	The size of the queue holding requests that the subsystem has to resend to the SPB.	10000
subsystem-to-policy-immediate-queue-size	The size of the queue between the subsystem and the policy engine on the SDE, returning completed events for records that failed.	100000
subsystem-to-policy-queue-size	The size of the queue between the subsystem and the policy engine on the SDE returning the completed events.	100000

2.10.42 set config service ip-overload-management

IP-overload management bypasses the inspection of flows that are overwhelming the switch fabric or modules of the PTS.

When the PTS internal switch fabric is overloaded by a huge amount of traffic from a single IP address, packet drops may occur. This is called a packet drop event. If a small number of IPs are producing the excess traffic, use IP-overload management to tune the performance of the PTS.

```

set config service ip-overload-management abusive-ip-threshold bytes <int:1000000..>
set config service ip-overload-management abusive-ip-threshold flows <int:1..>
set config service ip-overload-management abusive-ip-threshold packets <int:100..>
set config service ip-overload-management always-shunt file <file|url>
set config service ip-overload-management always-shunt limit <0..250>
set config service ip-overload-management concurrent-flows bins <int:0..50000000>
set config service ip-overload-management concurrent-flows enabled <true|false>
set config service ip-overload-management concurrent-flows limit <int:0..100000000>
set config service ip-overload-management drop-detection-interval <int:500..5000>
set config service ip-overload-management drop-threshold <int:1..1400000>
set config service ip-overload-management dynamic-shunt limit <0..250>
set config service ip-overload-management enabled <none|high-usage|shunting|full>
set config service ip-overload-management evaluation-interval <int:1..10>
set config service ip-overload-management holdoff-interval <int:1..10>
set config service ip-overload-management max-shunted-ips-per-violation <int:1..250>
set config service ip-overload-management never-shunt file <string>
set config service ip-overload-management never-shunt log-abusive <true|false>
set config service ip-overload-management shunt-time <int:20..2419200>

```

Attribute	Description
abusive-ip-threshold bytes	Configures the threshold of bytes per evaluation-interval for an IP being labeled abusive. Default is 6,000,000 bytes per evaluation-interval.
abusive-ip-threshold flows	Configures the threshold of flows per evaluation-interval for an IP being labeled abusive. Default is 100 flows per evaluation-interval.

Attribute	Description
abusive-ip-threshold packets	Configures the threshold of packets per evaluation-interval for an IP being labeled abusive. Default is 5000 packets per evaluation-interval.
always-shunt file	Configures the location of the text file containing the subnets to always shunt. Default is <code>/usr/local/sandvine/etc/staticShuntSubnets.txt</code> .
always-shunt limit	Maximum number of subnets which can be always shunted.
concurrent-flows bins	Number of distinct bins (buckets) to use for tracking flow usage per IP address.
concurrent-flows enabled	Whether the element will track the number of flows per internal IP address.
concurrent-flows limit	Maximum number of flows managed per internal IP address.
drop-detection-interval	Configures the interval at which packet drops are detected and IP-management is triggered. Works in conjunction with drop-threshold to define an average drop rate (threshold in packets divided by this interval). Default is 2000 milliseconds.
drop-threshold	The packet-drop threshold used to determine whether to trigger a shunt event. Default is 50 packets. When IP overload management is enabled, if the number of flows for a subscriber IP address exceeds the configured limit, no further flows are created. The excess packets are shunted without protocol recognition, policy or counting. However, shunted traffic is included in overall interface byte and packet counts.
dynamic-shunt limit	Configures the maximum number of dynamically shunted IPs. Default is 250.
enabled	Enables or disables subcomponents of the IP Overload Management service. Options are: <ul style="list-style-type: none"> <none> - disables the service. <high-usage> - detects and displays abusive IPs based on the threshold criteria, but disables the component that performs shunting. Use this mode to help identify if IP overload management is required. <shunting> - allows specifying subnets that the IP overload management feature will statically shunt, and/or never shunt; detecting abusive IPs is disabled. Note that inclusion of a subnet in the never-shunted subnets file does not prevent an IP from within the subnet from being shunted for other reasons. For example, <code>set interface shunt true</code> will still shunt packets whose IPs are contained within a never-shunt subnet. <full> - abusive IPS are detected, displayed, and you can specify IPs to always-shunt or never-shunt.
evaluation-interval	Configures the period over which drop conditions are evaluated and traffic is shunted. If packet drops continue to exceed the threshold after this amount of time, then the PTS will reevaluate the abusive IPs that need to be shunted and shunt. Default is 3 seconds.
holdoff-interval	Minimum hold-off interval in seconds between successive overload management requests on an individual processing module. Default is 3 seconds.
max-shunted-ips-per-violation	Configures the number of IPs to be dynamically shunted due to a drop event. Default is 10.
never-shunt file	Configures the location of the text file containing the subnets to never shunt. Default is <code>/usr/local/sandvine/etc/neverShuntSubnets.txt</code>
never-shunt log-abusive	Enables logging for abusive IPs that are in the list of subnets to never shunt. Default is false.
shunt-time	Configures the length of time for which the PTS will dynamically shunt IPs. Default is 1800 seconds. The maximum number of seconds is equal to four weeks.

2.10.43 set config service ip-overload-management alarms

Configures alarm behavior for IP overload management.

```
set config service ip-overload-management alarms ips-dynamically-shunted clear-threshold <int:0..249>
set config service ip-overload-management alarms ips-dynamically-shunted enabled <true|false>
set config service ip-overload-management alarms ips-dynamically-shunted threshold <int:1..250>
set config service ip-overload-management alarms ip-shunt-failure enabled <true|false>
set config service ip-overload-management alarms ip-shunt-failure threshold <int:1..2000>
```

Attribute	Description
ips-dynamically-shunted clear-threshold	Alarm will be cleared when the number of dynamically shunted IPs goes below this value
ips-dynamically-shunted enabled	Enables or disables the dynamically shunted IPs alarm. Default is true.
ips-dynamically-shunted threshold	Alarm will be raised when the number of dynamically shunted IPs exceeds this value
ip-shunt-failure enabled	Enables or disables the abusive IP shunt failure alarm. Default is true.
ip-shunt-failure threshold	Alarm will be raised when the number of consecutive IP shunt failures exceeds this value

2.10.44 set config service load-balancer

Distributes traffic across processing modules in the system.

```
set config service load-balancer failure-recovery-level <high|low|medium>
set config service load-balancer hashing-width <8|12>
set config service load-balancer inspection-delay <int:5..600>
set config service load-balancer ipv4 hashing-window <int:0..32>
set config service load-balancer ipv6 hashing-window <int:32..64>
set config service load-balancer layer2-mode <mapping|tunneling>
set config service load-balancer mode <static|ip-hash|policy>
```

The bit subset of the IP address, positioned by the hashing-window, selects the bits which are used to distribute subscriber IP addresses to different modules in the system. Selecting the bits that are least correlated with geography will result in the most even distribution of processing requirements in the PTS or cluster. In general, for IPv4, these are the least significant bits of the address, and for IPv6, the least significant bits of the subscriber prefix, but may vary depending on the network configuration.

The default width of the hashing window varies according to the hardware platform:

Platform	Load balancer hashing width
PTS14000	8 bits
PTS22000	12 bits
PTS24000	12 bits

Using a 12-bit hashing window on the PTS 22000 and 24000 platforms increases the efficiency of the PTS cluster, however, you can use the `set config service load-balancer hashing-width 8` command to revert to the 8-bit hashing window. This command is only available on the PTS 22000 and 24000.

Committing changes to these commands requires restarting SFCD:

- `set config service load-balancer ipv4 hashing-window <int:0..32>`
- `set config service load-balancer ipv6 hashing-window <int:32..64>`
- `set config service load-balancer layer2-mode <mapping|tunneling>`

Attribute	Description
failure-recovery-level	The amount of state that is replicated by the master load balancer.
hashing-width	For PTS 22000 and 24000 only. Sets the width of the hashing window. The default is 12 bits.
inspection-delay	The amount of time, in seconds, that the load-balancer is delayed before inspection.
ipv4 hashing-window	Specify an offset of which bits to use for the module balancing hash. The bit position, within the IP address, of the least significant bit of the multi-bit hash window, numbered such that bit 1 is the most significant bit of the IP address. The default is 32, meaning the least-significant bits are used. The range of the hashing window is validated based on the configured hashing width.
ipv6 hashing-window	Specify an offset of which bits to use for the module balancing hash. The bit position, within the IP address, of the least significant bit of the multi-bit hash window, numbered such that bit 1 is the most significant bit of the IP address. The default is 64, meaning the least significant bits of the 64-bit prefix are used. The range of the hashing window is validated based on the configured hashing width.
layer2-mode	The layer 2 mode of transmitting data traffic to and from inspection modules. Can be one of: <ul style="list-style-type: none"> • mapping - the default, the PTS maps external MACs to its own internal MAC addresses for switching inside the PTS switch fabric. • tunneling - all packets are encapsulated in a tunnel inside the PTS.
mode	Sets how the load balancer distributes traffic. Can be one of: <ul style="list-style-type: none"> • static - Balancing is achieved using 12 or 8 bits of the subscriber IP address (usually the least-significant bits). • ip-hash - Balancing is achieved using 8 bits of the subscriber IP address, as above, but the balancing decision is done centrally. • policy - A load-balancing policy is defined to group the incoming traffic into bundles (this can be based on IP address, subscriber ID, or subscriber attribute) and each bundle is assigned to a module. Further information about bundles is available in the <i>SandScript Configuration Guide</i>.

2.10.45 set config service nat enabled

Indicates to the element whether it should maintain a cache of NAT mappings, and perform public to private IP conversions before looking up subscribers.

`set config service nat enabled <false|true>`

2.10.46 set config service protocol

Enables or disables protocol recognition for the specified protocol.

```
set config service protocol tcp enabled <true|false>
set config service protocol udp enabled <true|false>
set config service protocol voip enabled <true|false>
```

2.10.47 set config service protocol flow reassembly

Configures the number of buffers used in applying recognition of flows. The buffers are used to store packet data from the flows so that further analysis can be done.

```
set config service protocol flow reassembly large-buffers <int:64..256>
set config service protocol flow reassembly medium-buffers <int:256..1024>
set config service protocol flow reassembly small-buffers <int:8192..32768>
```

2.10.48 set config service session-qualifier cluster-number

Sets the static number that identifies this cluster when the PTS is in cluster-number qualifier mode.

```
set config service session-qualifier cluster-number <int:0..2147483647>
```

You must run this command on every element in the cluster, because every PTS in a cluster should have the same cluster number. Defaults to 0. See also [set config service session-qualifier mode](#) on page 68.

2.10.49 set config service session-qualifier mode

Sets the PTS mode for qualifying traffic and subscriber mappings.

```
set config service session-qualifier mode <none|cluster-number|site-number>
```

Where mode is one of:

- none - The PTS does not use session-qualifiers. To be used when the PTS does not receive overlapping IPv4 addresses.
- cluster-number - The PTS qualifies all flows and subscriber sessions with a constant integer cluster-number. Use when the PTS deployment has overlapping IP addresses, but each PTS cluster individually sees no overlapping IP addresses. In this type of deployment, many PTS clusters are connected to a single SPB datahome, and each cluster may see a set of IP addresses that overlap with the IP addresses from a different cluster.

When this mode is selected, each cluster of PTS elements must be given a unique site number through this command: [set config service session-qualifier cluster-number](#) on page 68 and [add/set/delete config service session-qualifier s-vlan](#) on page 37.

- site-number - The PTS qualifies flows and subscriber sessions by a calculated site number. Use when the PTS deployment has overlapping IP addresses that contain a different VLAN tags or bridge-groups. This mode is useful when you have overlapping IP addresses within a single PTS cluster.

When this mode is selected one of these additional CLI commands should be used:

- If using VLAN tags as a unique identifier, then configure the PTS with VLAN tag to site number mappings using this command [add config service session-qualifier vlan](#).
- If using PTS clusters to identify unique traffic, then use [set config service session-qualifier cluster-number](#) on page 68.
- If using pair of VLAN tags as a unique identifier, then configure PTS with s-tag+c-tag to site number mappings.

These features are unsupported in this mode: divert, DNS analyzers, subscriber-aware load-balancing, and network protection.

Mode-specific settings may be configured at any time on the PTS, but they only become active when the PTS is configured in the applicable mode. For example, the PTS cluster-number may be configured at any time, but the PTS only uses the cluster-number to qualify IP addresses after it has been placed in cluster-number mode.

Switching modes is non-destructive to mode-specific configurations. For example, if the PTS is switched from cluster-number mode to site-number mode, the cluster-number specific configuration is not modified in any way. If the PTS is returned to cluster-number mode later, the old cluster-number configuration takes effect.

2.10.50 set config service session-qualifier warn-ip-policy

Enables or disables reload warnings when IP-specific policy issued while session qualifiers are enabled.

```
set config service session-qualifier warn-ip-policy <true|false>
```

2.10.51 set config service spb

Configures the SPB servers or version.

```
set config service spb servers <servers>
```

```
set config service spb version <5.40|5.51|5.60|6.00|6.20>
```



Note:

This command is used to set the default configured settings to use when connecting to an older SPB where capabilities cannot be negotiated. Select the highest version that matches the SPB that is connected. This setting is used when connecting to a SPB 6.40 or less.

Attribute	Description
servers	A space separated list of URIs for SPB servers. If the list contains more than one item, it must be in a quoted string. It accepts host names or IP addresses in the simplest case (for example, 10.1.1.23), or URIs (for example, ssl://spb.example.com:50000).
version	The SPB version the PTS will use if it cannot automatically negotiate the correct version. Note: If the PTS is connected to an SPB version less than 6.40.01, this value must be set to that SPB version. For example, use the closest version that is not higher than the actual SPB version.

To determine if the PTS has negotiated and what values are being used, use the command `show service spb capabilities-exchange`.

2.10.52 set config service statistics log-interval

Configures how often PTS reports statistics in seconds.

```
set config service statistics log-interval demographic <int:60..86400>
set config service statistics log-interval subscriber <int:60..86400>
set config service statistics log-interval subscriber-protocol <int:60..86400>
set config service statistics log-interval port <int:60..86400>
set config service statistics log-interval published-expression <int:60..86400>
set config service statistics log-interval histogram <int:60..86400>
set config service statistics log-interval histogram-protocol <int:60..86400>
```

Attribute	Description
demographic	Demographic statistics
subscriber	Subscriber basic statistics
subscriber-protocol	Subscriber protocol statistics
published-expression	Published expression statistics
histogram	Histogram basic statistics
histogram-protocol	Histogram protocol statistics
port	Port statistics

2.10.53 set config service statistics skip-headers

Configures the headers to skip. To skip multiple headers, use a space-separated list.

```
set config service statistics skip-headers <ether|tunnel|padding|fcs|min64bytes>
```

To unset all skip-headers set to "". For example:

```
set config service statistics skip-headers ""
```


Parameter	Description
ether	Excludes ether header.
tunnel	Skips all tunneling headers.
padding	Skips packet padding.
fsc	Skips the frame checksum.
min64bytes	Skips padding small packets up to 64bytes. This parameter is deprecated in favour of padding.
""	If the string is empty, this parameter unsets all skip headers.

2.10.54 set config service statistics subscriber minimum-bytes

These commands configure the minimum number of transmitted or received bytes to trigger a log to the database.

```
set config service statistics subscriber minimum-bytes tx <int:0.. 2147483647>
```

```
set config service statistics subscriber minimum-bytes rx <int:0.. 2147483647>
```

Attributes	Description
tx	Sets the minimum number of transmitted subscriber bytes needed to log to the database. Value 0 indicates log all statistics - all data is logged.
rx	Sets the minimum number of received subscriber bytes needed to log to the database. Value of 0 indicates log all statistics.  Note: set config service statistics subscriber minimum-bytes tx must be run before this command will be considered in the logging decision.

2.10.55 set config service statistics tunnel-fragment-extrapolation

Enables tunnel fragment extrapolation and configures its function.

```
set config service statistics tunnel-fragment-extrapolation enabled <true|false>
```

```
set config service statistics tunnel-fragment-extrapolation maximum-ip-packet-size <1..65535>
```

Attribute	Description
enabled	Enables/disables the tunnel fragment extrapolation. When enabled, the PTS estimates the size of the second fragment based on the length field in the IP header in the first fragment, and both the first and second fragment are counted. When disabled, only the actual size of the first fragment is counted. Default is false.
maximum-ip-packet-size	If enabled is true, if the inner-IP length of the first fragment exceeds this value, then extrapolation is not performed and only the actual size of the first fragment is counted. Default is 1600.

2.10.56 set config service streaming analyzer hds

This command is used to configure and monitor the HDS Analyzer.

```
set config service streaming analyzer hds video-state max <max states>
```

```
set config service streaming analyzer hds video-state timeout <timeout val>
```

Output	Description
max	Maximum stored video states (Min value :1 , Max value: 10000)
timeout	Stored video state timeout (Min value: 10, Max value: 300)

2.10.57 set config service streaming analyzer hls

This command is used to configure and monitor the HLS Analyzer.

```
set config service streaming analyzer hls video-state
set config service streaming analyzer hls video-state max <int:1..10000>
set config service streaming analyzer hls video-state timeout <int:10..300>
```

Attribute	Description
video-state	Stored session state.
max	Sets the maximum number of storable video states. Once the configured maximum number of states are in use, new flows containing streaming video are not analyzed until the old ones are freed or a timeout occurs. The maximum value is 10000 and the minimum is 1.
timeout	Sets the timeout, in seconds, for the stored video states. Each stored video state has its own timer. If a video ends early or the subscriber disconnects, the state information is freed when the timeout value is reached. The maximum value is 300 and the minimum is 10.

2.10.58 set config service streaming analyzer smooth-streaming video-state

Configures the smooth-streaming video analyzer's states. The video state is used to correlate the different video data chunks belonging to a video to analyze video quality.

```
set config service streaming analyzer smooth-streaming video-state max <int:1..10000>
set config service streaming analyzer smooth-streaming video-state timeout <int:30..1800>
```

Attribute	Description
maximum	Sets the maximum number of video states that can be stored. Once the configured maximum number of states are in use, new flows containing streaming video are not analyzed until the old ones are freed or timeout. Defaults to 10000.
timeout	Sets the timeout, in seconds, for the stored video states. Each stored video state has its own timer. If a video ends early or the subscriber disconnects, the state information is freed when the timeout value is reached. Defaults to 1 minute.

2.10.59 set config streaming analyzer hls video-state

Use these configuration parameters to configure and monitor the HLS Analyzer:

```
set config service streaming analyzer hls video-state max <int:1..10000>
set config service streaming analyzer hls video-state timeout <int:10..300>
```

Output similar to this is generated:

```
TotalHlsFlows           : 0
ManifestsParsed         : 0
ManifestParseFailures   : 0
```



```
ManifestCollisions           : 0
MaxVideoStatesReached       : 0
VideoStateTimeouts         : 0
VideoChunksSeenWithoutManifest : 0
MaxAlternateStreamLimitHit  : 0
PlaylistWithPartialMediaInfo : 0
PlaylistWithNoMediaInfo    : 0
```

Attribute	Description
maximum	Sets the maximum number of storable video states. Once the configured maximum number of states are in use, new flows containing streaming video are not analyzed until either the old ones are freed or a timeout occurs. The maximum value is 10000 and the minimum is 1.
timeout	Sets the timeout, in seconds, for the stored video states. Each stored video state has its own timer. If a video ends early, or the subscriber disconnects, the state information is freed when the timeout value is reached. The maximum value is 300 and the minimum is 10.

2.10.60 set config service subscriber-management auto-remap

This command configures PTS to remap all cached SPB subscriber mappings based on various SPB disconnection events. When this remap occurs, every session in Sandscript will receive a Session.IsEnd event, and any currently-active session remaps and receives a Session.IsNew event.

There are two different modes for automatic remapping:

- Disconnection-length-based remapping - A single disconnection event that lasts longer than a given time causes an automatic remapping.
- Disconnection-frequency-based remapping - Frequent recurring disconnection events causes automatic remapping.

You can enable these modes either independently of the each other, or you can use them simultaneously.

```
set config service subscriber-management auto-remap max-disconnect-length <int>
    set config service subscriber-management auto-remap disconnect-length-trigger
<immediate|wait-for-reconnect>
    set config service subscriber-management auto-remap disconnect-counting-period <int>
    set config service subscriber-management auto-remap max-disconnects-per-period <int>
```

Attribute	Description	Default
max-disconnect-length	Maximum tolerated length of a disconnection from the SPB, in seconds, before an automatic remap will be triggered. Set this to 0 to disable disconnection-length-based remapping.	0 second
disconnect-length-trigger	Controls behaviour of disconnection-length-based remapping. When set to 'immediate', the logout and Session.IsEnd in Sandscript will fire immediately after the max-disconnect-length period has been exceeded.	wait-for-reconnect

Attribute	Description	Default
	When set to 'wait-for-reconnect', the logout and Session.IsEnd in Sandscript will occur after the connection is re-established.	
disconnect-counting-period	Period (in seconds) over which disconnections are counted for disconnection-frequency-based remapping. If more than max-disconnects-per-period disconnections happen during an interval of this length, remapping is triggered.	30
max-disconnects-per-period	Maximum number of disconnection events that may occur within disconnection-counting-period seconds before remapping is triggered. Set this to 0 to disable disconnection-frequency-based remapping.	0

2.10.61 set config service subscriber-management end-session-event end-flows

Set this to `true` to end all active flows of the subscriber when the current session ends.

```
set config service subscriber-management end-session-event end-flows <true|false>
```

2.10.62 set config service subscriber-management login-events handle-notification


Configures the PTS to process IP assignment notifications from the SPB.

```
set config service subscriber-management login-events handle-notification <true|false>
```

2.10.63 set config service subscriber-management lookup

Configures subscriber management lookups.

```
set config service subscriber-management lookup max-attempts <int:0..255>
set config service subscriber-management lookup on-receive <false|true>
set config service subscriber-management lookup initial-delay mode <static|dynamic>
config service subscriber-management lookup initial-delay static delay <int:0...100000>
```

Attribute	Description
max-attempts	Maximum number of lookup requests to send for an IP address before giving up. Set to 0 for no limit.
on-receive	Configures the PTS to perform subscriber lookups when the subscriber IP address receives unidirectional data. Default is true.  Note: The PTS will always do subscriber lookups when the subscriber IP address is sending data.
initial-delay mode	Toggles the initial lookup delay algorithm between static mode and dynamic mode. To reduce network congestion, IP-address lookups to the SPB are controlled by an algorithm which may apply a delay before the first lookup request is sent for any newly-discovered subscriber IP address. The algorithm operates one of these modes: <ul style="list-style-type: none">• Dynamic mode (the default), adjusts the size of delay based on the number of unnecessary lookups. An unnecessary lookup is one where a look up was requested but the IP address becomes mapped by a push notification from the SPB before the lookup response arrives. If there are too many unnecessary lookups, the delay is increased and when the percentage of unnecessary lookups drops, the delay is decreased.• Static mode, has a pre-configured delay that does not change. If the static mode is enabled and the delay set to 0, there is no delay inserted before on any lookup request sent by the PTS.
initial-delay static delay	Sets the static lookup delay, in milliseconds, applied to the first lookup of any new subscriber IP address in static delay mode. If configured, bypasses dynamic lookup and sets a delay time for all lookups. Units of measure for configuration is milliseconds, therefore the maximum is equivalent to 100 seconds.

2.10.64 set config service subscriber-management new-session-event require-activity

Set this to true to expose new session events to SandScript only once subscriber activity is seen.

```
set config service subscriber-management new-session-event require-activity <true|false>
```

2.10.65 set config service subscriber-management timeout

These commands configure IP-to-subscriber timeouts.

```
set config service subscriber-management timeout inactivity <int:1..1209600>
set config service subscriber-management timeout late <int:1..120>
set config service subscriber-management timeout lookup initial <int:1..86400>
set config service subscriber-management timeout lookup max <int:1..86400>
```

Attribute	Description
inactivity	Configures the number of seconds after which a mapped IP address with no traffic will become unmapped.

Attribute	Description
late	Configures the maximum delay, in seconds, for an IP to be mapped 'on-time' after traffic arrives.
lookup initial	Configures the initial delay between subscriber lookups.
lookup max	Maximum delay between subscriber lookups.

2.10.66 set config service switch-fabric workfarm

Configures memory allocation of the workfarm switch modules. This command is primarily used, together with `set config service udp-prioritization`, to provide guaranteed service to prioritized UDP packets. The workfarm switch has both dynamic and static allocated memory.

```
set config service switch-fabric workfarm dynamic-cell-allocation <int:5..100>
set config service switch-fabric workfarm static-cell-allocation cos0 <int:1..93>
set config service switch-fabric workfarm static-cell-allocation cos1 <int:1..93>
set config service switch-fabric workfarm static-cell-allocation cos2 <int:1..93>
set config service switch-fabric workfarm static-cell-allocation cos3 <int:1..93>
set config service switch-fabric workfarm static-cell-allocation cos4 <int:1..93>
set config service switch-fabric workfarm static-cell-allocation cos5 <int:1..93>
set config service switch-fabric workfarm static-cell-allocation cos6 <int:1..93>
```

Attribute	Description
dynamic-cell-allocation percentage	Percentage of total available cells for dynamic allocation.
static-cell-allocation cos0 percentage	Percentage of total available cells to be allocated for a cos queue 0.
static-cell-allocation cos1 percentage	Percentage of total available cells to be allocated for a cos queue 1.
static-cell-allocation cos2 percentage	Percentage of total available cells to be allocated for a cos queue 2.
static-cell-allocation cos3 percentage	Percentage of total available cells to be allocated for a cos queue 3.
static-cell-allocation cos4 percentage	Percentage of total available cells to be allocated for a cos queue 4.
static-cell-allocation cos5 percentage	Percentage of total available cells to be allocated for a cos queue 5.
static-cell-allocation cos6 percentage	Percentage of total available cells to be allocated for a cos queue 6.
static-cell-allocation cos7 percentage	Percentage of total available cells to be allocated for a cos queue 7.

2.10.67 set config service switch-fabric core-fabric

Configures memory allocation of the core-fabric switch modules. The command is primarily used, together with the `set config service udp-prioritization` command to provide guaranteed service to prioritized UDP packets. The core-fabric has only static allocated memory.

```
set config service switch-fabric core-fabric static-cell-allocation cos0 percentage <int:1..93>
set config service switch-fabric core-fabric static-cell-allocation cos1 percentage <int:1..93>
set config service switch-fabric core-fabric static-cell-allocation cos2 percentage <int:1..93>
set config service switch-fabric core-fabric static-cell-allocation cos3 percentage <int:1..93>
set config service switch-fabric core-fabric static-cell-allocation cos4 percentage <int:1..93>
set config service switch-fabric core-fabric static-cell-allocation cos5 percentage <int:1..93>
set config service switch-fabric core-fabric static-cell-allocation cos6 percentage <int:1..93>
```

Attribute	Description
static-cell-allocation cos0 percentage	Percentage of total available cells to be allocated for a cos queue 0
static-cell-allocation cos1 percentage	Percentage of total available cells to be allocated for a cos queue 1.
static-cell-allocation cos2 percentage	Percentage of total available cells to be allocated for a cos queue 2.
static-cell-allocation cos3 percentage	Percentage of total available cells to be allocated for a cos queue 3.
static-cell-allocation cos4 percentage	Percentage of total available cells to be allocated for a cos queue 4.
static-cell-allocation cos5 percentage	Percentage of total available cells to be allocated for a cos queue 5.
static-cell-allocation cos6 percentage	Percentage of total available cells to be allocated for a cos queue 6.
static-cell-allocation cos7 percentage	Percentage of total available cells to be allocated for a cos queue 7.

2.10.68 set config service tunneling

Configures how tunneled traffic is handled.

```
set config service tunneling l2tp action <action>
set config service tunneling gre action <action>
set config service tunneling gtpu action <action>
set config service tunneling ip-in-ip action <action>
set config service tunneling ipv6-in-ipv4 action <action>
set config service tunneling mpls default-action <action>
set config service tunneling mpls inspect-labels <label-list>
set config service tunneling mpls inspect-eompls <label-list>
set config service tunneling mpls rule <row> type <row> action
    <shunt|discard|ip|eompls>
set config service tunneling protocols <protocols>
set config service tunneling tcp-mss-clamp [client|server] enabled [true|false]
set config service tunneling tcp-mss-clamp [client|server] max-mss <1:65535>
set config service tunneling tcp-ws-clamp [client|server] enabled [true|false]
set config service tunneling tcp-ws-clamp [client|server] max-mss <1:255>
set config service tunneling udpgeneric subscriber udp-port <port>
set config service tunneling udpgeneric internet udp-port <port>
set config service tunneling vlan default-action <action>
set config service tunneling vlan rule <row> depth <row> action <shunt|discard|ip>
set config service tunneling q-in-q ethertype <88a8|9100>
```

Committing changes to the `set config service tunneling mpls inspect-labels` requires a restart of PTSM and PTSD.

Attribute	Description
protocols	A quoted space-separated list of tunneling protocols to inspect. Possible protocols include: <ul style="list-style-type: none">• l2tp• capwap• dslite• gre• gtpu• gtpv0• ipip• map• mpls• qinq• udpgeneric• vlan

Action Parameter	Description
disable	The PTS does not inspect the inner frame, but reports the traffic as the tunnel protocol.
discard	The PTS drops all packets matching this tunnel type.
inspect-ip	The PTS strips tunneling headers and inspects the inner frame. Not supported for l2tp protocol.
shunt	Packets are shunted and not reported on.

MPLS Action Parameter	Description
discard	The PTS drops all packets matching this tunnel type.
eompls	The PTS strips tunneling headers and inspects the inner Ethernet frame.
ip	The PTS strips tunneling headers and inspects the inner frame.
shunt	Packets are shunted and not reported on.
none	Unsets label inspection.

MPLS Inspect-labels Parameter	Description
label-list	The list of MPLS labels to inspect, or none to undo a previous configuration.
all	Inspect all labels.

VLAN Action Parameter	Description
discard	The PTS drops all packets matching this tunnel type.
ip	The PTS strips tunneling headers and inspects the inner frame.
shunt	Packets are shunted and not reported on.

QinQ Ethertype Parameter	Description
88a8	Packets with ethertype 0x88a8 will be recognized as QinQ.
9100	Packets with ethertype 0x9100 will be recognized as QinQ.



Note:

Packets with VLAN etherypes 0x8100, 0x9100, and 0x88a8 will all be bumped to the modules, regardless of how QinQ is configured/enabled. The QinQ deployment supports a configured outer VLAN tag of either 0x9100 or 0x88a8. If QinQ tunnel inspection is enabled, the PTS will parse packets with the configured ethertype to payload and bridge packets with the non-configured ethertype without inspection. If QinQ tunnel inspection is disabled, the PTS will bridge both without inspection.

The `set config server tunneling tcp-mss-clamp` command clamps the TCP maximum segment size for all packets. If the TCP packet has the maximum segment size option, the PTS changes the window scale value whenever the packet's value is greater than the max-mss value.

Clamp Parameter	Description
client server	Determines whether to clamp packets from either the client or the server.
enabled [true false]	Set to true to enable the feature. The PTS will clamp the window scale.

Clamp Parameter	Description
max-mss [1:65535]	If the packet's maximum size is larger than the max-mss, the PTS modifies the packet to change this value. The default for this is 65535.

The `set config server tunneling tcp-ws-clamp` command clamps the TCP window scale for all packets. If the TCP packet has the window scale option, the PTS changes the window scale value whenever the packet's value is greater than the max-ws value.

Clamp Parameter	Description
client server	Determines whether to clamp packets from either the client or the server.
enabled [true false]	Set to true to enable the feature. The PTS will clamp the window scale.
max-mss [1:65535]	If the packet's maximum size is larger than the max-ws, the PTS modifies the packet to change this value. The default for this is 255.

set config service tunneling capwap udp-ports

Configures how tunneled traffic is handled.

```
set config service tunneling capwap udp-ports <port-list> p
```

Attribute	Description
port-list	A comma-separated list of maximum 8 ports

2.10.69 set config service udp-prioritization

This command configures the maximum allowable number of UDP Prioritization entries; the default is 1. This value directly affects the number of entries when UDP Prioritization is enabled alongside IOM. A log message indicates the new maximum number of entries.

These UDP prioritization commands provide improved guarantees for the reliable delivery of subscriber mapping control packets.

- `set config service udp-prioritization enabled <false|true>`
- `set config service udp-prioritization max-entries <int:0..64>`

Parameter	Description
enabled	Enable/disable the UDP Prioritization feature.
max-entries	Maximum number of entries supported.



Note:

You also need these CLI commands to configure the service properly:

- `add/set/delete config service udp-prioritization`
- `set config service switch-fabric`

2.10.70 set config support notification-email-address

Configures the list of email addresses that receive support notifications in case of a module or service failure. There is no limit to the number of email addresses that you can add to this comma delimited list. Run this command again to modify the list.

```
set config support notification-email-address <email-addresses>
```


2.10.71 set config system accounting

Sets the IP address of the interface connected to the peer(s). Takes an IPv4 or an IPv6 address.

```
set config system accounting batch-size <int:1..1000>
set config system accounting error-interval <int:1000..10000>
set config system accounting queue-size <int:1..1000>
set config system accounting send-interval <int:1..1000>
set config system accounting tacacs+
```

Attribute	Description
batch-size	The number of records that are sent at a time. Range is 1 – 1000.
error-interval	The delay, in milliseconds, before retrying after an error. Range is 1000 – 10000.
queue-size	The maximum number of accounting records that can be queued. Range is 1 – 1000.
send-interval	The time, in milliseconds, between sending batches of records. Range is 1 – 1000.
tacacs+	Remote accounting configuration using TACACS+.
mandatory best-effort	Controls whether or not a login is denied if the accounting record cannot be logged.

2.10.72 set config system accounting tacacs+

This command is used to configure TACACS+ accounting on the element.

```
set config system accounting tacacs+ debug true|false
set config system accounting tacacs+ enabled <true|false>
set config system accounting tacacs+ login <mandatory|best-effort>
set config system accounting tacacs+ secret <string>
set config system accounting tacacs+ servers <server-pair>
set config system accounting tacacs+ timeout <int:1..30>
```

Attribute	Description
debug	Enable/disable debugging.
enabled	Accounting enabled or disabled.
login	Controls whether or not a login is denied if the accounting record cannot be logged.
secret	The secret key shared with the RADIUS or TACACS+ server.
servers	A space-separated list of one or two servers.
timeout	The timeout in seconds for communicating with the TACACS+ server(s). The range is 1 through 30 seconds. Default value is set 3 seconds.

2.10.73 set config system authentication tacacs+

This command is used to configure Terminal Access Controller Access-Control System (TACACS+) authentication on the element.

```
set config system authentication tacacs+ debug <true|false>
set config system authentication tacacs+ default-group <admin|service|operator>
set config system authentication tacacs+ default-shell <bash|cli>
set config system authentication tacacs+ enabled <true|false>
set config system authentication tacacs+ secret <string>
set config system authentication tacacs+ servers <server-pair>
set config system authentication tacacs+ service <string>
set config system authentication tacacs+ timeout <int:1..30>
```

Attribute	Description
debug	Enable/disable debugging.
default-group	The default privilege level for remote users.
default-shell	Default login shell.
enabled	Authentication enabled or disabled.
secret	The secret key shared with the TACACS+ server.
servers	A space-separated list of one or two servers.
service	The name of the service used to authorize users.
timeout	The timeout in seconds for communicating with the TACACS+ server(s). The range is 1 to 30 seconds. Default value is 3 seconds.

2.10.74 set config system authentication

Sets remote authentication using RADIUS.

```
set config system authentication radius secret <secret>
set config system authentication radius servers <servers>
```

Committing this change requires restarting the authentication service.

Attribute	Description
secret	The secret shared with the RADIUS.
servers	A space separated list of RADIUS authentication servers. If the list contains more than one item, it must be in a quoted string. It accepts host names or IP addresses in the simplest case (for example, 10.1.1.23), or URIs (for example, ssl://spb.example.com:50000).

2.10.75 set config system reload bridge-mode alarm timeout

Configures the time limit for Alarm model 63: Bridge mode time limit exceeded. If one or more modules on the PTS element fail to bridge packets for a time period greater than this value, then Alarm model 63 is raised.

2.10.76 set config system services last-reload

Configures if a given reload failure will generate an alarm. See the `show service last-reload` CLI command.

```
set config system services last-reload <index> enabled <true|false>
```

2.10.77 set config traffic flow-limit

Configures the maximum number of flows displayed for an IP or subscriber by the `show traffic ip` and `show traffic subscriber` CLI commands.

```
set config traffic flow-limit <int:1..>
```

2.11 Operational set Commands

Operational set commands let you change the configuration of an interface dynamically. They are applied when you press enter; they are not part of the 'configuration' config set commands. You can run operational set commands within an configuration session, and those operational set commands take effect immediately.

2.11.1 set interface shunt

Enables or disables traffic shunting.

```
set interface shunt <true|false>
```

This command configures the PTS to shunt all traffic on bridge-groups. The NPU processes shunted traffic and is then sent to the corresponding interface(s) in the bridge-group. No traffic is inspected and no SandScript is applied for traffic on the bridge-group. Bandwidth reports show all traffic from this element as shunted. In a cluster, only traffic that this elements data ports intersect is shunted, so it is possible for the inspection modules on this element to continue processing traffic because traffic that other elements intersect can be load-balanced to them.

2.11.2 set policy destination

Sets the configured policy destinations and determines status for these destinations. Sets the admin status of the destination. If a destination has its admin status set to down then no new flows will be diverted to that destination.

```
set policy destination <destination-name> admin-status <up|down>
```

Attribute	Description
destination	Operational state and actions related to policy destinations.
up down	Administrative status of the destination is up or down.

2.11.2.1 set policy destination file flush

Flushes all packet capture files to disk.

The packet capture files are specified in SandScript policy with the keywords `destination "<name>" file`.

2.11.3 set service load-balancer

Enables or disables an element for load-balancing.

Dynamically reconfigures the load balancer so that the modules of the designated element are no longer used for processing traffic. This may be a prelude to doing maintenance on the element. This command must be run from the load-balancer master.

Press tab after entering `set service load-balancer host` or `set service load-balancer serial` to list the available hostnames or serial numbers.

```
set service load-balancer host <hostname> active <true|false> <time-out>
set service load-balancer serial <serial-number> active <true|false> <time-out>
```

Parameter	Description
serial	The serial number of the element to be restored or disabled.
host	The hostname of the element to be restored or disabled.
active	Disables the element when set to false; set to true to resume directing the load to the element.

2.12 monitor

Monitor commands continuously display system information without changing it. Data is updated on stdout every 2 seconds. To terminate a monitor command, press **Ctrl+c**.

2.12.1 monitor interface counters

Continuously displays input/output bytes, packets and errors for all external ports, broken into sections by port type: Data Interfaces, Cluster Interfaces and Management Interfaces. Counters are measured since the associated process, or PTS, was restarted. Data is updated on stdout every 2 seconds. To terminate a monitor command, press **Ctrl+c**.

```
monitor interface counters
monitor interface counters management
monitor interface counters cluster
monitor interface counters data
monitor interface counters <interface>
monitor interface counters module
monitor interface counters module <module>
monitor interface counters module <module> <interface>
monitor interface counters fabric
monitor interface counters fabric <interface>
monitor interface counters npu
monitor interface counters npu <interface>
```

Attribute	Description
cluster	Shows input/output bytes, packets and errors for external cluster ports.
data	Shows input/output bytes, packets and errors for external data ports.
fabric	Shows input/output bytes/packets/error on internal switch-fabric interfaces.
fabric <interface>	Shows details for a specific internal switch-fabric interface.
<interface>	Shows details for a specific external port.

Attribute	Description
management	Shows input/output bytes, packets and errors for external management ports.
module	Displays total input/output bytes/packets/errors for all modules, split into two sections Data Interfaces and Other Interfaces.
module <module>	Displays input/output bytes/packets/errors for each interface on a specific module.
module <module> <interface>	Displays details for a specific interface on a specific module.
npu	Shows input/output bytes/packets/error on NPU interfaces.
npu <interface>	Shows details for a specific NPU interface.

Output	Description
Port	Port name of the interface.
BytesIn	The number of bytes coming in.
BytesOut	The number of bytes going out.
PacketsIn	The number of packets coming in.
PacketsOut	The number of packets going out.
DropsIn	The number of packets dropped coming in.
DropsOut	The number of packets dropped going out.

Detailed Output	Description
UnicastPacketsIn	Number of incoming unicast packets.
MulticastPacketsIn	Number of incoming multicast packets.
BroadcastPacketsIn	Number of incoming broadcast packets.
UnicastPacketsOut	Number of out going unicast packets.
MulticastPacketsOut	Number of out going multicast packets.
BroadcastPacketsOut	Number of out going broadcast packets.
64BytePackets	Number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
65to127BytePackets	Number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
128to255BytePackets	Number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
256to511BytePackets	Number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
512to1023BytePackets	Number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
1024to1518BytePackets	Number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).

Detailed Output	Description
DiscardsIn	Number of inbound packets chosen to be discarded, even though no errors were detected, to prevent their being deliverable to a higher-layer protocol.
ErrorsIn	Number of errors on inbound traffic.
DiscardsOut	Number of outbound packets chosen to be discarded, even though no errors had been detected, to prevent their being deliverable to a higher-layer protocol.
ErrorsOut	Number of errors on outbound traffic.
UndersizePackets	Number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
OversizePackets	Number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
Fragments	Number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets) and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
AlignmentErrors	Total number of packets received that had a length between 64-1518 octets (excluding framing bits, but including FCS octets), but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
FcsErrors	Number of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check. This count does not include frames received with a frame-too-long or frame-too-short error.
MacTransmitErrors	Number frames for which transmission on a particular interface has failed due to an internal MAC sublayer transmit error.
MacReceiveErrors	Number frames for which reception on a particular interface has failed due to an internal MAC sublayer receive error.
CarrierSenseErrors	Number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame on a particular interface. The count represented by an instance of this object is incremented at most once per transmission attempt, even if the carrier sense condition fluctuates during a transmission attempt.
FrameTooLong	Number of errors related to frames that are too long.
SymbolErrors	Number of symbol errors.

2.12.2 monitor interface rate

Continuously displays in and out bitrate, packet rate and drop rate for data interfaces, cluster interfaces and management interfaces. Data is updated on stdout every 2 seconds. To terminate a monitor command, press **Ctrl+c**.

```
monitor interface rate
monitor interface rate module
monitor interface rate module <module-id>
monitor interface rate link-aggregation-group
```

Attribute	Description
module	Shows a summary of the bitrates, packet rates and error rates in and out of the modules.

Attribute	Description
module <module-id>	Shows detailed bitrates, packet rates and error rates for all internal interfaces on a specific module.
link-aggregation-group	Shows cluster interfaces, grouped by LAG.

Output	Description
Port	The port.
Module	The module.
Interface	The interface.
In(bps)	Reception rate, in bits per second.
Out(bps)	Transmission rate, in bits per second.
PacketsIn(pps)	Reception rate, in packets per second.
PacketsOut(pps)	Transmission rate, in packets per second.

2.12.3 monitor system overview

Provides a continuous overview of what the PTS is doing. Data is updated on stdout every 2 seconds. To terminate a monitor command, press **Ctrl+c**.

Key Performance Indicators Output	Description
Service	Identifies the service that the indicator applies to.
Indicator	Identifies the name of the system indicator.
Value	Lists the value(s) of the indicator.
Units	Identifies the unit of indicator data.

Traffic Output	Description
ApplicationType	Application type for the traffic.
SessionRate	The session rate.
Downstream(bps)	The number of bits per second for downstream traffic.
Upstream(bps)	The number of bits per second for upstream traffic.
Total(bps)	Total number of bits per second for upstream and downstream traffic.

2.12.4 monitor traffic

Continuously displays information about traffic being processed by the system. All bits per second outputs are calculated as the sum of the bytes in the specified flows, over the lifetime of the flows. Data is updated on stdout every 2 seconds. To terminate a monitor command, press **Ctrl+c**.

```
monitor traffic
monitor traffic application-type <BulkTransfer|Email|Gaming|Miscellaneous|
                                NetworkStorage|PeerToPeer|RealTimeCommunication|
                                RealTimeEntertainment|SocialNetworking|Tunneling|
                                WebBrowsing
```

Output	Description
ApplicationType	Application type for the traffic
SessionRate	The session rate
Downstream(bps)	Number of bits per second for downstream traffic
Upstream(bps)	Number of bits per second for upstream traffic
Total(bps)	Total number of bits per second for upstream and downstream traffic

2.13 show

The show command inspects system information without changing it.

2.13.1 show alarms

Shows a list of the current alarms (severity minor or greater) on the system, details about a specific alarm instance, or alarms of all severities (`show alarms all`).

If active, details include information about any variables associated with the alarm. Information that accompanied the clear notification is displayable for cleared alarms, but their indices are no longer shown in the general listing. The show alarms variant also notes the number of alarms that were not shown, because they are of a lower severity.

```
show alarms
show alarms <alarm-instance-id:0..>
show alarms <id:0..>

show alarms all
```

Output	Description
AlarmId	ID for the alarm, used to identify the instance of the active alarm. Numbered from 1.
Severity	Alarm severity. Can be one of: <ul style="list-style-type: none">critical - requires immediate attention.major - service is impacted.minor - service is not currently impacted, but the condition needs to be corrected.

Output	Description
	<ul style="list-style-type: none"> warning - notification of some event on the system. clear - a previously raised alarm has been cleared.
EventTime	Time at which the event was logged.
Model	Alarm model number.
Description	Description of the alarm.

Alarm-specific Output	Description
Alarm Model	The alarm model number.
Severities	The severities of the alarm.
AlarmText	Description of the alarm.
RaiseNotification	The notification sent when the alarm is raised.
ClearNotification	The notification sent when the alarm is cleared.
Description	A description of the alarm.

2.13.2 show alarms history

Shows a list of all alarms generated, as inferred by any notifications that were logged.

```
show alarms history
show alarms history <id:1...>
show alarms history date <yyyy-mm-dd>
show alarms history date <yyyy-mm-dd> limit <limit:0..>
show alarms history limit <limit:0..>
```

The details of the alarm differ from the details of the notification in that they include information from the referenced alarm model. The default is set to list alarms resulting from the most recent 10 notifications on the current date.

If the output contains the words "Corrupted Log File", inspect the /var/log/notification.log file for possible reasons. For example:

```
EVENTDATE: 2012-06-14
=====

TrapLogId Severity  EventTime      Model
-----
81          [warning]  19:43:13      14
--          [--]      --          Corrupted Log File
85          [clear]   19:43:21      10
86          [clear]   19:43:34      10

TrapLogId Description
-----
81          Network interface administratively down: cluster 1-5
--          Information unavailable at MIB: Corrupted Log File
85          Service component online: ptsm
86          Service component online: ptsd
```

Attribute	Function
date	The specific date for which alarm history is required, defined as yyyy-mm-dd
limit	Limits the number of rows to display
id	Trap Log ID for which history should be displayed

Output	Description
EventDate	Date on which the event occurred
TrapLogId	Specific trap log ID
Severity	Alarm severity: critical, major, minor or warning
EventTime	Date and time at which the alarm was raised. (For example, 2010-05-10 22:03:47)
Model	Alarm model number
Description	Description of the alarm action

Output	Description
EventDate	Date on which the event occurred
TrapLogId	Specific trap log ID
Severity	Alarm severity: critical, major, minor, warning, clear
EventTime	Date and time at which the alarm was raised. (For example, 2010-05-10 22:03:47)
Model	Alarm model number
Description	Description of the alarm action
Notification	Notification message
Value	
NotificationID	Sandvine MIB notification
Details	Explanation of the event
DISMAN-EVENT-MIB	
SNMPv2-MIB	
SANDVINE-MIB	

2.13.3 show alarms model

Shows all alarm models available on this element, or the details for a specific alarm model.

```
show alarms model
```

```
show alarms model <id:1..>
```

Specific Model Output	Description
Alarm Model	Alarm model number
Severities	Severities supported by this alarm
Alarm Text	Text associated with this alarm
Raise Notification	MIB for raising the notification

Specific Model Output	Description
Clear Notification	MIB for clearing the notification
Description	Description of this alarm
NotificationId	MIB and alarm profile description

Output	Description
Model	Alarm model number
Severity	Severities supported by the alarm
NotificationId	MIB and alarm profile description
Description	Description of the alarm

Specific Model Output	Description
Alarm Model	Alarm model number
Severities	Severities supported by this alarm
Alarm Text	Text associated with this alarm
RaiseNotification	MIB for raising the notification
ClearNotification	MIB for clearing the notification
Description	Description of this alarm

2.13.4 show cli sessions

Displays details regarding active CLI sessions.

```
show cli sessions
```

Output	Description
ProcessID	ID of the CLI session
User	Login name of the user
StartTime	Date and time when the session started
LastActivityTime	Date and time when the last activity occurred

2.13.5 show config pending

Shows pending configuration changes. This command is only available in the configuration mode.

```
show config pending
```

2.13.6 show interface bridge-group

Shows the configuration and operational status for all defined bridge-groups for the element.

Output	Description
Index	Index for this bridge-group.
OperStatus	Bridging status can be one of: <ul style="list-style-type: none">• normal inspected — normal condition (traffic is inspected)• shunted by kernel — the kernel module is not functioning correctly (PTS 8210 only)• shunted by application — the PTS application is not running (PTS 8210 only)
SubscriberPorts	Subscriber-side ports in the group
InternetPorts	Internet-side ports in the group

**Note:**

If this command displays “No data interfaces are configured” then that means that the bridgeGroup/groupTable is empty.

MIB reference

Data displayed as part of this command is from the svBridgeGroupGroupTable and svBridgeGroupPortTable in the SANDVINE-MIB.

2.13.7 show interface bypass

Show status and watchdog timeout information for all bypass groups in the system.

Output	Description
Index	Index of the bypass group
AdminStatus	The bypass mode as defined using the <code>set config interface bypass external admin-status</code> CLI command. Can be one of: <ul style="list-style-type: none">• active - the PTS only drops into bypass mode when power is lost. Other system failures, such as an upgrade or component failure, do not result in the PTS dropping into bypass mode.• bypass - causes all traffic to bypass the PTS. No inspection or policies are applied.• software- the default mode. The bypass module will flip into bypass mode upon power loss, component failure, or system unresponsiveness. Bypass mode is not activated for a software upgrade or in case of link failure.
OperStatus	The current operational state of the bypass chassis. Can be one of: <ul style="list-style-type: none">• active - the bypass chassis is directing traffic to the PTS for inspection• bypass - the bypass chassis is directing traffic around the PTS
WdTimeout	Watchdog timeout. The watchdog timeout is loaded into the bypass card's EEPROM. When the bypass card is in KERNEL or USERLAND watchdog modes, and the difference in time between watchdog kicks is greater than the timeout, the card enters a BYPASS state. The timeout is specified in milliseconds. The timeout range is bypass card dependant-- all values are accepted, but they are normalized to be in the accepted range.
Ports	Ports on bypass

MIB reference

Data displayed as part of this command is from the svBypassGroupGroupTable and svBypassGroupPortTable in the SANDVINE-MIB.

SNMP notifications

If a bypass group goes into/comes out of bypass mode, these are the SNMP notifications defined in the SANDVINE-MIB:

- svIfBypassGroupInBypassNotification
- svIfBypassGroupActiveNotification

Related alarms

Alarm model 11: Interface bypass group is in bypass mode.

2.13.8 show interface bypass-chassis

Shows current settings and state of the bypass chassis. This command applies to PTS 24000 and PTS 22000 only.

Output	Description
Description (Optional)	Description of the bypass chassis to which the PTS is connected. This is optional. If not set, this field is empty.
AdminStatus	Administrative status of the chassis: <ul style="list-style-type: none">• down - bypass is not connected. This is the default. Note that if a bypass chassis is actually connected, it will operate in the bypass state.• bypass - the bypass module always operates in the bypass state. All traffic is directed around the PTS.• active - the bypass module operates in the active state under normal conditions. In the event of power loss, the bypass module will switch to the bypass state, redirecting the traffic around the PTS. In the event of system failure (such as component failure or system unresponsiveness) or link failure, the bypass module will still operate in the active state.• software - the bypass module operates in the active state under normal conditions. In the event of power loss, software upgrade, component failure or system unresponsiveness, the bypass module will switch to the bypass state, redirecting the traffic around the PTS. In the event of link failure, the bypass module will still operate in the active state.
OperStatus	Operational status of the PTS: <ul style="list-style-type: none">• active — the bypass chassis is directing traffic to the PTS for inspection.• bypass — the bypass chassis is directing traffic around the PTS. If the bypass mode is active or software, an OperStatus of bypass will result in a major alarm being raised (Alarm Model 11: Interface bypass element is in bypass mode)• down — the bypass mode was configured to down, indicating that there is no bypass chassis connected.• hb_fault (external only) — indicates that communication between the PTS and bypass chassis has been lost. This usually indicates that the bypass-chassis is powered down, mis-wired, or mis-configured. A separate alarm is raised (Alarm Model 11: Interface bypass element is in bypass mode).
OperTime	Amount of time in seconds since the last change in the OperStatus.
CommChannel	Console port on the PTS that is connected to the console port on the bypass chassis

2.13.9 show interface configuration

Displays configuration details for all external data and control interfaces in the system.

```
show interface configuration
```

Output	Description
Port	The name of the interface.
AdminStatus	Administrative status of the port - up or down.
OperStatus	Operational status of the port - up or down.
MTU	Maximum transmission unit size, in bytes, for the port. Note: The MTU values on version 6.00 is 16,360. On version 6.20.04 is 15796.
Medium	Port medium: <ul style="list-style-type: none">• 1000BASE-SX• 1000BASE-LX• 1000BASE-CX• 1000BASE-T• 100BASE-LX/LX10• 100BASE-FX• 10BASE-BX• 10BASE-PX• 10GBase-SR• 10GBase-LR• 10GBase-LRM• 10GBase-ER
IfAlias	Name of port if an alias has been specified (using <code>set config interface <interface> alias</code>).
Function	The function that the interface currently serves. One of: <ul style="list-style-type: none">• subscriber - interface is used to intersect data traffic, facing subscribers; in other words the interface's Rx is upstream traffic.• internet - interface is used to intersect data traffic, facing the internet; in other words the interface's Rx is downstream traffic.• cluster - interface is connected to another PTS element in a cluster.• service - interface is connected to a non-PTS service device (such as OCS, SRP). Spanning-tree is disabled.• switch - interface is connected to a non-PTS service device (such as OCS, SRP). Spanning-tree is enabled.• divert - interface is connected to a third-party divert host.• none - interface is not used. An interface cannot be enabled if the function is none. Use when transitioning an interface between functions.
LagPort	Link Aggregation Group associated with the interface.
Shunt	Indicates if a data port is shunting packets.

2.13.10 show interface counters

Shows input/output bytes, packets and errors for all external ports, broken into sections by port type: Data Interfaces, Cluster Interfaces and Management Interfaces. Counters are measured since the associated process, or PTS, was restarted.

```
show interface counters
show interface counters cluster
show interface counters data
show interface counters fabric
show interface counters fabric <interface>
show interface counters <interface>
show interface counters management
show interface counters module
show interface counters module <module>
show interface counters module <module> <interface>
show interface counters npu
show interface counters npu <interface>
```

Attribute	Description
cluster	Shows input/output bytes, packets and errors for external cluster ports.
data	Shows input/output bytes, packets and errors for external data ports.
fabric	Shows input/output bytes/packets/error on internal switch-fabric interfaces.
fabric <interface>	Shows details for a specific internal switch-fabric interface.
<interface>	Shows details for a specific external port.
management	Shows input/output bytes, packets and errors for external management ports.
module	Displays total input/output bytes/packets/errors for all modules, split into two sections Data Interfaces and Other Interfaces.
module <module>	Displays input/output bytes/packets/errors for each interface on a specific module.
module <module> <interface>	Displays details for a specific interface on a specific module.
npu	Shows input/output bytes/packets/error on NPU interfaces.
npu <interface>	Shows details for a specific NPU interface.

Output	Description
Port	Port name of the interface.
BytesIn	The number of bytes coming in.
BytesOut	The number of bytes going out.
PacketsIn	The number of packets coming in.
PacketsOut	The number of packets going out.
DropsIn	The number of packets dropped coming in.
DropsOut	The number of packets dropped going out.

Detailed Output	Description
UnicastPacketsIn	Number of incoming unicast packets.

Detailed Output	Description
MulticastPacketsIn	Number of incoming multicast packets.
BroadcastPacketsIn	Number of incoming broadcast packets.
UnicastPacketsOut	Number of out going unicast packets.
MulticastPacketsOut	Number of out going multicast packets.
BroadcastPacketsOut	Number of out going broadcast packets.
64BytePackets	Number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
65to127BytePackets	Number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
128to255BytePackets	Number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
256to511BytePackets	Number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
512to1023BytePackets	Number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
1024to1518BytePackets	Number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
DiscardsIn	Number of inbound packets chosen to be discarded, even though no errors were detected, to prevent their being deliverable to a higher-layer protocol.
ErrorsIn	Number of errors on inbound traffic.
DiscardsOut	Number of outbound packets chosen to be discarded, even though no errors had been detected, to prevent their being deliverable to a higher-layer protocol.
ErrorsOut	Number of errors on outbound traffic.
UndersizePackets	Number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
OversizePackets	Number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
Fragments	Number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets) and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
AlignmentErrors	Total number of packets received that had a length between 64-1518 octets (excluding framing bits, but including FCS octets), but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
FcsErrors	Number of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check. This count does not include frames received with a frame-too-long or frame-too-short error.
MacTransmitErrors	Number frames for which transmission on a particular interface has failed due to an internal MAC sublayer transmit error.
MacReceiveErrors	Number frames for which reception on a particular interface has failed due to an internal MAC sublayer receive error.

Detailed Output	Description
CarrierSenseErrors	Number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame on a particular interface. The count represented by an instance of this object is incremented at most once per transmission attempt, even if the carrier sense condition fluctuates during a transmission attempt.
FrameTooLong	Number of errors related to frames that are too long.
SymbolErrors	Number of symbol errors.

2.13.10.1 monitor interface counters

Continuously displays input/output bytes, packets and errors for all external ports, broken into sections by port type: Data Interfaces, Cluster Interfaces and Management Interfaces. Counters are measured since the associated process, or PTS, was restarted. Data is updated on stdout every 2 seconds. To terminate a monitor command, press **Ctrl+c**.

```
monitor interface counters
monitor interface counters management
monitor interface counters cluster
monitor interface counters data
monitor interface counters <interface>
monitor interface counters module
monitor interface counters module <module>
monitor interface counters module <module> <interface>
monitor interface counters fabric
monitor interface counters fabric <interface>
monitor interface counters npu
monitor interface counters npu <interface>
```

Attribute	Description
cluster	Shows input/output bytes, packets and errors for external cluster ports.
data	Shows input/output bytes, packets and errors for external data ports.
fabric	Shows input/output bytes/packets/error on internal switch-fabric interfaces.
fabric <interface>	Shows details for a specific internal switch-fabric interface.
<interface>	Shows details for a specific external port.
management	Shows input/output bytes, packets and errors for external management ports.
module	Displays total input/output bytes/packets/errors for all modules, split into two sections Data Interfaces and Other Interfaces.
module <module>	Displays input/output bytes/packets/errors for each interface on a specific module.
module <module> <interface>	Displays details for a specific interface on a specific module.
npu	Shows input/output bytes/packets/error on NPU interfaces.
npu <interface>	Shows details for a specific NPU interface.

Output	Description
Port	Port name of the interface.
BytesIn	The number of bytes coming in.
BytesOut	The number of bytes going out.

Output	Description
PacketsIn	The number of packets coming in.
PacketsOut	The number of packets going out.
DropsIn	The number of packets dropped coming in.
DropsOut	The number of packets dropped going out.

Detailed Output	Description
UnicastPacketsIn	Number of incoming unicast packets.
MulticastPacketsIn	Number of incoming multicast packets.
BroadcastPacketsIn	Number of incoming broadcast packets.
UnicastPacketsOut	Number of out going unicast packets.
MulticastPacketsOut	Number of out going multicast packets.
BroadcastPacketsOut	Number of out going broadcast packets.
64BytePackets	Number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
65to127BytePackets	Number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
128to255BytePackets	Number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
256to511BytePackets	Number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
512to1023BytePackets	Number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
1024to1518BytePackets	Number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
DiscardsIn	Number of inbound packets chosen to be discarded, even though no errors were detected, to prevent their being deliverable to a higher-layer protocol.
ErrorsIn	Number of errors on inbound traffic.
DiscardsOut	Number of outbound packets chosen to be discarded, even though no errors had been detected, to prevent their being deliverable to a higher-layer protocol.
ErrorsOut	Number of errors on outbound traffic.
UndersizePackets	Number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
OversizePackets	Number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
Fragments	Number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets) and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

Detailed Output	Description
AlignmentErrors	Total number of packets received that had a length between 64-1518 octets (excluding framing bits, but including FCS octets), but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error)
FcsErrors	Number of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check. This count does not include frames received with a frame-too-long or frame-too-short error.
MacTransmitErrors	Number frames for which transmission on a particular interface has failed due to an internal MAC sublayer transmit error.
MacReceiveErrors	Number frames for which reception on a particular interface has failed due to an internal MAC sublayer receive error.
CarrierSenseErrors	Number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame on a particular interface. The count represented by an instance of this object is incremented at most once per transmission attempt, even if the carrier sense condition fluctuates during a transmission attempt.
FrameTooLong	Number of errors related to frames that are too long.
SymbolErrors	Number of symbol errors.

2.13.10.2 clear interface counters

Resets the counters used by `show interface counters` to zero. Use this command to analyze traffic or troubleshoot the system.

2.13.10.3 restore interface counters

Restores interface counters displayed by `show interface counters` that have been cleared by `clear interface counters` back to the count since the associated process, or PTS, was restarted.

2.13.11 show interface divert-vlan

Shows currently configured divert VLAN assignments and associated divert ports.

Output	Description
Port	The port that is diverting the VLAN assignment.
VLAN	The VLAN ID.

2.13.12 show interface drops

Displays counters relating to packet drops in the system. PTS only.

External Interfaces Output	Description
Port	Port name of the interface
InDiscards	Number of inbound packets chosen to be discarded, even though no errors had been detected, to prevent their being deliverable to a higher-layer protocol

External Interfaces Output	Description
OutDiscards	Number of outbound packets chosen to be discarded, even though no errors had been detected, to prevent their being deliverable to a higher-layer protocol
AlignErr	Total number of packets received that had a length between 64-1518 octets (excluding framing bits, but including FCS octets), but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error)
FCSErr	Number of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check. This count does not include frames received with a frame-too-long or frame-too-short error.
MacRxErr	Number of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error
MacTxErr	Number of transmission errors associated with a MAC address
SymErr	Number of symbol errors

Switch Fabric NPU Output	Description
Npu	NPU that dropped the packet
SpiPortRxDrop	The number of packets discarded by the NPU when receiving on the SPI port
SpiPortTxDrop	Discard transmitting a packet to the SPI port
XgmiiPortRxDrop	Discard receiving a packet on the XGMII port
XgmiiPortTxDrop	Discard transmitting a packet to the XGMII port

Switch Fabric NPU Output	Description
Port	Port name of the interface
InDiscards	Number of inbound packets chosen to be discarded, even though no errors were detected, to prevent their being deliverable to a higher-layer protocol
OutDiscards	Number of outbound packets chosen to be discarded, even though no errors had been detected, to prevent their being deliverable to a higher-layer protocol
AlignErr	Total number of packets received that had a length between 64-1518 octets (excluding framing bits, but including FCS octets), but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error)
FCSErr	Number of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check. This count does not include frames received with frame-too-long or frame-too-short error.
MacRxErr	Number of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error
MacTxErr	Number of transmission errors associated with a MAC address
SymErr	Number of symbol errors

Switch Fabric Crossbar Output	Description
Port	Port name of the interface
InDiscards	Number of inbound packets chosen to be discarded, even though no errors had been detected, to prevent their being deliverable to a higher-layer protocol
OutDiscards	Number of outbound packets chosen to be discarded, even though no errors had been detected, to prevent their being deliverable to a higher-layer protocol

Switch Fabric Crossbar Output	Description
AlignErr	Total number of packets received that had a length between 64-1518 octets (excluding framing bits, but including FCS octets), but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error)
FCSErr	Number of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check. This count does not include frames received with frame-too-long or frame-too-short errors.
MacRxErr	Number of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error
MacTxErr	Number of transmission errors associated with a MAC address
SymErr	Number of symbol errors

Inspection Modules Output	Description
Port	Port name of the interface
InDiscards	Number of inbound packets chosen to be discarded, even though no errors had been detected, to prevent their being deliverable to a higher-layer protocol
OutDiscards	Number of outbound packets chosen to be discarded, even though no errors had been detected, to prevent their being deliverable to a higher-layer protocol
AlignErr	Total number of packets received that had a length between 64-1518 octets (excluding framing bits, but including FCS octets), but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error)
FCSErr	Number of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check. This count does not include frames received with frame-too-long or frame-too-short error.
MacRxErr	Number of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error
MacTxErr	Number of transmission errors associated with a MAC address

Policy Drops Output	Description
Instance	x.y, where x is the PTS module and y is the processing instance
Block	Number of packets dropped due to the block action
Tcp_reset	Number of packets dropped due to the tcp_reset action
Captive_portal	Number of packets dropped due to the captive_portal and http_response actions
Shaper	Shaper name
Priority	Priority name
Channel	Channel name
Drops	Number of packets dropped by this shaper channel

Packet Inspection Error Output	Description
Instance	x.y, where x is the PTS module and y is the processing instance
DivertError	Error transmitting a packet to a divert destination
PacketParseError	Error parsing a malformed packet
InvalidFlowIndex	Number of packets dropped due to an internal error

Resource Allocation Failure Output	Description
Instance	x.y, where x is the PTS module and y is the processing instance
Packets	Packet dropped because a packet memory buffer could not be allocated
ShapingPackets	Packet dropped because a shaping packet buffer could not be allocated
ShapingQueues	Packet dropped because a shaping queue could not be allocated

2.13.13 show interface internal-mac-lookup

Use this CLI command to perform a lookup of mac, vlan, and ports (external non-data) of a PTS device.

```
show interface internal-mac-lookup port <port>
show interface internal-mac-lookup <vlan>
show interface internal-mac-lookup mac <mac> vlan <vlan>
```

Each command takes either <mac-address>, <vlan>, <vlan> or <port> on which you want to perform lookup. The command output is displayed in tabular format showing up mac, vlan, and port entries.

This command displays a message when no entries are found that correspond to the values specified in the input. It also displays a warning whenever an error occurs during the lookup.

For example,

```
PTS> show interface internal-mac-lookup port 1-7
      No entries available.
```

Attribute	Description
internal-mac-lookup	Show the MAC learned on external non-data ports of the PTS.
Port	The external non-data port is in the form of n-n or lag-n for example 1-1 or lag-2.
VLAN	VLAN ID on which lookup is performed. This range is from 1 to 4094.
MAC	MAC address in the form of XX:XX:XX:XX:XX:XX.

2.13.14 show interface ip-address-tracking

Shows statistics for IP addresses seen on data interfaces.

Output	Description
AddressTrackingEnabled	Indicates if address tracking is enabled.
TotalExternalAddressesOnInternalPorts	Number of external addresses on internal ports

2.13.15 show interface link-group

Shows information about link-groups.

```
show interface link-group
```

```
show interface link-group ports
```

Output	Description
Id	The link-group identifier.
OperStatus	The overall operating status of link-group. Can be one of: <ul style="list-style-type: none"> someLinksDown - The link-group is down due to one or more ports not in linkUp status. allLinksUp - The link-group is transitioning to up; all ports are either linkPartner or linkUp, but their transmitter has not been enabled yet. groupPending - The link-group is transitioning to up; the transmitter of all ports is being enabled. transmitEnabled - The link-group is up, and all ports are linkUp. groupFault - The link-group is faulted due to an internal hardware error. linkGroupDisabled - The link-group has been disabled in the configuration.
Enabled	Indicates whether link-group function is enabled.
Ports	List of ports/interfaces assigned to link-group.

Ports Output	Description
Port	The port/interface number
Group	The link-group identifier that this port is assigned to (0 indicates that the port is not assigned to any link-group).
Status	Operating status of the port. Can be one of: <ul style="list-style-type: none"> linkDown - no incoming signal is detected, and the transmitter is disabled. transmitEnabled - no incoming signal is detected, but the transmitter is enabled. linkPartner - incoming signal detected, but the transmitter is disabled by link-group function. remoteLinkFault - incoming link-fault signal detected from the remote end of the link. linkUp - incoming signal is normal and the transmitter is enabled. adminDown - the port is administratively disabled. localFault - indicates an internal error while applying configuration to hardware.

2.13.16 show interface mac-address-table

Lists the layer 2 addresses learned by one or all data interfaces. This command can be used to see which interface is receiving traffic from a particular MAC, VLAN pair. In some cases, a VLAN of * may be seen, in which case the interface has learned the specified MAC for all VLANs.

```
show interface mac-address-table
```

Output	Description
Vlan	VLAN IDs tagged to ingress packets. May be * to indicate all VLAN IDs
MacAddress	Ethernet MAC address seen on the interface
Interface	Name of the interface that has learned this MAC,VLAN pair

2.13.17 show interface management

Shows the configuration and status of the management interfaces.

```
show interface management
```

Aggregate Output	Description
Port	Indicates that this output concerns the management port.
Redundancy	Indicates if this port is configured with redundancy enabled (failback) or not.
IPAddress	The IP address of this port.
AdminStatus	Administrative status - up or down.
OperStatus	Operational status - up, down, or degraded.
PrimaryPort	If failback is configured, indicates which port is acting as the primary port.
Secondary Port	If failback is configured, indicates which port is acting as the secondary port.
Mtu	The Maximum Transmission Unit (MTU) size.

Member Interfaces	Description
Port	The name of the port.
AdminStatus	Administrative status - up or down.
OperStatus	Operational status - up or down.

Output	Description
Port	Indicates that this output concerns the management port.
Redundancy	Indicates if this port is configured to failback or not.
IPAddress	The IP address of this port.
AdminStatus	Administrative status - up or down.
OperStatus	Operational status - up, down, or degraded.
PrimaryPort	If failback is configured, indicates which port is acting as the primary port.

Output	Description
Port	The name of the port.
Secondary Port	If failback is configured, indicates which port is acting as the secondary port.
MTU	The Maximum Transmission Unit (MTU) size.

2.13.18 show interface modules

This command shows detailed information on pluggable interface modules, such as XFP or SFP+, for each external interface. You can use this command on either the PTS 24000 or 22000.

```
show interface modules
```

```
show interface modules <interface>
```

Output	Description
Port	External interface name
ModuleType	Type of module, if present
AdminStatus	Administrative status - up or down
ModuleStatus	Module status - up or not present
SerialNumber	Module serial number

Module-specific Output	Description
Port	External interface name
ModuleType	Type of module, if present
AdminStatus	Administrative status - up or down
ModuleStatus	Module status - up or not present
SerialNumber	Module serial number
VendorName	The name of the vendor for this module
VendorRevision	The vendor's revision of this module
DataCode	The data code
Medium	The connection medium
Temperature	Temperature of the module
TxPower	The transmitting power
RxPower	The receiving power
Connector	The connector
SupportedInterfaces	The interfaces this module supports
SerialEncoding	The type of serial encoding
NormalBitRate	The normal bit rate for the module
UpperBitRate	The upper bit rate for the module
LowerBitRate	The lower bit rate for the module
Options	The module's options

2.13.19 show interface neighbors

Show peer PTS elements to which local cluster interfaces are connected. Valid for PTS 22000 and 24000 only.

Output	Description
LocalPort	The type and name of the local port.
LocalLAG	The local link aggregation group (LAG) ID.
NeighborPort	The name of the neighbor port on the neighbor PTS element.
NeighborSerial	The serial number of the neighbor PTS element.

2.13.20 show interface network

Shows details for the service and management network interfaces.

Output	Description
Port	Name of the port, either service or management.
AdminStatus	Administrative status - up or down
OperStatus	Operational status - up or down
MTU	Maximum transmission unit size, in bytes, for the port
IPAddresses	Assigned IP address of the port. If the IP address is not configured for the given interface, NA is displayed.

2.13.21 show interface npu assignment

Shows the port, the NPU assignments and the link assignments in the system. For PTS 24000 and 22000 only.

Output	Description
Port	The port name.
NpuAssignment	The NPU processing the traffic to this port.
LinkAssignment	The NPU link processing the traffic to this port.

2.13.22 show interface rate

Shows in and out bitrate, packet rate and drop rate for data interfaces, cluster interfaces and management interfaces.

```
show interface rate
show interface rate module
show interface rate module <module-id>
show interface rate link-aggregation-group
```

Attribute	Description
module	Shows a summary of the bitrates, packet rates and error rates in and out of the modules.
module <module-id>	Shows detailed bitrates, packet rates and error rates for all internal interfaces on a specific module.
link-aggregation-group	Shows cluster interfaces, grouped by LAG.

Output	Description
Port	The port.
Module	The module.
Interface	The interface.
In(bps)	Reception rate, in bits per second.
Out(bps)	Transmission rate, in bits per second.
PacketsIn(pps)	Reception rate, in packets per second.
PacketsOut(pps)	Transmission rate, in packets per second.

2.13.23 show interface spanning-tree instance

Show details for all multiple spanning tree instances in the system, or for the specified instance. Not valid for PTS 8210.

`show interface spanning-tree instance [mstp-instance-id]`

Output	Description
Msti	Multiple spanning-tree instance ID
Port	Name of the port or LAG (Link Aggregation Group)
ForwardingState	Action being applied to this instance and port. Possible forwarding states are: <ul style="list-style-type: none"> Discarding: the port is blocking data traffic, but still forwards BPDUs. Learning: the port is in an intermediate state. Forwarding: the port is open and forwarding traffic. Disabled: the port is not forwarding data traffic or BPDUs. ManualFwd: the port is forced to forward data traffic. NotParticipate: no spanning tree protocol actions will be taken on this port.

2.13.24 show interface spanning-tree instance cst

This command displays CST state on each port contributing to the CST. For example

`show interface spanning-tree instance cst`

```

Instance Port ForwardState
-----
cst      1-1    [disabled]
```

```
cst      1-2      [disabled]
cst      1-3      [disabled]
cst      1-4      [disabled]
cst      1-5      [disabled]
cst      1-6      [disabled]
cst      1-7      [disabled]
cst      1-8      [disabled]
cst      lag-1    [disabled]
cst      lag-2    [disabled]
cst      lag-3    [disabled]
cst      lag-4    [disabled]
cst      lag-5    [disabled]
cst      lag-6    [disabled]
cst      lag-7    [disabled]
cst      lag-8    [disabled]
```

2.13.25 show interface spanning-tree port

Show details about the spanning tree state.

```
show interface spanning-tree port
```

Output	Description
Port	Port name
MstpState	Whether or not multiple spanning-tree protocol is enabled on this port
MstpBpduRx	Number of received Bridge Data Protocol Unit (BPDU) packets. A BPDU packet is used by switches to establish loop-free topologies in a bridged network.
MstpBpduTx	Number of transmitted BPDU packets

2.13.26 show interface spanning-tree vlans

Shows which VLAN IDs the MSTP has assigned to each of the elements in a cluster, and the current state of the VLAN assignments. Not valid for PTS 8210.

VLAN IDs are a value between 3 and 18. The VLAN state can be one of:

- Disabled - the VLAN is not allowed to be assigned to any PTS element.
- Offline - the VLAN is allowed for assignment. It may not be assigned to any PTS element yet, or the network connection to the PTS element that has this VLAN assigned is not established yet.
- Learn - the connection to the PTS element that has this VLAN assigned is being established.
- Online - the local element has the VLAN assigned, or the connection to the PTS element that has this VLAN assigned has been established.

Output	Description
Serial	Element's serial number
VlanId	VLAN ID assigned to that element
VlanIdState	State of the VLAN ID assignment
HostName	Host name of the element. For example, clusterX PTS1

Output	Description
Msti	The MSTP instance associated to the VLAN ID

2.13.27 show interface vlan-tagging

Shows the data-ports on the element, their configured VLAN IDs and, optionally, their VLAN priority.

Output	Description
Port	Port name for the data-interface.
Vlan	Configured VLAN ID for this port.
Priority	Configured VLAN priority for this port.

2.13.28 show log

Shows the log file of all significant events or issues detected by the system. Shows high level version information for the system including installed Sandvine products.

```
show log
```

2.13.29 show log authentication

This command displays the contents of the authentication log file.

```
show log authentication
```

2.13.30 show log cli

Shows the audit log for every CLI command run on the element. Use this information to track configuration changes.

```
show log cli
```

Logged information includes:

- Date
- Start and end time
- Element on which the command was run
- User that ran the command
- Group that the user belongs to
- The command that was run
- Session ID for commands run from the CLI

Use the `monitor log cli` CLI command to monitor the CLI audit logs.

2.13.31 show log control-center

This command displays the Control Center related audit logs.

```
show log control-center
```

2.13.32 show log install

This command lists logs related to PTS installations, upgrades and so on.

```
show log install
```

2.13.33 show log mac-movement

This command is used to display the MAC movement logs captured on external non-data interfaces.

```
show log mac-movement
```

2.13.34 show policy

Displays the contents of the policy.conf file. If other policy files are included in the policy.conf file, then those files are listed using tab completion of this command.

```
show policy
show policy <policy-file>
```

2.13.35 show policy attacks

Shows statistics generated by the detection aggregator that give an overall view of attacks being detected, processed and dispatched for mitigation. Its a useful mechanism for refining an attack policy.

Output	Description
Type	Type of attack and the corresponding numeric ID: <ol style="list-style-type: none">1. Events Detected2. Active Detection Sessions3. Active Group Sessions4. All Detections5. Total Detection Sessions6. Events Received7. Events Processed8. Current Attack Objects
Value	Number of instances by type

2.13.36 show policy attacks detections

Shows the attack type by ID and the number of times that attack type was detected. The attack type is defined by policy. The number of attacks is counted from the time the attack type is defined and implemented in policy.

Output	Description
Attack types	The type of attack and the corresponding numeric Id: <ol style="list-style-type: none">1. address-scan2. flow-flood3. signature-match4. syn-flood5. user-bandwidth6. spam7. dns-domain-flood8. dns-request-flood9. dns-outstanding-sessions For attack type definitions, see the <i>SandScript Configuration Guide</i> .
Detections	Number of attacks by type.

2.13.37 show policy attacks detections stats

Shows statistics related to attack detection.

Attack Detection Stats Output	Description
Instances	The sum of the values returned from previous executions of this command
Actions	Number of actions taken against detection
AllocationFailures	The number of memory failures upon attack detection
Published	Number of times attack detection has been written to the database
PublishedRecords	Number of times event logs have been written to the database. The PTS writes to the SPB.

2.13.38 show policy attacks rules

Shows information related to attack policy rules in place. The rules are written in policy.

Rules are supplied and updated by Sandvine in the policy.sandvine.conf file. If additional rules are required, they can be added to the policy.cluster.conf file on an element:

- detection-config rules configure algorithms used to find events
- aggregator-config rules determine how events are grouped and filtered to determine if an attack is occurring
- wmd-rules are used to configure mitigation to block malicious traffic
- monitor-config rules are used to configure non-detection related features such as QoE and VOIP.

Output	Description
Id	The numeric rule ID as defined by user policy
Active	Rule is active - true or false
Start	Specifies the start time for the rule in a 24 hour cycle. The rule is not active all the time. It is started by a time assignment in the policy, similar to a job on UNIX.
End	Specifies the end time for the rule in a 24 hour cycle. The rule is not active all the time. It is ended by a time assignment in the policy, similar to a job on UNIX.
Rule	Rule name. For example, address-scan src-class all-external transport udp. This name is set by the client policy.

2.13.39 show policy attacks rules counts

Shows the attack rules counts based on rule ID as defined in policy.

Output	Description
Id	The ID of the rule
ActiveActions	The number of active actions
TotalActions	The total number of actions
Packets	The number of packets this rule acted on
Bytes	The number of bytes this rule acted on
DroppedPackets	The number of packets dropped by this rule
DroppedBytes	The number of bytes dropped by this rule
DroppedActions	The number of actions dropped by this rule

2.13.40 show policy attacks rules <id>

Shows information related to a single attack policy rule called by ID. The output is based on the hard-coded numeric ID of the attack policy.

Output per Attack Rule	Description
Active	Rule is active - true or false
Start	Specifies the start time for the rule in a 24-hour cycle. The rule is not active all the time. It is started by a time assignment in the policy, similar to a job on UNIX.
End	Specifies the end time for the rule in a 24-hour cycle. The rule is not active all the time. It is ended by a time assignment in the policy, similar to a job on UNIX.
Order	The rule's precedent, as set in policy
Status	Rule status. If the rule is not active (Active is False), then additional information may be provided.
ActiveActions	Number of active actions for this rule from its commencement

Output per Attack Rule	Description
TotalActions	Number of actions taken as response to this rule
Packets	Number of packets that the detection thinks are part of the attack
Bytes	Number of bytes that the detection thinks are part of the attack
DroppedPackets	Number of dropped packets resulting from the attack
DroppedBytes	Number of dropped bytes resulting from the attack
DroppedActions	Number of dropped actions resulting from the attack
Rule	Rule name. For example, address-scan src-class all-external transport udp. This name is set by the client policy.

2.13.41 show policy attacks rules patterns

Shows information related to attack patterns.

Output	Description
Id	Numeric ID of the rule pattern. Set in policy.
PatternName	Pattern name. For example: aol-admin.
MalwareName	Malware associated with the pattern. For example: AOL Admin Trojan.

2.13.42 show policy attacks rules stats

Shows statistics about policy attack rules.

Output	Description
Instances	The number of rule instances
Actions	The number of actions
AllocationFailures	The number of allocation failures
Published	The number of published rules
PublishedRecords	The number of published records

2.13.43 show policy attacks rules status

Shows the attack rule status.

Output	Description
Id	Numeric ID of the rule. Set in policy.
Active	Rule is active - true or false

Output	Description
Rule	A description of the rule and the time delimitation by which it is run. For example: 5 min.
Status	Rule status. For example: Rule has insufficient priority.

2.13.44 show policy attacks signature-match

Shows the cumulative signature match counters for packet inspection.

If the signature that you require does not exist in pattern.sandvine.conf, you can create the signature. Network protection signatures are added to /usr/local/sandvine/etc/policy.cluster.conf.

Output	Description
FlowsMatched	Number of flows that had a signature-match
FlowsProcessed	Number of flows processed
RegexesApplied	Number of regular expressions that were applied
CurrentInfectedHosts	Number of hosts currently infected
CurrentActiveSignatures	Number of signatures currently active

2.13.45 show policy attacks spam

Shows statistics generated by the spam detection engine.

Output	Description
ActiveSpamProcessors	Number of active spam processors
PacketsParsed	Number of packets parsed
SmtpFlows	Number of email traffic flows
SmtpFlowsForwardedToProcessor	Number of email traffic flows forwarded for processing
SmtpFlowTimersExpired	Number of email traffic flows that have an expired timer
SmtpHosts	Number of email hosts
InvalidDomains	Number of invalid domains

2.13.46 show policy classifier

Shows information about all classifiers or a specific classifier defined in SandScript. You can use classifiers to apply labels to SandScript contexts like flows or subscribers, and to categorize SandScript contexts into meaningful groups.

```
show policy classifier
```

```
show policy classifier [classifier-name]
```

```
show policy classifier *
```

You can publish traffic that is measured unique-by for one or more classifiers and generate custom reports in Network Demographics.

Output	Description
Name	Name of the classifier
Type	The classifier type
Instances	Number of instances of the classifier
Value	Value that SandScript defines for the classifier type
SetCount	Number of times the classifier or the value of the classifier is set

2.13.47 show policy classifier stats

Shows statistics of all classifiers.

```
show policy classifier stats
```

Output	Description
MaxInstances	Maximum number of instances
CurrentInstances	Number of current instances
MaxInstancesExceeded	Number of times the maximum number of instances was exceeded
UnassignedInstances	Number of unassigned instances
InvalidAssignments	Number of invalid assignments

2.13.48 show policy controller

Shows general information about each Dynamic Control System instance defined in policy using the controller syntax. Using the * wildcard results in details being shown for all controllers.

```
show policy controller
```

```
show policy controller <name> instance <int>
```

Output	Description
Name	Controller name defined in policy
Interval	The sample interval as defined in policy. This value represents the amount of time the controller will collect data before calculating QoE and generating a new output.
Minimum	The minimum value as defined in policy. The controller output, which can determine the bitrate of a shaper, will not go below this value.
Maximum	The maximum value as defined in policy. The controller output, which can determine the bitrate of a shaper, will never go beyond this limit.
Instances	The total count of unique instances of the controller (unique values in the controller unique-by clause).

Output	Description
UniqueBy	The unique by expression specified in the policy definition. This restricts the expression data types when performing a unique by controller action, and ensures schema synchronization with the SPB for publishing.

Instance Output	Description
Output	The current value of the controller. This value is updated on a time interval as specified by the 'interval' parameter in the controller definition. This value may be used as the rate for a dynamic shaper. This value carries little or no meaning if no dynamic shaper is specified. The value has no units, but will represent a bitrate when in use by a dynamic shaper.
Score	The current QoE score calculated by the controller. This value is updated according to the interval specified in the controller definition. This value is used by the controller to determine the output value.
Demand	This value will only be populated if there is a dynamic shaper present, and will display '---' otherwise. When a dynamic shaper exists, the current demand on the shaper will be displayed here. If the demand is below the output, it can be understood that there is no enforcement occurring; conversely, a demand greater than the output indicates enforcement is occurring.
Audited	Determines whether that particular controller instance is audited or not. Returns "true" or "false".

Instance Output	Description
Name	The metric name as defined in policy
ZeroScoreBenchmark	The metric value that results in a score of zero. This is derived from (<i>benchmark*tolerance factor</i>)
Benchmark	The QoE benchmark value as defined in SandScript
Value	The value that has been calculated for this metric during the last run of the controller. This value represents the <i>Nth</i> percentile QoE measurement, where N is taken from the sandScript 'percentile' configuration parameter. This value is used to calculate the overall instance score.
Samples	This parameter provides number of samples of a metric that a QualityGuard instance collects during an evaluation interval.

2.13.49 show policy count

Shows statistics about counts defined in policy, including port, demographic, subscriber, and protocol statistics. This command also shows various logging information, including last interval timestamps.

Port Stats Output	Description
LogTimePrev	Last time port statistics were logged
LogTimeRemaining	Seconds left until port statistics are logged
LogIntervalCount	Number of intervals that port statistics have been logged

Demographic Stats Output	Description
LogTimePrev	Last time demographic statistics were logged
LogTimeRemaining	Seconds left until demographic statistics are logged

Demographic Stats Output	Description
LogIntervalCount	Number of intervals that demographic statistics have been logged
Instances	Number of stat rows that were written
Actions	Number of policy actions that were applied to a flow to run demographic stats
AllocationFailures	Number of demographic statistic records that failed to publish
FlowSkippedInterval	Number of skipped flow intervals
Published	Number of times the expression has been published
PublishedRecords	Number of published demographic statistic records

Subscriber Stats Output	Description
BasicLogTimePrev	Last time subscriber statistics were logged
BasicLogTimeRemaining	Seconds left until subscriber statistics are logged
BasicLogIntervalCount	Number of intervals that subscriber statistics have been logged
ProtocolLogTimePrev	Last time when protocol statistics were logged
ProtocolLogTimeRemaining	Seconds left until protocol statistics are logged
ProtocolLogIntervalCount	Number of intervals that protocol statistics have been logged
SubBasicFilterCount	Subscriber basic filter count

2.13.50 show policy count demographic

Shows statistics for network class to network traffic, as well as basic port statistics. Use this command to view logging and interval information, as well as to view how many statistic records have been published to the SPB.

Demographic Stats Output	Description
LogTimePrev	Last time demographic statistics were logged
LogTimeRemaining	Seconds left until port statistics are logged
LogIntervalCount	Number of intervals that port statistics have been logged
Instances	Number of instances
Actions	Number of actions
AllocationFailures	Number of demographic statistic records that failed to publish
FlowSkippedInterval	Number of skipped flow intervals
Published	Number of times the expression has been published
PublishedRecords	Number of published demographic statistic records

2.13.50.1 show policy count demographic connections

Shows information for demographic network protocols that have been seen during statistic generation.

Demographic Connections Output	Description
ProtocolCounted	The number of protocols counted
NewProtocolCounted	The number of new protocols counted.

2.13.50.2 show policy count demographic hosts

Shows information for demographic host information, including hash statistics and number of protocols counted.

Hosts Output	Description
HashEntries	The number of entries
HashCollisions	The number of collisions
HashPopulatedBuckets	The number of populated buckets
HashSize	The size of the hash
HashSmallHostNodes	The number of small host nodes
HashLargeHostNodes	The number of large host notes
PrevHashEntries	The number of previous hash entries
PrevHashCollisions	The number of previous hash collisions
PrevHashPopulatedBuckets	The number of previous populated buckets
PrevHashSize	The previous size of the hash
PrevHashSmallHostNodes	The number of previous small host nodes
PrevHashLargeHostNodes	The number of previous large host nodes
PeakHashEntries	The peak number of has entries
Counted	The count
NewCounted	The new count
ProtocolCounted	The number of protocols counted
NewProtocolCounted	The number of new protocols counted
Current	The current
MaxHostsExceeded	The maximum number of hosts exceeded

2.13.51 show policy count port

Shows basic port statistics. Use this command to display logging information and interval counts.

Output	Description
LogTimePrev	Last time port statistics were logged
LogTimeRemaining	Seconds left until port statistics are logged
LogIntervalCount	Number of intervals that port statistics have been logged

2.13.52 show policy count subscriber

Shows statistics about subscriber counts defined in policy. Use this command to display logging information and interval counts.

Subscriber Stats Output	Description
BasicLogTimePrev	Last time subscriber statistics were logged
BasicLogTimeRemaining	Seconds left until subscriber statistics are logged
BasicLogIntervalCount	Number of intervals that subscriber statistics have been logged.
BasicFilterCount	Subscriber basic filter count
ProtocolLogTimePrev	Last time protocol statistics were logged
ProtocolLogTimeRemaining	Seconds left until protocol statistics are logged
ProtocolLogIntervalCount	Number of intervals that protocol statistics have been logged

2.13.52.1 show policy count subscriber [*, basic, protocol]

Shows statistics about subscriber counts defined in policy. Use this command to display information about statistic record generation.

```
show policy count subscriber *  
show policy count subscriber basic  
show policy count subscriber protocol
```

Basic and Protocol Stats Output	Description
Published	Number of times the expression has been published
Instances	Number of instances
AllocationFailures	Number of subscriber/protocol statistic records that failed to publish
Actions	Number of actions
PublishedRecords	Number of published subscriber/protocol statistic records

2.13.53 show policy destination

Identifies configured policy destinations and determines status for these destinations.

```
show policy destination  
show policy destination <name>  
show policy destination <destination>
```

Tee Destinations Output	Description
Name	Destination name
Status	Reachability of the destination
PacketsTeed	Number of packets teed to the destination
BytesTeed	Number of bytes teed to the destination
Payload	Indicate which part of the original packet is being teed

Tee Destinations Output	Description
Headers	Indicate the headers prepended to the original packet in order
IpAddr	Specified IP address of the destination
EtherAddr	Ethernet address of the destination
Actions	Number of flows considered to be teed, not necessarily actually teed (internal debugging only)

IPMAP Destinations Output	Description
Name	Destination name
Status	Reachability of the destination
PacketsTeed	Number of packets teed to the destination
BytesTeed	Number of bytes tee occurred to the tee destination
Payload	Which part of the original packet is being teed
Headers	Headers prepended to the original packet in order
IpAddr	Specified IP address of the destination
EtherAddr	Ethernet address of the destination
Actions	Number of flows considered to be teed, not necessarily actually teed (internal debugging only)

FILE Destinations Output	Description
Name	Destination name
FileName	Capture file
Status	Reachability of the destination
Payload	Which part of the original packet is being teed
MaxSize	Maximum size of a single file used for capture
MaxFiles	Maximum number of files used for capture
OverWrite	If the maximum number of files used for capture is reached, should capturing overwrite existing files so that only the latest are captured
Actions	Number of flows considered to be teed, not necessarily actually teed (internal debugging only)
PacketsTeed	Number of packets sent to the file destination
BytesTeed	Number of bytes sent to the file destination

DIVERT Destinations Output	Description
Name	Destination name.
TotalFlows	The total number of flows the destination has diverted.
Status	Reachability of the destination.
currentFlows	Number of flows diverted to the divert destination.
currentErrors	The current number of flows the desination is diverting.
rxPackets	Number of packets received on the divert port.
txPackets	Number of packets sent from the divert port.
RxBytes	The total number of bytes the PTS has received from the destination.

DIVERT Destinations Output	Description
TxBytes	The total number of bytes the PTS has sent to the destination.
admin status	Indicates whether the destination is administratively up or down. If it is up then the destination behaves as normal. If it is set to down then no new flows will be diverted to that destination.
ClientRsts	Total number of flows where client sends RST on diverted flow.
ServerRsts	Total number of flows where server sends RST on diverted flow.
ReplayedBytes	The number of bytes that have been replayed to the divert host.
HostReplayOutOfOrder	Total number of packets not forwarded to client/accepted by PTS as replayed packet because it is out of order.
RetransmitToDivertHost	Total number of replayed/TCP handshake packets that need to be retransmitted by PTS.
HostTimeout	The number of times the connection to the divert host has timed out.
IncompatibleOption	The number of times the divert host sent options that were incompatible with the flow.
HostModifyReplayedPkt	The number of times the divert host has modified one of the replay packets.
UnableToSend	The number of times the PTS was unable to send data to the divert host.

Divert Sequence Destinations Output	Description
Name	Destination name
Status	Reachability of the destination
Flows	Number of flows diverted to the destination
Errors	Number of errors in divert
MaxConnections	Maximum number of flows which can be diverted at any time
Mtu	Maximum transmission unit specified
ResetServer	Divert destination in the policy. If true, half divert is used. Otherwise full divert is used.
TcpSyn	Divert destination needs to have the TCP packets in the 3-way handshake diverted to it - true or false
Actions	Number of flows considered to be teed, not necessarily actually teed (internal debugging only)
MaxConnectionsExceeded	Number of times that the maximum connections limit was exceeded
ChildDestinations	List of divert destinations specified for the sequence

Group Destinations Output	Description
Name	Destination name
Type	Type of destination within the destination group
RampInterval	Ramping is in process - true or false
RampIteration	Specifies Number of ramp-up iterations to perform before teeing/diverting a full load of traffic to the destination

Destination Counters	Description
hostTimeout	The number of times the divert host connection has timed out.
incompatibleOption	The number of times the divert host sent options that were incompatible with the flow.

Destination Counters	Description
hostModifyReplayedPkt	The number of times the divert host modified replay packets.
unableToSend	The number of times that the PTS could not send data to the divert host.
errors	Identifies the current number of errors.
totalErrors	Identifies the total number of errors.
TotalFlows	Identifies the total number of flows sent to the divert destination.
TotalRxBytes	The total number of bytes received from the divert host. Note: The number of bytes, including the Ethernet CRC header, received on the divert port. The minimum Ethernet payload is calculated to be 46 octets according to IEEE 802.3.
TotalTxBytes	The total number of bytes sent to the divert destination. Note: The number of bytes, including the Ethernet CRC header, sent from the divert port. The minimum Ethernet payload is calculated to be 46 octets according to IEEE 802.3.
ClientRST	The total number of flows where the client sends an RST on a diverted flow.
ServerRST	The total number of flows where the server sends an RST on a diverted flow.
HostReplayOutOfOrder	The total number of packets not forwarded to client, or that the PTS accepts as replayed packets because they are out of order.
RetransmitTotDivertHost	The total number of replayed/TCP handshake packets that the PTS has to retransmit.

2.13.54 show policy divert

This shows the total number of flows diverted.

```
show policy divert
```

2.13.55 show policy dpm

Shows DNS Policy Module (DPM) statistics.

Output	Description
Id	DPM counter ID
Name	DPM counter name
Value	Numeric value of the DPM counter
Units	Unit of measurement for the DPM counter

2.13.56 show policy errors

Shows error conditions that can occur at SandScript runtime.

```
show policy errors
```

Output	Description
Error	Type of error

Output	Description
Count	Number of times the error occurred
Severity	Severity of the error

Output	Description
Id	Policy error ID
Name	Error name
Count	Error count

2.13.57 show policy flow-detector

Shows statistics for individual flow detectors.

Subscriber flows are analyzed using rules in the policy.conf file for the cluster. Rules define the type of Top Talker search to be run and the actions to be taken based on data collected by detailed user statistics.

Output	Description
Id	Numeric ID of the flow detector
NewFlows	
RetiredFlows	
FlowPackets	
FlowDetector	Type of flow detector
AbortedFlows	
Consumer	
UserLimitMessages	The limit for user messages
LimitMessageConsumer	Indicates if a limit is applied to the message consumer
UserTxLimitMessages	The outgoing limit for user messages

2.13.58 show policy healthcheck

Shows information about health checks that have been defined in policy.

Health checks are used in destination groups to monitor destination health and balance accordingly across the destinations in the group.

Ping Health Checks Output	Description
Description	Name and IP combination as specified in policy
Name	Name of the health check as specified in policy

Ping Health Checks Output	Description
IntervalSec	Interval in seconds that the health check is transmitted
TimeoutMs	Timeout in milliseconds to wait for a health check response
Retry	Number of consecutive intervals to retry a failed health check before it is transitioned to a down state
RetryFailure	Number of consecutive intervals that a health check must succeed before it is transitioned to the up state
Ip	IP address of the host that is being checked
Status	Whether or not the host is up or down as determined by the health check
Checks	Number of health checks that have been initiated as defined by the interval
Failures	Number of health checks that have failed
Timeouts	Number of health checks with no response

HTTP Health Check Output	Description
Description	Name and IP combination as specified in policy
Name	Name of the health check as specified in policy
IntervalSec	Interval in seconds that the health check is transmitted
TimeoutMs	Timeout in milliseconds to wait for a health check response
Retry	Number of consecutive intervals to retry a failed health check before it is transitioned to a down state
RetryFailure	Number of consecutive intervals that a health check must succeed before it is transitioned to the up state
Port	Listening port on the server used to accept HTTP connections
Path	Resource path that is specified in the HTTP header request
RequestVersion	Request version to be used in the HTTP header
ResponseRegex	Regular expression applied to the HTTP response to determine the health of the host
Ip	IP address of the host that is being health checked
Status	Whether or not the host is up or down as determined by the health check
Checks	Number of health checks that have been initiated as defined by the interval
Failures	Number of health checks that have failed
Timeouts	Number of health checks with no response

Inline Health Check Output	Description
Description	Name and VLAN combination as specified in policy
Name	Name of the health check as specified in policy
IntervalSec	Interval in seconds that the health check is transmitted

Inline Health Check Output	Description
TimeoutMs	Timeout in milliseconds to wait for a health check response
Retry	Number of consecutive intervals to retry a failed health check before it is transitioned to a down state
RetryFailure	Number of consecutive intervals that a health check must succeed before it is transitioned to the up state
SrcIp	Source IP address used in the health check packet. Can arbitrarily be any private IP. The default is 10.0.0.0.
DstIp	Destination IP address used in the health check packet. Can arbitrarily be any private IP. The default is 10.0.0.1.
Ttl	Time to live used in the health check packet
Vlan	VLAN to encapsulate the health check packet in
Status	Whether or not the configured L2 network managing this VLAN is considered to be up or down as determined by the health check
Checks	Number of health checks that have been initiated as defined by the interval
Failures	Number of health checks that have failed
Timeouts	Number of health checks with no response

2.13.59 show policy histogram

Displays information about histograms defined in SandScript. You can declare histograms through SandScript to define bins for use with histogram measurements.

```
show policy histogram
```

```
show policy histogram *
```

See the *SandScript Configuration Guide* for a detailed description of histograms and the syntax to define them.

Output	Description
Name	Name of the histogram that the measurement uses to count its data.
Type	Type of histogram. SandScript defines histograms by type. The types of histograms listed in this field mirror the ones in the client SandScript. The types of histograms are: <ul style="list-style-type: none">• Linear—Evenly-spaced bins that you can define over a range of floating point numbers• Custom—Bin ranges that you define explicitly
Bins	Size of the bin. SandScript defines a histogram as a bucket/bin specification. It also defines the number and size of each bucket/bin. Measurements use histograms to do meaningful calculations.
Lookups	The number of lookups performed on this histogram.

2.13.60 show policy inspection

Shows general inspection counters.

```
show policy inspection
```

```
show policy inspection actions
```

```
show policy inspection flows
```

```
show policy inspection traffic
```

The counters are:

- number of flows timed out in the inspected state
- number of flows not inspected because the inspection engine was too busy
- number of flows discarded by the inspection engine
- total number of flows sent to the inspection engine.

Attribute	Description
actions	inspection counts for actions
flows	inspection counts for flows
traffic	inspection counts for traffic

Inspection Output	Description
Timeout	Timeout in seconds
PacketNotInspected	Number of packets not inspected
NoDaemon	Number of times there was no daemon
PacketsToDaemon	Number of packets to the daemon

Actions Output	Description
Allowing Flow	Allowing flow
Counting Flow	Counting flow
Diverting Tcp Flow	Divert TCP flow
Diverting Udp Flow	Divert UDP flow
Marking Tcp Flow	Marking TCP flow
Marking Udp Flow	Marking UDP flow
Reset Flows	Reset flow
Captive Portal	Number of captive portals

Flows Output	Description
Total	Total number of inspection flows
Available	Total number of available flows
New	Number of new flows

Flows Output	Description
Available Exceeded	The available exceeded

Traffic Output	Description
Bitrate	Bitrate
BridgedPackets	The number of packets being bridged
Rx Packets	Received packets
Rx Ip	Received IP bytes
Rx Tcp	Received TCP
Rx Udp	Received UDP
Rx Icmp	Received ICMP
Rx Other Ip	Data received from other IPs
Rx Bytes	Received bytes
Rx Ip Bytes	Received IP bytes
Rx Keepalive	Received keep alive
Rx Keepalive Bytes	Received keep alive bytes

2.13.61 show policy limiter

Shows statistics on limiters that have been implemented for Session Management.

Limiters provide advanced control over when actions are executed. They can be used to apply actions after a threshold (like number of connections) is exceeded, or can be used to define a control system to manage the amount of bandwidth on the network. Limiters are declared in policy and referenced by rules. For details on limiters, refer to the *SandScript Configuration Guide* for this release.

Syntax

```
show policy limiter
```

```
show policy limiter [name]
```

Output	Description
Name	Limiter name.
ClusterLimit	Limit allowed across the cluster.
Limit	Maximum value allowed by the limiter per module.
Current	Current value of the limiter.
Units	Units of the limiter as defined in policy.
Limited	The number of times the Limit action associated with this limiter has evaluated to true.

Additional Output for named Limiters	Description
Priority	Name of the limiter priority.
Probability	
Evaluations	Number of times the Limit action associated with this limiter has been evaluated.
IError	
DError	
PTerm	
ITerm	
DTerm	
Control	

2.13.62 show policy map

Shows information about configured SandScript maps or for a specific map by name. You can use SandScript maps to define groups of items and test to see if the items are part of a SandScript group.

```
show policy map
```

```
show policy map [map name]
```

Output	Description
Name	Map name defined in PTS policy
Type	Type of patterns held in the map. Possible options are string, hostname and URL.
LabelType	Optional label type for map entries: integer, string or none
Normalize	Map is normalized - true or false
ResourceParamMatchOrder	How URL parameters should be matched against the pattern. Possible options are exact (the order of parameters is important) or any (the order of parameters does not matter). Only valid for URL maps.
Entries	Number of entries in the map
Size	Memory used by the map on the PTS in bytes
Hits	Number of map lookups that returned true
Queries	Number of map lookups initiated from policy
LastReloadStatus	Status of the last attempted hitless reload of the map - success or fail

Output	Description
Name	Map name that you defined in SandScript.
Type	Type of patterns in the map. Possible options are string, hostname, and URL.
LabelType	Optional label type for map entries: integer, string, or none.
ResourceParamMatchOrder	How the map matches Uniform Resource Locator (URL) parameters against the pattern. Possible options are exact (the order of parameters is important) or any (the order of parameters is irrelevant). This output field is valid for URL maps only.
Entries	Number of entries in the map.
Size	Memory on the SDE (in bytes) that the map uses.

Output	Description
Hits	Number of map lookups that returned true.
Queries	Number of map lookups initiated from SandScript.
LastReloadStatus	Whether the last attempt of a hitless reload of the map was successful.
Normalize	Whether the map is normalized.
CaseSensitive	Whether the map is case sensitive.

2.13.63 show policy measurement

Shows information about the results of detailed measurements created for policies.

```
show policy measurement <list>
show policy measurement <list> instance <unique-instance>
show policy measurement namespace *
show policy measurement namespace <name>
show policy measurement
```

Measurements Output	Description
Name	Measurement name.
Over	Interval over which the measurement was taken.
Units	Units of the measured data.
Value	Numeric value of the measurement.
Peak	Measurement peak.
LastValue	Last numeric value of the measurement.
LastPeak	Last measurement peak.

Unique-by Measurements Output	Description
Name	Measurement name.
UniqueBy	What this measurement is unique-by.
Over	Interval over which the measurement was taken.
Units	Units of the measured data.
Instances	Number of instances of a unique-by measurement during the current publish interval.
PeakInstances	Peak number of instances of a unique-by measurement during the current publish interval.
Peak	Measurement peak.
Total	Total for the measurement.
PeakTotal	Peak total for the measurement.
Average	Average value measured in the histogram (sum divided by samples).

Unique-by Measurements Output	Description
LastPeakInstances	Last peak instance.
LastPeak	Last measurement peak.
LastPeakTotal	Total of the last peak.

Top-N Measurements Output	Description
Name	Measurement name.
UniqueBy	What this measurement is unique-by.
Over	Interval over which the measurement was taken.
Units	Units of the measured data.
LastPeakInstances	Last peak instance.
LastPeakTotal	Total of the last peak.
Top	Quantity in the top.

Histogram Measurements Output	Description
Name	Measurement name.
Histogram	Histogram that the measurement uses to count its data.
Over	Interval over which the measurement was taken.
Units	Units of the measured data.
Min	The minimum value observed by the measurement during the current publish interval.
Max	The maximum value observed by the measurement during the current publish interval.
Sum	The sum of all values observed by the measurement during the current publish interval.
Samples	Number of measured values during the current publish interval.
Average	Average value measured in the histogram (sum divided by samples).
LastMin	The minimum value observed by the measurement during the previous publish interval.
LastMax	The maximum value observed by the measurement during the previous publish interval.
LastSum	The sum of all values observed by the measurement during the previous publish interval.
LastSamples	Number of measured values during the previous publish.
LastAverage	Average value measured in the histogram during the previous publish interval (LastSum divided by LastSamples).
BinLower	The lower range of this histogram bin (inclusive).
BinUpper	The upper range of this histogram bin (exclusive).
Samples	Number of measured values during the previous publish interval in this histogram bin.
Percent	The percentage of samples that fell in this histogram bin during the previous publish interval.

Histogram Measurements Output	Description
Cumulative	The percentage of samples that fell in this or any preceding histogram bin during the previous publish interval.
Graph	A graphical representation of the size of this histogram bin in the previous publish interval.

Unique-by Histogram Measurement	Description
Name	Measurement name.
Histogram	Histogram that the measurement uses to count its data.
UniqueBy	What this measurement is unique-by.
Over	Interval over which the measurement was taken.
Units	Units of the measured data.
Instances	Number of instances of a unique-by measurement during the current publish interval.
Min	The minimum value observed by the measurement during the current publish interval.
Max	The maximum value observed by the measurement during the current publish interval.
Sum	The sum of all values observed by the measurement during the current publish interval.
Samples	Number of measured values during the current publish interval.
Average	Average value measured in the histogram (sum divided by samples).
LastInstances	Number of instances of a unique-by measurement during the previous publish interval.
LastMin	The minimum value observed by the measurement during the previous publish interval.
LastMax	The maximum value observed by the measurement during the previous publish interval.
LastSum	The sum of all values observed by the measurement during the previous publish interval.
LastSamples	Number of measured values during the previous publish.
LastAverage	Average value measured in the histogram during the previous publish interval (LastSum divided by LastSamples).

2.13.64 show policy publish

Shows a list of published expressions that are currently active.

You can use published expressions for custom reports. Published expressions provide a way to report on the value of a SandScript expression over time. The value of an expression is periodically sampled and stored in the database. Network Demographics Server reports use this data.

The sampling period defaults to 15 minutes (900 seconds), but you can configure it.

 **Note:** The sampling period is a global variable which affects all published expressions.

An expression for publishing must be a scalar, integer-valued expression. A scalar expression is one whose value is not tied to a particular flow, packet, or subscriber.

Published expressions are part of the `/usr/local/sandvine/etc/policy.conf` file.

`show policy publish`

Published Expressions Output	Description
Name	Expression name as defined in SandScript
LastGaugeValue	Value of the expression at the end of the most recent publication interval
LastIntervalValue	Value of the expression at the end of the most recent publication interval minus its value at the end of the previous publication interval
Units	Units of the published expression
Published	Number of times the expression was published
LastPublishTime	Last time the expression was published

Unique-by Published Expressions Output	Description
Name	Expression name as defined in SandScript
Units	Units of the published expression
Published	Number of times the expression was published
Instances	Number of unique instances or records that were published
LastInstances	Number of instances that were published the last time the expression was published
LastPublishTime	Last time the expression was published

2.13.65 show policy shaper

Shows statistics on shapers that are implemented for SandScript policies, including the shapers that are configured, and those that are functioning correctly.

The values that the `show policy shaper` commands display are instantaneous, giving a snap-shot of shaper activity. Traffic bursts and queue sizes can contribute to outputs that are not necessarily representative of the overall shaper behavior.

See the *SandScript Configuration Guide* for a detailed description of shaping policies.

```
show policy shaper
show policy shaper <list>
show policy shaper <list> instance <unique-instance>
show policy shaper <list> instance <unique-instance> priority
show policy shaper <list> instance <unique-instance> priority *
show policy shaper <list> instance <unique-instance> priority <name>
show policy shaper <list> instance <unique-instance> priority <name> channel
show policy shaper <list> instance <unique-instance> priority <name> channel *
show policy shaper <list> instance <unique-instance> priority <name> channel <name>
show policy shaper <list> priority
show policy shaper <list> priority *
show policy shaper <list> priority <list>
show policy shaper <list> priority <list> channel
show policy shaper <list> priority <list> channel *
show policy shaper <list> priority <list> channel <list>
show policy shaper <name> config
show policy shaper <name> detail
```

Parameter	Description
shaper <list>	The name of a shaper in the system, as defined in SandScript.
instance <unique-instance>	A comma separated list of expressions which identify a unique by instance. It must match up with the "unique by" clause given to the shaper in SandScript.
priority <name>	The name of the shaper priority, as defined in SandScript.
channel <name>	The name of the shaper channel, as defined in SandScript.

Output	Description
Name	This is the shaper's name.
ClusterRate(bps)	This is the shaper rate that is defined in SandScript.
RateIn(bps)	The rate of traffic currently going in to the shaper.
RateOut(bps)	The rate of traffic currently going out of the shaper.
OutOfProfileBytes	Total number of bytes that the shaper, priority, or channel, drops. If this value increases, it means the shaper, priority or channel is receiving more traffic than the shaper rate.
UniqueBy	The expression that this shaper is unique-by, if any. If multiple actions are specified with different unique by expressions, all are shown with slashes separating each.
AvgRateOut	The rate of traffic currently going out of the shaper, priority or channel (average over the instances).

Output	Description
Priority	The name of the priority as defined in SandScript.
Channel	The name of the channel as defined in SandScript.

Output	Description
RateIn	The rate of traffic entering the shaper.
RateOut	The rate of traffic leaving the shaper (i.e., being bridged out by the PTS).
RateOutOfProfile	The rate of traffic which is beyond the defined shaper rate. Traffic is dropped, marked, or left alone - depending on the configured out_of_profile_action for the SandScript.
RatePacketsDropped	The rate at which packets are dropped, in order to maintain the shaper's defined rate.
RateBytesDropped	The rate at which bytes are dropped in order to maintain the shaper's defined rate.
RatePacketsMarked	If the priority is configured with a marking out_of_profile_action, this will contain the rate at which packets are marked.
RateBytesMarked	If the priority is configured with a marking out_of_profile_action, this will contain the rate at which bytes are marked.

Output	Description
Name	The name of the shaper as defined in SandScript.
Distributed	If true, the shaper is configured to make use of level distribution.
ClusterRate	The rate of the shaper, as defined in SandScript.
Priority	The name of the priority as defined in SandScript.
Channel	The name of the channel as defined in SandScript.
Algorithm	The algorithm used to control the rate of the shaper.
OutOfProfileAction	The action to perform on packets which exceed the configured shaper rate.
Weight	The weight of the shaper channel.
SharedBy	The expression, if any, that defines how the channel is sharing bandwidth equally.

Output	Description
MinRate(bps)	The rate of traffic reserved from drops.
MaxRate(bps)	The maximum rate of traffic that this priority (and the ones above it) will output.
Module	The element that the shaper object resides on.
Instance	The processing instance that the shaper object resides on.

2.13.66 show policy subnets

Displays the contents of the `/usr/local/sandvine/etc/subnets.txt` file.

2.13.67 show policy table

Shows policy tables and statistics. Tables are used to store state and build state machines in policy. Tables in policy are similar to tables in a database.

```
show policy table
show policy table stats
show policy table [table-name] row <key>
show policy table namespace ...
show policy table secondary-index
```

Table Output	Description
Name	Table name.
RowTimeout	Row timeout in seconds.
ResetTimeout	What actions will reset the row timeout timer as defined in policy.
UniqueBy	Key used to access the table.
GenerationNumber	Generation number which was set the last time policy was loaded.
RowSizeBytes	Size of one table row in bytes.
Rows	Number of rows.
RowsCreated	Number of rows created.
RowsDeleted	Number of rows deleted.
RowLookups	Number of row lookups.
RowCreateFailures	Number of failed row creations.
RowNullKeyCreate	Number of attempts to read a row with a null key.
RowNullKeyGet	Number of attempts to write a row with a null key.
RowNullKeyDelete	Number of attempts to delete a row with a null key.

Table Stats Output	Description
totalRows	Total number of rows.
totalBytes	Total number of bytes used by table rows.
maxBytesExceeded	Indicates how many row allocations have failed because they would have caused the total number of bytes allocated to table rows to be exceeded.

Table Columns Output	Description
Name	Column name.
Type	Column data type.
Default	Default value of column.
DefaultReads	Number of times the default value has been read from this column.
ValueReads	Number of times a value explicitly stored in this column has been read.

Table Columns Output	Description
Writes	Number of times a value has been written to this column.

2.13.68 show policy timer

Shows details about SandScript timers.

```
show policy timer
```

```
show policy timer <timer-name>
```

You can use SandScript timers to generate an event in the future. When the event occurs, SandScript evaluates the rules available in the context of the timer.

Output	Description
Name	Name of the timer
Repeating	Whether the timer repeats
Resolution	Numeric resolution of the timer in milliseconds
Tolerance	Tolerance of the timer in milliseconds
Lag	How far the timer is behind in milliseconds
Urgency	Current urgency of the timer, as determined by the values of tolerance and lag
ToleranceExceeded	Number of times the timer tolerance was exceeded
Fired	Number of times the timer was fired
ArmCount	Number of times an instance of the timer has been armed
ClearCount	Number of times an instance of the timer has been cleared
ArmedInstances	Number of instances of the timer currently armed
UnarmedInstances	Number of instances of the timer currently unarmed
Instances	Number of instances of the timer.

2.13.69 show policy timer instances

Shows global instances of SandScript timers.

```
show policy timer instances
```

```
show policy timer <timer-name> instances
```

Output	Description
Name	Name of the timer
Armed	Whether the timer is armed
Duration	Duration of the timer
Expiry	Expiry date and time of the timer

2.13.70 show policy timer stats

Shows statistics on SandScript timers.

```
show policy timer stats
```

Output	Description
ArmedTimers	Number of timer instances currently armed
UnarmedTimers	Number of timer instances currently unarmed
TimersFired	Number of times a timer instance has fired
ArmCount	Total number of times a timer instance was armed
ClearCount	Total number of times a timer instance was cleared
ToleranceExceeded	Total number of times any timer tolerance was exceeded

2.13.71 show policy whitelist

Shows subscriber IDs that are white-listed by the attack policy, meaning they have privileges which transcend the policy.

Output	Description
Id	Whitelist ID number
User	User name

2.13.72 show service bgp attributes

Shows the BGP attributes for the specified IP.

```
show service bgp attributes <ip-address>
```

Output	Description
Mapped	Indicates if the IP address is mapped
Subnet	The subnet for the IP address
AsPath	The AS path of the IP address
CommunitySet	The community set the IP address belongs to

2.13.73 show service bgp errors

Shows a list of error counters related to BGP messages.

```
show service bgp errors
```

Output	Description
OpenMessageParseErrors	The number of errors encountered while parsing BGP open messages. No BGP connections can be established.

Output	Description
UnsupportedExtCommunity	The number of extended communities found of an unsupported type.
IgnoredAs4PathAttribute	If a wrong AS4_PATH attribute is included in an update message, it will be ignored and this counter will be incremented. This occurs if a 4byte AS capable peer sends this attribute or if there are more AS numbers in the AS4_PATH than the AS_PATH.
InvalidAsInAsPath	An error counter incremented when AS_TRANS is found inside an AS4_PATH or when AS_TRANS is found inside an AS_PATH from a 4byte AS capable peer.

2.13.74 show service bgp peer

Shows summary information about all the BGP peer routers connected to the PTS.

```
show service bgp peer
```

```
show service bgp peer all
```

Output	Description
IPAddress	IP address of the peer router
Port	BGP connection port number (normally 179)
Password	MD5 password configured for this router. This will be blank if no password is set.
LocalAS	Local Autonomous System (AS) number configured for the PTS
RemoteAS	Remote AS number associated with this router
4ByteASCapable	For each peer this indicates, with a true or false value, whether the peer is capable of handling 4byte AS numbers.
BgpType	Type of BGP connection. E-BGP indicates external BGP (between different AS numbers). I-BGP indicates internal BGP (within an AS number).
HoldTime	Maximum connection hold time without Update or KeepAlive, in seconds
ConnectionState	The current state of the BGP protocol session with the router: <ul style="list-style-type: none">• [idle] is the normal BGP state for configured routers on a PTS which is not the active BGP master.• [connect]• [active]• [openSent]• [openConfirm]• [established] is a fully operational BGP connection.
Priority	The priority

2.13.75 show service bgp peer <ipv4-address>

Shows details and statistics for all peer routers (*) or specified peer routers connected to the PTS.

Output	Description
Port	BGP connection port number (normally 179)
Password	MD5 password configured for this router. This will be blank if no password is set.
LocalAS	Local Autonomous System (AS) number configured for the PTS
RemoteAS	Remote AS number associated with this router
BgpType	Type of BGP connection. E-BGP indicates external BGP (between different AS numbers). I-BGP indicates internal BGP (within an AS number).
HoldTime	Maximum connection hold time without Update or KeepAlive, in seconds
Priority	
ConnectionState	<p>The current state of the BGP protocol session with the router:</p> <ul style="list-style-type: none"> • [idle] is the normal BGP state for configured routers on a PTS which is not the active BGP master. • [connect] • [active] • [openSent] • [openConfirm] • [established] is a fully operational BGP connection.
OpenSent	Number of BGP OPEN packets sent to the router since BGP process startup
OpenReceived	Number of BGP OPEN packets received from the router since BGP process startup
UpdateSent	Number of BGP UPDATE packets sent to the router since BGP process startup
UpdateReceived	Number of BGP UPDATE packets received from the router since BGP process startup
KeepaliveSent	Number of BGP KEEPALIVE packets sent to the router since BGP process startup
KeepaliveReceived	Number of BGP KEEPALIVE packets received from the router since BGP process startup
NotificationSent	Number of BGP NOTIFICATION packets sent to the router since BGP process startup
NotificationReceived	Number of BGP NOTIFICATION packets received from the router since BGP process startup
AddedSubnets	Number of subnets added in UPDATE messages from the router
RemovedSubnets	Number of subnets removed in UPDATE messages from the router

2.13.76 show service bgp peer all

Shows detailed information about all BGP peers.

Output	Description
IPAddress	IP address of the peer router
Port	BGP connection port number (normally 179)
Password	MD5 password configured for this router. This will be blank if no password is set.
LocalAS	Local Autonomous System (AS) number configured for the PTS

Output	Description
RemoteAS	Remote AS number associated with this router
BgpType	Type of BGP connection. E-BGP indicates external BGP (between different AS numbers). I-BGP indicates internal BGP (within an AS number).
HoldTime	Maximum connection hold time without Update or KeepAlive, in seconds
ConnectionState	The current state of the BGP protocol session with the router: <ul style="list-style-type: none">• [idle] is the normal BGP state for configured routers on a PTS which is not the active BGP master.• [connect]• [active]• [openSent]• [openConfirm]• [established] is a fully operational BGP connection.
OpenSent	Number of BGP OPEN packets sent to the router since BGP process startup
OpenReceived	Number of BGP OPEN packets received from the router since BGP process startup
UpdateSent	Number of BGP UPDATE packets sent to the router since BGP process startup
UpdateReceived	Number of BGP UPDATE packets received from the router since BGP process startup
KeepaliveSent	Number of BGP KEEPALIVE packets sent to the router since BGP process startup
KeepaliveReceived	Number of BGP KEEPALIVE packets received from the router since BGP process startup
NotificationSent	Number of BGP NOTIFICATION packets sent to the router since BGP process startup
NotificationReceived	Number of BGP NOTIFICATION packets received from the router since BGP process startup
AddedSubnets	Number of subnets added in UPDATE messages from the router
RemovedSubnets	Number of subnets removed in UPDATE messages from the router

2.13.77 show service bgp route

Lists subnets received from each BGP peer router.

Output	Description
AS	Autonomous System (AS) number associated with the router
Selected	Whether the subnet has been selected to be used in the BGP routing information base. This means that it will be advertised through policy and subnets.txt. It will also be advertised to all PTSs in the cluster. The selected subnets are sent from the master BGPD of the PTS cluster to all other PTSes.
Priority	The priority of the subnet (determined from the peer that received the subnet)
Subnet	An individual subnet learned from the associated router
OrigAS	Origin AS number for the subnet
Community	The community, if any, associated with the subnet

2.13.78 show service bgp route-distribution

Shows the learned subnets, per client.

```
show service bgp route-distribution
LocalSSN      : SDVN86010813
LocalHost     : PTS.sandvine.com
TotalReceivedNetworks: 6
```



Note:

For optimal results, run this command on the master element. Use the `show service bgp status` command to identify which element is the master.

Output	Description
LocalSSN	Serial number of the local machine.
LocalHost	The host name of the local machine.
TotalReceivedNetworks	The total number of received networks from BGP peers. If a BGP peer is restarted and resends us the same BGP networks (that we had already received and counted) then this counter gets incremented again. That is this does not count the number of unique received networks from peers.

Output	Description
Host	The hostname, "local" for the local element.
Module	The PTS module the process is running on
App	The application name. Can be one of: CND BGPD PTSD1 PTSD2 PTSD3 PTSD4
CurrentNetworks	The current number of networks in the BGP routing information base.
ReceivedNetworks	Number of subnets that the client has received
UnsentMessages	Number of messages still in the queue of messages to be transmitted to that client
UnackedMessages	Number of messages sent but not yet acknowledged by the client
ReTxMessages	Number of messages which have been sent and then resent because they were not acknowledged in time

2.13.79 show service bgp status

Shows the status of the BGP daemon process on the local PTS.

Output	Description
OperatingRole	Local BGP daemon is acting as the BGP master or BGP slave

Output	Description
MasterSerialNumber	Serial number of the PTS on which the master BGP daemon is running. This will match the value contained in the file <code>/etc/serial</code> . During startup of the <code>svbgpd</code> process, this may temporarily display 'unknown'.
MasterHostName	Host name of the PTS on which the master BGP daemon is running. During startup of the <code>svbgpd</code> process, this may temporarily display 'unknown'.
MasterEligible	Indicates whether this PTS is configured to be eligible to act as the BGP master

2.13.80 show service bgp subnet

Lists stored subnets, learned via BGP, together with classification information.

All subnets learned from BGP peer routers are displayed, showing AS number and communities. Pagination, if necessary, is controlled using normal Unix **less** command controls.

Output	Description
Subnet	An individual subnet learned via BGP
ASPath	AS number associated with the subnet
Communities	The community information for the subnet

2.13.81 show service cluster-discovery

Shows configuration and elements details for a cluster.

If the `show service cluster-discovery elements` command returns:

No data available

You should:

- Verify that other devices are neighbors. Run `show interface neighbors`.
- Ensure each element can ping the other elements in the cluster via the cluster IP.

```
show service cluster-discovery config
show service cluster-discovery elements
show service cluster-discovery seeds
show service cluster-discovery stats
show service cluster-discovery unicast
```

Attribute	Function
config	Configuration details for the local cluster element.
elements	List of remote cluster elements.
seeds	Cluster seeds that have been configured for (inter-cluster) SCDP discovery.
stats	Statistics for cluster-discovery.

Attribute	Function
unicast	Cluster elements that have been statically configured to use SCDP unicast.

Elements Output	Description
Id	The element's Id.
Name	Cluster name.
HostName	The element's hostname.
State	The element's state.
IpAddr	The element's IP address.
MasterEligible	Indicates if the element is eligible to be elected master.
ProductName	The platform.
SerialNumber	The element's serial number.

Stats Output	Description
Clustered	Indicates if clustering is enabled.
Uptime	Time, in seconds, since the last initialization.
Tx	Transmission, in bytes, since the last initialization.
RX	Reception, in bytes, since the last initialization.
TxErrors	Number of transmission errors.
RxErrors	Number of reception errors.
RefreshTx	Number of cluster communication refreshes that have been transmitted to neighboring cluster elements.
RefreshRx	Number of reception refreshes.
RefreshTxErrors	Number of refresh transmission errors.
Ignored	Number of ignored transmissions.
ParseErrors	Number of parse errors.
Discovered	Total number of elements that have been discovered. Each time an entry is added to an element table, this counter is incremented. If an element joins the cluster, times out, is removed from the table and then joins again, it is counted both times.
Unvalidated	Number of elements in the element table that have not been authenticated.
FailedAuthentication	Number of authentications that have failed in the cluster.
RefreshErrors	Number of refresh errors.
AppTx	Number of application transmissions.
AppTxErrors	Number of application transmission errors.
InternalTx	Number of internal transmissions.
InternalTxErrors	Number of internal transmission errors.

Stats Output	Description
SubElementErrors	Number of errors attributed to sub-elements in the cluster.

2.13.82 show service control-center stats

Shows statistics for Control Center.

Heartbeat Output	Description
Full	The number of detailed heartbeat messages sent to the Control Center server.
Brief	The number of brief heartbeat messages sent to the Control Center server.
Total	The total number of heartbeat messages sent to the Control Center server.
UnknownSystem	Number of unknown system errors in the local heartbeat server.
UknownPlatform	Number of unknown platform errors in the local heartbeat server.
TransmissionErrors	Number of errors from sending heartbeats to the Control Center server.
HearbeatServerErrors	Number of errors from the local heartbeat server.

Requests Output	Description
Type	The different types of requests sent by Control Center. Can be one of: <ul style="list-style-type: none">• FetchFiles• ExpandList• GetNEConfig• RunOperationalCommand
Received	The number of requests received.
Authorized	The number of successfully authorized requests.
Executed	The total number of requests executed.
Success	The number of successful requests.
Failed	The number of failed requests.

2.13.83 show service diameter

The `show service diameter` suite of commands shows information about the Diameter stack, such as dictionary data, message data, and client and server peer data.

2.13.83.1 show service diameter dictionary

Shows all configured dictionaries with transmission and reception statistics.

```
show service diameter dictionary
```


2.13.83.2 show service diameter dictionary <name>

Shows detailed information about the specified dictionary.

```
show service diameter dictionary <name>
```

Output	Description
EventName	Diameter command/action that the dictionaries support
MessageCode	Code for the Diameter command
ApplicationId	Application ID that the dictionary supports
IsRequest	Whether the command is a request
IsError	Whether the command is an error
IsProxiable	Whether the command can be proxied
MessagesSent	Number of messages that the element sent
MessagesReceived	Number of messages that the element received
MessagesDropped	Number of outgoing messages that the element dropped

2.13.83.3 show service diameter messages

Shows information for sent and received Diameter messages.

```
show service diameter messages
```

Message Stats Output	Description
TotalSentMessages	Number of messages that the element sent
TotalReceivedMessages	Number of messages that the element received

Message Drops Output	Description
TotalDroppedOutgoing	Number of outgoing messages that the element dropped
TotalDroppedIncoming	Number of incoming messages that the element dropped

Message Rate Output	Description
TotalInMessagesPerSec	Incoming message rate
TotalOutMessagesPerSec	Outgoing message rate

2.13.83.4 show service diameter messages detail

Shows the reasons why the element dropped Diameter messages.

```
show service diameter messages detail
```

Transmit Message Output	Description
OutgoingDroppedRateTooHigh	Number of outgoing messages that the element dropped because the outgoing message rate exceeded the limit.

Transmit Message Output	Description
PeerNotFound	Number of outgoing messages that the element dropped because it was unable to find a destination peer.
OutgoingDroppedOnSessionExpiry	Number of outgoing messages that the element dropped because the session expired.
OutgoingDroppedOnSessionExpiryQueueFull	Number of outgoing messages that the element dropped when the session expired because the outgoing queue was full.
DroppedDuplicatePendingRequest	Number of requests that the element dropped because they were duplicate outgoing messages.
RequestsDropped	Number of outgoing request messages that the element dropped because it did not receive a response after retransmission and timeout.
OutgoingDroppedExpired	Number of outgoing messages that the element dropped because they were too old.
OrphanedRequestsDropped	Number of outgoing messages that the element dropped because the destination peer was not connected.
OutgoingDroppedQueueFull	Number of outgoing messages that the element dropped because the outgoing queue was full.
OutgoingDroppedNoSession	Number of outgoing messages that the element dropped because it was unable to create a session. This happens if the number of active sessions reaches the maximum number of allowed sessions.
OutgoingDroppedFailedOut	Number of failed outgoing requests that the element dropped because of a full application queue.
DroppedDuplicatePendingAnswer	Number of duplicate answers that the element dropped.
OutgoingBlockedDroppedExpired	Number of outgoing blocked messages that the element dropped because their age exceeded the limit.
OutgoingDroppedCreationFailures	Number of outgoing messages that the element dropped because the SandScript application encountered failures while creating the message.

Receive Message Output	Description
IncomingWithUnsupportedApplId	Number of incoming messages that the element dropped because it did not support the application ID in the messages.
IncomingDroppedInvalid	Number of incoming messages that the element dropped as invalid messages.
IncomingMessageTooLarge	Number of incoming messages that the element dropped because they were too large.
IncomingDroppedUnexpectedBaseMessage	Number of incoming Capabilities Exchange Request (CER)/Capabilities Exchange Answer (CEA) messages that the element dropped because they were not expected.
IncomingDroppedMissingOriginHost	Number of incoming messages that the element dropped because they were missing the Origin-Host AVP.
IncomingDroppedQueueFull	Number of incoming messages that the element dropped because the application queue was full.
IncomingUnsolicitedAnswersDropped	Number of incoming answers that the element dropped because they did not match any outgoing pending requests. This counter increments if:

Receive Message Output	Description
	<ul style="list-style-type: none"> The element receives an answer for an outstanding request message after the request timed out on the sender Diameter node. The Diameter answer was in transit from the server and did not reach the client. In this case, after a timeout, the client tries to resend the request message. The server receives two requests and responds to the duplicate request too. The server then sends two answers to the client, but the client drops the second answer as unsolicited. The server sends an answer with a hop-by-hop Id, which the client did not send.
FabricatedDroppedQueueFull	Number of internally fabricated messages that the element dropped because the application queue was full.
IncomingDroppedExpired	Number of incoming messages that the element dropped because they were considered too old.
IncomingWithUnsupportedCommandCode	Number of incoming messages that the element dropped because they contained an unsupported command code.

2.13.83.5 show service diameter peer

Shows the identity, message statistics and message activity for a Diameter peer client and server.

```
show service diameter peer
show service diameter peer *
```

Client Peer Table

Output	Description
RemotelIdentity	Remote Diameter peer ID
LocalIdentity	Local Diameter peer ID
ConnectionStatus	Operational status of the peer
FailOverStatus	Failover status of the peer (Boolean)
MessagesSent	Number of messages sent to the remote peer
MessagesReceived	Number of messages received from the remote peer
MessagesQueued	Number of outgoing messages queued
CerSent	Number of Capabilities Exchange Requests sent by the local peer
CeaReceived	Number of Capabilities Exchange Answers received by the local peer
DWRSent	Number of Device Watchdog Requests sent by the local peer
DWRReceived	Number of Device Watchdog Requests received by the local peer
DWASent	Number of Device Watchdog Answers sent by the local peer
DWARReceived	Number of Device Watchdog Answers received by the local peer
DPRSent	Number of Disconnect Peer Requests sent by the local peer
DPRReceived	Number of Disconnect Peer Requests received by the local peer
DPASent	Number of Disconnect Peer Answers sent by the local peer
DPARReceived	Number of Disconnect Peer Answers received by the local peer
LastCEResult	Last Capabilities Exchange Request

Server Peer Table

Output	Description
Remoteldentity	Remote Diameter peer ID
Localldentity	Local Diameter peer ID
ConnectionStatus	Operational status of the peer
FailOverStatus	Failover status of the peer (Boolean)
MessagesSent	Number of messages sent to the remote peer
MessagesReceived	Number of messages received from the remote peer
MessagesQueued	Number of outgoing messages queued
CerSent	Number of Capabilities Exchange Requests sent by the local peer
CeaReceived	Number of Capabilities Exchange Answers received by the local peer
DWRSent	Number of Device Watchdog Requests sent by the local peer
DWRReceived	Number of Device Watchdog Requests received by the local peer
DWASent	Number of Device Watchdog Answers sent by the local peer
DWARReceived	Number of Device Watchdog Answers received by the local peer
DPRSent	Number of Disconnect Peer Requests sent by the local peer
DPRReceived	Number of Disconnect Peer Requests received by the local peer
DPASent	Number of Disconnect Peer Answers sent by the local peer
DPARReceived	Number of Disconnect Peer Answers received by the local peer
LastCEResult	Last Capabilities Exchange Request

Output	Description
Remoteldentity	Remote Diameter peer ID
Localldentity	Local Diameter peer ID
ConnectionStatus	Operational status of the peer
FailOverStatus	Failover status of the peer (Boolean)
MessagesSent	Number of messages sent to the remote peer
MessagesReceived	Number of messages received from the remote peer
MessagesQueued	Number of outgoing messages queued
CerSent	Number of Capabilities Exchange Requests sent by the local peer
CeaReceived	Number of Capabilities Exchange Answers received by the local peer
DWRSent	Number of Device Watchdog Requests sent by the local peer
DWRReceived	Number of Device Watchdog Requests received by the local peer
DWASent	Number of Device Watchdog Answers sent by the local peer
DWARReceived	Number of Device Watchdog Answers received by the local peer
DPRSent	Number of Disconnect Peer Requests sent by the local peer
DPRReceived	Number of Disconnect Peer Requests received by the local peer
DPASent	Number of Disconnect Peer Answers sent by the local peer
DPARReceived	Number of Disconnect Peer Answers received by the local peer

Output	Description
LastCEResult	Last Capabilities Exchange Request

Connected Peers Table

Output	Description
RemotelIdentity	Remote Diameter peer ID
LocalIdentity	Local Diameter peer ID
ConnectionStatus	Operational status of the peer
FailOverStatus	Failover status of the peer (Boolean)
MessagesSent	Number of messages sent to the remote peer
MessagesReceived	Number of messages received from the remote peer
MessagesQueued	Number of outgoing messages queued
CerSent	Number of Capabilities Exchange Requests sent by the local peer
CeaReceived	Number of Capabilities Exchange Answers received by the local peer
DWRSent	Number of Device Watchdog Requests sent by the local peer
DWRReceived	Number of Device Watchdog Requests received by the local peer
DWASent	Number of Device Watchdog Answers sent by the local peer
DWAReceived	Number of Device Watchdog Answers received by the local peer
DPRSent	Number of Disconnect Peer Requests sent by the local peer
DPRReceived	Number of Disconnect Peer Requests received by the local peer
DPASent	Number of Disconnect Peer Answers sent by the local peer
DPAReceived	Number of Disconnect Peer Answers received by the local peer
LastCEResult	Last Capabilities Exchange Request

2.13.83.6 show service diameter peer client

Shows the identities, message statistics and message activity for a Diameter peer client and connected peer clients.

Client Peer Table

Output	Description
RemotelIdentity	Remote Diameter peer ID
LocalIdentity	Local Diameter peer ID
ConnectionStatus	Operational status of the peer
FailOverStatus	Failover status of the peer (Boolean)
MessagesSent	Number of messages sent to the remote peer
MessagesReceived	Number of messages received from the remote peer
MessagesQueued	Number of outgoing messages queued
CerSent	Number of Capabilities Exchange Requests sent by the local peer
CeaReceived	Number of Capabilities Exchange Answers received by the local peer
DWRSent	Number of Device Watchdog Requests sent by the local peer

Output	Description
DWRReceived	Number of Device Watchdog Requests received by the local peer
DWASent	Number of Device Watchdog Answers sent by the local peer
DWARReceived	Number of Device Watchdog Answers received by the local peer
DPRSent	Number of Disconnect Peer Requests sent by the local peer
DPRReceived	Number of Disconnect Peer Requests received by the local peer
DPASent	Number of Disconnect Peer Answers sent by the local peer

Connected Peers Table

Output	Description
RemoteIdentity	Remote Diameter peer ID
LocalIdentity	Local Diameter peer ID
ConnectionStatus	Operational status of the peer
FailOverStatus	Failover status of the peer (Boolean)
MessagesSent	Number of messages sent to the remote peer
MessagesReceived	Number of messages received from the remote peer
MessagesQueued	Number of outgoing messages queued
CerSent	Number of Capabilities Exchange Requests sent by the local peer
CeaReceived	Number of Capabilities Exchange Answers received by the local peer
DWRSent	Number of Device Watchdog Requests sent by the local peer
DWRReceived	Number of Device Watchdog Requests received by the local peer
DWASent	Number of Device Watchdog Answers sent by the local peer
DWARReceived	Number of Device Watchdog Answers received by the local peer
DPRSent	Number of Disconnect Peer Requests sent by the local peer
DPRReceived	Number of Disconnect Peer Requests received by the local peer
DPASent	Number of Disconnect Peer Answers sent by the local peer
DPARReceived	Number of Disconnect Peer Answers received by the local peer
LastCEResult	Last Capabilities Exchange Request

MIB reference

Data displayed as part of this command is from the svDiameterStatsClientPeerTable in the SANDVINE-MIB.

SNMP notifications

If the connection with a remote Diameter peer is lost and/or re-established, these are the SNMP notifications defined in the SANDVINE-MIB:

- svDiameterPeerDiscNotification
- svDiameterPeerConnNotification

Related alarms

- Alarm Model 32: Diameter client peer connection lost
- Alarm Model 40: Diameter peer failed over

2.13.83.7 show service diameter peer server

Shows the identities, message statistics and message activity for a Diameter peer server and connected peer servers.

Server Peer Table

Output	Description
RemoteIdentity	Remote Diameter peer ID
LocalIdentity	Local Diameter peer ID
ConnectionStatus	Operational status of the peer
FailOverStatus	Failover status of the peer (Boolean)
MessagesSent	Number of messages sent to the remote peer
MessagesReceived	Number of messages received from the remote peer
MessagesQueued	Number of outgoing messages queued
CerSent	Number of Capabilities Exchange Requests sent by the local peer
CeaReceived	Number of Capabilities Exchange Answers received by the local peer
DWRSent	Number of Device Watchdog Requests sent by the local peer
DWRReceived	Number of Device Watchdog Requests received by the local peer
DWASent	Number of Device Watchdog Answers sent by the local peer
DWAReceived	Number of Device Watchdog Answers received by the local peer
DPRSent	Number of Disconnect Peer Requests sent by the local peer
DPRReceived	Number of Disconnect Peer Requests received by the local peer
DPASent	Number of Disconnect Peer Answers sent by the local peer

Connected Peers Table

Output	Description
RemoteIdentity	Remote Diameter peer ID
LocalIdentity	Local Diameter peer ID
ConnectionStatus	Operational status of the peer
FailOverStatus	Failover status of the peer (Boolean)
MessagesSent	Number of messages sent to the remote peer
MessagesReceived	Number of messages received from the remote peer
MessagesQueued	Number of outgoing messages queued
CerSent	Number of Capabilities Exchange Requests sent by the local peer
CeaReceived	Number of Capabilities Exchange Answers received by the local peer
DWRSent	Number of Device Watchdog Requests sent by the local peer
DWRReceived	Number of Device Watchdog Requests received by the local peer

Output	Description
DWASent	Number of Device Watchdog Answers sent by the local peer
DWAReceived	Number of Device Watchdog Answers received by the local peer
DPRSent	Number of Disconnect Peer Requests sent by the local peer
DPRReceived	Number of Disconnect Peer Requests received by the local peer
DPASent	Number of Disconnect Peer Answers sent by the local peer
DPAReceived	Number of Disconnect Peer Answers received by the local peer
LastCEResult	Last Capabilities Exchange Request

MIB reference

Data displayed as part of this command is from the svDiameterStatsServerPeerTable in the SANDVINE-MIB.

SNMP notifications

If the Diameter peer fails over to a secondary peer or fails back to the primary peer, these are the SNMP notifications defined in the SANDVINE-MIB:

- svDiameterPeerFailedOverNotification
- svDiameterPeerFailedBackNotification

If the connection with a remote Diameter peer is lost and/or re-established, these are the SNMP notifications defined in the SANDVINE-MIB:

- svDiameterServerErrorNotification
- svDiameterServerNoErrorNotification

Related alarms

Alarm Model 41: Diameter server connection with client peer lost

2.13.83.8 show service diameter routes

Shows the Diameter realm routing table.

```
show service diameter routes
```

Output	Description
RealmName	Name of a reachable Diameter realm
ApplicationId	Application ID
Peers	Comma-separated list of peer IDs that can reach the realm and support the application ID
IsLocal	Whether the route is local
MessagesSentToRealm	Number of messages sent to this route
LocalRouteMessagesSent	Number of messages sent to the local route

2.13.84 show service election

Shows the processes elected as the feature master across all like processes in the cluster. A single process can participate in feature master elections for more than one feature.

Output Table	Description
MASTER	Table displays services registered for master election and the serial number of the element which is the elected master.
PEER RANDOM	Table displays services registered for peer election and the serial number of the element which is the elected master.
FEATURE MASTER	Table displays features registered for election and the serial number of the element which is the elected master.

Output Rows	Description
Description	Name of the eligible process.
NumRegistered	Registered number of eligible processes.
Elements	Serial number of the element the process is running on.

2.13.85 show service election feature

Represents a single process elected as the feature master across all like processes in the cluster. A single process can participate in feature master elections for more than one feature.

Feature Master Table Output	Description
Description	Name of the master election eligible process
NumRegistered	Registered number of master election eligible processes
Element	Serial number of the element the master elected process is running on
AppId	Numerical application ID of the process

2.13.86 show service election master

Shows all registered local master eligible processes and the elements running the master elected processes.

Master Table Output	Description
Description	Name of the master election eligible process
NumRegistered	Registered number of master election eligible processes
Element	Serial number of the element the master elected process is running on
AppId	Numerical application ID of the process

2.13.87 show service election master peer

Shows all registered peer (other elements in cluster) master elections along with the master if one has been elected.

Output	Description
Description	A description of the table. For example, SCDPD.
NumRegistered	Registered number
Element	Element name

2.13.88 show service election random

Shows all registered local random elections along with the elected element if one has been elected.

Output	Description
Description	Description of the table. For example, SCDPD.
NumRegistered	Registered number
Element	Element name
Appld	Application ID (a number)

2.13.89 show service election random peer

Shows all registered peer (other elements in cluster) random elections along with the elected element if one has been elected.

Output	Description
Description	Description of the table. For example, SCDPD.
NumRegistered	Registered number
Element	Element name

2.13.90 show service id-allocation

The `show service id-allocation` suite of commands displays percentiles, statistics, and transaction errors for the ID allocation subsystem.

2.13.90.1 show service id-allocation performance

Shows the current performance statistics of the subsystem based on latency histogram percentiles.

```
show service id-allocation performance
```

In the CLI output, `Request-Latency-nth-Percentile` means that n percent of the operations between the subsystem and the SPB was completed in a time less than displayed, or (100-n)% of the operations took longer to complete. For example, this

output means that 75% of the operations took less than 2 milliseconds to complete and 25% of the operations took longer than 2 milliseconds.

Request-Latency-75th-Percentile: 2 ms

2.13.90.2 show service id-allocation stats

Shows the current statistics of all requests sent by the subsystem to the SPB. The output displays the name of the requests, the number of requests searched, the number of requests deleted, and their total.

```
show service id-allocation stats
```

Output	Description
TotalNumActions	Requests sent by the subsystem to the SPB since the restart of the <code>svsde</code> service.
FailSpbNotAvailable	Requests that failed because the SPB was not available, disconnected, or not working.
FailStatManager	Requests that failed because the SPB was not available. These requests specify that the ID allocation subsystem should not perform a retry if they fail.
FailDecodeRequest	Requests that failed because the SPB failed to decode the request.
FailSpbUnsupported	Requests that failed because the subsystem sent them to a version of SPB that does not support the requests.
FailInvalidParameters	Requests that failed because of invalid parameters, for example, a negative ID. These requests return a transaction ID of zero.
QueuedToSpb	Requests that are queued to the SPB.
CompletedSucceed	Requests that are complete, which means they have completed the full route from the invoked request to the <code>IsComplete</code> event without error.
CompletedFailed	Requests that completed the full route from the invoked request to the <code>IsComplete</code> event and have encountered an error.
ToSubsystemDropped	Requests that the SPB dropped because the queue from the policy engine on the SDE to the subsystem was full.
RetryDropped	Requests that the SPB dropped because the retry queue was full.
ToPolicyDropped	Requests that the SPB dropped because the queue from the subsystem to the policy engine on the SDE was full.
ToPolicyImmediateDropped	Requests that the SPB dropped because the immediate queue from the subsystem to the policy engine on the SDE was full. The immediate queue handles all failed requests described in <code>FailStatManager</code> .

2.13.90.3 show service id-allocation transaction-errors

Shows details for all or specific transactions between the subsystem and the SPB and displays the last 20 records on the SPB that have encountered a problem during execution.

```
show service id-allocation transaction-errors
```

```
show service id-allocation transaction-errors <int:1..>
```

where <int:1..> is the transaction ID for which you want to display further details.

Output	Description
RowCreationTime	Time when the row containing the record was created on the SPB.

Output	Description
TransactionId	The transaction ID.
RecordCreationTime	Time when the record was created on the SPB.
AutoCreate	Specifies whether the subsystem creates a record in the SPB during a lookup, in case the record does not exist in the SPB. This output has a value of true or false. The default value is true. If this value is set to false, the subsystem does not create a record in the SPB even if the record does not exist.
RetryOnFailure	Specifies whether or not the subsystem attempts to resend a record that failed previously. This output has a value of true or false. The default value is false.
OperationType	Specifies whether the purpose of the transaction is to delete or search for a record.
Requests	This output groups details about requests in the subsequent rows and appears when you specify a transaction ID.
Index	The request index in the subsystem operation. For example, Name[3] refers to a request at index 3.
Name	The name of the record (if it exists) used to identify it in the SPB.
Id	The ID of the record used to identify it in the SPB. The SPB generates this ID.
Created	If true, indicates that the request represented by this row was created on the SPB by the specific action represented by the transaction ID.
ErrorType	The type of error message, such as request failed or dropped.
ErrorMessage	An accompanying error message, if it exists.

2.13.91 show service ip-overload-management never-shunted-subnets

Shows the subnets that can never be shunted by the IP overload management service.

Note that inclusion of a subnet in the never-shunted subnets file does not prevent an IP from within the subnet from being shunted for other reasons. For example, `set interface shunt true` will still cause packets whose IPs are contained within a never-shunt subnet to be shunted.

2.13.92 show service ip-overload-management shunted-subnets

Lists the subnets currently being either always or dynamically shunted.

Output	Description
Subnet	The subnet for which traffic is being shunted
Expiry	When the traffic for the IP will no longer be dynamically shunted. In the case of an always-shunt subnet, this field will display "never".

2.13.93 show service ip-overload-management stats

Lists operational statistics for IP overload management.

```
show service ip-overload-management stats overview
show service ip-overload-management stats shunted-bytes
show service ip-overload-management stats shunted-packets
```

Overview Output	Description
DynamicSubnetsShunted	The total number of dynamically shunted subnets, currently being shunted
StaticSubnetsShunted	The total number of statically shunted subnets, currently being shunted
TotalRequests	The number of times that dropped packets caused the PTS to dynamically shunt IPs
Successful	The number of times that an attempt to shunt IPs was at least partially successful
Failed	The number of drop events where IPs could not be shunted, and why they could not be shunted. Can be one of: <ul style="list-style-type: none">• Too Soon - a drop event for a module occurred within the configured management holdoff interval, since the previous drop event for the module• No High-usage IPs - no IPs identified as abusive were detected on the module associated with the drop event• IPs Cannot Be Shunted - either because abusive IPs conflicted with the never shunt list or because shunting the IP would exceed the configured shunted IP limit

Shunted Bytes Output	Description
TotalShuntedBytes	The total number of shunted bytes, for both static and dynamic subnets
IntervalShuntedBytes	The number of shunted bytes over the interval, for both static and dynamic subnets

Shunted Packets Output	Description
TotalShuntedPackets	The total number of shunted packets, for both static and dynamic subnets
IntervalShuntedPackets	The number of shunted packets over the interval, for both static and dynamic subnets

2.13.94 show service ip-overload-management usage-detection

Lists the top abusive IPs.

Output	Description
Module	The processing module to which the IP is assigned.
Process	The number of the process to which the IP is assigned.
IpAddress	The IP address.
Units	The threshold(s) crossed by the IP. One or more of bytes, flows or packets.

2.13.95 show service load-balancer bundle

Searches for the bundle described by the specified bundle identifier and displays both the bundle and the module to which it is assigned.

This command is only applicable for centralized load balancing. If centralized load-balancing is configured the `show config service load-balancer mode` command will return "policy".

Further information about bundles is available in the *SandScript Configuration Guide*.

```
show service load-balancer bundle id <int:0..>
show service load-balancer bundle value <string>
```

Output	Description
BundleIdentifier	The element's internal, unique bundle identifier, derived from the CLI parameter.
BundleFound	Indicates if the bundle exists.
NumIPsInBundle	The number of IPs contained in the bundle.
Bundle Assignment	Lists where the IPs belonging to the bundle are assigned. If the bundle is not yet assigned, a message is displayed indicating this.
Bundle IP Addresses	Lists a subset of the IPs contained in the bundle and whether or not the cluster has seen traffic for any of them.

Conditions and values

If balancing by...	Then the value is...
internal-ip or ip_hash	IP address.
subscriber ID	ID of a subscriber.
network-class	IP address.
policy-class	IP address.
subscriber attribute	Subscriber attribute value.

2.13.96 show service load-balancer cluster compatibility

Shows the load-balancer cluster compatibility. Use this command to verify that each element of a PTS cluster is compatible with the load-balancing configuration. It is mandatory that each element be identically configured on a PTS cluster. Non compatible elements will function as a standalone PTS inspecting traffic on its data ports only.

Output	Description
Serial	The serial number of the element.
Compatible	If true, this element has a compatible configuration; false otherwise.
LoadBalancingMode	The load balancing mode. Can be one of:

Output	Description
	<ul style="list-style-type: none"> static - Balancing is achieved using 12 or 8 bits of the subscriber IP address (usually the least-significant bits). ip-hash - Balancing is achieved using 8 bits of the subscriber IP address, as above, but the balancing decision is done centrally. policy - A load-balancing policy is defined to group the incoming traffic into bundles (this can be based on IP address, subscriber ID, or subscriber attribute) and each bundle is assigned to a module. Further information about bundles is available in the <i>SandScript Configuration Guide</i>.
Layer2Mode	<p>The layer 2 mode. Can be one of:</p> <ul style="list-style-type: none"> mapping - the default, the PTS maps external MACs to its own internal MAC addresses for switching inside the PTS switch fabric. tunneling - all packets are encapsulated in a tunnel inside the PTS.
HashMode	<p>The hash mode. Can be one of:</p> <ul style="list-style-type: none"> simple - The trunk distribution algorithm uses source/destination MAC addresses as hashing keys to distribute data traffic across trunk links sv-mpls - The trunk distribution algorithm uses MPLS label as hashing keys to distribute data traffic across trunk links. This mode is enabled by default on a BLD 24080. <p>Set using the <code>set config interface trunk-distribution</code> command.</p>
IPv4Window	When using the static load-balancing algorithm, a window of 8 or 12 bits from the subscriber IPv4 address that are hashed to determined the module to balance to.
IPv6Window	When using the static load-balancing algorithm, a window of 8 or 12 bits from the subscriber IPv6 address that are hashed to determined the module to balance to.

2.13.97 show service load-balancer ip

Shows load balancer assignments, assigned IPs and bundle information on a cluster element. Accepts an IPv4 or IPv6 address.

This command can only be run on the cluster element that is running the load-balancing master. Use `show service load-balancer master` to determine its hostname.

Centralized vs. non-centralized mode:

- In centralized mode, run this CLI command only on the cluster element that is running the load-balancing master.
- In non-centralized mode, run this CLI command on any element in the cluster.

```
show service load-balancer ip <ip-address>
```

Centralized mode

Load Balancer Assignment Output	Description
BundleIdentifier	Numeric identifier of the bundle calculated from the load_balance by type configured in policy.
BundleFound	Indicates if the bundle has been assigned to a module.
NumIpsInBundle	Number of IPs currently contained in the bundle.

Bundle Assignment Output	Description
Serial	Serial number of the element the bundle is assigned to.
Hostname	Hostname of the element that the bundle is assigned to.
Module	Module ID on the element that the bundle is assigned to.
Instance	Instance on the module that is handling flows for the IP.

Bundle IP Addresses Output	Description
IP	IP(s) contained in the bundle. A maximum of 10 IPs is displayed.
Discovered	Indicates if the central load-balancer has assigned this bundle to a module.

Non-centralized mode

Output	Description
Serial	Serial number of the element the IP is assigned to.
Hostname	Hostname of the element the IP has been assigned to.
Module	Local module ID of the element to which the IP has been assigned.
Instance	Instance on the module that is handling flows for the IP.

2.13.98 show service load-balancer element status

Shows the current status of all elements in a cluster that have been marked for removal. The status can be checked only on the element that is elected as the master load balancer, and is valid only in centralized mode.

Output	Description
Serial	Serial number of the element marked for removal.
IpsAssigned	Number of remaining IPs still assigned to the element.
Status	Status indicator for the removal: <ul style="list-style-type: none">• pending while removal is in progress.• complete when removal is finished.

2.13.99 show service load-balancer master

Shows the serial number and hostname elected master for load balancing. This command is applicable to both centralized and non-centralized load-balancing mode.

Output	Description
SerialNumber	Serial number of the master load balancer.
HostName	Host name of the master load balancer.

2.13.100 show service load-balancer modules

Shows a list of all modules in the system and their status. Specifying detail is only valid on the master load-balancer, and additional load metrics are displayed.

```
show service load-balancer modules
```

```
show service load-balancer modules detail
```

Output	Description
Row	The number of this row of the output.
Hostname	Hostname of the element.
Module	ID of the module in the element.
Instance	ID of the inspection engine running on a particular module.
ClusterStatus	Status of the module: <ul style="list-style-type: none">• Up• Shunt - In this state, traffic bypasses the PTS hardware, is not inspected and no statistics are reported for it.• Down
LocalStatus	Indicates if the system is ready to start balancing traffic. Status can be one of: <ul style="list-style-type: none">• Pending - A module is transitioning to up.• Up• Shunt - In this state, traffic bypasses the PTS hardware, is not inspected and no statistics are reported for it.• Down• Timed Shunt - Traffic is shunted for 30 seconds, usually due to an event such as a new element has come online or a topology change has been detected in the cluster.• Limiting Down - A module is set to down due to a configuration mismatch in the cluster.• Admin Disabled - A module is set to down as an element is administratively removed from the cluster.

Additional Details Output	Description
Serial	Serial number of the element which contains the module.
SubCluster	Name of the subcluster to which the element belongs.
Load	Measured load of the module as a percentage. between 0-100%.
Bundles	Number of traffic bundles assigned to each module. A bundle is defined by the type of load balancing being performed. Further information about bundles is available in the <i>SandScript Configuration Guide</i> .

MIB Reference

The details shown by the load-balancer commands are currently not available in the MIB.

SNMP Notifications

These SNMP notifications occur on errors for load-balancer operations:

- svLBOperStatusDownNotification
- svLBOperStatusUpNotification.

Related Alarms

Alarm model 15: Load balancer is down.

2.13.101 show service load-balancer preload

Shows the current state of current preload operation. Preload data can only be read on the element which is elected master load balancer.

This command is only applicable for centralized load balancing. If centralized load-balancing is configured the `show config service load-balancer mode` command will return "policy".

When a bundle definition contains information in the database (subscriber or attribute), it can take some time for the PTS to query it and set up the proper bundle definitions for the IPs that are discovered.

To minimize the amount of communication, the load balancer has a mode where it will preload the IP/bundle mapping to the load balancer from the SPB when the load balancer is either elected master or clears its state. The preload attempts to reduce the need for the communication between the PTS and SPB for determining bundle definitions. As IPs are discovered they can get mapped directly to the bundle defined by their definition.

Output	Description
Enabled	Whether or not preload is enabled.
Active	Whether or not preload is active.
Events	Number of preload events received by the master load balancer.
Duration	Duration of the preload in seconds after it has completed.
Cancellations	Number of times the preload was canceled.
Failures	Number of failures in trying to communicate with the SPB.

2.13.102 show service load-balancer stats

Shows some of the runtime statistics for the load balancer. If in centralized load-balancing mode, statistics can be read only on the elected master load balancer.

```
show service load-balancer stats
```

```
show service load-balancer stats detail
```

Output	Description
IpAssignments	Number of IPs that have been discovered and assigned to bundles.
BundleAssignments	Number of bundles assigned to modules in the cluster.

Output	Description
SubscriberRequests	Number of subscriber requests to the SPB issued by the load balancer. There is one request for each IP discovered that did not have a corresponding bundle. Requests are only sent when using the subscriber or attribute BundleDefinitions.
SubscriberResponses	Number of subscriber responses from the SPB. If the IP does not have a subscriber in the database then no response will be received by the load balancer.
IpChanges	Number of times a subscriber changed their IP.
Logins	Number of login events received by the load balancer from the SPB.
Logouts	Number of login events received by the load balancer from the SPB.
AttributeChanges	Number of times attribute changes were handled by the load balancer.
LocalityViolated	If true, the load balancer could not assign any new IPs to a subcluster because all the modules in that subcluster exceeded their load capacity. Will only be set if locality has been enabled.
SubClusterOverloaded	Contains the name of the subcluster that was last overloaded.
Reloads	Number of times a load balancer configuration change occurred on a reload.
Reconfigurations	Number of times a load balancer configuration change resulted in changes being applied. This could cause clearing the current load balancer state.
PendingIpTimeouts	In central load balancing mode, the number of IPAddresses that LBC forwarded to CND for IP address discovery and did not receive a IP address assignment response within the pending IP address timeout interval.
PendingIps	In central load balancing mode, the current number of IP addresses that LBC forwarded to CND for IP address discovery and is awaiting an IP address assignment response.

2.13.103 show service nat

Shows statistics about the functioning of Network Address Translation (NAT) and or a list of specified NAT mappings. The element uses the NAT tables to identify unique IPv4 subscriber sessions.

```
show service nat
show service nat public-ip-address <ip-address>
show service nat public-ip-address <ip-address> low-port <int:0..65535> high-port <int:0..65535>
```

Attribute	Description
public-ip-address	Shows all the NAT mappings for the provided public IP. When a public IP is in use, with a port in any of these ranges, the corresponding private IP address is used to look up any subscriber information.
low-port	The lower or upper port number of the range associated with the NAT mapping.
high-port	If you specify a low-port and high-port then the output is filtered to include only the ports which overlap the provided port range.

Public IP Address Output	Description
LowPort	Lower bound (inclusive) of the ports for this IP.
HighPort	Upper bound (inclusive) of the ports for this IP.

Public IP Address Output	Description
PrivatelpAddress	The mapped private IP address.

Mappings Output	Description
Current	Number of current NAT mappings in the element.
Created	Number of NAT mappings created on the element.
Deleted	Number of NAT mappings removed on the element.
Overwritten	Number of NAT mappings overwritten by overlapping NAT mappings on the element.

Lookups without Match Output	Description
NoIPAddressMatch	Number of NAT IP addresses being looked up with no NAT block. For example, when looking up 4.0.0.0:30, but 4.0.0.0 has no NAT mappings at all.
NoPortRangeMatch	Number of NAT IP addresses currently being looked up that have a NAT block for ports other than the desired port. For example, when looking up 4.0.0.0:30, but the only NAT blocks for 4.0.0.0 are 10-20 and 40-50. Port 30 is not in the NAT blocks.

2.13.104 show service protocol voip

Shows information about VoIP service providers.

```
show service protocol voip providers
```

```
show service protocol voip unknown-providers
```



Note:

If the number of unknown VoIP providers is too large, the data may not be displayed. To clear the unknown provider list, run the `clear service protocol voip unknown-providers` command.

2.13.105 show service protocol parsed-fields

Provides details about SandScript fields for protocols.

Field	Description
Id	The Id of the field.
Field	The name of the protocol field.
Active	True indicates the field is in use in policy.
ParsedCount	The number of times information was parsed for supplying to the field.

2.13.106 show service route

Shows information about the service route.

Syntax

```
show service route
show service route inet
show service route inet6
```

Attribute	Function
inet	Service route for inet
inet6	Service route for inet6

Output	Description
Destination	IP address of the route destination
Gateway	Gateway
Flags	Flag for the route
Refs	References for the route
Use	Use by count
Netif	Network device ID
Expire	Expiry

2.13.107 show service statistics tunnel-fragment-extrapolation

Shows the configuration of tunnel-fragment-extrapolation.

Output	Description
ExtrapolatedBytes	Total number of bytes extrapolated (bytes reported minus bytes in first packet)
ExtrapolatedPackets	Total number of packets on which tunnel extrapolation was applied
ExceedMaxExtrapolation	Number of times extrapolation did not occur because the length was greater than the maximum-ip-packet-size configuration
ForwardMiddleFragments	Number of non-last fragments that were not counted because the subscriber IP could not be determined from the packet
ForwardLastFragments	Number of last fragments that were not counted because the subscriber IP could not be determined from the packet

2.13.108 show service session-management config

Displays the configuration for session-management. Session management is the method for PTS to terminate flows by sending reset packets.

Output	Description
FastPathEnabled	If true, the reset packets bypass the PTS's controller
NextHopRouter	The configured IP of the next router

Output	Description
RouterMac	The MAC address of the router, derived from the IP of the next-hop router

2.13.109 show service shaping stats

This command provides details about PTS-wide shaping statistics.

```
show service shaping stats
```

Output	Description
Zombies	The current number of shaper objects waiting.
PeakObjects	The peak number of shaper objects seen on this PTS.
CurrentObjects	The current count of shaper objects seen on this PTS.
PeakPipelines	The peak pipeline count (1 for each unique set of "shape to" clauses) seen on this PTS.
CurrentPipelines	The current count of pipelines seen on this PTS.
PeakPacketStrips	The peak count of packet strips (used to implement queues) seen on this PTS.
CurrentPacketStrips	The current count of packet strips seen on this PTS.
VLANsMarked	The number of packets which have had their vlan priority marked by a shaper.
VLANsInserted	The number of packets which have had a vlan injected into them by a shaper.
IPv4Marked	The number of IPv4 packets which have had their TOS field marked by a shaper.
IPv6Marked	The number of IPv6 packets which have had their traffic class field marked by a shaper.
VLANInsertionFailures	The number of times we were unable to insert a vlan (not enough size in packet).
TruncatedMarkValue	The number of times policy loaded with a mark action specifying a value larger then the mark field.
TruncatedMarkMask	The number of times policy loaded with a mark action specifying a mask larger then the mark field.
NullMarkValue	The number of times policy loaded with a null mark value expression.
NullMarkMask	The number of times policy with a null mark mask expression.

2.13.110 show service spb config

The PTS sends batches of statistics to the SPB. This information shows the batch size and the maximum delay that statistics will wait before being sent as a partial batch.

Output	Description
BatchTimeoutMs	Maximum time, in milliseconds, the element will wait between sending out a batch of requests to the SPB
MaxStatWeight	The maximum number of stat rows to include in a single stats publishing message to the SPB
ConnectionTimeoutSec	TCP connection timeout, in seconds, for the SPB connection
ConnectionPingIntervalSec	How often, in seconds, the element sends keep-alive ping packets to the SPB to check the health of the TCP connection

2.13.111 show service spb connections

Shows the SPB connections.

```
show service spb connections
```

```
show service spb connections <id:0..>
```

Attribute	Function
Id	Show SPB connections for the SPB specified by the Id.

Output	Description
Id	The ID of the service.
Type	The type of service.
Failures	The number of failures.
OperStatus	The operation status of the device.
AdminStatus	The administration status of the device.
ConfiguredURI	The configured URI.
ConnectedURI	The connected URI.
LastTimeConnected	The last connection time.
APIVersion	The API version.

Connection-specific Output	Description
URI	The IP and port of the specified SPB connection.
ConnectionRetryInterval	The connection retry interval.
FailedConnectionRetryInterval	The retry interval for a failed connection.
ConnectionTimeoutSec	The connection's timeout, in seconds.
ConnectionPingIntervalSec	The connection's ping interval, in seconds.
ActiveConnections	The number of active connections.
LastTimeConnected	Time and date of the last connection.
Disconnects	Number of disconnects.
ConnectionFailures	Number of connection failures.
QueriesExecuted	Number of queries executed on this connection.
QueryErrors	Number of queries that experienced an error.
LastErrorTime	The time and date of the last error.
LastError	The last error.
Pending	The number of queries that are pending.
OperStatus	The operational status of the connection.

Connection-specific Output	Description
AdminStatus	The administrative status of the connection.
ConnectedURI	The connected URI.

2.13.112 show service spb

Shows operational information for the SPB.

```
show service spb capabilities-exchange
show service spb config
show service spb connections
show service spb connections diagnostics
show service spb connections primary
show service spb messages
show service spb stats
show service spb subscribers
```

show service spb capabilities-exchange

Display the capabilities exchange API versions in use when communicating with the SPB.

```
show service spb capabilities-exchange
```

Output	Description
Capability	The name of the capability.
Version	The current API version to use.
HandshakeMethod	HandshakeMethod is classified as: <ul style="list-style-type: none">• [unknown] - Not configured and no SPB has been connected, will use configured settings.• [configured] - Communicating to older pre-capability aware SPB, will use configured settings.• [negotiated] - Using API versions that were negotiated with the SPB.

2.13.113 show service spb connections diagnostics

Displays the results of running diagnostics.

Output	Description
Diagnostic	The diagnostic being reported on
Result	The result of the diagnostic

Diagnostic	Description
ResolveHostName	If a hostname is configured as the SPB server address, this will display 'Success' if the hostname can be resolved to an IP, or an error message otherwise. If no hostname is configured (for example, only IP addresses are used), this will display 'n/a'.
PingIps	If the configured SPB server can be reached via ICMP ping, this will display 'Success'. Otherwise, this will display an error message.
ClientProcess	If the SPB server address is configured to use SSL, this will display 'Success' if the TCP secure tunnel process is running on the element, or an error message if the process is not running. If the SPB server address is not configured to use SSL, this will display 'n/a'.
ServerSocket	This will display the result of a connection test to the SPB, either via SSL or TCP depending on the SPB server address. If a connection was successfully made, this will display 'Success', otherwise an error message will be displayed.
BrokerMessage	If a connection to the message broker on the SPB could be established and a simple ping request could be made, this will display 'Success', or an error message otherwise.

2.13.114 show service spb messages

Shows the statistics about messages for the SPB.

Output	Description
Category	The category of the messages.
Received	The number of received messages.
Errors	The number of errors.
Pending	The number of transmit messages pending.
Transmitted	The number of messages transmitted.
Throttled	The number of messages that have been throttled.
Timeouts	The number of messages that have timed out.
Expired	The number of messages that have expired.
Overflows	The number of overflows.
Discarded	The number of messages discarded.
RequestsPending	The number of requests that are pending.
RequestsSent	The number of requests sent.
RequestsThrottled	The number of requests that have been throttled.
RequestTimeouts	The number of requests that have timed out.
RequestsExpired	The number of requests that have expired.
RequestOverflows	The number of requests that have overflowed.
RequestErrors	The number of requests that have an error.
ResponsesPending	The number of responses that are pending.

Output	Description
ResponsesRecieved	The number of responses that have been received.
ResponsesExpired	The number of responses that have expired.
ResponsesInvalid	The number of responses that are invalid.
RspponsesUnexpected	The number of unexpected responses.
ResponsesErrors	The number of responses that have an error.
ResponsesPartial	The number of responses from SPB indicating the request was only partially successful. Some items in the batch request were processed successfully, while others failed.

2.13.115 show service spb stats

This command shows detailed counts for transmitted messages, with each output row representing a single statistic type.

For example:

Description Timeouts	Pending	Transmitted	Throttled
-----	-----	-----	-----

Historical.Network.Malware	0	7	0
0			
Historical.Network.Malware.DroppedPackets	0	7	0
0			
Historical.Voip.ApplicationProtocol.VoipProvider	0	7	0
0			
Historical.Dns.Server.Quality	0	7	0
0			
Historical.Dns.Server.Mttr.Distribution	0	7	0
0			
Historical.InterNetwork.ApplicationProtocol	0	7	0
0			
Historical.Subscriber.ApplicationProtocol	0	0	0
0			
Historical.Network.ApplicationProtocol	0	7	0
0			
Historical.NetworkElement.Performance	0	7	0
0			
Historical.Network.Traffic	0	7	0
0			
Historical.NetworkElement.NetworkInterface	0	9	0
0			
Historical.NetworkElement.NetworkInterface.ApplicationProtocol	0	12	0
0			
Historical.NetworkElement.PublishedExpression	0	7	0
0			
Historical.NetworkElement.Classifier.ApplicationProtocol	0	0	0
0			
Historical.NetworkElement.Classifier.Basic	0	0	0
0			
Historical.Subscriber.ApplicationProtocol.Basic	0	0	0
0			
Historical.NetworkElement.PolicyHistogram.Basic	0	0	0
0			
Historical.NetworkElement.PolicyHistogram.ApplicationProtocol	0	0	0
0			
Historical.Dns.ResponseManagement	0	14	0

0

Expired	Overflows	Errors	Discarded
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0

Output	Description
Description	This row's statistic type
Pending	Number of messages currently queued to be sent to the SPB
Transmitted	Number of messages successfully transmitted to the SPB
Throttled	Number of message attempts rejected by the SPB due to load. These messages are resent after a delay.
Timeouts	Number of messages that received no response from the SPB after a given timeout. These messages are resent after a delay.
Expired	Number of messages that passed their expiry time while on the transmit queue. These messages were dropped.
Overflows	Number of messages dropped because the transmit queue was full
Errors	Number of messages that could not be decoded and processed by the SPB due to errors
Discarded	Number of messages that were discarded

2.13.116 show service spb subscribers

Shows detailed counts of the communicated subscriber messages.

Receive Output	Description
Description	Type of message received
Received	Number of messages received by the element (PTS or SDE) for the given category
Errors	Number of messages received by the element that could not be decoded and processed

Request/Response Output	Description
Description	Type of request.

Request/Response Output	Description
RequestsPending	Number of requests of this type queued to be sent to the SPB.
RequestsSent	Number of requests of this type sent to the SPB.
RequestsThrottled	Number of requests of this type rejected by the SPB due to load. These messages are resent after a delay.
RequestTimeouts	Number of requests of this type that received no response from the SPB after a given timeout. These messages are resent after a delay.
RequestsExpired	Number of requests of this type that passed their expiry time while on the transmit queue. These messages are dropped.
RequestOverflows	Number of requests of this type dropped because the transmit queue was full.
RequestErrors	Number of requests of this type that could not be decoded and processed due to errors.
ResponsesPending	Number of requests of this type sent to which the SPB has not yet responded.
ResponsesReceived	Number of responses received from the SPB to requests of this type.
ResponsesExpired	Number of responses not received from the SPB to requests of this type before a timeout was reached.
ResponsesInvalid	Number of invalid responses received from the SPB to requests of this type.
ResponsesUnexpected	Number of responses that arrived from the SPB to requests of this type without an associated request.
ResponsesErrors	Number of responses received from the SPB to requests of this type, indicating the request failed.
ResponsesPartial	The number of responses from SPB indicating the request was only partially successful. Some items in the batch request were processed successfully, while others failed.

2.13.117 show service streaming analyzer

Shows various useful statistics about streaming.

```
show service streaming analyzer http
show service streaming analyzer rtmp
show service streaming analyzer rtsp
show service streaming analyzer smooth-streaming
show service streaming analyzer hds
show service streaming analyzer hls
```

Output	Description
StatsTotalResponses	Total responses
DropStreamResponseCount	Count for the dropped stream
StatsTotalFlows	Total flows
FailedHttpResponseMultipacketResponse	Failed multipacket HTTP responses
MultipacketResponseHeaders	Multipacket response headers
StatsTotalRequests	Total requests
FailedHttpResponseInsufficientSpace	Failed responses due to insufficient space
DropStreamRequestCount	Number of dropped streams by request

Output	Description
StallCount	Stall count
StatsTotalResponses	Total responses
DropStreamResponseCount	Count for the dropped stream
StatsTotalFlows	Total flows
FailedHttpResponseMultipacketResponse	Failed multipacket HTTP responses
MultipacketResponseHeaders	Multipacket response headers
StatsTotalRequests	Total requests
FailedHttpResponseInsufficientSpace	Failed responses due to insufficient space
DropStreamRequestCount	Number of dropped streams by request
TotalRtmpFlows	Total number of flows
Handshakes	Number of handshakes
NumMessagesParsed	Number of messages parsed
DropsDueToAmfParseErrors	Number of packet drops due to parse errors
DropsDueToMaxPayloadSize	Number of packet drops due to the maximum payload size being exceeded
DropsDueToMaxStreamLength	Number of packet drops due to the maximum stream length being exceeded
DropsDueToStalls	Number of packet drops due to stall
DropsDueToContextTooLarge	Number of packet drops due to the context being too large
TotalSmoothStreamingFlows	Number of flows identified as using smooth streaming.
ManifestsParsed	Number of video manifests parsed by the analyzer.
ManifestParseFailures	Number of video manifests the analyzer failed to parse.
ManifestCollisions	Number of manifests parsed by the analyzer that match an existing stored manifest.
MaxVideoStatesReached	Indicates if the maximum allowed video states has been reached.
VideosHandled	Number of videos processed.
VideoStateTimeouts	Number of times a video state has timed out.
VideoChunksSeenWithoutManifest	Number of video chunks that the analyzer sees as having no manifest.
MaxAlternateStreamLimitHit	Number of times the upper limit on the maximum number of alternate streams stored in the video state has been reached.

2.13.118 show service streaming analyzer smooth-streaming

Shows statistics for the video streaming analyzer.

Output	Description
TotalSmoothStreamingFlows	Number of flows identified as using smooth streaming.
ManifestsParsed	Number of video manifests parsed by the analyzer.

Output	Description
ManifestParseFailures	Number of video manifests the analyzer failed to parse.
ManifestCollisions	Number of manifests parsed by the analyzer that match an existing stored manifest.
MaxVideoStatesReached	Indicates if the maximum allowed video states has been reached.
VideoStateTimeouts	Number of times a video state has timed out.
VideoChunksSeenWithoutManifest	Number of video chunks identified by the analyzer as having no manifest.
MaxAlternateStreamLimitHit	Number of times the upper limit on the maximum number of alternate streams stored in the video state has been reached.

2.13.119 show service streaming errors

Shows errors in the streaming service.

TCPReorderingOutput	Description
GlobalBuffers	Number of global buffers
GlobalBuffersPeak	Global buffer peak
FlowBufferLimitReached	Whether or not the flow buffer has been reached
GlobalBufferLimitReached	Whether or not the global buffer limit has been reached
StallsDueToAcks	Number of streaming stalls due to error
StallsDueToRetransmits	Number of streaming stalls due retransmissions

Parse Errors Output	Description
Name	Streaming protocol's name
TotalFlows	Number of flows streaming
ParseErrorFlows	Number of flows with parse errors
PercentThreshold(%)	Percent threshold
ParseErrorAbsoluteThreshold	The absolute parse error threshold
ParseErrorAlarmEnabled	Indicates if the parse error alarm is enabled for the specified protocol

Concurrent Flows Output	Description
Name	Streaming protocol's name
Flows	Number of flows streaming

2.13.120 show service streaming stats

Shows statistics about streaming, including TCP reordering, parse errors and concurrent flows.

It takes one parameter, errors, which shows stats pertaining to errors only.

TCP Reordering Output	Description
GlobalBuffers	Number of global buffers
GlobalBuffersPeak	Global buffer peak
FlowBufferLimitReached	Whether or not the flow buffer has been reached
GlobalBufferLimitReached	Whether or not the global buffer limit has been reached
StallsDueToAcks	Number of streaming stalls due to error
StallsDueToRetransmits	Number of streaming stalls due retransmissions

Parse Errors Output	Description
Name	Error name
TotalFlows	Total number of flows
ParseErrorFlows	Number of parse error flows
ParseErrorPercent	Parse error percentage
Threshold (%)	Threshold percentage
ParseErrorAbsoluteThreshold	Absolute threshold for the parse error
ParseErrorAlarmEnabled	Whether or not the parse error alarm is enabled

Concurrent Flows Output	Description
Name	Name of concurrent flow
ConcurrentFlows	Number of concurrent flows
MaxConcurrentFlows	Maximum number of concurrent flows allowed
DropsDueToMaxConcurrentFlows	Number of packet drops due to the maximum concurrent flows flag being exceeded
ConcurrentFlowsAlarmEnabled	Whether or not the alarm related to concurrent flows is enabled

2.13.121 show service subscriber-management stats

Shows counters and statistics regarding IP-to-subscriber mapping.

`show service subscriber-management stats`

Session Cache Output	Description
SessionsCurrentlyMapped	Number of IP-to-subscriber mappings currently tracked by the system
SessionsPendingLogout	Number of IP-to-subscriber mappings logged-out, awaiting a final policy run
SessionsPendingLookup	Number of IP addresses the system is currently looking up
NetworkGroupsPendingLookup	Shows IP addresses being looked up, grouped into subnets
TotalSessionsMappedOnTime	Total number of IP addresses mapped on-time after traffic is seen

Session Cache Output	Description
TotalSessionsMappedLate	Total number of IP addresses mapped late after traffic is seen
TotalSessionsLoggedOut	Total sessions unmapped by an explicit IP unassignment notification
TotalSessionsExpired	Total sessions expired due to inactivity

Change Notification	Description
IpAssignmentNotifications	IP Assignment notifications received by the element
IpUnassignmentNotifications	IP Unassignment notifications received by the element
AttributeChangeNotifications	Attribute Change notifications received by the element

Management Notifications	Description
ClearStateNotifications	Clear Subscriber State notifications received by the element
EnableIpAddressLookupNotifications	IP Address Lookups Enabled notifications received by the element
DisableIpAddressLookupNotifications	IP Address Lookups Disabled notifications received by the element

Session IP Address Lookup	Description
IpAddressLookups	Total number of IP address lookups sent to the SPB
SkippedLookups	Total number of IP address lookups skipped based on config
MaxLookupsExceeded	Total number of IP address lookups suppressed due to max-retry limit reached
MappedResponses	Total number of IP address lookup responses containing a valid mapping
UnmappedResponses	Total number of IP address lookup responses containing no mapping
PendingResponses	Total number of IP address lookup responses currently pending
LookupsMappedByNotification	Total number of IP address lookups which were mapped by an IP Assignment notification before the response arrived
LookupsMappedByLookupResponse	Total number of IP address lookups which were mapped by a lookup response
CurrentLookupDelayMs	The current delay, in milliseconds, before the first lookup for any new subscriber IP is sent to SPB

Attributes Output	Description
AttributeValuesSet	Total number of attribute values set based on SPB notifications
AttributeValuesCleared	Total number of attribute values cleared (set to NULL) based on SPB notifications
CurrentAttributeStrings	Current number of subscriber attribute strings allocated by the system
SPBAttributesNoPolicyDefinition	Total number of attribute updates received from the SPB for attributes not defined in policy


2.13.122 show service subscriber-management dashboard

Shows a dashboard of Subscriber Management counters and statistics, which automatically refreshes with updated information.

```
show service subscriber-management dashboard
```

```
show service subscriber-management dashboard once
```

```
show service subscriber-management dashboard totals
```

 **Note:**
The dashboard runs continually. To exit, press **Ctrl-c**.

Attribute	Description
once	Dashboard iterates once and exits
totals	Shows lifetime totals for the element. By default, the dashboard shows counts starting at 0 when it starts.

Global System Statistics Output	Description
IpAddressesMappedToSubscribers	Number of subscriber-classes IP addresses mapped to a subscriber
IpAddressesNotMappedToSubscribers	Number of subscriber-classes IP addresses unmapped
MappingRate(perSec)	Rate at which IP addresses are becoming mapped (due to lookup or IP assignment notification)
UnmappingRate(perSec)	Rate at which IP addresses are becoming unmapped (due to timeout or IP unassignment notification)
AttributeRate(perSec)	Rate at which attributes are changing
MappedByNotificationAfterTraffic	Number of IP addresses mapped by an IP assignment notification after traffic was seen for that IP
MappedByLookup	Number of IP addresses mapped by a lookup response
MappedByNotificationBeforeTraffic	Number of IP addresses mapped by an IP assignment notification before traffic was seen for that IP
UnmappedByNotification	Number of IP addresses unmapped by an IP unassignment notification
UnmappedByTimeout	Number of IP addresses unmapped due to idle timeout
Attributes	Number of set-attribute actions taken

Per-element/per-module Notification Statistics	Description
TotalIpAssignments	Total number of IP assignments received by the element
ModuleTotalIpAssignments	IP assignment notifications received by the modules of the element
TotalIpUnassignments	IP unassignment notifications received by the element
ModuleTotalIpUnassignments	IP unassignment notifications received by the modules of the element
TotalAttrUpdates	Total number of attribute update notifications received by the element
ModuleTotalAttrUpdates	Total number of attribute updates by module
TotalNotificationsRecvd	Total number of notifications received by element

Per-element/per-module Notification Statistics	Description
ModuleTotalNotificationsRecvd	Attribute update notifications received by the modules of the element

Per-element/per-module Lookup Statistics	Description
LookupRequestsSent	IP Lookup requests sent by the element
ModuleLookupRequestsSent	IP Lookup requests sent by the modules of the element
LookupRepliesRecvd	IP Lookup responses received by the element
ModuleLookupRepliesRecvd	IP Lookup responses received by the modules of the element
LookupsTimedOut	IP lookup requests sent by the element timed out before response received
ModuleLookupsTimedOut	IP lookup requests sent by the modules of the element timed out before response received

Discarded Notifications	Description
AttrSkippedTypeMismatch	Attribute values dropped - type mismatch
SubscriberNameError	Notifications dropped - no subscriber name
SetAttrFailedNoRecord	Attribute values dropped - no subscriber mapping when attribute update received
IpNotInSubscriberClass	Notifications dropped - IP address not contained in a subscriber netclass

2.13.123 show service tunneling config

Displays the configuration for tunneling protocols.

```
show service tunneling config layer2
show service tunneling config packet-inspection
show service tunneling config udp
```

Options	Description
layer2	Layer 2 tunneling table.
packet-inspection	Packet inspection table.
udp	UDP tunneling table.

2.13.124 show service udp-prioritization

Shows the statistics of the UDP prioritized traffic.

Output	Description
Interface	The interface name on which the prioritized packets are received.
PrioritizedPackets	The number of prioritized UDP packets.

Output	Description
PrioritizedBytes	The number of prioritized bytes.

2.13.125 show subscriber all

This command writes all known subscriber sessions, and their attributes, in CSV format either to a console or to a file on the disk. If you output to console, the CSV output can be scanned or searched.

```
show subscriber all
```

```
show subscriber all file <filename>
```



Note:

This command may take up to 4 minutes to run.

Output	Description
Module Processing	Module containing the active session.
Instance Processing	Instance on the module containing the active session.
IP	IP Address (or IP prefix), with session qualifier, that is mapped.
State	State of the session: <ul style="list-style-type: none">• [trying] - The element is attempting to look-up the IP assignment details for this IP.• [mapped] - The element has mapped this IP address to a subscriber.
SessionID	Unique identifier of this session in the Sandvine system.
Subscriber	The name of the subscriber that owns this session
CreationTime	The epoch timestamp, in seconds, indicating the time this session record was created on this element.
AssignedTime	The epoch timestamp, in seconds, indicating the time this session record was mapped to a subscriber on this element.
ExpirationTime	The epoch timestamp, in seconds, indicating when this record is due to expire if it becomes idle.
NetworkAssignedTime	The epoch timestamp, in seconds, indicating the time this session was mapped to a subscriber in the network (on the SPB or on the AAA server).
IsActive	"True" if the session has seen data traffic activity, "false" otherwise.
Attributes	Each of the remaining columns describes the value of one attribute in the system for this session. The column headers are the attribute names.

2.13.126 show subscriber ip

Shows information about a particular subscriber IP assignment.

```
show subscriber ip <ip-address>
```

```
show subscriber ip <ip-address> port <int:0..65535>
```

```
show subscriber ip <ip-address> site <site>
```



Note:

If the subscriber has recently been re-balanced from one module to another (for example, because a module was overloaded, or a PTS in the cluster was restarted), the subscriber information may appear for two separate modules until the subscriber record times out (20 minute maximum) on the original module.

Attribute	Description
ip	User-specified IP address (IPv4 format only).
port	The port number for which to show subscriber information.
site	Session qualifier site number to use for lookup of subscriber session. Default is 0.

Output	Description
IpAddress IP	Address assigned.
PrefixLength	Size of the IP prefix of the assignment.
Name	The subscriber's name.
Status	One of: <ul style="list-style-type: none">• [trying] - The element is attempting to look-up the IP assignment details for this IP.• [mapped] - The element has mapped this IP address to a subscriber.• [login] - PTS has received IP to subscriber mapping notification from SPB but the subscriber is not active.
NetworkClass	Network class of the IP address, as defined in subnets.txt.
NetworkMappedTime	Time when this subscriber mapping was created in the network (on the SPB or on the AAA server).
PolicyClass	Policy class of the IP address, as defined in subnets.txt.
Module	Processing module on which this IP assignment is active.
SiteNumber	Session qualifier site number of the displayed session.
Session ID	Unique identifier of this session in the sandvine system.

2.13.127 show subscriber name

Shows information about all IP assignments for a particular subscriber.

```
show subscriber name <name>
```



Note:

If the subscriber has recently been re-balanced from one module to another (for example, because a module was overloaded, or a PTS in the cluster was restarted), the subscriber information may appear for two separate modules until the subscriber record times out (20 minute maximum) on the original module.

Output	Description
IpAddress IP	Address assigned.
PrefixLength	Size of the IP prefix of the assignment.
Name	The subscriber's name.

Output	Description
Status	One of: <ul style="list-style-type: none"> [trying] - The element is attempting to look-up the IP assignment details for this IP. [mapped] - The element has mapped this IP address to a subscriber. [login] - PTS has received IP to subscriber mapping notification from SPB but the subscriber is not active.
NetworkClass	Network class of the IP address, as defined in subnets.txt.
NetworkMappedTime	Time when this subscriber mapping was created in the network (on the SPB or on the AAA server).
PolicyClass	Policy class of the IP address, as defined in subnets.txt.
Module	Processing module on which this IP assignment is active.
SiteNumber	Session qualifier site number of the displayed session.
Session ID	Unique identifier of this session in the sandvine system.

2.13.128 show subscriber all file

Writes all known subscriber sessions, including their attributes (in CSV format) to either a console or disk file.

```
show subscriber all
show subscriber all file <filename>
```

Attribute	Description
File	User-specified file name

Column	Description
Module	The processing module running the active session.
Instance	The processing instance on the module with the active session.
IP	This is the mapped IP address (or IP prefix), with session qualifier.
State	Identifies the session state: <ul style="list-style-type: none"> [trying]—The element is attempting to look-up the IP assignment details for this IP. [mapped]—The element has mapped this IP address to a subscriber.
SessionID	Unique identifier of this session in the sandvine system.
Subscriber	Identifies the subscriber that owns the current session.
CreationTime	The epoch timestamp, in seconds, indicating the time that the session record was created on this element.
AssignedTime	The epoch timestamp, in seconds, indicating the time that the session record was mapped to a subscriber on this element.
ExpirationTime	The epoch timestamp, in seconds, indicating when this record will expire if it becomes idle.

Column	Description
NetworkAssignedTime	The epoch timestamp, in seconds, indicating the time that the session was mapped to a subscriber in the network (on the SPB or on the AAA server).
IsActive	Indicates whether the session has seen data traffic: <ul style="list-style-type: none">Set to <code>true</code> if the session has seen data traffic activity.Set to <code>false</code> if no traffic activity has occurred.
Attributes	Each of the remaining columns describes the value of one attribute in the system for this session. The column headers are the attribute names.

2.13.129 show system accounting

This command is used for remote accounting using TACACS+

```
show system accounting
```

Output	Description
Name	Protocol that is used for accounting.
Enabled	Specifies whether accounting is enabled or disabled. Note: When accounting is not configured, it is disabled.
Queued	Number of packets queued.
QueuePercentFull	Queued records percentage calculated based on the "queue size" configured at accounting configuration.
Sent	Number of accounting records sent.
Errors	Accounting errors caused due to server unavailability or any TACACS+ server error.
Dropped	Number of Dropped records once the configured queue limit exceeds.

2.13.130 show system blades

Shows the blades that are plugged into each slot and displays information regarding each blade.

Output	Description
Slot	The slot number Possible values: 1 and 2.
Type	The blade model.
OperStatus	Operational status of the blade. Possible values are: <ul style="list-style-type: none">Up - blade operationalNot installed - no blade in slotNot active - blade is plugged in, but has not been powered on. Most likely to happen when a blade is plugged in after the system has been powered onFaulted - there is a hardware issue with the blade.
SerialNumber	The serial number of the blade.

2.13.131 show system environmental

Shows the environmentally monitored devices in the system.

Fan Output	Description
Description	A description of the fan.
Value	The fan speed in revolutions per minute (RPM).

Temperature Output	Description
Description	Description of the machine component.
Value	Value of the sensor, as measured in Celsius.
Status	Status of the temperature alarm.

Power Supplies Output	Description
Description	Description of the power supply.
Value	Value of the device, which could be its status, voltage, current or temperature.

Voltage Output	Description
Description	Description of the machine component.
Value	Value of the device, as measured in volts.

Current Output	Description
Description	Description of the machine component.
Value	Value of the device, as measured in amps.

2.13.132 show system environmental fans

Shows information from the fan sensors.

Fan Output	Description
Description	A description of the fan.
Value	The fan speed in revolutions per minute (RPM).

2.13.133 show system environmental power

Shows devices with power supplies or a specific power supply.

```
show system environmental power
```

Power Output	Description
Description	Description of the machine component
Value	Value of the sensor or device, as measured in its scale. For example, Celsius for temperature, or mA for current.

2.13.134 show system environmental temperature

Shows all monitored temperatures and statuses in the system. Typically, this includes disks, power supplies, and CPUs.

CPU temperatures are reported for both the PTS and the SPB. In addition to the CPU temperature, there is a CPU thermal warning counter for each module. The CPU thermal warning counter is incremented on a per-minute basis whenever the CPU is in thermal throttling mode due to high temperature.

Power supplies have multiple temperature sensors. One sensor reports a temperature measurement while the other sensors generate temperature alarms. As a result, it is possible for temperature alarms to trigger on a particular temperature threshold, without the temperature measurement reading values that exceed that same threshold. This does not indicate a malfunctioning temperature alarm.

Temperature alarm thresholds vary depending on the particular device and power supply model.

```
show system environmental temperature
```

Temperature Output	Description
Description	Description of the machine component.
Value	Value of the sensor, as measured in Celsius.
Status	Status of the temperature alarm.

2.13.135 show system environmental voltage

Shows all monitored voltages in the system.

Voltage Output	Description
Description	Description of the machine component.
Value	Value of the device, as measured in volts.

2.13.136 show system firewall

Shows configuration of the firewall subsystem based on current state.

If settings have been changed but not yet applied, this output may differ from the configuration output. In addition, those ports required for product functionality will appear in the command output.

Output	Description
Port	The port number
Status	Whether the port is open or closed

Output	Description
Protocol	The type of protocol

2.13.137 show system hardware

Shows all hardware installed in the system.

Output	Description
Id	Hardware component ID
Description	Description of the hardware
SerialNum	Serial number of the hardware
ModelName	Model name of the hardware

2.13.138 show system hardware machine-check

Displays hardware errors by severity.

```
show system hardware machine-check  
show system hardware machine-check controller  
show system hardware machine-check module <id:1..10>
```

Parameter	Description
ID	The ID of the module to show

Output	Description
Description	Name of the hardware
Correctable	Number of correctable errors
Uncorrectable	Number of uncorrectable errors
Fatal	Number of fatal errors

2.13.139 show system history enable

Show the history of the command `sv_enable`, including permission changes.

Output	Description
Date	Date of the change
User	The user that made the change
OldPrivileges	The old privilege
NewPrivileges	The new privilege

2.13.140 show system history login

Shows the history of SSH logins.

Output	Description
Date	Date and time of the login
User	The User who logged in
Ip	The connecting IP
Port	The connecting port
Authentication	The authentication method.

2.13.141 show system history reload

Shows when the svreload command was run, the result and what configuration files were modified.

Output	Description
Date	Date and time svreload was run
PolicyModified	Indicates if SandScript configuration was modified
SubnetsModified	Indicates if subnets configuration was modified
RcModified	Indicates if system configuration was modified
Result	Indicates if the reload was a success

2.13.142 show system indicators

Shows the state of the physical indicators (LEDs) on the system.

Indicator devices

Via SNMP, the INDICATOR DEVICE MIB shows the status of all indicator LEDs on the system — power, online, fault, and alarm. A table is provided for each of the LEDs and their current state. Depending upon the indicator, the possible states are: off, green or red.

The power LED will always be green in a stable power condition.

The online LED should be green. If the online LED is off, services are not running properly. Execute the show system services command to see the operational status of the services running on the element.

On the PTS 8210, the fault LED is used to indicate an over temperature condition. Off indicates normal operation. Red indicates an over temperature fault. When an over temperature condition is detected, the CPU shuts down. The fault LED is not used on any other platform.

The alarm LED should be off. This alarm is red if any alarm of severity minor or greater is currently present in the alarmActive table. It is automatically cleared if the alarm is cleared. This indicator is controlled by the alarm MIB device. If the alarm LED is on, reference the MIB to determine what generated the alarm.

Output	Description
Id	Indicator ID
Type	Type of indicator
State	Indicator state

2.13.143 show system information

Shows basic information about the system.

```
Hostname       : PTS1
Model          : PTS24100-A
SerialNumber   : SDVN86010771
ControlMAC     : 00:09:35:1e:10:00
ControlIP      : 10.135.18.166/30
InternalServiceIP : 5.0.0.1/24
ExternalServiceIP : 4.0.0.1/24
CurrentTime    : 2013-09-20 09:58:47 EDT
Uptime         : 2 hours, 13 minutes
LastReboot     : 2013-09-20 07:45:59 EDT
LastUpdate     :
```

Output	Description
Hostname	The hostname for the element.
Model	The Sandvine model number.
Serial Number	The element's serial number.
ControlMac	MAC address for the control interface.
ControlIP	The IP for the control interface.
ExternalServiceIP	The IP address used to connect to devices over the service interface(s).
InternalServiceIP	The IP address used to connect to other elements in the cluster and for internal service communication.
CurrentTime	The current time.
Uptime	How long the system has been running.
LastReboot	The date and time the element was last rebooted.
LastUpdate	The date and time the element was last updated.

2.13.144 show system licenses

This command shows all the licenses that the system uses. If a license ID is provided, it will show all the features currently included in that license.

```
show system licenses
```

```
show system licenses <id:0..>
```

Output	Description
Name	Identifies the feature. Describes the state of the license.
State	Describes the state of the license.
ExpirationDate	Identifies the date that the license is set to expiration.

Output	Description
Id	The ID of the feature.
Name	Identifies the feature.
State	Identifies the date that the license is set to expiration.
Major	
Minor	
Start Date	The date this licence was started.
ExpirationDate	Identifies the date that the license is set to expiration.
Days to Expiry	Identifies the time, in days, remaining before this licence will expire.

**Note:**

In PTS version 6.30 and higher, the `show system licenses` command shows valid (active) and invalid (expired) licenses.

2.13.145 show system modules

Shows details about the modules in the system.

Output	Description
Id	Module ID
AdminStatus	Administrative status of the system module - up or down
OperStatus	Operational status of the system module - up or down
LastOnlineTime	Last online time of the module, or defined as online at the moment the command was run
RebootCause	Cause of a module reboot. For example, powerLoss.

MIB reference

Data displayed as part of this command is from the `svModuleControllerModuleTable` in the SANDVINE-MIB.

SNMP notifications

The following SNMP notifications occur when a module has gone down or returns to operational status:

- `svSysModuleDownNotification`
- `svSysModuleUpNotification`.

For more information, see the SANDVINE-MIB.

Related alarms

Alarm model 9: Processing module down

2.13.146 show system nat

Shows the active Network Address Translation (NAT) configuration.

Output	Description
InputInterface	Input interface for the NAT configuration
OutputInterface	Output interface for the NAT configuration

2.13.147 show system overview

Shows an overview of what the PTS is doing.

Key Performance Indicators Output	Description
Service	Identifies the service that the indicator applies to.
Indicator	Identifies the name of the system indicator.
Value	Lists the value(s) of the indicator.
Units	Identifies the unit of indicator data.

Traffic Output	Description
ApplicationType	Application type for the traffic.
SessionRate	The session rate.
Downstream(bps)	The number of bits per second for downstream traffic.
Upstream(bps)	The number of bits per second for upstream traffic.
Total(bps)	Total number of bits per second for upstream and downstream traffic.

2.13.148 show system processes

Shows system processes running on the controller for all modules.

```
show system processes
show system processes module <module-id>
show system processes controller
```

Output	Description
User	Process user. For example, pgsql.

Output	Description
PID	Process ID.
%Cpu	Percentage of CPU the process is using at the time the command is run.
%Mem	Percentage of the total system memory the process is using.
Vsz	Total virtual memory used by the process.
Rss	Total resident memory used by the process.
Tt	Tty associated with the process.
Stat	Current state of the process.
Started	Date the process started.
Time	Total CPU time used by the process over its lifetime.
Command	Process name.

2.13.149 show system resources

Shows a list of system resources for the system, a specific resource ID, controller or module. System resources include hard disk space, memory, flows, and other resources that, if exhausted, will impact the proper functioning of the system.

```
show system resources
show system resources <id:1..>
show system resources controller
show system resources module
show system resources module <id:1..>
```

Output	Description
Id	Resource or module ID.
Description	Description of the resource.
Instances	This is the total number (or instances) of this type of resources in the system.
Min	Across all of the instances in the system, this is the value of the one with the lowest utilization.
Max	Across all of the instances in the system, this is the value of the one with the highest utilization.
Avg	This is the average utilization across all of the instances in the system.
AllocationFailures	Number of allocation failures.

This table lists the resources and their descriptions

Output	Description
Real memory	The sum total of real memory installed on all the modules of PTS.
Swap space	The sum total of swap space on every module.
Mbuf clusters	The total space of mbuf cluster available on each module.
Packet memory	The total memory allocated to store packets for each PTSD instance across each module.

Output	Description
Filesystem /	Disk space on / directory for the PTS.
Filesystem /d2	Disk space on /d2 directory for the PTS.
File descriptors	The total number of File descriptors present across all the modules.
Kernel memory	The sum of memory being used by the freebsd kernel on each module.
PTS Flows	The total number of flows which PTS can handle. This value is arrived at by adding the PTS flows allocated on every PTSD instance.
PTS Subscriber Mappings	The total number of subscribers which PTS can map. Sum of the number of subscribers mapped by each PTSD instance.
DNS Users	The total number of subscribers which PTS can report of DNS statistics. Sum of the number of DNS users at each PTSD instance.
PTS bandwidth detection bins	The total sum of bandwidth detected on each PTSD instance.
NPU MacVlan table space	The total number of Mac address associated to VLAN on PTS.
WDTM Detection Session	The total number of session Worm Service Traffic Mitigation (WDTM) detected by each PTSD instance.
WDTM Detection Session (on CND)	The total number session of WDTM detected on aggregates statistic on CND.
WDTM Attack Object	The total number of WDTM Attack Object detected by PTS on each PTSD instance.
Attribute string memory	The total set of attribute (such as network protocol info etc) that are being store by each PTSD instance in the memory.
PTS shaping memory	The sum of memory being used by the shapers for shaping the traffic on each PTSD instance.
PTS level distribution instances	The total amount of PTSD level distribution instances allocated on each PTSD instance.
PTS tee header entries	The total sum of Tee Header entries accumulated on PTS across all the PTSD instances.
Measurements	The total number of measurements which PTS can define. The total number is arrived at by adding the total number of measurements in each PTSD instance.
PTS shaping packets	The total number of shaped packet being process across all the PTSD instances.
PTS demographic stats hosts	The total amount of statistic being collected and inspected based on network classes & demographic.
Classifiers	The total number of Classifiers which PTS can define.
PTS policy table rows	The total number of PTS table rows which PTS can define.
TCP Reassembly Buffering	The total of reassembled TCP packet buffer in memory.
Stream Analysis Buffering	The total of TCP Datagram Reassembly in memory buffer.
PTS Map Memory	The total of memory being used for mapping subscriber.
Streaming Flows	The total amount of streaming being flow being process by PTSD.
PTS Primed Flow Classification instances	The total amount of PTS pre-determines specific types of traffic.
PTS IP Fragmentation Records	The total amount of IP Fragmentation being recorded by PTSD process.
External Ethernet MAC address pairs	The total memory being used for External MAC Address being pair in PTS.
Spam Detector SMTP Host State	The total memory being allocated for SMTP Spam Host.
WDTM Detection User	The total number of subscribers which PTS can apply policy for WDTM across each module.

Output	Description
Statistic Records	The total number of statistic being recorded by PTS.
Reassembly Buffers (Small)	The total of reassembly small datagram stored in memory buffer.
Reassembly Buffers (Medium)	The total of reassembly medium datagram stored in memory buffer.
Reassembly Buffers (Large)	The total of reassembly large datagram stored in memory buffer.
RTMP Streaming Flows	The total amount of streaming flows on PTS.
Process memory	The total amount of memory available to software processes on each module.
Process CPU (Hertz)	The total amount of time Of CPU used by each process like SCDPD, SFCD, PTSD, CND on each module.
Processor CPU (Hertz)	The total amount of time the processor on each module executed the process code.
HTTP Streaming Flows	The total amount of HTTP Streaming Flow on PTS.
PTS Policy Controller Server memory	The total amount of memory being used for aggregate statistic on Policy from PTSD on PTS.
PTS Policy Controller Client memory	The total amount of memory being used and sent of policy to CND from PTSD.
BGP client RIB memory	The total amount of memory used in BGP Routing Information Base.
PTS policy table row memory	The total size policy table per row is being used in memory.
Dynamic Shunted Subnets	The total amount of dynamic shunted subnetwork being process by PTS.
Subscriber NAT Mappings	The total amount of Subscriber with NAT entry mapping in PTS.
PTS Map Entries	The total size of Mapping Entries Subscriber on PTS.
Central LB Table Rows	The total IP Load-Balancer in PTS.
JVM Memory	Identifies the runtime memory usage. This output only appears on the SPB.
HTTP Threads	The number of HTTP threads in use. This output only appears on the SPB.
HTTPS Threads	The number of HTTPS threads in use. This output only appears on the SPB.

MIB Reference

Data displayed as part of this command is from the hrStorageTable in the HOST-RESOURCES-MIB.

Data displayed as part of this command is from the svSpbAppResourceTable in the SANDVINE-SPB-APP-MIB.

SNMP Notifications

These SNMP notifications occur when a module has gone down or returns to operational status:

- svSystemResourceLowNotification
- svSystemResourceOkNotification.

For more information, see Alarm Model 7.

Related Alarms

Alarm Model 7: Resource usage exceeds recommendations

Alarm Model 35: Resource allocation failures

2.13.150 show system services

Shows services provided by the system, along with their operational status, uptime, and other data.

Output	Description
Name	System service name.
AdminStatus	Administrative status - up or down
OperStatus	Operational status: <ul style="list-style-type: none">• online — the service is functioning correctly• degraded — some parts of the service is not functioning• stopped — the service has been stopped, or has not started• faulted — the service has experienced a fault• reloading — the service is reloading• starting — the service has just started• initializing — the service is initializing• disabled — the service has been administratively disabled• unlicensed — the service is not licensed and will not run.• diagnostic — the service is providing special functionality to validate the integrity of the software and/or hardware.
AdminStarts	Number of administrative starts of the service since it was initialized
AdminStops	Number of administrative stops of the service since it was initialized
Faults	Number of faults the service has had since initialization
LastFaultTime	Time and date of the last service fault
LastOnlineTime	Last time and date the service was online
LastReloadTime	Last time and date the service was reloaded

2.13.151 show system services last-reload

Shows information for monitored system services.

```
show system services last-reload
```

Output	Description
LastReloadTime	Date and time of the last service reload
LastReloadSuccessful	Whether the last reload of the service was successful
Id	ID of the reload error
Description	Description of the reload error
ErrorSeverity	Severity of the reload error
TrapEnabled	Whether the trap for the reload error is enabled (true) or disabled (false)

Output	Description
InError	Whether the reload error occurred during the last reload

2.13.152 show system storage container

Shows information about storage containers.

```
show system storage container
```

Controller Output	Description
Id	Controller ID
DeviceName	Device name as recognized by the OS, for example, /dev/aac0
Vendor	Vendor name
Description	A description of the device. For example, AAC-RAID RAID Controller.
IsRaid	Device is RAID - true or false
BatteryState	State of battery
Controllers found	Number of controllers found
Logical Device Output	Description
Logical device number	Logical device number
Logical device name	Name of the logical device. For example, OS.
RAID level	RAID level
Status of logical device	Status
Size	Size
Read-cache mode	Controller is set to read cache mode - enabled or disabled
Write-cache mode	Controller is set to write cache mode - enabled or disabled
Write-cache setting	Controller is set to write cache setting - enabled or disabled
Partitioned	Logical device is partitioned - yes or no
Protected by Hot-Spare	Logical device is protected by a hot spare - yes or no
Bootable	Logical device is bootable - yes or no
Failed stripes	Device is set to failed stripes, - yes or no
Power setting options	Power setting - enabled or disabled
Segment [#]	Whether delimited segment is present or not

Controller Output	Description
Logical device number	Logical device number
Logical device name	Name of the logical device. For example, OS.
RAID level	RAID level

Controller Output	Description
Status of logical device	Status
Size	Size
Read-cache mode	Controller is set to read cache mode - enabled or disabled
Write-cache mode	Controller is set to write cache mode - enabled or disabled
Write-cache setting	Controller is set to write cache setting - enabled or disabled
Partitioned	Logical device is partitioned - yes or no
Protected by Hot-Spare	Logical device is protected by a hot spare - yes or no
Bootable	Logical device is bootable - yes or no
Failed stripes	Device is set to failed stripes, - yes or no
Power setting options	Power setting - enabled or disabled

2.13.153 show system storage controller

Shows information about storage controllers.

```
show storage controller
```

```
show storage controller <id:0..>
```

Controller Output	Description
Id	Controller ID.
DeviceName	Device name as recognized by the OS, for example, /dev/aac0.
Vendor	Vendor name.
Description	A description of the device. For example, AAC-RAID RAID Controller.
IsRaid	Device is RAID - true or false.
BatteryState	State of battery.
Firmware	The version of firmware running on the storage controller.

2.13.154 show system storage disk

Shows information about storage disk.

```
show system storage disk
```

```
show system storage disk <id:0..>
```

Output	Description
ID	The ID number of the device.
DeviceName	The name of the device.

Output	Description
PassDeviceName	The pass name of the device.
Vendor	The vendor's name.
Model	The device's model number.
Description	A description of the device.
SerialNumber	The device's serial number.
Revision	The revision number of this device.
Slot	The slot the device is installed in.
BusSpeed	The speed of the interface used to communicate with the disk, in MHz.
WriteCache	Indicates whether the disk's write cache is enabled (on) or disabled (off).
StopCount	Number of times the disk has gone idle and stopped spinning since powered on.
MaxStopCount	Maximum value that StopCount has ever reached.
GrowthDefects	The number of growth defects on the device. For platforms with solid state disk drives, growth defects are expected over time. You can analyze UncorrectableReadErrors, UncorrectableWriteErrors, and PercentageLifetimeUsed to determine the health of an SSD disk.
UncorrectableReadErrors	The number of read errors on the device.
UncorrectableWriteErrors	The number of write errors on the device
SmartStatus	Pass if S.M.A.R.T. data indicates that the drive is in working order, fail if S.M.A.R.T. indicates that a disk failure may be imminent.
MRIE	Method of Reporting Interval Exceptions (MRIE) mode that the drive has been configured to use.
Size	The size of the disk.
Bus	Identifies the SCSI bus to which this disk is attached.
Target	Identifies the SCSI target to which the disk is attached.
HasTasks	Indicates whether the drive is busy or not.
Timestamp	Last time that data was gathered for this disk.
Status	Current status of the disk (faulted or online).
PercentageLifetimeUsed	This field is only applicable for solid state disk drives. For non-SSDs, this value is always 0 and you can ignore it. For platforms with SSDs, this field represents the percentage of the number of write cycles (0-100) used up on the disk. The solid state drives (SSD) in the PTS 22000 can only be written to a fixed number of times before the disk will begin to fail.
PowerOnHours	Cumulative number of hours that this drive has been powered on.

2.13.155 show system version

Shows high level version information for the system including installed Sandvine products. If detail is requested, it also includes a list of software packages installed. If protocols is requested, it also includes currently running versions of protocol libraries.

```
show system version
```

```
show system version detail
```

```
show system version protocols
```

Output	Description
Product	Product name
Version	Product version

Output	Description
Software Package	The installed software package
Version	Software package version

Output	Description
LibContents	The names of the protocols in this library.
LibName	The filename of the library loaded for these protocols.
Build	The build version of this library.
BuildDate	The date on which this library was built.
MinorVersion	Protocol version number
MajorVersion	The major protocol pack version to which this library belongs.

2.13.156 show traffic

Provides information about traffic being processed by the system. All bits per second outputs are calculated as the sum of the bytes in the specified flows, over the lifetime of the flows.

Output	Description
ApplicationType	Application type for the traffic
SessionRate	The session rate
Downstream(bps)	Number of bits per second for downstream traffic
Upstream(bps)	Number of bits per second for upstream traffic
Total(bps)	Total number of bits per second for upstream and downstream traffic

2.13.156.1 show traffic ip, show traffic subscriber

Provides an overview about the traffic being processed for a specific IP or specific subscriber IP.

```
show traffic ip <ip-address>
show traffic ip <ip-address> site <site>
show traffic subscriber <subscriber-name>
```

Attribute	Description
ip	IP address to show traffic overview for.
site	The number of the site that this subscriber's traffic passes through. Default is 0.
subscriber	The name of the subscriber to show traffic overview for.

IP Address Output	Description
Site	The subscriber's site. Used together with the IP to uniquely identify the subscriber.
IP	The subscriber's IP address. Used together with the Site to uniquely identify the subscriber.
Flows	The number of flows for a specific IP address or subscriber.
BytesUpIn	The number of bytes sent from the subscriber to the internet.
BytesDownOut	The number of bytes sent from the internet to the subscriber (after routing through the PTS).
RateUpIn(bps)	The rate of flow (bits-per-second) from the subscriber to the internet.
RateDownOut(bps)	The rate of flow (bits-per-second) from the internet to the subscriber (after routing through the PTS).

Policy Action Output	Description
Action	The policy action name.
Flows	The number of flows the policy action is being applied to.
BytesUpIn	The number of bytes sent from the subscriber to the internet.
BytesDownOut	The number of bytes sent from the internet to the subscriber (after routing through the PTS).
RateUpIn(bps)	The rate of flow (bits-per-second) from the subscriber to the internet.
RateDownOut(bps)	The rate of flow (bits-per-second) from the internet to the subscriber (after routing through the PTS).

Application Output	Description
Application	The protocol application (for example, HTTP).
Flows	The number of flows with this specific application.
BytesUpIn	The number of bytes sent from the subscriber to the internet.
BytesDownOut	The number of bytes sent from the internet to the subscriber (after routing through the PTS).
RateUpIn(bps)	The rate of flow (bits-per-second) from the subscriber to the internet.
RateDownOut(bps)	The rate of flow (bits-per-second) from the internet to the subscriber (after routing through the PTS).

2.13.156.2 show traffic ip flows, show traffic subscriber flows

Provides a list of traffic flows being processed for a specific IP or subscriber.

```
show traffic ip <ip-address> flows
show traffic ip <ip-address> site <site> flows
show traffic subscriber <subscriber-name> flows
```

Attribute	Description
ip	IP address to show traffic overview for.
site	The number of the site that this subscriber's traffic passes through.
subscriber	Subscriber to show traffic overview for.

Output	Description
Site	The site of the subscriber. Used together with the SubscriberIP to uniquely identify the subscriber.
SubscriberIP	The IP address of the subscriber. Used together with the Site to uniquely identify the subscriber.
SubscriberPort	The port of the subscriber.
InternetIP	The internet IP address.
InternetPort	The internet port.
L4	The layer 4 protocol (for example, TCP, UDP).
Application	The application protocol (for example, HTTP).
RateUpIn(bps)	The rate of flow (bits-per-second) from the subscriber to the internet.
RateDownOut(bps)	The rate of flow (bits-per-second) from the internet to the subscriber (after routing through the PTS).

2.13.156.3 show traffic ip flows detail, show traffic subscriber flows detail

Provides an overview about the traffic being processed for a specific subscriber IP or subscriber name.

```
show traffic ip <ip-address> flows detail
show traffic ip <ip-address> site <site> flows detail
show traffic subscriber <subscriber-name> flows detail
```

Attribute	Description
ip	IP address to show traffic overview for.
site	The number of the site that this subscriber's traffic passes through.
subscriber	Subscriber to show traffic overview for.

Output	Description
Site	The site of the subscriber. Used together with SubscriberIP to uniquely identify the subscriber.
SubscriberIP	The IP address of the subscriber. Used together with Site to uniquely identify the subscriber.
SubscriberPort	The port of the subscriber.
InternetIP	The internet IP address.
InternetPort	The internet port.

Output	Description
L4	The layer 4 protocol (for example, TCP, UDP).
Application	The application protocol (for example, HTTP).
RateUpIn(bps)	The rate of flow (bits-per-second) from the subscriber to the internet.
RateDownOut(bps)	The rate of flow (bits-per-second) from the internet to the subscriber (after routing through the PTS).
BytesDownIn	The number of bytes sent from the internet to the subscriber.
BytesDownOut	The number of bytes sent from the internet to the subscriber (after routing through the PTS).
RateUpIn(bps)	The rate of flow (bits-per-second) from the subscriber to the internet.
RateUpOut(bps)	The rate of flow (bits-per-second) from the subscriber to the internet (after routing through the PTS).
RateDownIn(bps)	The rate of flow (bits-per-second) from the internet to the subscriber.
RateDownOut(bps)	The rate of flow (bits-per-second) from the internet to the subscriber (after routing through the PTS).
Age(s)	The age of the flow (in seconds).
SubscriberRTT	The subscriber round trip time, in milliseconds.
InternetRTT	The internet round trip time, in milliseconds.
Actions	The policy actions applied to the flow.


2.13.157 show user

This command lists local or remote user(s) who were created due to local or remote authentication. You can also specify a name to view details of a specific user.

```
show user
```

```
show user <name>
```

Output	Description
Name	The user's name.
Group	The user's privilege level.
Type	The type of user account (local or remote to indicate if they were created locally or due to remote authentication).
DefaultShell	The user's default shell, either "bash" or "cli".
LastLogin	The last time the user logged in to the system.



Sandvine Incorporated
408 Albert Street
Waterloo, Ontario, Canada
N2L 3V3

Phone: (+1) 519-880-2600
Fax: (+1) 519-884-9892

Web Site: www.sandvine.com