Packet Flow Operating Software (PFOS) 6.x
CLI Reference Guide

Software Version 6.5.1

733-1945 / June 2024

Use of this product is subject to the End User License Agreement available at http://www.NetScout.com/legal/terms-and-conditions or which accompanies the product at the time of shipment or, if applicable, the legal agreement executed by and between NETSCOUT Systems, Inc. or one of its wholly-owned subsidiaries ("NETSCOUT") and the purchaser of this product ("Agreement").

Government Use and Notice of Restricted Rights: In U.S. government ("Government") contracts or subcontracts, Customer will provide that the Products and Documentation, including any technical data (collectively "Materials"), sold or delivered pursuant to this Agreement for Government use are commercial as defined in Federal Acquisition Regulation ("FAR") 2.101 and any supplement and further are provided with RESTRICTED RIGHTS. All Materials were fully developed at private expense. Use, duplication, release, modification, transfer, or disclosure ("Use") of the Materials is restricted by the terms of this Agreement and further restricted in accordance with FAR 52.227-14 for civilian Government agency purposes and 252.227-7015 of the Defense Federal Acquisition Regulations Supplement ("DFARS") for military Government agency purposes, or the similar acquisition regulations of other applicable Government organizations, as applicable and amended. The Use of Materials is restricted by the terms of this Agreement, and, in accordance with DFARS Section 227.7202 and FAR Section 12.212, is further restricted in accordance with the terms of NETSCOUT'S commercial End User License Agreement. All other Use is prohibited, except as described herein.

This Product may contain third-party technology. NETSCOUT may license such third-party technology and documentation ("Third- Party Materials") for use with the Product only. In the event the Product contains Third-Party Materials, or in the event you have the option to use the Product in conjunction with Third-Party Materials (as identified by NETSCOUT in the Documentation provided with this Product), then such Third-Party Materials are provided or accessible subject to the applicable third-party terms and conditions contained in the "Read Me" or "About" file located in the Software, on an Application CD provided with this Product, in an appendix located in the documentation provided with this Product, or in a standalone document where you access other online Product documentation. To the extent the Product includes Third-Party Materials licensed to NETSCOUT by third parties, those third parties are third-party beneficiaries of, and may enforce, the applicable provisions of such third-party terms and conditions.

Open-Source Software Acknowledgement: This product may incorporate open source components that are governed by the GNU General Public License ("GPL") or licenses similar to the GPL license ("GPL Compatible License"). In accordance with the terms of the GPL Compatible Licenses, NETSCOUT will make available a complete, machine-readable copy of the source code components covered by the GPL Compatible License, if any, upon receipt of a written request. Please identify the NETSCOUT product and open source component, and send a request to:

NETSCOUT SYSTEMS, INC

Open Source Code Request

310 Littleton Road

Westford, MA 01886

Attn: Legal Department

To the extent applicable, the following information is provided for FCC compliance of Class A devices:

> This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.
>
> Modifications to this product not authorized by NETSCOUT could void the FCC approval and terminate your authority to operate the product. Please also see NETSCOUT's Compliance and Safety Warnings for NetScout Hardware Products document, which can be found in the documents accompanying the equipment, or in the event such document is not included with the product, please see the compliance and safety warning section of the user guides and installation manuals.

No portion of this document may be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine form without prior consent in writing from NETSCOUT. The information in this document is subject to change without notice and does not represent a commitment on the part of NETSCOUT.

The products and specifications, configurations, and other technical information regarding the products described or referenced in this document are subject to change without notice and NETSCOUT reserves the right, at its sole discretion, to make changes at any time in its technical information, specifications, service, and support programs. All statements, technical information, and recommendations contained in this document are believed to be accurate and reliable but are presented "as is" without warranty of any kind, express or implied. You must take full responsibility for their application of any products specified in this document. NETSCOUT makes no implied warranties of merchantability or fitness for a purpose as a result of this document or the information described or referenced within, and all other warranties, express or implied, are excluded.

Except where otherwise indicated, the information contained in this document represents the planned capabilities and intended functionality offered by the product and version number identified on the front of this document. Screen images depicted in this document are representative and intended to serve as example images only.

Copyright 2009-2024 NETSCOUT Systems, Inc. All rights reserved.

Table of Contents

NETSCOUT

Revision History

Date	Rev	Description
June 2024	A	**PFOS 6.5.1** • The `generate csr` command has been enhanced to support: ◦ wildcards for the `common-name` option ◦ a `san` option (Subject Alternative Name)
April 2024	A	**PFOS 6.5.0** • Prior to 6.5.0, pStack+ used L2GRE for implementing pStack+ tunnels. For 6.5.0 and later, to expand pStack+ support on newer PFS platforms, PFOS now supports VxLAN for implementing pStack+ tunnels instead of L2GRE. Due to the transport change from L2GRE to VxLAN: ◦ **The pStack version in PFOS 6.5.0 has been updated to version 30.6; pStack+ links will not be compatible between PFS devices running pStack version 30.6 and previous versions. Refer to "pfsMesh pStack Protocol Requirements" in the PFOS User Guide for additional pfsMesh compatibility details.** ◦ pStack+ uses a range of 8388608 to 16777215 internally for VNIDs for VXLAN tunnels; therefore, when a PFS device has at least one pStack-plus port configured, the maximum value for VNIDs for user-configured VXLAN tunnels and VXLAN stripping is 8388607. • A new `tx-laser` option for the `interface` command enables users to disable the transceiver transmitter on PFS 5000/7000 ports. • PFOS now supports Port Mirroring and Packet Slicing on PFS 7000 devices. The following commands support these features: ◦ `mirror-session` ◦ `map mirror-session` ◦ `feature slicing` ◦ `feature slicing-offset` • PFOS has been enhanced to provide more detailed PFS 5000/7000 power usage: ◦ The `show power supply` command has been enhanced to display more information. ◦ New `show energy-consumption` command ◦ New `show power-consumption` command • PFOS provides a new option `source-port-vlan-forwarding` for the Simple Tool Chain mode. **Documentation Updates** • Removed all references to PFS 5130-128X.

1 About This Document

This document describes the command line interface (CLI) of the NETSCOUT SYSTEMS, INC. (NETSCOUT®) Packet Flow Operating Software (PFOS).

Audience

This guide is intended for network administrators who are responsible for provisioning and monitoring network traffic, assuming understanding of network principles and configurations, as well as programming knowledge that relates to using the CLI of PFOS. This includes familiarity with networking and routing concepts.

Related Documentation

The following documents provide additional information about PFOS. All of the documents are downloadable at my.netscout.com.

- **PFOS 6.x User Guide:** Describes the PFOS features and explains how to set up and manage the system using the Web UI.
- **PFOS 6.x NETCONF XML API Reference Guide:** Describes the NETCONF XML application programing interface (API).

Additionally, PFOS RESTCONF API online documentation can be accessed from the Help menu in the Web UI. Refer to Management Interfaces for details.

For product warranty information, go to my.netscout.com.

Applicable Hardware Systems

PFOS on NETSCOUT Hardware

PFOS 6.x runs on the following NETSCOUT and VSS Monitoring hardware:

- nGenius® PFS 5000 Series packet flow switches
- nGenius® PFS 6000 Series packet flow switches
- nGenius® PFS 7000 Series packet flow switches
- VB6000 Network Packet Broker

The VSS VB6000 network packet broker is functionally identical to the NETSCOUT PFS 6010 packet flow switch and differs only in physical appearance.

For information on these systems and specific requirements, refer to the release notes, product briefs, datasheets, hardware installation guides, and quick connection guides for each system. These documents are downloadable at my.netscout.com.

PFOS on Certified Hardware

PFOS 6.x runs on Certified hardware available from NETSCOUT resellers. Refer to the *PFOS 6.x User Guide* for licensing details. For more information on Certified hardware, contact your NETSCOUT representative.

PFOS on Third-Party Qualified Hardware

PFOS 6.x also runs on Qualified hardware that meets NETSCOUT's specifications available from various switch vendors as PFS 5000 Series and PFS 7000 Series. The PFS 7000 Series is the same hardware as the PFS 5000 series with a PFS 7000 license installed to support additional feature functionality. Refer to the *PFOS 6.x User Guide* for details about licensing and also limitations and configuration considerations for specific PFS models.

Vendor Model	NETSCOUT Model Numbers	
	PFS 5000 Series	**PFS 7000 Series**
Edgecore Networks AS5812-54X	PFS 5010 PFS 5010-16X[1]	PFS 7010
Edgecore Networks AS7712-32X	PFS 5100	PFS 7100
Edgecore Networks AS7312-54XS	PFS 5110	PFS 7110
Edgecore Networks AS7816-64X	PFS 5120	PFS 7120
Edgecore Networks AS7726-32X	PFS 5030-32X	PFS 7030-32X
Edgecore Networks PFS AS9726-32DB	PFS 5040-32D	PFS 7040-32D
Edgecore Networks AS5835-54X	PFS 5030-54X	PFS 7030-54X
Dell S5048-ON	PFS 5111	PFS 7111
Dell Z9100-ON	PFS 5101	PFS 7101
Dell Z9264F-ON	PFS 5121-64X	PFS 7121-64X
Dell S5232F-ON	PFS 5031-32X	PFS 7031-32X
Dell S5248F-ON	PFS 5031-56X	PFS 7031-56X
Dell Z9432F-ON	PFS 5041-32D	PFS 7041-32D

Refer to the *PFOS Installation Guide for Qualified PFS Devices* for PFOS installation instructions for Qualified hardware. For more information about supported third-party qualified hardware, contact your NETSCOUT representative.

Related NETSCOUT Products

- Packet Flow eXtender (PFX) is a software application enabling expert packet conditioning for service assurance and cybersecurity monitoring. The solution is built on the NETSCOUT InfiniStreamNG platform and framework leveraging patented technologies. As part of the nGenius® Packet Flow System portfolio, PFX integrates with NETSCOUT’s broad set of packet broker products to enable expert-level capabilities, such as NetFlow generation and IP tunnel termination. The PFX application runs on multiple InfiniStreamNG hardware appliances and on several x86 server platforms, providing scalability on demand in a cost-effective manner.
- nGenius PFS Fabric Manager is a central management pane of glass that enables administrators to easily configure, deploy, and troubleshoot monitoring networks consisting of the nGenius 5000/7000 and 6000 series packet flow switches. It provides an intuitive, drag-and-drop configuration with powerful but simple-to-use workflows that cover the three major areas, or lifecycles, of a packet flow switch system: configuration, deployment, and monitoring.

For more information about PFX and PFS Fabric Manager, contact your NETSCOUT representative.

2 Introduction

This chapter explains how to access and use the PFOS command line interface (CLI).

Management Interfaces

The following interfaces are available to manage systems that run PFOS:

- **CLI:** Command-based user interface, described in this guide.
- **Web UI:** Web user interface, described in the PFOS User Guide.
- **NETCONF XML API:** An IETF-standard XML-based API to PFOS, described in the *PFOS 6.x NETCONF XML API Reference Guide* for details.
- **RESTCONF API:** An IETF-standard REST API to PFOS. You can access documentation for the RESTCONF API from the Web UI Help Menu.

Accessing the CLI

Access the PFOS CLI through the serial console, over Ethernet using SSH, or by clicking the CLI button in the Web UI.

Serial console access

Use the following settings:

- Data Rate:
  - PFS 5000/7000 Series: 115200 bps
  - PFS 6000 Series: 38400 bps
- Parity: None
- Data bits: 8
- Stop bits: 1
- Flow control: No flow control
- Terminal keyboard: VT100+

SSH

Use the following command.

```
ssh { hostname | ip_addr }
```

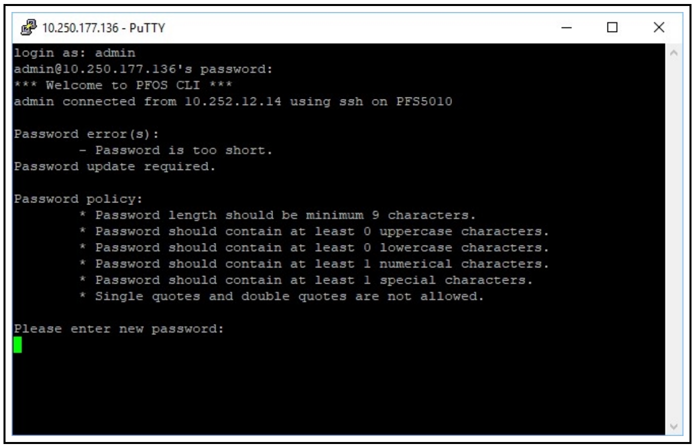
When connecting, log in using your user name and password.

```
Login: username
Password: password
PFOS#
```

PFOS enforces system-wide password policies which include password expiration and minimum password length and character requirements. If a user's password has expired or is not compliant with the current password policy, the user is prompted to update it on the next login.

Note: PFOS does not perform a password compliant check in the following scenarios:

- User login to NETCONF XML API interface. A user can continue to login successfully using a non-compliant password.
- Imported users. User information imported through File Management that contains non-compliant passwords is not checked. When the imported users attempt to login to the CLI or Web UI, they will be prompted to update their passwords.



```
login as: admin
admin@10.250.177.136's password:
*** Welcome to PFOS CLI ***
admin connected from 10.252.12.14 using ssh on PFS5010

Password error(s):
        - Password is too short.
Password update required.

Password policy:
        * Password length should be minimum 9 characters.
        * Password should contain at least 0 uppercase characters.
        * Password should contain at least 0 lowercase characters.
        * Password should contain at least 1 numerical characters.
        * Password should contain at least 1 special characters.
        * Single quotes and double quotes are not allowed.

Please enter new password:
```

Logging in with an SSH public key

If the administrator has uploaded an SSH public key to PFOS, then users can log in with ssh from any system whose public key is in the file that has been uploaded to PFOS.

Only the RSA type of SSH public keys is supported. The SSH public key file should have at least one sshpubkey of type RSA; otherwise, file upload will be rejected.

The SSH public key file can have keys from multiple systems, but only one SSH public key file can be present on PFOS at any one time. Before uploading a new SSH public key file, you must first delete any existing file.

On PFS 6010 systems with multiple management modules, uploaded SSH public key files are copied to both modules.

For details on managing SSH public key files in the CLI, refer to these commands: copy, delete, show sshpubkey.

Change Default Password

When you log in to PFOS for the first time, either through the CLI or the Web UI, PFOS will prompt you to change the admin user's default password. The new password must be different from the existing password.

License agreement

When you log in to PFOS for the first time, either through the CLI or the Web UI, PFOS displays an End User License Agreement. In the CLI, you can use the up, down, left, and right arrow keys to scroll horizontally or vertically as desired to read the agreement. After reading the agreement, press `A` to accept or `D` to decline.

To use PFOS, you must accept the license agreement. After an administrator installs a new release of PFOS, a user with Admin or File Management privileges (such as `admin`) must again review and accept the license agreement before continuing to use PFOS. This user can be one that is either defined locally on PFOS or remotely (such as through RADIUS or TACACS), as long as that user is first granted the Admin role in PFOS.

CLI Features

Command Results

If you run a CLI command to show information, the information is displayed on the screen.

If you run a configuration command, a prompt is returned if the command completes successfully.

Example show command with output:

```
PFOS# show system
system serial number 14100443
system productID 2301
system disk-usage install 10%
system disk-usage activelog 20%
PFOS#
```

Example configuration command:

```
PFOS(config)# logging host 1.2.3.4
PFOS(config)#
```

Command Help

Type `help` to see the list of commands and descriptions for the current mode.

```
PFOS(config)# help
Possible commands:
abort Abort configuration session
```

```
app-lib Application libraries
authentication Authentication related settings, like order, etc.
clear Clear parameter messages
delete Delete a file
...
PFOS(config)#
```

Using Special Characters in CLI Commands

You can use special characters as input for parameters for any CLI command by enclosing the input in double quotes. Refer to the following examples for the `copy` and `username` commands:

Copy Command

```
PFS5010-115# copy "scp://smith:abcpfs!@10.250.177.115:1234:/root/vxos_
PFS5k_5.6.1.23-4319c6bb" software:
Are you sure? [no,yes] yes
```

Username Command

```
PFOS(config)# username ssmith password "asdf!" confirm-password "asdf!"
```

CLI Command Modes

PFOS has the following CLI command modes:

- Operational Mode
- Configuration Mode
- Configuration Submodes

Operational Mode

The Operational command mode is the default mode after logging in.

In this mode the user can show system information, operational data, and CLI session configuration and allows the user to perform some basic tasks.

When in operational mode the show commands will show operational data for each entity. It should be noted that this is not the same as configuration. For example, to show operational information about a traffic map named test:

```
PFOS# show map test
map test
map_status state enable
ERROR
INGRESS CODE MGID
----------------------
1-1 None 0
pstack-paths status None
```

To show the current (running) configuration while in the Operational mode use the show running-config [link to that command] command. For example to show the configuration of a traffic map named test:

```
PFOS# show running-config map test
map test
type Monitor
mode Basic
filter unfiltered
input_ports [ 1-1 ]
output_ports [ 1-10 ]
action Forward
!
```

To return to Operational mode from Configuration mode, type `exit`.

The CLI prompt will not show any modifiers in Operational mode:

```
PFOS#
```

Operational Mode Commands

Type `?` to see the list of possible completions for the current mode.

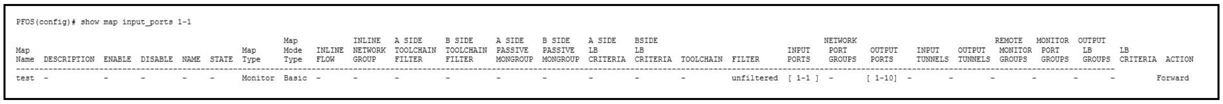
```
PFOS# ?
Possible completions:

  abort          Abort ongoing long action of defined type via abort/ESC
  clear          Clear parameter
  clock          System date and time
  compare        Compare configuration
  config         Manipulate software configuration information
  copy           Copy from one file to another

   ...
   PFOS#
```

Configuration Mode

The Configuration command mode is entered by typing `config` in Operational mode.

In this mode the user can make changes to or show the existing configuration.

For example, to show the configuration of traffic maps using input port 1-1 in Configuration mode:



```
PFOS(config)# show map input_ports 1-1

                                                Map             INLINE   A SIDE     B SIDE     A SIDE    B SIDE    A SIDE    BSIDE                                            NETWORK                                    REMOTE   MONITOR  OUTPUT
Map                                     Map     Mode   INLINE   NETWORK  TOOLCHAIN  TOOLCHAIN  PASSIVE   PASSIVE   LB        LB                                   INPUT        PORT    OUTPUT    INPUT    OUTPUT    MONITOR  PORT      LB     LB
Name  DESCRIPTION  ENABLE  DISABLE  NAME  STATE  Type    Type   FLOW     GROUP    FILTER     FILTER     MONGROUP  MONGROUP  CRITERIA  CRITERIA  TOOLCHAIN  FILTER      PORTS        GROUPS  PORTS     TUNNELS  TUNNELS   GROUPS   GROUPS    GROUPS CRITERIA  ACTION
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
test  -            -       -        -     -      Monitor Basic  -        -        -          -          -         -         -         -         -          unfiltered  [ 1-1 ]  -       [ 1-10]   -        -         -        -         -      -               Forward
```

The prompt will show when the CLI is in Configuration mode:

```
PFOS(config)#
```

Configuration Mode Commands

Type `?` to see the list of possible completions for the current mode.

```
PFOS(config)# ?
Possible completions:

  abort                 Abort configuration session
  access-policy         User access control policy settings
  app-lib               Application libraries
  authentication        Authentication related settings, like order, etc.
  clear                 Clear parameter
  clock                 System date and time
  copy                  Copy from one file to another
  ...
```

Separating Commands with Semicolons

You can use a semicolon (;) to separate multiple commands. PFOS executes the commands sequentially in one transaction, running each command at the completion of the previous command.

In the following example, the tunnel feature is enabled, a tunnel termination group called `ep1` is created and then assigned to port 4-6 on interface 4.

```
PFOS(config)# feature tunnel enable; app-lib tunnel-termination ep1 ip [
10.10.10.1 10.10.10.2]; interface 4 eth 4-6 tunnel-termination enable
tunnel-termination-name ep1
```

Configuration Submodes

From Configuration mode, issuing configuration commands enters command submodes.

Use the `top` command to return to the top level Configuration mode prompt.

From Configuration mode, issue a configuration command to enter a submode. If you issue a command with only some of the required parameters, the CLI prompts you for the additional information and then enters the submode.

An example showing the prompt when configuring port 10-9:

```
PFOS(config-eth-10-9)#
```

The following example shows the CLI prompting for required parameters:

```
PFOS(config)# username def
Value for 'password' (<AES encrypted
string, min: 5 units>): 123
Value for 'confirm-password' (<AES
encrypted string, min: 5 units>): 123
PFOS(config-username-def)#
```

CLI Output Modifiers

It is possible to process the output from a command using an output redirect. This is done using the | (pipe) character. The commands can be chained to achieve more complex processing.

In PFOS CLI, the commands are called - append, count, exclude (except), display annotations, display tags, hide annotations, hide tags, begin (find), include (match), linnum, match-all, match-any, more, nomore, notab (auto-rendered show commands only), repeat (auto-rendered show commands only), save, tab (show commands only) and until. For example:

```
PFOS(config)# show running-config | ?
Possible completions:
annotation    Show only statements whose annotation matches a pattern
append        Append output text to a file
begin         Begin with the line that matches
count         Count the number of lines in the output
details       Display commit progress
display       Display options
exclude       Exclude lines that match
extended      Display referring entries
hide          Hide display options
include       Include lines that match
linnum        Enumerate lines in the output
match-all     All selected filters must match
match-any     At least one filter must match
more          Paginate output
nomore        Suppress pagination
save          Save output text to a file
select        Select additional columns
sort-by       Select sorting indices
tab           Enforce table output
tags          Show only statements whose tags matches a pattern
until         End with the line that matches
```

The show annotations/tags and hide annotations/tags pipe targets are only available when viewing the configuration, and only if attributes have been enabled in the confd.conf file.

Sort the Output

The sort-by target makes it possible for the CLI user to control in which order instances should be displayed, and can be used when the path points to a list. The argument to sort-by can either be a secondary index or an arbitrary set of leafs in the list. If a secondary index is given as an argument, the table will be sorted in the order defined by the secondary index. If a set of leafs is given as an argument, the table will be sorted in the order in which the leafs are entered. For example:

```
PFOS(config)# show configuration server | sort-by port ip | tab
NAME    IP         PORT   DESCRIPTION
-----------------------------------
1      1.1.1.1    1010   -
7      1.1.1.17   1020   -
```

```
10     1.1.1.11   1040   -
3      1.1.1.3    1070   -
6      1.1.1.4    1070   -
5      1.1.1.5    1070   -
4      1.1.1.7    1070   -
8      1.1.1.8    1070   -
9      1.1.1.9    1070   -
11     1.1.1.10   1070   -
2      1.1.1.12   1070   -
[ok][2020-08-31 13:49:44]
```

Count the Number of Lines in the Output

This redirect target counts the number of lines in the output. For example:

```
PFOS(config)# show configuration | count
[ok][2020-08-31 13:49:44]
Count: 99 lines
```

```
PFOS(config)# show configuration aaa | count
[ok][2020-08-31 13:50:12]
Count: 90 lines
```

Search for a String in the Output

The include target is used to only include lines matching a regular expression. For example:

```
PFOS(config)# show configuration aaa | include{
aaa {
authentication {
users {
user admin {
user oper {
user private {
user public {
groups {
group admin {
group oper {
authorization {
cmdrules {
cmdrule 1 {
cmdrule 2 {
cmdrule 3 {
cmdrule 150 {
datarules {
datarule 101 {
datarule 203 {
```

In the example above only lines containing { are shown. Similarly lines not containing a regular expression can be included. This is done using the exclude target. For example:

```
PFOS(config)# show configuration aaa authentication | exclude {
uid 1000;
gid 100;
password $1$fB$0w68PmacQ4VmE3/M3nK3Ug==;
ssh_keydir /var/confd/homes/admin/.ssh;
homedir /var/confd/homes/admin;
}
uid 1000;
gid 100;
password $1$S6$brGZW9wSDifHoU7Rf5KSHA==;
ssh_keydir /var/confd/homes/oper/.ssh;
homedir /var/confd/homes/oper;
}
uid 1000;
gid 100;
password $1$L4$YcCoIivO4mrzoj8vCrEjlw==;
ssh_keydir /var/confd/homes/private/.ssh;
homedir /var/confd/homes/private;
}
uid 1000;
gid 100;
password $1$Ft$9zTEc79NWFE0E8v7I2RxVQ==;
ssh_keydir /var/confd/homes/public/.ssh;
homedir /var/confd/homes/public;
}
}
users "admin private";
}
users "oper public";
}
}
}
```

It is also possible to display the output starting at the first match of a regular expression, using the begin target. For example:

```
PFOS(config)# show configuration aaa authentication users | begin private
user private {
uid 1019;
gid 1013;
password $1$AO$hbQEgdGQLzlWhX/1FNL5f.;
ssh_keydir /var/confd/homes/private/.ssh;
homedir /var/confd/homes/private;
}
user public {
uid 1019;
gid 1013;
password $1$Kh$0Lor2g1yrSQ7MYDLxFr9h0;
ssh_keydir /var/confd/homes/public/.ssh;
homedir /var/confd/homes/public;
}
```

Output can also be ended when a line matches a regular expression. This is done with the until target. For example:

```
PFOS(config)# show configuration aaa authentication users | find private | until public
user private {
uid 1019;
gid 1013;
password $1$AO$hbQEgdGQLzlWhX/1FNL5f.;
ssh_keydir /var/confd/homes/private/.ssh;
homedir /var/confd/homes/private;
}
user public {
```

It is also possible to filter the output by using a sequence of select statements followed by match-any or match-any. Consider the configuration:

```
PFOS(config)# show configuration servers server
server a {
ip 1.2.3.4;
port 23;
}
server b {
ip 2.3.4.5;
port 24;
}
server c {
ip 3.4.5.6;
port 25;
}
```

If we were to show all servers that has either ip 1.2.3.4 *or* port 24, this can be done by using select statements, like so:

```
PFOS(config)# show configuration servers server | select ip 1.2.3.4 | select port 24 server a
{
ip 1.2.3.4;
port 23;
}
server b {
ip 2.3.4.5;
port 24;
}
```

whereas a match-all filtering would in this case result in

```
PFOS(config)# show configuration servers server | select ip 1.2.3.4 | select port 24
```

```
No entries found.
```

as there are no servers that have both ip 1.2.3.4 *and* port 24.

Regular Expressions

The regular expressions is a subset of the regular expressions found in egrep and in the AWK programming language. Some common operators are:

.	Matches any character.
^	Matches the beginning of a string.
$	Matches the end of a string.
[abc...]	Character class, which matches any of the characters abc... Character ranges are specified by a pair of characters separated by a -.
[^abc...]	Negated character class, which matches any character except abc....
r1 | r2	Alternation. It matches either r1 or r2.
r1r2	Concatenation. It matches r1 and then r2.
r+	Matches one or more rs.
r*	Matches zero or more rs.
r?	Matches zero or one rs.
(r)	Grouping. It matches r.

For example, to only display uid and gid you can do the following:

```
PFOS(config)# show configuration | match "(uid)|(gid)"
uid 1000;
gid 100;
uid 1000;
gid 100;
uid 1000;
gid 100;
uid 1000;
gid 100;
```

Display Line Numbers

The linnum target causes a line number to be displayed at the beginning of each line in the display.

```
PFOS(config)# show configuration | match "(uid)|(gid)" | linnum
1: uid 1019;
2: gid 1013;
3: uid 1019;
4: gid 1013;
5: uid 1019;
6: gid 1013;
7: uid 1019;
8: gid 1013;
```

Command Completion

The CLI supports command completion. Press the spacebar or tab key after typing some characters to complete the command, or to display the matching options if the characters do not uniquely identify the command.

In this example, typing c does not uniquely identify a command, so the matching options are displayed.

```
PFOS# c (tab)
Possible completions:
clear Clear parameter
clock System date and time
config Manipulate software configuration information
copy Copy from one file to another
```

Typing an additional characters causes a unique match, and the command is automatically completed.

```
PFOS# cop (tab)
PFOS# copy
```

Keyboard Shortcuts

The following table lists useful keyboard shortcuts for the CLI:

Shortcut	Description
Up and down arrows	Scroll up or down the list of previously-entered commands.
Tab or Spacebar	Complete the next portion of the current command.
Ctrl-B or Left Arrow	Move the cursor back one character.
Ctrl-C	Interrupt the current command and return to the prompt for the previous mode (if in Configuration mode or submode). If in Operational mode, returns to the Operational mode prompt.
Esc-B or Alt-B	Move the cursor back one word.
Ctrl-F or Right Arrow	Move the cursor forward one character.
Esc-F or Alt-F	Move the cursor forward one word.
Ctrl-A or Home	Move the cursor to the beginning of the command line.
Ctrl-E or End	Move the cursor to the end of the command line.
Ctrl-H, Delete, or Backspace	Delete the character before the cursor.
Ctrl-D	Delete the character following the cursor.
Ctrl-K	Delete all characters from the cursor to the end of the line.
Ctrl-U or Ctrl-X	Delete the whole line.
Ctrl-W, Esc-Backspace, or Alt-Backspace	Delete the word before the cursor.
Esc-D or Alt-D	Delete the word after the cursor.
Ctrl-Y	Insert the most recently deleted text at the cursor.

Shortcut	Description
Ctrl-P or Up Arrow	Scroll backward through the command history.
Ctrl-N or Down Arrow	Scroll forward through the command history.
Ctrl-R	Search the command history in reverse order.

Scripting

You can use an SSH scripting application to create scripts of multiple CLI commands to run at one time.

Syntax Conventions

The following conventions are used in this guide:

<table>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>Italic</td><td>Variables for which you need to substitute actual values when you enter a command.
Example:
<code>logging host <i>host</i></code></td></tr>
<tr><td>Square brackets</td><td>Indicates optional variables or keywords.
Example:
<code>filter filter-name expression string [type traffic]</code></td></tr>
<tr><td>Curly brackets</td><td>Indicates a list of required variables or keywords from which to select.
Example:
<code>role role-name description value rule rule-name feature value access { create | delete | exec | read | update } context { all | cli | webui | netconf }</code></td></tr>
<tr><td>Pipe symbol |</td><td>Indicates exclusive choices (specify only one of the options).
Example:
<code>interface card slot eth slot-port class {Monitor | Service | Span | Span-Monitor} link_state {auto | force-down | force-up} name port-name vlan_tagging {enable | disable}</code></td></tr>
<tr><td>Multiple values</td><td>Syntax for specifying multiple values depends on the command.
Examples:
Specifying multiple ports. Use a comma-separated list enclosed in square brackets (with spaces as shown).
<code>PFOS(config)# load-balance lbg4 ports [8-3 8-4 9-5] failover_action Drop</code>
Specifying multiple access options for roles. Use a comma-separated list with no spaces.
<code>PFOS(config)# role sys-role rule sys1 feature System context CLI access create,read,delete</code></td></tr>
</table>

3 Configuration Tasks

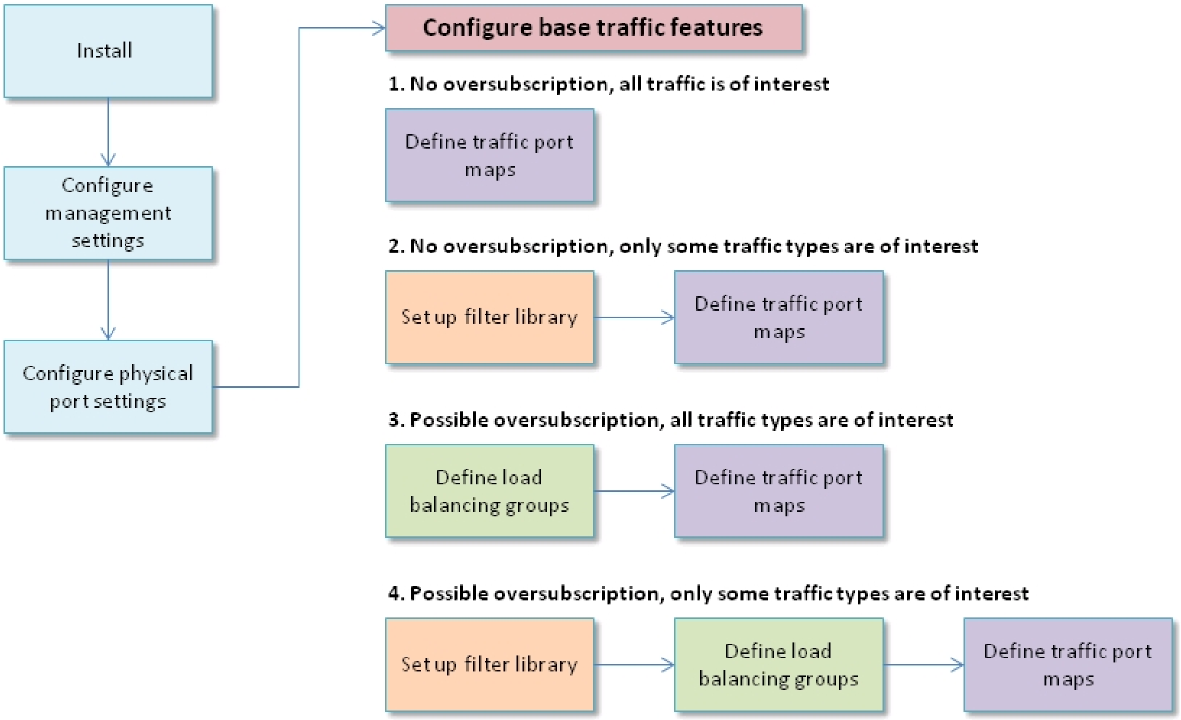
This chapter provides example command sequences for base feature configuration tasks and provides CLI configuration examples. See the individual command reference pages for additional details.

Configuration Task Flow

Follow this task flow to set up and configure PFOS following installation and initial setup. See the figure on the next page.

1. Configure system settings, including system, network, and time settings. See Configure System Settings.
2. Configure user accounts and authentication for accessing PFOS. See Configure Access Control.
3. Configure physical port settings. See Configure Ports.
4. Configure filtering rules, as needed. See Define Filtering Rules.
5. Configure load balancing criteria and groups, as needed. See Define Load Balance Criteria, Groups, and Traffic Maps.
6. Set up traffic maps. See Define Traffic Maps.

After these steps are complete, traffic is automatically forwarded through the system according to the specified conditions.


Install
Configure management settings
Configure physical port settings
Configure base traffic features
1. No oversubscription, all traffic is of interest
Define traffic port maps
2. No oversubscription, only some traffic types are of interest
Set up filter library
Define traffic port maps
3. Possible oversubscription, all traffic types are of interest
Define load balancing groups
Define traffic port maps
4. Possible oversubscription, only some traffic types are of interest
Set up filter library
Define load balancing groups
Define traffic port maps

Configuration Examples

Configure System Settings

The following example commands configure global system settings.

System name, contact, and location

```
PFOS(config)# system name vb6000_b1 location building1 contact
ssmith@example.com
```

Network settings

```
PFOS(config)# interface mgmt 0 ip address 192.168.20.12/24 dns
192.168.10.100 gateway 192.168.20.1
```

Syslog servers

The following command specifies a syslog server using an IPv6 address.

```
PFOS(config)# logging host FE80::0202:B3FF:FE1E:8329
```

System clock

Set time manually or using NTP.

Manual setting:

```
PFOS(config)# clock set 2015-03-09T09:40:45
set current time = Mon Mar 9 16:40:45 UTC 2015
```

NTP setting:

```
PFOS(config)# ntp time-server [ 1.2.3.4 1.2.3.6 ]
PFOS(config)#
```

Configure Access Control

The following sequence shows the current users and role assignments.

Note: Users not associated with a role will not have permission to read, write, or execute any commands after logging in. Local users without a role assigned to them only have permission to change their local password after login.

```
PFOS# show running-config username
username admin
 password         $4$wIo7Yd068FRwhYYI0d4IDw==
 confirm-password  $4$wIo7Yd068FRwhYYI0d4IDw==
 role             admin
!

PFOS# show running-config role
role admin
 description "admin role"
 rule all
  feature All
  access  create,read,update,delete,exec
  context all
 !
!role role_time_source
 description "role time source"
 rule rule_time_source
  feature "Timing Source"
  access  create,read,update,delete,exec
  context all
 !
!
role role_file_management
 description "file management role"
 rule file_management_rule
  feature "File Management"
  access  create,read,update,delete,exec
  context all
 !
!
```

The following sequence sets up two user roles, role_file_management and role_time_source, with read, create, and delete access to the system features of the CLI.

```
PFOS# config
Entering configuration mode terminal
PFOS(config)# role role_file_management rule sys1 feature System context CLI access
create,read,delete

PFOS(config)# role role_time_source rule sys1 feature System context CLI access
create,read,delete
PFOS(config-rule-sys1)# top
```

The sequence then creates a user, abc, with those roles. In this example, the password is not specified in the `username` command, so the system prompts for the password.

```
PFOS(config)# username abc role [ role_file_management role_time_source ]
Value for 'password' (<AES encrypted string, min: 5 units>): 12345
Value for 'confirm-password' (<AES encrypted string, min: 5 units>): 12345
PFOS(config-username-abc)#
```

Configure Ports

The following command sequences show examples for defining port classes and defining Monitor port and Span port VLAN tagging.

Configure port classes:

```
PFOS(config)# interface 7 eth 7-1 class Span
PFOS(config-eth-7-1)# top
PFOS(config)# interface 10 eth 10-9 class Span
PFOS(config-eth-10-9)# top
PFOS(config)# interface 10 eth 10-6 class Monitor
PFOS(config-eth-10-6)# top
PFOS(config)# interface 10 eth 10-7 class Monitor
PFOS(config-eth-10-7)# top
PFOS(config)# interface 10 eth 10-8 class Monitor
PFOS(config-eth-10-8)# top
PFOS(config)#
```

Monitor port VLAN tagging:

```
PFOS(config)# interface 1 eth 1-26 class Monitor vlan_tagging enable
PFOS(config-eth-1-26)#
```

Span port VLAN tag selection:

```
PFOS(config)# interface 1 eth 1-16 class Span vid 101
PFOS(config-eth-1-16)#
```

Define Filtering Rules

See the “Base Features and Tasks” chapter in the *PFOS User Guide* for information on the syntax for creating filter expressions.

The following filter matches HTTP request packets:

```
PFOS(config)# filter HTTP expression "ip protocol 6 and tcp destination
port 80"
```

```
PFOS(config-filter-HTTP)# top
PFOS(config)#
```

The following filter monitors a particular connection, conversation, or session between two nodes (1.2.3.4 and 5.6.7.8):

```
PFOS(config)# filter nodeconversation expression "(ip source 1.2.3.4 and
ip destination 5.6.7.8) or (ip source 5.6.7.8 and ip destination
1.2.3.4)"
PFOS(config-filter-nodeconversation)# top
PFOS(config)#
```

Define Load Balance Criteria, Groups, and Traffic Maps

The following example commands show how to set up load balancing based on the port configurations defined in Configure Ports. The example defines Layer 2 load balance criteria with destination and source MAC address and creates a load balance group with the rebalancing failover action.

The following command creates Layer 2 load balance criteria, L2, with destination and source MAC address.

```
PFOS(config)# lb-criteria L2 layer2 enable layer2_header_keys
Destination_MAC_address,Source_MAC_address
PFOS(config-lb-criteria-L2)# top
PFOS(config)#
```

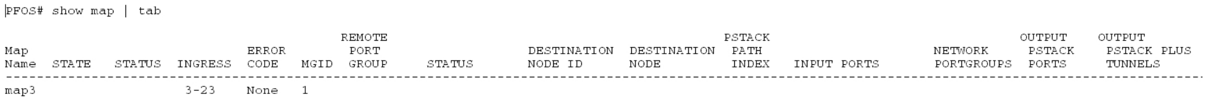
The following command creates a load balance group, lbg1, with ports 10-6, 10-7, and 10-8 and rebalancing as the failover action.

```
PFOS(config)# load-balance lbg1 failover_action Rebalance type Monitor
ports [ 10-6 10-7 10-8 ]
PFOS(config-load-balance-lbg1)# top
PFOS(config)#
```

Define Traffic Maps

The following command creates a map, map3, that maps the traffic on input port 3-23 to output port 3-24 with no filtering or load balancing applied. The show command shows the results.

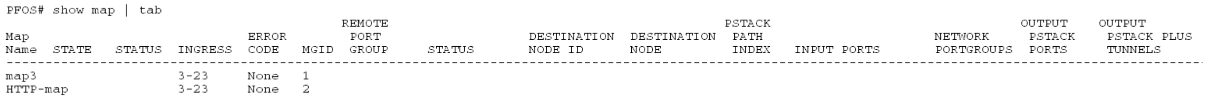
```
PFOS(config)# map map3 filter unfiltered input_ports 3-23 output_ports 3-24

PFOS(config-map-map3)# top

PFOS(config)# exit
```



```
PFOS# show map | tab

                                        REMOTE                                                PSTACK                                      OUTPUT    OUTPUT
Map                             ERROR          PORT                     DESTINATION  DESTINATION  PATH                          NETWORK     PSTACK    PSTACK PLUS
Name   STATE    STATUS  INGRESS CODE   MGID GROUP      STATUS           NODE ID      NODE         INDEX   INPUT PORTS           PORTGROUPS  PORTS     TUNNELS
----------------------------------------------------------------------------------------------------------------------------------------------------------------------
map3                    3-23    None   1
```

The following command creates a map, HTTP-map, that applies the HTTP filter defined in Define Filtering Rules to traffic sent from input port 3-23 to output ports 3-24 and 3-25 (as configured in Configure Ports) with no load balancing applies. The `show` commands show the results of the filter and map configuration.

```
PFOS(config)# map HTTP-map filter HTTP input_ports 3-23 output_ports [ 3-24 3-25 ]
PFOS(config-map-HTTP-map)# exit
PFOS(config)# exit
PFOS# show filter

            USED
            IN
NAME        MAPS  MAP NAME  NAME
----------------------------------
HTTP        1     HTTP-map
nonmatch    0
unfiltered  1     map3

PFOS# show running-config filter HTTP
filter HTTP
 type       traffic
 expression "IP Protocol 6 and ( TCP Dest Port 80-81 or TCP Source Port 80-81 ) "
!
```



```
PFOS# show map | tab
                                           REMOTE                                            PSTACK                            OUTPUT   OUTPUT
Map                              ERROR      PORT                     DESTINATION  DESTINATION PATH                   NETWORK    PSTACK   PSTACK PLUS
Name  STATE     STATUS  INGRESS  CODE MGID  GROUP      STATUS        NODE ID      NODE        INDEX  INPUT PORTS     PORTGROUPS PORTS    TUNNELS
----------------------------------------------------------------------------------------------------------------------------------------------------
map3                    3-23     None  1
HTTP-map                3-23     None  2
```

```
PFOS# show running-config map
map map3
 type         Monitor
 mode         Basic
 filter       unfiltered
 input_ports  [ 3-23 ]
 output_ports [ 3-24 ]
 action       Forward
!
map HTTP-map
 type         Monitor
 mode         Basic
 filter       HTTP
 input_ports  [ 3-23 ]
 output_ports [ 3-24 3-25 ]
 action       Forward
!

PFOS#
```

The following command creates a traffic map that takes traffic entering on port 10-9 and applies the load balance group and load balance criteria defined in Define Load Balance Criteria, Groups, and Traffic Maps.

```
PFOS(config)# map map1 filter unfiltered input_ports 10-9 output_lb_
groups lbg1 lb_criteria L2
```

```
PFOS(config-map-map1)# top
PFOS(config)#
```

The following command takes the previous example and adds the HTTP filter defined in Define Filtering Rules.

```
PFOS(config)# map map1 filter HTTP input_ports 10-9 output_lb_groups
lbg1 lb_criteria L2
PFOS(config-map-map1)# top
PFOS(config)#
```

Define Traffic Map for Port Aggregation

The following command sequence configures ports and then creates a traffic map that aggregates span ports 8-6 and 8-7 to the output port 8-12, with no filtering or load balancing applied.

```
PFOS(config)# interface 8 eth 8-6 class Span
PFOS(config-eth-8-6)# top
PFOS(config)# interface 8 eth 8-7 class Span
PFOS(config-eth-8-7)# top
PFOS(config)# interface 8 eth 8-12 class Monitor
PFOS(config-eth-8-12)# top
PFOS(config)# map span filter unfiltered input_ports [ 8-6 8-7 ] output_
ports 8-12
PFOS(config-map-span)#
```

Define Traffic Map for Port Replication

The following command sequence configures ports and then replicates the traffic coming in on port 1-1 to output ports 1-18 through 1-20, with no filtering or load balancing applied.

```
PFOS(config)# interface 1 eth 1-1 class Span
PFOS(config-eth-1-1)# top
PFOS(config)# interface 1 eth 1-18 class Monitor
PFOS(config-eth-1-18)# top
PFOS(config)# interface 1 eth 1-19 class Monitor
PFOS(config-eth-1-19)# top
PFOS(config)# interface 1 eth 1-20 class Monitor
PFOS(config-eth-1-20)# top
PFOS(config)# map serv1 filter unfiltered input_ports 1-5 output_ports [
1-18 1-19 1-20 ] type Monitor
PFOS(config-map-serv1)# top
```

The following command sequence modifies the previous example to include service port mapping.

```
PFOS(config)# interface 1 eth 1-1 class Span
PFOS(config-eth-1-1)# top
PFOS(config)# interface 1 eth 1-5 class Service
PFOS(config-eth-1-5)# top
PFOS(config)# interface 1 eth 1-18 class Monitor
PFOS(config-eth-1-18)# top
PFOS(config)# interface 1 eth 1-19 class Monitor
PFOS(config-eth-1-19)# top
PFOS(config)# interface 1 eth 1-20 class Monitor
PFOS(config-eth-1-20)# top
PFOS(config)# map span1 filter unfiltered input_ports 1-1 output_ports
1-5
PFOS(config-map-span1)#
PFOS(config)# map serv1 filter unfiltered input_ports 1-5 output_ports [
1-18 1-19 1-20 ] type Monitor
PFOS(config-map-serv1)# top
PFOS(config)#
```

4 System Commands

This chapter contains reference pages for the following system commands, which include global system, network, and port settings for PFOS, user accounts, and SNMP.

Commands include:

- access-policy login ip-lockout
- access-policy login session-limit
- access-policy login user-lockout
- access-policy password expiration
- access-policy password minimum
- authentication order
- clock
- feature
- firewall rule
- gps
- interface
- interface dhcp
- interface gre
- interface ip
- interface mgmt
- interface vxlan
- ldap-server
- logging
- monitor_port_vlan
- move
- notification event
- ntp time-server
- passwd
- poweroff
- ptp
- radius-server
- redundancy
- role
- rollback
- snmp
- snmp-server
- system
- system-alarms
- system banner
- system notes
- tacacs-server
- tracelog
- username

access-policy login ip-lockout

PFOS detects multiple failures to log in, and blocks access to the system when a defined threshold is met. You can configure the number of failed login attempts that PFOS allows before the IP address is locked out. The new setting will take effect when the next login attempt occurs; existing sessions are not affected.

Note: This setting does not affect the current failed login count.

You can also disable the lockout feature so there is no limit to the number of failed IP login attempts.

For details about failed login attempts, refer to the ***PFOS 6.x User Guide***. See also show client-ip-lockout and access-policy login user-lockout.

Syntax

```
> access-policy login ip-lockout-failed-attempts-max <1..5>
> no access-policy login ip-lockout-failed-attempts-max

> access-policy login ip-lockout-disable
> no access-policy login ip-lockout-disable
```

Options

number	Specifies the number of failed IP login attempts PFOS allows before an IP is locked out (default is 5).

Mode

Configuration

Examples

Configure PFOS to allow 3 failed IP login attempts before locking out IP

```
PFOS(config)# access-policy login ip-lockout-failed-attempts-max 3
```

Disable the lockout feature so there is no limit to the number of failed IP login attempts

```
PFOS(config)# access-policy login ip-lockout-disable
```

access-policy login session-limit

You can enable this feature to limit the total number of concurrent PFOS sessions from 1-3 sessions per user (3 is default). Concurrent session counts are supported per user on the following interfaces (excluding API interface):

- Web UI via HTTP/HTTPS
- CLI via SSH

Syntax

```
access-policy login session-limit
no access-policy login session-limit

access-policy login session-limit session-limit-max number
no access-policy login session-limit-max
```

Options

number	Specifies the maximum number of concurrent PFOS sessions you want to limit per user (default is 3).

Mode

Configuration

Examples

Enable limitation

```
PFOS(config)# access-policy login session-limit
PFOS(config)# access-policy login session-limit session-limit-max 2
```

Disable limitation

```
PFOS(config)# no access-policy login session-limit
```

access-policy login user-lockout

PFOS detects multiple failures to log in, and blocks access to the system when a defined threshold is met. You can configure the following settings:

- The number of failed login attempts that PFOS allows before a user account is locked out. The new setting will take effect when the next login attempt occurs; existing sessions are not affected.

  Note: This setting does not affect the current failed login count.
- Disable the user lockout feature so there is no limit to the number of failed user login attempts.
- The number of minutes users are locked out after failed login attempts

For details about failed login attempts, refer to the ***PFOS 6.x User Guide***. See also access-policy login ip-lockout.

Syntax

```
> access-policy login user-lockout-failed-attempts-max <1..5> max number

> no access-policy login user-lockout-failed-attempts-max

> access-policy login user-lockout-disable
> no access-policy login user-lockout-disable

> access-policy login user-lockout-duration <minutes, 5 .. 60> duration
minutes
> no access-policy login user-lockout-duration
```

Options

max number	Specifies the number of failed user login attempts PFOS allows before a user is locked out (default is 5).
duration minutes	Specifies the number of minutes users are locked out after failed login attempts. Valid values are 5-60; 60 is the default.

Mode

Configuration

Examples

Configure PFOS to allow 3 failed user login attempts before locking out user

```
PFOS(config)# access-policy login user-lockout-failed-attempts-max 3
```

Disable the lockout feature so there is no limit to the number of failed user login attempts.

```
PFOS(config)# access-policy login user-lockout-disable
```

Modify the lockout duration to 30 minutes.

```
PFOS(config)# access-policy login user-lockout-duration 30
```

access-policy password expiration

Specify the number of days user passwords are valid before expiring.

To view the current password expiration interval, use `show running-config access-policy`.

To restore the current password expiration interval to the default of 9,999 days, use `no access-policy`.

Syntax

```
access-policy password expiration days
```

Options

`days`	Number of days before passwords must be changed. Valid values are integers from 1 to 9999. The default is 9,999 days (about 27.4 years).

Mode

Configuration

Examples

```
PFOS(config)# access-policy password expiration 90
PFOS(config)# abort
PFOS# show running-config access-policy
access-policy password expiration 90
PFOS# conf
PFOS(config)# no access-policy
PFOS(config)# abort
PFOS# show running-config access-policy
access-policy password expiration 9999
```

access-policy password minimum

Specify the minimum number of character types required in a user password. If a user's password is not compliant with the current password policy, the user is prompted to update it on the next login. Refer to `username` for details about configuring user accounts and passwords.

To view the current password minimum parameters, use `show running-config access-policy password minimum`.

To restore the current password minimum to the default values, use `no access-policy minimum`.

Syntax

```
access-policy password minimum parameter name size
```

Options

<table>
<tr><td rowspan="7">parameter name and size</td><td colspan="2">Name of the policy parameter to update and the minimum number of characters required for a user password. Valid values range from 0-128 for all parameters except length which has a minimum of 5).</td></tr>
<tr><td>length</td><td>Minimum password length (default is 5).</td></tr>
<tr><td>lowercase</td><td>Minimum number of lowercase letters required (default is 0).</td></tr>
<tr><td>special</td><td>Minimum number of special characters required (default is 0). Single quote (‘) and double quote (“) characters cannot be used as special characters as part of password string. To define special characters in CLI, the character needs to be surrounded by double quotes or preceded by a backslash (\) as an escape character (see username for details).</td></tr>
<tr><td>uppercase</td><td>Minimum number of uppercase letters required (default is 0).</td></tr>
<tr><td>numerical</td><td>Minimum number of numerical characters required (default is 0).</td></tr>
<tr><td>positions-changed</td><td>Minimum number of character *positions* within the new password which must be changed from the old password. Note that this setting does not require *character* changes, but character *position* changes. For example:
• If the current password is "abc1234" and positions-changed is set to 5, the new password "1234abc" is valid
• If the current password is "1234abc" and positions-changed is set to 2, the new password "1234abc56" is valid.</td></tr>
</table>

Mode

Configuration

Examples

```
PFOS(config)# access-policy password minimum length 10
PFOS(config)# access-policy password minimum uppercase 1
PFOS(config)# access-policy password minimum lowercase 2
PFOS(config)# access-policy password minimum numerical 1
PFOS(config)# access-policy password minimum special 2
PFOS(config)# access-policy password minimum positions-changed 2
```

Or

```
PFOS(config)# access-policy password minimum length 8 lowercase 2
uppercase 1 special 1 numerical 2 positions-changed 5
```

authentication order

Specify the order in which sources are used for authentication.

Syntax

```
authentication order order
```

Options

`order`	Specifies the order in which sources (`local`, `radius`, `tacacs`, and `ldap`) are used for authentication. `local`must be present, and it must be first or last.

Mode

Configuration

Examples

```
PFOS(config)# authentication order local ldap radius tacacs
PFOS(config)# authentication order tacacs local
PFOS(config)# authentication order ldap local
```

clock

Specify time manually for PFOS. If multiple management modules are installed, then the time is set on all installed management modules.

Syntax

```
clock set time
```

Options

`time`	Manual setting for date and time. Format is `YYYY-MM-DDTHH:MM:SS`.

Mode

Operational, Configuration

Examples

```
PFOS(config)# clock set 2017-03-09T09:40:45
set current time = Mon Mar 9 16:40:45 UTC 2017
```

feature

Enable system-wide feature settings. (Use the `no` prefix to disable.)

Syntax

```
feature common-criteria-mode
feature custom-bytes <2 | 4>
feature custom-hash
feature fips-mode
feature hash-algorithm [alg-name]
feature front-panel
feature { http | https } { netconf | webui [ port tcp-port ] }
feature map-profile { auto | dip-ipv6-mode | dip-mode | legacy | sip-
ipv6-mode | sip-mode }
feature powersafe
feature ssh cli [ port tcp-port ]
feature slicing
feature slicing-offset [value]
feature stripping mpls
feature stripping mpls-max-labels [value]
feature stripping mpls-cleanup-mode [type]
feature tunnel { enable | disable }
```

Options

`common-criteria-mode`	This feature is only supported on PFS 5000/7000 devices. When Common Criteria mode is enabled: • SSH session rekeying functionality is enabled. An SSH session will rekey after an hour or 1G of data transferred. • Strict Host Key Checking is enabled. Both RSA and ECDSA types of SSH public keys are supported in Strict Host Key Checking; however, if Common Criteria mode is enabled with FIPS mode , only ECDSA type keys are supported. Refer to the `copy` command (`ssh-knownhost:`) in this guide and "Maintaining SSH Knownhost" in the ***PFOS 6.x User Guide*** for details. • PFOS CLI login using TACACS, RADIUS, or LDAP is supported with configuration limitation. Refer to "CLI Remote Authentication with FIPS or Common Criteria Modes Enabled" in the ***PFOS 6.x User Guide*** for details. • PFOS supports Syslog, LDAP, and RADIUS over TLS functionality when Common Criteria mode is enabled; however, this functionality is not compliant to Common Criteria requirements. • TLS certificates are periodically verified via the Online Certificate Status Protocol (OCSP). See “Online Certificate Status Protocol” in the ***PFOS 6.x User Guide*** for details. **Note:** Access over IPv6 is not supported in Common Criteria mode when FIPS mode is enabled due to a deficiency in client IP logging. **Warning!!! All the active CLI sessions will be cleared automatically upon confirmation for common criteria mode change to take effect.**

`feature custom-bytes`	Configure the number of Custom Hash bytes reserved in memory. Options are 2 or 4 bytes; 2 is the default. This configuration will take effect on next reboot.
`feature custom-hash`	Enable/disable a custom hash algorithm for load balancing for PFS 5000/7000 series devices. The Custom Hash functionality enables users to configure up to four bytes of packet data (configurable using lb-criteria) to be used in a custom hashing mechanism for traffic distribution. For details about how to associate a configured Custom Hash to a traffic map, refer to map. This configuration will take effect on next reboot.
`fips-mode`	This feature is available on PFS 5000/7000. When FIPS mode is enabled: • PFOS uses only cryptographic algorithms that comply with the Federal Information Processing Standard. • Web UI logging of client connections via IPv6 will not correctly reflect the client's IPv6 address. • Only Elliptic Curve (EC) TLS certificates are supported. PFOS will not allow FIPS mode to be enabled if an RSA browser certificate is currently installed; this means the user must upload and install an EC browser certificate before enabling FIPS mode. • Only the ECDSA type of SSH public keys are supported. Therefore, if both the Common Criteria Mode and FIPS mode are enabled, PFOS will only use ECDSA key type for Strict Host Key Checking. Refer to the `copy` command (`ssh-knownhost:`) in this guide and "Maintaining SSH Knownhost" in the ***PFOS 6.x User Guide*** for details. • Refer to "Certificate Limitations and Configuration Considerations" in the ***PFOS 6.x User Guide***.
`hash-algorithm`	Enable a hash algorithm for load balancing for PFS 5000/7000 series devices. Options are: • `xor16` (default) • `crc16` • `crc16-ccitt` • `crc16-xor1` • `crc16-xor2` • `crc16-xor4` • `crc16-xor8` • `crc32-lo` • `crc32-hi` • `crc32-eth-lo` • `crc32-eth-hi` • `crc32-koopman-lo` • `crc32-koopman-hi`
`front-panel`	This option is only available on the PFS 6000 series. It enables or disables the LCD panel on the front of the system.
`http`	Enable HTTP to access the management interface. (Default TCP port 80)
`https`	Enable HTTPS to access the management interface. (Default TCP port 443)
`ssh cli`	Enable SSH to access the CLI of the management interface. (Default TCP port 22)
`netconf`	Enable access to the NETCONF XML API. (Default TCP port 830 for HTTP, 832 for HTTPS)
`webui`	Enable access to the Web UI. (Default TCP port 80 for HTTP, TCP port 443 for HTTPS)
`tcp-port`	TCP port number on which to enable access.

`map-profile`	Configure how PFOS uses the Ternary Content-Addressable Memory (TCAM) for Forwarding Filters. Options include: • `auto` (default) • `sip-mode` • `dip-mode` • `sip-ipv6-mode` • `dip-ipv6-mode` • `legacy` For details about configuring map profile options, see the “Map Profile” section in the *PFOS User Guide.*
`powersafe`	**This feature is applicable only on the PFS 7000 Series.** Enable the powersafe feature. This feature works with the External PowerSafe TAP platform to provide bypass switch support for failover protection for the PFS 7000 Series. Refer to the **PFOS 6.x User Guide** for more information about how the PowerSafe feature works. Once enabled, PFOS detects the PowerSafe modules and links/segments. See the `powersafe` commands for configuring PowerSafe settings.
`slicing`	**This feature is applicable only on the PFS 7000 Series. Packet slicing is only supported as part of the port mirroring feature on PFS 703x and PFS 704x devices.** Enables users to remove unwanted or sensitive data from packets while preserving crucial data found in headers or early in the payload. PFOS uses the following default slicing locations from the packet start: • PFS 703x devices: 192 bytes (including FCS) • PFS 704x devices: 190 bytes (including FCS)
`slicing-offset [value]`	**This feature is applicable only on the PFS 7000 Series. Packet slicing is only supported as part of the port mirroring feature on PFS 703x and PFS 704x devices. The `slicing-offset` option is only supported on PFS 704x devices.** Configure the slicing offset (which spans from 30-63 bytes). When configured, the slicing offset causes the packets to be sliced the configured number of bytes: • after the IP header for IP traffic (without UDP/TCP/SCTP L4) • after L4 header for UDP/TCP/SCTP traffic • after MPLS headers for MPLS traffic
`stripping mpls`	**This feature is applicable only on the PFS 7000 Series.** Enable/disable the MPLS stripping feature. Modifying this setting requires a reboot; you are prompted with a system message asking you to confirm the reboot. To disable this feature, use the `no feature stripping mpls` command.

`stripping mpls-max-labels [value]`	**This feature is applicable only on the PFS 7000 Series.** Configure the maximum number of MPLS labels that PFOS can automatically program from incoming traffic. Valid values are between 1 and 24576; the default value is 1024. The maximum value of 24576 (24K) is supported on PFS 7120 and PFS 7010; the maximum value supported for other 7000 platforms is 12288 (12K). **Note:** The current number of MPLS label entries can be viewed with the `show stripping mpls | include -mpls | count` command. If the number of programmed MPLS labels reaches the maximum allocated MPLS entries, they can be cleared automatically or manually; see the `feature stripping mpls-cleanup-mode` command. **Caution:** *The hardware table used to store the entries is shared across other tunneling protocols such as VXLAN and L2GRE. Prior to setting the maximum MPLS label limit, ensure you are planning enough space for all required protocols. It is recommended that MPLS use only 70% of the resource table entries.* **Note:** Modifying this setting requires a reboot; you are prompted with a system message asking you to confirm the reboot.
`stripping mpls-cleanup-mode [type]`	**This feature is applicable only on the PFS 7000 Series.** Configure the clean-up method used to clear auto-defined MPLS labels when the maximum limit is reached. Two types are available: • `auto` – PFOS Software will trigger a 60-second timer to clear the MPLS labels once the maximum limit is reached. • `manual` - (Default) User must manually clear the MPLS labels using CLI command stripping clear mpls. This configuration will take effect on next reboot. **Note:** During cleanup traffic disruptions will occur on MPLS labeled packets.
`tunnel`	Enable/disable the tunnel termination feature. Modifying this setting requires a reboot; you are prompted with a system message asking you to confirm the reboot.

Mode

Configuration

Examples

Enable common criteria mode:

```
PFOS(config)# feature common-criteria-mode
```

Disable common criteria mode:

```
PFOS(config)# no feature common-criteria-mode
```

Set custom hash bytes to 4:

```
feature custom-bytes 4
```

Enable custom hash:

```
PFOS(config)# feature custom-hash
```

Disable custom hash:

```
PFOS(config)# no feature custom-hash
```

Enable FIPS mode operation:

```
PFOS(config)# feature fips-mode
```

Enable a hash algorithm:

```
PFOS(config)# feature hash-algorithm xor16
```

Disable front panel access:

```
PFOS(config)# no feature front-panel
```

Enable SSH access to the CLI on TCP port 22:

```
PFOS(config)# feature ssh cli port 22
```

Disable HTTP access to the Web UI:

```
PFOS(config)# no feature http webui
```

Enable HTTP access to the Web UI on default TCP port 80:

```
PFOS(config)# feature http webui
```

Enable HTTPS access to the NETCONF interface on default TCP port 832:

```
PFOS(config)# feature https netconf
```

Enable the map-profile feature with sip-mode:

```
PFOS(config)# feature map-profile sip-mode
```

Enable the powersafe feature:

```
PFOS(config)# feature powersafe
```

Disable the powersafe feature:

```
PFOS(config)# no feature powersafe
```

Configure maximum MPLS labels PFOS can automatically define:

```
PFOS(config)# feature stripping mpls-max-labels 4094
```

Enable the tunnel termination feature:

```
PFOS(config)# feature tunnel enable
```

Disable the tunnel termination feature:

```
PFOS(config)# feature tunnel disable
```

Enable the PFS 703x/704x slicing feature:

```
PFOS(config)# feature slicing
```

Enable the PFS 704x slicing offset feature:

```
PFOS(config)# feature slicing-offset 32
```

firewall rule

Firewalls examine a data packet and perform a comparison with a set of pre-configured firewall rules to determine whether a specific packet should be allowed to pass through or should be dropped.

Firewall rules control how the PFOS firewall protects your PFS from malicious programs and unauthorized access. The `firewall rule` command enables you to control system access to/from certain IPs, including an option to deny all access to a PFS device except for explicitly defined firewall permit rules. See also `show running-config firewall`.

Syntax

```
firewall rule <rule name> ip <IP address>/<prefix length> <permit|deny>
[ingress|egress] description [description]

no firewall rule [rule name]
```

Options

rule name	Unique user-assigned name for each rule. **Note:** When using the `no firewall rule` command and no rule name is defined, all firewall rules will be deleted.
IP address/prefix length	Network IP address and netmask prefix length. Both IPv4 and IPv6 addresses are supported. *Deny All Option* - Using the following IP address syntax with a Deny Action enables users to block all access to the PFS except for explicitly permitted by firewall rules: IPv4 - *0.0.0.0/0* IPv6 - *::/0* **Note:** In order to block all access, user must configure at least one firewall rule that permits access to the client.
permit|deny	Manage system access: • **Permit** traffic on specified IP. • **Deny** traffic on specified IP. **Note:** To prevent user from inadvertently locking themselves out, the Deny command will fail if: • The user client IP is in Usable Host IP range. For example, if user defines `firewall rule 216.130.207.9/22 deny ingress`,and the user client IP is within 216.130.204.1 - 216.130.207.254 IP range, the deny command will fail. • The Switch Gateway IP is in usable host IP range. • The Input IP is 127.0.0.0/8 (or ::1 for IPv6).
ingress|egress	Manage system traffic: • **ingress**: manage system inbound traffic on specified IP (default). • **egress**: manage system outbound traffic on specified IP.
`description`	Optional description for the rule. Description string should be entered within quotes.

Mode

Configuration

Examples

Deny ingress traffic on IP address 216.130.207.9/22.

```
PFS(config)# firewall rule z_ipv4_rule ip 216.130.207.9/22 deny ingress description "IPv4
deny ingress rule"
```

Permit egress traffic on IP address 2001:db8:0:b::1a/64.

```
PFS(config)# firewall rule a_ipv6_rule ip 2001:db8:0:b::1a/64 permit egress description "IPv6
permit rule"
```

Delete a firewall rule.

```
PFS(config)# no firewall rule
Possible completions:
  z_ipv4_rule  a_ipv6_rule  c_ipv6_rule  <cr>
PFS(config)# no firewall rule z_ipv4_rule
PFS(config)# end
```

Deny all access - failed

```
PFS(config)# firewall rule deny_eg ip 0.0.0.0/0 deny egress remark "deny all egress"
Aborted: 'firewall rule deny_eg': User input IP 0.0.0.0/0 will block client IP 10.20.30.40.
Add rule to allow client IP access before this rule.
Error: failed to apply modifications
```

Add permit firewall rule

```
PFS(config)# firewall rule clnt_eg ip 10.20.30.40/32 permit egress remark "Client permit
egress"
PFS(config-rule-clnt_eg)# exit
```

Deny all access - success

```
PFS(config)# firewall rule deny_eg ip 0.0.0.0/0 deny egress remark "deny all egress"
PFS5010(config-rule-deny_eg)# exit
PFS5010(config)# exit
```

gps

Configures Global Positioning System (GPS) settings for PFOS.

Syntax

```
gps cable-length number
```

Options

number	Specifies the maximum length, in meters, of cable between the system chassis and the GPS receiver (1-300m, default 100m).

Mode

Configuration

Examples

```
PFOS(config)# gps cable-length 150
```

interface

Configure port settings. See interface mgmt for information on using the `interface mgmt` command to configure IP address settings for the system chassis. Available options depend upon the type of line card on which a port is being configured.

Syntax

Slot options

```
interface slot clear config
interface slot configured-card card-type
interface slot reset
interface slot shutdown
```

slot	Chassis line card slot.
clear config	Clear configuration for the slot.
configured-card *card-type*	Pre-provision the type of line card to be installed in this slot. Valid values are 6Cstd, 15Qstd, 36S6Qstd, and 40SadvR.
reset	Reset line card.
shutdown	Shut down line card.

Port Options

```
interface slot eth port
```

Multiple port options can be combined from this list:

```
interface slot eth port class port-class
interface slot eth port clear config
interface slot eth port egress-vlan-action name
interface slot eth port external-device-tagging
interface slot eth port FEC fec-option
interface slot eth port fec-type fec-type-option
interface slot eth port geo-probe-time-format-encapsulation geo-probe-
option
interface slot eth port link_state link-state
interface slot eth port lldp [rx {disable|enable}] [tx {disable|enable}]
interface slot eth port name port-name
interface slot eth port port_breakout breakout-option
interface slot eth port reset
interface slot eth port speed port-speed
interface slot eth port stripping egress-vlan-tag
interface slot eth port stripping vlan-tag count num-tags
interface slot eth port stripping vn-tag
interface slot eth port stripping vxlan
interface slot eth port stripping l2gre
interface slot eth port stripping mpls
interface slot eth port stripping mpls l2-mpls
interface slot eth port stripping mpls unstrippable-mpls-dest port-num
interface slot eth port timestamp [tx [ tx-id id ]][rx [ rx-id id ]]
interface slot eth port tunnel-termination tunnel-option
interface slot eth port tunnel-termination disable
interface slot eth port tx-laser
interface slot eth port vid vlan-id
interface slot eth port vlan_tagging vlan-tagging-option
```

PFS 6000-Only Port Options

```
interface slot eth port De-Duplication dedup-settings
interface slot eth port monitor_output_portstamping ps-option
interface slot eth port monitor_output_timestamping ts-option
interface slot eth port protocol-stripping protocol-strip-option
interface slot eth port slicing slicing-option slicing-name slice-name
interface slot eth port extended-lb elb-option
```

`classport-class`	Type of port: • `Monitor` • `Service` • `Span-Monitor` • `Span` (default) • `Inline-Network` • `Inline-Monitor` • `pStack` • `pStack-plus` (**Note: The pStack+ feature requires the PFS 7000 functionality license.**). ◦ If pStack-plus ports are connected over an IP interface, you must configure `source-ip-address` and `destination-ip-address` for the port; (`gateway IP address` is optional). **Note:** The IP Source and IP Destination addresses must be unique across the pfsMesh and the IP network; the IP addresses cannot be assigned to more than one port within a pfsMesh and each port can be used in only one point-to-point connection. ◦ If pStack-plus ports are physically connected, PFOS automatically assigns the IP addresses. **Notes for pStack and pStack-plus ports:** • If switching the port class from **pStack to pStack-plus**, or from **pStack-plus to pStack**, you must first configure the port class to Span, then configure the port class to the new option. You cannot change the port class directly from pStack to pStack-plus (or vice-versa), you must configure the port to Span first. • When changing port class from **pStack-plus without IP** to **pStack-plus with IP**, configure port as Span and then as pStack-plus with IP. • When changing port class from **pStack-plus with IP** to **pStack-plus without IP**, configure port as Span and then as pStack-plus without IP.
`clear config`	Clear configuration for the port.

`De-Duplication` *`dedup-settings`*	**Note: This feature is only available on PFS 6000 Series.** Enables or disables deduplication. Options are: `disable` (default) `enable dedup_name dedup-library` When enabled, can specify a previously defined name from the deduplication library.
`egress-vlan-action` *`name`*	**Note: This feature requires the PFS 7000 functionality license.** Configure the name of the egress-vlan-action for this Inline Monitor Port. Egress VLAN profiles are configured using the `app-lib egress-vlan-action` command. One egress-vlan-action profile is supported per Inline Monitor port.
`eth` *`port`*	Line card port in the format `slot-port`. Example: `7-4` **Note:** For PFS 5010s with limited 16-port capacity licensing, you can only configure ports 1-16; if you attempt to configure port 17 or greater an error displays.
`extended-lb` *`elb-option`*	**Note: This feature is only available on PFS 6000 Series. Refer to "Extended Load Balancing" in the PFOS User Guide for details.** Enables or disables extended load balancing. Options are: `disable` (default) `enable extended-lb-name elb-library` When enabled, specify a previously defined name (user-defined or pre-configured) from the extended load balancing library. Pre-configured extended load balancing names are `G&G&M&V&V+IPD&L4D`, `G&G&M&V&V+IPS&L4S`, `G&G&M&V&V+IPSD&L4S`D, `VXLAN+IPD&L4D`, `VXLAN+IPS&L4S`, and `VXLAN+IPSD&L4SD`.
`external-device-tagging`	This option is only available for Span-Monitor ports. This option is used in PFS/PFX inner filtering and inner load balancing configurations. When this option is enabled, PFOS does not add the port's VLAN tag during ingress processing. This replaces source-port VLAN tagging with tags added by the external device (PFX). Refer to "PFOS/PFX Inner Filtering and Inner Load Balancing" in the *PFOS 6.x User Guide* for details.
`FEC` *`fec-option`*	Available on PFS 51xxs/71xx models, 25G, 100G, and 100G breakout to 25G and 50G ports. Forward Error Correction (FEC) is an error correction technique that adds redundant information to a data transmission, enabling a receiver to identify and correct errors without the need for retransmission. However, there is a latency penalty when using FEC. FEC is disabled by default, which offers the lowest latency delay. FEC is typically disabled with single mode (LR) connections. Valid options: • `disable` (default) • `enable`

`fec-type` *`fec-type-option`*	FEC should be enabled when the peer (or tapped network) has FEC enabled. Once enabled, FEC can be operated in one of three modes: FC-FEC mode (CL74) or RS-FEC mode (CL91), or RS544 mode depending on the network peer FEC setting and the PFS model. Refer to "FEC Support" in the *PFOS 6.x User Guide*. Valid options: • `cl91`(default) • `cl74` • `rs544`
`geo-probe-time-format-encapsulation` *`geo-probe-option`*	Geo Probe time format encapsulation options: `disable` (default) `enable`
`link_state` *`link-state`*	Link state options for the port: `auto` – Normal operation. `force-down` – Force the link down. `force-up` – Force the link up. For fiber ports only, the `force-up` option can be used to force a port to establish a link, even if nothing is plugged into the port. This option is intended for use with fiber ports, including SFP+, QSFP+, and CFP2 transceivers that normally will not acknowledge a link unless something is plugged into the Rx side of the transceiver. Forcing the port to link will allow the port to output data from the Tx side of the fiber-optic port, even if nothing is plugged into the Rx side of the port.
`lldp [rx {`*`disable`*` | `*`enable`*`}] [tx {`*`disable`*` | `*`enable`*`}]`	**Note: This feature requires the PFS 7000 functionality license.** Enable/disable transmission (TX) and reception (RX) of Link Layer Discovery Protocol (LLDP) packets on this port to support neighbor discovery. Neighbor discovery allows devices to advertise device information to their directly connected peers/neighbors. Default value is Rx enable and Tx disable. Refer to "Neighbor Discovery Using LLDP" in the *PFOS 6.x User Guide* for details.
`monitor_output_portstamping`*`ps-option`*	**Note: This feature is only available on PFS 6000 Series. Refer to "Port and Time Stamping" in the PFOS User Guide for details.** Port stamping options (on advanced line cards): `disable` (default) `enable [ portstamping_option { one_byte | two_byte_flat } ]`
`monitor_output_timestamping` *`ts-option`*	**Note: This feature is only available on PFS 6000 Series. Refer to "Port and Time Stamping" in the PFOS User Guide for details.** Time stamping options (on advanced line cards): `disable` (default) `enable`
`name` *`port-name`*	Name to identify the port.

`port_breakout` *`breakout-option`*	`disable` (default) `enable { 4x25g | 2x50g | 4x10g }` Available on 40G and 100G ports (see exceptions in Notes). When port breakout is enabled, it divides the port into multiple subports. The subports use *`slot-port.num`* syntax, where *`slot`* is the slot number, *`port`* is the main port number, and *`num`* is an ascending number for each breakout. **Notes**: • Only certain ports on the PFS 5120/7120 and PFS 5121/ 7121-64x have breakout capability; refer to "PFS 5120/7120 Port Breakout Limitations" and "PFS 5121/7121-64X Port Breakout Limitations" in the ***PFOS User Guide*** for details. • PFS 5030-32X/7030-32X and 5031-32X/7031-32X devices also support breakout to 4x1G. • PFS 5031-32X/7031-32X devices support 1G copper transceivers when breakout to 4x1G is enabled. The 1G copper transceivers can be used in combination with a QSFP28-to-SFP28 adapter that supports plugging an SFP/SFP+/SFP28 transceiver into a QSFP28 slot. Contact your NETSCOUT account team for adapter details. • Disabling Port Breakout on pStack/pStack-plus ports: If you need to disable Port Breakout for any pStack/pStack-plus ports that are actively used by maps or pStack maps, the port class must be changed to Span first in order to disable port breakout. Once port breakout is disabled, you can change the port class back to pStack/pStack-plus.
`protocol-stripping`*`protocol-strip-option`*	**Note: This feature is only available on PFS 6000 Series. Refer to "Protocol De-encapsulation and Stripping" in the PFOS User Guide for details.** Protocol stripping options: `disable` (default) `enable`
`reset`	Reset the port.
`slicing` *`slicing-option`*	**Note: This feature is only available on PFS 6000 Series. Refer to "Conditional Packet Slicing" in the PFOS User Guide for details.** Conditional slicing and masking options: `disable` (default) `enable`
`slicing slicing-name` *`slice-name`*	**Note: This feature is only available on PFS 6000 Series. Refer to "Conditional Packet Slicing" in the PFOS User Guide for details.** Name of slicing library to use on this port.

speed port-speed	Specifies the port speed in bits per second. Available options depend on the features of the line cards. Press ? for a list of options. **Note:** PFS 5110s and PFS 5031/7031-56Xs support SFP28, SFP+, and SFP transceivers in ports 1-48. These ports may be configured for operation at 1G, 10G, or 25G however the port speed is a common setting for each group of four sequential ports, starting at port 1 (for example, ports 1-4 must all have the same speed). PFOS enables you to set the speed of the base port (the first of the group of 4 ports); you cannot set a port speed for the 2nd through 4th port in the group (PFOS will display an error message).
stripping egress-vlan-tag	Enable egress vlan tag stripping. Use the no form of the command to disable stripping. **Notes:** • The PFS PFS 503x/703x and PFS 504x/704x devices do not support Egress VLAN Tag stripping. • To remove a specific set of VLAN IDs from an inline monitor egress port, refer to egress-vlan-action.
stripping vlan-tag count *value*	Enable ingress VLAN tag stripping. Use the no form of the command to disable stripping. The *count* option enables you to enter either **1** or **2** (the default) for the number of VLAN tags to strip.
stripping vn-tag	Enable ingress VN tag stripping. Use the no form of the command to disable stripping. **Note:** The PFS 503x/703x and PFS 504x/704x devices do not support Vn Tag stripping.
stripping vxlan	Enable ingress VXLAN tag stripping. Use the no form of the command to disable stripping. To configure a set of VTEP addresses, UDP ports, and VNIDs, refer to app-lib standard-stripping vxlan. **Note:** PFOS does not support both VxLAN and MPLS stripping on the same port; you must configure VxLAN and MPLS stripping on separate ports.
stripping l2gre	**Note: This feature requires the PFS 7000 functionality license.** Enable ingress L2GRE stripping. To configure a set of destination IP addresses and L2GRE IDs, refer to app-lib standard-stripping l2gre command. **Notes:** • The PFS 704x devices do not support L2GRE stripping. • PFOS does not support both L2GRE and MPLS stripping on the same port; you must configure L2GRE and MPLS stripping on separate ports.
stripping mpls	**Note: This feature requires the PFS 7000 functionality license.** Specify mpls to enable L3 (IP over MPLS). Once enabled, PFOS automatically defines MPLS labels based on incoming traffic. You can use the app-lib standard-stripping mpls command to define additional custom MPLS labels.

`stripping mpls l2-mpls`	**Note: This feature requires the PFS 7000 functionality license.** Specify `l2-mpls` to enable L3 (IP over MPLS) and L2 (Ethernet over MPLS). Once enabled, PFOS automatically defines MPLS labels based on incoming traffic. You can use the `app-lib standard-stripping mpls` command to define additional custom MPLS labels.

`stripping mpls`
`unstrippable-mpls-dest`
`port-num`
	Note: This feature requires the PFS 7000 functionality license.
	Note: This option is not applicable for service ports.
	Port ID where MPLS unstrippable packets will be sent. Incoming MPLS packets with partially matching labels or with more than two labels are sent to the designated unstrippable MPLS destination port. Partially matching labels occur when packets have two labels, and the outer label matches a configured label, but the inner label does not. Port options include a list of configured Monitor, Service or Span-Monitor ports.
	If not configured, the unstrippable packets will be dropped.

`timestamp`	**Note: This feature is only supported on certain PFS devices; see "PFS 7000 Timestamping" in the PFOS User Guide for details.** To configure timestamping for a port, specify the following: • `tx` - include `tx` option to enable egress timestamping on traffic transmitted on this port. • `tx-id` - configure a unique ID to be included in the egress timestamp. If not configured, the port's VLAN-ID (VID) will be included in the egress timestamp. • `rx` - include `rx` option to enable ingress timestamping on traffic received on this port. • `rx-id` - configure a unique ID to be included in the ingress timestamp. If not configured, the port's VLAN-ID (VID) will be included in the ingress timestamp.

`tunnel-option`	Tunnel termination options:
	`enable tunnel-termination-name tunnel-name`
	`disable`
	`tunnel-name`: Name of the tunnel termination group to associate with tunnel termination on this port.

`tx-laser`	Tx-laser options for PFS 5000/7000 ports: `on` (default) `off` Disabling the transceiver transmitter for passive or unused ports helps reduce power consumption of the device.

`vid vlan-id`[1]	To configure a VLAN ID, choose from the following options: • `default`: PFOS assigns a default VLAN ID based on the Starting VLAN ID configured using the `monitor-port-vlan` command. • Enter a custom VLAN ID for the port; valid values range 1-4094. **Note:** User-defined VLANs for all the member ports of a Consolidated network group will be ignored. Incoming packets from the member ports are tagged with a Common VLAN ID value from the Consolidated network port group. If a Common VLAN ID is not set, then it is tagged with a VLAN ID assigned by the pStack protocol. For VLAN ID behavior over pfsMesh refer to "pfsMesh" in the ***PFOS User Guide***.
`vlan-strip-option`	VLAN tag stripping options: `disable` (default) `enable`
`vlan-tagging-option`	VLAN tagging options: `disable` (default) `enable`

[1] You can view this VLAN ID by using the `show interface <x> eth <y> vid` command. This VID value is derived based on following priority:

1. VID =pStack VLAN, a unique VLAN ID assigned by the pStack protocol if there is a local port with Class=pStack, OR if this device is connected to a pfsMesh using pStack+ and there is a pStack port present in the connected pfsMesh (refer to"pfsMesh" in the ***PFOS User Guide*** for details).
2. VID = User defined VLAN, if Scenario #1 is not applicable.
3. VID = Default VLAN, if Scenario #1 and #2 are not applicable.

Refer to "Source Port VLAN Tagging" in the ***PFOS User Guide*** for details about what VLAN ID to expect on egress packets.

Mode

Configuration

Examples

```
PFOS(config)# interface 9 eth 9-1 name port9-1 class Monitor link_state
force-up
PFOS(config)# interface 1 eth 1-26 class Monitor vlan_tagging enable
PFOS(config)# interface 1 eth 1-9 port_breakout enable breakout-option
4x10g
PFOS(config)# interface 3 eth 3-1 slicing enable slicing-name slice-1
PFOS(config)# interface 6 eth 6-1 De-Duplication enable
PFOS(config)# interface 6 eth 6-1 De-Duplication enable dedup_name
dedup1
PFOS(config)# interface 6 eth 6-1 extended-lb enable extended-lb-name
VXLAN+IPS&L4S
PFOS(config)# interface 1 eth 1-2 external-device-tagging
PFOS(config)# no interface 1 eth 1-2 external-device-tagging
PFOS(config)# interface 1 eth 1-1 class Span-Monitor
PFOS(config)# interface 1 eth 1-11 class Inline-Network
PFOS(config)# interface 1 eth 1-16 class Span vid 101
PFOS(config)# interface 1 configured-card 36S6Qstd
PFOS(config)# interface 4 eth 4-6 tunnel-termination enable tunnel-
termination-name ep1
PFOS(config)# interface 1 eth 1-1 class pStack
PFOS(config)# interface 1 eth 1-1 class pStack-plus
PFOS(config)# interface 1 eth 1-15 class pStack-plus source-ip-address
10.10.10.14 destination-ip-address 20.20.20.15 gateway-ip-address
10.10.10.1
PFOS(config)# interface 1 eth 1-2 stripping vlan-tag count 2
PFOS(config)# interface 1 eth 1-33 stripping mpls l2-mpls unstrippable-
mpls-dest 1-1
PFOS(config)# no interface 1 eth 1-33 stripping mpls
PFOS(config)# interface 1 eth 1-33 stripping l2gre
PFS(config)# interface 1 eth 1-34 FEC enable fec-type cl74
PFS(config)# interface 1 eth 1-33 lldp [rx disable] [tx enable]
PFS(config)# tx-laser off
```

interface dhcp

Enable or disable the use of DHCP to automatically configure management network addresses. To view the network addresses currently configured, use show interface.

Available only on PFS 5000/7000 Series systems.

Syntax

```
[ no ] interface dhcp
```

Options

None

Mode

Configuration

Examples

```
PFOS(config)# interface dhcp
PFOS(config)# no interface dhcp
```

Disable/Enable DHCP on PFS 5000/7000 Series

PFS system default with PFOS 6.0.4 or later image has DHCP enabled. Users need to disable DHCP before configuring a static IP address. A serial console connection is recommended for changing DHCP and static IP settings to prevent losing network connection. If a serial console connection is not available, perform one of the following procedures to ensure a successful network setting change.

Disable DHCP and Configure a Static IP

Use the following commands to disable DHCP and add a static IPv4 or IPv6 static IP address. The two commands are separated by a semicolon; PFOS processes them sequentially in the same transaction.

```
PFS5010(config)# no interface dhcp ; interface mgmt 0 ip address
10.250.177.115/23 gateway 10.250.176.1
```

A validation warning message appears for confirmation before continuing:

```
The following warnings were generated:
'interface': Changing the DHCP settings may lead to the change of
the system IP address. Active sessions may be lost.
Proceed? (yes/no)
```

Reconnect the device with the static IP address.

Notes

- PFOS allows disabling DHCP without configuring a static IP; PFOS detects the existing static IP (PFOS default static IP is 192.168.0.250). When disabling DHCP without configuring a new static IP, the current static IP address appears at "Static Network Connection" and is used after DHCP is disabled.
- PFOS does not allow assigning a new static IP without first disabling DHCP; a validation error message appears.

```
PFS5010(config)# interface mgmt 0 ip address 10.250.177.129/23 gateway
10.250.176.1
Aborted: 'interface mgmt 0 ip': DHCP is enabled. Please disable DHCP to
set static IPs. Disable DHCP using CLI command "no interface dhcp" or
webUI->System->Network->DHCP page.
Error: failed to apply modifications
```

Enable DHCP

PFOS DHCP can be enabled to receive an IP address from the DHCP server. Ensure a DHCP server is reachable and configured before enabling. If PFOS does not receive a DHCP response after DHCP is enabled, PFOS uses the existing static IP.

Note: The current IP address connection will be lost after DHCP is enabled; therefore, you need to use the new IP address assigned from the DHCP Server to reconnect.

```
PFS5010(config)# interface dhcp
```

A warning message appears for confirmation before continuing.

```
PFS5010(config)# The following warnings were generated:
'interface': Changing the DHCP settings may lead to the change of the
system IP address. Active sessions may be lost.
Proceed? (yes/no)
```

interface gre

Configure a Generic Routing Encapsulation (GRE) tunnel interface. To view the currently configured GRE tunnel interfaces , see show interface gre . Refer to the ***PFOS 6.x User Guide*** for GRE Tunnel Origination/Termination feature details.

Syntax

```
interface gre name destination ipaddress source l3_if_name key
identifier [ gateway ipaddress ] vlan-tagging [ingress-tag/no-tag]
no interface gre name
```

Options

name	Name to identify the GRE tunnel interface.
ipaddress	IPv4 IP address
l3_if_name	IP interface name
identifier	L2GRE Key value; valid values range from 1 to 268435455. **Note:** PFS 7030s and PFS 7031s support an L2GRE key value of 0.
vlan-tagging	To enable ingress port VLAN tags to be added to the packets being forwarded to the GRE tunnel. VLAN tagging options: • `ingress-tag` to enable • `no-tag` to disable (Default)

Mode

Configuration

Example

```
PFOS(config)# interface gre gre1 destination 2.2.2.2 source ip1 key 1234
PFOS(config)# no interface gre gre1

PFOS(config)# interface gre tun1 destination 2.2.2.1 source ip1 key 2221
gateway 2.2.2.22 vlan-tagging ingress-tag
PFOS(config)# interface gre tun1 destination 2.2.2.1 source ip1 key 2221
gateway 2.2.2.22 vlan-tagging no-tag
```

interface ip

Configure an IP interface for GRE or VXLAN Tunnel Origination/Termination. To view currently configured ip interfaces , see show interface ip. Refer to the ***PFOS 6.x User Guide*** for GRE and VXLAN Tunnel Origination/Termination feature details.

Syntax

```
interface ip name address ipaddress port port-num
no interface ip name
```

Options

name	Name to identify the IP interface.
ipaddress	IPv4 IP address
port-num	Port for configuring IP address in <slot>-<port> format.

Mode

Configuration

Example

```
PFOS(config)# interface ip ip1 address 1.1.1.1 port 1-1
PFOS(config)# no interface ip ip1
```

interface mgmt

Configure IP addresses for system access to the network. See interface for information on using the `interface` command to configure line card ports.

Syntax

```
interface mgmt id [ip address address/mask] [dns address]
    [gateway address]
interface mgmt id ipv6 address address/mask [ip6-dns address] [ipv6
gateway address]
```

Options

id	Interface ID. Valid values are `0` for the management port of the currently active management module, or `1` and `2` for management modules 1 and 2 on systems with multiple management modules installed.
`ip address` *address/mask*	IPv4 address and netmask of the system in x.x.x.x/n format (default 192.168.0.250/24).
`dns` *address*	IPv4 address of DNS server for the system (default 0.0.0.0).
`gateway` *address*	IPv4 address of default gateway for the system (default 192.168.0.1).
`ipv6 address` *address/mask*	IPv6 address and netmask of the system system (default ::). Example: fe80::113/64
`ip6-dns` *address*	IPv6 address of DNS server for the system.
`ipv6 gateway` *address*	IPv6 address of default gateway for the system. If not specified PFOS will request gateway addresses via Router Solicitation (neighbor learning protocol).

Mode

Configuration

Examples

```
PFOS(config)# interface mgmt 0 ip address 192.168.20.12/24 dns
192.168.10.100 gateway 192.168.20.1
PFOS(config)# interface mgmt 0 ipv6 address 2001:db8::1/24
PFOS(config)# interface mgmt 2 ipv6 address 2001:db8::1/24
PFOS(config)# interface mgmt 0 ipv6 address 2001:db8::1/24 ip6-dns
fd49:b785:0906:fab0::4
PFOS(config)# interface mgmt 0 ipv6 address 8049::1/64 gateway 8049::10
```

interface vxlan

Configure a VXLAN tunnel interface. To view the currently configured VXLAN tunnel interfaces , see show interface vxlan. Refer to the ***PFOS 6.x User Guide*** for VXLAN Tunnel Origination/Termination feature details.

Syntax

```
interface vxlan vxlanname destination ipaddress source l3_if_name key
identifier [ gateway ipaddress ] vlan-tagging [ingress-tag/no-tag] udp-
src-port [ src-port int32]
```

Options

vxlanname	Name to identify the VXLAN tunnel interface.
ipaddress	IPv4 IP address
l3_if_name	IP interface name
identifier	VXLAN Key value; valid values range from 1 to 16777215. **Note:** pStack+ uses a range of 8388608 to 16777215 internally for VNIDs for VXLAN tunnels; therefore, when a PFS device has at least one pStack-plus port configured, the maximum value for VNIDs for user-configured VXLAN tunnels is 8388607.
vlan-tagging	To enable ingress port VLAN tags to be added to the packets being forwarded to the VXLAN tunnel. VLAN tagging options: • `ingress-tag` to enable • `no-tag` to disable (Default)
`src-port int32`	UDP Source Port for L4 layer on encapsulated traffic; valid values range from 1 to 65535.

Mode

Configuration

Example

```
PFOS(config)# interface vxlan vxlan1 destination 2.2.2.2 source ipint333
key 1234
PFOS(config)# no interface vxlan vxlan1
PFOS(config)# interface vxlan vxlan2 destination 1.1.1.1 source ipint333
key 1111  vlan-tagging ingress-tag
```

ldap-server

Specify an LDAP server for user authentication.

Notes:

- If using a LDAP server with FIPS or Common Criteria modes, refer to "CLI Remote Authentication with FIPS or Common Criteria Modes Enabled" in the *PFOS User Guide* prior to adding the server.
- PFOS cannot support the semicolon (;) or backslash (\) characters in passwords for external authentication through LDAP even though these special characters may be supported at the authentication server.

Syntax

```
ldap-server <host-name> tls <enable/disable> authenticate-certificate
<enable/disable> base-dn <base DN> binding-dn <binding DN> binding-mode
<anonymous/authenticated> binding-password <binding DN password> port
<int> retransmit <int> timeout <int> user-attribute <string> group-
attribute <string>
```

Options

`host-name`	LDAP server IP address or host name. **Note:** If enabling `tls` and `authenticate-certificate`, PFOS requires the fully qualified domain name.
`tls`	**Note:** PFOS supports LDAP over TLS functionality when Common Criteria mode is enabled; however, this functionality is not compliant to Common Criteria requirements. `enable` - PFOS connects to LDAP server over TLS. `disable` - PFOS will not connect to LDAP server over TLS.
`authenticate-certificate`	`enable` - PFOS will authenticate the LDAP server's TLS certificate using any installed Certificate Authority certificates. `disable` - PFOS will not authenticate the LDAP server's TLS certificate.
`base-dn`	Base Distinguished Name (DN) is the starting search point in the LDAP tree. For example, for domain netscout.com, the Base DN is dc=netscout,dc=com.
`binding-mode`	Select mode for binding to LDAP server: • Anonymous - allows PFS to connect and search the directory (bind and search) without first authenticating using binding DN and password to log in. • Authenticated - PFS connects to the LDAP server using the configured Binding DN and Binding password.

`binding-dn`	**Note:** This setting is not applicable if using Anonymous `binding-mode`. Binding DN value to be used to bind to LDAP server when the binding-mode is set to Authenticated.
`binding-password`	**Note:** This setting is not applicable if using Anonymous `binding-mode`. Password to be used to connect to the LDAP server when the binding-mode is set to Authenticated. LDAP Binding Passwords cannot start with "$8$". For example, password "$8$Plt&mnb" is not supported.
`port port-number`	Port used to connect to the LDAP Server. Authentication fails if using incorrect port numbers.
`retransmit`	Number of times PFS attempts to contact the LDAP server (default 3).
`timeout`	Maximum time (in seconds) that PFS waits for a response from the LDAP server (default 30 seconds).
`user-attribute`	LDAP attribute for user name searches in the LDAP database (typically `sAMAccountName` for legacy Windows user names, `uid` for User ID, or `cn` for Canonical Name)
`group-attribute`	Attribute used to find group membership of user, typically `memberOf` or `primaryGroupID`.

Mode

Configuration

Examples

```
PFS(config)# ldap-server ad.example.com port 636 binding-dn
CN=ADBind,CN=Users,DC=ad,DC=example,DC=com binding-password somepassword
binding-mode authenticated tls enable authenticate-certificate enable
base-dn CN=Users,dc=ad,dc=example,dc=com retransmit 3 timeout 10 user-
attribute sAMAccountName group-attribute memberOf
```

linux-ptp

Notes:

- This command is only applicable for the PFS 5000/7000 devices. For PFS 6000 series PTP timing support, see the `ptp` command.
- PTP does not support server authentication; to avoid unsecure time sources, continue using NTP with keys (see `ntptime-server`).

Configure Linux-assisted Precision Time Protocol (PTP) time settings for the PFS 5000/7000 series. PFOS supports Linux-assisted PTP timing via the device management port. See also `show linux-ptp`.

When PTP and NTP are both configured and available, PFOS prioritizes PTP timing (this is not user configurable). PFOS monitors PTP status:

- If PTP is available, PFOS will disable NTP service and set NTP status to "N/A".
- If PTP becomes unavailable, PFOS starts NTP service. When PTP becomes available again, PFOS disables NTP again.

Syntax

```
linux-ptp <enable/disable>
linux-ptp enable [ domain-number <value> | hybrid-mode | ptp-delay-
mechanism <value>]
```

Options

`[enable	disable]`	Enable or disable Linux-assisted PTP for time setting (default is disable).
`domain-number`	Number assigned to a group of PTP clocks that synchronize to each other in the network. Valid values are 0 to 255.
`hybrid-mode`	**Note**: PFOS Hybrid mode is based on IEEE 1588 specification, which is considered draft status and may be updated or replaced by other documents. Also, this feature is currently not fully tested with PFOS. • **Enable:** PTP server and clients use mixed multicast/unicast PTP messaging. The PTP Server multicasts sync messages in End-to-End mode with clients and clients respond in unicast. This mode offers the most efficient PTP message processing and minimizes PTP message traffic. • **Disable:** PTP server and clients use multicast PTP messaging. Clients receive their own messages plus all other client messages and must process/discard messages not applicable to them. For larger networks, this can impact processing loads.

`ptp-delay-mechanism`	Choose the mechanism for measuring the communication path delay between the PTP server and client: **Auto**: PFOS selects appropriate delay measurement **E2E**: End-to-end delay measurement **P2P**: Peer-to-peer delay measurement **None**: No delay measurement

Mode

Configuration

Examples

```
PFOS(config)# linux-ptp enable
PFOS(config)# linux-ptp domain-number 3
PFOS(config)# linux-ptp ptp-delay-mechanism E2E
```

logging

The following commands allow you to control Syslog servers and Syslog buffering.

- logging host
- logging buffered

logging host

Configure the IP address or hostname of servers to receive Syslog messages from PFOS. Up to three servers can be configured. PFOS also supports sending system logs to a remote server over an encrypted SSH tunnel; refer to Send Syslog Messages to Remote Server over SSH Tunnel in the Examples in this section.

Syntax

```
logging host host protocol proto port port-num severity-level level tls-config tls-config ssh-port ssh port-num username name
```

Options

host	IPv4 or IPv6 address or hostname of the syslog server. Note that you must have a valid dns server configuration to be able to configure hostnames.
proto	Name of the transport protocol to be used with this syslog server. You can select UDP, TCP, TLS or SSH. If you do not define a protocol, UDP will be used as the default. **Note:** When the TLS protocol is used for Syslog server: • PFOS will use a TLS client certificate for mutual authentication. By default the installed browser certificate is used but a separate syslog client certificate can be installed, see "Maintaining Certificate Files" in Chapter 7 of the *PFOS 6.x User Guide* for details. • If `tls-config` is set to Yes (the default), PFOS will verify the syslog server's certificate for validity using any installed CA Certificates, see "Maintaining Certificate Files" in Chapter 7 of the *PFOS 6.x User Guide* for details. If the Syslog server's certificate cannot be verified, PFOS will refuse to connect to the Syslog server. • PFOS supports Syslog over TLS functionality when common criteria mode is enabled; however, this functionality is not compliant to Common Criteria requirements. **Note:** The SSH option uses an SSH public key to connect to the specified `ssh-port` as user `username`. An SSH key pair is automatically generated by the system. The public key must be displayed (using `show logging host`) and added to the list of authorized keys of `username` on the syslog SSH server.

port-num	Valid port number; valid values range from 1 to 65535. If you do not define a specific port, a default port number will be used for the protocol being used: • UDP (514) • TCP (601) • TLS (6514) • SSH (601)
level	Name of the minimum desired severity level at which messages should be logged in the remote Syslog server. PFOS forwards messages with the severity you define and the severity levels above your defined severity. Available severity options: • Emergency • Alert • Critical • Error • Warning • Notification • Info • Debug For example, defining "Critical" severity forwards Critical messages as well as Alert and Emergency severity messages to the specified Syslog server.
tls-config	**This option is only valid when TLS protocol is used.** Configure whether the Syslog server's certificate is verified: **Yes**: Verify the Syslog server's certificate. **No**: Do not verify the Syslog server's certificate.
ssh-port	**This option is only valid when SSH protocol is used.** Valid port number; valid values range from 1 to 65535. This is the port number of the SSH server on the syslog server; the default is port 22.
username	**This option is only valid when SSH protocol is used.** The username for the remote (SSH) server user account.

Mode

Configuration

Examples

Using hostname:

```
PFOS(config)# logging host 123SFLab protocol tcp
```

Using IPv4 address:

```
PFOS(config)# logging host 10.2.20.200 protocol tcp
```

Using IPv6 address:

```
PFOS(config)# logging host FE80::0202:B3FF:FE1E:8329 protocol tls
```

Setting severity level to Critical (all Critical, Alert, and Emergency severity messages will be forwarded)

```
PFOS(config)# logging severity level critical
```

Verify the Syslog server's certificate

```
PFOS(config)# logging host 1.1.1.1 protocol tls tls-config peer-verify
yes
```

Do not verify the Syslog server's certificate

```
PFOS(config)# logging host 1.1.1.1 protocol tls tls-config peer-verify
no
```

Send Syslog Messages to Remote Server over SSH Tunnel

Note: See note in proto description for SSH details.

```
PFOS(config)# logging host 10.250.178.10 protocol ssh username rsyslog-
user

PFOS(config-host-10.250.178.10)# do show running-config logging host
logging host 10.250.178.10
protocol ssh
port 601
ssh-port 22
username rsyslog-user
!

PFOS# show logging host
logging host 4.5.6.7
logging host 10.250.178.10
ssh public key "ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBmIxjqwTBl4Npe5c7vd
pXaEeWd+vuI8gm3rRtUJ9R9wmSJwNZaybK3WHeDU9LulK+Ep4GjQV+ex+Bf9Ke4LeLg=
root@PFS5010\n"
ssh tunnel status up
logging host 10.250.178.253
ssh public key "ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBmIxjqwTBl4Npe5c7vd
pXaEeWd+vuI8gm3rRtUJ9R9wmSJwNZaybK3WHeDU9LulK+Ep4GjQV+ex+Bf9Ke4LeLg=
root@PFS5010\n"
ssh tunnel status up
```

logging buffered

You can select the minimum severity level of Syslog messages to store in the local Syslog buffer. The Syslog severity levels include:

- Emergency
- Alert

- Critical
- Error
- Warning
- Notification
- Info
- Debug

For example, defining "Critical" severity saves Critical messages as well as Alert and Emergency severity messages to the local buffer.

Note: A maximum of 1000 Syslog messages are logged in the local buffer of PFS 5000/7000 Series and PFS 6002 devices; a maximum of 200 Syslog messages are logged in PFS 6010 local Syslog buffer. PFOS deletes the oldest messages when new messages are added.

Syntax

```
logging buffered severity-level level
no logging buffered
```

Options

level	Name of the minimum desired severity level at which messages should be logged to the local buffer. PFOS logs messages with the severity you define and the severity levels above your defined severity. Available severity options: • Emergency • Alert • Critical • Error • Warning • Notification • Info • Debug For example, defining "Critical" severity saves Critical messages as well as Alert and Emergency severity messages to the local Syslog buffer.

Mode

Configuration

Examples

Setting severity level to Critical (all Critical, Alert, and Emergency severity messages will be forwarded)

```
logging buffered severity-level level
```

monitor_port_vlan

Configure VLAN settings for the system.

Syntax

```
monitor_port_vlan starting_vlanID id tpid_ether_type value
```

Options

`starting_vlanID` *`id`*	The first VLAN ID used when numbering VLANs on the entire system. The default value is 1. When using VLAN tags for port stamping, the system starts counting at the far left and uppermost hardware port and proceeds consecutively, top to bottom and left to right.
`tpid_ether_type` *`value`*	EtherType for VLAN tags: 88A8 (default), 8100, or 9100.

Mode

Configuration

Examples

```
PFOS(config)# monitor_port_vlan starting_vlanID 204 tpid_ether_type 8100
```

move

Reorder a list of items in a configuration.

Syntax

```
move { map | role | statistics | username } item1 { after item2 |
 before item2 | first | last }
```

Options

map	Reorder list of traffic maps.
role	Reorder list of access control roles.
statistics	Reorder list of displayed statistics.
username	Reorder list of local usernames.
item1	Item to reorder.
after item2	Place item1 immediately after item2 in the list.
before item2	Place item1 immediately before item2 in the list.
first	Place item1 at the beginning of the list.
last	Place item1 at the end of the list.

Mode

Configuration

Examples

```
PFOS(config)# show map
OUTPUT
Map   Map                                   OUTPUT    LB      LB
Name  Type     FILTER    INPUT PORTS        PORTS     GROUPS  CRITERIA
--------------------------------------------------------------------
map1  Monitor  http      [ 1-31 1-32 ]  [ 1-33 ]  -       -
map2  Monitor  nonmatch  [ 1-31 1-32 ]  [ 1-34 ]  -       -
PFOS(config)# move map map2 before map1
PFOS(config)# show map
OUTPUT
Map   Map                                   OUTPUT    LB      LB
Name  Type     FILTER    INPUT PORTS        PORTS     GROUPS  CRITERIA
--------------------------------------------------------------------
map2  Monitor  nonmatch  [ 1-31 1-32 ]  [ 1-34 ]  -       -
map1  Monitor  http      [ 1-31 1-32 ]  [ 1-33 ]  -       -
```

notification event

Configure notification event settings.

Syntax

```
notification event all notify-options
notification event chassis chassis-options
notification event configuration config-options
notification event none
notification event user user-options
```

Options

<table>
<tr><td>notify-options</td><td>all – Send both Syslog and SNMP notification.
netconf – Send NETCONF notification.
none – Do not send notification.
snmp – Send SNMP notification.
syslog – Send Syslog notification.</td></tr>
<tr><td>chassis-options</td><td>all notify-options
env { all | temp-high } notify-options
fru (all | error | in-out | reset } notify-options
mgmt { all | | chassis-mac | coldstart | core-dump | disk-space | file-mgmt | health-stats | high-availability | hw-error | restart | trigger-policy} notify-options
none
port { all | enhanced-link-state-snmp | health-check-state | in-out | link-state } notify-options
<b>Notes:</b>
• The port link-state traps (link Down and link Up Objects in standard IF-MIB) and the port enhanced-link-state-snmp traps (vsLinkUpNotif and vsLinkDownNotif in proprietary VSS-SYSTEM-MIB) are similar traps, but the enhanced-link-state-snmp traps have two additional trap components: PFOS port number (such as, “1-13”), and the user-assigned name for the port. Due to their similarity, it is not necessary to enable both sets of traps; enable the best option for your network. For details on SNMP traps, see the “SNMP MIB and Trap Definitions” section in the <i>PFOS User Guide</i>.
• The port enhanced-link-state-snmp option does not support all notify options; only the snmp notify option is supported.</td></tr>
</table>

config-options	all notify-options application { all | deduplication | egress-vlan-action | extended-lb | protocol-stripping | slicing | standard-stripping |triggers | tunnel-termination | vlan-tag-strip } notify-options none port { advanced | all | basic } notify-options system { access-ctl | all | features | info | network | notifications } notify-options traffic { all | filter | lbg | map } notify-options **Note:** For Port configuration events, configuring advanced notification types has no effect.
user-options	all notify-options authentication { access | all | access-snmp} notify-options none

Mode

Configuration

Examples

Send both an SNMP trap and a Syslog event for all config events:

```
PFOS(config)# notification event configuration all all
```

Send no notifications for any type of configuration events (port/system/traffic):

```
PFOS(config)# notification event configuration none
```

Send both an SNMP trap and a Syslog event for all port configuration events:

```
PFOS(config)# notification event configuration port all all
```

Send no notifications for port configuration events:

```
PFOS(config)# notification event configuration port none
```

Send both an SNMP trap and a Syslog event for basic port setting events:

```
PFOS(config)# notification event configuration port basic all
```

Send no notifications for basic port setting events:

```
PFOS(config)# notification event configuration port basic none
```

Send NETCONF link-up and link-down notifications:

```
PFOS(config)# notification event configuration port basic all
```

Send a Syslog event when an egress-vlan-action event occurs:

```
notification event configuration application egress-vlan-action syslog
```

Send NETCONF “access” notifications:

```
PFOS(config)# notification event user authentication access all
PFOS(config-authentication-access)# end
PFOS# show running-config notification event user
notification event user authentication access
syslog,snmp,netconf
```

Send access-snmp notifications:

```
PFOS(config)# notification event user authentication snmp-access all
syslog,snmp,netconf
```

Send link state SNMP notifications (based on standard IF-MIB):

```
PFOS(config)# notification event chassis port link-state snmp
```

Send enhanced link state SNMP notifications (based on proprietary VSS-SYSTEM-MIB):

```
PFOS(config)# notification event chassis port enhanced-link-state-
snmp snmp
```

Note: The port `enhanced-link-state-snmp` option does not support all notify options; only the snmp notify option is supported. If another option is used, an error message appears:

```
PFOS(config)#  notification event chassis port enhanced-link-state-
snmp syslog
Aborted: resource denied: Only snmp allowed
Error: failed to apply modifications
```

ntp time-server

Configure time settings for the system.

Syntax

```
ntp time-server [address] key [key number]
ntp time-server [address]
no ntp time-server [address] key
no ntp time-server [address]
no ntp time-server
```

Options

address	DNS name, IPv4 address, or IPv6 address of an NTP server.
key number	Enter the authentication key that corresponds to the key-value for this server. If this key does not match a number defined in the uploaded NTP key file, NTP will not use the server for time synchronization. **Note:** If an authentication key number is configured with the NTP server, the NTP daemon looks for that key in the ntp key file that is uploaded (refer to the copy command for upload details). If the NTP daemon is not able to find the key number and its corresponding key in the ntp key file, that server will not be used for time synchronization. Refer to "Maintaining NTP Key Files" in the ***PFOS 6.x User Guide*** for details.

Mode

Configuration

Examples

```
PFS(config)# ntp time-server 10.250.176.3 key 3
PFS(config)# no ntp time-server 10.250.176.3 key
```

passwd

Allows users to change their own password.

Note: Users with access control permissions can update other usernames and passwords using the username command.

Syntax

```
passwd current-password current-pw string new-password new-pw string
confirm-new-password confirm-new-pw string
```

Options

current-pw string	User's current password.
new-pw string	User's new password (compliant with defined password policies). Single quote (’) and double quote (“) characters cannot be used as special characters as part of password string. To define passwords with special characters in CLI, the password string needs to be surrounded by double quotes.
confirm-new-pw string	Password confirmation (must enter the same password).

Mode

Configuration

Examples

```
PFOS# passwd current-password 1234abcd new-password 4567efgh confirm-
new-password 4567efgh
Your password has been changed successfully.
```

poweroff

Power down the system. After executing this command, users will be prompted to confirm power down procedure by typing "I agree."

Syntax

```
poweroff
```

Options

None

Mode

Configuration

Examples

```
PFS5010# poweroff Command will power off the switch upon confirmation.
Enter 'I agree' to proceed. Enter any other text to abort or wait for a
timeout (10 seconds) I agree
```

ptp

Note: This command is only applicable for the PFS 6000 Series. For PTP timing support for PFS 5000/7000 devices, see `linux-ptp`.

Configure Precision Time Protocol (PTP) time settings for the system. To see all the settings, enable the feature.

Syntax

```
ptp [enable | disable] announce_msg_interval number
  announce_recv_timeout number
  delay_mechanism {end-end | peer-peer}
  dhcp {enable | disable}
  domain number
  ip address/mask
  port {ethernet | ptp}
  pps_source {gps_port | pps_port | ptp_connector cable-length value}
  sync_interval number
  transport {ethernet | udp}
  telecom {enable | disable}
```

Options

`[enable	disable]`	Enable or disable PTP for time setting (default is disable).
`announce_msg_interval number`	Configures the interval between PTP announcement messages (-4 to 5, default 1).
`announce_recv_timeout number`	Configures the number of attempts before timeout of receive messages (2 to 10, default 3).
`domain number`	Specifies the PTP domain (1-255, default 0).
`delay_mechanism {end-end	peer-peer}`	Configures either end-to-end or peer-to-peer for PTP delay messages (default is end-end).
`dhcp {enable	disable}`	Enables or disables DHCP for the IP address of the PTP module on the chassis (default is disable). If disabled, specified an IP address in the IP Address field.
`ip address/mask`	Configures the IP address/mask of the PTP module on the chassis (different from the main management interface). Assign a static IP address or enable the DHCP field.
`port {ethernet	ptp}`	Specifies the port as Ethernet or PTP (default ptp).
`pps_{gps_port	pps_port	ptp_connector cable-length value}`	Specifies the source for pulse per second (PPS) (default is `ptp_port`). If you specify `ptp_connector`, you can also specify a maximum cable length, in meters, for the distance between the system chassis and the PTP receiver (1-300m, default 100m).
`sync_interval number`	Configures the synchronization interval (0-8 to 2, default 0).
`transport {ethernet	udp}`	Specifies the transport type for PTP messages (Ethernet or UDP, default UDP).
`telecom {enable	disable}`	Enable or disable the telecom profile.

Mode

Configuration

Examples

```
PFOS(config)# ptp enable pps_source gps_port
PFOS(config)# ptp disable
PFOS(config)# ptp enable announce_msg_interval 2 announce_recv_timeout 5
delay_mechanism peer_peer pps_source pps_connector
PFOS(config)# ptp cable_length 150
```

radius-server

Specify a RADIUS server for user authentication.

Prerequisites:

- If using a RADIUS server with FIPS or Common Criteria modes, refer to "CLI Remote Authentication with FIPS or Common Criteria Modes Enabled" in the *PFOS User Guide* prior to adding the server.
- A RADIUS certificate must be installed **prior** to enabling TLS.
- PFOS cannot support the semicolon (;) or backslash (\) characters in passwords for external authentication through RADIUS even though these special characters may be supported at the authentication server.

Syntax

```
radius-server host:IP address key value port port-number retransmit
 number timeout number protocol protocol
```

Options

host:IP address	IP address or a fully qualified domain name to identify the server. Note that you must have a valid DNS server configuration to be able to configure hostnames. **Note:** If enabling TLS, PFOS requires the fully qualified domain name.
key *value*	For UDP, this is the AES encrypted string to authenticate to the server. RADIUS keys have the following limitations: • Backslash "\" characters in keys must be entered as a double backslash "\\". For example, the key "test\123" must be entered as "test\\123". • Keys cannot start with "$8$". For example, key "$8$TestKey" is not supported. For TLS, PFOS ignores this field and uses an internally defined key. **Note:** PFOS does not overwrite any existing key used for UDP; users can leave the key in case they want to use UDP in the future.
port *port-number*	Port for access to the server (default 0).
retransmit *number*	For UDP, this is the number of times PFOS attempts to contact the server (valid values are 1-10; default is 3). For TLS, this field is not applicable. PFOS ignores any user configured retransmit value.
timeout *number*	Time after which requests to the server time out (default 30 seconds).
protocol	Transport protocol: UDP or TLS. A RADIUS certificate must be installed **prior** to enabling TLS; see "Maintaining Certificate Files" in the *PFOS User Guide* for details. **Note:** PFOS supports RADIUS over TLS functionality when Common Criteria mode is enabled; however, this functionality is not compliant to Common Criteria requirements.

Mode

Configuration

Examples

```
PFOS(config)# radius-server 10.20.30.40 key abcdefg port 11111
retransmit 2 timeout 5 protocol tls
```

redundancy

Configure redundancy manual switchover or DB Sync.

Syntax

```
redundancy force-switchover
redundancy force-db-sync
```

Options

`force-switchover`	Initiate a manual switchover from the active management card to the standby management card. Once issued, another switchover cannot be started until a stable standby management card is available.
`force-db-sync`	Available only on PFS6010 systems. This option is only enabled when the Redundancy Status is **upgrade needed**; it is disabled for all other Redundancy states. DB Sync should be performed prior to rebooting the active CPU during software upgrade to avoid system malfunction.

Mode

Operational, Configuration

Examples

```
PFOS# redundancy force-switchover
Are you sure? [no,yes] yes
Mgmt card force-switchover is initiated.

VB6000# redundancy force-db-sync
Are you sure? [no,yes] yes
Manual DB sync initiated.
```

role

Configure user roles. A separate command instance is required for each role, rule, and feature. See Configure Access Control for information on setting up user accounts.

Note: Users not associated with a role will not have permission to read, write, or execute any commands after logging in. Local users without a role assigned to them only have permission to change their local password after login.

Syntax

```
role role-name description value rule rule-name feature area
   access { create | delete | exec | read | update }
   context { all | cli | webui | netconf }
```

Options

`role role-name`	Name to identify the role. **Notes:** • Role names support upper and lower case alphanumeric ASCII characters, limited special characters, and spaces (avoid leading and trailing spaces). • Role names used in remote authorization cannot be numerical-only (for example, a role named "1234" is not supported for remote authorization.
`description value`	Description of the role.
`rule rule-name`	Name to identify the rule.

`feature area`	Functional area included in the rule. If `area` has more than one word, enclose the string in double quotes ("") or use the backslash character before the space, as shown in the Examples. Valid values for `area` are:
	`Access Control`
	`Advanced Applications`
	`All`
	`Features`
	`File Management`
	`Filter`
	`LCD`
	`Load Balance`
	`Load Balance Criteria`
	`Logging`
	`nCM`
	`NMS`
	`Network Data`
	`Notifications`
	`Password management`
	`pMesh`
	`Port Groups`
	`Ports`
	`Powersafe`
	`Rollback`
	`SNMP`
	`System`
	`Timing Source`
	`Tool Chain`
	`Trace log`
	`Traffic Maps`
	`Triggers`
	`Tunnel`
	`VLAN Settings`
	Note: Users with **only** the Password management feature are not able to change other users' passwords in the Web UI (only via other interfaces such as the CLI).

`access [ create | delete | exec | read | update ]`	Type of access. Use commas (with no spaces) to specify multiple access types, as in the example on this page.
`context [ all | cli | webui | netconf ]`	Context to which the access applies.

Mode

Configuration

Examples

```
PFOS(config)# role role1 description "oper1" rule ruleA feature "Load
Balance" access create,read,delete context cli

PFS(config)# role pw_role_cli rule pw_rule feature Password\ management
context cli access create,read,delete,exec,update

PFS(config)# role pw_role_api rule pw_rule feature "Password management"
context netconf access create,read,delete,exec,update
```

rollback

Each time configuration changes have been saved, a rollback file is created containing the changes made since the last time they were saved. The rollback command enables users to load a previously saved configuration. When loaded, the changes stored in the selected rollback file are reverted.

Note: The rollback command can only be executed by users who have at least one role that has a rule for feature “All” or feature "Rollback" (see `role` command).

Syntax

```
rollback configuration
rollback selective number
```

Options

`configuration`	Roll back database to most recent committed version. Type ? for the list of previously saved configurations.
`selective` *`number`*	Apply a specific previously saved configuration by entering the corresponding number. Type ? for the list of previously saved configurations.

Mode

Configuration

Examples

```
PFOS(config)# rollback configuration ?
Possible completions:
  0      2021-11-12 14:52:55 by admin via webui
  1      2021-11-12 14:46:58 by admin via cli
  2      2021-11-12 14:46:50 by admin via cli
  3      2021-11-12 14:46:47 by System_Internally via system
  4      2021-11-12 14:46:47 by admin via webui
  5      2021-11-12 14:46:45 by admin via webui
  6      2021-11-12 14:46:44 by admin via maapi
  7      2021-11-12 14:46:41 by admin via maapi
  8      2021-11-12 14:46:41 by admin via maapi
  9      2021-11-12 14:46:39 by admin via maapi
  10     2021-11-12 14:46:38 by admin via webui
  11     2021-11-12 14:39:46 by admin via maapi
  12     2021-11-12 14:39:37 by admin via maapi
  13     2021-11-12 14:39:34 by System_Internally via system
  14     2021-11-12 14:39:34 by admin via maapi
  15     2021-11-12 14:39:32 by admin via maapi
  16     2021-11-12 14:39:31 by admin via maapi
  17      2021-11-12 14:39:28 by admin via maapi
  18      2021-11-12 14:39:28 by admin via maapi
  19      2021-11-12 14:39:27 by admin via maapi
  20      2021-11-12 14:39:27 by admin via maapi

PFOS(config)# rollback configuration

PFOS(config)# rollback selective ?
Possible completions:
  0       2021-11-12 14:52:55 by admin via webui
  1       2021-11-12 14:46:58 by admin via cli
  2       2021-11-12 14:46:50 by admin via cli
  3       2021-11-12 14:46:47 by System_Internally via system
  4       2021-11-12 14:46:47 by admin via webui
  5       2021-11-12 14:46:45 by admin via webui
  6       2021-11-12 14:46:44 by admin via maapi
  7       2021-11-12 14:46:41 by admin via maapi

  8       2021-11-12 14:46:41 by admin via maapi
  9       2021-11-12 14:46:39 by admin via maapi
  10      2021-11-12 14:46:38 by admin via webui

  11      2021-11-12 14:39:46 by admin via maapi

  12      2021-11-12 14:39:37 by admin via maapi
  13      2021-11-12 14:39:34 by System_Internally via system
  14      2021-11-12 14:39:34 by admin via maapi
  15      2021-11-12 14:39:32 by admin via maapi
  16      2021-11-12 14:39:31 by admin via maapi
  17      2021-11-12 14:39:28 by admin via maapi
  18      2021-11-12 14:39:28 by admin via maapi
  19      2021-11-12 14:39:27 by admin via maapi
  20      2021-11-12 14:39:27 by admin via maapi

PFOS(config)# rollback selective 4
```

snmp

Configure SNMP settings.

Syntax

```
snmp agent agent-options
snmp community community-options
snmp notify notify-options
snmp target target-options
snmp usm usm-options
snmp vacm vacm-options
```

Options

`agent-options`	`enabled`
	Enable SNMP.
	`disabled`
	When SNMP is disabled, PFOS does not reply to SNMP get/set operations, and no traps are received.
	`version { v1 | v2c | v3 }`
	Configure SNMP agent version. All three versions are enabled by default. To disable a version, use the no form of this command. Any or all versions can be specified, separated by spaces.
	`max-message-size byte-count`
	Specify the SNMP packet size permitted when the SNMP server is receiving a request or generating a reply. Valid values are integers between 484 and 214748364; the default is 50000. To restore the default value, use the `no` form of this command.

`community-options`	`community-string` Community string that acts like a password and permits access to SNMP. Valid string length is between 1 and 32 characters. To remove the specified community string, use the `no` form of this command.
`notify-options`	`notify-name tag tag-list type trap` Specifies the tag values to be used by the targets that will receive SNMP notifications. Use the `no` form of this command to remove the specified notify entry. `notify-name` – Unique name that identifies the notify entry. `tag-list` – value used to select targets.

`target-options`	`target-name {`
	`ip ip-address |`
	`tag tag-name |`
	`udp-port port-num |`
	`usm { sec-level { auth-no-priv |`
	`no-auth-no-priv |`
	`auth-priv }`
	`user-name username } |`
	`v1 sec-name security-name |`
	`v2c sec-name security-name`
	`}`
	Specifies the recipient of an SNMP notification operation. Use the `no` form of this command to remove the specified host.
	`target_name` – Unique target name
	`ip-address` – IP address of the trap receiving host
	`tag-name` – List of tag values used to select target address
	`port-num` – User Datagram Protocol (UDP) port of the host to use. The default is 162.
	`v1
		v2c	usm` – Version of SNMP used to send the traps
			`auth-no-priv
				no-auth-no-priv	auth-priv` – Security level
					`username` – USM username
					`security-name` – v1 or v2c security name

`usm-options`	`user username {` `auth { md5	sha } password pwd-string	` `priv { aes	des } password pwd-string` `}` Configure an SNMP v3 user to permit access to SNMP. To remove the specified v3 user, use the no form of this command. `auth` – Specifies authentication of a packet `md5` – The HMAC-MD5-96 authentication level `sha` – The HMAC-SHA-96 authentication level `priv` – Specifies authentication of a packet with encryption. `aes` – The CFB128-AES-128 Privacy Protocol level `des` – CBC-DES Symmetric Encryption Protocol level `pwd-string` – Authentication password that enables the agent to receive packets from the host

`vacm-options`	`group group-name {`
	`    access { any | v1 | v2c | usm }`
	`        { auth-no-priv | auth-priv |`
	`            no-auth-no-priv }`
	`        notify-view notifyview`
	`        read-view readview`
	`        write-view writeview |`
	`    member security-name`
	`        sec-model { v1 | v2c | usm }`
	`}`
	Configure a new SNMP group that maps SNMP users/community to SNMP views. To remove a specified SNMP group, use the no form of this command.
	`group_name` – The name of the group
	`any | v1 | v2c | usm` – security models
	`no-auth-no-priv` – no authentication no encryption of a packet
	`auth-no-priv` – authentication of a packet without encrypting it
	`auth-priv` – authentication of a packet with encryption
	`notifyview` – A string (not to exceed 32 characters) that is the name of the view that enables you to specify a notify trap
	`readview` – A string (not to exceed 32 characters) that is the name of the view that enables you only to view the contents of the agent
	`writeview` – A string (not to exceed 32 characters) that is the name of the view that enables you to enter data and configure the contents of the agent
	`view view-name`
	`subtree oid-tree [ included | excluded ]`
	Configure a view entry. To remove this entry, use the `no` form of this command.
	`view-name` – Label for the view record that you are updating or creating.
	`oid-tree` – Object identifier of the ASN.1 subtree to be included or excluded from the view. To identify the subtree, specify a text string consisting of numbers, such as 1.3.6.2.4. Replace a single subidentifier with the asterisk (*) wildcard to specify a subtree family; for example, 1.3.*.4.
	`included | excluded` – Type of view. You must specify either included or excluded.

Mode

Configuration

Examples

```
PFOS(config)# snmp agent enable

PFOS(config)# snmp community private
PFOS(config-community-private)# end
PFOS# show running-config snmp community
snmp community private
!
snmp community public
```

```
!

PFOS(config)# snmp notify new_notify tag v2_trap type trap
PFOS# show running-config snmp notify
snmp notify new_notify
 tag  v2_trap
 type trap
!
snmp notify std_v2_trap
 tag  std_v2_trap
 type trap
!
snmp notify std_v3_trap
 tag  std_v3_trap
 type trap
!

PFOS(config)# snmp target new v2c sec-name private
Value for 'snmp target new ip' (<IP address>): 143.63.105.66
PFOS(config-target-new)# udp-port 3000
PFOS(config-target-new)# tag std_v2_trap
PFOS# show running-config snmp target
snmp target new
ip       143.63.105.66
udp-port 3000
tag      [ std_v2_trap ]
v2c sec-name private
!

PFOS(config)# snmp usm user alice auth md5 password foobar123
PFOS(config-user-alice)# priv aes password 123foobar
PFOS(config-user-alice)#
PFOS# show running-config snmp usm
snmp usm user alice
auth md5 password $3$nN/6OQgJUFDe1SpF2EC9iA==
 priv aes password $3$tZ6KtIp268two2bLpEth8Q==
!

PFOS(config)# snmp vacm group usm_new member alice sec-model usm
PFOS(config)# snmp vacm group new_1 member private sec-model v2c

PFOS# show running-config snmp vacm
snmp vacm group all-rights
 member public
  sec-model [ v1 v2c usm ]
 !
 member remote
  sec-model [ usm ]
 !
 access any no-auth-no-priv
  read-view   internet
  write-view  internet
  notify-view internet
 !
!
snmp vacm group new_1
 member private
  sec-model [ v2c ]
 !
 access any no-auth-no-priv
  read-view   internet
  write-view  internet
  notify-view internet
 !
!
snmp vacm group usm_new
 member alice
  sec-model [ usm ]
 !
 access usm auth-no-priv
  read-view   internet
  write-view  internet
  notify-view internet
 !
!
snmp vacm view internet
 subtree 1.3.6.1
  included
 !
!
```

snmp-server

Enable or disable SNMP traps. For details on SNMP traps, see the “SNMP MIB and Trap Definitions” section in the *PFOS User Guide*.

Syntax

```
snmp-server enable traps { all | linkUpDown | system system-traps |
   snmp coldstart }
```

To disable SNMP traps, use the `no` form of the command:

```
no snmp-server enable traps [ all | linkUpDown | system system-traps |
   snmp [ coldstart ] ]
```

Note: The `linkUpDown` traps (link Down and link Up Objects in standard IF-MIB) and the `enhanced-linkUpDown` system traps (vsLinkUpNotif and vsLinkDownNotif in proprietary VSS-SYSTEM-MIB) are similar traps, but the `enhanced-linkUpDown` system traps have two additional trap components: PFOS port number (such as, “1-13”), and the user-assigned name for the port. Due to their similarity, it is not necessary to enable both sets of traps; enable the best option for your network. For details on SNMP traps, see the “SNMP MIB and Trap Definitions” section in the *PFOS User Guide*.

Options

`all`	Enable all SNMP traps. With `no` prefix: Has no effect.
`linkUpDown`	Enable the linkUpDown traps (link Down and link Up Objects in standard IF-MIB). With `no` prefix: Disable the standard SNMP IF-MIB linkUpDown traps.

`system` *`system-traps`*	Enable the specified proprietary SNMP VSS-SYSTEM-MIB trap(s). You can include one or more values for *`system-traps`*, separated by spaces. Valid values for *`system-traps`* are: `access`: Enable SNMP system access trap `access-snmp`: Enable SNMP system snmp access trap `all`: Enable SNMP all VSS-SYSTEM-MIB traps `config-change`: Enable SNMP system configuration change trap `enhanced-linkUpDown`: Enable the enhanced LinkUpDown traps (vsLinkUpNotif and vsLinkDownNotif in proprietary VSS-SYSTEM-MIB). `file-mgmt`: Enable SNMP system file management trap `fru`: Enable SNMP system FRU (Field Replaceable Unit) trap `health-check-state`:Enable SNMP system health check state trap `health-stats`: Enable SNMP system health stats trap `high-availability`:Enable SNMP system high availability trap `pfsMesh`:Enable SNMP system pfsMesh trap `restart`: Enable SNMP system restart trap `stripping`: Enable SNMP system stripping trap `temperature`: Enable SNMP system temperature trap `trigger-policy`: Enable SNMP system trigger policy trap `tunnel-state`: Enable SNMP system tunnel state trap With `no` prefix: Disable the specified trap(s), or disable all system traps if no trap is specified.
`snmp coldstart`	Enable the SNMP SNMPv2-MIB coldStart trap. With `no` prefix: Disable the SNMP SNMPv2-MIB coldStart trap.

Mode

Configuration

Examples

Enable specific traps:

```
PFOS(config)# snmp-server enable traps snmp coldstart
PFOS(config)# snmp-server enable traps system config-change
PFOS(config)# snmp-server enable traps system pfsMesh
PFOS(config)# snmp-server enable traps high-availability
```

Enable all system traps:

```
PFOS(config)# snmp-server enable traps system all
```

Enable link state up/down traps (based on standard IF-MIB):

```
PFOS(config)# snmp-server enable traps linkUpDown
```

Enable enhanced link state up/down traps (based on proprietary VSS-SYSTEM-MIB):

```
PFOS(config)# snmp-server enable traps system enhanced-linkUpDown
```

Disable all SNMP traps:

```
PFOS(config)# no snmp-server enable traps snmp
```

Disable all system traps:

```
PFOS(config)# no snmp-server enable traps system
```

Disable all traps:

```
PFOS(config)# no snmp-server enable traps
```

system

Configure system name, location, and contact.

Syntax

```
system name system-name
system contact contact-name
system location location-name
```

Options

`name system-name`	Name to identify the system.
`location location-name`	System location
`contact contact-name`	Contact for the system. This is a free-form string that the system reports when queried. It is not used by any other process.

Mode

Configuration

Examples

```
PFOS(config)# system name vb6000_b1 location building1 contact
ssmith@example.com
```

system-alarms

Configure the acknowledge field of an alarm unit.

Syntax

```
system-alarms [ alarm-unit ] acknowledge { true | false }
```

Options

`alarm-unit`	Name to identify the alarm unit. Press `?` for a list of available alarm units.
`acknowledge`	Set the value of the acknowledge field for the specified alarm unit. Valid values are `true` and `false`.

Mode

Configuration

Examples

```
PFOS(config)# system-alarms volt-10 acknowledge true
```

system banner

This feature allows you to create a custom banner to be seen by users when they log in to the CLI or Web UI. You can notify users of your corporate IT policies or communicate other important messages to all users system-wide.

Syntax

```
system banner message
```

To disable the system banner, use the `no` form of the command:

```
no system banner
```

Options

`message`	Text message up to 4000 characters in length using quotes.

Mode

Configuration

Examples

```
PFOS(config)# system banner "Access to electronic resources in this system
is restricted to authorized users. Use of this system is subject to all
policies and procedures set forth by its owner. Unauthorized use is
prohibited.”
```

```
PFOS(config)# system banner "Testing in progress. Please contact UI Team”
```

system notes

This feature allows you to add additional device, location, or contact details to a PFS configuration. You can use `show running-config system notes` to view the notes.

Syntax

Single Line Input

```
system notes "message"
```

Multiple Line Input

```
system notes <Return>
(<string, min: 0 chars, max: 4000 chars>):
[Multiline mode, exit with ctrl-D.]
```

Disable

```
no system notes
```

Options

`"message"`	Single Line input Enter text message using quotes; maximum 4000 characters.

`<Return>`
`message`
	Multiple Line Input
	Press the Enter key to enter multiline mode and enter text message without using quotes. Maximum 4000 characters.
	Press Ctrl-D to exit the multiline mode.

Mode

Configuration

Examples

```
PFOS(config)# system notes "Contact j.smith@netscout.com or mobile: 972-555-3245"
```

```
PFOS(config)# system notes
(<string, min: 0 chars, max: 4000 chars>):
[Multiline mode, exit with ctrl-D.]
> Location:
>   123 Circle Drive
>   San Jose
> Site Contact:
>   j.smith@netscout.com
>   mobile: 972-555-3245
> Hardware Lab
>   Rack 6B
>   RU 13-14
```

tacacs-server

Specify a TACACS server for user authentication.

Note:

- If using a TACACS server with FIPS or Common Criteria modes, refer to "CLI Remote Authentication with FIPS or Common Criteria Modes Enabled" in the *PFOS User Guide* prior to adding the server.
- PFOS cannot support the semicolon (;) or backslash (\) characters in passwords for external authentication through TACACS even though these special characters may be supported at the authentication server.

Syntax

```
tacacs-server address key value port port-number prompts
   value service value retransmit number timeout number
```

Options

`address`	IP address of the TACACS server.
`key value`	AES encrypted string to authenticate to the server. TACACS keys have the following limitations: • Backslash "\" characters in keys must be entered as a double backslash "\\". For example, the key "test\123" must be entered as "test\\123". • Keys cannot start with "$8$". For example, key "$8$TestKey" is not supported.
`port port-number`	Port for access to the server (default 49).
`prompts value`	TACACS prompts parameter.
`service value`	TACACS service parameter.
`retransmit number`	Number of times the system attempts to contact the TACACS server (default 3).
`timeout number`	Time after which requests to the server time out (default 30 seconds).

Mode

Configuration

Examples

```
PFOS(config)# tacacs-server 192.168.2.3 key abc port 45 prompts 123
service xyz retransmit 5 timeout 60
```

tracelog

Configure settings for tracelog.

Syntax

```
tracelog level facility severity
```

Options

facility	Area covered by the settings: One of access-control, app-libs, chassis, flowmapper, hal, lcd, load-balance, notif-mgmt, port-mgmt, snmp, stats-collector, switch-mgmt, system-mgmt.
severity	Log level: One of alert, critical, debug, emergency, error, info, notification, warning.

Mode

Configuration

Examples

```
PFOS(config)# tracelog level access-control warning
```

username

Configure user accounts and passwords. See tacacs-server, radius-server, and ldap-server for information on setting up connections to remote servers for authentication.

Note: Users without access policy permissions can use the passwd command to change their own password.

Syntax

```
username user-name password password confirm-password password
   role rolename
no username user-name
```

Options

user-name	Name of the user account. To delete a username from the system, use the no form of this command. **Notes**: • User names support upper and lower case alphanumeric ASCII characters and limited special characters. User names cannot contain spaces. • The *admin* user cannot be deleted. If PFS Fabric Manager is in use, the *pfmadmin* user should not be deleted.
password *password*	Password for the account (compliant with defined password policies). Single quote (‘) and double quote (“) characters cannot be used as special characters as part of password string. To define passwords with special characters in CLI, the password string needs to be surrounded by double quotes.
confirm-password *password*	Password confirmation (must enter the same password).
role *rolename*	Specify a previously defined role. See role. **Notes:** • Role names support upper and lower case alphanumeric ASCII characters, limited special characters, and spaces (avoid leading and trailing spaces). • Role names used in remote authorization cannot be numerical-only (for example, a role named "1234" is not supported for remote authorization). • Users not associated with a role will not have permission to read, write, or execute any commands after logging in. Local users without a role assigned to them only have permission to change their local password after login.

Mode

Configuration

Examples

```
PFOS(config)# username ssmith role Operator password 12345 confirm-
password 12345
```

Defining Special Characters

```
PFOS(config)# username ssmith password "asdf!" confirm-password "asdf!"
```

Delete a User

```
PFOS(config)# no username ssmith
```

6 Base Feature Commands

This chapter contains command reference pages for the base feature set. For additional examples on using these commands, see Configuration Task Flow.

Commands include:

app-lib healthcheck

filter

lb-criteria

load-balance

map

merge-maps

port-group

toolchain group

trigger

app-lib healthcheck

Create a new health check library for use with Inline Monitor port groups.

Syntax

```
app-lib healthcheck hc-name
    { return return-info | noreturn noreturn-info }
    [ destination-mac-address mac-addr ]
    [ filter-expression filter ] [ payload payload-str ]
    [ transmit-rate tx-time  ] [ wait-time wait-time ]
```

Options

`hc-name`	Name of health check library to create. Maximum length is 64 characters.
`return`	Specify for a positive health check.
`noreturn`	Specify for a negative health check.
`mac-addr`	Destination MAC address in hexadecimal format, such as `ff:ff:ff:ff:ff:ff`.
`filter`	Filter expression to match returned health check packets. See the *PFOS User Guide* for information and examples on creating filter expressions.
`payload-str`	Health check payload. Must be a 232-digit hexadecimal string. The default value is `08` followed by 230 zeros.
`tx-time`	Transmit rate, in milliseconds. Valid values are 200 to 4294967295. The default value is 10000 milliseconds.
`wait-time`	Number of milliseconds to wait for a response. Valid values are 200 to 4294967295. Valid only when `return return-info` is specified. `wait-time` cannot be greater than or equal to `tx-time`. The default value is 500 milliseconds.

Mode

Configuration

Examples

```
PFOS(config)# app-lib healthcheck hc1 return return-info destination-
mac-address 01:aa:bb:cc:dd:ee filter-expression "ip protocol 6"
transmit-rate 5000 wait-time 2000

PFOS(config)# app-lib healthcheck hc2 noreturn noreturn-info
destination-mac-address 02:aa:bb:cc:dd:ee transmit-rate 20000
```

To create a health check with actions for both positive and negative results, use two commands:

```
PFOS(config)# app-lib healthcheck hc2 return return-info destination-
mac-address 01:aa:bb:cc:dd:ee filter-expression "ip protocol 6"
transmit-rate 20000 wait-time 5000
PFOS(config)# app-lib healthcheck hc2 noreturn noreturn-info
destination-mac-address 02:aa:bb:cc:dd:ee transmit-rate 20000
```

```
PFOS(config)# show app-lib healthcheck
       GROUP
NAME   NAME
--------------
hc2
```

filter

Configure entries for the forwarding filters library.

Syntax

```
filter filter-name expression string [type traffic]
```

Options

`filter-name`	Name to identify the filter.
`expression string`	Expression that defines the filter. See the *PFOS User Guide* for information and examples on creating filter expressions.
`type traffic`	Optional (`traffic` is the only currently supported type).

Mode

Configuration

Examples

```
PFOS(config)# filter jm_test expression "ip protocol 6 and tcp
destination port 80"
PFOS(config-filter-jm_test)#
```

The `extvlan` filter is used in PFS/PFX inner load balancing configurations. Refer to "PFS+PFX Inner Filtering and Inner Load Balancing" in the *PFOS User Guide* for details.

```
PFOS(config)# filter extvlanfilter1 expression "extvlan 100"
PFOS(config-filter-filter1)# end
```

lb-criteria

Configure global settings and custom hash settings for load balancing. Refer to feature for hash alogrithm and custom hash configuration details. For details about how to associate lb-criteria to a traffic map, refer to map.

Syntax

Header

```
lb-criteria name src-port {exclude | include} layer2 {enable | disable}
[layer2_header_keys value]
lb-criteria name src-port {exclude | include} mpls {enable | disable}
[mpls_header_keys value]
lb-criteria name src-port {exclude | include} layer3 {enable | disable}
[layer3_header_keys value]
lb-criteria name src-port {exclude | include} layer4 {enable | disable}
[layer4_header_keys value]
```

Inner Header

```
lb-criteria name src-port {exclude | include} inner-header-criteria
layer2 {enable | disable} [layer2_header_keys value]
lb-criteria name src-port {exclude | include} inner-header-criteria
layer3 {enable | disable} [layer3_header_keys value]
lb-criteria name src-port {exclude | include} inner-header-criteria
layer4 {enable | disable} [layer4_header_keys value]
```

Custom Criteria

```
lb-criteria name custom-criteria type <l2 | l3 | l4 > offset <0-127>
length <1-4>
```

Options

`name`	Name to identify the load balance criteria.
`src-port {exclude	include}`	Include or exclude the physical source port number as an entry for the hashing algorithm. Including the source port results in the best traffic distribution, but is not appropriate if you have asymmetric traffic links. Default: include.
Header Options	
`layer2 {enable	disable}` `mpls {enable	disable}` `layer3 {enable	disable}` `layer4 {enable	disable}`	Headers with the value enable become available choices for the hashing algorithm's use on a traffic map that has a load balance group as an output. Default: disable.

`layer2_header_keys value`
`mpls_header_keys value`
`layer3_header_keys value`
`layer4_header_keys value`
	Optionally specify additional options for the header. These are used in the hashing algorithm and are the same for all traffic maps for which you select the load balance criteria. Use commas to specify multiple values, as in the example.
	Layer 2 header key options: `Destination_MAC_address`, `Ethertype`, `Source_MAC_address`
	MPLS header key options: `Label 1`, `Label 2`, `Label 3`
	Layer 3 header key options: `Destination_IP_address`, `Source_IP_address, IP Protocol`
	Layer 4 header key options: `Destination_port`, `Source_port`

Inner Header Options (**PFS 7040-32D and 7041-32D Only**)	
`inner-header-criteria`	Configuration parameters for inner header load balancing for L2GRE, L3GRE, L3 MPLS and VXLAN packets. **Note:** Inner header criteria configuration is only supported for L2GRE, L3GRE, L3 MPLS and VXLAN packets; existing load balance criteria is not affected.

`layer2 {enable | disable}`
`layer3 {enable | disable}`
`layer4 {enable | disable}`
	Inner headers with the value enable become available choices for the hashing algorithm's use on a traffic map that has a load balance group as an output. Default: disable.

`layer2_header_keys value`
`layer3_header_keys value`
`layer4_header_keys value`
	Optionally specify additional options for the inner header. These are used in the hashing algorithm and are the same for all traffic maps for which you select the load balance criteria. Use commas to specify multiple values, as in the example.
	Layer 2 inner header key options: `Destination_MAC_address`, `Ethertype, Source_MAC_address`
	Layer 3 inner header key options: `Destination_IP_address`, `Source_IP_address, IP Protocol`
	Layer 4 inner header key options: `Destination_port`, `Source_port`

Custom Criteria Options	
`custom-criteria type`	Custom Hash starting offset point: L2, L3, or L4.
`offset`	Offset of first byte to be used in hash (0-127 bytes), starting from the header specified in `custom-criteria type`.
`length`	Field length of packet to be used in hashing mechanism (1 to 4 bytes).

Mode

Configuration

Examples

```
PFOS(config)# lb-criteria L2 layer2 enable layer2_header_keys
Destination_MAC_address,Source_MAC_address
PFOS(config)# lb-criteria lc1 mpls enable mpls_header_keys
label,label2,label3
PFOS(config)# lb-criteria lc3 mpls enable mpls_header_keys label,label2
layer3 enable layer3_header_keys Destination_IP_address,Source_IP_
address,IP_Protocol
```

```
PFOS(config)# lb-criteria lbc_ih inner-header-criteria layer2 enable
layer2_header_keys Ether type
PFOS(config)# lb-criteria lbc-ih inner-header-criteria layer3 enable
layer3_header_keys IP_Protocol
PFOS(config)# lb-criteria lbc_ih inner-header-criteria layer4 enable
layer4_header_keys Source_port

PFOS(config)# lb-criteria lbg-custhash custom-criteria type l2 offset 68
length 4
```

load-balance

Set up load balancing groups. Load balancing groups provide a structured method for defining one or more load balancing groups of ports or tunnels and how these groups behave when one or more tools or ports/tunnels go down or become unavailable.

Note: Ports and tunnels cannot be in same load balance group.

Syntax

Load Balancing - Ports

```
load-balance group-name ports port-list failover_action {drop |
rebalance | redistribute | RoundRobin | WeightedRedistribute} [type
monitor]
```

Load Balancing - Ports (Weighted)

```
load-balance group-name ports port-list failover_action
WeightedRedistribute port-weight port weight weight
```

Load Balancing - Tunnels

```
load-balance group-name tunnels [list of tunnels] failover_action
   {rebalance | redistribute} [type monitor]
```

Load Balancing - PFX

```
load-balance group-name pfx
no load-balance group-name pfx
```

Options

`group-name`	Name to identify the load balancing group.
`ports port-list`	Ports to include in the group. Use `[ a-b c-d e-f ]` format (with spaces as shown) to specify multiple ports.

`failover_action`	Action to take if a member of the group is not available: • **Rebalance** - (Default) rebalance the load among the remaining active group members - *traffic will be disturbed*. If the load balance group will be used in a map with a custom hash load balance criteria, Rebalance failover is recommended. • **Redistribute** - redistribute the offline traffic to the remaining group members, without disturbing the traffic on the remaining active members. • **Drop** - Drop the traffic for the offline group member – traffic is not rebalanced or redistributed. This option is not available for tunnel load balancing. • **RoundRobin** - evenly distribute the online traffic among load balanced ports. PFOS forwards packets in the order they are received to each active port, in a rotating, sequential manner. This option is not available for tunnel load balancing. Refer to the *PFOS User Guide* for details about Round Robin limitations and configuration considerations. • **WeightedRedistribute** - (**this option is only available for load balanced ports and not applicable for PFS 6000 Series**) distribute the traffic to remaining load balance weighted ports, without disturbing the traffic. Refer to the ***PFOS 6.x User Guide*** for details about how PFOS calculates distribution percentage.
`port-weight`	**This option is only valid when `failover action` value is `WeightedRedistribute`.** Specific port in the group to which you want to assign a weight.
`weight`	**This option is only valid when `failover action` value is `WeightedRedistribute`.** Weight assigned to the specific port used to determine the distribution of traffic forwarded to the port.
`tunnels [list of tunnels]`	**This feature requires the PFS 7000 functionality license.** Specify a list of configured GRE or VXLAN tunnels to distribute traffic.
`type monitor`	Optional load balance group type (`monitor` is the only currently supported type).
`pfx`	This option is used in PFS/PFX inner load balancing configurations. Refer to "PFS+PFX Inner Filtering and Inner Load Balancing" in the *PFOS User Guide.* • **Enabled**: Distribution of traffic is based on VLAN tags added by PFX appliance (vlan-id 4001 to 4016, which is added as outer-vlan-id by PFX). • **Disabled**: Normal load-balance group functionality.

Mode

Configuration

Examples

Load Balancing - Ports

```
PFOS(config)# load-balance lbg4 ports [ 8-3 8-4 9-5 ] failover_action
Drop
PFOS(config)# load-balance RRlbg ports [ 8-3 8-4 9-5 ] failover_action
RoundRobin
```

Load Balancing - Ports (Weighted)

```
load-balance lbg1 failover_action WeightedRedistribute ports [ 1-1 1-2
1-3 ] port-weight 1-1 weight 20
load-balance lbg1 failover_action WeightedRedistribute ports [ 1-1 1-2
1-3 ] port-weight 1-2 weight 30
load-balance lbg1 failover_action WeightedRedistribute ports [ 1-1 1-2
1-3 ] port-weight 1-3 weight 50
```

Load Balancing - Tunnels

```
PFOS(config)# load-balance lbg1 tunnels [ gre1 gre2 ]
```

Load Balancing - PFX

```
PFOS(config)# load-balance PFX_LBG pfx
```

map

Map Commands

- Map Creation Commands
- Map Commands for GRE or VXLAN Tunnel Origination/Termination

Map Creation Commands

Define traffic maps. Before defining maps, configure ports (see interface) and set up any filters, port groups, load balance criteria, load balance groups, and mirror sessions first.

Syntax

```
map [name] action [drop | forward]
map [name] description
map [name] disable
map [name] enable
map [name] filter filter-name
map [name] input-tunnels tunnel-name
map [name] input_ports port-num
map [name] lb_criteria criteria
map [name] mirror-session session name
map [name] mode [Basic | Extended]
map [name] monitor-port-groups mpg name
map [name] network-port-groups npg name
map [name] output-tunnels tunnel-name
map [name] output_lb_groups group-list
map [name] output_ports port-num
map [name] remote-monitor-groups remote-group-list
map [name] trigger-profile [triggerName] state
map [name] type map-type
```

Options

`name`	Name to identify the traffic map.
`action`	Action to take for filter: Drop or Forward.
`description`	Add a string description for the map.
`disable`	Disable the map.
`enable`	Enable the map.
`filter` *`filter-name`*	Specify an existing filter for the map.
`input-tunnels` *`tunnel-name`*	See Map Commands for GRE or VXLAN Tunnel Origination/Termination.

`input-ports` *`port-num`*	Source ports for this traffic map.
	To use individual ports:
	`input_ports port-list`
	To use port groups:
	`network-port-groups group-list`
	To specify more than one entry in `port-list` or `group-list`, use the format `[ item1 item2 ... ]`, where each item is either a port identifier or a network port group as appropriate.
	You can use both individual ports and port groups in the same map.

`lb_criteria` *`criteria`*	Assign pre-defined or user-defined load balancing method as defined in the load balance criteria library (see lb-criteria). **Note**: The PFX pre-defined criteria is used in maps for PFS/PFX inner load balancing configurations. Refer to "PFS+PFX Inner Filtering and Inner Load Balancing" in the *PFOS User Guide.*
`mirror-session` *`session name`*	Define the mirror session name to associate with the map.
`mode` *`map-mode`*	Type of map to create. Valid values are `Basic` (the default) and `Extended`. An Extended map allows you to use extended load balancing with this map on hardware that supports this feature.
`monitor-port-groups` *`mpg name`*	Specify the monitor port group(s) to associate with this map.
`network-port-groups` *`npg name`*	Specify the network port group(s) to associate with this map.
`output-tunnels` *`tunnel-name`*	See Map Commands for GRE or VXLAN Tunnel Origination/Termination.
`output_lb_groups` *`group-list`*	Output load balance groups for the map. Use `[ g1 g2 ... ]` format (with spaces as shown) to specify multiple groups. You can specify output ports, a load balance group and load balance criteria, or both. If you specify multiple output ports, traffic is replicated across the ports.

`output_ports`	Destination ports for this traffic map.
	To use individual ports:
	`output_ports port-list`
	To use port groups:
	`monitor-port-groups group-list`
	To specify more than one entry in `port-list` or `group-list`, use the format `[ item1 item2 ... ]`, where each item is either a port identifier or a monitor port group as appropriate.
	You can specify output ports, a load balance group and load balance criteria, or both. If you specify multiple output ports, traffic is replicated across the ports.
	You can use both individual ports and port groups in the same map.

`remote-monitor-groups remote-group-list`	One or more remote monitor port groups on other systems (not on this system) connected via pfsMesh. Specify the list of remote port groups which will be the destination for this map. Use `[ a~pg1 b~pg2 ... ]` format (with spaces as shown) to specify multiple ports, and where `a`, `b`, and `c` are the remote node IDs.
`trigger-profile` *`triggerName`*	Name of trigger whose outcome will enable this map.

`trigger-profile` *`triggerName`*`state`	Trigger state which will enable this map: active or inactive. • `active`: map will be enabled when the trigger profile is active. • `inactive`: map will be enabled when the trigger profile is inactive.
`type map-type`	Type of traffic map. Valid values are `monitor` and `inline-monitor`.

Mode

Configuration

Examples

```
PFOS(config)# map M1 enable
PFOS(config)# map M1 disable
PFOS(config)# map map3 filter unfiltered input_ports 10-9 output_lb_
groups lbgroup1 lb_criteria lbcriteria1

PFOS(config)# map custhashmap filter unfiltered lb-criteria lbg-CustHash
 input-ports [ 1-1 1-2 ] output-ports [ 1-6 1-7 ] output_lb_groups lbg-
name action forward

PFOS(config)# map map4 mode Basic input_ports [ 1-2 1-3 ] filter
unfiltered remote-monitor-groups FFB9A000_PG_A_1-5_to_1-8

PFOS(config)# map elb-map2 mode Extended filter unfiltered input_ports [
10-3 10-4 ] output_lb_groups lbgroup1 lb_criteria ELB

PFOS(config)# map newmap input_ports 5-11 network-port-groups [ ]
output_ports 5-2 monitor-port-groups [ ] filter unfiltered

PFOS(config)# map sample-map input_ports [ 1-3 1-4 ] network-port-groups
NPG1 output_ports [ 1-5 1-6 ] monitor-port-groups [ MPG-A MPG-B ] filter
unfiltered

PFOS(config)# map PFX_Return_ILBfilter nonmatch lb-criteria PFX
 input-ports 1-4 output_lb_groups PFX_InnerLB_LBG

PFOS(config)# map M1 trigger-profile TG1 state active
PFOS(config)# map M2 trigger-profile TG1 state inactive

PFOS(config)# map Traffic-Map mirror-session Mirror-Session2
PFOS(config)# do show running-config map
map Traffic-Map
type Monitor
mode Basic
filter VLAN-100
input_ports [ 1-3 1-4 ]
output_ports [ 1-10 ]
action Forward
mirror-session [ Mirror-Session2 ] !
```

Map Commands for GRE or VXLAN Tunnel Origination/Termination

Refer to the following sections for mapping traffic to and from a GRE or VXLAN tunnel:

- Mapping All Traffic from Input Port to GRE or VXLAN Tunnel
- Mapping All Traffic from GRE or VXLAN Tunnel to Output Port

Refer to the ***PFOS 6.x User Guide*** for GRE and VXLAN Tunnel Origination/Termination feature details.

Note: PFOS does not support both input tunnels and output tunnels in the same map.

Mapping All Traffic from Input Port to GRE or VXLAN Tunnel

Use the following commands to map all traffic from an input port to the GRE or VXLAN tunnel interface.

Note: When using CLI to configure a traffic map with GRE or VxLAN tunnels as input-tunnels, the selection list may not display all existing tunnel names. To complete the configuration, manually enter the existing tunnel names even though they are not in the list.

Syntax

```
map name input_ports port-num filter [filter-name] output-tunnels
tunnel-name
no map name
```

Options

name	Name to identify map.
port-num	Port on which to map traffic in <slot>-<port> format.
filter-name	Existing filter to be used on traffic (Unfiltered/Nonmatch/user filters).
tunnel-name	GRE or VXLAN tunnel to which traffic will be sent.

Mode

Configuration

Examples

```
map m1 input_ports 1-1 filter unfiltered output-tunnels gre1

map m2 input_ports 2-2 filter unfiltered output-tunnels vxlan1

no map m1
```

Mapping All Traffic from GRE or VXLAN Tunnel to Output Port

Use the following commands to map all traffic from the GRE or VXLAN tunnel interface to the output port.

Note: When using CLI to configure a traffic map with GRE or VxLAN tunnels as output-tunnels, the selection list may not display all existing tunnel names. To complete the configuration, manually enter the existing tunnel names even though they are not in the list.

Syntax

```
map name input_tunnels tunnel-name filter unfiltered output_ports Port-num
no map name
```

Options

name	Name to identify map.
tunnel-name	GRE or VXLAN tunnel from which traffic will be sent.
unfiltered	Input tunnels support only unfiltered traffic.
port-num	Port on which to map traffic in <slot>-<port> format.

Mode

Configuration

Examples

```
map m2 input-tunnels gre1 filter unfiltered output_ports 1-1

map m3 input-tunnels vxlan1 filter unfiltered output_ports 3-1

no map m1
```

merge-maps

Merge traffic maps where possible. PFOS can merge the output ports if the traffic maps have the same input port(s) and filter combination. When traffic maps are merged, PFOS performs all possible consolidations. You cannot limit the set of traffic maps that are considered for merging.

Syntax

```
merge-maps
```

Options

None

Mode

Operational, Configuration

Examples

This example creates three traffic maps with the same input port and different output ports, and then merges them into one traffic map.

```
PFOS(config)# map map1 filter unfiltered input_ports 6-4 output_ports 6-13
PFOS(config-map-map1)# map map2 filter unfiltered input_ports 6-4 output_ports 6-16
PFOS(config-map-map2)# map map3 filter unfiltered input_ports 6-4 output_ports 6-17
PFOS(config-map-map3)# show map

                            Map                                   REMOTE   OUTPUT
Map                Map      Mode               INPUT    OUTPUT    MONITOR  LB      LB
Name  DESCRIPTION  Type     Type   FILTER      PORTS    PORTS     GROUPS   GROUPS  CRITERIA
---------------------------------------------------------------------------------------------
map1  -            Monitor  Basic  unfiltered  [ 6-4 ]  [ 6-13 ]  -        -       -
map2  -            Monitor  Basic  unfiltered  [ 6-4 ]  [ 6-16 ]  -        -       -
map3  -            Monitor  Basic  unfiltered  [ 6-4 ]  [ 6-17 ]  -        -       -

PFOS(config-map-map3)# merge-maps
PFOS(config-map-map3)# show map

                            Map                                             REMOTE   OUTPUT
Map                Map      Mode               INPUT                        MONITOR  LB
LB
Name  DESCRIPTION  Type     Type   FILTER      PORTS    OUTPUT PORTS        GROUPS   GROUPS
CRITERIA
---------------------------------------------------------------------------------------------
----------
map1  -            Monitor  Basic  unfiltered  [ 6-4 ]  [ 6-13 6-16 6-17 ]  -        -
```

port-group

Create a port group for use with traffic maps. Before configuring a port group, configure the applicable ports (see interface.)

Syntax

```
port-group monitor group-name [ ports port-list |
    [ lb-criteria criteria |
    load-balance-groups lbg-list |
    pmesh [ enable | disable ] ]

port-group network group-name [ common-vlan vlan-id ]
    [ consolidate [ enable | disable ] ] ports port-list

port-group inline-monitor group-name port-pair portid-a
    b-port portid-b [ a-health-monitor-library a-hc-name ]
    [ b-health-monitor-library b-hc-name ] [ link-safe [ enable
| disable ] ] weight [weight]

port-group inline-network group-name Vlan-tag vlan-tag option power-safe
port-pair portid-a b-port portid-b [ link-safe [ enable | disable ] ]
```

Options

`group-name`	Name to identify the monitor port group. Maximum length is 64 characters.
`ports ports-list`	Member ports for the port group. Use `[ a-b c-d e-f ]` format (with spaces as shown) to specify multiple ports. • Ports with port class Monitor, Service, and Span-Monitor can be part of a port group of type `monitor`. • Ports with port class Span, Service, and Span-Monitor can be part of a port group of type `network`. • Ports with port class Inline Monitor can be part of a port group of type `inline-monitor`. • Ports with port class Inline Network can be part of a port group of type `inline-network`.
`lb-criteria criteria`	User-defined load balancing method as defined in the load balance criteria library.
`load-balance-groups lbg-list`	Output load balance groups for the map. Use `[ g1 g2 g3 ]` format (with spaces as shown) to specify multiple groups. You can specify output ports, a load balance group and load balance criteria, or both. If you specify multiple output ports, traffic is replicated across the ports.
`pfsmesh [ enable | disable ]`	Specify pfsMesh visibility for this port group. To allow this port group to be available across a pfsMesh, specify `enable`.

`common-vlan vlan-id`	Specify a common VLAN ID to be used by this port group. This is an optional parameter. Before configuring this, each port in the port group must already be configured to use the specified user-defined VLAN ID. Valid values are 1 to 4094.
`[consolidate [ enable | disable ]`	**This option is only Available on PFS 6000 Series.** Select **Enable** to group the ports to create a trunk. ***Note:*** *If pStack is enabled, (that is, the PFS has a port with Class =* `pStack` *or* `pStack-plus`*), the following restrictions apply:* • *User-defined VLANs for all the member ports of a Consolidated network group will be ignored. Incoming packets from member ports are tagged with the configured Common VLAN ID value from the Consolidated network port group. If a Common VLAN ID is not set, then it will be tagged with a VLAN ID assigned by the pStack protocol.* • *If a port is part of a Consolidated network group and is also used as input port in maps, make sure all the maps using the port and the Consolidated port group as Input have the same set of remote port groups as output.*
`vlan-tag { enable | disable }`	Specify whether VLAN tags should be added to packets before they are sent to tools (Inline Monitor port group). VLAN tagging options: • `enable` • `disable`
`power-safe`	This option should be set when the Inline Network ports are connected to the External PowerSafe TAP.
`port-pair portid-a`	Specify the A side of the port pair. Must have the same class as the type of port group being created (Inline Monitor or Inline Network).
`b-port portid-b`	Specify the B side of the port pair. Must have the same class as the type of port group being created (Inline Monitor or Inline Network).
`a-health-monitor-library a-hc-name`	If specified, use health library `a-hc-name` on the A-side port.
`b-health-monitor-library b-hc-name`	If specified, use health library `b-hc-name` on the B-side port.
`link-safe`	Inline Network port pairs and Inline Monitor port pairs can be configured to use the NETSCOUT proprietary LinkSafe algorithm to enforce the same state on both interfaces. Linksafe options: • `enable` • `disable`
`weight`	Prioritize a specific port pair over other port pairs in the inline monitor port group by assigning a weight to it. Valid values range from 0-100; if all are set to 0 then PFOS uses equal distribution. Refer to the ***PFOS 6.x User Guide*** for details about how PFOS calculates distribution percentage.

Mode

Configuration

Examples

Create a monitor port group named PG1 and containing ports 1-5 and 1-6 and load balance groups LBG1 and LBG2 with user-defined criteria IPDest, and enable pfsMesh on these ports:

```
PFOS(config)# port-group monitor PG1 ports [ 1-5 1-6 ] load-balance-
groups [ LBG1 LBG2 ] lb-criteria IPDest pfsmesh enable
```

Create a consolidated network port group named NPG1 and containing ports 4-25 and 4-26, and use VLAN ID 101:

```
PFOS(config)# port-group network npg1 ports [ 4-25 4-26 ] common-vlan
101 consolidate enable
```

Create an inline network port group named INPG1 with port pair 1-1 and 1-2, with LinkSafe enabled:

```
PFOS(config)# port-group inline-network INPG1 port-pair 1-1 b-port 1-2
link-safe enable
```

Create an inline monitor port group named IMPG2 with port pair 2-3 and 2-4, using health monitor library asc on both sides, with LinkSafe enabled:

```
PFOS(config)# port-group inline-monitor IMPG2 port-pair 2-3 a-health-
monitor-library asc b-port 2-4 b-health-monitor-library asc link-safe
enable
```

Create an inline monitor port group named IMPG3 with port pair 2-3 and 2-4, setting port weights to 40:

```
PFOS(config)# port-group inline-monitor IMPG3 ports [ 2-3 2-4 ] weight
40
```

Create an inline monitor port group named tool1_SSLA_IMPG with port pair1-7, setting port weight to 50:

```
pfs5010(config)# port-group inline-monitor tool1_SSLA_IMPG port-pair 1-7
weight 50
```

toolchain group

Create a tool chain for use with inline traffic. To add multiple tools to the same chain, issue the command multiple times as needed; see the example below. Refer to the ***PFOS 6.x User Guide*** for tool chain use case examples.

Syntax

```
toolchain group chain-name tool tool-name type type-name
    inline-monitor-group inlinemon-group
    [ a-side-passive-mongroups mon-group ]
    [ b-side-passive-mongroups mon-group ]
    [ a-side-next-tool filter-name | tool-name| ignore-ingress-vlan
| bypass | inline-network-portport num ]
    [ b-side-next-tool filter-name | tool-name| ignore-ingress-vlan
| bypass | inline-network-portport num ]
    [ tool-failover-action ]
    [ source-port-vlan-forwarding ]
```

Options

`toolchain group` *`chain-name`*	Name to identify the tool chain. Maximum length is 64 characters.
`tool` *`tool-name`*	Name of a tool within this tool chain. Maximum length is 64 characters. The same *`tool-name`* can be used in different tool chains, but they will be different tools.
`type` *`type-name`*	Name of the type of tool chain: • `simple` tool chains allow you to create uncomplicated chains for traffic flow tool in series; that do not allow filtering between tools. The initial ingress network traffic can be filtered before forwarding to the first tool within the tool chain. PFOS automatically generates all the tool-to-tool connections to forward all traffic to next tools and passive monitor port groups; users are not required to configure tool connections. • `advanced` tool chains allow users to create more complex tool chains. Users can define traffic flow by configuring connections and filters for each tool's "A" side and "B" side throughout the entire chain.
`inline-monitor-group` *`inlinemon-group`*	Name of previously-created inline monitor port group to associate with this tool. Each tool must have an associated inline monitor port group.
`a-side-passive-mongroups` *`mon-group`*	Optional name of previously-created monitor port group to receive traffic from the A side of this tool.
`b-side-passive-mongroups` *`mon-group`*	Optional name of previously-created monitor port group to receive traffic from the B side of this tool.

`a-side-next-tool` `b-side-next-tool`	- `filter-name`: Name of previously-created filter expression to apply to traffic before sending it to the next tool in this chain. - `tool-name`: Name of next tool in chain to receive traffic - `ignore-ingress-vlan`: Used with `next-tool tool-name` filter. Normally PFOS prepends “Inline-network” VLAN to filters. When enabling this option, PFOS will not prepend any VLAN to the filter. **Note:** If enabling this option, it is recommended you not use the specific tool for multiple toolchains. - `bypass`: Bypass the rest of this chain. PFOS prepends “VLAN filter” to send traffic back to 1-1 pair of inline-network ports. - `Inline-network-port`: Specify the port or ports in inline-network-port pair to forward traffic; PFOS will not prepend VLAN. This option differs from the Bypass option, during which PFOS prepends “VLAN filter” to send back to 1-1 pair of inline-network ports.
`tool-failover-action`	Action to be taken on the tool failure: - `Skip`: Bypass the failed tool. - `Drop`: Block the traffic at the failed tool. - `Bypass`: Bypass the entire tool chain when the tool fails.
`source-port-vlan-forwarding`	This option is only supported in Simple tool chains. When enabled, packets entering a tool chain are forwarded based on the VLAN ID assigned at ingress inline network ports (INP). The traffic is sequentially forwarded from the first tool to the last tool (or from the last tool to the first tool, depending on traffic from A-side to B-side or from B-side to A-Side), and then egresses to the inline network pairing port.

Mode

Configuration

Examples

Create advanced tool chain `chain1`, consisting of two tools, `tool1` and `tool2`. When packets reach tool2, if they match the `tcp` filter, then forward them to `tool1`; otherwise, bypass the rest of the chain. Also, forward A-side traffic to monitor port group `mpg1`, and B-side traffic to group `mpg2`.

```
PFOS(config)# toolchain group chain1 type advanced
PFOS(config)# toolchain group chain1 tool tool1 inline-monitor-group
impg1 a-side-passive-mongroups mpg1 b-side-passive-mongroups mpg2
PFOS(config)# toolchain group chain1 tool tool2 inline-monitor-group
impg1 a-side-next-tool tcp tool1
PFOS(config)# toolchain group chain1 tool tool2 b-side-next-tool tcp
tool1
PFOS(config)# toolchain group chain1 tool tool2 a-side-next-tool
nonmatch bypass
```

```
PFOS(config)# toolchain group chain1 tool tool2 b-side-next-tool
nonmatch bypass
```

For toolchain chain1, set tool failover to SKIP, to bypass tool1 if it fails.

```
toolchain group chain1 tool tool1 tool-failover-action SKIP
```

For toolchain chain1, tool1, set filter1 for filtering traffic and forward to inline port 1-1 for A-side and B-side.

```
toolchain group chain1 tool tool1 a-side-next-tool filter1 inline-
network-ports [ 1-1 ] toolchain group chain1 tool tool1 b-side-next-tool
filter1 inline-network-ports [ 1-1 ]
```

For toolchain chain1, tool1, set filter2 for filtering traffic and forward to tool2 without prepending VLAN for A-side.

```
toolchain group chain1 tool tool1 a-side-next-tool filter2 next-tool
tool2 ignore-ingress-vlan
```

For toolchain chain1, tool1, set filter2 for filtering traffic and forward to inline port 1-1 for B-side.

```
toolchain group chain1 tool tool1 b-side-next-tool filter2 inline-
network-ports [ 1-1 ]
```

For toolchain SourcePort_TC, enable source port VLAN forwarding.

```
PFOS(config)# toolchain group SourcePort_TC type simple source-port-
vlan-forwarding
```

trigger

You can define trigger policies to configure PFOS to perform actions when certain trigger events occur. PFOS can be configured to automatically modify traffic map forwarding rules based on events, to send notifications based on events, and/or to automatically place the network access into a failsafe state based on trigger policy outcomes. The system continuously monitors these conditions and manages actions based on the outcome of these conditions. Up to 64 user-defined trigger policies can be created on a single system.

Trigger policies can be configured as:

- local triggers to monitor local events, that occur on the node on which it was created (default); or
- remote triggers to monitor remote events that occur on other nodes within pfsMesh (see `pfsmesh enable` and `combo` triggers).

Refer to the following sections for more information:

- Configuring trigger name and type
- Configuring ports or port groups
- Configuring trigger action
- Configuring pfsMesh Option

Configuring trigger name and type

Use the following sections to define trigger name and type.

Syntax

```
trigger [name] type [type-option] [parameters]
```

Options

`name`	Name to identify the trigger policy. Maximum length is 64 characters. **Note:** If the trigger will be used in pfsMesh as a remote trigger policy, ensure that the trigger name is unique to avoid conflict with other trigger policy names and so it is easily identifiable within pfsMesh.

type-option	Type of event to be monitored: • linkstate policy to trigger when one or more specified port links are online or offline. • healthcheck policy to trigger when health check status fails to enable logical link down of the port pairs in the inline monitor port group. • overflow policy to trigger w`hen port overflow drops occur on one or more specified ports. • bandwidth utilization policy to trigger when bandwidth utilization of one or more specified ports exceeds user-defined limits. • combo policy to trigger based on the states of other policies including remote trigger policies. • pps-threshold policy to trigger when packets per second of one or more specified ports exceeds user-defined limits. **Note:** These triggers are only supported on the PFS 5000/7000 series.
parameters	See Parameters (Type).

Parameters (Type)

Parameters vary per trigger type.

Linkstate	• trigger-link: Condition to activate trigger when link goes offline/online. Values are all-offline, all-online, any-offline, any-online • active-set-time: amount of time in seconds the trigger condition must be true before it is set to Active state. • active-clear-time: amount of time in seconds the trigger condition must be false before it is set to Inactive state.
healthcheck	• trigger- healthcheck: Condition to activate trigger when health check fails on any/all inline monitor ports • active-set-time: amount of time in seconds the trigger condition must be true before it is set to Active state. • active-clear-time: amount of time in seconds the trigger condition must be false before it is set to Inactive state.
overflow	• active-set-time: amount of time in seconds the trigger condition must be true before it is set to Active state. • active-clear-time: amount of time in seconds the trigger condition must be false before it is set to Inactive state.
bandwidth-utilization	• direction: RX or TX; only the specified direction will be monitored. • max: The maximum level threshold, above which the trigger is activated. Enter 100% utilization to disable the maximum level of Bandwidth threshold. • min: The minimum level threshold, below which the trigger is activated. Enter 0% utilization to disable the minimum level of Bandwidth threshold. • active-set-time: amount of time in seconds the trigger condition must be true before it is set to Active state. • active-clear-time: amount of time in seconds the trigger condition must be false before it is set to Inactive state.

combo	- condition: Condition that this trigger depends on any/all of the other selected profiles - remote-trigger-profile: pfsMesh-enabled triggers that are visible to all nodes in pfsMesh - other-profiles: list of other trigger profiles that this trigger depends on - active-set-time: amount of time in seconds the trigger condition must be true before it is set to Active state. - active-clear-time: amount of time in seconds the trigger condition must be false before it is set to Inactive state. - state: active/inactive state to be monitored on the selected profiles.
pps-threshold	**Note:** These triggers are only supported on the PFS 5000/7000 series. - direction: RX or TX; only the specified direction will be monitored. - maximum-pps: The maximum level threshold, above which the trigger is activated. Enter 0 Packets per Second to disable the maximum level of PPS threshold. Specify unit of measure: ◦ PPS – Packets Per Second ◦ KPPS – Kilo/Thousand Packets Per Second ◦ MPPS – Million Packets Per Second - minimum-pps: The minimum level threshold, below which the trigger is activated. Enter 0 Packets per Second to disable the minimum level of PPS threshold. Specify unit of measure (PPS/KPPS/MPPS). - active-set-time: amount of time in seconds the trigger condition must be true before it is set to Active state. - active-clear-time: amount of time in seconds the trigger condition must be false before it is set to Inactive state.

Mode

Configuration

Examples

```
PFOS(config)# trigger TG1 type linkstate trigger-link all-offline
active-set-time 5 active-clear-time 5
PFOS(config)# trigger TG2 type bandwidth-utilization direction rx min 20
max 80 active-set-time 5 active-clear-time 5
PFOS(config)# trigger TG3 type overflow active-set-time 5 active-clear-
time 5
PFOS(config)# trigger TG4 type healthcheck active-set-time 5 active-
clear-time 5
PFOS(config)# trigger TG5 type combo condition any other-profiles [ TG1
TG2 TG3 ] state Active active-set-time 5 active-clear-time
PFOS(config)# trigger TG5 type combo condition any remote-trigger-
profile [ Trigger1 Node_119_Trigger_link1 ] state Active active-set-time
5 active-clear-time
PFOS(config)# trigger PPS-T1 type pps-threshold direction rx minimum-pps
100 KPPS maximum-pps 11.2 MPPS
```

Configuring ports or port groups

Some trigger policies allow you to select specific ports or port groups to monitor for the trigger condition. *Available port classes and port groups vary depending on trigger type; therefore these options are only available after trigger type has been defined.*

Syntax

```
trigger [name] ports [list-of-ports]
trigger [name] portgroup [portgroup-option] [list-of-portgroups]
```

Options

`name`	Name to identify the trigger policy. Maximum length is 64 characters.
`list-of-ports`	List of ports to be monitored. Enclose the ports in brackets in slot-port format, with multiple ports separated by spaces: `[slot-port slot-port slot-port]`
`portgroup-option`	Type of port group to be monitored. Four different types of port group options are available: • `Network` • `Monitor` • `Inline-network` • `Inline-monitor`
`list-of-portgroups`	Specify the port groups to be monitored. Enclose the names in brackets [] and separate multiple names with spaces: `[portgroup1 portgroup2 portgroup3]`

Examples

```
trigger TG1 ports [ 1-1 1-30 ]
trigger TG1 portgroup network [ npg1 npg2 ] monitor [ mg1 mg2 ] inline-
network [ inpg1 inpg2 ] inline-monitor [ impg1 impg2 impg3 ]
```

Configuring trigger action

Use the following syntax to define actions for a trigger:

- Send a notification:
  - Send a message to a Syslog server if one has been configured.
  - Send an SNMP trap to an SNMP server if one has been configured.
  - Send a NETCONF notification
- Disable (force link-down) one or more ports.

You can also enable/disable traffic maps based on the outcome of a trigger policy; refer to the map for more details.

Syntax

```
trigger [name] action [action-option] [parameters]
```

Options

name	Name to identify the trigger policy. Maximum length is 64 characters.
action	Action to be taken as a result of trigger status going active: • notification: enable notifications for this trigger. See notification event for details about configuring notifications. • force-link-down
parameters	For force-link-down, specify the ports to force down when the trigger policy is active. Use the following format, with multiple ports separated by spaces: [slot-port slot-port slot-port]

Examples

```
trigger TG1 action notifications
trigger TG1 action force-link-down [ 1-6 1-30 ]
```

Configuring pfsMesh Option

You can configure whether a trigger is visible to all nodes in pfsMesh.

Notes:

- Only 16 triggers can be configured as pfsMesh Enable.
- A combo trigger can be configured as “pfsMesh enabled” only if its profile does not contain any remote trigger profiles.
- See also `show trigger` and `show remote-trigger` for details.

Syntax

```
trigger name pfsMesh option
```

Options

name	Name to identify the trigger policy. Maximum length is 64 characters.
option	• disable: trigger is only visible to the node on which it was created. • enable: trigger is visible to all nodes in pfsMesh.

Examples

```
trigger T1 pfsMesh enable
trigger T1 pfsMesh disable
```

7 Enhanced Port Features

Enhanced Port feature support varies per PFS series. Refer to the following sections for details:

- PFS 5000/7000 Enhanced Port Features
- PFS 6000 Enhanced Port Features

PFS 5000/7000 Enhanced Port Features

The following enhanced port features are supported on the PFS 5000/7000 Series. For details about PFS 6000 enhanced port features, refer to PFS 6000 Enhanced Port Features.

app-lib egress-vlan-action (PFS 7000 only)

app-lib standard-stripping

mirroring_slicing_7k

app-lib egress-vlan-action

Note: This feature requires the PFS 7000 functionality license.

PFOS supports an option for Inline Monitor (IM) ports to strip specific VLANs from PFS egress traffic. The `app-lib egress-vlan-action` command allows you to create a group to define the VLAN IDs to be removed from PFS egress traffic:

- Each egress-vlan-action group can support a maximum of 16 VLAN IDs.
- Each Inline Monitor port supports one egress-vlan-action group (refer to the `interface` command)
- Each PFS Device supports a total of 8 egress-vlan-action groups.

You can also configure notifications for egress-vlan-action events. Refer to "Inline Monitor Egress VLAN Stripping" in the *PFOS User Guide* for details about this feature.

Syntax

```
app-lib egress-vlan-action <name> vlan <vlan-id>
```

Options

`name`	Name to identify the egress VLAN group. Maximum length is 64 characters.

`vlan-id`	Specify an egress VLAN ID; valid values are between 1 and 4094. Configuring VLAN ID ranges is not supported. You can add a maximum of 16 VLAN IDs to the group by adding each VLAN ID individually.

Mode

Configuration

Examples

```
PFOS(config)# app-lib egress-vlan-action AED1 vlan 1234
PFOS(config)# app-lib egress-vlan-action AED1 vlan 1235
PFOS(config)# app-lib egress-vlan-action AED2 vlan 4000
```

app-lib standard-stripping

Refer to the following sections for details about standard stripping options:

- app-lib standard-stripping vxlan
- app-lib standard-stripping mpls
- app-lib standard-stripping l2gre

app-lib standard-stripping vxlan

VXLAN stripping is a two-part configuration:

- First, configure a set of VTEP addresses, UDP ports, and VNIDs (`app-lib standard-stripping vxlan`).
- Then, configure the desired port(s) to enable or disable VXLAN stripping (see `stripping vxlan` option for `interface` command).

Refer to the following details to configure VTEP addresses, UDP ports, and VNIDs.

Available only on PFS 5000/7000 Series systems.

Syntax

```
app-lib standard-stripping vxlan
    [ udp-port portnum ]
    vtep-address vtep-list
    vnid vnid-list
```

Options

portnum	Valid 16-bit UDP port number to use, usually 4789 or 8472. This option is for **outer UDP destination** port.
vtep-list	List of VTEP addresses in CIDR IP/prefix format. If a network is to be specified, then the host bits must be 0 with a proper prefix. If an endpoint address is to be specified, then the prefix must be 32. Enclose multiple addresses in square brackets []. This option is for **outer IP Destination** address.
vnid-list	A list of individual VNIDs, a range of VNIDs, or a combination of both. Enclose a list in square brackets []. Up to 1024 VNID values (input either as individual values or in a range) can be configured per PFS. Valid VNID values range from 1 to 16777215. **Note:** pStack+ uses a range of 8388608 to 16777215 internally for VNIDs for VXLAN tunnels; therefore, when a PFS device has at least one pStack-plus port configured, the maximum value for VNIDs for VXLAN stripping is 8388607.

Mode

Configuration

Examples

```
PFOS(config)# app-lib standard-stripping vxlan udp-port 4789 vtep-
address [ 10.20.30.0/24 10.40.0.0/16 10.50.60.70/32 ] vnid [ 400-500
6000 8000-9000 ]
```

app-lib standard-stripping mpls

Note: This feature requires the PFS 7000 functionality license and you must enable the Features MPLS option before you can use this feature.

Once MPLS Standard Stripping is enabled (see `stripping mpls` option for `interface` command), PFOS automatically defines MPLS labels based on incoming traffic. You can use the `app-lib standard-stripping mpls` command to define additional custom MPLS labels.

> **Note:** L2 MPLS packets with pseudowire control word (pwc) will not be stripped correctly in automatic MPLS stripping. To overcome this issue, you must configure the specific L2 MPLS label with control-word option (refer to `pwc presence` in this section).

Syntax

```
app-lib standard-stripping mpls tunnel-label [ val(s) ]
app-lib standard-stripping mpls l2-mpls-labels val  pwc presence
```

Options

`tunnel-label val`	A list of valid L3 MPLS tunnel labels (16 to 1048575; 0 to 15 are reserved), or range of label values or a combination of both.
`l2-mpls-labels val`	A list of valid L2 MPLS labels (16 to 1048575; 0 to 15 are reserved), or range of label values or a combination of both.
`pwc` *`presence`*	Indicates whether or not incoming packets will have a pseudowire control word: • `true` • `false`

Mode

Configuration

Examples

```
PFOS(config)# app-lib standard-stripping mpls tunnel-label [ 555 666 ]
PFOS(config)# app-lib standard-stripping mpls l2-mpls-labels 2345 pwc
false
```

stripping clear mpls

Enables you to clear the hardware table in which PFOS stores automatically programmed MPLS labels. Once cleared, PFOS relearns MPLS labels from incoming traffic.

Note: During cleanup traffic disruptions will occur on MPLS labeled packets.

Syntax

```
stripping clear mpls
```

Options

None

Mode

Configuration

Example

```
PFS(config)# stripping clear mpls
Are you sure? [no,yes] yes
```

app-lib standard-stripping l2gre

Available only on PFS 7000 Series systems.

L2GRE stripping is a two-part configuration:

- Configure a set of destination IP addresses and L2GRE IDs (`app-lib standard-stripping l2gre`)
- Configure the desired port(s) to enable or disable L2GRE stripping (see `stripping l2gre` option for `interface` command).

Refer to the following details to configure L2GRE IP addresses and L2GRE IDs.

Syntax

```
app-lib standard-stripping l2gre destination-address IP/prefix-list l2gre-id id-range | id
```

Options

`IP/prefix-list`	List of destination addresses in CIDR IP/prefix format. If a network is to be specified, the host bits must be 0 with a proper prefix. If a end point address is to be specified the prefix must be 32. Enclose multiple addresses in square brackets [ ].
`id-range | id`	A list of individual L2GRE IDs, a range of L2GRE IDs, or a combination of both. Enclose a list in square brackets [ ]. Up to 1024 L2GRE ID values (input either as individual values or in a range) can be configured per PFS. Valid L2GRE ID values range from 1 to 268435455 (up to 28 bits). **Note:** PFS 7030s and PFS 7031s support an L2GRE ID value of 0.

Mode

Configuration

Examples

```
PFOS(config)# app-lib standard-stripping l2gre destination-address [
10.20.30.0/24 10.40.0.0/16 10.50.60.70/32 ] l2gre-id [ 400-500 6000
8000-9000 ]
```

mirror-session

Note: This feature requires the PFS 7000 functionality license. The PFS 704x devices support a maximum of four mirror sessions.

The Port mirroring feature duplicates traffic from one or more source ports and sends the duplicated traffic to one or more destinations for analysis. Users configure port mirror sessions by defining source ports and an associated destination (port or Load Balance Group) using the `mirror-session` command. Mirroring is an independent feature that does not affect the traffic configured using Traffic Maps. Once a mirror session is created, users can associate the mirror session to a traffic map. Packets matching the traffic map filters are duplicated to the destination defined in the mirroring session.

As part of port mirroring, users can enable a packet slicing feature. The Packet Slicing feature enables users to remove unwanted or sensitive data from packets while preserving crucial data found in headers or early in the payload. PFOS uses the following default slicing locations from the packet start:

- PFS 703x devices: 192 bytes (including FCS)
- PFS 704x devices: 190 bytes (including FCS)

Refer to the ***PFOS User Guide*** for additional information about port mirroring.

Syntax

```
mirror-session name destination [ interface port | load-balance-group
lbg ]
mirror-session name slicing
mirror-session name source-interface [port]
mirror-session name source-interface port [direction {tx | rx | both}]
```

Options

name	Define a name for the mirror session.

`destination`	Configure the mirror destination. - `interface`: Define the port number you want for the destination. The destination port can only be MON or SPAN-MON port class. - `load-balance-group`: Define the name of the load balancing group you want for the destination. **Notes:** - PFS 704x devices do not support LBGs as a mirror session destination. - Mirror sessions using load balance groups as a destination will use the existing LB-criteria configured on a traffic map. If no map is configured, it uses the default LB-criteria (SIP and DIP).
`slicing`	**Packet slicing is only supported as part of the port mirroring feature on PFS 703x and PFS 704x devices.** To enable slicing in a mirror-session, you must enable the `feature slicing` option. PFS 704x systems provide an additional option enabling you to configure the `feature slicing-offset` (which spans from 30-63 bytes).
`source-interface`	Configure one or more mirror source ports and the direction of traffic PFOS will mirror (tx, rx, both) **Notes:** - The source port can be any port class. - If mirroring both traffic directions on Service ports, the destination will receive double the number of packets due to loopback to the Service ports. - Mirroring sessions associated with traffic maps do not require source interfaces because PFOS uses the Ingress ports defined in the traffic map.

Mode

Configuration

Examples

Creating a mirror session with LBG as a destination

```
PFOS(config)# mirror-session MS1 destination load-balance-group LB1 source-interface 1-1.1
direction tx
```

Creating a mirror session with port as a destination

```
PFOS(config)# mirror-session Mirror-Session1 destination interface 1-11 source-interface 1-1
direction both
PFOS(config)# do show running-config mirror-session
mirror-session Mirror-Session1
 destination interface 1-11
 source-interface 1-1
  direction rx
!
```

Adding more source interfaces to an existing session

```
PFOS(config)# mirror-session Mirror-Session1 source-interface 1-2 direction tx
PFOS(config)# do show running-config mirror-session
mirror-session Mirror-Session1
```

```
destination interface 1-11
source-interface 1-1
 direction rx
!
source-interface 1-2
 direction tx
```

PFS 6000 Enhanced Port Features

These features are supported on the 40-port 10G/1G Advanced-R (40SadvR) line card on the PFS 6000 Series. For details about PFS 5000/7000 enhanced port features, refer to PFS 5000/7000 Enhanced Port Features.

Commands for packet deduplication:

app-lib deduplication

Commands for extended load balancing:

app-lib extended-lb

Commands for conditional packet slicing and masking:

app-lib advanced-filter

app-lib maskdef

app-lib offset

app-lib slicing

Commands for generic stripping:

app-lib mpls-l3

app-lib protocol

app-lib protocol-stripping

Commands for VLAN tag stripping:

app-lib vlan-tag-strip

Commands for tunnel termination:

app-lib tunnel-termination

app-lib advanced-filter

Create filter definitions that can be used with conditional slicing.

Available only on PFS 6000 Series systems with at least one Advanced line card installed.

Syntax

```
app-lib advanced-filter name expression string
```

Options

`name`	Name of the advanced filter.
`string`	Expression that defines the filter. See the “Conditional Packet Slicing” section of the *PFOS User Guide* for information and examples of creating advanced filter expressions.

Mode

Configuration

Examples

```
PFOS(config)# app-lib advanced-filter adv-filter expression "IP Protocol
17" set my-offset offset-value 100 slicepoint start-of-packet
```

app-lib deduplication

Create packet deduplication settings.

Available only on PFS 6000 Series systems with at least one Advanced line card installed.

Syntax

```
app-lib deduplication name [ ignore option ] [ time-window number ]
```

Options

name	Name of the packet deduplication setting.
option	Specify one or more comma-separated packet fields to exclude from the duplicate packet detection. Options: ip_header_id – Ignore duplicated IP header ID. mac_header – Ignore duplicated MAC address. mpls_labels – Ignore duplicated MPLS. port_stamp – Ignore duplicated port stamp. time_stamp – Ignore duplicated time stamp. tos – Ignore duplicated TOS. ttl – Ignore duplicated TTL. vlan_tags – Ignore duplicated VLAN tags.
number	Sets the time window for tracking and comparing packets to determine duplication (1 - 4,000 milliseconds).

Mode

Configuration

Examples

```
PFOS(config)# app-lib deduplication dd1 ignore mac_header,mpls_labels
time-window 100
```

app-lib extended-lb

Configure extended load balancing.

Available only on PFS 6000 Series systems with at least one Advanced line card installed.

Syntax

```
app-lib extended-lb elb-name
    criteria elb-criteria
    protocoln protocol-name
```

Options

elb-name	Name of the extended load balancing configuration.
elb-criteria	Extended load balancing criteria. Valid values are: Dest_Inner_MAC_Address Dest_Src_Inner_MAC_Address IP_Dest IP_Dest_Src IP_Dest_Src_TCP_UDP_SCTP_Dest_Src IP_Dest_Src_TCP_UDP_SCTP_Dest_Src_Protocol_Type IP_Dest_TCP_UDP_SCTP_Dest IP_Src IP_Src_TCP_UDP_SCTP_Src Src_Inner_MAC_Address
protocoln	Specify up to six protocols to use in this extended load balancing configuration, where n is a digit from 1 to 6.
protocol-name	Protocol to use as basis for load balancing. Valid values are: Cisco-Fabricpath GRE_NVGRE GTP MPLS MVDCAP Mac-in-Mac TRILL VLAN_VNTAG VXLAN

Mode

Configuration

Examples

```
PFOS(config)# app-lib extended-lb elb-1 criteria IP_dest protocol1 MPLS
```

app-lib maskdef

Create mask definitions to use with conditional slicing and masking.

Available only on PFS 6000 Series systems with at least one Advanced line card installed.

Syntax

```
app-lib maskdef maskdef-name
   anchor-point anchor-point
   length length
   offset offset
   pattern pattern
```

Options

`maskdef-name`	Name to identify the mask library entry.

`anchor-point`	Starting point for this mask. Valid values are:
	`start-L2`
	`end-L2`
	`end-L3`
	`end-L4`

`length`	Length of mask in bytes, from 0 to 9,000.
`offset`	Offset after `anchor-point` as the reference point.
`pattern`	One-byte hexadecimal pattern to use as the mask.

Mode

Configuration

Examples

```
PFOS(config)# app-lib maskdef mask-2 anchor-point start-L2 length 100
offset 20 pattern ff
```

app-lib mpls-l3

Define MPLS-L3 stripping configuration.

Available only on PFS 6000 Series systems with at least one Advanced line card installed.

Syntax

```
app-lib mpls-l3 name
   configuration hex-label
   [ mpls-etype select-etype ]
   [ mpls-etype-value select-etype-value ]
   [ mac-source mac-source-bit ]
```

Options

`name`	Name to identify the application library entry.
`hex-label`	Unique five-digit hex number for each entry created in the MPLS-L3 library configuration.

`select-etype`	Specifies the EType. Valid values are:
	`shortcuts`
	`ipv4`
	`ipv6`
	`802.1p-q-tagged`
	`arp`
	`pppoe-discovery`
	`pppoe-session`
	`rarp`
	`xns`

`select-etype-value`	You can configure custom values for the selected EType. If you do not configure, the following default values are selected: shortcuts empty ipv4 0800 ipv6 86DD 802.1p-q-tagged 8100 arp 0806 pppoe-discovery 8863 pppoe-session 8864 rarp 8035 xns 0600
`mac-source-bit`	Include source MAC address.

Mode

Configuration

Examples

```
PFOS(config)# app-lib mpls-l3 my-stripping configuration 12345 mpls-
etype ipv4 mac-source mac-source-bit
```

app-lib offset

Create a slice point for use in conditional packet slicing.

Available only on PFS 6000 Series systems with at least one Advanced line card installed.

Syntax

```
app-lib offset name offset-value number slice-point value
```

Options

`name`	Name of the offset definition.
`number`	Amount of the offset in number of bytes.
`value`	Location of the slice point: `start-of-layer-4-data` – End of TCP/UDP header. `start-of-packet` – Start of packet. `start-of-tcp-or-udp` – End of IP header.

Mode

Configuration

Examples

```
PFOS(config)# app-lib offset my-offset offset-value 100 slice-point
start-of-packet
```

app-lib protocol-stripping

Configure protocol stripping library.

Available only on PFS 6000 Series systems with at least one Advanced line card installed.

Syntax

```
app-lib protocol-stripping name present-protocols
```

Options

`name`	Name of protocol stripping library entry.

`present-protocols`	One or more of the following, separated by spaces:
	`GRE`
	`GTP`
	`MPLS-L2`
	`MPLS-l3-protocol mpls-l3-lib-name`
	`protocol1 protocol-lib-name`
	`protocol2 protocol-lib-name`
	`protocol3 protocol-lib-name`
	`protocol4 protocol-lib-name`
	`protocol5 protocol-lib-name`
	`protocol6 protocol-lib-name`
	`protocol7 protocol-lib-name`
	`protocol8 protocol-lib-name`

`protocol-lib-name`	Protocol library name, either pre-defined or user-defined (see app-lib protocol). The following entries are pre-defined:
	`Cisco-Fabricpath`
	`Mac-in-Mac`
	`TRILL`
	`VXLAN`

Mode

Configuration

Examples

```
PFOS(config)# app-lib protocol-stripping strip-test gre mpls-l3 my-
stripping
```

app-lib protocol

Configure protocol library for use in stripping.

Available only on PFS 6000 Series systems with at least one Advanced line card installed.

Syntax

```
app-lib protocol name
app-lib protocol name protocol-matching-field field
app-lib protocol name protocol-etype-value number
app-lib protocol name protocol-matching-field ip-protocol
   ip-protocol-value number
app-lib protocol name protocol-matching-field { udp-dest-port |
   sctp-dest-port | tcp-dest-port } dest-port-value number
app-lib protocol name strip-headers headers-to-strip
app-lib protocol name strip-offset strip-location
app-lib protocol name strip-length strip-number
app-lib protocol name strip-reference_point value
```

Options

`name`	Name to identify the protocol library entry.

`protocol-matching-field field`	Specify the protocol matching field to be stripped. Valid values are:
	`etype`
	`ip-protocol`
	`sctp-dest-port`
	`tcp-dest-port`
	`udp-dest-port`

`protocol-etype-value number`	Specifies the Tag Protocol Identifier (TPID) to strip.
`ip-protocol-value number`	Hexadecimal string with one octet represented as hex digits.
`dest-post-value number`	Destination port number.
`headers-to-strip`	Headers to strip. Valid values are `L2_header` (the default), `L2_L3_L4_header`, and `L2_L3_header`.
`strip-location`	Number of bytes to offset from the strip reference point (<256).
`strip-number`	Number of bytes to be stripped from strip offset (<256).
`strip-reference_point`	Reference point for strip-offset and strip-length. Valid values are `start-L2` (the default), `end-L2`, `end-L3`, and `end-L4`.

Mode

Configuration

Examples

```
PFOS(config)# app-lib protocol mystrip protocol-matching-field ip-
protocol ip-protocol-value 06 strip-offset 30 strip-length 8 strip-
reference_point start-L2
```

app-lib slicing

Configure conditional slicing and masking.

Available only on PFS 6000 Series systems with at least one Advanced line card installed.

Syntax

```
app-lib slicing slice-name slice
    config-num advanced-filter filter-name offset offset-name


app-lib slicing slice-name mask
config-num advanced-filter filter-name maskdef mask-name
```

Options

`slice-name`	Name of slicing library entry to configure.
`slice`	Configure this library entry for conditional slicing.
`mask`	Configure this library entry for conditional masking.
`config-num`	Configuration number to add for this library entry. Valid values are `configuration1` through `configuration8`. **Tip:** After entering the first couple characters of the word `configuration`, you can press the space bar to auto-complete the word and then enter the desired digit from 1 to 8.
`filter-name`	Name of the advanced filter to use in this library entry.
`offset-name`	Name of the offset definition to use in this library entry.
`mask-name`	Name of the packet mask definition to use in this library entry.

Mode

Configuration

Examples

```
PFOS(config)# app-lib slicing slice-1 slice configuration1 advanced-
filter http offset offset-1

PFOS(config)# app-lib slicing mask-1 mask configuration1 advanced-filter
http maskdef mask-1
```

app-lib tunnel-termination

Configure an IP tunnel termination group.

Available only on PFS 6000 Series systems with at least one Advanced line card installed.

Syntax

```
app-lib tunnel-termination tunnel-name ip ipv4-list
```

Options

`tunnel-name`	User-specified name for this tunnel termination group.
`ipv4-list`	One to 16 IPv4 addresses. If more than one IPv4 address is specified, the list must be enclosed in square brackets with spaces separating each address, for example: `[ 1.1.1.1 2.2.2.2 ]` If an existing tunnel termination group is specified, the addresses in `ipv4-list` are added to those already specified for this group.

Mode

Configuration

Examples

```
PFOS(config)# app-lib tunnel-termination ep1 ip 10.10.10.1
PFOS(config)# app-lib tunnel-termination ep1 ip 10.10.10.2
```

The above commands are functionally equivalent to this one command:

```
PFOS(config)# app-lib tunnel-termination ep1 ip [ 10.10.10.1 10.10.10.2]
```

app-lib vlan-tag-strip

Configure VLAN tag stripping.

Available only on PFS 6000 Series systems with at least one Advanced line card installed.

Syntax

```
app-lib vlan-tag-strip name tag-count number
app-lib vlan-tag-strip name tpid string
```

Options

`name`	Name to identify the application library entry.
`tag-count number`	Specifies the number of VLAN tags to strip (`None`, `1`, `2`, or `All`).
`tpid string`	Specifies the Tag Protocol Identifier(s) (TPIDs) to strip. Separate multiple TPIDs by spaces, and enclose the list in square brackets.

Mode

Configuration

Examples

```
PFOS(config)# app-lib vlan-tag-strip vlanstrip1 tag-count 1 tpid 8100
PFOS(config)# app-lib vlan-tag-strip vtstrip1 tag-count 2 tpid [ 8888
aa88 ]
```

8 General CLI Commands

This chapter contains reference pages for the following general CLI commands:

- abort
- clear
- compare
- config
- copy
- copy bulk
- debug
- delete
- describe
- dir
- do
- end
- exit
- generate csr
- generate ssh-key
- help
- history
- id
- idle-timeout
- load
- locate system
- logout
- ncm server
- no
- paginate
- ping
- powersafe
- generate ssh-key
- pwd
- quit
- reboot
- replace config
- reroute-maps
- screen-length
- screen-width
- send
- session idle-timeout
- show-defaults
- statistics
- timestamp
- top
- who
- write

abort

Abort an in-progress `copy` or `load` command.

Syntax

```
abort { copy | load } abort-type [ mgmt-card ]
```

Options

`copy`	Abort a `copy` command.
`load`	Abort a `load` command.
`abort-type`	Type of command to abort. Valid values are `bulk`, `config`, `firmware`, `log`, `software`.
`mgmt-card`	Management module on which to perform this command. Valid values are `mgmt-1` and `mgmt-2`. If no `mgmt-card` is specified, then perform this command on the currently active management module. Option is valid only on PFS 6010 with two management modules installed.

Mode

Operational, Configuration

Examples

```
PFOS(config)# abort copy log mgmt-2
There are no processes to abort.
```

clear

Clear command history or system core files.

Syntax

```
clear { cores | history } [ mgmt-card ]
```

Options

`cores`	Clear core files. Large core files can fill the disk. Use the command with this option if you notice a system issue, such as a system image or configuration that cannot be loaded. You are prompted for a confirmation; you must type `y` or `yes` to confirm.
`history`	Clear the command history that is accessible using the up and down arrows.
`mgmt-card`	Management module on which to perform this command. Valid values are `mgmt-1` and `mgmt-2`. If no `mgmt-card` is specified, then perform this command on the currently active management module. Option is valid only on PFS 6010 with two management modules installed.

Mode

Operational, Configuration

Examples

```
PFOS(config)# clear cores
Are you sure? [no,yes] y
OK. Cleared.
PFOS#
PFOS# clear history mgmt-1
PFOS#
```

compare

Compare configuration files.

Syntax

```
compare { file file1 file2 | startup [ section ] }
```

Options

`file`	Compare two configuration files file1 and file2. Each file specification can be one of these:
	`running-config`
	`config:file_name`
	`home:file_name`

`startup`	Compare the running configuration to the startup configuration. If specified, `section` can be one of the following sections: `app-lib authentication fabric_module fan_tray feature filter gps hw-info interface lb-criteria load-balance logging management_module map monitor_port_vlan notification ntp port_timestamp power_supply ptp radius-server role session snmp snmp-server system tacacs-server tracelog username webui`

Mode

Operational

Examples

```
PFOS# compare file config:startup-config_0314.txt config:running-config_0314.txt
--- /sda3/uploads/configs/startup-config_0314.txt
+++ /sda3/uploads/configs/running-config_0314.txt
@@ -7,7 +7,7 @@
  *                vxos        6.3.0.60-7eb78ee9
  *                pstack      30.2
  * Date created:
- *                2023-03-14 21:33:51 UTC
+ *                2023-03-13 10:44:58 UTC
  ***************************************************/
 snmp agent disabled
 snmp agent ip    0.0.0.0
```

config

Enter Configuration mode.

Syntax

```
config [terminal]
```

Options

`terminal`	Not used

Mode

Operational

Examples

```
PFOS# config
Entering configuration mode terminal
PFOS(config)#
```

copy

Copy various file types.

Note: The password is optional when using this command with scp or sftp methods. If a password is not provided by the user, the system looks for SSH keys to authenticate with the remote device. In FIPs mode, the `copy` command will use only ECDSA SSH keys. In non-FIPs mode, this command will use RSA and ECDSA SSH keys. Note, however, that in non-FIPS mode if the SSH server supports ECDSA, the RSA key will not be used even if it is the only key available. The command fails if the SSH key authentication also fails or if the user provided an invalid username/password. For details about the different file types, refer to the Maintenance chapter in the *PFOS 6.x User Guide*.

Note: PFOS will not connect to SSH hosts that only offer SHA-1 hash algorithms for RSA keys.

Syntax

```
copy source dest

source:
log:|config:|core:|[mgmt-card]|[startup|running]-config) or
URL(scp:|sftp:|ftp:)* or
debug-info

dest:
(log:|software:[mgmt-card]|firmware:[mgmt-card] |
    certificate:|certificate-authority:|certificate-syslog:
|certificate-ldap:|license:|sshpubkey:|ntp-key:| ssh-knownhost:|config:
[mgmt-card]|[startup|running]-config) or
URL(scp:|sftp:|ftp:)*
```

Options

`log:`*`filename`*	Name of log file. When a file name is not specified, all logs are included. The command can take up to 30 minutes to execute, depending on the size of the log files.
`config:`*`filename`*	Copy a configuration file. **Note**: This option is not valid when copying the running-config to the startup-config. See examples for proper syntax using keywords.
`core:`*`filename`*	(Source only) Copy a core file.
`software`	(Destination only) Copy a software image file.
`firmware`	Copies to the system firmware. Firmware can be uploaded only to the currently active management module.

`certificate`	Uploads a user certificate. An uploaded certificate is used for HTTPS access to the PFOS Web UI and, if Syslog over TLS is used, and a separate Certificate-Syslog (see below) is not installed, as a client certificate for Syslog TLS mutual authentication. On a system with more than one management module, the file is uploaded to both modules. If Common Criteria mode is enabled, and a CA certificate is not present on the system, a new user certificate upload will be successful, but the install will fail.
`certificate-syslog`	Upload certificate file for syslog server. Syslog certificates are used as a client certificate for Syslog TLS mutual authentication. If no syslog-certificate is installed, the (browser) Certificate is used as the syslog client certificate. On a system with more than one management module, the file is uploaded to both modules. If Common Criteria mode is enabled syslog certificates are not used because syslog over TLS is not supported.
`certificate-ldap`	Upload TLS client certificate file for LDAP mutual authentication. If supplied, the certificate-ldap certificate is used as a client certificate for LDAP mutual TLS authentication. If no certificate-ldap is installed, mutual authentication is not enabled. On a system with more than one management module, the file is uploaded to both modules.
`certificate-authority`	Uploads a certificate authority file. A certificate file is considered a certificate authority if it contains a Basic Constraints certificate extension with CA set to TRUE. • PFOS only allows up to 10 certificate authority files to be uploaded. • Uploaded CAs are used to validate browser certificates in Common Criteria mode and to validate the peer's certificate if syslog TLS is used. • If Common Criteria mode is enabled, and a CA certificate is not present on the system, a new user certificate upload will be successful, but the install will fail.
`license:`	Uploads a license file. On a system with more than one management module, the file is uploaded to both modules.
`sshpubkey:`	**Note**: PFOS SSH Public Key support is for Local authentication only. Uploads a remote device's SSH public key file to PFS. On a system with more than one management module, the file is uploaded to both modules.
`ntp-key:`	Uploads an NTP key file. On a system with more than one management module, the file is uploaded to both modules. Refer to "Maintaining NTP Key Files" in the ***PFOS 6.x User Guide*** for details.

`ssh-knownhost:`	Uploads an SSH known host file used in Strict Host Key Checking, which is enabled in Common Criteria mode. Refer to "Maintaining SSH Knownhost" in the ***PFOS 6.x User Guide*** for details. **Note:** The CLI copy command uses scp/ssh to upload/download files on PFS. Once Common Criteria mode is enabled, scp/ssh only works if the ssh-knownhost file is present and has a public key of the remote host. Therefore, in order to upload the ssh-knownhost file using CLI, you must first disable Common Criteria mode. The Web UI does not use ssh/scp, so you can upload the ssh-knownhost file regardless of the set Common Criteria mode.
`startup-config`	Reserved keyword for startup configuration. See examples for proper syntax using keywords.
`running-config`	Reserved keyword for running configuration. See examples for proper syntax using keywords.
`scp:url`	URL available through SCP connection.
`sftp:url`	URL available through SFTP connection.
`ftp:url`	URL available through FTP connection.
`debug-info`	Information to help in troubleshooting.
`mgmt-card`	Identify source or destination management module for the file. Valid values are `mgmt-1` and `mgmt-2`. If no `mgmt-card` is specified, then the currently active management module is used. Option is valid only on PFS 6010 with two management modules installed.

Mode

Operational, Configuration

Examples

This example uploads a configuration file from a server and loads the configuration.

```
PFOS# copy scp://username:password@10.8.2.243:/home/nms/ssmith/
configs/t-107-100g.conf config:
Are you sure? [no,yes] yes
OK. Uploaded scp://username:password@10.8.2.243:/home/nms/ssmith/
configs/t-107-100g.conf to config/.
PFOS#
PFOS# show config
config-files
CONFIG NAME UPDATED TIME SIZE
-------------------------------------------
t-107-100g.conf Mar-10-2017 22:15 48235
PFOS# load config t-107-100g.conf
PFOS#
```

This example copies the running configuration to the startup configuration database and also updates the startup configuration file.

```
PFOS# copy running-config startup-config
Are you sure? [no,yes] yes
OK. Saved running-config to startup-config.
```

This example shows incorrect syntax for copying the running configuration to the startup configuration and the resulting error message.

```
PFOS# copy config:running-config config:startup-config
Are you sure? [no,yes] yes
Error: Selected configuration filename startup-config is not allowed -
reserved or already exists
```

This example uploads an image file from a server and loads the image.

```
PFOS# copy scp://username:password@10.8.2.243:/home/nms/ssmith/
sw/vxos_4.1.0.98-b9fe099f software:
Are you sure? [no,yes] yes
OK. Uploaded scp:// username:password@10.8.2.243:/home/nms/smith/
sw/vxos_4.1.0.98-b9fe099f to software:.
PFOS#
PFOS# show software
software vxos_4.1.1.150515-1448-a23cbc1a-continuous-Internal
version 4.1.1.150515~1448-a23cbc1a-continuous
state standby
size 35893448
software vxos_4.1.1.150515-2240-8e157074-continuous-Internal
version 4.1.1.150515~2240-8e157074-continuous
state current
size 35899128
```

Below example uses sftp without password to download PFOS image.

```
PFOS# copy sftp://user@10.250.176.44:/home/user/manish/vxos_core_
5.0.0.107-5417b52d software:
Are you sure? [no,yes] yes
OK. Uploaded sftp://user@10.250.176.44:/home/user/manish/vxos_core_
5.0.0.107-5417b52d to software:.
```

This example uploads an image file from a server to the second management module.

```
PFOS# copy scp://username:password@10.8.2.243:/home/nms/ssmith/
sw/vxos_5.0.0.98-b9fe099f software:mgmt-2
Are you sure? [no,yes] yes
OK. Uploaded scp:// username:password@10.8.2.243:/home/nms/smith/
sw/vxos_5.0.0.98-b9fe099f to software:mgmt-2.
```

This example uploads an SSH public key file.

```
PFOS# copy scp://user:password@10.250.176.44:/home/user/smith/ssh_key
sshpubkey:
```

This example uploads an NTP key file.

```
PFS# copy scp://user:password@192.168.100.100:/user/ntpkey ntp-key:
Are you sure? [no,yes] yes OK. Uploaded NTP key file ntp.key.txt.
```

This example uploads a certificate-authority file.

```
PFOS# copy scp://user:password@10.250.176.44:/home/user/AuthorityCA.crt
certificate-authority:
Are you sure? [no,yes] yes
OK. Uploaded scp://user@10.250.176.44:/home/user/AuthorityCA.crt to
certificate-authority:.
```

This example uploads an SSH known host file.

```
PFOS# copy scp://user:password@10.250.176.44:/home/user/user_knownhosts_
135 ssh-knownhost:
Are you sure? [no,yes] yes
OK. Uploaded scp://user@10.250.176.44:/home/user/user_knownhosts_135 to
ssh-knownhost:.
```

This example uploads a certificate-syslog file.

```
PFOS# copy scp://user:password@10.250.176.44:/home/user/syslogCert.crt
certificate-syslog: Are you sure? [no,yes] yes OK. Uploaded
scp://user@10.250.176.44:/home/user/manish/syslogCert.crt to
certificate-syslog:.
```

This example uploads a certificate-ldap file.

```
PFOS# copy scp://user:password@10.250.176.44:/home/user/ldapCert.crt
certificate-ldap: Are you sure? [no,yes] yes OK. Uploaded
scp://user@10.250.176.44:/home/user/manish/ldapCert.crt to certificate-
ldap:.
```

copy bulk

Copy multiple files from the system as a single zipped archive to a user-specified remote destination. A confirmation prompt is given before the copy begins. To view the progress of a copy operation, see show copy.

Note: The password is optional when using this command with scp or sftp methods. If a password is not provided by the user, the system looks for SSH keys to authenticate with the remote device. In FIPs mode, the `copy bulk` command will use only ECDSA SSH keys. In non-FIPs mode, this command will use RSA and ECDSA SSH keys. Note, however, that in non-FIPS mode if the SSH server supports ECDSA, the RSA key will not be used even if it is the only key available. The command fails if the SSH key authentication also fails or if the user provided an invalid username/password. For details about the different file types, refer to the Maintenance chapter in the *PFOS 6.x User Guide*.

Note: PFOS will not connect to SSH hosts that only offer SHA-1 hash algorithms for RSA keys.

Syntax

```
copy bulk location:file-list destination
```

Options

`location`	Type of PFOS file(s) in file-list. Valid values are: `config` – Configuration file(s) `core` – Core file(s) `log` – Log file(s) `home` – User-created file(s) in user home directory
`file-list`	Comma-separated list of files, or an asterisk (`*`) to copy all files of the specified type. If `file-list` is omitted, then all files of the specified type are selected.
`destination`	Remote destination to which the zipped file will be saved. The format is a standard URL beginning with `ftp://`, `sftp://`, `scp://`, `http://`, or `https://`, followed by other components (such as hostname or IP address) according to the selected protocol.

Mode

Operational, Configuration

Examples

```
PFOS# copy bulk config:*,log:* ftp://10.250.179.12/mydir
Are you sure? [no,yes] yes
```

debug

Retrieve debugging information for load balancing groups and traffic maps. All debug output is logged into a debug.log file under the directory /vss/vxos/var/log/ on the system.

NETSCOUT recommends that you use this command only at the direction of technical support. You can contact NETSCOUT Technical Support by opening a case at my.netscout.com or call +1-888-357-7667 (US) or +800 4764 3337 (outside US) for assistance.

Syntax

```
debug [ lbg lbg-option | map map-option ]
```

Options

`lbg lbg-option`	Retrieve debugging information for load balancing groups. `lbg-option` is one of the following: `all_lbg`: All load balancing groups. `lbg_name lbg-name`: Only the specified load balancing group. `lbg_ports port-id`: Only load balancing groups that use the specified port. `lbg_reply_slot slot-num`: Only load balancing groups that use one or more ports on the specified hardware slot. `sync_lbg`: Synchronize load balancing groups.
`map map-option`	Retrieve debugging information for traffic maps. map-option is one of the following: `all_maps`: All traffic maps. `filter filter-name`: Only traffic maps that use the specified filter. `input_ports port-id`: Only traffic maps that use the specified port as an input port. `name map-name`: Only the specified traffic map. `slot slot-num`: Only traffic maps that use one or more ports on the specified hardware slot `sync_map`: Synchronize traffic maps.

Mode

Operational, Configuration

Examples

```
PFOS# debug lbg lbg_name sjc-lbg
PFOS# debug map all_maps
```

delete

Delete various file types.

Syntax

```
delete { certificate | certificate-authority | certificate-syslog |
certificate-ldap | config | core | firmware | home | license | log |
ntp-key | software | ssh-key | ssh-knownhost | sshpubkey } filename [
mgmt-card ]
```

Options

`certificate`	Delete a certificate. The default certificate cannot be deleted. It can be replaced by installing a valid CA certificate.
`certificate-authority`	Delete a certificate authority file.
`certificate-syslog`	Delete a syslog certificate file.
`certificate-ldap`	Delete an LDAP certificate file.
`config`	Delete a configuration file.
`core`	Delete a core file.
`firmware`	Delete a firmware file.
`home`	Delete a user home directory file.
`license`	Delete a PFS 7000 trial license file.
`log`	Delete a system log, backup log, or tech support log file.
`ntp-key`	Delete an NTP key file.
`software`	Delete a software image.
`ssh-key`	Delete SSH key.
`ssh-knownhost`	Delete an ssh-knownhost file.
`sshpubkey`	Delete client SSH public key file.
`mgmt-card`	This option is valid only on PFS 6010 with two management modules installed. Management module on which to perform this command. Valid values are `mgmt-1` and `mgmt-2`. If no `mgmt-card` is specified, then perform this command on the currently active management module.

Mode

Operational, Configuration

Examples

```
PFOS# delete log ?
Possible completions:
  NETCONF.1
  NETCONF.idx
  NETCONF.siz
  audit.log
  audit.log.0.gz
  audit.log.1.gz
  audit.log.2.gz
  . . .
PFOS# delete log logfile1
```

```
PFS6010# delete log chassis.1 mgmt-2
Are you sure? [no,yes] no
Aborted: by user


PFS# delete ntp-key ntp.key.txt
Are you sure? [no,yes] yes
OK. Deleted NTP key ntp.key.txt on mgmt-1


PFS# delete certificate-authority AuthorityCA.crt
Are you sure? [no,yes] yes
OK. Deleted file AuthorityCA.crt by user admin


PFOS# delete Certificate-syslog syslogCert.crt
Are you sure? [no,yes] yes
OK. Deleted file syslogCert.crt by user admin


PFOS# delete Certificate-ldap ldapCert.crt
Are you sure? [no,yes] yes
OK. Deleted file ldapCert.crt by user admin


PFOS# delete license PFS 7000
Are you sure? [no,yes] yes
OK. Deleted license file PFS 7000 by user admin


PFOS# delete ssh-knownhost user_knownhosts_135
Are you sure? [no,yes] yes
OK. SSH knownhost file user_knownhosts_135 is deleted by user admin


PFOS# delete ssh-key
Are you sure? [no,yes] yes
OK. Deleted server SSH keys for user admin
```

describe

Display information about a specified command.

Syntax

```
describe command
```

Options

`command`	Specify any CLI command.

Mode

Operational

Examples

```
PFOS# describe copy
Common
    Source : built-in

Help
    Copy from one file to another

Info
    Copy from one file to another
```

dir

List files in a file system.

Syntax

```
dir { config | core | software | firmware | log | home | license |
     certificate | sshpubkey }  [ mgmt-card ]
```

Options

`config`	List all available configuration files.
`core`	List all cores and their sizes (bytes).
`software`	List each uploaded image and its version, size, status.
`firmware`	List each uploaded firmware and its version, size, status.
`log`	List all available log files.
`home`	List all user-generated files.
`license`	List of software licenses.
`certificate`	List all certificate files.
`sshpubkey`	List all SSH public key files.
`mgmt-card`	Management module on which to perform this command. Valid values are `mgmt-1` and `mgmt-2`. If no `mgmt-card` is specified, then perform this command on the currently active management module. Option is valid only on PFS 6010 with two management modules installed.

Mode

Operational, Configuration

Examples

```
PFOS# dir config

CONFIG
NAME      UPDATED TIME       SIZE
------------------------------------
tmp.conf  Mar-13-2015 08:47  18849


PFOS# dir license mgmt-1
NAME      DESCRIPTION                          TYPE  STATE    EXPIRATION DATE        MAC
ADDRESS
---------------------------------------------------------------------------------------------
-------
Support   Supports base features and upgrades  full  current  Jun 2021
c4:ee:ae:01:f1:a8
```

```
PFS 7000  Supports PFS 7000 features           full  current    -
c4:ee:ae:01:f1:a8
```

do

Execute an Operational mode command while in Configuration mode.

Syntax

```
do command_syntax
```

Options

`command_syntax`	Operational mode command.

Mode

Configuration

Examples

```
PFOS(config)# do show version

/**************************************************
 * Vendor:         NETSCOUT/VSS
 * Platform:       PFOS
 * Versions:
 *                 vxos_core   0.225
 *                 vxos_cfg    5.3.7.1-88941
 *                 vxos        4.6.0.62-f84face9
 * Date created:
 *                 2017-02-16 20:44:24 UTC
 **************************************************/
```

end

Leave the current Configuration session. Use `exit` to leave the current Operational mode session.

Syntax

```
end
```

Options

None

Mode

Configuration

Examples

```
PFOS(config)# end
```

exit

Leave the current Configuration mode or session. You can use `exit` or `end` to leave the current Configuration mode session.

Syntax

```
exit
```

Options

None

Mode

Operational, Configuration

Examples

```
PFOS# config
Entering configuration mode terminal
PFOS(config)# exit
PFOS#
```

generate csr

Generate a Certificate Signing Request (CSR) that contains information a Certificate Authority (CA) needs to create the TLS certificate. This command generates a new private key file (user input for key-file-name) and `server.csr` (RSA) or `ecc_server.csr` (ECC). Both the `.key` and `.csr` files are copied to certificate folder. See also `show csr`.

Syntax

```
generate csr key-file-name <file name> [ common-name <string> ] [
organization <string> ] [ organization-unit <string> ] [ city <string> ]
[state <string> ] [ country <string> ] [ san <string> ] [ type
<RSA/ECC>] [ key-curve <secp256r1/secp384r1/secp521r1> ]
```

Options

`key-file-name`	File name of the certificate private key file generated along with CSR.
`common-name`	The Fully-Qualified Domain Name (FQDN) you want to secure with the certificate such as www.examples.com, secure.website.org. This option supports using an asterisk (*) as a wildcard. For example, *.PFS.MyCompany.com.
`Organization`	The full legal name of your organization including the corporate identifier.
`Organization Unit`	Your department such as 'Information Technology' or 'Website Security.'
`City`	The locality or city where your organization is legally incorporated. Do not abbreviate.
`State`	The state or province where your organization is legally incorporated. Do not abbreviate.
`Country`	The official two-letter country code (such as, US, CH) where your organization is legally incorporated.
`type`	Type of encryption to be used. Supported types are RSA and Elliptic Curve Cryptography (ECC). The default value is RSA.
`key-curve`	Elliptic curve type to use to generate ECC CSR. This option is only available if type value is ECC. Elliptic curve secp256r1 (default), secp384r1, secp521r1 are supported.
`san`	The Subject Alternative Name (SAN) option enables you to define additional host names (sites, IP addresses, common names, etc.) to be protected by the CSR. Use "," to add multiple entries. This option supports using an asterisk (*) as a wildcard.For example, "DNS.1 =*.pfs.netscout.com, DNS.2 =security.netscout.com, IP.1 = 192.168.0.10"

Mode

Operational, Configuration

Examples

```
PFOS# generate csr key-file-name rsaKey.key common-name example-
pfs.netscout.com city “San Jose” state California country us
organization “Netscout Systems” organization-unit “PFS Engineering” type
```

```
RSA
OK. Generated Certificate Signing Request. Use command 'show csr type
RSA' to get CSR string

PFOS# generate csr key-file-name ecc_cert.key common-name
*.PFS.MyCompany.com city "Jersey City" state "New Jersey" organization
"MyCompany" organization-unit "Engineering Team" san "DNS.1 =
*.PFS.MyCompany.com, DNS.2 = security.pfos.MyCompany.com, IP.1 =
10.20.30.40" type ECC country US key-curve secp256r1
OK. Generated Certificate Signing Request. Use command 'show csr type
ECC' to get CSR string

PFOS# generate csr type ECC
Value for 'key-file-name' (<string>): ecc.key
OK. Generated Certificate Signing Request. Use command 'show csr type
ECC' to get CSR string
PFOS# generate csr type ECC key-curve secp384r1
Value for 'key-file-name' (<string>): sfad.key
OK. Generated Certificate Signing Request. Use command 'show csr type
ECC' to get CSR string
```

generate ssh-key

Generate SSH RSA and ECDSA private and public keys on PFS for the current logged in user. See also: `show ssh-key` and `delete`.

Syntax

```
generate ssh-key [ overwrite ]
```

Options

overwrite	Overwrites existing SSH keys.

Mode

Operational, Configuration

Example

Generate SSH key without overwrite:

```
PFS# generate ssh-key
Are you sure? [no,yes] yes
OK. Generated SSH keys for user admin.
```

Generate SSH key with overwrite:

```
PFS# generate ssh-key overwrite
Are you sure? [no,yes] yes
OK. Generated SSH keys for user admin.
```

help

List command descriptions.

Syntax

```
help [ command ]
```

Options

`command`	Restricts the list to the specific command.

Mode

Operational, Configuration

Examples

```
PFOS# help
Possible commands:
  abort           Abort ongoing long action of defined type via abort/ESC
  clear           Clear parameter
  clock           System date and time
  compare         Compare configuration
  config          Manipulate software configuration information
  copy            Copy from one file to another
  debug           debug commands to help trouble shoot any traffic data
                  forwarding issues that are caused by mis-configuration of
                  MAP/LBG
  delete          Delete a file
  describe        Display transparent command information
. . .
```

history

Configure the number of commands kept in the command history.

Syntax

```
history number
```

Options

`number`	Number of commands to keep in command history. For example, If number is 4, you can use the up arrow to scroll back four commands. Setting the value to 0 clears the history setting.

Mode

Operational

Examples

```
PFOS# history 20
```

id

Show the IDs of users and groups with accounts on the system.

Syntax

```
id
```

Options

None

Mode

Operational

Examples

```
PFOS# id
user = admin(1002), gid=1002, groups=admin,vxosuser, gids=1001
```

idle-timeout

Set the time, in seconds, after which an idle CLI session times out. See also `session idle-timeout`.

Syntax

```
idle-timeout seconds
```

Options

`seconds`	Time in seconds. Valid values are 0 to 8192; the default is 1800 seconds (30 minutes). To disable idle timeout, use the value 0.

Mode

Operational

Examples

```
PFOS# idle-timeout 3600
```

load

Load a certificate, configuration, software, or firmware file.

- Load a configuration file into the system to merge with the running config. To preserve the configuration following reboot, you must also copy it to the startup configuration. See copy.
- Load a software image to take effect following reboot.
- Load a firmware file with enhanced features.

Syntax

```
load certificate file
load certificate-syslog file
load certificate-ldap file
load config file [ mgmt-card ]
load software file [ mgmt-card ]
load firmware file [ mgmt-card ]
```

Options

file	Name of the certificate, configuration, software image, or firmware file to load.
mgmt-card	Management module on which to perform this command. Valid values are `mgmt-1` and `mgmt-2`. If no `mgmt-card` is specified, then perform this command on the currently active management module. Option is valid only on PFS 6010 with two management modules installed.

Mode

Operational, Configuration

Examples

This example uploads a configuration file from a server and loads the configuration.

```
PFOS# copy scp://
username:password@10.8.2.243:/home/nms/weilin/configs/t-107-100g.conf
config:
Are you sure? [no,yes] yes

OK. Uploaded scp://
username:password@10.8.2.243:/home/nms/weilin/configs/t-107-100g.conf to
config/.

PFOS#
PFOS# show config

config-files
CONFIG NAME UPDATED TIME SIZE
```

```
-------------------------------------------
t-107-100g.conf Mar-10-2015 22:15 48235


PFOS# load config t-107-100g.conf
PFOS#
```

This example uploads a software image file from a server and loads the image.

```
PFOS# copy scp://username:password@10.8.2.243:/home/nms/ssmith/
sw/vxos_5.0.0.76-61323fda software:
Are you sure? [no,yes] yes
OK. Uploaded scp:// username:password@10.8.2.243:/home/nms/ssmith/
sw/vxos_5.0.0.76-61323fda to image:.
PFOS#
PFOS# show software
show software NAME VERSION STATE SIZE TIME TYPE ------------------------
------------------------------------------------------------------------
--- vxos_5.0.0.76-61323fda-Internal 5.0.0.76-61323fda current 209664068
Dec 4 2017 19:51:21 vxos
PFOS# load software vxos_5.0.0.76-61323fda mgmt-1
PFOS#
```

This example loads a certificate-syslog.

```
PFOS# load certificate-syslog syslogCert.crt
Certificate syslogCert.crt installed successfully.
```

This example loads a certificate-ldap.

```
PFOS# load certificate-ldap ldapCert.crt
Certificate ldapCert.crt installed successfully.
```

locate system

On systems that support this feature, turns on the LOC indicator on the front of the system.

Syntax

```
locate system
```

Options

None

Mode

Operational, Configuration

Examples

```
PFOS# locate system
Are you sure? [no,yes] yes
System locator activated.
```

logout

Log out of the session for the current user in the current command window.

Syntax

```
logout [ session-value ] [ username ]
```

Options

`session-value`	Log out of the session with the specified session number or user information.
`username`	Log the specified user out.

Mode

Operational

Examples

```
PFOS# logout
```

no

Negates a command or resets to default.

Syntax

```
no command
```

Options

`command`	See the description of the command for options that are supported.

Mode

Operational, Configuration

Examples

```
PFOS(config)# no snmp-server
```

ncm server

This setting supports nGeniusONE PFS Monitoring. Refer to the PFOS 6.x User Guide for details about this feature.

Syntax

```
ncm server <IP address>
no ncm server
```

Options

`IP address`	Enter the nGeniusONE Configuration Manager (nCM) server IP address to which the PFS device will send data. To remove the nCM server configuration, use the `no` form of this command.

Mode

Operational, Configuration

Examples

```
PFOS(config)# ncm server 111.222.333.444
PFOS(config)# no ncm server
```

pfm server

This command enables you to configure the IP address or hostname of a PFS Fabric Manager Central Server (also known as the NMS server).

Note: This field is only applicable to PFS Fabric Manager 6.0 or later.

Syntax

```
pfm server <IP address>
no pfm server
```

Options

`IP address`	Enter the PFS Fabric Manager Central Server (NMS server) IP address to which the PFS device will send data. To remove the PFM server configuration, use the `no` form of this command.

Mode

Operational, Configuration

Examples

```
PFOS(config)# pfm server 111.222.333.444
PFOS(config)# no pfm server
```

paginate

Specify whether to include page controls when displaying command output.

Syntax

```
paginate { true | false }
```

Options

`true`	Enables page controls. If true, output is shown for one screen (page) at a time, with a `More` prompt to show the next screen.
`false`	Disables page controls.

Mode

Operational

Examples

```
PFOS# paginate true
```

ping

Send an ICMP echo command to the specified host to check connectivity. Press Ctrl-C to interrupt the command output and return to the prompt.

Syntax

```
ping host
```

Options

`host`	IP address or hostname of the host.

Mode

Operational

Examples

```
PFOS# ping 10.250.176.82
PING 10.250.176.82 (10.250.176.82): 56 data bytes
64 bytes from 10.250.176.82: seq=0 ttl=64 time=1.259 ms
64 bytes from 10.250.176.82: seq=1 ttl=64 time=0.216 ms
64 bytes from 10.250.176.82: seq=2 ttl=64 time=0.213 ms
64 bytes from 10.250.176.82: seq=3 ttl=64 time=0.182 ms
64 bytes from 10.250.176.82: seq=4 ttl=64 time=0.225 ms
64 bytes from 10.250.176.82: seq=5 ttl=64 time=0.263 ms
64 bytes from 10.250.176.82: seq=6 ttl=64 time=0.180 ms
...
```

powersafe

Display or set the PowerSafe settings for a specified module and segment. For details about the PowerSafe feature and the External PowerSafe TAP device, refer to the ***PFOS 6.x User Guide***. See also show powersafe.

Syntax

```
powersafe <Module Number> <Segment Number> manual-mode <option>
powersafe <Module Number> <Segment Number> poweroff-mode <option>
powersafe <Module Number> <Segment Number> segment-name <string>
powersafe <Module Number> <segment Number> inline-network-ports [ list
of ports ]
powersafe <Module Number> <segment Number> trigger-mode [ disable |
bypass | forward] trigger-name <string>
powersafe <Module Number> <segment Number> state [active | inactive]
powersafe usbreconnect
```

Options

`manual-mode`	Display or set the PowerSafe manual override mode for a specified module and segment. This configuration takes effect immediately and is preserved during reboot. It overrides the PowerSafe configuration that is applied during power loss. • `off` - Normal operational mode. This is the default behavior for the PowerSafe segments. When manual override is off, the **poweroff-mode setting** is applied when the PFS loses power. The `trigger-mode` settings only take effect when Manual mode is set to OFF. • `bypass` - Force fail-open. Force traffic to continue through the network, bypassing the PFS device. • `forward` - Force fail-closed. Forward traffic to PFS device for analysis/processing before continuing through network. When PFS fails, traffic is prevented from continuing through the network. • `block` - Prevent traffic from continuing through the network by dropping the packets at the Inline Network Ports connected to the PowerSafe segment (see `inline-network-ports [ list of ports ]` for details). • `InPairdown` - Bring down the defined inline-network ports connected to the PowerSafe segment (see `inline-network-ports [ list of ports ]` for details).

poweroff-mode	Display or set the PowerSafe Poweroff mode for a specified module and segment. The Poweroff Mode setting defines the EPT connection state that the segment adopts if and when power from the PFS device is lost, including: • PFS device system reboot • PFS device power cycle or power down (lost power) • USB connection from PFS device to EPT is dropped or fails The PowerSafe segments will adopt the programmed state automatically when such scenarios occur, and they will not come out of this state until the USB connection from PFS is well established and the PFS device is fully up running. The *powersafe manual-mode* and *powersafe trigger-mode* override this setting. • forward - Fail-closed. When the EPT detects power failure or loss of heartbeat then traffic will continue to be forwarded to the PFS. If the PFS has lost power then this will result in the network link being brought down. If, on the other hand, the failure is caused by the removal of the USB cable then the network link will stay up and the PFS will process traffic normally. • bypass - Pass-through or fail-open. When PFS fails, traffic continues through the network, bypassing the PFS device. • block - Prevent traffic from continuing through the network by dropping the packets at the Inline Network Ports connected to the PowerSafe segment (see inline-network-ports [list of ports] for details). • InPairdown - Bring down the defined inline-network ports connected to the PowerSafe segment (see inline-network-ports [list of ports] for details).
segment-name	Display or set a name for a specified segment. If spaces are used in the name, the string must be surrounded by quotes.
inline-network-ports [list of ports]	Define the list of inline-network ports connected to the PowerSafe segment. The ports defined with this command are the ports PFOS brings down using the manual-mode and poweroff-mode InPairdown or Block settings.

`trigger-mode`	Display or set the PowerSafe Trigger mode for a specified module and segment. This option allows you to control traffic flow based on the outcome of a trigger policy. The configuration takes effect when the trigger is activated, and it overrides the Poweroff Mode setting that is applied when the PFS unit loses power. Valid settings: • `disable` - Trigger mode is OFF. • `forward` - Fail-closed. See *poweroff-mode forward* description for details. • `bypass` - Pass-through or fail-open. See *poweroff-mode bypass* description for details. For example, you can define a link state trigger policy to trigger when one or more specified port links are offline, and then configure the External PowerSafe TAP to Bypass (force fail-open) or Forward (force fail-close) based on the Link State Trigger outcome. **Note:** Once trigger-mode is activated, in order to set the External Powersafe TAP back to normal operation, you must configure trigger-mode to Disable. Refer to the *PFOS User Guide* "PowerSafe Trigger Mode" section for details and a use case example.
`trigger-name`	`Trigger-name` is mandatory when trigger-mode is `bypass` or `forward`. Enter a predefined trigger policy name to be monitored.
`state`	(Optional) Select the State of the trigger policy you want to enable the Trigger Mode action (default is active): • **Active**: indicates the condition defined in the trigger **has** occurred. • **Inactive**: indicates the condition defined in the trigger has **not yet** occurred. PFOS applies trigger mode action when trigger's state is met.
`usbreconnect`	**Note**: This command is only applicable to the PFS 7110. Reset USB port.

Mode

Configuration

Examples

```
PFOS(config)# powersafe 1 2 manual-mode bypass
PFOS(config)# powersafe 1 2 manual-mode block
PFOS(config)# powersafe 1 2 poweroff-mode bypass
PFOS(config)# powersafe 1 2 segment-name "Port 1-2&1-3"
PFOS(config)# powersafe 1 2 inline-network-ports [ 1-1 1-2 ]
PFOS(config)# powersafe 1 2 manual-mode InPairdown
PFOS(config)# powersafe 1 2 poweroff-mode InPairdown
PFOS(config)# powersafe 1 1 trigger-mode bypass trigger-name DFW_
Trigger_Bypass
PFOS(config)# powersafe 1 1 state active

PFOS# powersafe usbreconnect
USB reconnected

or
```

```
PFOS# config
Entering configuration mode terminal
PFOS(config)# powersafe usbreconnect
USB reconnected
```

pwd

Display the current mode/submode path. Refer to CLI Command Modes for details about CLI modes and submodes.

Syntax

```
pwd
```

Options

None

Mode

Operational, Configuration

Examples

```
PFOS(config-username-ssmith)# pwd
Current submode path:
access_control username ssmith
```

quit

Leave the current CLI session.

Syntax

```
quit
```

Options

None

Mode

Operational

Examples

```
PFOS# quit
```

reboot

Reboot the system.

Syntax for PFS 5000s/7000s, PFS 6002 and PFS 6010 Single CPU

```
reboot [ restart | reset_to_factory_default | clear-config ]
```

Syntax for PFS 6010 Dual CPUs

```
reboot [ system | mgmt-card ] [ restart | reset_to_factory_default |
clear-config ]
```

Options

`system`	**This option is for PFS 6010 with dual CPUs only.** Restarts both management modules.
`mgmt-card`	**This option is for PFS 6010 with dual CPUs only.** Management module on which to perform this command. Valid values are `mgmt-1` and `mgmt-2`. If neither `mgmt-card` nor `system` is specified, then perform this command on the currently active management module.
`restart`	Restarts software and hardware.
`reset_to_factory_default`	Restarts software and hardware and applies the factory default configuration.
`clear-config`	Restarts software and hardware and clears the configuration except for system basic and networking settings.

Mode

Operational

Examples

Reboot options for PFS 5000s/7000s and PFS 6010 single CPU:

```
PFOS# reboot ?

Description: Identifies management card(s) for reboot

Possible completions:

clear_config              Clear configuration except basic networking
settings.

reset_to_factory_default  Reset to factory default settings

restart                   Normal warm reboot
```

Reboot the PFS 5000/7000 or currently active management module on PFS 6010, and reset it to factory default:

```
PFOS# reboot reset_to_factory_default
Are you sure? [no,yes] yes
```

Reboot options for PFS 6010 dual CPUs:

```
PFOS# reboot ?

Description: Identifies management card(s) for reboot

Possible completions:

clear_config              Clear configuration except basic networking
settings.

mgmt-1                    Identifies management module 1

mgmt-2                    Identifies management module 2

reset_to_factory_default  Reset to factory default settings

restart                   Normal warm reboot

system                    Identifies entire system
```

Request a reboot of PFS 6010 management module 1, but then abort the request:

```
PFOS# reboot mgmt-1
Are you sure? [no,yes] no
Aborted: by user
```

Reboot PFS 6010 management module 2, and clear its configuration:

```
PFOS# reboot mgmt-2 clear_config
Are you sure? [no,yes] yes
```

Reboot both management modules at PFS 6010 with dual CPUs:

```
PFOS# reboot system
Are you sure? [no,yes] yes
```

replace config

This command replaces the existing system configuration with the file provided in an input file.

This command initiates a reboot with clear config before applying the new configuration.

Note: This command is different from existing `load config` command. Load config command *merges* the configuration from the config file with the existing configuration on the system.

See also `show replace config-info`.

Note: The password is optional when using this command with scp or sftp methods. If the password is not provided by the user, the system looks for SSH keys to authenticate with the remote device. In FIPs mode, the `replace config` command will use only ECDSA SSH keys. In non-FIPs mode, this command will use RSA and ECDSA SSH keys. Note, however, that in non-FIPS mode if the SSH server supports ECDSA, the RSA key will not be used even if it is the only key available. The command fails if the SSH key authentication also fails, or if the user has provided an invalid username/password.

Note: PFOS will not connect to SSH hosts that only offer SHA-1 hash algorithms for RSA keys.

Syntax

```
replace config <remote configuration file URL>
```

Options

`Remote configuration file URL`	URL for the remote configuration file. Supported methods are sftp, scp and ftp. User password and SSH keys authentication is supported for sftp and scp methods.

Mode

Operational, Configuration

Examples

This example replaces the existing configuration file with the configuration file located at scp://user@10.250.176.44:/home/user/adv-replace-config.

```
PFS# replace config scp://user@10.250.176.44:/home/user/adv-replace-
config
Replace config initiated for file adv-replace-config. System will reboot
now. Clear config is initiated on mgmt-1.
PFS# # Connection to 10.250.177.115 closed by remote host. Connection to
10.250.177.115 closed.

PFS6010# replace config
scp://username:password@10.250.176.44:/home/user/manish/replace-config-
6010 Replace config initiated for file replace-config-6010. System will
reboot now. Clear config is initiated on system.
```

reroute-maps

The pStack protocol assigns a path/pStack/pStack+ port to a map whenever you update the map or its related maps. If a pStack/pStack+ link goes down, the pStack protocol reroutes impacted maps. However, if you add new pStack/pStack+ links, the pStack protocol will not use the new links for existing maps.

This command re-assigns paths to all the maps on a node. Ideally, use this command once you are done adding all the new pStack/pStack+ links; you can see them converged in pfsMesh.

Note: During the rerouting process, traffic will be stopped and restarted and data will be lost regardless if a new routing path is found or if traffic stays with the existing routing path.

Syntax

```
reroute-maps
```

Options

None

Mode

Configuration

Examples

```
PFOS# reroute-maps
This will impact traffic on this node and downstream nodes for re-routed
maps. Do you want to continue? [no,yes]
```

screen-length

Configures the length of the window for the CLI session.

Syntax

```
screen-length rows
```

Options

`rows`	Number of rows for the CLI session window.

Mode

Operational

Examples

```
PFOS# screen-length 100
```

screen-width

Configures the width of the window for the CLI session.

Syntax

```
screen-width columns
```

Options

columns	Number of rows for the CLI session window.

Mode

Operational

Examples

```
PFOS# screen-width 150
```

send

Sends a message to the CLI terminal window of all users or a specified user. Does not send any message to Web UI users.

Syntax

```
send { all | user } message
```

Options

`all`	Sends the message to the terminal of all users.
`user`	Sends the message to the terminal of the specified user.
`message`	Text message. Use double quotes for messages with multiple words.

Mode

Operational

Examples

```
PFOS# send all "Maintenance interval starts in 10 minutes. Log out now."
PFOS#
Message from admin@sitehq at 2017-01-22 12:24:35...
Maintenance interval starts in 10 minutes. Log out now.
PFOS#
```

session idle-timeout

Set the time, in minutes, after which an idle CLI session or Web UI times out. See also `idle-timeout`. To view current settings see `show running-config session`.

Syntax

```
session cli idle-timeout minutes
session webui idle-timeout minutes
```

Options

minutes	Time in minutes. Valid values are 1 to 30; the default is 30 minutes.

Mode

Configuration

Examples

```
PFOS(config)# session cli idle-timeout 15
PFOS(config)# session webui idle-timeout 15
```

show-defaults

Specify whether to display current or default values when showing the configuration.

Syntax

```
show-defaults { true | false }
```

Options

`true`	Show default values.
`false`	Show current values.

Mode

Operational

Examples

```
PFOS# show-defaults true
```

statistics

Reset port deduplication or network statistics for all slots or a selected slot. See also show statistics and show statistics tunnel.

Syntax

```
statistics reset
   { control-packets | deduplication | flow | l2gre-stats | network |
vxlan-stats}
   { slot | all }
```

Options

control-packets	Reset control packet statistics.
deduplication	Reset deduplication statistics.
flow	Reset flow statistics.
l2gre-stats	Reset L2GRE statistics.
network	Reset network statistics.
vxlan-stats	Reset vxlan-stats statistics. **Note:** Use this option to reset pStack+ map statistics.
slot	Reset statistics only on the specified line card.
all	Reset statistics on all line cards.

Mode

Operational

Examples

```
PFOS# statistics reset network 3
Are you sure? [no,yes] y
PFOS# statistics reset deduplication all
Are you sure? [no,yes] y
PFOS# statistics reset control-packets 1
Are you sure? [no,yes] y
PFOS# statistics reset l2gre-stats 1
Are you sure? [no,yes] y
PFOS# statistics reset vxlan-stats 1
Are you sure? [no,yes] y
PFOS# statistics reset flow
Value for '' (<Slot number 1-10, or 'all' to reset counters on all
slots>): all Are you sure? [no,yes] y
```

To reset pStack+ map statistics:

```
statistics reset vxlan-stats all
```

timestamp

Enable or disable display of timestamp as part of command output.

Syntax

```
timestamp { enable | disable }
```

Options

`enable`	Enable display of the timestamp.
`disable`	Disable display of the timestamp.

Mode

Operational

Examples

Output of `show config` command with timestamp disabled.

```
PFOS# timestamp disable
PFOS# show config

config-files
CONFIG
NAME      UPDATED TIME      SIZE
-----------------------------------
SaveFile  Mar-3-2017 11:11  36046

PFOS#
```

Output of `show config` command with timestamp enabled.

```
PFOS# timestamp enable
PFOS# show config
Tue Mar  3  13:38:54.130 UTC

config-files
CONFIG
NAME      UPDATED TIME      SIZE
-----------------------------------
SaveFile  Mar-3-2017 11:11  36046

PFOS#
```

top

Return to the top configuration level.

Syntax

```
top
```

Options

None

Mode

Configuration

Examples

```
PFOS(config-username-ssmith)# top
PFOS(config)#
```

who

Display information about the current CLI user and session.

Syntax

```
who
```

Options

None

Mode

Operational

Examples

```
PFOS# who
Session User  Context From           Proto Date     Mode
*40     admin cli     10.250.133.251 ssh   10:19:10 operational
```

write

Write the current configuration.

Syntax

```
write { memory | terminal }
```

Options

`memory`	Copy the running configuration to the startup configuration database. **Note:** This option does NOT update the startup-configuration file. To update the startup-configuration file use the `copy running-config startup-config` command (see `copy` command).
`terminal`	Writes the current configuration to the CLI terminal.

Mode

Operational

Examples

```
PFOS# write memory
```

9 Show Commands

This chapter contains reference pages for the following show commands:

show app-lib

List entries in the application library. If no item is specified, then all entries for all items are displayed.

Syntax

```
show app-lib
show app-lib advanced-filter [ filter-name ] [ lib-list ]
show app-lib deduplication [ dedup-name ]
show app-lib extended-lb [ elb-name ] [ port-list ]
show app-lib healthcheck [ hc-name ] [ inline-mon-groups-ref ]
show app-lib lb-protocol [ lbprot-name ] [ lib-list ]
show app-lib maskdef [ mask-name ] [ lib-list ]
show app-lib mpls-l3 [ mpls-name ]
show app-lib offset [ offset-name ] [ lib-list ]
show app-lib protocol [ prot-name ] [ lib-list ]
show app-lib protocol-stripping [ strip-name ]
show app-lib slicing [ slice-name ]
show app-lib standard-stripping l2gre [l2gre-configured-address] [l2gre-
configured-id]--This feature requires the PFS 7000 functionality
license.
show app-lib standard-stripping mpls [l2mpls label configured count]
[tunnel-label-configured-count]--This feature requires the PFS 7000
functionality license.
show app-lib tunnel-termination [ term-name ] [ port-list ]
show app-lib vlan-tag-strip [name]
show app-lib standard-stripping vxlan [vnids-configured-count] [vteps-
configured-count]--This feature is only applicable to the PFS 5000/7000
Series.
```

Options

dedup-name	Name of deduplication library to display. If not specified, then display all entries.
elb-name	Name of extended load balancing configuration to display. If not specified, then display all entries.
filter-name	Name of advanced filter (used in slicing) to display. If not specified, then display all advanced filters.
hc-name	Name of health check library entry to display. If not specified, then display all entries.
inline-mon-groups-list	List all inline monitor port groups that use the specified health check library entry.
l2gre-configured-address	Number of L2GRE Destination addresses currently configured.
l2gre-configured-id	Number of L2GRE IDs currently configured.
l2mpls-label-configured-count	Number of L2 MPLS labels currently configured.

`lbprot-name`	Name of load balancing protocol to display. If not specified, then display all entries.
`lib-list`	List all libraries that use the specified item.
`mask-name`	Name of slicing mask to display. If not specified, then display all entries.
`mpls-name`	Name of MPLS-L3 entry (used in stripping) to display. If not specified, then display all entries.
`offset-name`	Name of offset library (used in slicing) to display. If not specified, then display all entries.
`port-list`	List all ports that use the specified item.
`prot-name`	Name of stripping protocol to display. If not specified, then display all entries.
`slicing-name`	Name of slicing configuration to display. If not specified, then display all entries.
`strip-name`	Name of protocol stripping configuration to display. If not specified, then display all entries.
`term-name`	Name of tunnel termination configuration to display. If not specified, then display all entries.
`tunnel-label-configured-count`	Number of tunnel labels currently configured.
`vlanstrip-name`	Name of VLAN tag stripping configuration to display. If not specified, then display all entries.
`vnids-configured-count`	Number of VNIDs currently configured.
`vteps-configured-count`	Number of VTEPs currently configured.

Mode

Operational

Examples

```
PFOS# show app-lib
                  PROTOCOL
                  STRIPPING
NAME              NAME
-----------------------------
Cisco-Fabricpath
Mac-in-Mac
TRILL
VXLAN

      PORT
NAME  NAME
------------
tt_1

                     PORT
NAME                 NAME
---------------------------
```

```
G&G&M&V&V+IPD&L4D
G&G&M&V&V+IPS&L4S
G&G&M&V&V+IPSD&L4SD
VXLAN+IPD&L4D
VXLAN+IPS&L4S
VXLAN+IPSD&L4SD
ip_normalization

NAME                LOADBALANCING NAME
---------------------------------------
Cisco-Fabricpath  ip_normalization
GRE_NVGRE         G&G&M&V&V+IPD&L4D
                  G&G&M&V&V+IPS&L4S
                  G&G&M&V&V+IPSD&L4SD
                  ip_normalization
GTP               G&G&M&V&V+IPD&L4D
                  G&G&M&V&V+IPS&L4S
                  G&G&M&V&V+IPSD&L4SD
                  ip_normalization
MPLS              G&G&M&V&V+IPD&L4D
                  G&G&M&V&V+IPS&L4S
                  G&G&M&V&V+IPSD&L4SD
MVDCAP
Mac-in-Mac        ip_normalization
TRILL             ip_normalization
VLAN_VNTAG        G&G&M&V&V+IPD&L4D
                  G&G&M&V&V+IPS&L4S
                  G&G&M&V&V+IPSD&L4SD
                  ip_normalization
VXLAN             VXLAN+IPD&L4D
                  VXLAN+IPS&L4S
                  VXLAN+IPSD&L4SD
new_protocol1

          SLICING
NAME      NAME
-------------------
nonmatch

                SLICING
NAME            NAME
-------------------------
default-offset

                 SLICING
NAME             NAME
--------------------------
default-maskdef
```

```
      GROUP
NAME  NAME
-------------
hc1
hc2

PFOS# show app-lib standard-stripping l2gre
app-lib standard-stripping l2gre l2gre configured address 256
app-lib standard-stripping l2gre l2gre configured id 91


PFOS# show app-lib standard-stripping mpls
app-lib standard-stripping mpls l2mpls label configured count 101
app-lib standard-stripping mpls tunnel label configured count 91

PFOS# show app-lib standard-stripping vxlan
app-lib standard-stripping vxlan vteps configured count 512
app-lib standard-stripping vxlan vnids configured count 1024
```

show boottime

Show when the system last booted.

Syntax

```
show boottime [ mgmt-card ]
```

Options

`mgmt-card`	Management module on which to perform this command. Valid values are `mgmt-1` and `mgmt-2`. If no `mgmt-card` is specified, then perform this command on the currently active management module. Option is valid only on PFS 6010 with two management modules installed.

Mode

Operational

Examples

```
PFOS# show boottime
boottime 2017-12-05T03:05:49.976414+00:00
```

show certificate

Show information about saved certificates and private keys.

Syntax

```
show certificate
show certificate-authority
show certificate-syslog
show certificate-ldap
```

Options

None

Mode

Operational

Examples

```
PFOS# show certificate
             STATUS
NAME         SIZE  STATE    START DATE                 END DATE                 PRIVATE KEY  MESSAGE
----------------------------------------------------------------------------------------------------
gtglobal.crl 993  standby  0000-00-00T00:00:00+00:00 0000-00-00T00:00:00+00:00
acmeCert.crt 2155 current  2017-01-30T21:59:39-00:00 2027-02-07T21:59:39-00:00  acmeKey.key
acmeKey.key  3272 current  0000-00-00T00:00:00+00:00 0000-00-00T00:00:00+00:00   RSA key ok
```

```
PFOS# show certificate-syslog
NAME           SIZE  STATE    START DATE                 END DATE                  PRIVATE KEY     STATUS
MESSAGE
----------------------------------------------------------------------------------------------
client-115.crt  3137 current 2021-03-22T18:02:15-00:00 2022-03-22T18:02:15-00:00  client-115.key  Public
Key Algorithm: rsaEncryption
acmeCert.crt   2155  standby  2017-01-30T21:59:39-00:00  2027-02-07T21:59:39-00:00  acmeKey.key    Public
Key Algorithm: rsaEncryption

client-115.key 916   current  0000-00-00T00:00:00+00:00  0000-00-00T00:00:00+00:00
acmeKey.key    3272  standby  0000-00-00T00:00:00+00:00  0000-00-00T00:00:00+00:00
```

```
PFS# show certificate-ldap
NAME           SIZE  STATE    START DATE                 END DATE                   PRIVATE KEY        STATUS MESSAGE
------------------------------------------------------------------------------------------------------------------------------
client-115.crt 3137  current  2021-03-22T18:02:15-00:00  2022-03-22T18:02:15-00:00  client-115.key      Public Key Algorithm:
rsaEncryption

acmeCert.crt   2155  standby  2017-01-30T21:59:39-00:00  2027-02-07T21:59:39-00:00  acmeKey.key         Public Key Algorithm:
rsaEncryption
client-115.key 916   current  0000-00-00T00:00:00+00:00  0000-00-00T00:00:00+00:00

acmeKey.key    3272  standby  0000-00-00T00:00:00+00:00  0000-00-00T00:00:00+00:00
```

show cli

Show current CLI session parameters.

Syntax

```
show cli
```

Options

None

Mode

Operational

Examples

```
PFOS# show cli
autowizard true
complete-on-space true
display-level 99999999
history 100
ignore-leading-space true
output-file terminal
paginate true
prompt1 \h\M#
prompt2 \h(\m)#
screen-length 51
screen-width 107
service prompt config true
show-defaults false
terminal xterm
timestamp disable
PFOS#
```

show client-ip-lockout

Displays the client IP address where the login attempt originated.

Syntax

```
show client-ip-lockout [ip address] [ invalid-login-attempts-count |
first-invalid-login-time |account-lock-time]
```

Options

`ip address`	Display information only for this IP address. If no IP address is specified, then display information for all configured IPs.
`invalid-login-attempts-count`	If specified, then display only the number of invalid login attempts.
`first-invalid-login-time`	If specified, then display only the timestamp of the first invalid login.
`account-lock-time`	If specified, then display only the timestamp of when the account was locked.

Mode

Operational

Examples

```
PFS# show client-ip-lockout
               INVALID
               LOGIN                                IP
               ATTEMPTS  FIRST INVALID LOGIN        LOCK
IP ADDRESS     COUNT     TIME                       TIME
----------------------------------------------------------
1.2.3.4        1         2019-10-30T21:09:45-00:00  -
```

show config

Displays configuration files. With no `name` specified, lists all configuration file names with update time and size. When a `name` is specified, displays the contents of that configuration file.

Syntax

```
show config [ file ] [ mgmt-card ]
```

Options

`file`	Name of a specific configuration file.
`mgmt-card`	Management module on which to perform this command. Valid values are `mgmt-1` and `mgmt-2`. If no `mgmt-card` is specified, then perform this command on the currently active management module. Option is valid only on PFS 6010 with two management modules installed.

Mode

Operational, Configuration

Examples

```
PFOS# show config

CONFIG NAME     SIZE   UPDATED TIME
---------------------------------------------
running-config  14967  Feb 18 2017 03:59:35
startup-config  8878   Feb 18 2017 01:26:07


PFOS# show config running-config mgmt-1

/***************************************************
 * Vendor:         NETSCOUT/VSS
 * Platform:       PFS6010
 * Versions:
 *                 vxos_core   0.253
 *                 vxos_cfg    5.3.7.3-92685
 *                 vxos        5.0.0.76-61323fda
 * Date created:
 *                 2017-12-05 03:07:53 UTC
 ***************************************************/
snmp agent disabled
snmp agent ip    0.0.0.0
snmp agent udp-port 161
snmp agent version v1
snmp agent version v2c
snmp agent version v3
snmp agent engine-id enterprise-number 21671
snmp agent engine-id from-text testing
snmp agent max-message-size 50000
snmp target "127.0.0.1 v2"
 ip       127.0.0.1
 udp-port 6000
 tag      [ std_v2_trap ]
 timeout  1500
 retries  3
 v2c sec-name public
!
snmp target "127.0.0.1 v3"
 ip       127.0.0.1
 udp-port 7000
 tag      [ std_v3_trap ]
 timeout  1500
 retries  3
 usm user-name public
 usm sec-level no-auth-no-priv

...
```

show configuration

Show history of configuration actions.

Syntax

Operational mode:

```
show configuration commit list [ command ]
```

Configuration mode:

```
show configuration commit { changes | list }
show configuration merge [ command ]
show configuration rollback changes [ number | diff | latest ]
show configuration [ commit | merge | rollback | running ]
```

Options

`commit list [command]`	(Operational mode) History of committed configuration files. If a command is specified, lists the history for that command. Type `?` for the list of commands.
`commit {changes | list}`	With `list` option, shows history of configuration commits. With `changes` option, shows the changes that were made.
`merge [command]`	Shows merged configuration. With `command` option, restricts the output to the specified command.
`rollback changes [number | diff | latest]`	Shows rollback configuration changes. Optionally specify the ID of a change, the differences in the configuration, or the latest changes. To show the IDs, use the command with no additional options.
`running list [command]`	Shows the running configuration. With `command` option, restricts the output to the specified command.

Mode

Operational, Configuration

Examples

Operational mode:

```
PFOS# show config commit list
2017-02-21 18:50:37
SNo. ID        User       Client      Time Stamp          Label       Comment
~~~~ ~~        ~~~~       ~~~~~~      ~~~~~~~~~~          ~~~~~       ~~~~~~~
0    10891     admin      maapi       2017-02-18 03:03:42
1    10890     admin      maapi       2017-02-18 03:03:42
2    10889     admin      maapi       2017-02-18 03:03:37
```

Configuration mode:

```
PFOS(config)# show configuration rollback changes
chassis line_cards 1
 no ports 1-38.4
!
PFOS(config)# show configuration running interface 5 eth 5-6
interface 5
 eth 5-6
  name                     “”
  class                    Span
  link_state               auto
  speed                    100000
  vid default
  tunnel-termination       enable
  tunnel-termination-name ep1
 !
!
```

show copy

Display the status of file downloads. If no options are specified, then all available status information displays. Information is kept on up to the 100 most recent file download attempts.

Syntax

```
show copy status [ copy-id ] [ file-name | progress | status-msg ]
```

Options

`copy-id`	Numeric identifier of the copy operation. If no copy-id is specified, then display information for all available copy operations.
`file-name`	Show the archive file name.
`progress`	Show the progress of the file creation in percent, or -1 if an error occurred.
`status-msg`	Show the status of the file creation.

Mode

Operational

Examples

```
PFOS# show copy status
copy status 1
 file name  VB6000_4.3.0.160510~1516_2016-05-12_15:41:16.log.tar.gz
 progress   -1
 status msg "Error : Invalid file or directory name "
copy status 2
 file name  VB6000_4.3.0.160510~1516_2016-05-12_16:00:40.log.tar.gz
 progress   17
 status msg InProgress
PFOS# show copy status file-name
ID  FILE NAME
-------------------------------------------------------------
1   VB6000_4.3.0.160510~1516_2016-05-12_15:41:16.log.tar.gz
2   VB6000_4.3.0.160510~1516_2016-05-12_16:00:40.log.tar.gz
VB6000# show copy status 1 progress
progress -1
PFOS#
```

show cores

Display a list of generated core dump files, their sizes, and their creation times.

Syntax

```
show cores [ mgmt-card ]
```

Options

`mgmt-card`	Management module on which to perform this command. Valid values are `mgmt-1` and `mgmt-2`. If no `mgmt-card` is specified, then perform this command on the currently active management module. Option is valid only on PFS 6010 with two management modules installed.

Mode

Operational, Configuration

Examples

```
PFOS(config)# show cores

NAME                                SIZE            TIME
-----------------------------------------------------------------------------
core-chassis.gz                      737395          Dec  14  2016  08:25:31

PFOS(config)#
```

show cpu

Show CPU related information.

Syntax

```
show cpu [ mgmt-card ]
```

Options

`mgmt-card`	Management module on which to perform this command. Valid values are `mgmt-1` and `mgmt-2`. If no `mgmt-card` is specified, then perform this command on the currently active management module. Option is valid only on PFS 6010 with two management modules installed.

Mode

Operational, Configuration

Examples

```
PFOS# show cpu mgmt-1

Mem: 1492268K used, 6572344K free, 0K shrd, 130540K buff, 652320K cached
CPU:   9% usr   0% sys   0% nic  90% idle   0% io   0% irq   0% sirq
Load average: 3.64 3.81 4.04 3/185 3156
  PID  PPID USER     STAT   VSZ %VSZ %CPU COMMAND
 2542     1 root     S    1729m  22%  10% /vss/vxos/bin/switchmgrmain
 2594     1 root     S    1182m  15%   0% /vss/vxos/bin/hal_main
 2543     1 root     S    1091m  14%   0% /vss/vxos/bin/appinframain
 2711     1 root     S     422m   5%   0% /vss/vxos/bin/statcollector
 2654     1 root     S     341m   4%   0% /vss/vxos/bin/chassis
 1040     1 root     S     275m   4%   0% /usr/lib/systemd/systemd-journald
 2709     1 root     S     272m   3%   0% /vss/vxos/bin/flowmapper
 2712     1 root     S     268m   3%   0% /vss/vxos/bin/loadbalance
...
```

show csr

Display the generated Certificate Signing Requests (CSR) string that you can use to request a certificate file from the Certification Authority. See also `generate csr`.

Syntax

```
show csr type <RSA/ECC>
```

Options

`type`	Type of encryption to be used. Supported types are RSA and ECC.

Mode

Operational, Configuration

Examples

```
PFOS# show csr

-----BEGIN CERTIFICATE REQUEST-----
MIIClDCCAXwCAQAwTzELMAkGA1UEAwwCc2ExCzAJBgNVBAoMAm5zMQwwCgYDVQQL
DANwZnMxCzAJBgNVBAcMAmZlMQswCQYDVQQIDAJjYTELMAkGA1UEBhMCdXMwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDmNuCr42h2z923eGlbXu6Pk7jX
ixV+JQCgSPp49D8d9RoIj1y2Cg2ZVpF+lztCIpBFBwttB1uWHYzkyACQnrWq1ALq
5v2S7TlC0q7EuGSwblHqDcQC2UvquTJWes/BU9b1N+esYA2sQfGrjuAVosw3lQKK
1BHZmI9AVzYvoF7gLkARPJv+cxszKTHmFSeZIFH+ALX7oTrMzz5CrTPTZI+VNvjV
bbocz5I8U0XsIg3DwW4e8lohwyO5ssC7QcFgH8snygb46ja3LKctDx+nFC+3V2SW
Lfc/cD7isTcjzF3VKWllstmuJ2oP5j2hVFofS/KapnCE5gQ9OrmKQdFCEFk1AgMB
AAGgADANBgkqhkiG9w0BAQsFAAOCAQEALEh6Ixz+5zA9ktP7gj3X3kBdOigF1/OX
24kunRL6EL7+08/cljU4ut8NdXI6t5zawWvIRxTLJrpKiW02Y+zKLXT+IUWaqzTv
opOFI+0VAt2tWw/7e21n6PILKEXHmlPvT5d5afhRBmc2f15cEWhxP4ldcNU99iJ3
sRGpSKmGe8K3kAUoB9ccLZssmYE27d8ngHQb3wW22lMlXAVTdoReGvrbhmTI2BvS
7v7szfJUtD20LEGwaSYSqOTgXK7e+Bvp4Z1in7b/HW8hs4Y61IECT/QJsGcPECLb
2LEHI6uBQqAnwYQyPho/hf3te1XwIuYk+tMsAks3QsoFaKZGsToDWw==
-----END CERTIFICATE REQUEST-----

PFOS# show csr type RSA

-----BEGIN CERTIFICATE REQUEST-----
MIIClDCCAXwCAQAwTzELMAkGA1UEAwwCc2ExCzAJBgNVBAoMAm5zMQwwCgYDVQQL
DANwZnMxCzAJBgNVBAcMAmZlMQswCQYDVQQIDAJjYTELMAkGA1UEBhMCdXMwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDmNuCr42h2z923eGlbXu6Pk7jX
ixV+JQCgSPp49D8d9RoIj1y2Cg2ZVpF+lztCIpBFBwttB1uWHYzkyACQnrWq1ALq
5v2S7TlC0q7EuGSwblHqDcQC2UvquTJWes/BU9b1N+esYA2sQfGrjuAVosw3lQKK
1BHZmI9AVzYvoF7gLkARPJv+cxszKTHmFSeZIFH+ALX7oTrMzz5CrTPTZI+VNvjV
bbocz5I8U0XsIg3DwW4e8lohwyO5ssC7QcFgH8snygb46ja3LKctDx+nFC+3V2SW
```

```
Lfc/cD7isTcjzF3VKWllstmuJ2oP5j2hVFofS/KapnCE5gQ9OrmKQdFCEFk1AgMB
AAGgADANBgkqhkiG9w0BAQsFAAOCAQEALEh6Ixz+5zA9ktP7gj3X3kBdOigF1/OX
24kunRL6EL7+08/cljU4ut8NdXI6t5zawWvIRxTLJrpKiW02Y+zKLXT+IUWaqzTv
opOFI+0VAt2tWw/7e21n6PILKEXHmlPvT5d5afhRBmc2f15cEWhxP4ldcNU99iJ3
sRGpSKmGe8K3kAUoB9ccLZssmYE27d8ngHQb3wW22lMlXAVTdoReGvrbhmTI2BvS
7v7szfJUtD20LEGwaSYSqOTgXK7e+Bvp4Z1in7b/HW8hs4Y61IECT/QJsGcPECLb
2LEHI6uBQqAnwYQyPho/hf3te1XwIuYk+tMsAks3QsoFaKZGsToDWw==
-----END CERTIFICATE REQUEST-----

PFOS# show csr type ECC

-----BEGIN CERTIFICATE REQUEST-----
MIIBDDCBswIBADBRMQwwCgYDVQQDDANmcmUxCzAJBgNVBAoMAm5zMQwwCgYDVQQL
DANwZnMxDDAKBgNVBAcMA2ZyZTELMAkGA1UECAwCY2ExCzAJBgNVBAYTAnVzMFkw
EwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEt2pWzeYLlyi8+l4BDQhz52DD94d2eHVT
eMjl/w7I3EbZNMBjIH/evKSj5iNddWaPU3ulsDzDTK/c7RJp0TDzqqAAMAoGCCqG
SM49BAMCA0gAMEUCIQC6mdpW4axgfap3tSKczGS8QBuuxRhyhpO4PoYwSOtoXwIg
D8N2u+bP0Kzh7MPrYB30pYhIdL25gdBIlKwIdn6AeBw=
-----END CERTIFICATE REQUEST-----

PFOS# show csr type ECC

-----BEGIN CERTIFICATE REQUEST-----
MIG7MGICAQAwADBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IABFHzXCQ9t8iA5vod
+OryBSYGbhF0NlYWMjyFyw+SciO4Uwci5dRta7WDF0Mrceb0CJ9o3NTFTGv6MCXg
S21EM+2gADAKBggqhkjOPQQDAgNJADBGAiEA1cxVFRcM8vu9yqjONgkOKnnZ7wvG
bHEHfzRIpzwSWFECIQCE1+QjBQLPuuSWk/MyUXnrpbcKrnKavwlDaanhWeX4BQ==
-----END CERTIFICATE REQUEST-----
```

show currenttime

Display the current system time.

Syntax

```
show currenttime
```

Options

None

Mode

Operational

Examples

```
PFOS# show currenttime
currenttime 2017-02-11T19:57:04.624571+00:00
```

show disk-type

Display the current disk type.

Syntax

```
show disk-type
```

Options

None

Mode

Operational

Examples

```
PFOS# show disk-type
ATP_mSATA_99001160122000000081

PFOS# show disk-type
M.2__S42__3ME4_YCA12203280150038
```

show disk-usage

Display the current disk usage.

Syntax

```
show disk-usage [ mgmt-card ]
```

Options

`mgmt-card`	Management module on which to perform this command. Valid values are `mgmt-1` and `mgmt-2`. If no `mgmt-card` is specified, then perform this command on the currently active management module. Option is valid only on PFS 6010 with two management modules installed.

Mode

Operational, Configuration

Examples

```
PFOS# show disk-usage

Filesystem           1K-blocks      Used Available Use% Mounted on
/dev/root             27442744    751344  25297360   3% /
devtmpfs               8152844         0   8152844   0% /dev
tmpfs                  8154592      3072   8151520   0% /dev/shm
tmpfs                  8154592       224   8154368   0% /run
tmpfs                  8154592         0   8154592   0% /sys/fs/cgroup
tmpfs                  8154592        32   8154560   0% /tmp
/dev/sda3              2798840   1188676   1467992  45% /sda3
/dev/sda4                38888      4595     32285  12% /sd4
169.254.0.3:/         27442744    648752  25399952   2% /mnt/remote

PFOS# show disk-usage mgmt-2

Filesystem           1K-blocks      Used Available Use% Mounted on
/dev/root             27442744    648756  25399948   2% /
devtmpfs               8152844         0   8152844   0% /dev
tmpfs                  8154592         4   8154588   0% /dev/shm
tmpfs                  8154592       224   8154368   0% /run
tmpfs                  8154592         0   8154592   0% /sys/fs/cgroup
tmpfs                  8154592        28   8154564   0% /tmp
/dev/sda3              2798840   1041596   1615072  39% /sda3
/dev/sda4                38888      4595     32285  12% /sd4
```

show energy-consumption

Displays the PFS 5000/7000 total estimated daily power usage in kWh based on sampling over the past 1 hour.

Syntax

```
show energy-consumption
```

Options

None

Mode

Operational

Example

```
PFOS# show energy-consumption
energy consumption 2.88
```

show eula

Display the End User License Agreement that an administrator must accept before any users can use PFOS.

Syntax

```
show eula
```

Options

None

Mode

Operational, Configuration

Examples

```
PFOS# show eula
License agreement displays
End of document
PFOS#
```

show fabric_module

Show information about switch fabric cards.

Syntax

```
show fabric_module [ card-num ] [ option ]
```

Options

card-num	Specific fabric card (1-4).
option	Optionally specify the type of information. Type ? for a list of options.

Mode

Operational

Examples

```
PFOS# show fabric_module 1
fabric_module 1 state OK
fabric_module 1 Product ID 1361
fabric_module 1 model "vFabric 201"
fabric_module 1 module part number VP_01941
fabric_module 1 module revision number VP_0
fabric_module 1 module serial number 15077268
fabric_module 1 PCBA part number VA_00684
fabric_module 1 PCBA revision 06
fabric_module 1 PCBA serial number VSSAL-14100828
fabric_module 1 CAT part number VP_01941
fabric_module 1 temperature 47
```

show fan_tray

Show information about the fan trays.

Syntax

```
show fan_tray [ tray-num ] [ option ]
```

Options

`tray-num`	Specific a tray (1 or 2).
`option`	Optionally specify the type of information. Type `?` for a list of options.

Mode

Operational

Examples

```
PFOS# show fan_tray model
fan_tray 1 model "vBlower 500"
fan_tray 2 model "vBlower 500"
```

show filter

List the filters currently in the filter library.

Syntax

```
show filter [ filtername ] [ used_in_maps ]
```

Options

`filtername`	Name of a specific filter from the filter library.
`used_in_maps`	Lists only the filters that are included in traffic maps.

Mode

Operational

Examples

```
PFOS# show filter used_in_maps

         USED
         IN
NAME     MAPS
---------------
jm_test  1
```

show firmware

List the firmware that has been uploaded to the chassis.

Syntax

```
show firmware [ mgmt-card ]
```

Options

`mgmt-card`	Management module on which to perform this command. Valid values are `mgmt-1` and `mgmt-2`. If no `mgmt-card` is specified, then perform this command on the currently active management module. Option is valid only on PFS 6010 with two management modules installed.

Mode

Operational

Examples

```
PFOS# show firmware
UPGRADE  UPGRADE
NAME                                VERSION        SIZE      TYPE  STATE    SLOTS  MODE
SLOTS    TIME
---------------------------------------------------------------------------------------------
-----------------------------
firmware_11111212-000E-150513~0945  11111212-000E  17964984  1410  standby  --     --       -
-       Oct 8 2016 03:50:12
```

show full-configuration

Display information about the current running configuration.

Syntax

```
show full-configuration [ option ]
```

Options

`option`	Type of configuration information to display. Type `?` for a list of options.

Mode

Configuration

Examples

```
PFOS(config)# show full-configuration filter
filter JCTest
 type           traffic
 expression     "EType 0800"
 created_by_gui true
!
filter nonmatch
 type           traffic
 expression     " "
 created_by_gui false
!
filter unfiltered
 type           traffic
 expression     " "
 created_by_gui false
!
```

show gps

Show GPS status.

Syntax

```
show gps [ satellite-count | status ]
```

Options

satellite-count	Number of satellites used for the GPS signal.
status	Current status of GPS.

Mode

Operational

Examples

```
PFOS# show gps
gps status "GPS not connected"
gps satellite count 0
```

show history

Show CLI command history.

Syntax

```
show history [ number ]
```

Options

`number`	Number of commands to display.

Mode

Operational, Configuration

Examples

```
PFOS# show history 4
10:14:06 -- show-defaults true
10:14:23 -- show configuration
10:14:36 -- show configuration commit list
10:15:32 -- statistics reset_port_stats
```

show home

List files stored in the user home directory.

Syntax

```
show home [ mgmt-card ]
```

Options

`mgmt-card`	Management module on which to perform this command. Valid values are `mgmt-1` and `mgmt-2`. If no `mgmt-card` is specified, then perform this command on the currently active management module. Option is valid only on PFS 6010 with two management modules installed.

Mode

Operational, Configuration

Examples

```
PFOS# show home

NAME      SIZE  TIME
--------------------------------------
test.log  134   Jul 24 2017 23:33:40
```

show hw-info

Show information about the chassis hardware.

Syntax

```
show hw-info [ option ]
```

Options

option	Specify the type of information to display. Type ? for a list of options.

Mode

Operational

Examples

```
PFOS# show hw-info fabric_module 1
 state                  OK
 Product ID             1361
 model                  "vFabric 201"
 module part number     VP_01941
 module revision number AF
 module serial number   16092036
 PCBA part number       VA_00684
 PCBA revision          AE
 PCBA serial number     VSSAL-14071070
 sku part number        VA_00684_12345
 temperature            42
 fan1 speed             13351
 fan2 speed             13606
 fan3 speed             13629
```

```
PFS6010# show hw-info management_module 2
hw-info management_module 2
 state                  standby
 Product ID             1350
 model                  "vCPU 300"
 module part number     VP_01940
 module revision number AE
 module serial number   16099504
 PCBA part number       VA_00722
 PCBA revision          AL
 PCBA serial number     VMSVS-16025589
 sku part number        VP_02011
 FPGA                   "00007000 rev 0018"
```

show interface

Show information about the specified interface.

Syntax

```
show interface [ slot ] [ option ]
```

Options

If no options are specified, then active interface IP addresses (IPv4 address, IPv6 address, gateway IP address and DNS IP addresses) and the management MAC address are displayed.

`slot`	Slot number.	
`option`	Specify the type of information to display. Valid options are:	
	`FPGA_1`	FPGA-1 ID and rev.
	`FPGA_2`	FPGA-2 ID and rev.
	`PCBA_part_number`	PCBA Part Number
	`PCBA_revision`	Blade PCBA revision
	`PCBA_serial_number`	PCBA Serial Number
	`Product_ID`	Product Identity
	`eth portidsuboption`	Display information about a specific port.
	`model`	Card Model
	`module_part_number`	Part Number
	`module_revision_number`	Revision Number
	`module_serial_number`	Blade Serial Number
	`ports_num`	Number of ports on line card
	`sku_part_number`	SKU Part Number
	`state`	Slot state. For a PFS 5010 with a 16-port limited capacity license, ports 1-16 show as "OK" and ports 17 and greater show as "locked."
	`temperature`	Module temperature

suboption	VID	VLAN ID applied. PFOS derives VLAN IDs based on following: 1. If pStack is enabled and this port is being used as an inbound port in a map configuration, then the VLAN ID is assigned by the pStack protocol, OR 2. User-defined VLAN ID is used if (1) is not true, OR 3. Default VLAN ID is used if (1) and (2) are not true See also `show vlan-translation-table`.
	XCVR	Transceiver present
	XCVR-bias-current	Transceiver bias current (mA)
	XCVR-channel-bias-current	Transceiver bias current per channel (mA)
	XCVR-model	Transceiver model
	XCVR-power-Rx	Transceiver Optical Pwr, Rx (dBm)
	XCVR-channel-power-Rx	Transceiver Optical Pwr, Rx per channel (dBm)
	XCVR-power-Tx	Transceiver Optical Pwr, Tx (dBm)
	XCVR-channel-power-Tx	Transceiver Optical Pwr, Tx per channel (dBm)
	XCVR-revision	Transceiver revision number
	XCVR-serial-number	Transceiver serial number
	XCVR-supply-voltage	Transceiver supply voltage (Volts)
	XCVR-temperature	Transceiver temperature (degrees Celsius)
	XCVR-type	Transceiver type
	link	Port Link state
	mac-address	Port MAC Address
	paired-port	Paired Port for Inline
	port-group-ref	List of port groups using this port
	pstack-ref-map	List of traffic map using pStack port
	ref_lbg	List of load balancing groups using this port
	ref_map	List of traffic maps using this port

Mode

Operational

Examples

```
PFOS# show interface
interface active-network-connection ip4 address 10.250.177.115/23
interface active-network-connection ip6 address ::/0
interface active-network-connection ip4 gateway 10.250.176.1
ID  DNS IP
-------------
0   8.8.8.8

ID  IPv6 DNS
-----------------------
0   FD49:B785:906:FAB0::3
```

```
ID  MAC ADDRESS
-----------------------
0   8C:EA:1B:FF:BB:A4
```

```
PFOS# show interface state
ID  STATE
-----------
1   empty
2   empty
3   empty
4   empty
5   empty
6   empty
7   empty
8   empty
9   OK
10  OK

PFOS# show interface 10 state
state OK
```

Display the list of maps going via a specific interface:

```
PFOS# show interface 1 eth ref_map
PORT  MAP
ID    NAME
--------------
1-2   map4
1-48  map4
```

Display the list of port group references for the ports on a specific interface:

```
PFOS# show interface 2 eth port-group-ref
PORT  GROUP  GROUP  GROUP  GROUP
ID    NAME   NAME   NAME   NAME
----------------------------------
2-1          npg64
2-2          npg64
 . . .
```

Display the list of pStack maps going via a specific interface:

```
PFOS# show interface 1 eth pstack-ref-map
PORT
ID    MAP NAME
----------------------------
1-32   ffba7e00~map4~2241
1-48   ffba7e00~map4~2241
```

Display the VLAN ID associated with an interface:

```
PFOS# show interface 1 eth vid
PORT
ID    VID
------------
1-1   1
1-2   2241
1-3   3
1-4   4
1-5   5
1-6   6
 .  .  .
```

Show the list of port groups that a specific port belongs to:

```
PFOS# show interface 7 eth 7-21 port-group-ref
Inline
MPG
--------
AG-1
```

Display information about a specific port.

```
PFS5100# show interface 1 eth 1-1
eth 1-1
 VID                       1
 mac address               cc:37:ab:bd:46:69
 XCVR                      present
 XCVR model                "FINISAR CORP FTLC9551REPM   "
 XCVR revision             A
 XCVR serial number        "XYD04V1        "
 XCVR temperature          22.16
 XCVR supply voltage       3.19
 XCVR bias current         7.5
 XCVR channel bias current [ -4.24 -4.26 -4.24 -4.29 ]
 XCVR power Rx             -2.95
 XCVR channel power Rx     [ -2.92 -3.18 -2.28 -3.51 ]
 XCVR power Tx             0.69
 XCVR channel power Tx     [ 0.65 0.65 0.81 0.65 ]
 XCVR type                 100GBase-SR4
 link                      down
```

For a PFS 5010 with a 16-port limited capacity license, ports 1-16 show as "OK" and ports 17 and greater show as "locked."

```
PFS5010# show interface 1 eth 1-1 state
state OK

PFS5010# show interface 1 eth 1-17 state
state locked
```

show interface gre

Display GRE tunnel interface status. See interface gre for configuration details. Refer to the ***PFOS 6.x User Guide*** for GRE Tunnel Origination/Termination feature details.

Syntax

```
show interface gre [ name ]
```

Options

name	Name of a previously configured GRE tunnel interface.

Mode

Operational

Examples

```
PFOS# show interface gre
NAME  STATE  MAP NAME     MAP NAME      LBG NAME
---------------------------------------------------
tun1  up     m_to_pstack  m_from_pstack   lbg1
```

show interface ip

Display IP interface status for GRE or VXLAN tunnel origination/termination. See interface ip for configuration details. Refer to the ***PFOS 6.x User Guide*** for GRE and VXLAN Tunnel Origination/Termination feature details.

Syntax

```
show interface ip [ name ]
```

Options

name	Name of a previously configured interface ip.

Mode

Operational

Examples

```
PFS5010# show interface ip
             GRE   VXLAN
NAME  STATE  NAME  NAME
--------------------------
ip1   up     gre1   vxlan_01
             gre2   vxlan_11
```

show interface mgmt

Show details about the management interface.

Syntax

```
   show interface mgmt slot [ mac_address |ifconfig | ethtool ]
```

Options

If no options are specified, then output for ethtool, ifconfig, and mac_address are all displayed.

slot	Optional. Only slot 0 supported.
ethtool	Display management port settings such as link modes, speed, port type, auto-negotiation, etc.
ifconfig	Display link status, IPv4 and IPv6 addresses, and Rx/Tx packets.
mac_address	Displays Port MAC Address.

Mode

Operational

Examples

```
PFOS# show interface mgmt 0 ifconfig
ifconfig eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
                 inet 10.250.177.115  netmask 255.255.254.0  broadcast 10.250.177.255
                 inet6 fe80::8eea:1bff:feff:bba4  prefixlen 64  scopeid 0x20<link>
                 inet6 fd49:b785:906:fab0:8eea:1bff:feff:bba4  prefixlen 64  scopeid
0x0<global>
                 ether 8c:ea:1b:ff:bb:a4  txqueuelen 1000  (Ethernet)
                 RX packets 615  bytes 54449 (53.1 KiB)
                 RX errors 0  dropped 0  overruns 0  frame 0
                 TX packets 177  bytes 30714 (29.9 KiB)
                 TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
                 device memory 0xffff00000-ffff1ffff


PFOS# show interface mgmt ethtool
interface mgmt 0
ethtool Settings for eth0:
                Supported ports: [ TP ]
                Supported link modes:   10baseT/Half 10baseT/Full
                                        100baseT/Half 100baseT/Full
                                        1000baseT/Full
                Supported pause frame use: Symmetric
                Supports auto-negotiation: Yes
                Supported FEC modes: Not reported
                Advertised link modes:  10baseT/Half 10baseT/Full
                                        100baseT/Half 100baseT/Full
                                        1000baseT/Full
                Advertised pause frame use: Symmetric
                Advertised auto-negotiation: Yes
                Advertised FEC modes: Not reported
                Speed: 1000Mb/s
                Duplex: Full
                Port: Twisted Pair
                PHYAD: 1
                Transceiver: internal
                Auto-negotiation: on
                MDI-X: off (auto)
                Supports Wake-on: pumbg
                Wake-on: g
                Current message level: 0x00000007 (7)
                                       drv probe link
                Link detected: yes
```

```
PFOS# show interface mgmt 0 mac_address
mac address A8:2B:B5:58:4F:60
```

show interface vxlan

Display VXLANtunnel interface status. See interface vxlan for configuration details. Refer to the ***PFOS 6.x User Guide*** for VXLAN Tunnel Origination/Termination feature details.

Syntax

```
   show interface vxlan[ name ]
```

Options

name	Name of a previously configured VXLAN tunnel interface.

Mode

Operational

Example

```
PFS5010# show interface vxlan
             NETWORK   MONITOR  LBG
NAME  STATE  MAPS      MAPS     NAME
-------------------------------------
Vxlan1  up     m2        m1       lbg1
Vxlan2  up     m2        m1
Vxlan3  up     m2        m1
```

show ip

Display network statistics. The output from this command can be lengthy.

Syntax

```
show ip sockets [ mgmt-card ]
```

Options

`mgmt-card`	Management module on which to perform this command. Valid values are `mgmt-1` and `mgmt-2`. If no `mgmt-card` is specified, then perform this command on the currently active management module. Option is valid only on PFS 6010 with two management modules installed.

Mode

Operational, Configuration

Examples

```
PFOS# show ip sockets mgmt-2
Active Internet connections (servers and established) Proto Recv-Q Send-
Q Local Address Foreign Address State tcp 0 0 127.0.0.1:4565 0.0.0.0:*
LISTEN tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN tcp 0 0 0.0.0.0:443 0.0.0.0:*
LISTEN tcp 0 0 127.0.0.1:6268 0.0.0.0:*
. . .
```

show lb-criteria

Display defined load balance criteria.

Syntax

```
show lb-criteria [ lbg-criterion |
    port-group-ref [ inline-monitor-group | inline-network-group |
        monitor-group | network-group ]
    ref-map [ map-name ]
    used_in_maps count ] |
```

Options

`lbg-criterion`	Display only the single specified load balance criterion.
`port-group-ref`	Display the port groups that reference load balancing criteria. If `inline-monitor-group`, `inline-network-group`, `monitor-group`, or `network-group` is specified, then restrict the list to that type of port group.
`ref-map [ map-name ]`	Display only criteria that are currently referred to by a traffic map. If a `map-name` is specified, then display only criteria that are referred to by that specific traffic map.
`used_in_maps count`	Display the load balance criteria that are used in exactly `count` defined traffic maps.

Mode

Operational

Examples

```
PFOS#  show lb-criteria
                             USED
                             IN                          Inline   Inline
Group Name                   MAPS  MAP NAME    MPG  NPG  NPG      MPG
-------------------------------------------------------------------------
ELB                          0
IP_Dest                      0     map-TC-B
                                   map-TC-SSL
IP_Dest_Src                  0
IP_Dest_Src_and_L4_Dest_Src  0
IP_Dest_and_L4_Dest          0
IP_Src                       0     map-TC-B
                                   map-TC-SSL
IP_Src_and_L4_Src            0
MAC_Dest_Etype_Port          0
MAC_Dest_Src_Etype_Port      0
```

```
MAC_Src_Etype_Port           0
lbc7                         1     map7

PFOS# show lb-criteria used_in_maps 2
% No such element exists.
```

```
PFOS#  show lb-criteria ref-map
Group
Name     MAP NAME
---------------------
IP_Dest  map-TC-B
         map-TC-SSL
IP_Src   map-TC-B
         map-TC-SSL
```

```
PFOS# show lb-criteria port-group-ref
                                       Inline  Inline
Group Name                   MPG  NPG  NPG     MPG
-------------------------------------------------------
ELB
IP_Dest
IP_Dest_Src
IP_Dest_Src_and_L4_Dest_Src
IP_Dest_and_L4_Dest
IP_Src
IP_Src_and_L4_Src
MAC_Dest_Etype_Port
MAC_Dest_Src_Etype_Port
MAC_Src_Etype_Port
lbc7
```

show license

Display information about the currently installed license key. See also `show mgmt license` command for license details.

Syntax

```
show license
```

Options

None

Mode

Operational

Examples

PFS 5000 Support Full License

```
PFS# show license
                                                             EXPIRATION

NAME     DESCRIPTION                          TYPE  STATE    DATE        MAC ADDRESS
PORTS
---------------------------------------------------------------------------------------------
------
Support  Supports base features and upgrades  full  current  Nov 2020    8c:ea:1b:26:76:09
all
```

PFS 5000 Support Full License - 16-port License

```
PFS# show license
                                                             EXPIRATION

NAME     DESCRIPTION                          TYPE  STATE    DATE        MAC ADDRESS
PORTS
---------------------------------------------------------------------------------------------
------
Support  Supports base features and upgrades  full  current  Nov 2020    8c:ea:1b:26:76:09
16-ports
```

PFS 5000 Support Trial License

```
PFS# show license
                                                          EXPIRATION
```

```
NAME    DESCRIPTION                         TYPE  STATE   DATE           MAC ADDRESS       PORTS
-------------------------------------------------------------------------------------------------
Support Supports base features and upgrades trial current Trial license  8c:ea:1b:ff:bb:a4 all
                                                          valid 85 days
```

PFS 7000 License

```
                                                            EXPIRATION
NAME      DESCRIPTION                          TYPE  STATE    DATE        MAC ADDRESS        PORTS
---------------------------------------------------------------------------------------------------
Support   Supports base features and upgrades  full  current  Jul 2020    8c:ea:1b:ff:bb:a4   all
PFS 7000  Supports PFS 7000 features           full  current  -           8c:ea:1b:ff:bb:a4   all
```

PFS 7000 Trial License

```
                                                             EXPIRATION
NAME      DESCRIPTION                          TYPE  STATE     DATE           MAC ADDRESS      PORTS
-----------------------------------------------------------------------------------------------------
Support   Supports base features and upgrades  full  current   Dec 2020       8c:ea:1b:ff:bb:a4 all
PFS 7000  Supports PFS 7000 features           trial current   Trial license  8c:ea:1b:ff:bb:a4 all
                                                               valid 90 days
```

show linux-ptp

Note: This command is only applicable for the PFS 5000/7000 Series. To view PTP timing support for PFS 6000 devices, see `show ptp`.

Display PFS 5000/7000 Linux PTP information. See also `linux-ptp`.

Syntax

```
show linux-ptp [ status | clock-info]
```

Options

`status`	Show linux-ptp status information: • NA - Linux-ptp is not enabled. • Syncing - Linux-ptp is enabled and is syncing time with network PTP clocks. • Not Syncing - Linux-ptp is enabled but is not receiving valid PTP timing data.
`clock-info`	Show linux-ptp clock information. • NA - Linux-ptp is not enabled. • Clock data varies depending on current state

Mode

Operational

Examples

```
PFOS# show linux-ptp status
linux-ptp status Syncing

PFOS# show linux-ptp clock-info
sending: GET TIME_STATUS_NP
80a235.fffe.c4521c-0 seq 0 RESPONSE MANAGEMENT TIME_STATUS_NP
master_offset -46
ingress_time 1695149885799796428
cumulativeScaledRateOffset +0.000000000
scaledLastGmPhaseChange 0
gmTimeBaseIndicator 0
lastGmPhaseChange 0x0000'0000000000000000.0000
gmPresent true
gmIdentity 000efe.fffe.0110e2
```

show lldp

Display learned neighbor information from incoming Link Layer Discovery Protocol (LLDP) Packets. Refer to "Neighbor Discovery Using LLDP" in the *PFOS 6.x User Guide* for details.

Syntax

```
show lldp [neighbors [<local-port>] [remote-info [<chassis-id>] {hold-
time | port-desc | remote-port | system-desc | sys-mgmt-ip-addr |
system-name} ] ]
```

Options

`local-port`	Display LLDP Information learned on the “local-port” specified. If no local-port is specified, PFOS displays information learned on all ports in the system.
`chassis-id`	Display LLDP Information learned from Remote System with specified chassis-ID connected to the “local-port”.
`hold-time`	Displays LLDP Hold time of all learned neighbors on the specific local-port.
`port-desc`	Displays LLDP Port Description of all learned neighbors on the specific local-port.
`remote-port`	Displays LLDP Port Id of all learned neighbors on the specific local-port.
`system-desc`	Displays LLDP System Description of all learned neighbors on the specific local-port. When neighbor system description includes a space or any special character, it will be displayed in quotes. For example, a neighbor description of Cisco IOS Software, C3560E will be displayed as "Cisco IOS Software, C3560E".
`system-mgmt-ip-addr`	Displays the System Management IP Address of the specific remote LLDP neighbor on the local-port.
`system-name`	Displays LLDP System Name of all learned neighbors on the specific local-port.

Mode

Operational

Examples

This command can show option matching neighbors on all ports. The following example is for matching hold-time.

```
PFS5120# show lldp neighbors remote-info hold-time 120
LOCAL                  HOLD   SYSTEM   SYSTEM         MANAGEMENT
```

```
PORT  CHASSIS ID       TIME  NAME    DESCRIPTION     ADDRESS       REMOTE PORT    PORT
DESCRIPTION  --------------------------------------------------------------------------------
------------------
1-10 SPIRENT7-1/1type2 120 STC7  STC7-1/1-type2 10.250.176.7 SPIRENT7-1/1-type2  Spirent Port
7-1/1
1-64.1 SPIRENT7-1/1type2 120 STC7  STC7-1/1-type2 10.250.176.7 SPIRENT7-1/1-type2 Spirent
Port 7-1/1
```

The output of notab format is slightly different from the output of tab format.

```
PFS5120# show lldp neighbors | notab
lldp neighbors 1-10
remote-info SPIRENT7-1/1type1
  hold time   110
  remote port SPIRENT7-1/1-type1
remote-info SPIRENT7-1/1type2
  hold time           120
  system name         STC7
  system desc         STC7-1/1-type2
  system mgmt ip addr 10.250.176.7
  remote port         SPIRENT7-1/1-type2
  port desc           "Spirent Port 7-1/1"
remote-info SPIRENT7-1/1type3
  hold time           130
  system name         STC7
  system desc         STC7-1/1-type3
  system mgmt ip addr 10.250.176.7
  remote port         SPIRENT7-1/1-type3
  port desc           "Spirent Port 7-1/1"
lldp neighbors 1-64.1
remote-info SPIRENT7-1/1type1
  hold time   110
  remote port SPIRENT7-1/1-type1
remote-info SPIRENT7-1/1type2
  hold time           120
  system name         STC7
  system desc         STC7-1/1-type2
  system mgmt ip addr 10.250.176.7
  remote port         SPIRENT7-1/1-type2
  port desc           "Spirent Port 7-1/1"
remote-info SPIRENT7-1/1type3
  hold time           130
  system name         STC7
  system desc         STC7-1/1-type3
  system mgmt ip addr 10.250.176.7
  remote port         SPIRENT7-1/1-type3
  port desc           "Spirent Port 7-1/1"
```

```
PFS# show lldp neighbors ?
Description: LLDP remote information
Possible completions:
  1-1    Local system port ID
  1-7    Local system port ID
  1-39   Local system port ID
  1-40   Local system port ID

  |      Output modifiers

  <cr>

Possible match completions:

  remote-info   Remote system info


PFS# show lldp neighbors 1-1 remote-info ?
Description: Remote system info
Possible completions:
  8c:ea:1b:ff:b9:9e   System unique ID
  |                   Output modifiers
  <cr>
Possible match completions:
  hold-time             System LLDP TTL/Hold time value
  port-desc             System port description
  remote-port           System port ID
  system-desc           System description
  system-mgmt-ip-addr   System management IP address
  system-name           System namePFS5010# show lldp neighbors 1-1 remote-info

PFS# show lldp neighbors 1-1 remote-info 8c:ea:1b:ff:b9:9e ?
Description: Remote system info
Possible completions:
  hold-time             System LLDP TTL/Hold time value
  port-desc             System port description
  remote-port           System port ID
  system-desc           System description
  system-mgmt-ip-addr   System management IP address
  system-name           System name
  |                     Output modifiers
  <cr>
PFS# show lldp neighbors 1-1 remote-info 8c:ea:1b:ff:b9:9e remote-port
remote port 27
PFS# show lldp neighbors 1-1 remote-info 8c:ea:1b:ff:b9:9e system-mgmt-ip-addr
system mgmt ip addr 10.250.177.119
PFS# show lldp neighbors 1-1 remote-info 8c:ea:1b:ff:b9:9e system-name
system name PFS-5010-Node119
```

show load-balance

Display information about one or more load balancing groups.

Syntax

```
show load-balance [ lbg-name |
    Error_code [ error-code ] |
    Oper_status [ down | up ] |
    port-group-ref [ monitor-group | network-group ] |
    ref_map [ map-name ] |
    ports port-id ]
```

Options

`lbg-name`	Display information about the specified load balancing group. If no `lbg-name` is specified, then display information about all load balancing groups.
`Error_code`	Limit the columns displayed to error code. If an `error-code` is also specified, then further limit the display to that error code.
`Oper_status`	Limit the columns displayed to operational status. If `down` or `up` is also specified, then further limit the display to that status.
`port-group-ref`	Limit the columns displayed to port group references. If `monitor-group` or `network-group` is also specified, then further limit the display to that type of port group.
`ref_map`	Limit the columns displayed to traffic maps that use this load balancing group. If a `map-name` is also specified, then further limit the display to that traffic map.
`ports port-id`	Limit the columns displayed to load balancing groups that contain port `port-id`.

Mode

Operational

Examples

```
PFOS#  show load-balance
            ERROR  OPER    MAP   GROUP  GROUP         ERROR  OPER
Group Name  CODE   STATUS  NAME  NAME   NAME   PORT   CODE   STATUS
--------------------------------------------------------------------
regular_LB  None   Down    map7                1-5    None   Down
                                               1-6    None   Down
PFOS# show load-balance ports 1-5

                         FAILOVER
Group Name  DESCRIPTION  ACTION     TYPE     PORTS
```

```
----------------------------------------------------------
regular_LB  -            Rebalance  Monitor  [ 1-5 1-6 ]

PFOS# show load-balance port-group-ref monitor-group
Group Name     MPG
--------------------------
passive-A-LBG  MPG-LBG-A
passive-B-LBG  MPG-LBG-B


PFOS# show load-balance rrg
Group  ERROR  OPER    MAP                     ERROR  OPER
Name   CODE   STATUS  NAME  MPG  NPG  PORT    CODE   STATUS  NAME
-------------------------------------------------------------------
rrg    None   Up      rrm             1-13    None   Up
                                      1-49.1  None   Up
                                      1-49.2  None   Up
                                      1-49.3  None   Up
                                      1-49.4  None   Up
                                      1-53.2  None   Up
                                      1-53.3  None   Up
                                      1-53.4  None   Up
```

show log

Display directory of available log files, or display contents of log files. Optionally use page controls to manage the output.

Syntax

```
show log [ service ][ start-time time ][ end-time time ][ mgmt-card ]
```

Options

`service`	Display the contents of the specified service log file. If no `service` is specified, then display a list of all log files. • access_control: Display log messages for Access Control • app_framework: Display log messages for applications framework • applibs: Display log messages for all firmware application libraries • apps: Display log messages for all applications • asi: Display log messages for ASI • chassis: Display log messages for Chassis Manager • file_mgmt: Display log messages for File management • flowmapper: Display Flowmapper related log messages • framework_service: Display log messages for framework service • hal: Display log messages for HAL • lldp: Display log messages for LLDP • load_balancer: Display log messages for Load Balancer • ncm: Display log messages for NCM • ntp: Display log messages for NTP • port_config: Display log messages for Port configurator • powersafe: Display log messages for Powersafe • pstack: Display log messages for pStack • radsec: Display log messages for radsec • snmp: Display log messages for SNMP • startup: Display startup log messages • stats_collector: Display log messages for Stats Collector • switch_manager: Display log messages for Switch Manager • system_monitor: Display log messages for Startup system monitor • system_notification: Display log messages for System notification • system_settings: Display log messages for System Setting • trigger: Display log messages for trigger
`start-time`	Start time in the format `"YYYY-MM-DD HH:MM:SS"` (including the double quotes), or `boot` for last boot time.
`end-time`	End endtime in the format "`YYYY-MM-DD HH:MM:SS`" (including the double quotes), or `now` for current time.
`mgmt-card`	Management module on which to perform this command. Valid values are `mgmt-1` and `mgmt-2`. If no `mgmt-card` is specified, then perform this command on the currently active management module. Option is valid only on PFS 6010 with two management modules installed.

Mode

Operational, Configuration

Examples

```
PFOS# show log startup start-time boot
-- Logs begin at Tue 2019-02-05 01:56:25 UTC, end at Tue 2019-02-05 18:05:24 UTC. --
Feb 05 03:06:41 vss-kbp-proto systemd[1]: Starting VSS Initialization...
Feb 05 03:06:41 vss-kbp-proto systemd[1]: About to execute: /vss/vxos/bin/startup.sh
Feb 05 03:06:41 vss-kbp-proto systemd[1]: Forked /vss/vxos/bin/startup.sh as 2756
. . .
```

```
PFS5031-56X-ZTP# show log chassis
-- Logs begin at Wed 2023-09-20 23:03:57 UTC, end at Thu 2023-10-05 21:05:28 UTC. --
Sep 20 23:05:14 vss-kbp-proto wait4confd_status.py[831]: PFOS check CDB started ...
Sep 20 23:05:14 vss-kbp-proto wait4confd_status.py[831]: check_cdb_phase stderr:
Sep 20 23:05:14 vss-kbp-proto wait4confd_status.py[831]: check_cdb_phase stdout: phase: 2
flags: 0x0
Sep 20 23:05:14 vss-kbp-proto wait4confd_status.py[831]: PFOS check CDB done.
Sep 20 23:05:14 vss-kbp-proto chassis[843]: DEBUG:chassis:main:3410 /vss/vxos/bin/chassis
main - STARTED
Sep 20 23:05:14 vss-kbp-proto chassis[843]: Added group membership

. . .
```

```
PFS5031-56X-ZTP# show log system_monitor

-- Logs begin at Wed 2023-09-20 23:03:57 UTC, end at Thu 2023-10-05 21:08:48 UTC. --
Sep 20 23:05:05 vss-kbp-proto system_mon[632]: ALERT:system-mgmt:monitor_child:373 max
process 12
Sep 20 23:05:05 vss-kbp-proto system_mon[632]: ALERT:system-mgmt:monitor_child:435 Starting
System Monitoring...
Sep 20 23:05:15 vss-kbp-proto system_mon[632]: EMERGENCY:system-mgmt:s_sysmon_process_
tracelog:473 Log level changed from ERROR to WARNING
Sep 21 01:36:03 PFS5031-56X-ZTP system_mon[632]: ALERT:system-mgmt:s_sysmon_process_
request:698 process reset start msg for chassis_mgr:843 reset option 8
Sep 21 01:36:05 PFS5031-56X-ZTP system_mon[632]: ALERT:system-mgmt:s_sysmon_process_
timeout:1070 System reset option is 2
Sep 21 01:36:05 PFS5031-56X-ZTP system_mon[632]: Thu Sep 21 01:36:05 UTC 2023 handle_reboot_
options.
sh:input clear_config_mgmt_1
Sep 21 01:36:05 PFS5031-56X-ZTP system_mon[632]: Thu Sep 21 01:36:05 UTC 2023 handle_reboot_
options.
sh:remote mgmt available flag value is 1
. . .
```

show logging

Display message history.

Syntax

```
show logging [ log ]
```

Options

`log`	Restrict list to Syslog messages.

Mode

Operational

Examples

```
PFS5010# show logging | tab
ID  FACILITY  SEVERITY  TIMESTAMP                 MESSAGE


---------------------------------------------------------------------------------------------
-----...
7   system    notice    2020-05-13T20:56:23.593Z  SysAccCtl. Logged in
User:admin,IP:127.0.0.1,Conte
xt:cli,AccessType:CONSOLE
...
11  system    notice    2020-05-14T14:35:02.711Z  SysAccCtl. Logged in
User:admin,IP:10.252.69.42,Co
ntext:cli,AccessType:SSH
12  system    notice    2020-05-14T14:35:52.713Z  TrfCfgChg. Filter f1 is added: expression:
ip offs
et 10 10.1.2.3 mask 255.255.255.255 by admin
13  system    notice    2020-05-14T14:36:34.084Z  TrfCfgChg. Filter f1 is modified:
expression: ip o
ffset 10 10.1.2.3 mask 255.255.255.255 to ip offset 10 0a0b0c0d mask fffffff by admin
14  system    notice    2020-05-14T14:37:27.302Z  SysAccCtl. Logged out
User:admin,IP:10.252.69.42,C
ontext:cli,AccessType:SSH
15  system    alert     2020-05-18T22:45:20.520Z  SysPort. ports 1-28 is offline (link down)
16  system    warning   2020-05-18T22:48:51.211Z  SysPort. ports 1-28 is now online (link up)
17  system    alert     2020-05-18T23:53:58.037Z  SysPort. ports 1-28 is offline (link down)
18  system    warning   2020-05-18T23:55:44.443Z  SysPort. ports 1-28 is now online (link up)
```

show mac-address

Display chassis MAC address.

Syntax

```
show mac-address
```

Options

None. The MAC address cannot be changed.

Mode

Operational

Examples

```
PFOS# show mac-address
mac address c4:ee:ae:01:c2:a9
```

show management_module

Display information about installed management module(s).

Syntax

```
show management_module [ module-num ] [ component ]
```

Options

`module-num`	Restrict display to information about the specified management module. Valid values are `1`and `2`.
`component`	Restrict display to information about the specified components. Valid values are: `PCBA_part_number`: PCBA part number `PCBA_revision`: Blade PCBA revision `PCBA_serial_number`: PCBA serial number `Product_ID`: Product identity `fan1_speed`: Fan 1 speed (RPM) `fan2_speed`: Fan 2 speed (RPM) `fan3_speed`: Fan 3 speed (RPM) `model`: Card model `module_part_number`: Part number `module_revision_number`: Revision number `module_serial_number`: Blade serial number `sku_part_number`: SKU part number `state`: Slot state `temperature`: Module temperature

Mode

Operational

Examples

```
PFOS#  show management_module
management_module 1
 state                  OK
 Product ID             1350
 model                  "vCPU 300"
 module part number     VP_01940
 module revision number 04
 module serial number   14070603
 PCBA part number       VA_00692
 PCBA revision          09
 PCBA serial number     VSSAL-14070603
 sku part number        VA_00692
 temperature            31
 fan1 speed             13239
 fan2 speed             13173
 fan3 speed             13374
management_module 2
 state empty

PFOS# show management_module 1 fan1_speed
fan1 speed 13261
```

show map

List one or more traffic maps. If no options are specified, then list all traffic maps.

Syntax

```
show map [ map-name |
   filter filter-name |
   input_ports port-id |
   lb_criteria lb-criterion-name |
   output_lb_groups lbg-name |
   output_ports port-id |
   map_status |
   remote-monitor-group-status |
   pstack-paths ]
```

Options

`map-name`	Name of a map. Type `?` for a list of currently defined maps.
`filter filter-name`	Display only the maps that use filter `filter-name`.
`input_ports port-id`	Display only the maps that have port `port-id` as an input port.
`lb_criteria lb-criterion-name`	Display only the maps that use load balancing criterion `lb-criterion-name`.
`output_lb_groups lbg-name`	Display only the maps that output to load balancing group `lbg-name`.
`output_ports port-id`	Display only the maps that have port `port-id` as an output port.
`output-pstack-ports port-id`	Display only the maps that have port port-id as an output pStack port.
`map_status`	Display only map status, including error code and monitor group ID. Possible values for error code are: CardNotPresent ErrorUnknown HWError Init InvalidFilterEntry MaxCascadeEntriesLimitReached MaxFilterLimitReached MaxFilterQualifierLimitReached MaxFilterRangeLimitReached MaxQualLenReached MaxUserDefinedFilterLimitReached SomePortMayBeDown None (default)

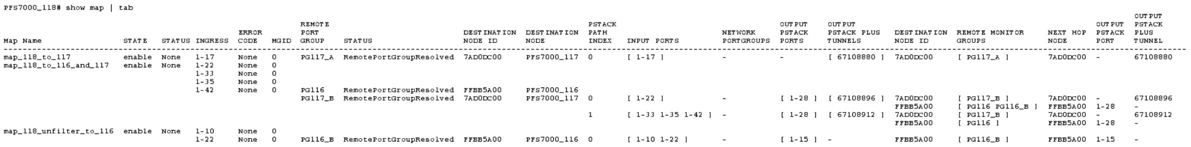
`remote-monitor-group-status`	Display only remote monitor group status for the maps. This shows the status of each remote monitor group present in the map. Possible values for status are: • `RemotePortGroupNotFound` – Unable to find given port group on any node in pfsMesh. • `RemotePortGroupNameConflicts`– Port group with same name exists on more than one node in pfsMesh. • `RemotePortGroupResolved` – Port group was found on one destination node, and map was routed to destination. • `HWErrorOnTransitOrDestination` – Destination node can be reached, but not enough hardware resources for this map on all the hops.
`pstack-paths`	**Note: The pStack+ feature requires the PFS 7000 functionality license.** Display output pStack ports and output pStack plus tunnels for given list of input ports and the pstack path status. This option also displays output detail for remote monitor groups per destination node, including output pstack ports and output pStack plus tunnels and next hop node per destination node. Possible status values are: • `None` – Default staus. There is no issue on map. • `Init` – pStack path update is in-progress. • `HWError` - pStack path was not programmed in HW due to some HW error.

Mode

Operational

Examples

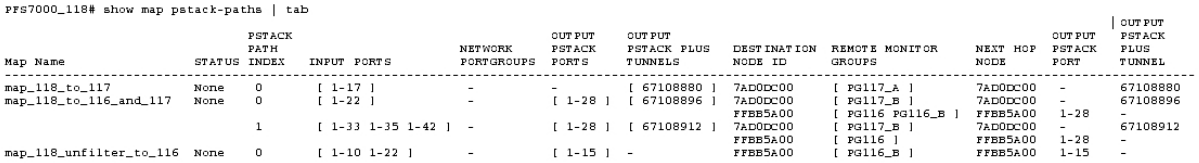
Note: The pStack+ feature requires the PFS 7000 functionality license.



```
PFS7000_118# show map | tab

                                                                                                                                                                                                                                                      OUTPUT
                                                                REMOTE                                                          PSTACK                                   OUTPUT    OUTPUT                                                     OUTPUT  PSTACK
                                                   ERROR        PORT                                 DESTINATION  DESTINATION   PATH                         NETWORK     PSTACK    PSTACK PLUS    DESTINATION  REMOTE MONITOR      NEXT HOP   PSTACK  PLUS
Map Name                   STATE   STATUS INGRESS  CODE   MGID  GROUP     STATUS                     NODE ID      NODE          INDEX   INPUT PORTS          PORTGROUPS  PORTS     TUNNELS        NODE ID      GROUPS              NODE       PORT    TUNNEL
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
map_118_to_117             enable  None   1-17     None   0     PG117_A   RemotePortGroupResolved    7AD0DC00     PFS7000_117   0       [ 1-17 ]             -           -         [ 67108880 ]   7AD0DC00     [ PG117_A ]         7AD0DC00   -       67108880
map_118_to_116_and_117     enable  None   1-22     None   0
                                          1-33     None   0
                                          1-35     None   0
                                          1-42     None   0     PG116     RemotePortGroupResolved    FFBB5A00     PFS7000_116
                                                                PG117_B   RemotePortGroupResolved    7AD0DC00     PFS7000_117   0       [ 1-22 ]             -           [ 1-28 ]  [ 67108896 ]   7AD0DC00     [ PG117_B ]         7AD0DC00   -       67108896
                                                                                                                                                                                                  FFBB5A00     [ PG116 PG116_B ]   FFBB5A00   1-28    -
                                                                                                                                1       [ 1-33 1-35 1-42 ]   -           [ 1-28 ]  [ 67108912 ]   7AD0DC00     [ PG117_B ]         7AD0DC00   -       67108912
                                                                                                                                                                                                  FFBB5A00     [ PG116 ]           FFBB5A00   1-28    -
map_118_unfilter_to_116    enable  None   1-10     None   0
                                          1-22     None   0     PG116_B   RemotePortGroupResolved    FFBB5A00     PFS7000_116   0       [ 1-10 1-22 ]        -           [ 1-15 ]  -              FFBB5A00     [ PG116_B ]         FFBB5A00   1-15    -
```

```
PFOS# show map map_status
Map                     ERROR
Name   STATE    INGRESS   CODE    MGID
-----------------------------------
map1   enable   1-1       None    0
map2   enable   1-1       None    0
                1-2       None    0
                1-3       None    0
                1-4       None    0
map3   enable   1-1       None    0
                1-2       None    0
                1-3       None    0


PFOS# Show map remote-monitor-group-status
      REMOTE
```

```
Map    PORT                                      DESTINATION  DESTINATION
Name   GROUP      STATUS                         NODE ID      NODE
-------------------------------------------------------------------
map1   MPG119_A   RemotePortGroupResolved  FFBA7C00     PFS5010
       PG116      RemotePortGroupResolved  FFBB5A00     PFS5010_116
       PG118_A    RemotePortGroupResolved  9703D400     PFS5010_118
       PG6010     RemotePortGroupResolved  C6BB00       PFS6010-233
map2   MPG119_A   RemotePortGroupResolved  FFBA7C00     PFS5010
       PG116      RemotePortGroupResolved  FFBB5A00     PFS5010_116
       PG6010     RemotePortGroupResolved  C6BB00       PFS6010-233
map3   PG116      RemotePortGroupResolved  FFBB5A00     PFS5010_116
       PG118_B    RemotePortGroupResolved  9703D400     PFS5010_118
       PG6010     RemotePortGroupResolved  C6BB00       PFS6010-233
```



```
PFS7000_118# show map pstack-paths | tab
                                                                                                                                   | OUTPUT
                                PSTACK                                      OUTPUT   OUTPUT                                                   OUTPUT  PSTACK
                                PATH                        NETWORK         PSTACK   PSTACK PLUS    DESTINATION  REMOTE MONITOR        NEXT HOP  PSTACK  PLUS
Map Name                 STATUS INDEX   INPUT PORTS         PORTGROUPS      PORTS    TUNNELS        NODE ID      GROUPS                NODE      PORT    TUNNEL
------------------------------------------------------------------------------------------------------------------------------------------------------------------
map_118_to_117           None   0       [ 1-17 ]            -               -        [ 67108880 ]   7AD0DC00     [ PG117_A ]           7AD0DC00  -       67108880
map_118_to_116_and_117   None   0       [ 1-22 ]            -               [ 1-28 ] [ 67108896 ]   7AD0DC00     [ PG117_B ]           7AD0DC00  -       67108896
                                                                                                    FFBB5A00     [ PG116 PG116_B ]     FFBB5A00  1-28    -
                                1       [ 1-33 1-35 1-42 ]  -               [ 1-28 ] [ 67108912 ]   7AD0DC00     [ PG117_B ]           7AD0DC00  -       67108912
                                                                                                    FFBB5A00     [ PG116 ]             FFBB5A00  1-28    -
map_118_unfilter_to_116  None   0       [ 1-10 1-22 ]       -               [ 1-15 ] -              FFBB5A00     [ PG116_B ]           FFBB5A00  1-15    -
```

show memory

Display information on memory capacity and usage.

Syntax

```
show memory [ mgmt-card ]
```

Options

mgmt-card	Management module on which to perform this command. Valid values are mgmt-1 and mgmt-2. If no mgmt-card is specified, then perform this command on the currently active management module. Option is valid only on PFS 6010 with two management modules installed.

Mode

Operational, Configuration

Examples

```
PFOS# show memory

MemTotal:         8064612 kB
MemFree:          6474440 kB
Buffers:           131792 kB
Cached:            707384 kB
SwapCached:             0 kB
Active:           1286012 kB
Inactive:          183752 kB
Active(anon):      662592 kB
Inactive(anon):       200 kB
Active(file):      623420 kB
Inactive(file):    183552 kB
...
```

show mgmt

Display information about management modules. If no options are specified, then `boottime` and `uptime` are displayed.

Syntax

```
show mgmt [ mgmt-card ] [ boottime | certificate | config | cores |
    firmware | home | license | log | software | sshpubkey | uptime ]
```

Options

`mgmt-card`	Management module on which to perform this command. Valid values are `mgmt-1` and `mgmt-2`. If no `mgmt-card` is specified, then perform this command on all currently installed management modules. Option is valid only on PFS 6010 with two management modules installed.
`boottime`	Display management module boot time.
`certificate`	List saved certificates and private keys.
`config`	List saved configuration files.
`cores`	List saved core dump files.
`firmware`	List uploaded firmware files.
`home`	List files saved in user home directory.
`license`	List saved license files. To list individual details, use the following modifiers: • `description` - License description • `expiration-date` - License expiration date • `mac-address` - MAC address used to generate license • `state` - License state • `type` - License type
`log`	List saved log files.
`software`	List uploaded software image files.
`sshpubkey`	List saved SSH public key files.
`uptime`	Display management module uptime.

Mode

Operational, Configuration

Examples

Show uptime and boot time for both management modules:

```
PFOS# show mgmt
mgmt mgmt-1
 uptime   "0 days, 13 hours, 37 mins and 31 seconds"
 boottime 2017-12-07T03:06:35.813234+00:00
```

```
mgmt mgmt-2
 uptime   "0 days, 13 hours, 37 mins and 32 seconds"
 boottime 2017-12-07T03:03:58.113277+00:00
```

List license files available on management module 1:

```
PFOS# show mgmt mgmt-1 license
license Support
 description     "Supports base features and upgrades"
 type            full
 state           current
 expiration date "Dec 2023"
 mac address     8c:ea:1b:34:d5:e9
```

List only license file expiration date:

```
PFS5010# show mgmt mgmt-1 license expiration-date
NAME      EXPIRATION DATE
---------------------------------------------------
Support   Dec 2023
```

List only license file type:

```
PFS5010# show mgmt mgmt-1 license type
NAME      TYPE
-----------------
Support   full
```

show module

Show information about the system chassis.

Syntax

```
show module_component
```

Options

`component`	Chassis component to display. Options are:
	`part_number`
	`revision`
	`serial_number`

Mode

Operational

Examples

```
PFOS# show module_part_number
module part number VP_01963
PFOS# show module_revision_number
module revision number AE
PFOS# show module_serial_number
module serial number 19999392
```

show netconf-state

Show information about the NETCONF XML API.

Syntax

```
show netconf-state [ component ]
```

Options

`component`	Restrict the display to information about the specified component. Options are: `capabilities`: Capabilities supported by the NETCONF server `datastores`: Available datastores `files`: Files available on the NETCONF server. `schemas`: Data models supported by the NETCONF server. `sessions`: Currently active sessions `statistics`: Statistics related to the NETCONF server `streams`: Currently active streams

Mode

Operational

Examples

```
PFOS# show netconf-state sessions
netconf-state sessions session 139
 transport   cli-ssh
 username    admin
 source host 10.200.201.26
 login time  2017-02-21T18:40:28+00:00


PFOS# show netconf-state streams
netconf-state streams stream NETCONF
 description              "NETCONF notifications"
 replay support           true
 replay log creation time 2017-02-18T03:59:26+00:00
 replay log aged time     2017-02-20T10:35:18.588636+00:00
netconf-state streams stream chassis
 description              "Chassis notifications"
 replay support           true
 replay log creation time 2017-02-18T03:59:26+00:00
netconf-state streams stream user
 description              "User notifications"
 replay support           true
 replay log creation time 2017-02-18T03:59:26+00:00
```

```
PFOS# show netconf-state datastores
netconf-state datastores datastore running
 transaction id 978-307280-776217
netconf-state datastores datastore startup
```

show ntp

This section describes the following commands:

- show ntp
- show ntp-key

show ntp

Display NTP status information.

Syntax

```
show ntp [ deviation ] [ status ] [authentication]
```

Options

Note: The following values correspond to the NTP server that the ntpd daemon selects for time synchronization (among the configured NTP servers). PFOS does not decide which NTP server is used to for time synchronization.

`deviation`	Display the amount of time the system clock deviates from the NTP source at the last update.
`status`	• **server-not-reachable**: No NTP server is reachable. • **syncing**: The system time is synchronized to one of the NTP servers. • **running**: NTP is running but has not started to synchronize to any NTP server. • **not-running**: No NTP server is configured.
`authentication`	• **ok**: Authentication is successful. The "ok" status only displays while the status is "syncing." • **bad**: Authentication failed. • **None**: No authentication is configured for this NTP server.

Mode

Operational

Examples

```
PFOS# show ntp
ntp status running
ntp deviation 8.678(ms)
ntp authentication ok
```

show ntp-key

Display information about the NTP key file.

Syntax

```
show ntp-key
```

Options

None

Mode

Operational

Examples

```
PFS# show ntp-key
NAME         SIZE  TIME
---------------------------------------------------
ntp.key.txt    140     May 27 2020 01:20:17
```

show PCBA

Show information about the system's printed circuit board assembly.

Syntax

```
show PCBA_component
```

Options

`component`	Specify PCBA component to display. Options are:
	`part_number`
	`revision`
	`serial_number`

Mode

Operational

Examples

```
PFOS# show PCBA_part_number
PCBA part number VA_00644
PFOS# show PCBA_revision
PCBA revision AC
PFOS# show PCBA_serial_number
PCBA serial number VSSAL-19999392
```

show pfsmesh

Note: The pStack+ feature requires the PFS 7000 functionality license.

Show information about pfsMesh connections via the pStack and pStack+ protocols.

Syntax

```
show pfsmesh [ node node-id [ ip-address | name | node-label | partner-
node | platform | pstack-version | topology-label | type ] ]
```

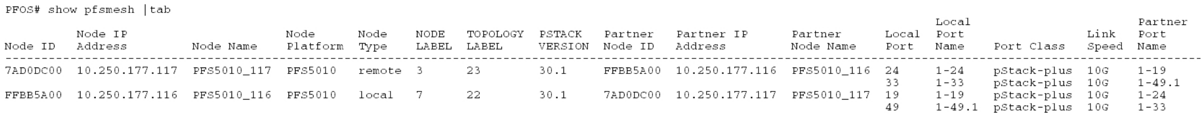
Options

`node`	Display only information about pfsMesh node `node-id`, or for all pfsMesh nodes if no `node-id` is specified.
`ip-address`	Display only the IP address of the pfsMesh node.
`name`	Display only the name of the pfsMesh node.
`node-label`	Count of number of times node details (such as, name, ip address) have changed.
`partner-node`	Display only the information about the partner nodes of this pfsMesh node.
`platform`	Display only the platform type of the pfsMesh node.
`pstack-version`	Display only the pStack/pStack+ protocol version of the pfsMesh node.
`topology-label`	Count of number of times topology (that is, partner node list) of this node has changed.
`type`	Display the type of pfsMesh node, either `remote` or `local`.

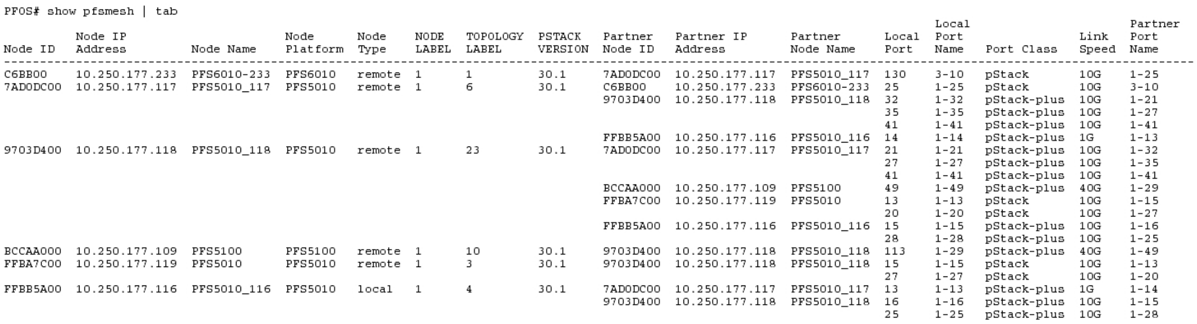
Mode

Operational

Examples



```
PFOS# show pfsmesh |tab

                                                                                                                                 Local                  Partner
          Node IP                      Node      Node    NODE   TOPOLOGY  PSTACK   Partner   Partner IP      Partner      Local  Port                 Link   Port
Node ID   Address         Node Name    Platform  Type    LABEL  LABEL     VERSION  Node ID   Address         Node Name    Port   Name    Port Class   Speed  Name
--------------------------------------------------------------------------------------------------------------------------------------------------------------------
7AD0DC00  10.250.177.117  PFS5010_117  PFS5010   remote  3      23        30.1     FFBB5A00  10.250.177.116  PFS5010_116  24     1-24    pStack-plus  10G    1-19
                                                                                                                          33     1-33    pStack-plus  10G    1-49.1
FFBB5A00  10.250.177.116  PFS5010_116  PFS5010   local   7      22        30.1     7AD0DC00  10.250.177.117  PFS5010_117  19     1-19    pStack-plus  10G    1-24
                                                                                                                          49     1-49.1  pStack-plus  10G    1-33
```



```
PFOS# show pfsmesh | tab
                                                                                                                                 Local                      Partner
          Node IP                                Node      Node    NODE   TOPOLOGY  PSTACK   Partner   Partner IP      Partner      Local  Port                 Link   Port
Node ID   Address         Node Name    Platform  Type    LABEL  LABEL     VERSION  Node ID   Address         Node Name    Port   Name   Port Class    Speed  Name
----------------------------------------------------------------------------------------------------------------------------------------------------------------------
C6BB00    10.250.177.233  PFS6010-233  PFS6010   remote  1      1         30.1     7AD0DC00  10.250.177.117  PFS5010_117  130    3-10   pStack        10G    1-25
7AD0DC00  10.250.177.117  PFS5010_117  PFS5010   remote  1      6         30.1     C6BB00    10.250.177.233  PFS6010-233  25     1-25   pStack        10G    3-10
                                                                                   9703D400  10.250.177.118  PFS5010_118  32     1-32   pStack-plus   10G    1-21
                                                                                                                          35     1-35   pStack-plus   10G    1-27
                                                                                                                          41     1-41   pStack-plus   10G    1-41
                                                                                   FFBB5A00  10.250.177.116  PFS5010_116  14     1-14   pStack-plus   1G     1-13
9703D400  10.250.177.118  PFS5010_118  PFS5010   remote  1      23        30.1     7AD0DC00  10.250.177.117  PFS5010_117  21     1-21   pStack-plus   10G    1-32
                                                                                                                          27     1-27   pStack-plus   10G    1-35
                                                                                                                          41     1-41   pStack-plus   10G    1-41
                                                                                   BCCAA000  10.250.177.109  PFS5100      49     1-49   pStack-plus   40G    1-29
                                                                                   FFBA7C00  10.250.177.119  PFS5010      13     1-13   pStack        10G    1-15
                                                                                                                          20     1-20   pStack        10G    1-27
                                                                                   FFBB5A00  10.250.177.116  PFS5010_116  15     1-15   pStack-plus   10G    1-16
                                                                                                                          28     1-28   pStack-plus   10G    1-25
BCCAA000  10.250.177.109  PFS5100      PFS5100   remote  1      10        30.1     9703D400  10.250.177.118  PFS5010_118  113    1-29   pStack-plus   40G    1-49
FFBA7C00  10.250.177.119  PFS5010      PFS5010   remote  1      3         30.1     9703D400  10.250.177.118  PFS5010_118  15     1-15   pStack        10G    1-13
                                                                                                                          27     1-27   pStack        10G    1-20
FFBB5A00  10.250.177.116  PFS5010_116  PFS5010   local   1      4         30.1     7AD0DC00  10.250.177.117  PFS5010_117  13     1-13   pStack-plus   1G     1-14
                                                                                   9703D400  10.250.177.118  PFS5010_118  16     1-16   pStack-plus   10G    1-15
                                                                                                                          25     1-25   pStack-plus   10G    1-28
```

```
PFOS# show pfsMesh node ?
Description: Stacking node details
Possible completions:
  7AD0DC00   Node ID
  FFBB5A00   Node ID
  |          Output modifiers
  <cr>
Possible match completions:
  ip-address       Node IP address
  name             User defined node name
  node-label       Count of number of times node details (e.g.
  partner-node     Partner node details
  platform         Node platform type
  pstack-version   pStack protocol version
  topology-label   Count of number of times topology (i.e.
  type             Local or remote node type
PFS5010_116# show pfsMesh node 7AD0DC00
pfsMesh node 7AD0DC00
 ip address     10.250.177.117
 name           PFS5010_117
 platform       PFS5010
 type           remote
 node label     3
 topology label 23
 pstack version 30.1
 partner-node FFBB5A00
  ip address 10.250.177.116
  name       PFS5010_116
  ports 24
   name         1-24
   class        pStack-plus
   speed        10G
   partner port 1-19
  ports 33
   name         1-33
   class        pStack-plus
   speed        10G
   partner port 1-49.1
```

show port-group

Show port groups defined on this system and any remote traffic maps that are using these groups.

Syntax

```
show port-group [
    monitor [ group-name | nodes-with-conflict |
        pstack-ref-map | ref-map | ref-toolgroup | status ] |
    network [ group-name | Error_code [ error-code ] |
        ref_map [ map-name ] |
    inline-monitor [ group-name ] |
    inline-network [ group-name ] ]
```

Options

`group-name`	Name of a port group. Type `?` for a list of currently defined port groups. If specified, then only that port group is shown. If no `group-name` is specified, then all defined port groups are shown.
`monitor`	Limit the display to monitor port groups. If `nodes-with-conflict`, `pstack-ref-map`, `ref-map`, `ref-toolgroup`, or `status` is also specified, then display only that column.
`network`	Limit the display to network port groups. If `Error_code` or `ref_map` is also specified, then display only that column.
`inline-monitor`	Limit the display to inline monitor port groups.
`inline-network`	Limit the display to inline network port groups.

Mode

Operational

Examples

```
PFOS# show port-group monitor
                                                  CONFLICTING  CONFLICTING  MAP
NAME                       STATUS                 NODE ID      NODE NAME    NAME  pStack MAP           NAME
------------------------------------------------------------------------------------------------------------
-
PFS5010-RPG_1@137_SanJose  PortGroupNameResolved
PFS5010-RPG_2@137_SanJose  PortGroupNameResolved
PG_A                       PortGroupNameResolved                                  26760900~mapA~1728
```

show port_timestamp

Show the time source for the system chassis.

Syntax

```
show port_timestamp
```

Options

None

Mode

Operational

Examples

```
PFOS# show port_timestamp
port_timestamp time source NTP
```

show power-consumption

Displays the PFS 5000/7000 current power consumption (in Watts) of each PSU in the device.

Syntax

```
show power-consumption
```

Options

None

Mode

Operational

Example

```
PFOS# show power-consumption
power consumption 140.0
```

show power_supply

Display status of the power supplies.

Syntax

```
show power_supply [ [ number ] state ]
```

Options

`number`	Number of power supply.
`state`	Has no effect.

Mode

Operational

Examples

```
 PFOS# show power_supply
                                                        Power
                                               Voltage  Consumption
ID  STATE  MODEL          TYPE  FAN DIRECTION  In (V)   (W)
---------------------------------------------------------------------
1   OK     CPR-4011-4M11  AC    Front-to-Back  202.0    66.0
2   OK     CPR-4011-4M11  AC    Front-to-Back  202.0    55.0
```

When one of the PSU is failed or removed:

```
PFOS# show power_supply
                                                         Power
                                                Voltage  Consumption
ID  STATE   MODEL          TYPE  FAN DIRECTION  In (V)   (W)
----------------------------------------------------------------------
1   OK      CPR-4011-4M11  AC    Front-to-Back  202.0    115.0
2   failed  N/A            N/A   Front-to-Back  0.0      0.0
```

```
PFOS# show power_supply
                                                        Power
                                               Voltage  Consumption
ID  STATE  MODEL          TYPE  FAN DIRECTION  In (V)   (W)
---------------------------------------------------------------------
1   OK     CPR-4011-4M11  AC    Front-to-Back  202.5    115.0
2   empty  -              -     -              -        -
```

show powersafe

Display status of the powersafe modules and segments.

Syntax

```
show powersafe
```

Options

None

Mode

Operational

Examples

```
PFOS# show powersafe
                                     FIBER
                                     PAIR    OPERATIONAL
MODULE SEGMENT MODULE TYPE           STATE   STATE
------------------------------------------------------------

1      1       LC-SingleMode        closed  normal
1      2       LC-SingleMode        closed  manual-block
2      1       LC-SingleMode-50     closed  manual-forward
2      2       LC-SingleMode-50     closed  manual-inpairdown
3      1       MPO-MultiMode        opened  manual-bypass
3      2       RJ45-10G/1G-Copper   closed  normal
4      1       RJ45-10G/1G-Copper   closed  normal
```

show powersafe-module

Display powersafe hardware information.

Syntax

```
show powersafe-module
```

Options

None

Mode

Operational

Examples

```
PFOS# show powersafe-module
powersafe-module state online
powersafe-module product id 3296
powersafe-module vendor id 14A6
powersafe-module serial number "1F3OB145180003    "
powersafe-module firmware revision 4
MODULE
ID      MODULE TYPE         SEGMENTS
--------------------------------------
1       LC-SingleMode       2
2       LC-MultiMode-50     2
3       MPO-MultiMode       1
4       RJ45-10G/1G-Copper  2
```

show process

Display status of current running processes.

Syntax

```
show process [ mgmt-card ]
```

Options

mgmt-card	Management module on which to perform this command. Valid values are mgmt-1 and mgmt-2. If no mgmt-card is specified, then perform this command on the currently active management module. Option is valid only on PFS 6010 with two management modules installed.

Mode

Operational, Configuration

Examples

```
PFOS# show process
vss.access_control.service loaded active   running   VSS Access Control
vss.acce...agement.service loaded active   running   VSS Access Management
vss.appinfra.service       loaded active   running   VSS App Infra
vss.applibs.service        loaded active   running   VSS Application Libraries
vss.arbitrator.service     loaded active   running   VSS Arbitration
vss.chassis.service        loaded active   running   VSS Chassis Manager
vss.confd.service          loaded active   running   VSS Data Model
vss.flowmapper.service     loaded active   running   VSS Flow Mapper
vss.ha_mgr.service         loaded active   running   VSS High Availability Manager
vss.hal.service            loaded active   running   VSS HAL Server
vss.lcd.service            loaded active   running   VSS LCD Controller
vss.loadbalancer.service   loaded active   running   VSS Load Balancer
vss.port...gurator.service loaded active   running   VSS Portconfigurator
vss.pstack.service         loaded active   running   VSS pStack Application
vss.replicator.service     loaded inactive dead      VSS Replicator
vss.settings.service       loaded active   running   VSS Settings
vss.snmpmibs.service       loaded active   running   VSS MIB implementation
vss.snmptransform.service  loaded active   running   VSS SNMP config transform
vss.startup.service        loaded inactive dead      VSS Initialization
vss.statcollector.service  loaded active   running   VSS Stats Collector
vss.switchmgr.service      loaded active   running   VSS Switch Manager
vss.sysmon.service         loaded active   running   VSS System Monitor
vss.system_notif.service   loaded active   running   VSS System Notification
```

show pstack

Note: The pStack+ feature requires the PFS 7000 functionality license.

Show traffic maps that have been created on this node by the pStack/pStack+ protocol. The node can be transit, destination, or both for the pStack map. See also `show pstack interfaces`.

Refer to the "pStack Map" section in the *PFOS 6.x User Guide*, for details about understanding pStack map input and outputs.

Syntax

```
show pstack map [ map-name [ output-field ] ]
```

Options

`map-name`	Display only the information about map `map-name`, or for all maps if no `map-name` is specified. • pStack map names are shown in the format: `head-node~name~vlan-id` where `head-node` is the node where the map was created, `name` is the user-specified map name, and `vlan-id` is the input port VLAN ID. • pStack+ map names are shown in the format: `head-node~name~tunnel key` where `head-node` is the node where the map was created, `name` is the user-specified map name, and `tunnel key` is the input tunnel key.
`output-field`	Display only the specified information about traffic maps. Some fields are only applicable to either pStack or pStack plus. **Applicable to both pStack and pStack plus** • `output-monitor-groups`: Local output monitor port groups. • `priority`: Priority of this map. • `status`: Overall pStack map status. **Applicable to only pStack** • `filter-expression`: Filter expression provided by pStack. • `input-pstack-ports`: List of local pStack ports used as input. • `output-pstack-ports`: List of local pStack ports used as output. **Applicable to only pStack plus** • `input-pstack-plus-tunnel`: Local pStack plus tunnel used as input. • `output-pstack plus-tunnels`: List of local pStack plus tunnels used as output to reach remote destination.

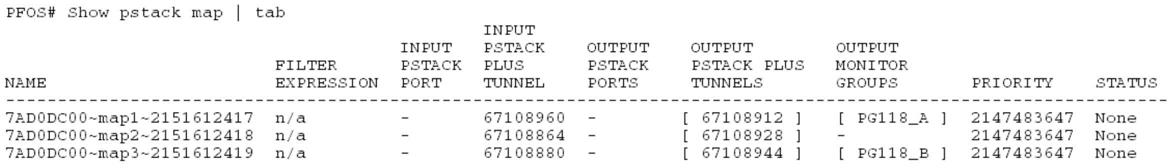
Mode

Operational

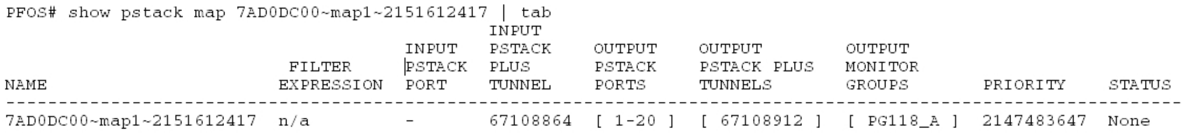
Examples

pStack+ Examples

```
PFOS# show pstack map ?
Description: Maps updated by pStack application
Possible completions:
  7AD0DC00~map1~2151612417   Remote map name appended with node ID
  7AD0DC00~map2~2151612418   Remote map name appended with node ID
  7AD0DC00~map3~2151612419   Remote map name appended with node ID
  |                          Output modifiers
  <cr>
Possible match completions:
  filter-expression            Filter expression provided by pStack APP
  input-pstack-plus-tunnel     Local pStack plus tunnel used as input
  input-pstack-port            Local pStack port used as input
  output-monitor-groups        Local output monitor port groups
  output-pstack-plus-tunnels   List of local pStack plus tunnels used as output to reach
remote destination
  output-pstack-ports          List of local pStack ports used as output
  priority                     Priority of this map
  status                       Overall pStack map status
PFOS# show pstack map 7AD0DC00~map1~2151612417
pstack map 7AD0DC00~map1~2151612417
 filter expression           n/a
 input pstack plus tunnel    67108864
 output pstack ports         [ 1-20 ]
 output pstack plus tunnels  [ 67108912 ]
 output monitor groups       [ PG118_A ]
 priority                    2147483647
 status                      None
```



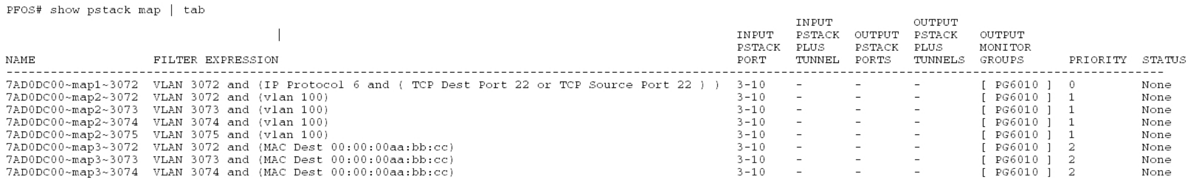
```
PFOS# Show pstack map | tab
                                              INPUT
                                     INPUT    PSTACK    OUTPUT    OUTPUT         OUTPUT
                          FILTER     PSTACK   PLUS      PSTACK    PSTACK PLUS    MONITOR
NAME                      EXPRESSION PORT     TUNNEL    PORTS     TUNNELS        GROUPS        PRIORITY    STATUS
---------------------------------------------------------------------------------------------------------------------
7AD0DC00~map1~2151612417  n/a        -        67108960  -        [ 67108912 ]   [ PG118_A ]   2147483647  None
7AD0DC00~map2~2151612418  n/a        -        67108864  -        [ 67108928 ]   -             2147483647  None
7AD0DC00~map3~2151612419  n/a        -        67108880  -        [ 67108944 ]   [ PG118_B ]   2147483647  None
```



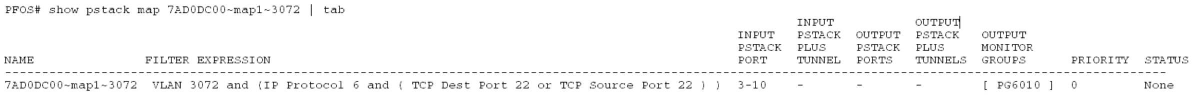
```
PFOS# show pstack map 7AD0DC00~map1~2151612417 | tab
                                              INPUT
                                     INPUT    PSTACK    OUTPUT    OUTPUT         OUTPUT
                           FILTER    |PSTACK  PLUS      PSTACK    PSTACK PLUS    MONITOR
NAME                      EXPRESSION PORT     TUNNEL    PORTS     TUNNELS        GROUPS        PRIORITY    STATUS
----------------------------------------------------------------------------------------------------------------------
7AD0DC00~map1~2151612417  n/a        -        67108864  [ 1-20 ]  [ 67108912 ]   [ PG118_A ]   2147483647  None
```

pStack Examples

```
PFOS# show pstack map ?
Description: Maps updated by pStack application
Possible completions:
  7AD0DC00~map1~3072   Remote map name appended with node ID
  7AD0DC00~map2~3072   Remote map name appended with node ID
  7AD0DC00~map2~3073   Remote map name appended with node ID
  7AD0DC00~map2~3074   Remote map name appended with node ID
  7AD0DC00~map2~3075   Remote map name appended with node ID
  7AD0DC00~map3~3072   Remote map name appended with node ID
  7AD0DC00~map3~3073   Remote map name appended with node ID
  7AD0DC00~map3~3074   Remote map name appended with node ID
  |                    Output modifiers
  <cr>
Possible match completions:
  filter-expression            Filter expression provided by pStack APP
  input-pstack-plus-tunnel     Local pStack plus tunnel used as input
  input-pstack-port            Local pStack port used as input
  output-monitor-groups        Local output monitor port groups
  output-pstack-plus-tunnels   List of local pStack plus tunnels used as output to reach
remote destination
  output-pstack-ports          List of local pStack ports used as output
  priority                     Priority of this map
  status                       Overall pStack map status
```



```
PFOS# show pstack map | tab
                                                                                                            INPUT           OUTPUT
                                     |                                                              INPUT   PSTACK  OUTPUT  PSTACK   OUTPUT
                                                                                                    PSTACK  PLUS    PSTACK  PLUS     MONITOR
NAME                FILTER EXPRESSION                                                               PORT    TUNNEL  PORTS   TUNNELS  GROUPS      PRIORITY  STATUS
--------------------------------------------------------------------------------------------------------------------------------------------------------------
7AD0DC00~map1~3072  VLAN 3072 and (IP Protocol 6 and ( TCP Dest Port 22 or TCP Source Port 22 ) )  3-10    -       -       -        [ PG6010 ]  0         None
7AD0DC00~map2~3072  VLAN 3072 and (vlan 100)                                                        3-10    -       -       -        [ PG6010 ]  1         None
7AD0DC00~map2~3073  VLAN 3073 and (vlan 100)                                                        3-10    -       -       -        [ PG6010 ]  1         None
7AD0DC00~map2~3074  VLAN 3074 and (vlan 100)                                                        3-10    -       -       -        [ PG6010 ]  1         None
7AD0DC00~map2~3075  VLAN 3075 and (vlan 100)                                                        3-10    -       -       -        [ PG6010 ]  1         None
7AD0DC00~map3~3072  VLAN 3072 and (MAC Dest 00:00:00aa:bb:cc)                                       3-10    -       -       -        [ PG6010 ]  2         None
7AD0DC00~map3~3073  VLAN 3073 and (MAC Dest 00:00:00aa:bb:cc)                                       3-10    -       -       -        [ PG6010 ]  2         None
7AD0DC00~map3~3074  VLAN 3074 and (MAC Dest 00:00:00aa:bb:cc)                                       3-10    -       -       -        [ PG6010 ]  2         None
```



```
PFOS# show pstack map 7AD0DC00~map1~3072 | tab
                                                                                                            INPUT           OUTPUT
                                                                                                    INPUT   PSTACK  OUTPUT  PSTACK   OUTPUT
                                                                                                    PSTACK  PLUS    PSTACK  PLUS     MONITOR
NAME                FILTER EXPRESSION                                                               PORT    TUNNEL  PORTS   TUNNELS  GROUPS      PRIORITY  STATUS
--------------------------------------------------------------------------------------------------------------------------------------------------------------
7AD0DC00~map1~3072  VLAN 3072 and (IP Protocol 6 and ( TCP Dest Port 22 or TCP Source Port 22 ) )  3-10    -       -       -        [ PG6010 ]  0         None
```

show pstack-interfaces

Note: The pStack+ feature requires the PFS 7000 functionality license.

Show pStack-plus IP interfaces and tunnels that have been created on this node by the pStack+ protocol.

Syntax

```
show pstack-interfaces [ ip | pstack-plus-tunnel ]
```

Options

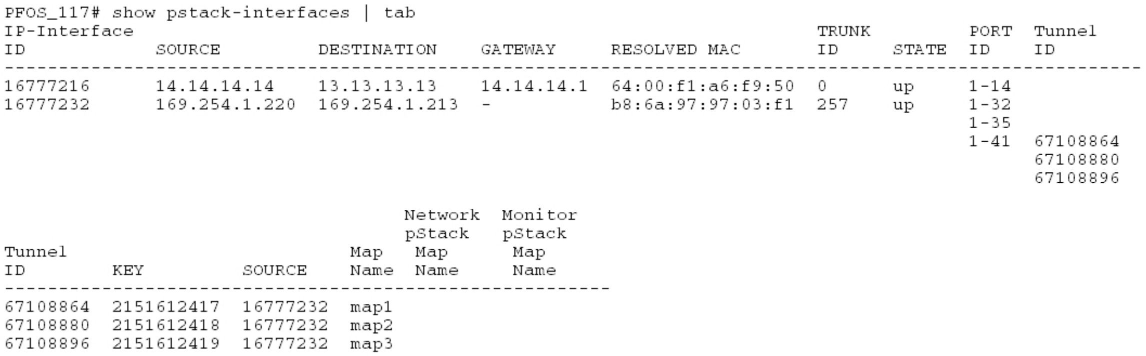
If no options are specified, PFOS displays all interfaces.

`ip`	Display only the information about pStack-plus IP interfaces created for this node.
`pstack-plus-tunnel`	Display only the information about pStack plus tunnels created for this node.

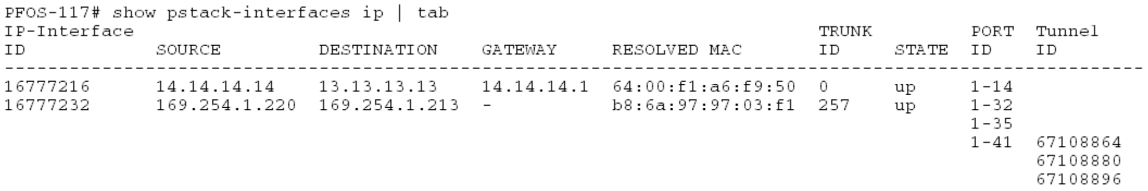
Mode

Operational

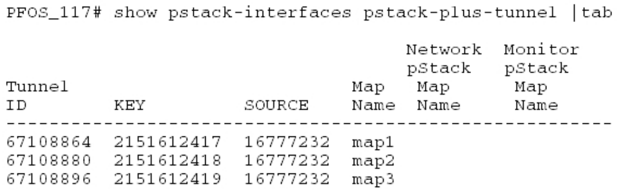
Examples



```
PFOS_117# show pstack-interfaces | tab
IP-Interface                                                               TRUNK         PORT  Tunnel
ID            SOURCE         DESTINATION    GATEWAY     RESOLVED MAC       ID     STATE  ID    ID
---------------------------------------------------------------------------------------------------------
16777216      14.14.14.14    13.13.13.13    14.14.14.1  64:00:f1:a6:f9:50  0      up     1-14
16777232      169.254.1.220  169.254.1.213  -           b8:6a:97:97:03:f1  257    up     1-32
                                                                                         1-35
                                                                                         1-41  67108864
                                                                                               67108880
                                                                                               67108896

                                     Network  Monitor
                                     pStack   pStack
Tunnel                          Map   Map      Map
ID        KEY         SOURCE    Name  Name     Name
--------------------------------------------------------
67108864  2151612417  16777232  map1
67108880  2151612418  16777232  map2
67108896  2151612419  16777232  map3
```



```
PFOS-117# show pstack-interfaces ip | tab
IP-Interface                                                               TRUNK         PORT  Tunnel
ID            SOURCE         DESTINATION    GATEWAY     RESOLVED MAC       ID     STATE  ID    ID
---------------------------------------------------------------------------------------------------------
16777216      14.14.14.14    13.13.13.13    14.14.14.1  64:00:f1:a6:f9:50  0      up     1-14
16777232      169.254.1.220  169.254.1.213  -           b8:6a:97:97:03:f1  257    up     1-32
                                                                                         1-35
                                                                                         1-41  67108864
                                                                                               67108880
                                                                                               67108896
```



```
PFOS_117# show pstack-interfaces pstack-plus-tunnel |tab

                                     Network  Monitor
                                     pStack   pStack
Tunnel                          Map   Map      Map
ID        KEY         SOURCE    Name  Name     Name
--------------------------------------------------------
67108864  2151612417  16777232  map1
67108880  2151612418  16777232  map2
67108896  2151612419  16777232  map3
```

show ptp

Display PTP information.

Syntax

```
show ptp [ status ]
```

Options

`status`	Has no effect.

Mode

Operational

Examples

```
PFOS# show ptp
ptp status "PTP cable disconnected"
```

show redundancy

Display the state and status of redundancy features.

Syntax

```
show redundancy [ state | status ]
```

Options

None

`state`	Display redundancy state. Possible displayed values are: `disabled`: Redundancy is disabled. No switchover can be performed. `sync`: Initial configuration database replication and any warm-boot related file synchronization. `ready`: Redundancy is ready. Switchover (either manual or auto) can occur.
`status`	Display redundancy status.

Mode

Operational

Examples

```
PFOS# show redundancy
redundancy state ready
redundancy status No issue.
PFOS# show redundancy status
redundancy status No issue.
```

show remote-monitor-group

Show remote monitor port groups defined on other systems connected via pfsMesh to this system. These port groups can be used as output for maps.

Syntax

```
show remote-monitor-group [ partner-node node-id ]
```

Options

None

`partner-node`	Display only information about remote monitor groups on partner node `node-id`, or for all pfsMesh nodes if no `node-id` is specified.

Mode

Operational

Examples

```
SW-137# show remote-monitor-group
          Partner
Partner   node
node ID   name     Port group name            Port group status
----------------------------------------------------------------------
26760900  SW-143   MPG1                       PortGroupNameResolved
34D2BB00  SW-156   PFS5010-RPG_1@156_SanJose  PortGroupNameResolved

SW-137# show remote-monitor-group partner-node ?
Description: Stacking partner node
Possible completions:
  34D2BB00   Partner node ID
  26760900   Partner node ID
  |          Output modifiers
  <cr>
Possible match completions:
  name         Partner node name
  port-group   List of remote monitor port groups
SW-137# show remote-monitor-group partner-node 34D2BB00
          Partner
Partner   node
node ID   name     Port group name            Port group status
----------------------------------------------------------------------
34D2BB00  SW-156   PFS5010-RPG_1@156_SanJose  PortGroupNameResolved
```

show remote-trigger

Display details about triggers configured as visible in pfsMesh; see `show trigger` for details about local triggers. See `trigger` for configuration details.

Syntax

```
show remote-trigger trigger [trigger name]
```

Options

`trigger name`	Specifying a trigger name displays only information about that specific trigger. If no name is specified, information for all remote triggers displays.

Mode

Operational

Examples

```
PFOS# show remote-trigger
                                Trigger pfsMesh       DESTINATION  DESTINATION
Trigger name            STATUS  status                NODE ID      NODE
---------------------------------------------------------------------------------
Node_119_Trigger_link1  active  TriggerNameResolved   FFB99E00     PFS-5010-119
Node_119_trigger2       active  TriggerNameResolved   FFB99E00     PFS-5010-119
Trigger1                active  TriggerNameConflicts  FFB99E00     PFS-5010-119


PFOS# show remote-trigger trigger Trigger1
Trigger           Trigger pfsMesh       DESTINATION  DESTINATION
name      STATUS  status                NODE ID      NODE
-------------------------------------------------------------------
Trigger1  active  TriggerNameConflicts  FFB99E00     PFS-5010-119
```

Field Descriptions

`trigger name`	Remote trigger name
`status`	Remote trigger status of as learned via pStack protocol. **Active**: indicates the condition defined in the trigger **has** occurred. **Inactive**: indicates the condition defined in the trigger has **not yet** occurred.
`pfsMesh status`	Trigger name resolution status as Resolved or Conflicts. Updated by pStack protocol.

`destination id`	Node ID and node name of the destination node to which this trigger is resolved. **Note:** If more than one remote trigger has same name, then the pStack protocol reports a name conflict and selects one of the Nodes as the Destination Node for the trigger. Users cannot select what the destination node is. To avoid this scenario, ensure the trigger name is unique so it does not conflict with other trigger policy names.
`destination name`	

show replace config-info

Use this command to query status of `replace config` command (if executed) prior to system reboot.

Syntax

```
show replace config-info
```

Options

None

Mode

Operational

Examples

```
PFS# show replace config-info
replace config-info status ok
replace config-info output "OK. Applied."

PFS# show replace config-info
replace config-info status failed
replace config-info output "Error: Failed to apply configuration. failed:
external error (19): /cha:chassis/line_cards{1}/ports{1-1}/class: Valid
PFS 7000 license required for this configuration."
```

show running-config

Display information about the current running configuration.

Syntax

```
show running-config [ category ]
```

Options

`category`	Restrict to specified type of information. Press ? for available options in each category. Available categories are: `access-policy password` – Password expiration threshold, password character requirements `app-lib` – Application libraries `authentication` – Authentication-related settings `feature` – View various feature settings (system-wide settings) `filter` – Table of filter expressions. See the *PFOS User Guide* for information and examples on creating filter expressions. `firewall`– firewall rules `gps` – GPS settings `hw-info` – Hardware information `interface` – Line cards `lb-criteria` – Load balancing criteria `ldap-server` – LDAP server settings `load-balance` – Load balancing groups `logging buffered` – Syslog message severity configured for buffer `logging host`– Syslog server settings `logging host severity-level`– Syslog message severity configured for Syslog server `map` – Packets forwarding maps `monitor_port_vlan` – Monitor port VLAN Tagging `notification` – Notification settings `ncm` – nGeniusONE Configuration Manager server `ntp` – NTP time servers `port_timestamp` – Port timestamping `powersafe` - External PowerSafe TAP `ptp` – PTP settings `radius-server` – External RADIUS servers `role` – Role management `session` –Global session parameters `snmp` – SNMP agent, community, target and user-related configuration `snmp-server` – SNMP server settings `system` – System settings and logs `system notes`– System notes `tacacs-server` – External TACACS servers `tracelog` – Trace log settings `username` – Local user management `webui` – Web UI specific configuration

Mode

Operational

Examples

```
PFOS# show running-config filter
filter jm_test
expression "IP Protocol 47"
```

The `extvlan` filter is used in PFS/PFX inner load balancing configurations. Refer to "PFS+PFX Inner Filtering and Inner Load Balancing" in the *PFOS User Guide* for details.

```
PFOS# show running-config filter extvlanfilter1
filter extvlanfilter1
type traffic
expression "extvlan 100"
!

PFOS# show running-config gps
gps cable_length 1

PFOS# show running-config authentication
authentication order local

PFOS# show running-config access-policy
access-policy password expiration 9999
access-policy password minimum length 5
access-policy password minimum uppercase 0
access-policy password minimum lowercase 0
access-policy password minimum numerical 0
access-policy password minimum special 0
access-policy password minimum positions-changed 1
access-policy login user-lockout-failed-attempts-max 5
access-policy login user-lockout-duration 60
access-policy login ip-lockout-failed-attempts-max 5

PFOS# show running-config interface 1 eth 1-21
interface 1
eth 1-21
  name               ""
  class              Span
  link_state         auto
  speed              40000
  timestamp rx
  timestamp rx-id 200
  timestamp tx
  timestamp tx-id 100
  vid default
  stripping vlan-tag count 2
  stripping vn-tag
  stripping mpls l2-mpls
  stripping mpls unstrippable-mpls-dest 1-31
  tunnel-termination disable
  port_breakout      disable

PFOS# show running-config load-balance lbg1
load-balance lbg1
 failover_action Rebalance
 type            Monitor
 tunnels         [ gre1 gre2 ]

PFOS# show running-config load-balance
load-balance rrg
 failover_action RoundRobin
 type            Monitor
 ports           [ 1-13 1-49.1 1-49.2 1-49.3 1-49.4 1-53.2 1-53.3 1-53.4
]
!

PFOS# show running-config interface 1 eth 1-21 stripping
interface 1
eth 1-21
stripping vlan-tag count 2
stripping vn-tag
stripping mpls l2-mpls
stripping mpls unstrippable-mpls-dest 1-31

PFOS#  show running-config app-lib standard-stripping vxlan
app-lib standard-stripping vxlan vtep-address [ 10.20.30.0/24 ]
app-lib standard-stripping vxlan udp-port 4789
app-lib standard-stripping vxlan vnid [ 400-500 ]

PFOS#  show running-config app-lib standard-stripping l2gre
app-lib standard-stripping l2gre dest-address [ 20.30.40.0/24 ]
app-lib standard-stripping l2gre l2greid [ 400-500 ]

PFOS# show running-config app-lib standard-stripping mpls
app-lib standard-stripping mpls tunnel-label [ 16-100 ]
app-lib standard-stripping mpls l2-mpls-labels 201-300
label-type vpls
pwc        false
!
app-lib standard-stripping mpls l2-mpls-labels 301-400
label-type vpws
pwc        true

PFS# show running-config ntp  | tab
SERVER                KEY
----------------------------
10.250.178.10         11
```

```
PFS# show running-config firewall
firewall rule z_ipv4_rule
 ip     216.130.207.9/22
  deny
  ingress
 description "IPv4 deny ingress rule"
!
firewall rule a_ipv6_rule
 ip     2001:db8:0:b::1a/64
  permit
  egress
 description "IPv6 permit rule"
!
PFS# show running-config firewall |tab
NAME         IP                    ACTION   DIRECTION   DESCRIPTION

------------------------------------------------------------------------
---
z_ipv4_rule  216.130.207.9/22     deny     ingress     IPv4 deny ingress
rule a_ipv6_rule  2001:db8:0:b::1a/64  permit  egress     IPv6 permit
rule

PFS# show running-config firewall
firewall rule clnt_in
ip 10.20.30.40/32 permit ingress remark "Client permit ingress"
!
firewall rule deny_in
ip 0.0.0.0/0 deny ingress remark "deny all ingress"
!
firewall rule clnt_eg
ip 10.20.30.40/32 permit egress remark "Client permit egress"
!
firewall rule deny_eg
ip 0.0.0.0/0 deny egress remark "deny all egress"
!
PFS# show running-config session
session webui idle-timeout 30
session cli idle-timeout 30

PFS# show running-config feature common-criteria-mode
feature common-criteria-mode

PFS# show running-config interface 1 eth 1-21 lldp
interface 1
 eth 1-1
   lldp rx disable
   lldp tx enable

PFOS# show running-config powersafe
powersafe 1 1
segment-name  ""
```

```
manual-mode   off
poweroff-mode bypass
!
powersafe 1 2
segment-name          Mod-1Segment-2
manual-mode           block
poweroff-mode         inpairdown
inline-network-ports [ 1-9 1-10 ]
!
powersafe 2 1
segment-name  ""
manual-mode   forward
poweroff-mode bypass
!
powersafe 2 2
segment-name          ""
manual-mode           inpairdown
poweroff-mode         block
inline-network-ports [ 1-11 1-12 ]
!
powersafe 3 1
segment-name  ""
manual-mode   bypass
poweroff-mode bypass
!

PFS# show running-config ldap-server
ldap-server                ad.example.com
 port                      636
 timeout                   10
 retransmit                1
 tls                       enable
 authenticate-certificate enable
 binding-dn             cn=ADBind,cn=Users,dc=ad,dc=example,dc=com
 binding-password          somepassword
 binding-mode              authenticated
 base-dn                   cn=Users,dc=ad,dc=example,dc=com
 user-attribute            sAMAccountName
 group-attribute           memberOf
!
PFOS(config)# do show running-config system notes
system notes Location:
               123 Circle Drive
               San Jose

             Site Contact:
               j.smith@netscout.com
               mobile: 972-555-3245
```

```
Hardware Lab
  Rack 6B
  RU 13-14
```

show sku_part_number

Show the system’s SKU part number.

Syntax

```
show sku_part_number
```

Options

None

Mode

Operational

Examples

```
PFOS# show sku_part_number
sku part number VF_01255
```

show SNMP

Show SNMP MIB information.

Syntax

```
show SNMP-mibname
```

Options

mibname	Specify MIB to display. Options are: FRAMEWORK-MIB MPD-MIB

Mode

Operational

Examples

```
PFOS# show SNMP-FRAMEWORK-MIB
SNMP-FRAMEWORK-MIB snmpEngine snmpEngineID 80:00:54:47:05:01
SNMP-FRAMEWORK-MIB snmpEngine snmpEngineBoots 2
SNMP-FRAMEWORK-MIB snmpEngine snmpEngineTime 19220
SNMP-FRAMEWORK-MIB snmpEngine snmpEngineMaxMessageSize 50000
PFOS# show SNMP-MPD-MIB
SNMP-MPD-MIB snmpMPDStats snmpUnknownSecurityModels 0
SNMP-MPD-MIB snmpMPDStats snmpInvalidMsgs 0
SNMP-MPD-MIB snmpMPDStats snmpUnknownPDUHandlers 0
```

show software

List software image files.

Syntax

```
show software [ mgmt-card ]
```

Options

mgmt-card	Management module on which to perform this command. Valid values are `mgmt-1` and `mgmt-2`. If no `mgmt-card` is specified, then perform this command on the currently active management module. Option is valid only on PFS 6010 with two management modules installed.

Mode

Operational

Examples

```
PFOS# show software

NAME                              VERSION            STATE    SIZE       TIME
TYPE
----------------------------------------------------------------------------------------------
------
vxos_5.0.0.76-61323fda-Internal  5.0.0.76-61323fda  current  209664068  Dec 4 2017 19:51:21
vxos
```

show ssh-key

Show the generated SSH RSA and ECDSA public key for the logged in user. See also: `generate ssh-key` and `delete`.

Syntax

```
show ssh-key
```

Options

None

Mode

Operational

Examples

```
PFS# show ssh-key
ssh-rsa-key ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQC0e5ELesNPVx+knXPV8cC9AxIIOFH/MZVzjMLXj4I4TLaU2xjzBT+ptkE3cfFPw
LuAQfbruGB2TrJ8TJjke7Qq+iMnJ2VNFeT+s7JwkfyfvwaIXY14DPURjPhYWZqFwhI6Y9ndeGf6tXhk9iXnKFRfNNkqTq
QxyvlEc2A23hGNnxpPfmpI7JIGkzZS9vEciA+mAfc5YsctzBuBrIj3Q0QckGK/XIWVvINJJRJKVbwnyczCamtwllBY19
bsRW6zMSx54rN4KpBLKLaDEICKASJphDLvK8KDoLvJEKTg4IyGWUiTPcjimqppbau0voR7knFCmQ5DGoiuJNap64yKkY9
root@PFS5010-115
ssh-ecdsa-key ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBCwPmKjfOZlcKNuiwRB2X8YQKWFrxR2nGEtj/tiIW
OtwOu3SzVFlImNK2YC1xlSsUCwNpm7nNUiovmt1sTyEqFc= root@PFS5010-115
```

show ssh-knownhost

List the uploaded SSH known host file details, if a file exists.

Syntax

```
show ssh-knownhost
```

Options

None

Mode

Operational

Examples

```
PFOS# show ssh-knownhost
NAME                 SIZE  TIME
-------------------------------------------------
user_knownhosts_135  587   Apr 20 2021 01:34:23
```

show sshpubkey

List the uploaded SSH public key file, if one exists.

Syntax

```
show sshpubkey
```

Options

None

Mode

Operational

Examples

```
PFOS# show sshpubkey

NAME        SIZE  TIME
----------------------------------------
id_rsa.pub  630   Dec 08 2017 00:39:16
```

show startup-config

Display information about the current startup configuration.

Syntax

```
show startup-config [ category ]
```

Options

category	Restrict to specified type of information. Type ? for a list of categories.

Mode

Operational

Examples

```
PFOS# show startup-config filter
filter jm_test
expression “IP Protocol 47”
!
```

show state

Display the system's current state. Possible values are `state OK`, `state Init` (system is initializing), and `state Failed`.

Syntax

```
show state
```

Options

None

Mode

Operational

Examples

```
PFOS# show state
state OK
```

show statistics

Display control packet, deduplication, flow, network, or port group statistics.

Syntax

```
show statistics control-packets
   [ interface slot-id [ eth port-id [ Control Packet Options ] [ reset-
time ] ]

show statistics deduplication
   [ interface slot-id [ eth port-id ] [ Deduplication Options ][ reset-
time ] ]

show statistics flow {
   interface
   map [ map_name | packets | pps]}
   map-reset-time

show statistics network
   [ interface slot-id [ eth port-id [ network-stat ] ]
   reset-time

show statistics port-group
   [ load-balance [ eth port-id [ network-stat ] ]
   [ monitor ] ]
```

Options

`interface` *`slot-id`*	Specify the line card slot number.
`eth` *`port-id`*	Specify Port ID.
`reset-time`	Display the most recent time the specified statistics were reset.
Control Packet Statistic Options	
`control-packets`	Display control packet statistics.
`Control Packet Options`	`Rx_arp_pkts`: Receive ARP packet count `Rx_icmp_pkts`: Receive ICMP packet count `Tx_arp_pkts`: Transmit ARP packet count `Tx_icmp_pkts`: Transmit ICMP packet count `drop_packets`: Excessive or checksum failure Packets `Rx-pfsmesh-pkts`: Received pfsMesh packet count `Tx-pfsmesh-pkts`: Transmitted pfsMesh packet count
Deduplication Packet Statistic Options	
`deduplication`	Display deduplication statistics.

Deduplication Options	• drop_packets: Number of erroneous packets received regardless of whether they were duplicates or not. • duplicate_packets: Number of duplicate packets received subject to the specified time window. • forwarded_packets: Number of packets forwarded over the egress interface. • input_packets: Ingress packet count.
Flow Packet Statistic Options	
flow	Display flow statistics, by either interface or map as indicated.
interface	Display port based filter statistics.
map	Display map statistics: • map-name: Traffic map name. • packets: Number of packets per traffic map. • pps: Number of packets per second processed per traffic map. **Note:** The PPS statistics are only supported on the PFS 5000/7000 series. **Notes:** • To view complete map-related statistics for specific parameters, use the command show statistics flow map. • Due to a hardware limitation, pStack+ flow map statistics for PFS 704x devices are not incremented; they will display a 0 value.
map-reset-time	Display the most recent time the traffic map statistic counters were reset.
Network Packet Statistic Options	
network	Display network statistics.
network-stat	link_recovery_count: Link recovery counter link_recovery_time: Time of last link recovery
	speed: Port speed
	rx_64: Receive 64-byte packets rx_65_to_127: Receive 65-byte to 127-byte packets rx_128_to_255: Receive 128-byte to 255-byte packets rx_256_to_511: Receive 256-byte to 511-byte packets rx_512_to_1023: Receive 512-byte to 1023-byte packets rx_1024_to_1518: Receive 1024-byte to 1518-byte packets rx_1519_to_2047 Receive 1519 bytes to 2047 bytes packets rx_1519_up: Receive packets larger than 1518 bytes rx_2048_to_4095: Receive 2048 bytes to 4095 bytes packets rx_4096_to_9216: Receive 4096 bytes to 9216 bytes packets rx_9217_up: Receive packets greater than 9216 bytes

`network-stat` (continued)	`tx_64`: Transmit 64 bytes packets `tx_65_to_127`: Transmit 65-byte to 127-byte packets `tx_128_to_255`: Transmit 128-byte to 255-byte packets `tx_256_to_511`: Transmit 256-byte to 511-byte packets `tx_512_to_1023`: Transmit 512-byte to 1023-byte packets `tx_1024_to_1518`: Transmit 1024-byte to 1518-byte packets `tx_1519_to_2047` Transmit 1519 bytes to 2047 bytes packets `tx_1519_up`: Transmit packets larger than 1518 bytes `tx_2048_to_4095`: Transmit 2048 bytes to 4095 bytes packets `tx_4096_to_9216`: Transmit 4096 bytes to 9216 bytes packets `tx_9217_up`: Transmit packets greater than 9216 bytes
	`rx_broadcast`: Receive broadcast packets `tx_broadcast`: Transmit broadcast packets
	`rx_bytes`: Receive counter bytes `tx_bytes`: Transmit counter bytes
	`rx_collisions`: Receive collision packets
	`rx_CRC_align`: Receive CRC error packets
	`rx_drop_percent`: Percentage of dropped packets out of total packets that should have been received. **Note:** This statistic is only supported on the PFS 5000/7000 series. `rx_dropped`: Receive counter drop `tx_drop_percent`: Percentage of dropped packets out of total packets that should have been transmitted. **Note:** This statistic is only supported on the PFS 5000/7000 series. `tx_dropped`: Transmit counter drop
	`rx_error_percent`: Percentage of error packets out of total packets that should have been received. **Note:** This statistic is only supported on the PFS 5000/7000 series. `rx_errors`: Receive counter errors `tx_error_percent`: Percentage of error packets out of total packets that should have been transmitted. **Note:** This statistic is only supported on the PFS 5000/7000 series. `tx_errors`: Transmit counter errors
	`rx_fragments`: Receive fragment packets `rx_jabbers`: Receive jabber packets
	`rx_multicast`: Receive multicast packets `tx_multicast`: Transmit multicast packets
	`rx_jumbo`: Receive jumbo packets `rx_oversize`: Receive oversize packets `rx_undersize`: Receive undersize packets
	`rx_packets`: Receive counter packets `tx_packets`: Transmit counter packets

network-stat (continued)	rx_peak_time: RX max utilization time tx_peak_time TX max utilization time
	Note: The PPS statistics are only supported on the PFS 5000/7000 series. rx_pps: Receive Packets Per Second (PPS) tx_pps: Transmit Packets Per Second (PPS)
	rx_throughput: Receive throughput in Mbps tx_throughput: Transmit throughput in Mbps rx_max_throughput: Receive throughput max value in Mbps tx_max_throughput: Transmit throughput max value in Mbps
	rx_unicast: Receive unicast packets tx_unicast: Transmit unicast packets
	rx_utilization: Receive utilization percentage tx_utilization: Transmit utilization percentage rx_max_utilization: RX max utilization percentage tx_max_utilization: Transmit max utilization percentage
Port Group Statistic Options **Note:** The Port Group statistics are only supported on the PFS 5000/7000 series.	
port-group	Display port group statistics.
load-balance	Display load-balance group statistics: • lgb-name: Load balance group name. • tx-pps: The total number of packets transmitted per second by the load balance group. • tx_bandwidth: Total Transmit bandwidth (Gbps) for the load balance group.
monitor	Display monitor port group statistics: • pg-name: Monitor port group name. • tx-pps: Total number of packets transmitted per second by the monitor port group. • tx_bandwidth: Total Transmit bandwidth (Gbps) for the monitor port group.
network	Display network port group statistics: • pg-name: Network port group name. • rx-pps: The total number of packets received per second by the network port group. • rx_bandwidth: Total Receive bandwidth (Gbps) for the network port group.

Mode

Operational

Examples

```
PFOS# show statistics control-packets interface 1 eth 1-1
                                       RX    TX
      RX    TX    RX    TX             PFS   PFS
PORT  ARP   ARP   ICMP  ICMP  DROP     MESH  MESH
ID    PKTS  PKTS  PKTS  PKTS  PACKETS  PKTS  PKTS
---------------------------------------------------
1-1   0     0     100   100   0        0     0


PFOS# show statistics flow map
MAP NAME               PACKETS        PPS
-----------------------------------------------
map_SSL_forward~834    2771400635326  8223134
map_SSL_forward~833    0              0
map_SSL_forward~832    2846316511439  8445414
map_SSL_forward~831    2846317736727  8445413
map_SSL_forward~830    2846318624625  8445414
map_SSL_forward~526    2771400346903  8223136


PFOS# show statistics flow map map_name map_SSL_forward~834
MAP NAME             PACKETS        PPS
-----------------------------------------
map_SSL_forward~834  2771400635326  8223134


PFOS# show statistics deduplication interface 1 eth 1-1
PORT  INPUT    DUPLICATE  DROP     FORWARDED
ID    PACKETS  PACKETS    PACKETS  PACKETS
----------------------------------------------
1-1   0        423          3893       0


PFOS# show statistics deduplication interface 1 eth 1-1 drop_packets
drop packets 3893
PFOS# show statistics deduplication interface 1 eth 1-1 duplicate_packets
duplicate packets 423


PFOS# show statistics network interface 1
statistics network interface 1

 reset time "Fri Sep  1 16:17:07 2023\n"
 eth 1-1
  speed          10000
  rx packets     61458422392
  rx errors      0
  rx dropped     0
  rx throughput  8648.73
  rx utilization 100.0
  tx packets     0
  tx errors      0
  tx dropped     0
  tx throughput  0.0
  tx utilization 0.0
 eth 1-2
  speed          10000
  rx packets     0
  rx errors      0
  rx dropped     0
  rx throughput  0.0
  rx utilization 0.0
  tx packets     59551785832
  tx errors      0
  tx dropped     0
  tx throughput  8420.95
  tx utilization 97.36
   . . .
PFOS# show statistics network interface 1 eth 1-7
eth 1-7
 speed          10000
 rx packets     355167
 rx errors      0
 rx dropped     0
 rx throughput  0.0
 rx utilization 0.0
 tx packets     1422475535270
 tx errors      0
 tx dropped     0
 tx throughput  0.0
 tx utilization 0.0

PFOS# show statistics network interface 1 eth 1-31 rx_pps
rx pps 8438717
PFOS# show statistics network interface 1 eth 1-11 tx_pps
tx pps 8215899


PFOS# show statistics network interface 1 eth 1-31.1 rx_drop_percent
rx drop percent 0.0
PFOS# show statistics network interface 1 eth 1-31.1 rx_error_percent
rx error percent 0.0
PFOS# show statistics network interface 1 eth 1-31.2 tx_drop_percent
tx drop percent 0.0
PFOS# show statistics network interface 1 eth 1-31.2 tx_error_percent
tx error percent 0.0
```

```
PFOS# show statistics port-group
PG               RX         RX
NAME             PPS        BANDWIDTH(Gbps)
-------------------------------------------
NW_PortGroup1    0          0.0

                                          TX
PG NAME                         TX PPS    BANDWIDTH(Gbps)
-----------------------------------------------------------
inline_passive_MPG              25318879  25.92
inline_replacement_passive_MPG  0         0.0

                                      TX
LBG NAME                     TX PPS   BANDWIDTH(Gbps)
-------------------------------------------------------
inline_toochain_passive_LBG  8452971  8.65
```

show statistics tunnel

Display GRE or VXLAN tunnel statistics. Refer to the ***PFOS 6.x User Guide*** for GRE and VXLAN Tunnel Origination/Termination feature details.

Note: Due to a hardware limitation, pStack+ tunnel statistics for PFS 704x devices are not incremented; they will display a 0 value.

Syntax

```
Show statistics tunnel gre
Show statistics tunnel vxlan
Show statistics tunnel reset-time
```

Options

`arp-req-sent`	Number of ARP Requests sent.
`arp-res-recv`	Number of ARP Response received.
`gre-tunnel-name`	Display the statistics for the specified GRE tunnel.
`vxlan-tunnel-name`	Display the statistics for the specified VXLAN tunnel.
`packet-rx`	Number of L2GRE or VXLAN packets received.
`packet-tx`	Number of L2GRE or VXLAN packets sent.
`rx-pps`	**Note:** This statistic is only supported on the PFS 5000/7000 series. Number of L2GRE or VXLAN packets received per second.
`tx-pps`	**Note:** This statistic is only supported on the PFS 5000/7000 series. Number of L2GRE or VXLAN packets transmitted per second.
`reset-time`	Display the most recent time the specified statistics were reset.

Mode

Operational

Examples

```
PFOS# show statistics tunnel gre

                             ARP   ARP
                             REQ   RES   PACKET  PACKET  TX    RX
GRE TUNNEL NAME              SENT  RECV  TX      RX      PPS   PPS
--------------------------------------------------------------------
GRE-tunnel-mac-unresolved    32    0     0       0       0     0
GRE_3333_gateway_1111        1     1     95702   0       1038  0
GRE_4444_gateway_1111        1     1     95604   0       1038  0
GRE_9999_port49_gateway1111  32    0     0       0       0     0
```

```
PFOS# show statistics tunnel vxlan
                           ARP   ARP
                           REQ   RES   PACKET  PACKET  TX    RX
VXLAN TUNNEL NAME          SENT  RECV  TX      RX      PPS   PPS
-------------------------------------------------------------------
vxlan_1-49_gateway1111     32    0     0       0       0     0
vxlan_1-9_tunnel1          32    0     0       0       0     0
vxlan_tunnel_1111_gateway  1     1     95533   0       1038  0
vxlan_tunnel_1113          1     1     95461   95457   1038  1039
vxlan_tunnel_1114          1     1     95387   0       1038  0
vxlan_tunnel_1115          1     1     94744   0       1038  0
vxlan_tunnel_2223_gateway  1     1     95309   0       1038  0


PFOS# show statistics tunnel vxlan vxlan-tunnel-name vxlan_tunnel_2223_gateway
                           ARP   ARP
                           REQ   RES              PACKET  TX    RX
VXLAN TUNNEL NAME          SENT  RECV  PACKET TX  RX      PPS   PPS
---------------------------------------------------------------------
vxlan_tunnel_2223_gateway  1     1     174896623  0       1059  0
```

show stripping mpls

Display the number of MPLS labels automatically defined by PFOS per port. See *Configure standard MPLS Stripping* in the PFOS 6.x User Guide for configuration details.

Syntax

```
show stripping mpls
```

Options

None

Mode

Operational

Examples

```
show stripping mpls
RX        LABEL     LABEL
PORT ID             TYPE
-------------------------------
41        100       l3_mpls
41        1000      l2_mpls
41        200       l3_mpls
41        300       l3_mpls
```

Field Descriptions

Rx Port ID	Port ID receiving incoming traffic used to program labels.
Label	Number of labels programmed by PFOS for the specified port.
Label Type	Specifies whether programmed labels are L2 (Ethernet over MPLS) or L3 (IP over MPLS).

show system

Display system settings.

Syntax

```
show system [ { disk-usage [ mgmt-card ] [ install | data ] |
    log [ audit | boot | browser | filter | framework | kernel | mgmt-
card | netconf | snmp ] | productID | serial_number } |
    pstack-version ]
```

Options

`disk-usage`	Restrict output to percentage of disk space in use on the currently active management card. The disk has two partitions: • `install` - Percentage of total disk space for system files (unreachable by users). It is the location for system execution files, including PFOS installation images. This value displays as "System Disk Usage" on the System Information page on the WebUI. • `data` - Percentage of total disk space that is accessible by users. It is the location for various log files, uploaded files (images, config, license, certificate etc.), and system core dump files. This value displays as "Data Disk Usage" on the System Information page on the WebUI.
`log`	Show log for a specified area. Each option provides two format options: JavaScript Object Notation (JSON) or raw data. • **audit** - Display the audit log • **boot** - Display data from current boot • **browser** - Display the browser log • **filter** - Display the filtering resources log • **framework** - Display the framework related log • **kernel** - Display the kernel messages from current boot • **mgmt-card** - *Option is valid only on PFS 6010 with two management modules installed.* If `mgmt-card` is specified, then specify the management module on which to perform this command. Valid values are `mgmt-1` and `mgmt-2`. If no `mgmt-card` is specified, then perform this command on the currently active management module. • **netconf** - Display the Netconf related log • **snmp** - Display the SNMP related log messages
`productID`	Restrict output to display product ID.
`system platform`	Restrict output to display hardware platform.
`system software platform`	Restrict output to display software platform.
`serial_number`	Restrict output to serial number.
`pstack-version`	Show version of the pStack protocol running on this system. Refer to the "pfsMesh pStack Protocol Requirements" section in the ***PFOS User Guide*** for details.

Mode

Operational

Examples

```
PFS5010_117# show system
system serial number PF3200375053
system productID  5812
system platform   PFS5010
system software platform PFS7010
system disk-usage install 13%
system disk-usage data 16%
system pstack version 30.1


PFOS# show system serial_number
system serial number 14100444


PFOS# show system disk-usage

system disk-usage install 11%

system disk-usage data 54%


PFOS# show system pstack-version

system pstack version 30.1

PFS5040-32D# show system log filter

+++++++++++++++++++++++++++++++++Filter Resources+++++++++++++++++++++++++++++++++++
+----------------------------------------------------------------------------------+
+ UDF Information(in units of bytes):  0 Used/19 Supported                         +
+----------------------------------------------------------------------------------+
+          UDF Type |  Chunks Used |   Max Chunks |  C_4B |  C_2B |  C_1B |        +
+----------------------------------------------------------------------------------+
+               MAC |            0 |            4 |     0 |     7 |     5 |        +
+                L4 |            0 |           12 |     0 |     7 |     5 |        +
+        L2WITHVLAN |            0 |           12 |     0 |     7 |     5 |        +
+         UNKNOWNL3 |            0 |           11 |     0 |     7 |     5 |        +
+              MPLS |            0 |           12 |     0 |     7 |     5 |        +
+              IPv4 |            0 |           12 |     0 |     7 |     5 |        +
+              IPv6 |            0 |            4 |     0 |     7 |     5 |        +

+         UNKNOWNL4 |            0 |           12 |     0 |     7 |     5 |        +
+               GRE |            0 |           12 |     0 |     7 |     5 |        +
+----------------------------------------------------------------------------------+
+                                                                                  +
+ Ranges Used/Supported:  0 / 32                                                   +
+----------------------------------------------------------------------------------+
+ TCAM Information:                                                                +
+  Group|  Priority| TCAM Total| TCAM Used| TCAM Free| Bits Used|       Group Mode +
+----------------------------------------------------------------------------------+
+----------------------------------------------------------------------------------+
+ PIPE: 1 (#1-9 to #1-12 and #1-21 to #1-24)                                       +
+----------------------------------------------------------------------------------+
+     10|     7fff5|      12287|         4|     12283|       262|           Double +
+----------------------------------------------------------------------------------+
+----------------------------------------------------------------------------------+
+----------------------------------------------------------------------------------+
+ PIPE: 2 (#1-1 to #1-8)                                                           +
+----------------------------------------------------------------------------------+
+     11|     7fff4|      10239|         4|     10235|       262|           Double +
+----------------------------------------------------------------------------------+
+     30|     7ffe1|      20479|         1|     20478|        58|           Single +
+----------------------------------------------------------------------------------+
+----------------------------------------------------------------------------------+
+----------------------------------------------------------------------------------+
+ PIPE: 3 (#1-13 to #1-20)                                                         +
+----------------------------------------------------------------------------------+
+     12|     7fff3|      12287|         4|     12283|       262|           Double +
+----------------------------------------------------------------------------------+
+----------------------------------------------------------------------------------+
+----------------------------------------------------------------------------------+
+ PIPE: 4 (#1-25 to #1-32)                                                         +
+----------------------------------------------------------------------------------+
+     13|     7fff2|      12287|         4|     12283|       262|           Double +
+----------------------------------------------------------------------------------+
+----------------------------------------------------------------------------------+
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
MODE: legacy
Status: ALL FLOWS ARE IN WORKING STATE
```

show system-alarms

Show one alarm entry. If no options are specified, then list all alarm entries.

Syntax

```
show system-alarms [ alarm-unit ] [ ack-timestamp | acknowledge |
     fail-timestamp | message | status | unit-name ]
```

Options

`alarm-unit`	Restrict output to a specific alarm unit. Press `?` for a list of available alarm unit.
`ack-timestamp`	Display only the ack-timestamp column.
`acknowledge`	Display only the acknowledge column.
`fail-timestamp`	Display only the fail-timestamp column.
`message`	Display only the message column.
`status`	Display only the status column.
`unit-name`	Display only the unit-name column.

Mode

Operational

Examples

```
PFOS# show system-alarms fan-01
                       FAIL       ACK
UNIT    UNIT NAME      TIMESTAMP  TIMESTAMP  STATUS  MESSAGE  ACKNOWLEDGE
---------------------------------------------------------------------------
fan-01  Blower tray 1                        ok               false

PFSOS# show system-alarms fan-02 status
status ok
```

```
PFOS# show system-alarms
system-alarms core-file
 unit name      "Core file"
 fail timestamp ""
 ack timestamp  ""
 status         ok
 message        ""
 acknowledge    false
system-alarms fan-01
 unit name      "Blower tray 1"
. . .
```

show tech-support

Display information for use by Technical Support. Performing this command might take some time.

Syntax

```
show tech-support [ mgmt-card ]
```

Options

mgmt-card	Management module on which to perform this command. Valid values are `mgmt-1` and `mgmt-2`. If no `mgmt-card` is specified, then perform this command on the currently active management module. Option is valid only on PFS 6010 with two management modules installed.

Mode

Operational, Configuration

Examples

```
PFOS# show tech-support
```

To save output to a file:

```
PFOS# show tech-support mgmt-2 | save my_tech_support.log
```

show trigger

Display trigger information; see `show remote-trigger` for triggers visible in pfsMesh. See `trigger` for configuration details.

Syntax

```
show trigger
```

Options

None

Mode

Operational, Configuration

Examples

```
PFOS# show trigger
                                          CONFLICTING  CONFLICTING
NAME      STATUS    PFS MESH STATUS       NODE ID      NODE NAME
----------------------------------------------------------------------
Trigger1  inactive  TriggerNameConflicts  FFB99E00     PFS-5010-119
Trigger2  inactive  TriggerNameResolved
combo_T1  active    TriggerNameResolved

PFOS# show trigger Trigger1
                                          CONFLICTING  CONFLICTING
NAME      STATUS    PFS MESH STATUS       NODE ID      NODE NAME
----------------------------------------------------------------------
Trigger1  inactive  TriggerNameConflicts  FFB99E00     PFS-5010-119
```

Field Descriptions

`name`	Trigger name
`status`	**Active**: indicates the condition defined in the trigger **has** occurred. **Inactive**: indicates the condition defined in the trigger has **not yet** occurred.
`pfsMesh status`	Trigger name resolution status as Resolved or Conflicts. Updated by pStack protocol.
`conflicting node id`	If pfsMesh status is TriggerNameConflicts, then this field reflects the node ID with which the conflict exists.
`conflicting node name`	If pfsMesh status is TriggerNameConflicts, then this field reflects the node name with which the conflict exists.

show uptime

Show how long the system has been up.

Syntax

```
show uptime [ mgmt-card ]
```

Options

`mgmt-card`	Management module on which to perform this command. Valid values are `mgmt-1` and `mgmt-2`. If no `mgmt-card` is specified, then perform this command on the currently active management module. Option is valid only on PFS 6010 with two management modules installed.

Mode

Operational

Examples

```
PFOS# show uptime
uptime "12 days, 5 hours, 16 mins and 16 seconds"
```

show username

Display list of all configured users, date last password changed, and their password expiration date.

Syntax

```
show username [ user ] [ last-password-change | password-expires |
invalid-login-attempts-count | first-invalid-login-time |account-lock-
time]
```

Options

`user`	Display information only for this username. If no `user` is specified, then display information for all configured users.
`last-password-change`	If specified, then display only the date of most recent password change.
`password-expires`	If specified, then display only the date of password expiration.
`invalid-login-attempts-count`	If specified, then display only the number of invalid login attempts.
`first-invalid-login-time`	If specified, then display only the timestamp of the first invalid login.
`account-lock-time`	If specified, then display only the timestamp of when the account was locked.

Mode

Operational

Examples

```
PFOS# show username

                                   INVALID   FIRST

        LAST                       LOGIN     INVALID  ACCOUNT

        PASSWORD     PASSWORD      ATTEMPTS  LOGIN    LOCK

NAME    CHANGE       EXPIRES       COUNT     TIME     TIME

--------------------------------------------------------------

admin  Jan 1, 2001   May 18, 2028  0         -        -
user1  Mar 26, 2019  Aug 10, 2045  0         -        -

PFOS# show username user1show
          LAST
          PASSWORD      PASSWORD
```

```
NAME      CHANGE        EXPIRES
--------------------------------------
user1     Mar 26, 2018  Aug 10, 2045
```

```
PFOS# show username last-password-change
          LAST
          PASSWORD
NAME      CHANGE
------------------------
admin     Mar 21, 2019
user1     Mar 26, 2019

PFOS# show username user1 password-expires
password expires "Aug 10, 2045"
```

show version

Display system version information.

Syntax

```
show version [ mgmt-card ]
```

Options

`mgmt-card`	Management module on which to perform this command. Valid values are `mgmt-1` and `mgmt-2`. If no `mgmt-card` is specified, then perform this command on the currently active management module. Option is valid only on PFS 6010 with two management modules installed.

Mode

Operational, Configuration

Examples

```
PFOS# show version

/***************************************************
 * Vendor:         NETSCOUT
 * Platform:       PFS5010
 * Versions:
 *                 vxos_core   0.433
 *                 vxos_cfg    7.4.5
 *                 vxos        6.1.2.26-60e8b99f
 *                 pstack      30.1
 * Date created:
 *                 2022-02-05 17:17:49 UTC
 ***************************************************/
```

show vlan-translation-table

Note: Due to a hardware limitation, the `show vlan-translation-table` command returns invalid data for the 5040/7040-32D and 5041/7041-32D devices. This command should not be used for these devices.

On egress ports, if a packet's VLAN matches the “pStack VLAN” it is replaced by the custom user-defined VLAN for that port. This table maps the pStack VLAN IDs assigned by the pStack protocol to their respective custom user-defined VLAN IDs. Every node in the pfsMesh maintains a copy of this table.

Syntax

```
show vlan-translation-table
```

Options

None

Mode

Operational

Examples

```
PFS# show vlan-translation-table
P       USER
STACK   DEFINED
VLAN    VLAN
----------------
3104    660
3105    1222
3113    1324
```

NETSCOUT SYSTEMS, INC.
310 Littleton Road
Westford, MA 01886-4105
Tel. 978 614-4000
+1-888-357-7667
Fax 978-614-4004
Web www.netscout.com

NETSCOUT SYSTEMS, INC. All rights reserved.